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 (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 opciones).

**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 opciones).

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 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 opciones).

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 opciones).

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 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 opciones).

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.

31.- Una empresa tiene cientos de cuentas de AWS dentro de una organización gestionada con AWS Organizations. La empresa opera en una sola región de AWS. Cuenta con una cuenta dedicada a herramientas de seguridad, la cual está configurada como administrador delegado de la organización tanto para Amazon GuardDuty como para AWS Security Hub.

El entorno está configurado para habilitar automáticamente GuardDuty y Security Hub en las cuentas de AWS existentes y también en las nuevas.

La empresa está realizando pruebas de control sobre ciertos hallazgos (findings) de GuardDuty para asegurarse de que el equipo de seguridad pueda detectar y responder a eventos de seguridad. Como parte de la prueba, el equipo de seguridad lanzó una instancia de Amazon EC2 e intentó hacer solicitudes DNS contra un dominio de prueba, example.com, para generar un hallazgo relacionado con DNS.

Sin embargo, el hallazgo nunca fue generado en la cuenta del administrador delegado de Security Hub.

¿Por qué no se generó el hallazgo en la cuenta del administrador delegado de Security Hub?

A. Los VPC Flow Logs no estaban habilitados para la VPC donde se lanzó la instancia EC2.

**B. La VPC donde se lanzó la instancia EC2 tenía configurada una opción DHCP con un resolvedor OpenDNS personalizado.**

C. La integración de GuardDuty con Security Hub nunca fue activada en la cuenta de AWS donde se generó el hallazgo.

D. La agregación entre regiones (Cross-Region aggregation) en Security Hub no fue configurada.

32.- Una empresa de comercio electrónico tiene una arquitectura de aplicación web que se ejecuta principalmente en contenedores. Los contenedores de la aplicación están desplegados en Amazon Elastic Container Service (Amazon ECS). Las imágenes de los contenedores de la aplicación se almacenan en Amazon Elastic Container Registry (Amazon ECR).

El equipo de seguridad de la empresa está realizando una auditoría de los componentes de la arquitectura de la aplicación. Durante esta auditoría, identifican problemas en algunas imágenes de contenedores almacenadas en los repositorios.

El equipo de seguridad quiere resolver estos problemas implementando un escaneo continuo y un escaneo al momento del push (on-push) de las imágenes. Además, necesitan una solución que les permita visualizar los hallazgos de estos escaneos en un panel de control centralizado. Planean usar este panel para ver estos hallazgos junto con otros hallazgos de seguridad que generarán en el futuro. También hay ciertos repositorios que necesitan excluir del proceso de escaneo.

¿Qué solución cumplirá con estos requisitos?

**A. Usar Amazon Inspector. Crear reglas de inclusión en Amazon ECR para que coincidan con los repositorios que deben ser escaneados. Enviar los hallazgos de Amazon Inspector a AWS Security Hub.**

B. Usar el escaneo básico de imágenes de contenedor de ECR. Crear reglas de inclusión en Amazon ECR para que coincidan con los repositorios que deben ser escaneados. Enviar los hallazgos a AWS Security Hub.

C. Usar el escaneo básico de imágenes de contenedor de ECR. Crear reglas de inclusión en Amazon ECR para que coincidan con los repositorios que deben ser escaneados. Enviar los hallazgos a Amazon Inspector.

D. Usar Amazon Inspector. Crear reglas de inclusión en Amazon Inspector para que coincidan con los repositorios que deben ser escaneados. Enviar los hallazgos de Amazon Inspector a AWS Config.

33.- Una empresa tiene una única cuenta de AWS y utiliza una instancia de Amazon EC2 para probar código de aplicaciones.

Recientemente, la empresa descubrió que la instancia fue comprometida y estaba sirviendo malware.

El análisis reveló que la instancia fue comprometida hace 35 días.

Un ingeniero de seguridad debe implementar una solución de monitoreo continuo que notifique automáticamente al equipo de seguridad de la empresa mediante una lista de distribución por correo electrónico cuando se detecten hallazgos de alta severidad.

El ingeniero debe implementar la solución lo antes posible.

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

A. Habilitar AWS Security Hub en la cuenta de AWS.

**B. Habilitar Amazon GuardDuty en la cuenta de AWS.**

**C. Crear un tema (topic) de Amazon Simple Notification Service (Amazon SNS). Suscribir la lista de distribución de correos electrónicos del equipo de seguridad a ese tema.**

D. Crear una cola de Amazon Simple Queue Service (Amazon SQS). Suscribir la lista de distribución del equipo de seguridad a la cola.

**E. Crear una regla de Amazon EventBridge para hallazgos de alta severidad de GuardDuty. Configurar la regla para que publique un mensaje en el tema SNS.**

F. Crear una regla de Amazon EventBridge para hallazgos de alta severidad de Security Hub. Configurar la regla para que publique un mensaje en la cola.

34.- Una empresa utiliza federación de identidad para autenticar usuarios en una cuenta de identidad (987654321987), donde los usuarios asumen un rol de IAM llamado IdentityRole. Luego, los usuarios asumen un rol de IAM llamado JobFunctionRole en la cuenta de destino de AWS (123456789123) para realizar sus funciones laborales.

Un usuario no puede asumir el rol de IAM en la cuenta de destino. La política adjunta al rol en la cuenta de identidad es:

¿Qué se debe hacer para permitir que el usuario asuma el rol adecuado en la cuenta de destino?

A. Actualizar la política de IAM adjunta al rol en la cuenta de identidad a:

**B. Actualizar la política de confianza (trust policy) del rol en la cuenta de destino a:**

C. Actualizar la política de confianza del rol en la cuenta de identidad a:

D. Actualizar la política de IAM adjunta al rol en la cuenta de destino a:

35.- Una empresa está utilizando AWS Organizations para gestionar varias cuentas de AWS correspondientes a sus departamentos de recursos humanos, finanzas, desarrollo de software y producción. Todos los desarrolladores de la empresa forman parte de la cuenta de desarrollo de software.

La empresa descubre que los desarrolladores han lanzado instancias de Amazon EC2 preconfiguradas con software que no está aprobado para su uso. La empresa quiere implementar una solución que garantice que los desarrolladores solo puedan lanzar instancias EC2 con aplicaciones de software aprobadas y únicamente dentro de la cuenta de desarrollo de software.

¿Qué solución cumplirá con estos requisitos?

A. En la cuenta de desarrollo de software, crea imágenes AMI de instancias preconfiguradas que incluyan solo el software aprobado. Incluye los IDs de las AMI en la sección de condiciones de una plantilla de AWS CloudFormation para lanzar la AMI apropiada según la región de AWS. Proporciona a los desarrolladores la plantilla de CloudFormation para lanzar instancias EC2 en la cuenta de desarrollo de software.

B. Crea una regla de Amazon EventBridge que se active cuando ocurra cualquier evento de la API RunInstances de EC2 en la cuenta de desarrollo de software. Especifica AWS Systems Manager Run Command como destino de la regla. Configura Run Command para ejecutar un script que instale todo el software aprobado en las instancias lanzadas por los desarrolladores.

**C. Usa un portafolio de AWS Service Catalog que contenga productos EC2 con AMIs apropiadas que incluyan solo el software aprobado. Concede a los desarrolladores permisos para acceder únicamente al portafolio del Service Catalog y lanzar productos dentro de la cuenta de desarrollo de software.**

D. En la cuenta de administración, crea AMIs de instancias preconfiguradas que incluyan solo el software aprobado. Usa AWS CloudFormation StackSets para lanzar las AMIs en cualquier cuenta de AWS de la organización. Concede a los desarrolladores permisos para lanzar los stack sets dentro de la cuenta de administración.

36.- Una empresa ha habilitado Amazon GuardDuty en todas las regiones de AWS como parte de su estrategia de monitoreo de seguridad. En una de sus VPC, la empresa aloja una instancia de Amazon EC2 que funciona como servidor FTP. Un gran número de clientes desde múltiples ubicaciones se conecta al servidor FTP. GuardDuty detecta esta actividad como un ataque de fuerza bruta debido al alto número de conexiones que se producen cada hora.

La empresa ha marcado este hallazgo como un falso positivo, pero GuardDuty sigue generando alertas. Un ingeniero de seguridad debe mejorar la relación señal-ruido sin comprometer la visibilidad de comportamientos anómalos potenciales.

¿Qué solución cumple con estos requisitos?

A. Desactivar la regla de FTP en GuardDuty en la región donde se encuentra el servidor FTP.

B. Agregar el servidor FTP a una lista de IPs confiables. Implementar esta lista en GuardDuty para dejar de recibir notificaciones.

**C. Crear una regla de supresión en GuardDuty para filtrar hallazgos, archivando automáticamente los nuevos hallazgos que coincidan con los criterios especificados.**

D. Crear una función de AWS Lambda con permisos adecuados para eliminar el hallazgo cada vez que se reporte una nueva ocurrencia.

37.- Una empresa ejecuta microservicios internos en Amazon Elastic Container Service (Amazon ECS) utilizando el tipo de lanzamiento Amazon EC2. La empresa usa repositorios privados de Amazon Elastic Container Registry (Amazon ECR).

Un ingeniero de seguridad necesita cifrar los repositorios privados usando AWS Key Management Service (AWS KMS). Además, debe analizar las imágenes de contenedor en busca de vulnerabilidades y exposiciones comunes (CVEs).

¿Qué solución cumplirá con estos requisitos?

A. Habilitar el cifrado con KMS en los repositorios de ECR existentes. Instalar el agente de Amazon Inspector desde los user data de las instancias ECS. Ejecutar una evaluación usando las reglas de CVE.

**B. Recree los repositorios de ECR con cifrado KMS y escaneo de ECR habilitado. Analizar el informe de escaneo después del próximo envío de imágenes.**

C. Volver a crear los repositorios de ECR con cifrado KMS y escaneo de ECR habilitado. Instalar el agente de AWS Systems Manager en las instancias ECS. Ejecutar un informe de inventario.

D. Habilitar el cifrado con KMS en los repositorios de ECR existentes. Usar AWS Trusted Advisor para revisar las instancias ECS y verificar los hallazgos en comparación con una lista de CVEs actuales.

38.- Un ingeniero de seguridad de una empresa ha recibido la tarea de restringir el acceso de la cuenta IAM de un contratista a solo la consola de Amazon EC2, sin permitirle acceso a ningún otro servicio de AWS. La cuenta IAM del contratista no debe poder obtener acceso a ningún otro servicio de AWS, incluso si se le asignan permisos adicionales por pertenecer a un grupo de IAM.

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

A. Crear una política IAM inline (incrustada) para el usuario IAM del contratista que permita el acceso a Amazon EC2.

**B. Crear una política de límite de permisos (permissions boundary) que permita acceso a Amazon EC2. Asociar la cuenta IAM del contratista con esta política de límite de permisos.**

C. Crear un grupo IAM con una política adjunta que permita el acceso a Amazon EC2. Asociar la cuenta IAM del contratista a ese grupo.

D. Crear un rol IAM que permita acceso a EC2 y deniegue explícitamente todos los demás servicios. Indicar al contratista que siempre debe asumir ese rol.

39.- Una empresa gestiona múltiples cuentas de AWS usando AWS Organizations. El equipo de seguridad de la empresa ha notado que algunas cuentas miembro no están enviando los registros de AWS CloudTrail a un bucket centralizado de Amazon S3. El equipo de seguridad quiere asegurarse de que haya al menos un trail (rastro) configurado en todas las cuentas existentes y en cualquier cuenta que se cree en el futuro.

¿Qué conjunto de acciones debería implementar el equipo de seguridad para lograr esto?

A. Crear un nuevo trail y configurarlo para que envíe los registros de CloudTrail a Amazon S3. Usar Amazon EventBridge para enviar una notificación si se elimina o detiene un trail.

B. Implementar una función de AWS Lambda en cada cuenta para verificar si existe un trail, y crear uno nuevo si es necesario.

**C. Editar el trail existente en la cuenta de administración de Organizations y aplicarlo a toda la organización.**

D. Crear una SCP (política de control de servicio) para denegar las acciones cloudtrail:Delete\* y cloudtrail:Stop\*. Aplicar la SCP a todas las cuentas.

40.- Una empresa tuvo recientemente una auditoría de seguridad, en la cual los auditores identificaron múltiples amenazas potenciales. Estas amenazas pueden provocar cambios en los patrones de uso, como picos de acceso DNS, tráfico anormal en instancias, tráfico inusual en interfaces de red y llamadas atípicas a la API de Amazon S3. Las amenazas pueden provenir de distintas fuentes y ocurrir en cualquier momento. La empresa necesita implementar una solución que supervise continuamente su sistema y detecte todas estas amenazas entrantes casi en tiempo real.

¿Qué solución cumple con estos requisitos?

A. Habilitar los registros de AWS CloudTrail, los registros de flujo de VPC y los registros DNS. Usar Amazon CloudWatch Logs para administrar estos registros desde una cuenta centralizada.

B. Habilitar los registros de AWS CloudTrail, los registros de flujo de VPC y los registros DNS. Usar Amazon Macie para monitorear estos registros desde una cuenta centralizada.

**C. Habilitar Amazon GuardDuty desde una cuenta centralizada. Usar GuardDuty para administrar los registros de AWS CloudTrail, registros de flujo de VPC y registros DNS.**

D. Habilitar Amazon Inspector desde una cuenta centralizada. Usar Amazon Inspector para administrar los registros de AWS CloudTrail, registros de flujo de VPC y registros DNS.

41.- Una empresa que utiliza AWS Organizations está usando AWS IAM Identity Center (anteriormente AWS Single Sign-On) para administrar el acceso a las cuentas de AWS. Un ingeniero de seguridad está creando un conjunto de permisos personalizado (permission set) en IAM Identity Center. La empresa planea usar este conjunto de permisos en varias cuentas.

Al conjunto de permisos se le han asignado una política administrada por AWS y una política administrada por el cliente. El ingeniero de seguridad tiene permisos administrativos completos y está operando desde la cuenta de administración.

Sin embargo, cuando intenta asignar ese conjunto de permisos a un usuario de IAM Identity Center que tiene acceso a múltiples cuentas, la asignación falla.

¿Qué debe hacer el ingeniero de seguridad para resolver este error?

**A. Crear la política administrada por el cliente en cada cuenta donde se va a asignar el conjunto de permisos. Asegurarse de que la política tenga el mismo nombre y los mismos permisos en cada cuenta.**

B. Eliminar la política administrada por AWS o la política administrada por el cliente del conjunto de permisos. Crear un segundo conjunto de permisos que contenga la política eliminada. Aplicar ambos conjuntos de permisos por separado al usuario.

C. Evaluar la lógica de ambas políticas (la administrada por AWS y la administrada por el cliente) y resolver cualquier conflicto dentro del conjunto de permisos antes de implementarlo.

D. No agregar el nuevo conjunto de permisos al usuario. En su lugar, editar el conjunto de permisos existente del usuario para incluir tanto la política administrada por AWS como la del cliente.

42.- Una empresa tiene miles de funciones AWS Lambda. Al revisar estas funciones, un ingeniero de seguridad descubre que se está almacenando información sensible en las variables de entorno y que esta información puede verse en texto plano desde la consola de Lambda. Los valores de esa información sensible tienen solo unos pocos caracteres.

¿Cuál es la forma MÁS rentable de resolver este problema de seguridad?

A. Configurar políticas de IAM desde la consola de Lambda para ocultar el acceso a las variables de entorno.

B. Usar AWS Step Functions para almacenar las variables de entorno. Acceder a las variables en tiempo de ejecución. Usar permisos de IAM para restringir el acceso únicamente a las funciones Lambda que lo necesiten.

C. Almacenar las variables de entorno en AWS Secrets Manager y acceder a ellas en tiempo de ejecución. Usar permisos de IAM para restringir el acceso a los secretos únicamente a las funciones Lambda que lo necesiten.

**D. Almacenar las variables de entorno en AWS Systems Manager Parameter Store como parámetros seguros y acceder a ellos en tiempo de ejecución. Usar permisos de IAM para restringir el acceso a los parámetros únicamente a las funciones Lambda que lo necesiten.**

43.- Un ingeniero de seguridad está utilizando AWS Organizations y quiere optimizar las políticas de control de servicio (SCPs).

El ingeniero necesita asegurarse de que las SCPs cumplan con las mejores prácticas.

¿Qué enfoque debe tomar el ingeniero de seguridad para cumplir con este requisito?

**A. Usar AWS IAM Access Analyzer para analizar las políticas. Ver los hallazgos de las validaciones de políticas.**

B. Revisar las verificaciones de AWS Trusted Advisor para todas las cuentas de la organización.

C. Configurar AWS Audit Manager. Ejecutar una evaluación en todas las regiones de AWS para todas las cuentas.

D. Asegurarse de que los agentes de Amazon Inspector estén instalados en todas las instancias de Amazon EC2 de todas las cuentas.

44.- Una empresa utiliza Amazon RDS para MySQL como motor de base de datos para sus aplicaciones. Una auditoría de seguridad reciente reveló una instancia de RDS que no cumple con la política de la empresa respecto al cifrado de datos en reposo. Un ingeniero de seguridad de la empresa necesita asegurarse de que todas las bases de datos RDS existentes estén cifradas usando cifrado del lado del servidor y que cualquier desviación futura de esta política sea detectada.

¿Qué combinación de pasos debería seguir el ingeniero de seguridad para lograr esto? (Elige dos.)

**A. Crear una regla de AWS Config para detectar la creación de bases de datos RDS sin cifrado. Crear una regla de Amazon EventBridge que se active ante cambios en el estado de cumplimiento de las reglas de AWS Config y usar Amazon SNS (Simple Notification Service) para notificar al equipo de operaciones de seguridad.**

B. Usar AWS Systems Manager State Manager para detectar desviaciones en la configuración de cifrado de las bases de datos RDS. Crear una regla de Amazon EventBridge para rastrear los cambios de estado y usar Amazon SNS para notificar al equipo de operaciones de seguridad.

C. Crear una réplica de lectura (read replica) de la base de datos RDS no cifrada y habilitar el cifrado durante el proceso. Una vez que la réplica esté activa, promoverla como una instancia independiente y eliminar la instancia de base de datos no cifrada.

**D. Tomar una instantánea (snapshot) de la base de datos RDS no cifrada. Copiar la instantánea y habilitar el cifrado durante el proceso. Restaurar la instancia de base de datos a partir de la nueva instantánea cifrada. Terminar la instancia no cifrada.**

E. Habilitar el cifrado para la instancia RDS identificada como no cifrada cambiando su configuración existente.

45.- Una empresa se ha recuperado recientemente de un incidente de seguridad que requirió la restauración de instancias de Amazon EC2 a partir de snapshots. La empresa utiliza una clave administrada por el cliente de AWS Key Management Service (AWS KMS) para cifrar todas las snapshots de Amazon Elastic Block Store (Amazon EBS).

La empresa realiza un análisis de brechas sobre sus procedimientos de recuperación ante desastres y estrategias de respaldo. Un ingeniero de seguridad necesita implementar una solución que permita a la empresa recuperar las instancias EC2 en caso de que la cuenta de AWS sea comprometida y se eliminen las snapshots de EBS.

¿Qué solución cumplirá con este requisito?

A. Crear un nuevo bucket de Amazon S3. Usar políticas de ciclo de vida de EBS para mover las snapshots de EBS al nuevo bucket de S3. Utilizar políticas de ciclo de vida para trasladar las snapshots a la clase de almacenamiento S3 Glacier Instant Retrieval. Usar S3 Object Lock para evitar que se eliminen las snapshots.

B. Usar AWS Systems Manager para distribuir una configuración que respalde todos los discos adjuntos en Amazon S3.

**C. Crear una nueva cuenta de AWS con privilegios limitados. Permitir que la nueva cuenta acceda a la clave de KMS que cifra las snapshots de EBS. Copiar las snapshots cifradas a la nueva cuenta periodicamente**

D. Usar AWS Backup para copiar las snapshots de EBS a Amazon S3. Usar S3 Object Lock para evitar que se eliminen las snapshots

46.- Un ingeniero de seguridad de una empresa está diseñando un procedimiento de aislamiento de instancias Amazon EC2 como parte de un plan de respuesta ante incidentes. El ingeniero necesita aislar una instancia objetivo para bloquear todo el tráfico de entrada y salida, excepto el tráfico proveniente del equipo forense de la empresa.

Cada instancia EC2 tiene su propio grupo de seguridad dedicado. Las instancias están desplegadas en subredes dentro de una VPC, y una subred puede contener múltiples instancias.

Durante las pruebas del procedimiento de aislamiento, el ingeniero abre una sesión SSH a la instancia objetivo. Luego, simula un acceso no autorizado (como si fuera un atacante). El ingeniero elimina las reglas existentes del grupo de seguridad y agrega reglas que solo permiten el acceso del equipo forense a la instancia en el puerto 22 (SSH).

Después de hacer estos cambios, el ingeniero nota que la conexión SSH sigue activa y funcional. Sin embargo, al ejecutar un comando ping hacia la IP pública de la instancia, el ping es bloqueado.

¿Qué debería hacer el ingeniero de seguridad para aislar correctamente la instancia objetivo?

A. Agregar una regla de entrada al grupo de seguridad para permitir tráfico desde 0.0.0.0/0 para todos los puertos. Agregar una regla de salida para permitir tráfico hacia 0.0.0.0/0 para todos los puertos. Luego, eliminar inmediatamente estas reglas.

**B. Eliminar la regla del puerto 22 del grupo de seguridad. Asignar un rol a la instancia que permita conexiones usando AWS Systems Manager Session Manager, de modo que el equipo forense pueda acceder a la instancia**.

C. Crear una ACL de red (network ACL) asociada a la subred de la instancia. Agregar una regla al principio del conjunto de reglas de entrada para denegar todo el tráfico desde 0.0.0.0/0. Agregar otra regla al principio del conjunto de reglas de salida para denegar todo el tráfico hacia 0.0.0.0/0.

D. Crear un documento de AWS Systems Manager que agregue una regla de firewall a nivel de host para bloquear todo el tráfico de entrada y salida. Ejecutar el documento en la instancia objetivo.

47.- Una empresa startup está utilizando una única cuenta de AWS que tiene recursos en una sola región de AWS. Un ingeniero de seguridad configura una pista de auditoría de AWS CloudTrail en esa misma región para enviar los archivos de registro a un bucket de Amazon S3, usando la CLI de AWS.

Debido a su expansión, la empresa agrega recursos en múltiples regiones. El ingeniero de seguridad nota que los registros de estas nuevas regiones no están llegando al bucket de S3.

¿Qué debe hacer el ingeniero de seguridad para solucionar este problema con el menor esfuerzo operativo posible?

A. Crear una nueva pista de CloudTrail. Seleccionar las nuevas regiones donde la empresa añadió recursos.

B. Cambiar el bucket de S3 para que reciba notificaciones que rastreen todas las acciones desde todas las regiones.

C. Crear una nueva pista de CloudTrail que se aplique a todas las regiones.

**D. Modificar la pista de CloudTrail existente para que se aplique a todas las regiones.**

48.- El Application Load Balancer (ALB) público de una empresa recientemente sufrió un ataque DDoS. Para mitigar este problema, la empresa implementó Amazon CloudFront delante del ALB, de manera que los usuarios no accedan directamente a las instancias de Amazon EC2 que están detrás del ALB.

La empresa descubre que aún hay tráfico que llega directamente al ALB y está siendo procesado por las instancias EC2.

¿Qué combinación de pasos debe seguir la empresa para asegurarse de que las instancias EC2 solo reciban tráfico proveniente de CloudFront? (Elige dos opciones).

A. Configurar CloudFront para agregar una política de clave de caché (cache key policy) que permita un encabezado HTTP personalizado que CloudFront envíe al ALB.

**B. Configurar CloudFront para agregar un encabezado HTTP personalizado a las solicitudes que envía al ALB.**

**C. Configurar el ALB para que solo reenvíe solicitudes que contengan el encabezado HTTP personalizado.**

D. Configurar el ALB y CloudFront para que usen el encabezado X-Forwarded-For para verificar las direcciones IP de los clientes.

E. Configurar el ALB y CloudFront para que usen el mismo certificado X.509 generado por AWS Certificate Manager (ACM).

49.- Una empresa detecta una anomalía en la facturación de su cuenta de AWS. Un consultor de seguridad investiga el incidente y descubre que un empleado que dejó la empresa hace 30 días todavía tiene acceso a la cuenta. La empresa no ha estado monitoreando la actividad en la cuenta hasta ahora.

El consultor de seguridad necesita identificar lo más rápido posible qué recursos fueron implementados o reconfigurados por ese empleado.

¿Qué solución cumpliría con estos requisitos?

A. En AWS Cost Explorer, filtrar los datos del gráfico para mostrar los resultados de los últimos 30 días. Exportar los resultados a una tabla de datos. Agrupar la tabla por recurso.

B. Usar AWS Cost Anomaly Detection para crear un monitor de costos. Acceder al historial de detección. Establecer el período de tiempo en los últimos 30 días. En el área de búsqueda, elegir la categoría del servicio.

**C. En AWS CloudTrail, filtrar el historial de eventos para mostrar los resultados de los últimos 30 días. Crear una tabla en Amazon Athena que contenga esos datos. Particionar la tabla por fuente del evento.**

D. Usar AWS Audit Manager para crear una evaluación de los últimos 30 días. Aplicar un marco basado en el uso a la evaluación. Configurar la evaluación para que se realice por recurso.

50.- Un ingeniero de seguridad está revisando una plantilla de AWS CloudFormation en busca de vulnerabilidades. El ingeniero encuentra un parámetro que tiene un valor por defecto que expone la clave API de una aplicación en texto plano. Este parámetro se usa varias veces a lo largo de la plantilla. El ingeniero de seguridad debe reemplazar el parámetro manteniendo la posibilidad de referenciar el valor dentro de la plantilla.

¿Qué solución cumpliría con estos requisitos de la forma MÁS segura?

A. Almacenar el valor de la clave API como un parámetro tipo SecureString en AWS Systems Manager Parameter Store. En la plantilla, reemplazar todas las referencias al valor con {{resolve:ssm:NombreDeMiParametroSSM:1}}.

**B. Almacenar el valor de la clave API en AWS Secrets Manager. En la plantilla, reemplazar todas las referencias al valor con {{resolve:secretsmanager:IdDeMiSecreto:SecretString}}.**

C. Almacenar el valor de la clave API en Amazon DynamoDB. En la plantilla, reemplazar todas las referencias al valor con {{resolve:dynamodb:NombreDeMiTabla:MiClavePrimaria}}.

D. Almacenar el valor de la clave API en un nuevo bucket de Amazon S3. En la plantilla, reemplazar todas las referencias al valor con {{resolve:s3:NombreDeMiBucket:NombreDeMiObjeto}}.

51.- Los registros de AWS CloudTrail de una empresa se almacenan de forma centralizada en un bucket de Amazon S3. El equipo de seguridad es quien controla la cuenta de AWS de la empresa. Este equipo debe prevenir el acceso no autorizado y la manipulación de los registros de CloudTrail.

¿Qué combinación de pasos debe tomar el equipo de seguridad? (Elige tres opciones)

**A. Configurar cifrado del lado del servidor con claves de cifrado administradas por AWS KMS (SSE-KMS).**

B. Comprimir los archivos de registro con gzip seguro.

C. Crear una regla de Amazon EventBridge para notificar al equipo de seguridad ante cualquier modificación en los archivos de registro de CloudTrail.

**D. Aplicar el principio de mínimo privilegio al bucket de S3 configurando una política del bucket.**

**E. Configurar la validación de integridad de los archivos de registro de CloudTrail.**

F. Configurar Access Analyzer para S3.

52.- Una empresa tiene varios petabytes de datos. Debe conservar esta información durante 7 años para cumplir con requisitos regulatorios. El equipo de cumplimiento le solicita a un oficial de seguridad que desarrolle una estrategia que impida que cualquier persona modifique o elimine los datos.

¿Qué solución cumplirá con este requisito de la forma MÁS rentable?

A. Crear un bucket de Amazon S3. Configurar el bucket para usar S3 Object Lock en modo de cumplimiento (compliance mode). Subir los datos al bucket. Crear una política basada en recursos (bucket policy) que cumpla con todos los requisitos regulatorios.

B. Crear un bucket de Amazon S3. Configurar el bucket para usar S3 Object Lock en modo de gobernanza (governance mode). Subir los datos al bucket. Crear una política basada en el usuario (IAM) que cumpla con todos los requisitos regulatorios.

**C. Crear un vault (bóveda) en Amazon S3 Glacier. Crear una política de Vault Lock en Glacier que cumpla con todos los requisitos regulatorios. Subir los datos a la bóveda.**

D. Crear un bucket de Amazon S3. Subir los datos al bucket. Usar una regla de ciclo de vida para mover los datos a una bóveda en S3 Glacier. Crear una política de Vault Lock que cumpla con todos los requisitos regulatorios.

53.- Una empresa utiliza un proveedor de identidad externo y SSO basado en SAML para acceder a sus cuentas de AWS.

Después de que el proveedor de identidad externo renovó un certificado de firma que había expirado, los usuarios vieron el siguiente mensaje al intentar iniciar sesión:

Error: Response Signature Invalid

(Service: AWSSecurityTokenService; Status Code: 400; Error Code: InvalidIdentityToken)

Un ingeniero de seguridad necesita proporcionar una solución que corrija el error y que minimice la carga operativa.

¿Qué solución cumple con estos requisitos?

A. Subir la nueva clave privada del certificado de firma del proveedor externo a la entidad del proveedor de identidad definida en AWS Identity and Access Management (IAM) usando la consola de administración de AWS.

B. Firmar el archivo de metadatos del proveedor de identidad con la nueva clave pública. Subir la firma a la entidad del proveedor de identidad definida en IAM usando la AWS CLI.

**C. Descargar el archivo actualizado de metadatos SAML del proveedor de identidad. Actualizar el archivo en la entidad del proveedor de identidad definida en IAM usando la AWS CLI.**

D. Configurar la entidad del proveedor de identidad definida en IAM para que recupere de forma síncrona la nueva clave pública mediante la consola de administración de AWS.

54.- Una empresa tiene varias cargas de trabajo ejecutándose en AWS. Los empleados deben autenticarse utilizando ADFS local (on-premises) y SSO para acceder a la Consola de Administración de AWS. Los desarrolladores migraron una aplicación web heredada a una instancia de Amazon EC2. Los empleados necesitan acceder a esta aplicación desde cualquier lugar por internet, pero actualmente la aplicación no tiene ningún sistema de autenticación incorporado.

¿Cómo debería el ingeniero de seguridad implementar acceso exclusivo para empleados a esta aplicación sin modificar la aplicación?

**A. Colocar la aplicación detrás de un Application Load Balancer (ALB). Usar Amazon Cognito como sistema de autenticación para el ALB. Definir un user pool de Amazon Cognito basado en SAML y conectarlo a ADFS.**

B. Implementar AWS IAM Identity Center (AWS Single Sign-On) en la cuenta de administración y vincularlo a ADFS como proveedor de identidad. Definir la instancia EC2 como un recurso administrado y luego aplicar una política de IAM sobre ese recurso.

C. Definir un identity pool de Amazon Cognito, luego instalar el conector en el servidor de Active Directory. Usar el SDK de Amazon Cognito en la instancia de la aplicación para autenticar a los empleados usando sus nombres de usuario y contraseñas de Active Directory.

D. Crear un autorizador personalizado en AWS Lambda como autenticador para un reverse proxy en Amazon EC2. Asegurarse de que el security group de la instancia EC2 solo permita acceso desde la función Lambda.

55.- Una empresa está utilizando AWS para ejecutar un proceso de análisis de larga duración sobre datos almacenados en buckets de Amazon S3. El proceso se ejecuta en un grupo de instancias de Amazon EC2 que pertenecen a un grupo de Auto Scaling. Las instancias EC2 están desplegadas en una subred privada de una VPC que no tiene acceso a internet. Las instancias EC2 y los buckets de S3 están en la misma cuenta de AWS.

Las instancias EC2 acceden a los buckets de S3 a través de un endpoint de gateway de S3 que tiene la política de acceso predeterminada. Cada instancia EC2 está asociada a un rol de perfil de instancia que tiene una política que permite explícitamente las acciones s3:GetObject y s3:PutObject únicamente para los buckets necesarios.

La empresa descubre que una o más instancias EC2 fueron comprometidas y están exfiltrando datos hacia un bucket de S3 que está fuera de la organización de la empresa en AWS Organizations. Un ingeniero de seguridad debe implementar una solución que detenga esta exfiltración de datos y al mismo tiempo mantenga funcional el trabajo de procesamiento en las instancias EC2.

¿Qué solución cumplirá con estos requisitos?

**A. Actualizar la política del endpoint de gateway de S3 para permitir las acciones de S3 solo si los valores de las claves de condición aws:ResourceOrgID y aws:PrincipalOrgID coinciden con los de la empresa.**

B. Actualizar la política del rol de perfil de instancia para permitir las acciones de S3 solo si el valor de la clave de condición aws:ResourceOrgID coincide con el de la empresa.

C. Agregar una regla en la ACL de red (network ACL) de la subred de las instancias EC2 para bloquear las conexiones salientes por el puerto 443.

D. Aplicar una política SCP (Service Control Policy) en la cuenta de AWS para permitir las acciones de S3 solo si los valores de las claves de condición aws:ResourceOrgID y aws:PrincipalOrgID coinciden con los de la empresa.

56.- Una empresa que opera en un entorno de nube híbrida debe cumplir con requisitos estrictos de cumplimiento normativo. La empresa quiere crear un informe que incluya evidencia de cargas de trabajo locales (on-premises) junto con evidencia de recursos en AWS.

Un ingeniero de seguridad debe implementar una solución para recopilar, revisar y gestionar dicha evidencia, con el fin de demostrar el cumplimiento de las políticas de la empresa.

¿Qué solución cumple con estos requisitos?

**A. Crear una evaluación en AWS Audit Manager usando un marco predefinido o personalizado. Subir evidencia manual desde las cargas de trabajo locales. Agregar esa evidencia a la evaluación. Generar un informe de evaluación después de que Audit Manager recopile automáticamente la evidencia de los recursos en AWS.**

B. Instalar el agente de Amazon CloudWatch en las cargas de trabajo locales. Usar AWS Config para implementar un conjunto de cumplimiento (conformance pack) a partir de una plantilla de ejemplo o una plantilla YAML personalizada. Generar un informe de evaluación después de que AWS Config identifique los recursos y cargas de trabajo que no cumplen con las políticas.

C. Configurar el estándar de seguridad apropiado en AWS Security Hub. Subir evidencia manual desde las cargas de trabajo locales. Esperar a que Security Hub recopile la evidencia de los recursos en AWS. Descargar la lista de controles como un archivo .csv.

D. Instalar el agente de Amazon CloudWatch en las cargas de trabajo locales. Crear un panel de CloudWatch para monitorear tanto los recursos locales como los de AWS. Ejecutar una consulta sobre las cargas de trabajo y recursos. Descargar los resultados.

57.- Para cumplir con los requisitos regulatorios, un ingeniero de seguridad necesita implementar una política de IAM que restrinja el uso de los servicios de AWS únicamente a la región us-east-1.

¿Qué política debe implementar el ingeniero?

A.

B.

**C.**

D.

58.- Una empresa tiene un servidor web en la nube de AWS. La empresa almacenará el contenido de ese servidor web en un bucket de Amazon S3. Un ingeniero de seguridad debe usar una distribución de Amazon CloudFront para acelerar la entrega del contenido. Ninguno de los archivos debe ser accesible públicamente desde el bucket de S3 directamente.

¿Qué solución cumplirá con estos requisitos?

A. Configurar los permisos en los archivos individuales del bucket de S3 para que solo la distribución de CloudFront tenga acceso a ellos.

**B. Crear un control de acceso de origen (OAC). Asociar el OAC con la distribución de CloudFront. Configurar los permisos del bucket de S3 para que solo el OAC pueda acceder a los archivos en el bucket S3.**

C. Crear un rol de S3 en AWS Identity and Access Management (IAM). Permitir que solo la distribución de CloudFront asuma el rol para acceder a los archivos en el bucket de S3.

D. Crear una política de bucket de S3 que use solo el ID de la distribución de CloudFront como principal y el ARN como destino.

59.- Un ingeniero de seguridad inicia sesión en la consola de AWS Lambda con permisos de administrador. El ingeniero intenta ver los registros en Amazon CloudWatch de una función Lambda llamada myFunction. Cuando selecciona la opción en la consola de Lambda para ver los registros en CloudWatch, aparece un mensaje de error que dice “error al cargar Log Streams”.

La política IAM del rol de ejecución de la función Lambda contiene lo siguiente:

¿Cómo debería el ingeniero de seguridad corregir este error?

A. Mover la acción logs:CreateLogGroup a la segunda declaración Allow.

B. Agregar la acción logs:PutDestination a la segunda declaración Allow.

C. Agregar la acción logs:GetLogEvents a la segunda declaración Allow.

**D. Agregar la acción logs:CreateLogStream a la segunda declaración Allow.**

60.- Una empresa ha establecido una nueva alianza con un proveedor. Este proveedor procesará datos de los clientes de la empresa. La empresa subirá archivos de datos como objetos en un bucket de Amazon S3. El proveedor descargará esos objetos para realizar el procesamiento de datos. Los objetos contendrán información sensible.

Un ingeniero de seguridad debe implementar una solución que evite que los objetos permanezcan en el bucket de S3 por más de 72 horas.

¿Qué solución cumple con estos requisitos?

A. Usar Amazon Macie para escanear el bucket de S3 en busca de datos sensibles cada 72 horas. Configurar Macie para eliminar los objetos que contengan datos sensibles cuando se descubran.

**B. Configurar una regla de ciclo de vida (Lifecycle) en el bucket de S3 para que expire (elimine) los objetos que hayan estado en el bucket durante más de 72 horas.**

C. Crear una regla programada de Amazon EventBridge que invoque una función de AWS Lambda todos los días. Programar la función Lambda para eliminar cualquier objeto que haya estado en el bucket de S3 por más de 72 horas.

D. Usar la clase de almacenamiento S3 Intelligent-Tiering para todos los objetos que se suban al bucket. Utilizar Intelligent-Tiering para que expire los objetos que hayan estado en el bucket por más de 72 horas.

61.- Una empresa eliminó accidentalmente la clave privada de una instancia de Amazon EC2 respaldada por Amazon Elastic Block Store (Amazon EBS). Un ingeniero de seguridad necesita recuperar el acceso a la instancia.

¿Qué combinación de pasos permitirá cumplir con este objetivo? (Elige dos opciones)

**A. Detener la instancia. Desasociar (detach) el volumen raíz. Generar un nuevo par de claves.**

B. Mantener la instancia en ejecución. Desasociar el volumen raíz. Generar un nuevo par de claves.

**C. Una vez que el volumen esté desasociado de la instancia original, adjuntar el volumen a otra instancia como volumen de datos. Modificar el archivo authorized\_keys con una nueva clave pública. Volver a asociar el volumen a la instancia original. Iniciar la instancia.**

D. Una vez que el volumen esté desasociado de la instancia original, adjuntar el volumen a otra instancia como volumen de datos. Modificar el archivo authorized\_keys con una nueva clave privada. Volver a asociar el volumen a la instancia original. Iniciar la instancia.

E. Una vez que el volumen esté desasociado de la instancia original, adjuntar el volumen a otra instancia como volumen de datos. Modificar el archivo authorized\_keys con una nueva clave pública. Volver a asociar el volumen a la instancia original que aún está en ejecución.

62.- Una empresa compró una suscripción a una solución de escaneo de seguridad en la nube de un proveedor externo, la cual se integra con AWS Security Hub. Un ingeniero de seguridad necesita implementar una solución que corrija automáticamente los hallazgos detectados por esta herramienta de terceros.

¿Qué solución cumplirá con este requisito?

**A. Configurar una regla de Amazon EventBridge que reaccione ante nuevos hallazgos de Security Hub. Configurar una función AWS Lambda como destino de la regla para corregir los hallazgos.**

B. Configurar una acción personalizada en Security Hub. Configurar esta acción para que ejecute runbooks de AWS Systems Manager Automation que corrijan los hallazgos.

C. Configurar una acción personalizada en Security Hub. Establecer una función AWS Lambda como destino de esta acción personalizada para corregir los hallazgos.

D. Configurar reglas en AWS Config para que utilicen runbooks de Systems Manager Automation con el fin de corregir los hallazgos.

63.- Una aplicación se está ejecutando en una instancia de Amazon EC2 que tiene un rol de IAM adjunto. Este rol proporciona acceso a una clave administrada por el cliente de AWS Key Management Service (AWS KMS) y a un bucket de Amazon S3. La clave se usa para acceder a 2 TB de datos sensibles almacenados en ese bucket de S3.

Un ingeniero de seguridad detecta una posible vulnerabilidad en la instancia EC2 que podría poner en riesgo los datos sensibles.

Debido a otras operaciones críticas, el ingeniero no puede apagar la instancia EC2 de inmediato para aplicar los parches necesarios.

¿Cuál es la forma MÁS RÁPIDA de evitar que los datos sensibles sean expuestos?

A. Descargar los datos del bucket de S3 existente a una nueva instancia EC2. Luego, eliminar los datos del bucket original. Reencriptar los datos usando una clave generada localmente. Subir los datos a un nuevo bucket de S3.

B. Bloquear el acceso al rango de direcciones IP públicas del endpoint de S3 mediante un firewall a nivel de host. Asegurarse de que el tráfico hacia Internet desde la instancia EC2 comprometida pase por ese firewall.

**C. Revocar los permisos de sesión activa del rol de IAM. Actualizar la política del bucket de S3 para denegar el acceso a ese rol. Quitar el rol del perfil de instancia de EC2.**

D. Desactivar la clave actual. Crear una nueva clave de KMS a la que el rol de IAM no tenga acceso, y reencriptar todos los datos con la nueva clave. Programar la eliminación de la clave comprometida.

64.- Una empresa está desarrollando una aplicación en AWS que almacenará información sensible. La empresa cuenta con un equipo de soporte que tiene acceso a la infraestructura de TI, incluidas las bases de datos. El ingeniero de seguridad de la empresa debe implementar medidas para proteger los datos sensibles contra cualquier posible brecha de seguridad, minimizando al mismo tiempo la carga de gestión. Las credenciales deben rotarse de forma regular.

¿Qué debería recomendar el ingeniero de seguridad?

A. Habilitar el cifrado de Amazon RDS para cifrar la base de datos y las instantáneas (snapshots). Habilitar el cifrado de Amazon Elastic Block Store (Amazon EBS) en las instancias de Amazon EC2. Incluir las credenciales de la base de datos en el campo de user data de EC2. Usar una función de AWS Lambda para rotar las credenciales de la base de datos. Configurar TLS para la conexión con la base de datos.

B. Instalar una base de datos en una instancia de Amazon EC2. Habilitar un cifrado de disco de terceros para cifrar el volumen de Amazon EBS. Almacenar las credenciales de la base de datos en AWS CloudHSM con rotación automática. Configurar TLS para la conexión con la base de datos.

**C. Habilitar el cifrado de Amazon RDS para cifrar la base de datos y las instantáneas. Habilitar el cifrado de Amazon EBS en las instancias EC2. Almacenar las credenciales de la base de datos en AWS Secrets Manager con rotación automática. Configurar TLS para la conexión con la base de datos alojada en RDS.**

D. Configurar un clúster de AWS CloudHSM junto con AWS Key Management Service (AWS KMS) para almacenar claves KMS. Configurar el cifrado de Amazon RDS utilizando AWS KMS para cifrar la base de datos. Almacenar las credenciales de la base de datos en AWS Systems Manager Parameter Store con rotación automática. Configurar TLS para la conexión con la base de datos alojada en RDS.

65.- Una empresa está utilizando Amazon Route 53 Resolver para su infraestructura DNS híbrida. La empresa ha configurado reglas de reenvío de Route 53 Resolver para dominios autorizados que están alojados en servidores DNS locales (on-premises).

Una nueva exigencia de seguridad requiere que la empresa implemente una solución para registrar (loggear) y consultar el tráfico DNS que se dirige a los servidores DNS on-premises. Los registros deben mostrar detalles de la dirección IP de origen de la instancia desde la que se originó la consulta. Además, deben mostrar el nombre de dominio (DNS) solicitado en Route 53 Resolver.

¿Qué solución cumplirá con estos requisitos?

A. Usar VPC Traffic Mirroring. Configurar todas las interfaces de red elásticas relevantes como fuente del tráfico, incluir amazon-dns en el filtro de mirroring, y establecer Amazon CloudWatch Logs como destino del tráfico duplicado. Usar CloudWatch Insights para ejecutar consultas sobre las sesiones de mirroring respecto a la IP de origen y el nombre DNS.

B. Configurar VPC Flow Logs en todas las VPC relevantes. Enviar los registros a un bucket de Amazon S3. Usar Amazon Athena para ejecutar consultas SQL sobre la dirección IP de origen y el nombre DNS.

**C. Configurar el registro de consultas (query logging) de Route 53 Resolver en todas las VPC relevantes. Enviar los registros a Amazon CloudWatch Logs. Usar CloudWatch Insights para ejecutar consultas sobre la dirección IP de origen y el nombre DNS.**

D. Modificar las reglas de Route 53 Resolver en los dominios autorizados que se reenvían a los servidores DNS on-premises. Enviar los registros a un bucket de Amazon S3. Usar Amazon Athena para ejecutar consultas SQL sobre la dirección IP de origen y el nombre DNS.

66.- Un ingeniero de seguridad está configurando un control de acceso basado en atributos (ABAC) para permitir que solo ciertos principales puedan subir objetos a un bucket de Amazon S3.

Estos principales ya tienen acceso a Amazon S3.

El ingeniero necesita configurar una política del bucket que permita subir objetos solo si el valor de la etiqueta (tag) Team del objeto coincide con el valor de la etiqueta Team asociada al principal.

Durante las pruebas, el ingeniero nota que un principal aún puede subir objetos al bucket de S3 incluso cuando los valores de las etiquetas no coinciden.

¿Qué combinación de factores está permitiendo que la operación PutObject tenga éxito a pesar de que los valores de las etiquetas son distintos? (Elige dos opciones)

**A. La política basada en la identidad del principal concede acceso para subir objetos al bucket de S3 sin condiciones**.

B. La política basada en la identidad del principal anula la condición porque contiene una autorización explícita (explicit allow).

**C. La política del recurso bucket de S3 no deniega el acceso para subir objetos.**

D. La política del bucket de S3 no puede permitir acciones al principal.

E. La política del bucket no aplica a principales dentro de la misma zona de confianza (zone of trust).

67.- Una empresa aloja múltiples aplicaciones dentro de una sola VPC en su cuenta de AWS. Las aplicaciones se ejecutan detrás de un Application Load Balancer que está asociado a una ACL web de AWS WAF. El equipo de seguridad de la empresa ha identificado que se están realizando múltiples escaneos de puertos provenientes de un rango específico de direcciones IP en internet.

Un ingeniero de seguridad necesita bloquear el acceso desde esas direcciones IP sospechosas.

¿Qué solución cumplirá con estos requisitos?

**A. Modificar la ACL web de AWS WAF con una regla de coincidencia de conjunto de IP (IP set match) para denegar las solicitudes entrantes desde ese rango de direcciones IP.**

B. Agregar una regla en todos los grupos de seguridad para denegar las solicitudes entrantes desde ese rango de direcciones IP.

C. Modificar la ACL web de AWS WAF con una regla basada en tasa (rate-based rule) para denegar las solicitudes entrantes desde ese rango de direcciones IP.

D. Configurar la ACL web de AWS WAF con condiciones de coincidencia por expresiones regulares (regex match conditions). Especificar un conjunto de patrones para denegar las solicitudes entrantes basándose en la condición de coincidencia.

68.- Una empresa ha contratado a un tercero para auditar varias cuentas de AWS. Para habilitar la auditoría, se han creado roles de IAM con acceso entre cuentas (cross-account) en cada cuenta objetivo. El auditor está teniendo problemas para acceder a algunas de las cuentas.

¿Cuál de las siguientes opciones podría estar causando este problema? (Elige tres opciones)

**A. El ID externo que usa el auditor está ausente o es incorrecto.**

B. El auditor está usando una contraseña incorrecta.

**C. Al auditor no se le ha otorgado el permiso sts:AssumeRole para el rol en la cuenta de destino.**

D. El rol de Amazon EC2 que utiliza el auditor debe estar configurado como el rol de la cuenta de destino.

E. La clave secreta (secret key) que usa el auditor está ausente o es incorrecta.

**F. El ARN del rol que usa el auditor está ausente o es incorrecto.**

69.- Un ingeniero de seguridad necesita configurar una política de bucket de Amazon S3 para restringir el acceso a un bucket llamado DOC-EXAMPLE-BUCKET. La política debe permitir el acceso a DOC-EXAMPLE-BUCKET solo si se accede desde el siguiente endpoint: vpce-1a2b3c4d. La política debe denegar todo acceso al bucket si no se utiliza ese endpoint especificado.

¿Cuál declaración de política de bucket cumple con estos requisitos?

A.

**B.**

C.

D.

70.- Una empresa tiene un grupo de instancias Amazon EC2 en una única subred privada de una VPC que no tiene una gateway de internet asociada. Un ingeniero de seguridad ha instalado el agente de Amazon CloudWatch en todas las instancias de esa subred para capturar los registros de una aplicación específica. Para garantizar que los registros se transmitan de forma segura, el equipo de redes de la empresa ha creado endpoints de VPC para el monitoreo de CloudWatch y los logs de CloudWatch, y los ha adjuntado a la VPC.

La aplicación está generando registros, pero cuando el ingeniero de seguridad consulta en CloudWatch, los registros no aparecen.

¿Qué combinación de pasos debe seguir el ingeniero de seguridad para solucionar este problema? (Elige tres opciones).

**A. Asegurarse de que el perfil de instancia EC2 (instance profile) adjunto a las instancias tenga permisos para crear flujos de registros (log streams) y escribir logs.**

B. Crear un filtro de métricas (metric filter) sobre los logs para que puedan visualizarse en la Consola de administración de AWS.

**C. Verificar el archivo de configuración del agente de CloudWatch en cada instancia EC2 para asegurarse de que esté recopilando los archivos de log correctos.**

**D. Verificar las políticas de los endpoints de VPC para asegurarse de que las instancias EC2 tengan permisos para usarlos.**

E. Crear una gateway NAT en la subred para que las instancias EC2 puedan comunicarse con CloudWatch.

F. Asegurarse de que los grupos de seguridad permitan que todas las instancias EC2 se comuniquen entre sí para agregar los logs antes de enviarlos.

71.- Una empresa utiliza AWS Signer con todas las funciones de AWS Lambda que posee. Recientemente, un desarrollador dejó de trabajar en la empresa. Ahora, la empresa quiere asegurarse de que ningún código escrito por ese desarrollador pueda volver a desplegarse en las funciones Lambda.

¿Qué solución cumple con este requisito?

**A. Revocar todas las versiones del perfil de firma asignadas al desarrollador.**

B. Revisar los roles de IAM del desarrollador y eliminar todos los permisos que le otorgaban acceso a AWS Signer.

C. Reencriptar todo el código fuente con una nueva clave de AWS Key Management Service (AWS KMS).

D. Usar Amazon CodeGuru para hacer un perfil del código utilizado por las funciones Lambda.

72.- Una empresa planea usar AWS Key Management Service (AWS KMS) para implementar una estrategia de cifrado que proteja los datos en reposo. La empresa requiere cifrado del lado del cliente (client-side encryption) para sus proyectos. Actualmente, la empresa está llevando a cabo múltiples proyectos de prueba para evaluar el uso de AWS KMS. Estas pruebas han provocado un aumento repentino en el consumo de recursos de AWS por parte de la empresa. Los proyectos de prueba incluyen aplicaciones que envían múltiples solicitudes por segundo a los endpoints de KMS para actividades de cifrado.

La empresa necesita desarrollar una solución que no limite (no aplique throttling a) su capacidad de usar AWS KMS. La solución debe mejorar el uso de claves para cifrado del lado del cliente y además debe estar optimizada en costos.

¿Qué solución cumplirá con estos requisitos?

A. Usar keyrings con AWS Encryption SDK. Usar cada keyring individualmente o combinar varios en un multi-keyring. Descifrar los datos utilizando un keyring que contenga la clave principal del multi-keyring.

**B. Usar almacenamiento en caché de claves de datos Utilizar la caché local que proporciona AWS Encryption SDK junto con un administrador de materiales criptográficos con caché**

C. Usar rotación de claves KMS. Usar una caché local en AWS Encryption SDK con un administrador de materiales criptográficos con caché.

D. Usar keyrings con AWS Encryption SDK. Usar cada keyring individualmente o combinarlos en un multi-keyring. Usar cualquiera de las claves de envoltura en el multi-keyring para descifrar los datos.

73.- Un equipo de seguridad está desarrollando una solución que utilizará Amazon EventBridge para monitorear nuevos objetos en Amazon S3.

La solución debe detectar accesos públicos y cualquier cambio en las políticas o configuraciones de los buckets de S3 que resulten en acceso público.

El equipo de seguridad configuró EventBridge para que observe llamadas específicas a la API que se registran en AWS CloudTrail. EventBridge tiene una acción configurada para enviar una notificación por correo electrónico a través de Amazon SNS al equipo de seguridad de forma inmediata con los detalles de la llamada a la API.

Específicamente, el equipo quiere que EventBridge detecte las llamadas a las API s3:PutObjectAcl, s3:DeleteBucketPolicy y s3:PutBucketPolicy según lo registrado en CloudTrail.

Durante el desarrollo de la solución en una sola cuenta, el equipo descubre que la llamada a s3:PutObjectAcl no genera un evento en EventBridge, mientras que las llamadas a s3:DeleteBucketPolicy y s3:PutBucketPolicy sí generan eventos.

El equipo de seguridad ha habilitado CloudTrail para eventos de administración de AWS con una configuración básica en la región donde se está probando EventBridge.

La verificación del patrón de eventos de EventBridge indica que el patrón está configurado correctamente.

El equipo de seguridad debe implementar una solución para que la llamada a s3:PutObjectAcl genere un evento en EventBridge.

La solución no debe generar notificaciones falsas.

¿Qué solución cumple con estos requisitos?

A. Modificar el patrón de eventos de EventBridge seleccionando Amazon S3. Seleccionar Todos los eventos como tipo de evento.

B. Modificar el patrón de eventos de EventBridge seleccionando Amazon S3. Seleccionar Operaciones a nivel de bucket como tipo de evento.

C. Habilitar CloudTrail Insights para identificar actividad inusual de la API.

**D. Habilitar CloudTrail para monitorear eventos de datos (data events) tanto de lectura como de escritura en los buckets de S3.**

74.- Una empresa utiliza Amazon GuardDuty. El equipo de seguridad de la empresa quiere que todos los hallazgos de severidad Alta generen automáticamente un ticket en un sistema de tickets de terceros mediante integración por correo electrónico.

¿Qué solución cumple con este requisito?

A. Crear una identidad verificada para el sistema de tickets de terceros en Amazon Simple Email Service (Amazon SES). Crear una regla de Amazon EventBridge con un patrón de eventos que coincida con los hallazgos de severidad Alta de GuardDuty. Especificar la identidad de SES como destino de la regla de EventBridge.

**B. Crear un tema de Amazon Simple Notification Service (Amazon SNS). Suscribir el sistema de tickets de terceros al tema SNS. Crear una regla de Amazon EventBridge con un patrón de eventos que coincida con los hallazgos de severidad Alta de GuardDuty. Especificar el tema SNS como destino de la regla de EventBridge.**

C. Usar la operación CreateFilter de GuardDuty para crear un filtro que supervise los hallazgos de severidad Alta. Exportar los resultados del filtro a un tema de Amazon SNS. Suscribir el sistema de tickets de terceros al tema SNS.

D. Usar la operación CreateFilter de GuardDuty para crear un filtro que supervise los hallazgos de severidad Alta. Crear un tema de Amazon SNS. Suscribir el sistema de tickets de terceros al tema SNS. Crear una regla de Amazon EventBridge con un patrón de eventos que coincida con los hallazgos de GuardDuty seleccionados por el filtro. Especificar el tema SNS como destino de la regla.

75.- Una empresa está utilizando AWS Organizations para implementar una estrategia de múltiples cuentas. La empresa no cuenta con infraestructura local (on-premises). Todas las cargas de trabajo se ejecutan en AWS. Actualmente, la empresa tiene ocho cuentas miembro, y prevé que en ningún momento tendrá más de 20 cuentas en total.

La empresa ha emitido una nueva política de seguridad que incluye los siguientes requisitos:

Ninguna cuenta de AWS debe usar una VPC propia para ejecutar cargas de trabajo.

La empresa debe utilizar una VPC gestionada de forma centralizada a la que todas las cuentas de AWS puedan acceder para lanzar cargas de trabajo en subredes.

Ninguna cuenta de AWS debe poder modificar los recursos de aplicación de otra cuenta dentro de la VPC centralizada.

La VPC centralizada debe estar ubicada en una cuenta existente llamada Account-A dentro de la organización.

La empresa usa una plantilla de AWS CloudFormation para crear una VPC que contiene múltiples subredes en Account-A. Esta plantilla exporta los IDs de las subredes a través de la sección Outputs de CloudFormation.

¿Qué solución completará la configuración de seguridad para cumplir con estos requisitos?

A. Usar una plantilla de CloudFormation en las cuentas miembro para lanzar cargas de trabajo. Configurar la plantilla para usar la función Fn::ImportValue y obtener así los valores de los IDs de las subredes.

B. Usar un Transit Gateway en la VPC dentro de Account-A. Configurar las cuentas miembro para que utilicen el transit gateway y accedan a las subredes de Account-A para lanzar cargas de trabajo.

**C. Usar AWS Resource Access Manager (AWS RAM) para compartir las subredes de la VPC de Account-A con las demás cuentas miembro. Configurar las cuentas miembro para que utilicen las subredes compartidas al lanzar cargas de trabajo.**

D. Crear una conexión de emparejamiento (peering) entre Account-A y las demás cuentas miembro. Configurar las cuentas miembro para que utilicen las subredes de Account-A a través de la conexión de peering para lanzar cargas de trabajo.

76.- El equipo de seguridad de una empresa necesita recibir una notificación siempre que una clave de acceso de AWS no haya sido rotada en 90 días o más. Un ingeniero de seguridad debe desarrollar una solución que envíe estas notificaciones de forma automática.

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

**A. Implementar una regla administrada de AWS Config que se ejecute de forma periódica cada 24 horas. Seleccionar la regla administrada access-keys-rotated y establecer el parámetro maxAccessKeyAge en 90 días. Crear una regla de Amazon EventBridge con un patrón de evento que detecte el tipo de cumplimiento NON\_COMPLIANT proveniente de AWS Config para dicha regla. Configurar EventBridge para que envíe una notificación a Amazon SNS dirigida al equipo de seguridad.**

B. Crear un script que exporte un archivo .csv desde el chequeo de Trusted Advisor para rotación de claves de acceso IAM. Cargar el script en una función de AWS Lambda que suba el archivo .csv a un bucket de Amazon S3. Crear una consulta de Amazon Athena que se ejecute cuando el archivo sea subido al bucket. Publicar los resultados de cualquier clave con más de 90 días usando una invocación de notificación a Amazon SNS para el equipo de seguridad.

C. Crear un script que descargue el informe de credenciales de IAM de forma periódica. Cargar el script en una función de AWS Lambda que se ejecute según una programación mediante Amazon EventBridge. Configurar el script para cargar el informe en memoria y filtrar los registros donde la clave no haya sido rotada en al menos 90 días. Si se detectan registros, enviar una notificación a Amazon SNS al equipo de seguridad.

D. Crear una función de AWS Lambda que consulte la API de IAM para listar todos los usuarios. Iterar sobre los usuarios usando la operación ListAccessKeys. Verificar que el valor del campo CreateDate no sea superior a 90 días. Si lo es, enviar una notificación a Amazon SNS al equipo de seguridad. Crear una regla de Amazon EventBridge para programar la ejecución diaria de la función Lambda.

77.- Una empresa mantiene una aplicación de código abierto que está alojada en un repositorio público de GitHub. Al hacer un nuevo commit, un ingeniero subió por error su clave de acceso de AWS y su clave secreta. El ingeniero informó del error a un gerente, y el gerente desactivó inmediatamente la clave de acceso.

La empresa necesita evaluar el impacto de haber expuesto esa clave de acceso. Un ingeniero de seguridad debe recomendar una solución que implique la menor cantidad posible de gestión o intervención manual.

¿Qué solución cumple con estos requisitos?

A. Analizar un informe de uso de AWS Identity and Access Management (IAM) desde AWS Trusted Advisor para ver cuándo se usó por última vez la clave de acceso.

B. Analizar los logs de Amazon CloudWatch para buscar actividad relacionada con la clave de acceso.

C. Analizar los logs de flujo de VPC (VPC Flow Logs) buscando actividad relacionada con la clave de acceso.

**D. Analizar un informe de credenciales en AWS Identity and Access Management (IAM) para ver cuándo se usó por última vez la clave de acceso.**

78.- Una empresa planea crear cuentas hijas individuales dentro de una organización existente en AWS Organizations para cada uno de sus equipos de DevOps. AWS CloudTrail ha sido habilitado y configurado en todas las cuentas para escribir los registros de auditoría en un bucket de Amazon S3 ubicado en una cuenta centralizada de AWS. Un ingeniero de seguridad necesita asegurarse de que los miembros de los equipos DevOps no puedan modificar ni deshabilitar esta configuración.

¿Cómo puede el ingeniero de seguridad cumplir con estos requisitos?

A. Crear una política de IAM que prohíba cambios en el trail específico de CloudTrail y aplicar esa política al usuario raíz de la cuenta de AWS.

B. Crear una política de bucket de S3 en la cuenta de destino especificada para el trail de CloudTrail que prohíba los cambios de configuración por parte del usuario raíz de la cuenta de origen.

**C. Crear una SCP (política de control de servicios) que prohíba los cambios en el trail específico de CloudTrail y aplicar la SCP a la unidad organizativa o cuenta correspondiente en AWS Organizations.**

D. Crear una política de IAM que prohíba los cambios en el trail específico de CloudTrail y aplicar la política a un nuevo grupo de IAM. Hacer que los miembros del equipo usen cuentas individuales de IAM que pertenezcan a ese grupo.

79.- La política de una empresa requiere que todas las claves API estén cifradas y almacenadas por separado del código fuente, en una cuenta centralizada de seguridad. Esta cuenta de seguridad es gestionada por el equipo de seguridad de la empresa. Sin embargo, una auditoría reveló que una clave API está almacenada junto con el código fuente de una función AWS Lambda en un repositorio de AWS CodeCommit dentro de la cuenta de DevOps.

¿Cómo debería el equipo de seguridad almacenar la clave API de forma segura?

A. Crear un repositorio de CodeCommit en la cuenta de seguridad usando AWS Key Management Service (AWS KMS) para cifrado. Exigir al equipo de desarrollo que migre el código fuente de Lambda a este repositorio.

B. Almacenar la clave API en un bucket de Amazon S3 dentro de la cuenta de seguridad, usando cifrado del lado del servidor con claves gestionadas por Amazon S3 (SSE-S3). Crear una URL prefirmada para acceder a la clave en S3, y especificar esta URL en una variable de entorno de la función Lambda dentro de la plantilla de AWS CloudFormation. Actualizar el código de Lambda para recuperar la clave usando esa URL y así llamar a la API.

**C. Crear un secreto en AWS Secrets Manager dentro de la cuenta de seguridad para almacenar la clave API, utilizando AWS Key Management Service (AWS KMS) para el cifrado. Conceder acceso al rol IAM que usa la función Lambda, de forma que la función pueda recuperar la clave desde Secrets Manager y así llamar a la API.**

D. Crear una variable de entorno cifrada para la función Lambda para almacenar la clave API, utilizando AWS Key Management Service (AWS KMS) para el cifrado. Conceder acceso al rol IAM usado por la función Lambda para que pueda descifrar la clave durante la ejecución.

80.- Un ingeniero de seguridad recibe la tarea de actualizar el prefijo de los archivos de registro (log file prefix) de un rastro (trail) existente en AWS CloudTrail. Al intentar guardar el cambio en la consola de CloudTrail, el ingeniero recibe el siguiente mensaje de error: "Hay un problema con la política del bucket”

¿Qué acción permitirá al ingeniero de seguridad guardar el cambio?

A. Crear un nuevo trail con el nuevo prefijo de archivos de registro, y luego eliminar el trail original. Actualizar la política del bucket existente en la consola de Amazon S3 con el nuevo prefijo, y luego actualizar el prefijo en la consola de CloudTrail.

B. Actualizar la política del bucket existente en la consola de Amazon S3 para permitir que el principal (usuario o rol) del ingeniero de seguridad ejecute la acción PutBucketPolicy, y luego actualizar el prefijo en la consola de CloudTrail.

**C. Actualizar la política del bucket existente en la consola de Amazon S3 con el nuevo prefijo de archivos de registro, y luego actualizar el prefijo en la consola de CloudTrail.**

D. Actualizar la política del bucket existente en la consola de Amazon S3 para permitir que el principal del ingeniero de seguridad ejecute la acción GetBucketPolicy, y luego actualizar el prefijo en la consola de CloudTrail.

81.- Una empresa utiliza AWS Organizations. La empresa quiere implementar credenciales temporales de corto plazo para que cuentas de AWS de terceros puedan acceder a las cuentas dentro de la organización. El acceso será tanto para la Consola de administración de AWS como para aplicaciones de software como servicio (SaaS) de terceros.

Se debe reforzar la confianza para evitar que dos cuentas externas usen las mismas credenciales. La solución debe requerir el menor esfuerzo operativo posible.

¿Qué solución cumple con estos requisitos?

A. Usar autenticación con tokens bearer usando OAuth o SAML para gestionar y compartir un pool de usuarios central de Amazon Cognito entre múltiples API de Amazon API Gateway.

B. Implementar AWS IAM Identity Center (anteriormente AWS Single Sign-On), y usar una fuente de identidad externa a elección. Conceder acceso a usuarios y grupos de otras cuentas usando conjuntos de permisos (permission sets) asignados por cuenta.

C. Crear un rol de IAM único para cada cuenta externa. Crear una política de confianza. Usar AWS Secrets Manager para generar una clave externa aleatoria.

**D. Crear un rol de IAM único para cada cuenta externa. Crear una política de confianza que incluya una condición basada en la clave sts:ExternalId.**

82.- Una empresa está evaluando su postura de seguridad. En el pasado, la empresa ha tenido problemas con combinaciones específicas de hosts y encabezados Host, lo cual afectó su operación. Como primer paso para mitigar estos problemas, la empresa ha configurado reglas de AWS WAF (web ACLs).

Ahora, la empresa necesita crear una solución de análisis de registros para los web ACLs de AWS WAF, con el fin de monitorear actividades problemáticas.

Desean procesar todos los registros de AWS WAF en una ubicación centralizada y tener la capacidad de filtrar solicitudes según hosts específicos.

Un ingeniero de seguridad comienza a habilitar el registro de acceso (access logging) para los web ACLs de AWS WAF.

¿Qué debe hacer el ingeniero de seguridad a continuación para cumplir con estos requisitos con la MAYOR eficiencia operativa?

A. Especificar Amazon Redshift como destino de los registros de acceso. Implementar el conector de Amazon Athena para Redshift. Usar Athena para consultar los datos desde Redshift y filtrar los registros por host.

**B. Especificar Amazon CloudWatch como destino de los registros de acceso. Usar CloudWatch Logs Insights para diseñar una consulta que filtre los registros por host.**

C. Especificar Amazon CloudWatch como destino de los registros de acceso. Exportar los registros de CloudWatch a un bucket de Amazon S3. Usar Amazon Athena para consultar los registros y filtrarlos por host.

D. Especificar Amazon CloudWatch como destino de los registros de acceso. Usar Amazon Redshift Spectrum para consultar los registros y filtrarlos por host.

83.- Un ingeniero de seguridad está intentando usar Amazon EC2 Image Builder para crear una imagen de una instancia EC2. El ingeniero ha configurado la canalización (pipeline) para que envíe los registros (logs) a un bucket de Amazon S3. Al ejecutar la canalización, el proceso falla con el siguiente error: "AccessDenied: Access Denied status code: 403"

El ingeniero de seguridad debe resolver este error implementando una solución que cumpla con las buenas prácticas de acceso con privilegios mínimos.

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

A. Asegurarse de que las siguientes políticas estén adjuntas al rol de IAM que está usando el ingeniero de seguridad: EC2InstanceProfileForImageBuilder, C2InstanceProfileForImageBuilderECRContainerBuilds, y AmazonSSMManagedInstanceCore.

**B. Asegurarse de que las siguientes políticas estén adjuntas al perfil de instancia de la instancia EC2: EC2InstanceProfileForImageBuilder, EC2InstanceProfileForImageBuilderECRContainerBuilds, y AmazonSSMManagedInstanceCore**.

C. Asegurarse de que la política AWSImageBuilderFullAccess esté adjunta al perfil de instancia de la instancia EC2.

D. Asegurarse de que el rol de IAM del ingeniero de seguridad tenga el permiso s3:PutObject para el bucket de S3.

**E. Asegurarse de que el perfil de instancia de la instancia EC2 tenga el permiso s3:PutObject para el bucket de S3.**

84.- Un ingeniero de seguridad debe usar AWS Key Management Service (AWS KMS) para diseñar una solución de gestión de claves para un conjunto de volúmenes de Amazon Elastic Block Store (Amazon EBS) que contienen datos sensibles.

La solución debe garantizar que el material de la clave expire automáticamente en 90 días.

¿Qué solución cumple con estos criterios?

**A. Una clave administrada por el cliente que utiliza material de clave proporcionado por el cliente**

B. Una clave administrada por el cliente que utiliza material de clave proporcionado por AWS

C. Una clave administrada por AWS

D. Cifrado a nivel de sistema operativo que utiliza GnuPG

85.- Un ingeniero de seguridad está desarrollando una aplicación en Java que se ejecuta en una instancia de Amazon EC2. La aplicación se comunica con una instancia de Amazon RDS y se autentica utilizando un nombre de usuario y una contraseña.

¿Qué combinación de pasos puede seguir el ingeniero para proteger las credenciales y minimizar el tiempo de inactividad cuando las credenciales se roten? (Elige dos opciones)

A. Pedir a un administrador de base de datos que cifre las credenciales y almacene el texto cifrado en Amazon S3. Otorgar permisos al rol de la instancia EC2 para que lea el objeto y descifre el contenido cifrado.

B. Configurar una tarea programada que actualice las credenciales en AWS Systems Manager Parameter Store y notifique al ingeniero que es necesario reiniciar la aplicación.

**C. Configurar la rotación automática de credenciales en AWS Secrets Manager.**

D. Almacenar las credenciales como un parámetro de cadena cifrada en AWS Systems Manager Parameter Store. Otorgar permisos al rol de la instancia EC2 para acceder al parámetro y a la clave de AWS KMS que se utiliza para cifrarlo.

**E. Configurar la aplicación Java para que capture errores de conexión e invoque AWS Secrets Manager para obtener credenciales actualizadas cuando se rote la contraseña. Otorgar permisos al rol de la instancia EC2 para acceder a Secrets Manager.**

86.- Una empresa usa federación SAML para otorgar acceso a las cuentas de AWS. Una de sus cargas de trabajo se ejecuta en una cuenta de AWS aislada y utiliza infraestructura inmutable, sin acceso humano directo a las instancias de Amazon EC2. La empresa requiere un usuario especial, conocido como “usuario de emergencia” (break glass user), que pueda acceder a la cuenta de AWS y a las instancias en caso de fallas con SAML.

Una auditoría reciente descubrió que la empresa no creó el usuario de emergencia para la cuenta que contiene dicha carga de trabajo.

La empresa debe crear este usuario de emergencia, registrar toda su actividad y enviar esos registros al equipo de seguridad.

¿Qué combinación de soluciones cumple con estos requisitos? (Elige dos opciones)

**A. Crear un usuario IAM local individual como usuario de emergencia para el equipo de seguridad. Crear un trail en AWS CloudTrail con el registro en Amazon CloudWatch Logs activado. Usar Amazon EventBridge para monitorear la actividad del usuario local.**

B. Crear un par de claves EC2 para el acceso de emergencia en la cuenta de AWS. Proporcionar el par de claves al equipo de seguridad. Usar AWS CloudTrail para monitorear la actividad relacionada al uso de las claves. Enviar notificaciones al equipo de seguridad utilizando Amazon SNS.

C. Crear un rol IAM de emergencia (break glass) para la cuenta. Permitir que los miembros del equipo de seguridad usen la operación AssumeRoleWithSAML. Crear un trail en AWS CloudTrail con registro en Amazon CloudWatch Logs activado. Usar Amazon EventBridge para monitorear la actividad del equipo de seguridad.

D. Crear un usuario IAM de emergencia local en el sistema operativo de cada instancia de carga de trabajo. Configurar grupos de seguridad sin restricciones en las instancias para permitir el acceso a estos usuarios de emergencia.

**E. Configurar AWS Systems Manager Session Manager para las instancias EC2. Configurar un filtro de AWS CloudTrail basado en el uso de Session Manager. Enviar los resultados a un tema de Amazon SNS.**

87.- Un ingeniero de seguridad está trabajando con un equipo de producto que está desarrollando una aplicación web en AWS. La aplicación usa Amazon S3 para alojar contenido estático, Amazon API Gateway para ofrecer servicios RESTful, y Amazon DynamoDB como base de datos. Los usuarios ya existen en un directorio que está expuesto mediante un proveedor de identidad SAML.

¿Qué combinación de acciones debe tomar el ingeniero para permitir que los usuarios se autentiquen en la aplicación web y puedan llamar a las APIs? (Elige tres opciones)

A. Crear un servicio de autorización personalizado usando AWS Lambda.

**B. Configurar un proveedor de identidad SAML en Amazon Cognito para mapear atributos con los atributos del user pool de Amazon Cognito.**

**C. Configurar el proveedor de identidad SAML para agregar el user pool de Amazon Cognito como una parte confiable.**

D. Configurar un identity pool de Amazon Cognito para integrarse con proveedores de inicio de sesión social.

E. Actualizar DynamoDB para almacenar las direcciones de correo electrónico y contraseñas de los usuarios.

**F. Actualizar API Gateway para que use un autorizador del tipo COGNITO\_USER\_POOLS.**

88.- Una empresa necesita mejorar su capacidad para identificar y prevenir políticas de IAM que otorguen acceso público o acceso entre cuentas a sus recursos. La empresa ha implementado AWS Organizations y ha comenzado a usar AWS Identity and Access Management Access Analyzer para refinar accesos demasiado amplios en las cuentas de la organización.

Un ingeniero de seguridad debe automatizar una respuesta dentro de la organización ante cualquier política nueva que sea demasiado permisiva. La automatización debe remediar el acceso externo y notificar al equipo de seguridad de la empresa.

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

**A. Crear una máquina de estado de AWS Step Functions que revise el tipo de recurso del hallazgo e incluya una instrucción explícita de Deny (denegación) en la política de confianza del rol IAM. Configurar la máquina de estado para que publique una notificación en un tema de Amazon SNS.**

B. Crear un trabajo de AWS Batch que reenvíe cualquier hallazgo sobre tipos de recursos a una función de AWS Lambda. Configurar la función Lambda para agregar una instrucción explícita de Deny en la política de confianza del rol IAM. Configurar el trabajo de AWS Batch para que publique una notificación en un tema de Amazon SNS.

**C. En Amazon EventBridge, crear una regla de evento que detecte hallazgos activos de IAM Access Analyzer e invoque AWS Step Functions para resolverlos.**

D. En Amazon CloudWatch, crear un filtro de métricas que detecte hallazgos activos de IAM Access Analyzer e invoque AWS Batch para resolverlos.

E. Crear una cola de Amazon SQS. Configurar la cola para reenviar una notificación al equipo de seguridad cuando se haya otorgado acceso a un principal externo a un rol específico de IAM y este haya sido bloqueado.

**F. Crear un tema de Amazon SNS para notificaciones de accesos externos o entre cuentas. Suscribir las direcciones de correo electrónico del equipo de seguridad a ese tema.**

89.- Un ingeniero de seguridad está configurando un mecanismo para enviar una alerta cuando se detecten tres o más intentos fallidos de inicio de sesión en la Consola de administración de AWS durante un período de 5 minutos. El ingeniero crea un trail en AWS CloudTrail para ayudar con esta tarea.

¿Qué solución cumple con estos requisitos?

A. En CloudTrail, activar los eventos Insights en el trail. Configurar una alarma sobre el insight con eventName igual a ConsoleLogin y errorMessage igual a "Failed authentication". Configurar un umbral de 3 y un período de 5 minutos.

**B. Configurar CloudTrail para que envíe los eventos a Amazon CloudWatch Logs. Crear un filtro de métricas para el grupo de logs correspondiente. Crear un patrón de filtrado donde eventName sea ConsoleLogin y errorMessage sea "Failed authentication". Crear una alarma de CloudWatch con un umbral de 3 y un período de 5 minutos.**

C. Crear una tabla en Amazon Athena a partir de los eventos de CloudTrail. Ejecutar una consulta donde eventName sea ConsoleLogin y errorMessage sea "Failed authentication". Crear una acción de notificación basada en la consulta que envíe una notificación mediante Amazon SNS cuando el conteo sea igual a 3 dentro de un período de 5 minutos.

D. En AWS Identity and Access Management Access Analyzer, crear un nuevo analizador. Configurar el analizador para que envíe una notificación de Amazon SNS cuando se produzcan 3 intentos fallidos de inicio de sesión por parte de cualquier usuario IAM en un período de 5 minutos.

90.- El ingeniero de seguridad de una empresa está desarrollando un plan de respuesta ante incidentes para detectar actividades sospechosas en una cuenta de AWS, enfocándose en los recursos alojados en VPC. El ingeniero necesita proporcionar visibilidad para la mayor cantidad de regiones de AWS posible.

¿Qué combinación de pasos cumplirá con estos requisitos de la forma más rentable? (Elige dos opciones)

A. Activar los VPC Flow Logs para todas las VPC de la cuenta.

**B. Activar Amazon GuardDuty en todas las regiones de AWS.**

C. Activar Amazon Detective en todas las regiones de AWS.

**D. Crear un tema de Amazon SNS. Crear una regla de Amazon EventBridge que responda a hallazgos y publique esos hallazgos en el tema de SNS.**

E. Crear una función de AWS Lambda. Crear una regla de Amazon EventBridge que invoque la función Lambda para publicar los hallazgos mediante Amazon SES (Simple Email Service).

91.- Una empresa almacena imágenes para su sitio web en un bucket de Amazon S3. La empresa está utilizando Amazon CloudFront para distribuir esas imágenes a los usuarios finales.

Recientemente descubrieron que las imágenes están siendo accedidas desde países donde no tienen licencia de distribución.

¿Qué acciones debe tomar la empresa para proteger las imágenes y limitar su distribución? (Elige dos opciones)

**A. Actualizar la política del bucket de S3 para restringir el acceso solo a través de un CloudFront Origin Access Control (OAC).**

B. Actualizar el registro DNS del sitio web para usar un registro de geolocalización en Amazon Route 53 con una lista de países denegados donde la empresa no tiene licencia.

**C. Agregar una restricción geográfica en CloudFront con una lista de países denegados donde la empresa no tiene licencia.**

D. Actualizar la política del bucket de S3 con una lista de países denegados donde la empresa no tiene licencia.

E. Habilitar la opción Restrict Viewer Access en CloudFront para crear una lista de países denegados donde la empresa no tiene licencia.

92.- Una empresa ha desplegado servidores en instancias de Amazon EC2 dentro de una VPC. Proveedores externos acceden a estos servidores por internet.

Recientemente, la empresa desplegó una nueva aplicación en instancias EC2 que están en un nuevo rango CIDR. La empresa necesita que esta aplicación esté disponible para los proveedores externos.

Un ingeniero de seguridad verificó que los grupos de seguridad y las ACLs de red (network ACLs) asociadas permiten los puertos necesarios en la dirección de entrada (inbound).

Sin embargo, los proveedores no pueden conectarse a la aplicación.

¿Qué solución permitirá a los proveedores acceder a la aplicación?

A. Modificar el grupo de seguridad asociado a las instancias EC2 para que tenga las mismas reglas de salida (outbound) que de entrada (inbound).

**B. Modificar la ACL de red asociada al rango CIDR para permitir tráfico de salida hacia puertos efímeros.**

C. Modificar las reglas de entrada (inbound) en la puerta de enlace de internet (internet gateway) para permitir los puertos requeridos.

D. Modificar la ACL de red asociada al rango CIDR para que tenga las mismas reglas de salida (outbound) que de entrada (inbound)

93.- Una empresa utiliza infraestructura como código (IaC) para crear infraestructura en AWS. La empresa escribe el código como plantillas de AWS CloudFormation para desplegar dicha infraestructura. Ya cuenta con una pipeline CI/CD que puede usar para desplegar esas plantillas.

Después de una reciente auditoría de seguridad, la empresa decide adoptar un enfoque de política como código para mejorar su postura de seguridad en AWS. La empresa debe evitar el despliegue de cualquier infraestructura que viole una política de seguridad, como por ejemplo un volumen de Amazon EBS sin cifrar.

¿Qué solución cumplirá con estos requisitos?

A. Activar AWS Trusted Advisor. Configurar notificaciones de seguridad como webhooks en la sección de preferencias de la pipeline CI/CD.

B. Activar AWS Config. Usar las reglas predefinidas o reglas personalizadas. Suscribir la pipeline CI/CD a un tema de Amazon SNS que reciba notificaciones desde AWS Config.

**C. Crear conjuntos de reglas en AWS CloudFormation Guard. Ejecutar validaciones de las plantillas de CloudFormation como una fase dentro del proceso de CI/CD.**

D. Crear conjuntos de reglas como SCPs (Service Control Policies). Integrar las SCPs como parte del control de validación en una fase del proceso CI/CD.

94.- Una empresa está ejecutando una instancia de Amazon RDS para MySQL dentro de una VPC. Esta VPC no debe enviar ni recibir tráfico de red a través de Internet. Un ingeniero de seguridad quiere usar AWS Secrets Manager para rotar automáticamente las credenciales de la base de datos. Sin embargo, debido a una política de seguridad, no puede usar la función estándar de AWS Lambda que proporciona Secrets Manager para realizar la rotación de credenciales. El ingeniero de seguridad despliega una función Lambda personalizada dentro de la misma VPC. Esta función se encargará de rotar el secreto en Secrets Manager. El ingeniero también edita el grupo de seguridad de la instancia RDS para permitir conexiones desde esta función. Sin embargo, cuando se invoca la función, no puede comunicarse con Secrets Manager para realizar correctamente la rotación del secreto.

¿Qué debe hacer el ingeniero de seguridad para que la función pueda rotar el secreto?

A. Agregar un egress-only Internet Gateway a la VPC. Permitir que solo la subred de la función Lambda enrute tráfico a través de ese gateway.

B. Agregar un NAT Gateway a la VPC. Configurar únicamente la subred de la función Lambda con una ruta por defecto hacia el NAT Gateway.

C. Configurar una conexión de peering con la VPC predeterminada de Secrets Manager. Configurar la subred de la función Lambda para que use esa conexión de peering en sus rutas.

**D. Configurar un endpoint de interfaz para Secrets Manager. Incluir la subred privada de la función Lambda durante el proceso de configuración.**

95.- El ingeniero de seguridad está gestionando una aplicación web tradicional de tres capas que se ejecuta en instancias de Amazon EC2. La aplicación se ha convertido en objetivo de un número creciente de ataques maliciosos desde internet.

¿Qué pasos debería tomar el ingeniero de seguridad para comprobar vulnerabilidades conocidas y reducir la superficie de ataque? (Elige dos opciones)

A. Usar AWS Certificate Manager para cifrar todo el tráfico entre el cliente y los servidores de la aplicación.

**B. Revisar los grupos de seguridad de la aplicación para asegurarse de que solo estén abiertos los puertos necesarios.**

C. Usar Elastic Load Balancing para descargar (offload) el cifrado de Secure Sockets Layer (SSL).

**D. Usar Amazon Inspector para escanear periódicamente las instancias de backend.**

E. Usar AWS Key Management Service (AWS KMS) para cifrar todo el tráfico entre el cliente y los servidores de la aplicación.

96.- Una empresa está usando Amazon Elastic Container Service (Amazon ECS) para ejecutar su aplicación basada en contenedores en AWS. La empresa necesita asegurarse de que las imágenes de los contenedores no contengan vulnerabilidades graves. También debe garantizar que solo roles IAM específicos y cuentas de AWS específicas puedan acceder a esas imágenes.

¿Qué solución cumplirá con estos requisitos con el menor esfuerzo de gestión?

A. Obtener las imágenes desde un registro público de contenedores. Publicar las imágenes en repositorios de Amazon Elastic Container Registry (Amazon ECR) con el escaneo al momento de subir configurado (scan on push) en una cuenta centralizada de AWS. Usar una canalización CI/CD para desplegar las imágenes en distintas cuentas de AWS. Usar políticas basadas en identidad para restringir qué roles IAM pueden acceder a las imágenes.

B. Obtener las imágenes desde un registro público de contenedores. Publicar las imágenes en un registro privado de contenedores alojado en instancias de Amazon EC2 dentro de una cuenta centralizada de AWS. Desplegar herramientas de escaneo de contenedores basadas en el sistema operativo en esas instancias EC2 que ejecutan Amazon ECS. Restringir el acceso a las imágenes usando autenticación básica sobre HTTPS.

**C. Obtener las imágenes desde un registro público de contenedores. Publicar las imágenes en repositorios de Amazon Elastic Container Registry (Amazon ECR) con escaneo al subir (scan on push) configurado en una cuenta centralizada de AWS. Usar una canalización CI/CD para desplegar las imágenes en distintas cuentas de AWS. Usar políticas del repositorio y políticas basadas en identidad para restringir qué roles IAM y cuentas pueden acceder a las imágenes.**

D. Obtener las imágenes desde un registro público de contenedores. Publicar las imágenes en repositorios de AWS CodeArtifact en una cuenta centralizada de AWS. Usar una canalización CI/CD para desplegar las imágenes en distintas cuentas de AWS. Usar políticas del repositorio y políticas basadas en identidad para restringir qué roles IAM y cuentas pueden acceder a las imágenes.

97.- Los científicos de datos de una empresa quieren crear modelos de entrenamiento de inteligencia artificial y aprendizaje automático (IA/ML) usando Amazon SageMaker. Los modelos utilizarán grandes conjuntos de datos almacenados en un bucket de Amazon S3. Estos conjuntos de datos contienen información sensible.

En promedio, los científicos de datos necesitan 30 días para entrenar los modelos. El bucket de S3 ha sido asegurado adecuadamente. La política de retención de datos de la empresa establece que todos los datos que tengan más de 45 días deben eliminarse del bucket de S3.

¿Qué acción debe tomar un ingeniero de seguridad para aplicar esta política de retención de datos?

**A. Configurar una regla de ciclo de vida (Lifecycle rule) en el bucket de S3 para eliminar los objetos después de 45 días.**

B. Crear una función de AWS Lambda que revise la fecha de última modificación de los objetos en S3 y elimine aquellos que tengan más de 45 días. Crear una notificación de evento en S3 para invocar la función Lambda cada vez que se realice una operación PutObject.

C. Crear una función de AWS Lambda que revise la fecha de última modificación de los objetos en S3 y elimine aquellos que tengan más de 45 días. Crear una regla de Amazon EventBridge para invocar la función Lambda una vez al mes.

D. Configurar S3 Intelligent-Tiering en el bucket de S3 para que los objetos se transfieran automáticamente a otra clase de almacenamiento.

98.- Un ingeniero de seguridad está solucionando un problema con una función de AWS Lambda llamada MyLambdaFunction. La función está generando un error cuando intenta leer los objetos de un bucket de Amazon S3 llamado DOC-EXAMPLE-BUCKET. El bucket tiene la siguiente política de bucket:

¿Qué cambio debe hacer el ingeniero de seguridad en la política para asegurarse de que la función Lambda pueda leer los objetos del bucket?

A. Eliminar el elemento Condition. Cambiar el elemento Principal al siguiente:

B. Cambiar el elemento Action al siguiente:

**C. Cambiar el elemento Resource a: "arn:aws:s3:::DOC-EXAMPLE-BUCKET/\*"**

D. Cambiar el elemento Resource a: "arn:aws:lambda:::function:MyLambdaFunction" Cambiar el elemento Principal al siguiente:

99.- Un usuario de IAM recibe un mensaje de “Acceso denegado” cuando intenta acceder a objetos en un bucket de Amazon S3. El usuario y el bucket S3 están en la misma cuenta de AWS. El bucket está configurado para usar cifrado del lado del servidor con claves de AWS KMS (SSE-KMS) para cifrar todos sus objetos en reposo, utilizando una clave administrada por el cliente (customer managed key) de la misma cuenta de AWS. El bucket no tiene ninguna política de bucket definida. Al usuario de IAM se le han otorgado permisos mediante una política de IAM que permite la acción kms:Decrypt sobre la clave administrada por el cliente. La política de IAM también permite las acciones s3:List\* y s3:Get\* sobre el bucket de S3 y sus objetos.

¿Cuál de las siguientes podría ser una razón por la cual el usuario de IAM no puede acceder a los objetos del bucket S3?

A. La política de IAM necesita permitir también el permiso kms:DescribeKey.

B. El bucket de S3 fue cambiado para usar una clave administrada por AWS (AWS managed key) para cifrar los objetos en reposo.

C. Se necesita agregar una política de bucket (bucket policy) que permita al usuario de IAM acceder a los objetos.

**D. La política de la clave KMS fue editada para quitar el acceso completo a la clave para la cuenta de AWS.**

100.- Una empresa tiene una política que exige que todos los datos de los buckets de Amazon S3 estén cifrados durante la transmisión. Un ingeniero de seguridad debe implementar una política de bucket de S3 que niegue cualquier operación si los datos no están cifrados.

¿Qué política de bucket de S3 cumplirá con este requisito?

A.

**B.**

C.

D.

101.- Un ingeniero de seguridad quiere usar Amazon Simple Notification Service (SNS) para enviar alertas por correo electrónico al equipo de seguridad de la empresa cuando Amazon GuardDuty detecte hallazgos con nivel de alta severidad. Además, quiere enviar estos hallazgos a una herramienta de visualización para analizarlos más a fondo.

¿Qué solución cumple mejor con estos requisitos?

A. Configurar GuardDuty para que envíe notificaciones a una alarma de Amazon CloudWatch con dos destinos. Desde CloudWatch, transmitir los hallazgos mediante Amazon Kinesis Data Streams hacia un dominio de Amazon OpenSearch Service como primer destino. Usar Amazon QuickSight para visualizar los hallazgos y realizar análisis adicionales mediante consultas en OpenSearch. Para las alertas por correo electrónico, configurar un tema de SNS como segundo destino de la alarma de CloudWatch. Usar reglas de eventos de Amazon EventBridge con patrones que filtren solo los hallazgos de alta severidad.

B. Configurar GuardDuty para que envíe notificaciones a AWS CloudTrail con dos destinos. Desde CloudTrail, transmitir los hallazgos mediante Amazon Kinesis Data Firehose hacia un dominio de OpenSearch como primer destino. Usar OpenSearch Dashboards para visualizar los hallazgos y consultas para analizarlos. Para las alertas por correo electrónico, configurar un tema de SNS como segundo destino de CloudTrail. Usar reglas de eventos de CloudTrail para filtrar solo los hallazgos de alta severidad.

**C. Configurar GuardDuty para que envíe notificaciones a Amazon EventBridge con dos destinos. Desde EventBridge, transmitir los hallazgos mediante Amazon Kinesis Data Firehose hacia un dominio de OpenSearch como primer destino. Usar OpenSearch Dashboards para visualizar los hallazgos y consultas para analizarlos. Para las alertas por correo electrónico, configurar un tema de SNS como segundo destino de EventBridge. Usar reglas de EventBridge con patrones para enviar solo los hallazgos de alta severidad.**

D. Configurar GuardDuty para que envíe notificaciones a Amazon EventBridge con dos destinos. Desde EventBridge, transmitir los hallazgos mediante Amazon Kinesis Data Streams hacia un dominio de OpenSearch como primer destino. Usar Amazon QuickSight para visualizar los hallazgos y consultas para analizarlos. Para las alertas por correo electrónico, configurar un tema de SNS como segundo destino de EventBridge. Usar reglas de EventBridge con patrones para enviar solo los hallazgos de alta severidad.

102.- Un ingeniero de seguridad necesita implementar un modelo de escritura única y lectura múltiple (WORM) para los datos que una empresa almacenará en buckets de Amazon S3. La empresa utiliza la clase de almacenamiento S3 Standard para todos sus buckets de S3. El ingeniero de seguridad debe asegurarse de que los objetos no puedan ser sobrescritos ni eliminados por ningún usuario, incluido el usuario root de la cuenta de AWS.

¿Qué solución cumplirá con estos requisitos?

**A. Crear nuevos buckets de S3 con S3 Object Lock habilitado en modo de cumplimiento. Colocar los objetos en los buckets de S3.**

B. Usar S3 Glacier Vault Lock para adjuntar una política de bloqueo de bóveda (Vault Lock) a nuevos buckets de S3. Esperar 24 horas para completar el proceso de bloqueo. Colocar los objetos en los buckets de S3.

C. Crear nuevos buckets de S3 con S3 Object Lock habilitado en modo de gobernanza (governance mode). Colocar los objetos en los buckets de S3.

D. Crear nuevos buckets de S3 con S3 Object Lock habilitado en modo de gobernanza (governance mode). Agregar una retención legal (legal hold) a los buckets de S3. Colocar los objetos en los buckets de S3.

103.- Una empresa necesita cifrado completo del tráfico entre los usuarios externos y una aplicación. La empresa aloja la aplicación en un conjunto de instancias de Amazon EC2 que se ejecutan en un grupo de Auto Scaling detrás de un Application Load Balancer (ALB).

¿Cómo puede un ingeniero de seguridad cumplir con estos requisitos?

A. Crear un nuevo certificado emitido por Amazon en AWS Secrets Manager. Exportar el certificado desde Secrets Manager. Importar el certificado en el ALB y en las instancias EC2.

B. Crear un nuevo certificado emitido por Amazon en AWS Certificate Manager (ACM). Asociar el certificado con el ALB. Exportar el certificado desde ACM. Instalar el certificado en las instancias EC2.

C. Importar un nuevo certificado de un proveedor externo en AWS Identity and Access Management (IAM). Exportar el certificado desde IAM. Asociar el certificado con el ALB y con las instancias EC2.

**D. Importar un nuevo certificado de un proveedor externo en AWS Certificate Manager (ACM). Asociar el certificado con el ALB. Instalar el certificado en las instancias EC2.**

104.- Una empresa tiene una organización configurada con SCPs (políticas de control de servicios) en AWS Organizations. La SCP raíz de la organización es la siguiente:

Los desarrolladores de la empresa forman parte de un grupo que tiene una política de IAM que permite el acceso a Amazon Simple Email Service (Amazon SES) mediante la acción ses:\*. La cuenta pertenece a una unidad organizativa (OU) que tiene una SCP que permite el uso de Amazon SES. Sin embargo, los desarrolladores están recibiendo un error de "no autorizado" al intentar acceder a Amazon SES desde la consola de administración de AWS.

¿Qué cambio debe implementar un ingeniero de seguridad para que los desarrolladores puedan acceder a Amazon SES?

A. Agregar una política de recursos que permita a cada miembro del grupo acceder a Amazon SES.

B. Agregar una política de recursos que permita "Principal": {"AWS": "arn:aws:iam::número-de-cuenta:group/Dev"}.

C. Eliminar el control de AWS Control Tower (guardrail) que restringe el acceso a Amazon SES.

**D. Eliminar Amazon SES de la SCP raíz.**

105.- Una empresa aloja un sitio web público en una instancia de Amazon EC2. El tráfico HTTPS debe poder acceder al sitio web. La empresa utiliza SSH para la administración del servidor web.

El sitio web se encuentra en la subred 10.0.1.0/24. La subred de administración es 192.168.100.0/24. Un ingeniero de seguridad debe crear un grupo de seguridad para la instancia EC2.

¿Qué combinación de pasos debe tomar el ingeniero de seguridad para cumplir con estos requisitos de la forma más segura posible? (Elige dos opciones).

A. Permitir el puerto 22 desde la fuente 0.0.0.0/0.

**B. Permitir el puerto 443 desde la fuente 0.0.0.0/0.**

**C. Permitir el puerto 22 desde 192.168.100.0/24.**

D. Permitir el puerto 22 desde 10.0.1.0/24.

E. Permitir el puerto 443 desde 10.0.1.0/24.

106.- Un ingeniero de seguridad quiere reenviar registros personalizados de seguridad de una aplicación desde una instancia de Amazon EC2 hacia Amazon CloudWatch. El ingeniero instala el agente de CloudWatch en la instancia EC2 y agrega la ruta de los registros al archivo de configuración de CloudWatch.

Sin embargo, CloudWatch no recibe los registros. El ingeniero de seguridad verifica que el servicio awslogs esté en ejecución en la instancia EC2.

¿Qué debería hacer el ingeniero de seguridad a continuación para resolver el problema?

A. Agregar AWS CloudTrail a la política de confianza de la instancia EC2. Enviar los registros personalizados a CloudTrail en lugar de CloudWatch.

B. Agregar Amazon S3 a la política de confianza de la instancia EC2. Configurar la aplicación para que escriba los registros personalizados en un bucket de S3 que CloudWatch pueda usar para ingerir los registros.

C. Agregar Amazon Inspector a la política de confianza de la instancia EC2. Usar Amazon Inspector en lugar del agente de CloudWatch para recopilar los registros personalizados.

**D. Adjuntar la política administrada CloudWatchAgentServerPolicy al rol de la instancia EC2.**

107.- Un ingeniero de sistemas está solucionando problemas de conectividad en un entorno de pruebas que incluye un dispositivo de seguridad virtual desplegado en línea. Además de usar este dispositivo de seguridad virtual, el equipo de desarrollo quiere utilizar grupos de seguridad y listas de control de acceso a la red (ACLs) para cumplir con distintos requisitos de seguridad en el entorno.

¿Qué configuración es necesaria para permitir que el dispositivo de seguridad virtual enrute el tráfico?

A. Desactivar las ACLs de red.

B. Configurar la interfaz de red elástica del dispositivo de seguridad en modo promiscuo.

**C. Deshabilitar la verificación de origen/destino de red en la interfaz de red elástica del dispositivo de seguridad.**

D. Colocar el dispositivo de seguridad en la subred pública con la gateway de internet.

108.- Un ingeniero de seguridad necesita crear una política de bucket de Amazon S3 para otorgar el mínimo privilegio de acceso de solo lectura a las cuentas de usuario IAM llamadas User1, User2 y User3. Estas cuentas de usuario IAM son miembros del grupo IAM llamado AuthorizedPeople.

El ingeniero de seguridad redacta la siguiente política para el bucket de S3:

Al intentar agregar la política al bucket de S3, aparece el siguiente mensaje de error: "Missing required field Principal" (Falta el campo requerido Principal).

El ingeniero de seguridad está añadiendo un elemento Principal a la política. Esta adición debe proporcionar acceso de lectura únicamente a User1, User2 y User3.

¿Qué solución cumple con estos requisitos?

**A.**

B.

C.

D.

109.- Un ingeniero de seguridad rotó recientemente todas las claves de acceso IAM en una cuenta de AWS. Luego, configuró AWS Config y habilitó las siguientes reglas administradas de AWS Config: mfa-enabled-for-iam-console-access iam-user-mfa-enabled access-keys-rotated iam-user-unused-credentials-check

El ingeniero de seguridad nota que todos los recursos aparecen como no conformes después de ejecutar la operación GenerateCredentialReport de la API de IAM.

¿Cuál podría ser la razón del estado de no conformidad?

**A. El informe de credenciales de IAM se generó en las últimas 4 horas.**

B. El ingeniero de seguridad no tiene el permiso GenerateCredentialReport.

C. El ingeniero de seguridad no tiene el permiso GetCredentialReport.

D. Las reglas de AWS Config tienen un valor de MaximumExecutionFrequency de 24 horas.

110.- Una empresa está usando AWS WAF para proteger un servicio de API pública personalizada que se basa en instancias de Amazon EC2. La API utiliza un Application Load Balancer.

La ACL web de AWS WAF está configurada con un grupo de reglas administradas por AWS (AWS Managed Rules). Después de una actualización del software de la API y de la aplicación cliente, algunos tipos de solicitudes dejaron de funcionar y están causando problemas de estabilidad en la aplicación. Un ingeniero de seguridad descubre que el registro (logging) de AWS WAF no está activado para la ACL web.

El ingeniero de seguridad necesita restaurar inmediatamente el servicio, resolver el problema y asegurarse de que el registro no se desactive en el futuro. El ingeniero activa el registro para la ACL web y establece Amazon CloudWatch Logs como destino.

¿Qué conjunto adicional de pasos debe tomar el ingeniero de seguridad para cumplir con estos requisitos?

**A. Editar las reglas en la ACL web para incluir reglas con acción Count. Revisar los registros para identificar qué regla está bloqueando las solicitudes. Modificar la política IAM de todos los administradores de AWS WAF para que no puedan eliminar la configuración de registro de ninguna ACL web de AWS WAF.**

B. Editar las reglas en la ACL web para incluir reglas con acción Count. Revisar los registros para identificar qué regla está bloqueando las solicitudes. Modificar la política de recursos de AWS WAF para que los administradores no puedan eliminar la configuración de registro de ninguna ACL web de AWS WAF.

C. Editar las reglas en la ACL web para incluir reglas con acciones Count y Challenge. Revisar los registros para identificar qué regla está bloqueando las solicitudes. Modificar la política de recursos de AWS WAF para que los administradores no puedan eliminar la configuración de registro de ninguna ACL web de AWS WAF.

D. Editar las reglas en la ACL web para incluir reglas con acciones Count y Challenge. Revisar los registros para identificar qué regla está bloqueando las solicitudes. Modificar la política IAM de todos los administradores de AWS WAF para que no puedan eliminar la configuración de registro de ninguna ACL web de AWS WAF.

111.- Un ingeniero de seguridad está creando una función AWS Lambda. Esta función necesita usar un rol llamado LambdaAuditRole para asumir un rol llamado AcmeAuditFactoryRole, que está en otra cuenta de AWS.

Cuando se ejecuta el código, aparece el siguiente mensaje de error: "An error occurred (AccessDenied) when calling the AssumeRole operation." (Se produjo un error (AccessDenied) al invocar la operación AssumeRole.)

¿Qué combinación de pasos debe seguir el ingeniero de seguridad para resolver este error? (Elige dos.)

**A. Asegurarse de que LambdaAuditRole tenga el permiso sts:AssumeRole para asumir el rol AcmeAuditFactoryRole.**

B. Asegurarse de que LambdaAuditRole tenga asociada la política administrada AWSLambdaBasicExecutionRole.

**C. Asegurarse de que la política de confianza (trust policy) del rol AcmeAuditFactoryRole permita la acción sts:AssumeRole desde el rol LambdaAuditRole.**

D. Asegurarse de que la política de confianza de LambdaAuditRole permita la acción sts:AssumeRole desde el servicio lambda.amazonaws.com.

E. Asegurarse de que la llamada a la API sts:AssumeRole se esté realizando contra el endpoint de la región us-east-1.

112.- Una empresa tiene cuentas de AWS dentro de una organización en AWS Organizations. La organización incluye una cuenta dedicada a la seguridad.

Toda la actividad en las cuentas miembro debe ser registrada y reportada a la cuenta de seguridad dedicada. La empresa debe conservar todos los registros de actividad en una ubicación de almacenamiento segura dentro de la cuenta de seguridad por un período de 2 años. No se permiten modificaciones ni eliminaciones de los registros.

¿Qué combinación de pasos cumplirá con estos requisitos con el menor esfuerzo operativo? (Elige dos opciones).

**A. En la cuenta de seguridad dedicada, crear un bucket de Amazon S3. Configurar S3 Object Lock en modo de cumplimiento con un período de retención de 2 años. Establecer una política del bucket que permita que la cuenta de administración de la organización escriba en el bucket.**

B. En la cuenta de seguridad dedicada, crear un bucket de Amazon S3. Configurar S3 Object Lock en modo de cumplimiento (compliance mode) con un período de retención de 2 años. Establecer una política del bucket que permita que las cuentas miembro de la organización escriban en el bucket.

C. En la cuenta de seguridad dedicada, crear un bucket de Amazon S3 con una configuración de ciclo de vida (Lifecycle) que expire los objetos después de 2 años. Establecer una política del bucket que permita que las cuentas miembro de la organización escriban en el bucket.

**D. Crear un AWS CloudTrail trail a nivel de organización. Configurar los registros para que se envíen al bucket de S3 de registro en la cuenta de seguridad dedicada.**

E. Activar AWS CloudTrail en cada cuenta. Configurar los registros para que se envíen a un bucket de Amazon S3 creado en la cuenta de administración de la organización. Reenviar los registros al bucket de S3 en la cuenta de seguridad dedicada utilizando AWS Lambda y Amazon Kinesis Data Firehose.

113.- Una empresa está probando su plan de respuesta ante incidentes por credenciales comprometidas. La empresa ejecuta una base de datos en una instancia de Amazon EC2 y guarda las credenciales sensibles de la base de datos como un secreto en AWS Secrets Manager. El secreto tiene habilitada la rotación mediante una función de AWS Lambda que utiliza la plantilla genérica de rotación. La instancia EC2 y la función Lambda están desplegadas en la misma subred privada. La VPC cuenta con un punto de enlace de VPC para Secrets Manager.

Un ingeniero de seguridad descubre que el secreto no se puede rotar. Determina que el punto de enlace de VPC funciona correctamente. Los registros de Amazon CloudWatch muestran el siguiente error: "setSecret: No se puede iniciar sesión en la base de datos".

¿Cuál solución resolverá este error?

A. Usar la consola de administración de AWS para editar la estructura JSON del secreto en Secrets Manager, de modo que el secreto cumpla automáticamente con el formato requerido por la base de datos.

**B. Asegurarse de que el grupo de seguridad asociado a la función Lambda permita conexiones salientes hacia la instancia EC2. Asegurarse de que el grupo de seguridad de la instancia EC2 permita conexiones entrantes desde el grupo de seguridad de la función Lambda.**

C. Usar el comando list-secrets de Secrets Manager en la AWS CLI para listar el secreto. Identificar las credenciales de la base de datos. Usar el comando rotate-secret de Secrets Manager en la CLI para forzar la rotación inmediata del secreto.

D. Agregar una puerta de enlace a Internet (Internet Gateway) a la VPC. Crear una puerta de enlace NAT en una subred pública. Actualizar las tablas de ruteo de la VPC para que el tráfico desde la función Lambda y desde la instancia EC2 pueda llegar al endpoint público de Secrets Manager.

114.- Una empresa implementa un conjunto de roles estándar de IAM en sus cuentas de AWS. Estos roles están basados en las funciones laborales dentro de la empresa. Para equilibrar la eficiencia operativa con la seguridad, un ingeniero de seguridad implementó SCPs (políticas de control de servicios) de AWS Organizations para restringir el acceso a servicios de seguridad críticos en todas las cuentas de la empresa.

Todas las cuentas y unidades organizativas (OU) dentro de AWS Organizations tienen adjunta por defecto la política FullAWSAccess. El ingeniero de seguridad necesita asegurarse de que nadie pueda desactivar Amazon GuardDuty ni AWS Security Hub. Además, debe evitar sobrescribir otros permisos que ya hayan sido concedidos por las políticas de IAM definidas en las cuentas.

¿Qué SCP debe adjuntar el ingeniero de seguridad a la raíz de la organización para cumplir con estos requisitos?

**A.**

B.

C.

D.

115.- na empresa necesita seguir las mejores prácticas de seguridad para implementar recursos a partir de una plantilla de AWS CloudFormation. La plantilla de CloudFormation debe poder configurar credenciales sensibles de una base de datos.

La empresa ya utiliza AWS Key Management Service (AWS KMS) y AWS Secrets Manager.

¿Qué solución cumplirá con los requisitos?

**A. Usar una referencia dinámica en la plantilla de CloudFormation para hacer referencia a las credenciales de la base de datos almacenadas en Secrets Manager.**

B. Usar un parámetro en la plantilla de CloudFormation para referenciar las credenciales de la base de datos. Cifrar la plantilla de CloudFormation usando AWS KMS.

C. Usar un parámetro tipo SecureString en la plantilla de CloudFormation para referenciar las credenciales de la base de datos en Secrets Manager.

D. Usar un parámetro tipo SecureString en la plantilla de CloudFormation para referenciar un valor cifrado con AWS KMS.

116.- Una empresa internacional quiere combinar los hallazgos de AWS Security Hub de todas las regiones de AWS de la empresa y de múltiples cuentas. Además, la empresa desea crear un panel centralizado personalizado para correlacionar estos hallazgos con datos operativos, con el fin de realizar un análisis más profundo y obtener información valiosa. La empresa necesita una herramienta de análisis para buscar y visualizar los hallazgos de Security Hub.

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

A. Designar una cuenta de AWS como administrador delegado de Security Hub. Publicar eventos en Amazon CloudWatch desde la cuenta administradora delegada, todas las cuentas miembro y las regiones necesarias habilitadas para los hallazgos de Security Hub.

**B. Designar una cuenta de AWS dentro de una organización en AWS Organizations como administrador delegado de Security Hub. Publicar eventos en Amazon EventBridge desde la cuenta administradora delegada, todas las cuentas miembro y las regiones necesarias habilitadas para los hallazgos de Security Hub.**

C. En cada región, crear una regla de Amazon EventBridge para enviar los hallazgos a un stream de Amazon Kinesis Data Streams. Configurar los streams de Kinesis para que escriban los registros en un único bucket de Amazon S3.

**D. En cada región, crear una regla de Amazon EventBridge para enviar los hallazgos a un stream de entrega de Amazon Kinesis Data Firehose. Configurar los streams de Kinesis Data Firehose para que entreguen los registros en un único bucket de Amazon S3.**

E. Usar AWS Glue DataBrew para rastrear el bucket de Amazon S3 y construir el esquema. Usar AWS Glue Data Catalog para consultar los datos y crear vistas que aplanen los atributos anidados. Construir paneles en Amazon QuickSight usando Amazon Athena.

**F. Particionar los datos del bucket de Amazon S3. Usar AWS Glue para rastrear el bucket de S3 y construir el esquema. Usar Amazon Athena para consultar los datos y crear vistas que aplanen los atributos anidados. Construir paneles de Amazon QuickSight que usen las vistas de Athena.**

117.- Un administrador de una cuenta de AWS creó un grupo de IAM y aplicó la siguiente política administrada para exigir que cada usuario se autentique usando autenticación multifactor (MFA):

Después de implementar la política, el administrador recibe informes de que los usuarios no pueden ejecutar comandos de Amazon EC2 usando la AWS CLI.

¿Qué debería hacer el administrador para resolver este problema y seguir exigiendo el uso de MFA?

A. Cambiar el valor de aws:MultiFactorAuthPresent a true.

**B. Indicar a los usuarios que ejecuten el comando aws sts get-session-token en la CLI y que incluyan los parámetros --serial-number y --token-code para MFA. Usar los valores resultantes para realizar llamadas a la API/CLI.**

C. Implementar acceso federado a la API/CLI usando SAML 2.0, y luego configurar el proveedor de identidad para exigir autenticación multifactor.

D. Crear un rol e imponer la autenticación multifactor en la política de confianza del rol. Indicar a los usuarios que ejecuten el comando sts assume-role en la CLI y que pasen los parámetros --serial-number y --token-code. Almacenar los valores resultantes en variables de entorno. Agregar sts:AssumeRole a NotAction en la política.

118.- Una empresa está desarrollando un mecanismo que permitirá a los científicos de datos usar Amazon SageMaker para leer, procesar y guardar datos en un bucket de Amazon S3. Cada científico de datos tendrá acceso a un prefijo dedicado dentro del bucket para cada uno de sus proyectos. La empresa implementará políticas de bucket que usen esos prefijos dedicados para restringir el acceso a los objetos en S3. Los proyectos pueden durar hasta 60 días.

El equipo de seguridad de la empresa exige que los datos no permanezcan en el bucket de S3 después de que finalicen los proyectos que usaron esos datos.

¿Qué solución cumplirá con estos requisitos de la manera más rentable?

A. Crear una función de AWS Lambda que identifique y elimine los objetos del bucket de S3 que no hayan sido accedidos en los últimos 60 días. Crear una regla programada de Amazon EventBridge que se ejecute todos los días para invocar la función Lambda.

B. Crear un nuevo bucket de S3. Configurarlo para usar S3 Intelligent-Tiering. Copiar los objetos al nuevo bucket.

**C. Crear una configuración de ciclo de vida en S3 para cada prefijo del bucket según el proyecto. Configurar la política para que los objetos expiren después de 60 días.**

D. Crear una función de AWS Lambda para eliminar objetos que no hayan sido accedidos en 60 días. Crear una notificación de evento en S3 que se dispare cuando S3 Intelligent-Tiering archive objetos automáticamente, y que invoque la función Lambda.

119.- Una empresa tiene cuentas de AWS que están organizadas dentro de una organización de AWS Organizations. Un bucket de Amazon S3 en una de las cuentas es accesible públicamente.

Un ingeniero de seguridad debe modificar la configuración para que el bucket de S3 deje de ser accesible públicamente. Además, debe garantizar que el bucket no pueda hacerse público en el futuro.

¿Qué solución cumple con estos requisitos?

A. Configurar el bucket de S3 para que use una clave de AWS Key Management Service (AWS KMS). Cifrar todos los objetos en el bucket mediante una política de bucket que exija cifrado. Configurar una SCP para denegar la acción s3:GetObject en la unidad organizativa (OU) que contiene la cuenta de AWS.

B. Habilitar la configuración de PublicAccessBlock en el bucket de S3. Configurar una SCP para denegar la acción s3:GetObject para la OU que contiene la cuenta de AWS.

**C. Habilitar la configuración de PublicAccessBlock en el bucket de S3. Configurar una SCP para denegar la acción s3:PutPublicAccessBlock para la OU que contiene la cuenta de AWS.**

D. Configurar el bucket de S3 para que use S3 Object Lock en modo de gobernanza. Configurar una SCP para denegar la acción s3:PutPublicAccessBlock para la OU que contiene la cuenta de AWS.

120.- Una empresa está diseñando una nueva pila de aplicaciones. El diseño incluye servidores web y servidores backend alojados en instancias de Amazon EC2. También incluye un clúster de base de datos Amazon Aurora MySQL.

Las instancias EC2 están en un grupo de Auto Scaling que usa plantillas de lanzamiento (launch templates). Las instancias EC2 para la capa web y la capa backend utilizan volúmenes de Amazon EBS, pero ninguna de las capas está cifrada en reposo. Un ingeniero de seguridad necesita implementar cifrado en reposo.

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

**A. Modificar la configuración predeterminada de cifrado de EBS en la región de AWS objetivo para habilitar el cifrado. Usar una actualización de instancias del grupo de Auto Scaling.**

B. Modificar las plantillas de lanzamiento para la capa web y la capa backend para agregar cifrado de AWS Certificate Manager (ACM) a los volúmenes EBS adjuntos. Usar una actualización de instancias del grupo de Auto Scaling.

**C. Crear un nuevo clúster de base de datos cifrado con AWS Key Management Service (AWS KMS) a partir de una instantánea del clúster existente.**

D. Aplicar cifrado de AWS Key Management Service (AWS KMS) al clúster de base de datos existente.

E. Aplicar cifrado de AWS Certificate Manager (ACM) al clúster de base de datos existente.

121.- Una empresa utiliza federación SAML con AWS Identity and Access Management (IAM) para proporcionar inicio de sesión único (SSO) a sus usuarios internos en las cuentas de AWS. Como parte del ciclo de vida normal, se rotó el certificado del proveedor de identidad de la empresa. Poco después, los usuarios comenzaron a recibir el siguiente error al intentar iniciar sesión:

"Error: Response Signature Invalid (Service: AWSSecurityTokenService; Status Code: 400; Error Code: InvalidIdentityToken)"

Un ingeniero de seguridad necesita resolver el problema inmediato y asegurarse de que no vuelva a ocurrir.

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

A. Descargar una nueva copia del archivo de metadatos SAML desde el proveedor de identidad. Crear una nueva entidad de proveedor de identidad IAM. Subir el nuevo archivo de metadatos a esta nueva entidad.

**B. Durante el próximo período de rotación del certificado y antes de que expire el certificado actual, agregar un nuevo certificado como secundario en el proveedor de identidad. Generar un nuevo archivo de metadatos y subirlo a la entidad de proveedor de identidad IAM existente. Realizar la rotación del certificado de forma automática o manual cuando sea necesario.**

**C. Descargar una nueva copia del archivo de metadatos SAML desde el proveedor de identidad. Subir los nuevos metadatos a la entidad de proveedor de identidad IAM ya configurada para la integración SAML en cuestión.**

D. Durante el próximo período de rotación del certificado y antes de que expire el certificado actual, agregar un nuevo certificado como secundario en el proveedor de identidad. Generar una nueva copia del archivo de metadatos y crear una nueva entidad de proveedor de identidad IAM. Subir el archivo de metadatos a esta nueva entidad. Realizar la rotación del certificado de forma automática o manual cuando sea necesario.

E. Descargar una nueva copia del archivo de metadatos SAML desde el proveedor de identidad. Crear una nueva entidad de proveedor de identidad IAM. Subir el nuevo archivo de metadatos a esta entidad. Actualizar la configuración del proveedor de identidad para que la aserción SAML use el nuevo nombre de la entidad de proveedor de identidad IAM.

122.- Una empresa está implementando una nueva aplicación en una nueva cuenta de AWS. Se ha creado una VPC y subredes para dicha aplicación. La aplicación ha sido emparejada (peered) con una VPC existente en otra cuenta, dentro de la misma región de AWS, para acceder a bases de datos.

Las instancias de Amazon EC2 se crearán y eliminarán regularmente en la VPC de la aplicación, pero solo algunas de ellas necesitarán acceso a las bases de datos en la VPC emparejada, específicamente a través del puerto TCP 1521.

Un ingeniero de seguridad debe asegurarse de que solo las instancias EC2 que lo requieran puedan acceder a las bases de datos a través de la red.

¿Cómo puede el ingeniero de seguridad implementar esta solución?

A. Crear un nuevo grupo de seguridad en la VPC de bases de datos y agregar una regla de entrada que permita todo el tráfico desde el rango de direcciones IP de la VPC de la aplicación. Crear una nueva regla en la ACL de red de las subredes de base de datos para permitir el tráfico TCP al puerto 1521 desde el rango de IP de la VPC de la aplicación. Asociar el nuevo grupo de seguridad a las instancias de base de datos que necesiten ser accedidas por la aplicación.

B. Crear un nuevo grupo de seguridad en la VPC de la aplicación con una regla de entrada que permita el rango de IP de la VPC de base de datos en el puerto TCP 1521. Crear un nuevo grupo de seguridad en la VPC de base de datos con una regla de entrada que permita el rango de IP de la VPC de la aplicación en el puerto 1521. Asociar estos grupos de seguridad tanto a las instancias de base de datos como a las instancias de aplicación que necesiten acceso.

**C. Crear un nuevo grupo de seguridad en la VPC de la aplicación sin reglas de entrada. Crear un nuevo grupo de seguridad en la VPC de base de datos con una regla de entrada que permita tráfico TCP al puerto 1521 desde ese grupo de seguridad de la VPC de la aplicación. Asociar el grupo de seguridad de la aplicación a las instancias que necesiten acceso y el grupo de seguridad de base de datos a las instancias de base de datos.**

D. Crear un nuevo grupo de seguridad en la VPC de la aplicación con una regla de entrada que permita el rango de IP de la VPC de base de datos en el puerto TCP 1521. Agregar una nueva regla en la ACL de red de las subredes de base de datos para permitir todo el tráfico desde el rango de IP de la VPC de la aplicación. Asociar este grupo de seguridad a las instancias de aplicación que necesiten acceso a la base de datos.

123.- Una empresa necesita una solución de registro forense para cientos de aplicaciones que se ejecutan en contenedores Docker sobre instancias de Amazon EC2. La solución debe: Realizar análisis en tiempo real de los registros, Soportar la reproducción de mensajes (replay), y Conservar (persistir) los registros.

¿Qué servicios de AWS deberían utilizarse para cumplir con estos requisitos? (Elige dos opciones).

A. Amazon Athena

**B. Amazon Kinesis**

C. Amazon SQS

**D. Amazon OpenSearch Service**

E. Amazon EMR

124.- Una empresa tiene muchas cuentas miembro dentro de una organización en AWS Organizations. La empresa está preocupada por el posible uso indebido de las credenciales del usuario raíz de las cuentas miembro. Para abordar este riesgo, la empresa quiere asegurarse de que incluso si se comprometen las credenciales del usuario raíz, la cuenta permanezca protegida.

¿Qué solución cumple con este requisito?

**A. Bloquear el acceso a los servicios mediante SCPs para el usuario raíz**

B. Eliminar la contraseña del usuario raíz

C. Eliminar las claves de acceso del usuario raíz

D. Crear una regla de Amazon EventBridge para detectar cualquier evento de API realizado por el usuario raíz de la cuenta

125.- Un grupo de Auto Scaling de Amazon EC2 lanza instancias EC2 con Amazon Linux e instala el agente de Amazon CloudWatch para publicar registros en Amazon CloudWatch Logs. Las instancias EC2 se inician con un rol de IAM que tiene una política IAM adjunta. Esta política otorga acceso para publicar métricas personalizadas en CloudWatch. Las instancias EC2 se ejecutan en una subred privada dentro de una VPC. La VPC proporciona acceso a internet para subredes privadas a través de un gateway NAT.

Un ingeniero de seguridad nota que no se están publicando registros en CloudWatch Logs desde las instancias EC2 que lanza el grupo de Auto Scaling. El ingeniero valida que el agente de CloudWatch Logs se está ejecutando y está correctamente configurado en las instancias EC2. Además, verifica que la comunicación de red con los servicios de AWS funciona correctamente.

¿Qué puede hacer el ingeniero de seguridad para asegurarse de que los registros se publiquen en CloudWatch Logs?

A. Configurar la política IAM usada por el rol de IAM para que tenga acceso a las acciones necesarias de la API cloudwatch: que publican registros.

B. Ajustar el rol vinculado al servicio de Auto Scaling para que tenga permisos para escribir en CloudWatch Logs.

**C. Configurar la política IAM usada por el rol de IAM para que tenga acceso a las acciones necesarias de la API logs: de AWS que publican registros.**

D. Agregar un endpoint de interfaz (VPC endpoint) para proporcionar una ruta hacia CloudWatch Logs.

126.- Una empresa utiliza contenedores de Amazon Elastic Container Service (Amazon ECS) con el tipo de lanzamiento Fargate. Los contenedores ejecutan aplicaciones web y móviles desarrolladas en Java y Node.js. Para cumplir con los requisitos de segmentación de red, cada unidad de negocio de la empresa implementa sus aplicaciones en su propia cuenta dedicada de AWS. Cada unidad de negocio almacena las imágenes de los contenedores en un registro privado de Amazon Elastic Container Registry (Amazon ECR) en su respectiva cuenta.

Un ingeniero de seguridad debe recomendar una solución para escanear los contenedores de ECS y los registros ECR en busca de vulnerabilidades en sistemas operativos y bibliotecas de lenguajes de programación. El equipo de auditoría de la empresa debe poder identificar vulnerabilidades potenciales en cualquiera de las cuentas donde se implementan las aplicaciones.

¿Qué solución cumplirá con estos requisitos?

**A. En cada cuenta, actualizar el registro ECR para usar Amazon Inspector en lugar del servicio de escaneo predeterminado. Configurar Amazon Inspector para enviar los hallazgos de vulnerabilidades a AWS Security Hub en una cuenta central de seguridad. Dar acceso al equipo de auditoría para que revise los hallazgos desde Security Hub.**

B. En cada cuenta, configurar AWS Config para monitorear la configuración de los contenedores ECS y del registro ECR. Configurar paquetes de conformidad (conformance packs) de AWS Config para escaneo de vulnerabilidades. Crear un agregador de AWS Config en una cuenta central para recopilar detalles de configuración y cumplimiento de todas las cuentas. Dar acceso al equipo de auditoría a AWS Config en la cuenta con el agregador.

C. En cada cuenta, configurar AWS Audit Manager para escanear los contenedores ECS y el registro ECR. Configurar Audit Manager para enviar los hallazgos de vulnerabilidades a AWS Security Hub en una cuenta central de seguridad. Dar acceso al equipo de auditoría para revisar los hallazgos desde Security Hub.

D. En cada cuenta, configurar Amazon GuardDuty para escanear los contenedores ECS y el registro ECR. Configurar GuardDuty para enviar los hallazgos de vulnerabilidades a AWS Security Hub en una cuenta central de seguridad. Dar acceso al equipo de auditoría para revisar los hallazgos desde Security Hub.

127.- Una empresa utiliza instancias Linux de Amazon EC2 en la nube de AWS. Un miembro del equipo de seguridad de la empresa recibió recientemente un informe sobre identificadores de vulnerabilidades comunes (CVE) en las instancias.

Un ingeniero de seguridad necesita verificar si las instancias están parchadas correctamente y realizar remediación si no tienen los parches necesarios instalados. El ingeniero debe identificar qué instancias EC2 están en riesgo y debe implementar una solución para actualizarlas automáticamente con los parches correspondientes.

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

**A. Usar AWS Systems Manager Patch Manager para ver los identificadores de vulnerabilidades de los parches faltantes en las instancias. Usar también Patch Manager para automatizar el proceso de parchado.**

B. Usar AWS Shield Advanced para ver los identificadores de vulnerabilidades de los parches faltantes en las instancias. Usar AWS Systems Manager Patch Manager para automatizar el proceso de parchado.

C. Usar Amazon GuardDuty para ver los identificadores de vulnerabilidades de los parches faltantes en las instancias. Usar Amazon Inspector para automatizar el proceso de parchado.

D. Usar Amazon Inspector para ver los identificadores de vulnerabilidades de los parches faltantes en las instancias. Usar también Amazon Inspector para automatizar el proceso de parchado.

128.- Una empresa aloja una aplicación en Amazon EC2 que está sujeta a reglas específicas de cumplimiento normativo. Una de estas reglas indica que el tráfico hacia y desde la carga de trabajo debe ser inspeccionado en busca de ataques a nivel de red, lo que implica inspeccionar el paquete completo.

Para cumplir con esta norma, un ingeniero de seguridad debe instalar software de detección de intrusos en una instancia EC2 c5n.4xlarge. Luego, debe configurar el software para monitorear el tráfico de entrada y salida de las instancias de la aplicación.

¿Qué debe hacer el ingeniero de seguridad a continuación?

A. Poner la interfaz de red en modo promiscuo para capturar el tráfico.

B. Configurar VPC Flow Logs para enviar el tráfico a la instancia EC2 de monitoreo mediante un Network Load Balancer.

**C. Configurar VPC Traffic Mirroring para enviar el tráfico a la instancia EC2 de monitoreo mediante un Network Load Balancer.**

D. Usar Amazon Inspector para detectar ataques a nivel de red y activar una función de AWS Lambda que envíe los paquetes sospechosos a la instancia EC2.

129.- Una empresa implementa una aplicación web distribuida en un grupo de instancias de Amazon EC2. Este grupo está detrás de un Application Load Balancer (ALB), el cual se configurará para terminar la conexión TLS. Todo el tráfico TLS hacia el ALB debe mantenerse seguro, incluso si la clave privada del certificado se ve comprometida.

¿Cómo puede un ingeniero de seguridad cumplir con este requisito?

A. Crear un listener HTTPS que utilice un certificado gestionado por AWS Certificate Manager (ACM).

**B. Crear un listener HTTPS que utilice una política de seguridad que emplee un conjunto de cifrado con Perfect Forward Secrecy (PFS).**

C. Crear un listener HTTPS que utilice la función de seguridad Server Order Preference.

D. Crear un listener TCP que utilice una política de seguridad personalizada que permita solo conjuntos de cifrado con Perfect Forward Secrecy (PFS).

130.- Una empresa adoptó recientemente nuevos estándares de cumplimiento que requieren que todas las acciones de los usuarios en AWS queden registradas. Las acciones deben registrarse para todas las cuentas que pertenecen a una organización en AWS Organizations. La empresa necesita configurar alarmas que se activen cuando ocurran acciones específicas. Las alarmas deben enviar alertas a una lista de distribución de correo electrónico y deben hacerlo lo más cerca posible del tiempo real.

¿Qué solución cumplirá con estos requisitos?

**A. Implementar un trail de AWS CloudTrail como trail organizacional. Configurar el trail para reenviar los registros a Amazon CloudWatch Logs. En CloudWatch Logs, establecer un filtro de métricas para los eventos de acciones de usuario que especifique la empresa. Crear una alarma de Amazon CloudWatch que genere alertas ante eventos detectados en un período definido y que publique mensajes en un tema de Amazon SNS.**

B. Implementar un trail de AWS CloudTrail. Configurar el trail para reenviar los registros a Amazon CloudWatch Logs. En CloudWatch Logs, establecer un filtro de métricas para los eventos de acciones de usuario que especifique la empresa. Crear una alarma de Amazon CloudWatch que genere alertas ante eventos detectados en un período definido y que envíe mensajes a una cola de Amazon SQS.

C. Implementar un trail de AWS CloudTrail como trail organizacional. Configurar el trail para almacenar los registros en un bucket de Amazon S3. Configurar una instancia de Amazon EC2 para montar el bucket de S3 como un sistema de archivos e ingresar los archivos de registros nuevos que se carguen en el bucket. Configurar también la instancia EC2 para que publique un mensaje en un tema de Amazon SNS cuando se encuentre una de las acciones especificadas en los registros.

D. Implementar un trail de AWS CloudTrail. Configurar el trail para almacenar los registros en un bucket de Amazon S3. Cada hora, crear un Catálogo de Datos de AWS Glue que haga referencia al bucket de S3. Configurar Amazon Athena para que inicie consultas contra el catálogo y detecte las acciones especificadas en los registros.

131.- Una empresa quiere crear una solución de análisis de logs para los registros generados por sus dispositivos on-premise. Los logs se recopilan en un servidor local. La empresa desea usar servicios de AWS para realizar un análisis casi en tiempo real de los logs. Además, quiere almacenar estos registros durante 365 días para poder hacer análisis de patrones y búsquedas por fragmentos de texto más adelante.

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

A. Instalar Amazon Kinesis Agent en el servidor on-premise para enviar los logs a Amazon DynamoDB. Configurar un disparador de AWS Lambda en los streams de DynamoDB para realizar análisis de logs casi en tiempo real. Exportar los datos de DynamoDB a Amazon S3 periódicamente. Ejecutar consultas con Amazon Athena para análisis de patrones y búsqueda por fragmentos. Configurar políticas de ciclo de vida en S3 para eliminar los datos después de 365 días.

B. Instalar Amazon Managed Streaming for Apache Kafka (Amazon MSK) en el servidor on-premise. Crear un clúster MSK para recolectar los datos en streaming y analizarlos en tiempo real. Establecer el período de retención de datos en 365 días para almacenar los logs de forma persistente y habilitar análisis de patrones y búsqueda.

**C. Instalar Amazon Kinesis Agent en el servidor on-premise para enviar los logs a Amazon Kinesis Data Firehose. Configurar Amazon Managed Service for Apache Flink (antes llamado Amazon Kinesis Data Analytics) como destino para el procesamiento en tiempo real. Almacenar los logs en Amazon OpenSearch Service para análisis de patrones y búsqueda por fragmentos. Configurar una política Index State Management (ISM) en OpenSearch para eliminar los datos después de 365 días.**

D. Usar Amazon API Gateway y AWS Lambda para escribir los logs desde el servidor on-premise en Amazon DynamoDB. Configurar un disparador Lambda en los streams de DynamoDB para hacer análisis de logs casi en tiempo real. Ejecutar consultas federadas de Amazon Athena sobre los datos en DynamoDB para análisis de patrones y búsqueda por fragmentos. Configurar un TTL para eliminar los datos después de 365 días.

132.- Una empresa tiene una gran cantidad de instancias Amazon EC2 con Linux y Windows que se ejecutan en subredes privadas. La empresa desea que toda la administración remota se realice de la forma más segura posible dentro de la nube de AWS.

¿Qué solución cumplirá con estos requisitos?

**A. No usar claves privadas SSH-RSA al lanzar nuevas instancias. Implementar AWS Systems Manager Session Manager.**

B. Generar nuevas claves privadas SSH-RSA para las instancias existentes. Implementar AWS Systems Manager Session Manager.

C. No usar claves privadas SSH-RSA al lanzar nuevas instancias. Configurar EC2 Instance Connect.

D. Generar nuevas claves privadas SSH-RSA para las instancias existentes. Configurar EC2 Instance Connect.

133.- Una empresa ha decidido migrar su conjunto de instancias de servidores web basados en Linux a un grupo de Auto Scaling en Amazon EC2. Actualmente, las instancias son estáticas y se inician manualmente. Cuando un administrador necesita ver los archivos de registro (logs), se conecta a las instancias mediante SSH y recupera los logs manualmente.

La empresa necesita consultar los logs frecuentemente para obtener resultados sobre sesiones de aplicaciones y problemas de usuarios. No quiere que la nueva arquitectura, al escalar automáticamente, provoque la pérdida de archivos de registro cuando se reduzca el número de instancias.

¿Cuál combinación de pasos debería seguir un ingeniero de seguridad para cumplir estos requisitos de la manera más rentable? (Elige dos opciones).

A. Configurar un cron job en las instancias para enviar los archivos de logs a Amazon S3 periódicamente.

B. Configurar AWS Glue y Amazon Athena para consultar los archivos de logs.

**C. Configurar el agente de Amazon CloudWatch en las instancias para enviar los logs a CloudWatch Logs.**

**D. Configurar CloudWatch Logs Insights para consultar los archivos de logs.**

E. Configurar las instancias para que escriban los logs en un volumen de Amazon Elastic File System (Amazon EFS).

134.- Una empresa utiliza un proveedor de identidad externo para permitir la federación hacia distintas cuentas de AWS. Un ingeniero de seguridad de la empresa necesita identificar qué usuario federado eliminó una instancia de Amazon EC2 de producción hace una semana.

¿Cuál es la forma MÁS RÁPIDA de que el ingeniero de seguridad identifique al usuario federado?

A. Revisar los registros del historial de eventos de AWS CloudTrail en un bucket de Amazon S3 y buscar el evento TerminateInstances para identificar al usuario federado mediante el nombre de sesión del rol.

**B. Filtrar el historial de eventos de AWS CloudTrail por el evento TerminateInstances e identificar el rol de IAM asumido. Revisar el evento AssumeRoleWithSAML en CloudTrail para identificar el nombre de usuario correspondiente.**

C. Buscar el evento TerminateInstances en los registros de AWS CloudTrail y anotar la hora del evento. Revisar la pestaña Access Advisor de IAM para todos los roles federados. El tiempo de último acceso debe coincidir con la hora en que se eliminó la instancia.

D. Usar Amazon Athena para ejecutar una consulta SQL sobre los registros de AWS CloudTrail almacenados en un bucket de Amazon S3, filtrando por el evento TerminateInstances. Identificar el rol correspondiente y ejecutar otra consulta filtrando por el evento AssumeRoleWithWebIdentity para obtener el nombre de usuario.

135.- Dos instancias de Amazon EC2 ubicadas en subredes diferentes deberían poder conectarse entre sí, pero no pueden. Se ha confirmado que otros hosts en las mismas subredes pueden comunicarse correctamente, y que los grupos de seguridad tienen reglas ALLOW válidas que permiten este tráfico.

¿Cuál de los siguientes pasos de resolución de problemas se debería realizar?

A. Revisar los grupos de seguridad de entrada y salida, buscando reglas DENY

**B. Revisar las reglas de entrada y salida de las listas de control de acceso de red (Network ACL), buscando reglas DENY**

C. Revisar los códigos de motivo de paquetes rechazados en los registros de flujo de VPC (VPC Flow Logs)

D. Usar AWS X-Ray para rastrear el flujo de la aplicación de extremo a extremo

136.- Una empresa tiene una aplicación que necesita obtener objetos desde un bucket de Amazon S3. La aplicación se ejecuta en instancias de Amazon EC2.

Todos los objetos del bucket de S3 están cifrados con una clave administrada por el cliente en AWS Key Management Service (AWS KMS). Los recursos en la VPC no tienen acceso a internet y utilizan un gateway VPC endpoint para acceder a Amazon S3.

La empresa descubre que la aplicación no puede obtener los objetos del bucket de S3.

¿Qué factores podrían estar causando este problema? (Elige tres opciones).

**A. El perfil de instancia IAM adjunto a las instancias EC2 no permite la acción s3:ListBucket para el bucket de S3.**

B. El perfil de instancia IAM adjunto a las instancias EC2 no permite la acción s3:ListParts para el bucket de S3.

C. La política de la clave KMS que cifra los objetos en el bucket de S3 no permite la acción kms:ListKeys para el ARN del perfil de instancia EC2.

**D. La política de la clave KMS que cifra los objetos en el bucket de S3 no permite la acción kms:Decrypt para el ARN del perfil de instancia EC2.**

**E. La política del bucket de S3 no permite el acceso desde el gateway VPC endpoint.**

F. El grupo de seguridad adjunto a las instancias EC2 no tiene una regla de entrada desde la prefix list administrada por S3 sobre el puerto 443.

137.- Una empresa ejecuta sus cargas de trabajo en la región us-east-1. La empresa nunca ha desplegado recursos en otras regiones de AWS y no tiene recursos multi-región. Ahora necesita replicar sus cargas de trabajo e infraestructura en la región us-west-1.

Un ingeniero de seguridad debe implementar una solución que use AWS Secrets Manager para almacenar secretos en ambas regiones. La solución debe usar AWS Key Management Service (AWS KMS) para cifrar los secretos. Además, debe minimizar la latencia y seguir funcionando incluso si solo una región está disponible.

El ingeniero de seguridad utiliza Secrets Manager para crear los secretos en us-east-1.

¿Qué debe hacer el ingeniero de seguridad a continuación para cumplir con los requisitos?

A. Cifrar los secretos en us-east-1 usando una clave KMS administrada por AWS. Replicar los secretos a us-west-1. Cifrar los secretos en us-west-1 usando una nueva clave KMS administrada por AWS en us-west-1.

B. Cifrar los secretos en us-east-1 usando una clave KMS administrada por AWS. Configurar los recursos en us-west-1 para que llamen al endpoint de Secrets Manager en us-east-1.

C. Cifrar los secretos en us-east-1 usando una clave KMS administrada por el cliente. Configurar los recursos en us-west-1 para que llamen al endpoint de Secrets Manager en us-east-1.

**D. Cifrar los secretos en us-east-1 usando una clave KMS administrada por el cliente. Replicar los secretos a us-west-1. Cifrar los secretos en us-west-1 usando la misma clave KMS administrada por el cliente desde us-east-1.**

138.- Una empresa está utilizando una clave administrada por AWS (AWS owned key) del Servicio de Administración de Claves de AWS (AWS KMS) en su aplicación para cifrar archivos en una cuenta de AWS. El equipo de seguridad de la empresa quiere tener la capacidad de cambiar a un nuevo material de clave para los archivos nuevos siempre que ocurra una posible filtración de clave. Un ingeniero de seguridad debe implementar una solución que permita al equipo de seguridad cambiar la clave en cualquier momento.

¿Qué solución cumplirá con estos requisitos?

A. Crear una clave administrada por el cliente (customer managed key) nueva. Agregarle una programación de rotación de clave. Invocar la rotación de clave cada vez que el equipo de seguridad solicite un cambio.

B. Crear una clave administrada por AWS (AWS managed key) nueva. Agregarle una programación de rotación de clave. Invocar la rotación cada vez que el equipo de seguridad solicite un cambio.

**C. Crear un alias de clave. Crear una nueva clave administrada por el cliente cada vez que el equipo de seguridad solicite un cambio de clave. Asociar el alias con la nueva clave.**

D. Crear un alias de clave. Crear una nueva clave administrada por AWS cada vez que el equipo de seguridad solicite un cambio. Asociar el alias con la nueva clave.

139.- Un ingeniero de seguridad necesita configurar una distribución de Amazon CloudFront para un bucket de Amazon S3 que aloja un sitio web estático. El ingeniero debe permitir el acceso solo a direcciones IP específicas y también evitar que los usuarios accedan al sitio web directamente mediante las URLs de S3.

¿Qué solución cumple con estos requisitos?

A. Generar una política de bucket S3. Especificar cloudfront.amazonaws.com como principal. Usar la clave de condición aws:SourceIp para permitir el acceso solo si la solicitud proviene de las IP especificadas.

**B. Crear un Origin Access Control (OAC) para CloudFront. Crear la política del bucket S3 para que solo el OAC tenga acceso. Crear una ACL web de AWS WAF y agregar una regla con un conjunto de IPs. Asociar la ACL web a la distribución de CloudFront.**

C. Implementar grupos de seguridad para permitir solo las IP especificadas y restringir el acceso al bucket S3 usando la distribución de CloudFront.

D. Crear un punto de acceso de S3 que permita el acceso solo desde la distribución de CloudFront. Crear una ACL web de AWS WAF y agregar una regla con un conjunto de IPs. Asociar la ACL web a la distribución de CloudFront.

140.- Una empresa utiliza scripts de datos de usuario que contienen información sensible para inicializar instancias de Amazon EC2. Un ingeniero de seguridad descubre que esta información sensible puede ser vista por personas que no deberían tener acceso a ella.

¿Cuál es la forma más segura de proteger esta información sensible usada en el proceso de inicialización de las instancias?

A. Almacenar los scripts en la AMI y cifrar los datos sensibles usando AWS KMS. Usar el perfil de rol de la instancia para controlar el acceso a las claves KMS necesarias para descifrar los datos.

**B. Almacenar los datos sensibles en AWS Systems Manager Parameter Store, utilizando parámetros cifrados tipo string, y asignar el permiso GetParameters al rol de la instancia EC2.**

C. Externalizar los scripts de inicialización en Amazon S3 y cifrarlos usando AWS KMS. Eliminar los scripts de la instancia y limpiar los registros después de configurar la instancia.

D. Bloquear el acceso de los usuarios al servicio de metadatos de la instancia EC2 mediante políticas IAM. Eliminar todos los scripts y limpiar los registros después de que los scripts se hayan ejecutado.

141.- Una empresa tiene una VPC sin acceso a internet, pero con la opción de nombres de host DNS privados habilitada. Dentro de esta VPC se está ejecutando una base de datos Amazon Aurora. Un ingeniero de seguridad quiere usar AWS Secrets Manager para rotar automáticamente las credenciales de la base de datos Aurora.

El ingeniero configura la función Lambda de rotación predeterminada de Secrets Manager para que se ejecute dentro de la misma VPC que utiliza la base de datos Aurora. Sin embargo, descubre que la contraseña no se puede rotar correctamente porque la función Lambda no puede comunicarse con el endpoint de Secrets Manager.

¿Cuál es la forma MÁS segura de permitir que la función Lambda se comunique con el endpoint de Secrets Manager?

A. Agregar un NAT Gateway a la VPC para permitir el acceso al endpoint de Secrets Manager.

B. Agregar un VPC endpoint de tipo gateway a la VPC para permitir el acceso al endpoint de Secrets Manager.

**C. Agregar un VPC endpoint de tipo interfaz (interface endpoint) a la VPC para permitir el acceso al endpoint de Secrets Manager.**

D. Agregar un Internet Gateway a la VPC para permitir el acceso al endpoint de Secrets Manager.

142.- Una empresa tiene dos cuentas de AWS: la Cuenta A y la Cuenta B. Cada cuenta tiene su propia VPC. Una aplicación que se ejecuta en la VPC de la Cuenta A necesita escribir en un bucket de Amazon S3 que está en la Cuenta B.

La aplicación en la Cuenta A ya tiene permisos para escribir en el bucket S3 de la Cuenta B.

La aplicación y el bucket de S3 están en la misma región de AWS. La empresa no puede enviar tráfico de red por Internet público.

¿Qué solución cumplirá con estos requisitos?

A. En ambas cuentas, crear un Transit Gateway y establecer asociaciones de VPC (VPC attachments) en una subred por cada zona de disponibilidad. Actualizar las tablas de ruteo de las VPC.

B. Implementar un appliance VPN de software en la Cuenta A. Crear una conexión VPN entre este appliance y una puerta de enlace virtual privada (virtual private gateway) en la Cuenta B.

C. Crear una conexión de emparejamiento de VPC (VPC peering) entre la VPC de la Cuenta A y la VPC de la Cuenta B. Actualizar las tablas de ruteo, listas de control de acceso de red (ACLs) y grupos de seguridad para permitir el tráfico entre los rangos de IP emparejados.

**D. En la Cuenta A, crear un punto de enlace VPC (gateway endpoint) para Amazon S3. Actualizar la tabla de ruteo de la VPC en la Cuenta A.**

143.- Un ingeniero de seguridad recibe una alerta sobre actividad sospechosa proveniente de una instancia de Amazon EC2 basada en Linux, que utiliza almacenamiento Amazon EBS. La instancia está realizando conexiones a direcciones maliciosas conocidas.

La instancia se encuentra en una cuenta de desarrollo, dentro de una VPC ubicada en la región us-east-1. La VPC tiene un Internet Gateway y subredes en us-east-1a y us-east-1b. Cada subred está asociada a una tabla de rutas que utiliza el Internet Gateway como ruta predeterminada. Además, cada subred usa la ACL de red predeterminada. La instancia sospechosa está corriendo en la subred de us-east-1b, y durante la investigación inicial se descubre que es la única instancia en esa subred.

¿Cuál de las siguientes respuestas mitigará inmediatamente el ataque y ayudará a investigar la causa raíz?

A. Iniciar sesión en la instancia sospechosa y usar el comando netstat para identificar las conexiones remotas. Usar las direcciones IP detectadas para crear reglas de denegación en el grupo de seguridad de la instancia. Instalar herramientas de diagnóstico en la instancia para investigarla. Actualizar la ACL de red de salida de la subred en us-east-1b para denegar explícitamente todas las conexiones como primera regla durante la investigación.

**B. Actualizar la ACL de red de salida de la subred en us-east-1b para denegar explícitamente todas las conexiones como primera regla. Reemplazar el grupo de seguridad de la instancia por uno nuevo que solo permita conexiones desde un grupo de seguridad de diagnóstico. Luego, eliminar la regla de denegación de la ACL. Lanzar una nueva instancia EC2 con herramientas de diagnóstico. Asignar el nuevo grupo de seguridad a esta nueva instancia y usarla para investigar la instancia sospechosa.**

C. Asegurarse de que los volúmenes EBS conectados a la instancia sospechosa no se eliminen al terminar la instancia. Terminar la instancia. Lanzar una nueva instancia EC2 en us-east-1a con herramientas de diagnóstico. Montar los volúmenes EBS de la instancia terminada para su análisis.

D. Crear una regla de AWS WAF que deniegue el tráfico hacia y desde la instancia sospechosa. Asignar esta regla WAF a la instancia para mitigar el ataque. Iniciar sesión en la instancia e instalar herramientas de diagnóstico para investigarla.

144.- Una empresa de medios en línea tiene una aplicación que los clientes usan para ver eventos en todo el mundo. La aplicación está alojada en un conjunto de instancias de Amazon EC2 que ejecutan Amazon Linux 2. La empresa utiliza AWS Systems Manager para administrar las instancias EC2. Aplica parches y actualizaciones de la aplicación usando la línea base de parches AWS-AmazonLinux2DefaultPatchBaseline en Systems Manager Patch Manager.

La empresa está preocupada por posibles ataques a la aplicación durante la semana de un evento importante. Necesitan una solución que permita desplegar parches inmediatamente a todas las instancias EC2 en respuesta a un incidente de seguridad o una vulnerabilidad. Además, la solución debe ofrecer evidencia centralizada de que los parches fueron aplicados correctamente.

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

**A. Crear una nueva línea base de parches en Patch Manager. Especificar Amazon Linux 2 como el producto. Especificar “Security” como la clasificación. Configurar la aprobación automática de parches en 0 días. Asegurarse de que esta nueva línea base sea la predeterminada para Amazon Linux 2.**

**B. Usar la opción "Patch Now" con la operación de escaneo e instalación en la consola de Patch Manager para aplicar los parches de la línea base a todos los nodos. Especificar un bucket de Amazon S3 como destino para guardar los registros del parcheo.**

C. Usar la función Clone de Patch Manager para crear una copia de la línea base incorporada AWS-AmazonLinux2DefaultPatchBaseline. Configurar la aprobación automática de parches en 1 día.

D. Crear una política de parches que actualice todos los nodos administrados y envíe los registros de operación de parches a un bucket de Amazon S3. Usar una programación personalizada de escaneo para que Patch Manager verifique cada hora si hay nuevos parches. Asignar la línea base a la política de parches.

E. Usar Systems Manager Application Manager para inspeccionar las versiones de los paquetes instalados en las instancias EC2. Además, usar Application Manager para validar que los parches fueron instalados correctamente.

145.- Un equipo de operaciones de desarrollo utiliza AWS Identity and Access Management (IAM) para gestionar los permisos de los usuarios. El equipo creó un rol de perfil de instancia de Amazon EC2 que utiliza la política administrada por AWS llamada ReadOnlyAccess. Cuando una aplicación que se ejecuta en una instancia EC2 intenta leer un archivo desde un bucket de Amazon S3 cifrado, la aplicación recibe un error AccessDenied.

El administrador del equipo ha verificado que la política del bucket S3 permite el acceso a todos los usuarios de la cuenta. No hay una ACL de objeto adjunta al archivo.

¿Qué debe hacer el administrador para solucionar el problema de acceso en IAM?

A. Editar la política ReadOnlyAccess para agregar permisos de kms:Decrypt

B. Agregar el rol IAM de EC2 como Principal autorizado en la política del bucket S3

**C. Adjuntar una política inline con permisos de kms:Decrypt al rol IAM**

D. Adjuntar una política inline con permisos S3:\* al rol IAM

146.- Una empresa utiliza AWS Organizations y tiene clústeres de Amazon Elastic Kubernetes Service (Amazon EKS) en muchas cuentas de AWS. Un ingeniero de seguridad integró Amazon EKS con AWS CloudTrail. Los trails de CloudTrail se almacenan en un bucket de Amazon S3 en cada cuenta para monitorear llamadas a la API. Sin embargo, el ingeniero de seguridad nota que los registros de CloudTrail no muestran eventos de creación de pods de Kubernetes.

¿Qué debe hacer el ingeniero de seguridad para ver los eventos de Kubernetes desde Amazon CloudWatch?

A. Configurar los clústeres de EKS para usar endpoints VPC privados de S3. Configurar los buckets de S3 para el registro de logs.

**B. Habilitar los registros del componente del servidor API de Kubernetes para cada clúster.**

C. Habilitar CORS (uso compartido de recursos entre orígenes) en el bucket de S3 que se utiliza para los registros.

D. Configurar CloudWatch. Ver los eventos en la consola de CloudWatch.

147.- Un ingeniero de seguridad necesita construir una solución para volver a activar AWS CloudTrail en múltiples regiones de AWS en caso de que alguna vez sea desactivado.

¿Cuál es la forma más eficiente de implementar esta solución?

**A. Usar AWS Config con una regla administrada para iniciar la remediación AWS-EnableCloudTrail.**

B. Crear un evento en Amazon EventBridge con una fuente de eventos cloudtrail.amazonaws.com y el nombre de evento StartLogging, para invocar una función de AWS Lambda que llame a la API StartLogging.

C. Crear una alarma en Amazon CloudWatch con una fuente de eventos cloudtrail.amazonaws.com y el nombre de evento StopLogging, para invocar una función de AWS Lambda que llame a la API StartLogging.

D. Monitorear AWS Trusted Advisor para asegurar que el registro de CloudTrail esté habilitado.

148.- Una empresa de comercio electrónico está desarrollando una nueva arquitectura para una versión de su aplicación. La empresa necesita implementar TLS para el tráfico entrante hacia la aplicación. El tráfico proviene de internet. No es necesario implementar TLS de extremo a extremo, ya que la empresa está preocupada por el impacto en el rendimiento.

Los tipos de tráfico entrante serán HTTP y HTTPS, y la aplicación utiliza los puertos 80 y 443.

¿Qué debe hacer un ingeniero de seguridad para cumplir con estos requisitos?

**A. Crear un Application Load Balancer (ALB) público. Crear dos listeners: uno en el puerto 80 y otro en el puerto 443. Crear un grupo de destino (target group). Crear una regla para redirigir el tráfico del puerto 80 al listener en el puerto 443. Provisionar un certificado TLS público en AWS Certificate Manager (ACM). Adjuntar el certificado al listener en el puerto 443.**

B. Crear un Application Load Balancer (ALB) público. Crear dos listeners: uno en el puerto 80 y otro en el puerto 443. Crear un grupo de destino. Crear una regla para redirigir el tráfico del puerto 80 al listener en el puerto 443. Provisionar un certificado TLS público en AWS Certificate Manager (ACM). Adjuntar el certificado al listener en el puerto 80.

C. Crear un Network Load Balancer (NLB) público. Crear dos listeners: uno en el puerto 80 y otro en el puerto 443. Crear un grupo de destino. Crear una regla para redirigir el tráfico del puerto 80 al listener en el puerto 443. Configurar el protocolo del listener en el puerto 443 como TLS.

D. Crear un Network Load Balancer (NLB) público. Crear un listener en el puerto 443. Crear un grupo de destino. Crear una regla para redirigir el tráfico del puerto 443 al grupo de destino. Configurar el protocolo del listener en el puerto 443 como TLS.

149.- Una empresa necesita una solución para proteger datos críticos y evitar que se eliminen de forma permanente. Los datos están almacenados en buckets de Amazon S3.

La empresa debe replicar los objetos de S3 desde la Región principal de AWS hacia una Región secundaria, para cumplir con los requisitos de recuperación ante desastres. Además, debe garantizar que los usuarios con acceso de administrador no puedan eliminar permanentemente los datos en la Región secundaria.

¿Qué solución cumple con estos requisitos?

A. Configurar AWS Backup para realizar copias de seguridad de S3 entre regiones. Seleccionar una bóveda de respaldo (backup vault) en la Región secundaria. Habilitar AWS Backup Vault Lock en modo de gobernanza para los respaldos en la Región secundaria.

**B. Implementar S3 Object Lock en modo de cumplimiento en la Región principal. Configurar la replicación de S3 para replicar los objetos a un bucket de S3 en la Región secundaria.**

C. Configurar la replicación de S3 para replicar los objetos a un bucket de S3 en la Región secundaria. Crear una política de bucket S3 que deniegue la acción s3:ReplicateDelete en el bucket de la Región secundaria.

D. Configurar la replicación de S3 para replicar los objetos a un bucket de S3 en la Región secundaria. Configurar el versionado de objetos S3 en el bucket de la Región secundaria.

150.- Una empresa en Francia utiliza Amazon Cognito con la interfaz hospedada de Cognito (Hosted UI) como intermediario de identidad para los procesos de inicio de sesión y registro. La empresa está promocionando una aplicación y espera que todos los usuarios provengan de Francia.

Cuando la empresa lanza la aplicación, el equipo de seguridad observa registros fraudulentos. La mayoría de estos registros provienen de usuarios fuera de Francia.

El equipo de seguridad necesita una solución que permita realizar validaciones personalizadas durante el registro. Según los resultados de esa validación, la solución debe aceptar o rechazar la solicitud de registro.

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

**A. Crear un disparador de tipo pre sign-up con AWS Lambda. Asociar esta función Lambda con el grupo de usuarios de Amazon Cognito.**

**B. Usar una regla de coincidencia geográfica para configurar una ACL web de AWS WAF. Asociar esta ACL con el grupo de usuarios de Amazon Cognito.**

C. Configurar un cliente de aplicación (app client) para el grupo de usuarios de Amazon Cognito de la aplicación. Usar el ID del cliente para validar las solicitudes en la interfaz hospedada (Hosted UI).

D. Actualizar el grupo de usuarios de Amazon Cognito de la aplicación para configurar una restricción geográfica.

E. Usar Amazon Cognito para configurar un proveedor de identidad social (IdP) para validar las solicitudes en la interfaz hospedada.

151.- Un ingeniero de seguridad está configurando AWS Config para una cuenta de AWS que utiliza una nueva entidad de IAM. Cuando intenta configurar reglas de AWS Config y opciones de remediación automática, se generan errores. En los registros de AWS CloudTrail, el ingeniero ve el siguiente mensaje de error: “Política de entrega insuficiente al bucket S3: DOC-EXAMPLE-BUCKET, no se puede escribir en el bucket, el prefijo de clave S3 proporcionado es 'null').

¿Qué combinación de pasos debe seguir el ingeniero de seguridad para resolver este problema? (Elige dos opciones).

**A. Revisar la política del bucket de Amazon S3. Verificar que la política permita al servicio config.amazonaws.com escribir en el bucket de destino.**

**B. Verificar que la entidad de IAM tenga permisos necesarios para ejecutar las operaciones s3:GetBucketAcl y s3:PutObject\* para escribir en el bucket de destino.**

C. Verificar que la política del bucket de Amazon S3 tenga los permisos necesarios para permitir las operaciones s3:GetBucketAcl y s3:PutObject\* para escribir en el bucket de destino.

D. Revisar la política asociada a la entidad de IAM. Verificar que la política permita al servicio config.amazonaws.com escribir en el bucket de destino.

E. Verificar que el rol de servicio de AWS Config tenga permisos para invocar la acción BatchGetResourceConfig en lugar de GetResourceConfigHistory y s3:PutObject\*.

152.- Una empresa está sufriendo un ataque DDoS de capa 3 y capa 4 en sus servidores web que se ejecutan en AWS.

¿Qué combinación de servicios y funcionalidades de AWS proporcionará protección en este escenario? (Elige tres opciones).

**A. Amazon Route 53**

B. AWS Certificate Manager (ACM)

C. Amazon S3

**D. AWS Shield**

**E. Network Load Balancer**

F. Amazon GuardDuty

153.- Una empresa quiere implementar seguridad a nivel de host para instancias de Amazon EC2 y contenedores almacenados en Amazon Elastic Container Registry (Amazon ECR). Ya han desplegado el agente de AWS Systems Manager (SSM Agent) en las instancias EC2. Todas las cuentas de la empresa están organizadas dentro de una organización en AWS Organizations.

La empresa necesita analizar las cargas de trabajo para detectar vulnerabilidades de software y exposiciones no intencionadas a la red. Los hallazgos deben enviarse a AWS Security Hub, que ya está configurado a nivel organizacional.

Además, la solución debe desplegarse automáticamente en todas las cuentas miembro, incluidas las nuevas cuentas. Cuando se activen nuevas cargas de trabajo, estas deben ser escaneadas automáticamente.

¿Cuál solución cumple con estos requisitos?

A. Usar SCPs (Service Control Policies) para configurar el escaneo de instancias EC2 y contenedores en ECR para todas las cuentas de la organización.

B. Configurar un administrador delegado para Amazon GuardDuty en la organización. Crear una regla de Amazon EventBridge para iniciar el análisis de contenedores en ECR.

**C. Configurar un administrador delegado para Amazon Inspector en la organización. Configurar el escaneo automático para nuevas cuentas miembro.**

D. Configurar un administrador delegado para Amazon Inspector en la organización. Crear una regla de AWS Config para iniciar el análisis de contenedores en ECR.

154.- Una empresa utiliza AWS Organizations para gestionar varias cuentas de AWS. La empresa procesa un gran volumen de datos sensibles y sigue un enfoque serverless para sus microservicios. Almacena todos los datos en Amazon S3 o Amazon DynamoDB, y accede a ellos mediante funciones de AWS Lambda o servicios basados en contenedores que ejecuta en Amazon Elastic Kubernetes Service (Amazon EKS) sobre AWS Fargate.

La empresa debe implementar una solución que cifre todos los datos en reposo y que haga cumplir controles de acceso con privilegios mínimos. Para ello, la empresa crea una clave administrada por el cliente (CMK) en AWS Key Management Service (AWS KMS).

¿Qué debe hacer la empresa a continuación para cumplir con estos requisitos?

A. Crear una política de clave que permita la acción kms:Decrypt solo para Amazon S3 y DynamoDB. Crear una SCP que deniegue la creación de buckets S3 y tablas DynamoDB que no estén cifrados con esa clave.

B. Crear una política de IAM que deniegue la acción kms:Decrypt para la clave. Crear una función Lambda que se ejecute de forma programada para adjuntar esta política a cualquier nuevo rol. Crear una regla de AWS Config que envíe alertas para recursos que no estén cifrados con la clave.

**C. Crear una política de clave que permita la acción kms:Decrypt solo para Amazon S3, DynamoDB, Lambda y Amazon EKS. Crear una SCP que deniegue la creación de buckets S3 y tablas DynamoDB que no estén cifrados con la clave.**

D. Crear una política de clave que permita la acción kms:Decrypt solo para Amazon S3, DynamoDB, Lambda y Amazon EKS. Crear una regla de AWS Config que envíe alertas para recursos que no estén cifrados con la clave.

155.- Una función de AWS Lambda fue mal utilizada para alterar datos, y un ingeniero de seguridad debe identificar quién invocó la función y qué salida produjo. El ingeniero no puede encontrar registros creados por la función Lambda en Amazon CloudWatch Logs.

¿Cuál de las siguientes opciones explica por qué los registros no están disponibles?

**A. El rol de ejecución de la función Lambda no tenía permisos para escribir datos de registro en CloudWatch Logs.**

B. La función Lambda fue invocada mediante Amazon API Gateway, por lo tanto, los registros no se almacenan en CloudWatch Logs.

C. El rol de ejecución de la función Lambda no tenía permisos para escribir en el bucket de Amazon S3 donde CloudWatch Logs almacena los registros.

D. La versión de la función Lambda que se invocó no era la actual.

156.- Una empresa está preocupada por posibles ataques DDoS. Tiene una aplicación web que se ejecuta en instancias de Amazon EC2. La aplicación usa Amazon S3 para servir contenido estático como imágenes y videos.

Un ingeniero de seguridad debe crear una arquitectura resistente que pueda soportar ataques DDoS.

¿Qué solución cumplirá con estos requisitos de la forma MÁS rentable?

A. Crear una alarma de Amazon CloudWatch que invoque una función de AWS Lambda cuando la utilización de CPU de una instancia EC2 alcance el 90%. Programar la función Lambda para actualizar los grupos de seguridad adjuntos a la instancia EC2 y denegar el tráfico entrante por los puertos 80 y 443.

**B. Colocar las instancias EC2 en un grupo de Auto Scaling detrás de un balanceador de carga de Elastic Load Balancing (ELB). Usar Amazon CloudFront con Amazon S3 como origen.**

C. Configurar un entorno de recuperación ante desastres (disaster recovery, DR) en espera activa (warm standby). Cambiar a este entorno si se detecta un ataque DDoS en la aplicación.

D. Suscribirse a AWS Shield Advanced. Configurar permisos para permitir que el Shield Response Team gestione los recursos en nombre de la empresa durante un evento DDoS.

157.- Una empresa utiliza una organización en AWS Organizations para administrar cientos de cuentas de AWS. Algunas de estas cuentas otorgan acceso a principales externos de AWS mediante roles de IAM entre cuentas (cross-account) y políticas de buckets de Amazon S3. La empresa necesita identificar qué principales externos tienen acceso a qué cuentas.

¿Qué solución proporcionará esta información?

**A. Habilitar AWS Identity and Access Management Access Analyzer para la organización. Configurar la organización como una zona de confianza. Filtrar los hallazgos por ID de cuenta de AWS.**

B. Crear una regla personalizada de AWS Config para monitorear los roles de IAM en cada cuenta. Implementar un agregador de AWS Config en una cuenta central. Filtrar los hallazgos por ID de cuenta de AWS.

C. Activar Amazon Inspector. Integrarlo con AWS Security Hub. Filtrar los hallazgos por ID de cuenta de AWS para los tipos de recursos "rol de IAM" y "política de bucket de S3".

D. Configurar la organización para usar Amazon GuardDuty. Filtrar los hallazgos por ID de cuenta de AWS para el tipo de hallazgo Discovery:IAMUser/AnomalousBehavior.

158.- Una empresa tiene varias cuentas de AWS organizadas mediante AWS Organizations. La empresa necesita instalar un paquete de software corporativo en todas las instancias de Amazon EC2 de todas las cuentas de la organización.

Una cuenta central proporciona las AMIs base para las instancias EC2. La empresa usa AWS Systems Manager para el inventario de software y las operaciones de parchado.

Un ingeniero de seguridad debe implementar una solución que detecte automáticamente las instancias EC2 que no tengan el software requerido, y que también instale el software automáticamente si no está presente.

¿Qué solución cumplirá con estos requisitos?

A. Proporcionar nuevas AMIs con el software requerido ya preinstalado. Aplicar una etiqueta (tag) a las AMIs para indicar que contienen el software. Configurar una SCP que permita lanzar nuevas instancias EC2 solo si usan AMIs con dicha etiqueta. Etiquetar todas las instancias EC2 existentes.

B. Configurar una línea base de parches personalizada en Systems Manager Patch Manager. Agregar el nombre del paquete del software requerido a la lista de paquetes aprobados. Asociar esta línea base de parches a todas las instancias EC2. Configurar una ventana de mantenimiento para la instalación del software.

**C. Habilitar AWS Config de forma centralizada. Configurar la regla administrada ec2-managedinstance-applications-required de AWS Config en todas las cuentas. Crear una regla de Amazon EventBridge que reaccione a los eventos de AWS Config. Configurar esta regla para invocar una función Lambda que use Systems Manager Run Command para instalar el software requerido.**

D. Crear un nuevo paquete en Systems Manager Distributor con el software requerido, especificando la ubicación de descarga. Seleccionar todas las instancias EC2 de las distintas cuentas. Instalar el software usando Systems Manager Run Command.

159.- Un equipo de desarrollo está creando un conjunto de herramientas de código abierto para gestionar una aplicación de tipo SaaS (software como servicio) de la empresa. El código se almacena en un repositorio público, de modo que cualquiera puede ver y descargar el código de las herramientas.

La empresa descubre que el código contiene una clave de acceso IAM y una clave secreta que otorgan acceso a recursos internos dentro del entorno de AWS de la compañía.

Un ingeniero de seguridad debe implementar una solución que permita identificar si se ha producido uso no autorizado de las credenciales expuestas. Además, la solución debe evitar cualquier uso adicional de dichas credenciales.

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

**A. Usar Access Analyzer de AWS Identity and Access Management para determinar qué recursos se accedieron con las credenciales expuestas y quién las usó.**

**B. Desactivar la clave de acceso IAM expuesta de la cuenta del usuario en IAM.**

C. Crear una regla en Amazon GuardDuty para bloquear el uso de la clave de acceso presente en el código fuente.

D. Crear una nueva clave de acceso y clave secreta IAM para el usuario cuyas credenciales se expusieron.

E. Generar un informe de credenciales IAM. Revisar el informe para determinar cuándo fue la última vez que inició sesión el usuario dueño de la clave.

160.- Una empresa necesita crear una solución centralizada para analizar archivos de registros (logs). La empresa utiliza una organización en AWS Organizations para administrar sus cuentas de AWS.

La solución debe agregar y normalizar eventos desde las siguientes fuentes:

Toda la organización en AWS Organizations

Todas las ofertas de AWS Marketplace que se ejecutan en las cuentas de AWS de la empresa

Los sistemas on-premises (locales) de la empresa

¿Qué solución cumplirá con estos requisitos?

A. Configurar un bucket centralizado de Amazon S3 para los logs. Habilitar VPC Flow Logs, AWS CloudTrail y logs de Amazon Route 53 en todas las cuentas. Configurar todas las cuentas para que usen el bucket centralizado. Configurar AWS Glue crawlers para analizar los archivos de logs. Usar Amazon Athena para consultar los datos de los logs.

B. Configurar flujos de logs (log streams) en Amazon CloudWatch Logs para las fuentes que necesitan monitoreo. Crear filtros de suscripción de logs para cada flujo. Reenviar los mensajes a Amazon OpenSearch Service para análisis.

**C. Configurar una cuenta administradora delegada para Amazon Security Lake dentro de la organización en AWS Organizations. Habilitar y configurar Security Lake para toda la organización. Agregar las cuentas que deben ser monitoreadas. Usar Amazon Athena para consultar los datos de logs.**

D. Aplicar una SCP (Service Control Policy) para configurar que todas las cuentas miembro y servicios entreguen los archivos de logs a un bucket centralizado de Amazon S3. Usar Amazon OpenSearch Service para consultar ese bucket en busca de entradas de logs.

161.- Una empresa utiliza AWS Organizations. Tiene más de 100 cuentas de AWS y planea aumentar ese número. Además, la empresa usa un proveedor de identidad corporativo externo (IdP).

La empresa necesita proporcionar a los usuarios acceso basado en roles a las cuentas. La solución debe maximizar la escalabilidad y la eficiencia operativa.

¿Qué solución cumplirá con estos requisitos?

A. En cada cuenta, crear un conjunto de usuarios IAM dedicados. Asegurarse de que todos los usuarios asuman estos usuarios IAM mediante federación con el IdP existente.

B. Implementar un rol IAM en una cuenta de identidad central. Permitir que los usuarios asuman ese rol mediante federación con el IdP existente. En cada cuenta, implementar un conjunto de roles IAM que coincidan con los patrones de acceso deseados. Incluir una política de confianza que permita el acceso desde la cuenta de identidad central. Editar la política de permisos del rol en cada cuenta según los requerimientos de acceso de los usuarios.

**C. Habilitar AWS IAM Identity Center (anteriormente AWS SSO). Integrarlo con el IdP corporativo existente. Crear conjuntos de permisos que se ajusten a los patrones de acceso deseados. Asignar permisos de acuerdo con los requerimientos de acceso de los usuarios.**

D. En cada cuenta, implementar un conjunto de roles IAM que coincidan con los patrones de acceso deseados. Crear una política de confianza con el IdP existente. Actualizar la política de permisos de cada rol para que use condiciones IAM basadas en SAML, según los requerimientos de acceso del usuario.

162.- Una empresa tiene una aplicación web que se ejecuta detrás de un Application Load Balancer (ALB). La aplicación está sufriendo un ataque de relleno de credenciales (credential stuffing) que está generando muchos intentos fallidos de inicio de sesión. El ataque proviene de muchas direcciones IP y los intentos de inicio de sesión utilizan una cadena de user agent de un emulador de dispositivo móvil conocido.

Un ingeniero de seguridad necesita implementar una solución para mitigar el ataque, pero que siga permitiendo los inicios de sesión legítimos en la aplicación.

¿Qué solución cumplirá con estos requisitos?

A. Crear una alarma de Amazon CloudWatch que reaccione a intentos de inicio de sesión que contengan la cadena de user agent especificada. Agregar un tema de Amazon SNS a la alarma.

B. Modificar el grupo de seguridad de entrada del ALB para denegar el tráfico desde las direcciones IP involucradas en el ataque.

**C. Crear una ACL web de AWS WAF para el ALB. Crear una regla personalizada que bloquee las solicitudes que contengan la cadena de user agent del emulador.**

D. Crear una ACL web de AWS WAF para el ALB. Crear una regla personalizada que permita solo las solicitudes con cadenas de user agent legítimas.

163.- Una empresa está evaluando controles para proteger datos sensibles. Utiliza temas de Amazon SNS (Simple Notification Service) para publicar mensajes desde los componentes de sus aplicaciones hacia servicios de registro personalizados.

La empresa está preocupada porque algún componente de la aplicación podría publicar datos sensibles que se expongan accidentalmente en registros de transacciones o registros de depuración (debug).

¿Qué solución protegerá los datos sensibles en estos mensajes y evitará que se expongan accidentalmente?

A. Usar Amazon Macie para escanear los temas de SNS en busca de elementos de datos sensibles en los mensajes. Crear una función de AWS Lambda que enmascare los datos sensibles dentro de los mensajes cuando Macie genere un hallazgo.

**B. Configurar una política de protección de datos para mensajes entrantes. En la política, incluir la operación De-identify para enmascarar los datos sensibles dentro de los mensajes. Aplicar la política a los temas de SNS.**

C. Configurar los temas de SNS con una clave administrada por el cliente en AWS KMS para cifrar los elementos de datos dentro de los mensajes. Otorgar permisos a todos los roles IAM que publican mensajes para que puedan acceder a la clave y cifrar los datos.

D. Crear un hallazgo de Amazon GuardDuty para datos sensibles transmitidos a los temas de SNS. Crear una acción de remediación personalizada en AWS Security Hub para bloquear los mensajes que contengan datos sensibles antes de que se entreguen a los suscriptores de los temas de SNS.

164.- Una empresa ha creado un conjunto de funciones de AWS Lambda para automatizar los pasos de respuesta ante incidentes que ocurren en instancias de Amazon EC2. Las funciones Lambda deben recopilar artefactos relevantes, como el ID de la instancia y la configuración del grupo de seguridad. Luego, las funciones Lambda deben escribir un resumen en un bucket de Amazon S3.

La empresa ejecuta sus cargas de trabajo en una VPC que utiliza subredes públicas y privadas. Las subredes públicas usan un internet gateway para acceder a internet. Las subredes privadas usan un NAT gateway para acceder a internet.

Todo el tráfico de red hacia Amazon S3 relacionado con el proceso de respuesta a incidentes debe utilizar la red de AWS. Este tráfico no debe viajar por internet.

¿Qué solución cumplirá con estos requisitos?

A. Implementar las funciones Lambda en una subred privada de la VPC. Configurar las funciones Lambda para acceder al servicio S3 a través del NAT gateway.

**B. Implementar las funciones Lambda en una subred privada de la VPC. Crear un endpoint de tipo gateway para acceder al servicio S3.**

C. Implementar el bucket de S3 y las funciones Lambda en la misma subred privada. Configurar las funciones Lambda para usar el endpoint predeterminado del servicio S3.

D. Implementar una cola de Amazon SQS y las funciones Lambda en la misma subred privada. Configurar las funciones Lambda para enviar los datos a la cola SQS. Configurar la cola SQS para enviar los datos al bucket S3.

165.- Una empresa utiliza una organización en AWS Organizations para gestionar sus cuentas de AWS. La empresa ha implementado una Política de Control de Servicios (SCP) en la cuenta raíz para evitar que se compartan recursos con cuentas externas.

Ahora, la empresa necesita permitir que las aplicaciones en la cuenta de AWS del equipo de marketing compartan recursos con cuentas externas. Al mismo tiempo, debe seguir evitando que todas las demás cuentas de la organización compartan recursos con cuentas externas. Todas las cuentas de la organización son miembros de la misma Unidad Organizativa (OU).

¿Qué solución cumplirá con estos requisitos?

A. Crear una nueva SCP en la cuenta del equipo de marketing. Configurar la SCP para permitir explícitamente el uso compartido de recursos.

**B. Editar la SCP existente para agregar una declaración Condition que excluya la cuenta del equipo de marketing.**

C. Editar la SCP existente para incluir una instrucción Allow que especifique la cuenta del equipo de marketing.

D. Crear una política de límites de permisos (permissions boundary) de IAM para permitir explícitamente el uso compartido de recursos. Adjuntar la política a los usuarios de IAM en la cuenta del equipo de marketing.

166.- Un administrador de seguridad ha habilitado AWS Security Hub para todas las cuentas de AWS dentro de una organización en AWS Organizations. El equipo de seguridad desea una respuesta y remediación casi en tiempo real para los recursos de AWS implementados que no cumplan con los estándares de seguridad. Todos los cambios deben ser registrados de forma centralizada para fines de auditoría.

La organización ya alcanzó los límites de cuota tanto para la cantidad de políticas SCP adjuntas a una unidad organizativa (OU) como para el tamaño del documento SCP. El equipo quiere evitar hacer cambios en cualquier SCP. La solución debe maximizar la escalabilidad y la rentabilidad.

¿Qué combinación de acciones debe tomar el administrador de seguridad para cumplir con estos requisitos? (Elige tres opciones).

**A. Crear una regla personalizada de AWS Config para detectar cambios de configuración en recursos de AWS. Crear una función de AWS Lambda para remediar los recursos de AWS en la cuenta delegada de administración.**

B. Usar AWS Systems Manager Change Manager para rastrear cambios de configuración en los recursos de AWS. Crear un documento de Systems Manager para remediar los recursos en la cuenta delegada de administración.

**C. Crear una acción personalizada de Security Hub para hacer referencia en una regla de eventos de Amazon EventBridge en la cuenta delegada de administración.**

**D. Crear una regla de eventos de Amazon EventBridge para invocar una función de AWS Lambda que tome acción sobre los recursos de AWS.**

E. Crear una regla de eventos de Amazon EventBridge para invocar una función de AWS Lambda que evalúe la configuración de recursos de AWS para un conjunto de llamadas a la API y genere un hallazgo para recursos no conformes.

F. Crear una regla programada en Amazon EventBridge para invocar una función de AWS Lambda que evalúe reglas específicas de AWS Config.

167.- Un ingeniero de seguridad debe implementar monitoreo sobre las instancias de base de datos Amazon Aurora MySQL de una empresa. La empresa desea recibir notificaciones por correo electrónico cuando usuarios desconocidos intenten iniciar sesión en el endpoint de la base de datos.

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

**A. Activar Amazon GuardDuty. Habilitar la función Amazon RDS Protection en GuardDuty para detectar intentos de inicio de sesión por parte de usuarios desconocidos. Crear una regla de Amazon EventBridge para filtrar los hallazgos de GuardDuty. Enviar notificaciones por correo electrónico usando Amazon SNS (Simple Notification Service).**

B. Activar el parámetro server\_audit\_logging en las instancias Aurora MySQL. Usar una función AWS Lambda para escanear periódicamente los archivos de registro en busca de intentos de inicio de sesión por parte de usuarios desconocidos. Enviar notificaciones por correo electrónico mediante Amazon SNS.

C. Crear una AMI personalizada de Amazon RDS. Incluir un agente de seguridad de terceros en la AMI para detectar intentos de inicio de sesión por parte de usuarios desconocidos. Implementar instancias RDS Custom. Migrar los datos desde la instalación actual a las nuevas instancias. Configurar las notificaciones por correo electrónico desde el agente de terceros.

D. Escribir un procedimiento almacenado que detecte intentos de inicio de sesión de usuarios desconocidos. Programar un trabajo recurrente dentro del motor de base de datos. Configurar Aurora MySQL para usar Amazon SNS y enviar las notificaciones por correo electrónico.

168.- Una empresa opera un sitio web global de comercio electrónico que está alojado en AWS. La empresa utiliza Amazon CloudFront para distribuir contenido a sus usuarios. Ahora, la empresa quiere bloquear el tráfico entrante de un conjunto específico de países para cumplir con nuevas regulaciones de datos.

¿Qué solución cumplirá con estos requisitos de la forma más rentable?

A. Crear una ACL web de AWS WAF con una condición de coincidencia de IP (IP match) para denegar los rangos de IP de esos países. Asociar la ACL web con la distribución de CloudFront.

B. Crear una ACL web de AWS WAF con una condición de coincidencia geográfica (geo match) para denegar los países específicos. Asociar la ACL web con la distribución de CloudFront.

**C. Usar la función de restricción geográfica de CloudFront para denegar los países específicos.**

D. Usar los encabezados de geolocalización de CloudFront para denegar los países específicos.

169.- Una empresa implementa su aplicación como un servicio en un clúster de Amazon Elastic Container Service (Amazon ECS) utilizando el tipo de lanzamiento AWS Fargate. Un ingeniero de seguridad sospecha que algunas solicitudes entrantes son maliciosas. El ingeniero necesita inspeccionar el contenedor en ejecución recuperando archivos de logs y volcados de memoria (memory dumps).

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

A. Migrar la aplicación a un clúster de ECS con tipo de lanzamiento Amazon EC2. Configurar las instancias EC2 con acceso remoto adecuado. Iniciar sesión e inspeccionar el contenedor.

B. Actualizar la aplicación para que envíe los datos requeridos a STDOUT. Usar el controlador de logs awslogs para enviar los registros a Amazon CloudWatch Logs. Examinar los archivos de logs en CloudWatch Logs.

C. Activar Amazon CloudWatch Container Insights para el clúster de ECS. Enviar los datos de logs a Amazon CloudWatch Logs usando AWS Distro for OpenTelemetry. Examinar los datos de logs en CloudWatch Logs.

**D. Actualizar el rol de tarea ECS con permisos de AWS Systems Manager. Habilitar la funcionalidad ECS Exec para el servicio ECS. Usar ECS Exec para inspeccionar el contenedor.**

170.- Una empresa utiliza AWS Organizations y tiene muchas cuentas de AWS. Ahora tiene un nuevo requisito: usar cifrado del lado del servidor con claves proporcionadas por el cliente (SSE-C) en todas las nuevas cargas de objetos a los buckets de Amazon S3.

Un ingeniero de seguridad está creando una SCP (política de control de servicio) que incluya un efecto Deny para la acción s3:PutObject.

¿Qué condición debe agregar el ingeniero de seguridad a la SCP para hacer cumplir el nuevo requisito de SSE-C?

**A.**

B.

C.

D.

171.- Una empresa quiere denegar el acceso a un bucket de Amazon S3 llamado DOC-EXAMPLE-BUCKET a un usuario federado específico llamado Bob. La empresa desea cumplir este requisito utilizando una política del bucket.

Además, es necesario asegurarse de que esta política del bucket afecte únicamente los permisos de Bob en S3. Cualquier otro permiso que tenga Bob debe mantenerse intacto.

¿Qué política debe usar la empresa para cumplir con estos requisitos?

A.

**B.**

C.

D.

172.- Una empresa ejecuta un juego en línea en AWS. Cuando los jugadores se registran en el juego, sus credenciales de nombre de usuario y contraseña se almacenan en una base de datos Amazon Aurora.

El número de usuarios ha crecido hasta alcanzar cientos de miles de jugadores. La cantidad de solicitudes de restablecimiento de contraseñas y asistencia para iniciar sesión se ha convertido en una carga para el equipo de atención al cliente de la empresa.

La empresa necesita implementar una solución que permita a los jugadores otra forma de iniciar sesión en el juego. La solución debe eliminar la carga de restablecer contraseñas y brindar asistencia de inicio de sesión, y al mismo tiempo proteger de forma segura las credenciales de cada jugador.

¿Qué solución cumplirá con estos requisitos?

A. Cuando un nuevo jugador se registre, usar una función de AWS Lambda para crear automáticamente una clave de acceso IAM y una clave secreta de acceso. Programar la función Lambda para almacenar las credenciales en el dispositivo del jugador. Crear claves IAM para los jugadores ya registrados.

B. Migrar las credenciales de los jugadores desde la base de datos Aurora a AWS Secrets Manager. Cuando un nuevo jugador se registre, crear un par clave-valor en Secrets Manager con el ID de usuario y la contraseña del jugador.

**C. Configurar Amazon Cognito user pools para federar el acceso al juego con proveedores de identidad externos (IdP), como proveedores sociales. Migrar el mecanismo de autenticación del juego a Cognito.**

D. En lugar de usar nombres de usuario y contraseñas para la autenticación, emitir claves de API para jugadores nuevos y existentes. Crear una API en Amazon API Gateway para que el cliente del juego acceda a la funcionalidad del juego.

173.- Una empresa sospecha que un atacante explotó un rol con permisos excesivos para exportar credenciales desde los metadatos de una instancia de Amazon EC2. La empresa utiliza Amazon GuardDuty y AWS Audit Manager, y tiene habilitados los registros de AWS CloudTrail y Amazon CloudWatch en todas sus cuentas de AWS.

Un ingeniero de seguridad debe determinar si las credenciales fueron utilizadas para acceder a los recursos de la empresa desde una cuenta externa.

¿Qué solución proporcionará esta información?

**A. Revisar los hallazgos de GuardDuty para encontrar eventos de tipo InstanceCredentialExfiltration.**

B. Revisar los informes de evaluación en la consola de Audit Manager para encontrar eventos de tipo InstanceCredentialExfiltration.

C. Revisar los registros de CloudTrail en busca de llamadas a la API GetSessionToken del servicio AWS STS que provengan de un ID de cuenta externo a la empresa.

D. Revisar los registros de CloudWatch en busca de llamadas a la API GetSessionToken del servicio AWS STS que provengan de un ID de cuenta externo a la empresa.

174.- Un ingeniero de seguridad necesita ejecutar un script de AWS CloudFormation. El script construye infraestructura en AWS para soportar una pila (stack) que incluye servidores web y una base de datos MySQL. La pila ya se ha implementado en entornos de preproducción y está lista para producción.

El script de producción debe cumplir con el principio de privilegios mínimos. Además, debe existir una separación de funciones entre la cuenta IAM del ingeniero de seguridad y CloudFormation.

¿Qué solución cumplirá con estos requisitos?

**A. Usar IAM Access Analyzer para generar una política que permita al script de CloudFormation ejecutarse y administrar la pila. Adjuntar la política a un nuevo rol de IAM. Modificar los permisos de la cuenta IAM del ingeniero de seguridad para que pueda pasar el nuevo rol a CloudFormation.**

B. Crear una política de IAM que permita permisos ec2:\* y rds:\*. Adjuntar la política a un nuevo rol de IAM. Modificar los permisos del ingeniero de seguridad para que pueda asumir el nuevo rol.

C. Usar IAM Access Analyzer para generar una política que permita al script de CloudFormation ejecutarse y administrar la pila. Modificar los permisos del ingeniero de seguridad para que pueda ejecutar directamente el script de CloudFormation.

D. Crear una política de IAM que permita permisos ec2:\* y rds:\*. Adjuntar la política a un nuevo rol de IAM. Usar el simulador de políticas de IAM para confirmar que la política permite las llamadas a la API necesarias para construir la pila. Modificar los permisos del ingeniero de seguridad para que pueda pasar el nuevo rol a CloudFormation.

175.- Una empresa que usa AWS Organizations está migrando cargas de trabajo a AWS. El equipo de aplicaciones de la empresa ha determinado que las cargas de trabajo usarán instancias de Amazon EC2, buckets de Amazon S3, tablas de Amazon DynamoDB y Application Load Balancers. Para cada tipo de recurso, la empresa exige que los despliegues cumplan con los siguientes requisitos:

Todas las instancias EC2 deben ser lanzadas desde cuentas de AWS aprobadas.

Todas las tablas de DynamoDB deben crearse siguiendo una convención de nombres estandarizada.

Toda la infraestructura que se aprovisione en cualquier cuenta de la organización debe desplegarse mediante plantillas de AWS CloudFormation.

¿Qué combinación de pasos debe tomar el equipo de aplicaciones para cumplir con estos requisitos? (Elige dos opciones).

**A. Crear plantillas de CloudFormation en una cuenta de administrador de AWS. Compartir los stack sets con una cuenta de aplicaciones. Restringir el uso de la plantilla específicamente a la cuenta de aplicaciones.**

B. Crear plantillas de CloudFormation en una cuenta de aplicaciones de AWS. Compartir los resultados con una cuenta de administrador para revisar los recursos que cumplen. Restringir los resultados solo a la cuenta de administrador.

C. Usar permissions boundaries para evitar que la cuenta de aplicaciones aprovisione ciertos recursos a menos que se cumplan las condiciones de cumplimiento interno.

**D. Usar SCPs para evitar que la cuenta de aplicaciones aprovisione ciertos recursos a menos que se cumplan las condiciones de cumplimiento interno.**

E. Activar reglas administradas de AWS Config para cada servicio en la cuenta de aplicaciones de AWS.

176.- Una empresa tiene un sistema de procesamiento por lotes que utiliza Amazon S3, Amazon EC2 y AWS Key Management Service (AWS KMS). El sistema opera con dos cuentas de AWS: la Cuenta A y la Cuenta B.

La Cuenta A aloja un bucket de S3 que almacena los objetos que serán procesados, así como los resultados del procesamiento. Todos los objetos del bucket están cifrados con una clave de KMS administrada en la Cuenta A.

La Cuenta B aloja una VPC que contiene un grupo de instancias EC2 que acceden al bucket S3 de la Cuenta A mediante políticas definidas en el bucket. La VPC fue creada con nombres DNS de host habilitados y resolución DNS habilitada.

Un ingeniero de seguridad necesita actualizar el diseño del sistema sin modificar el código existente. Además, ninguna llamada a la API de AWS desde las instancias EC2 de procesamiento por lotes puede viajar por Internet.

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

**A. En la VPC de la Cuenta B, crear un endpoint de VPC tipo gateway para Amazon S3. Para el endpoint, crear una política de recursos que permita las acciones s3:GetObject, s3:ListBucket, s3:PutObject y s3:PutObjectAcl sobre el bucket S3.**

B. En la VPC de la Cuenta B, crear un endpoint de VPC tipo interfaz para Amazon S3. Para este endpoint, crear una política de recursos que permita las acciones s3:GetObject, s3:ListBucket, s3:PutObject y s3:PutObjectAcl sobre el bucket S3.

**C. En la VPC de la Cuenta B, crear un endpoint de VPC tipo interfaz para AWS KMS. Para este endpoint, crear una política de recursos que permita las acciones kms:Encrypt, kms:Decrypt y kms:GenerateDataKey para la clave KMS. Asegurarse de que DNS privado esté activado para el endpoint.**

D. En la VPC de la Cuenta B, crear un endpoint de VPC tipo interfaz para AWS KMS. Para este endpoint, crear una política de recursos que permita las acciones kms:Encrypt, kms:Decrypt y kms:GenerateDataKey para la clave KMS. Asegurarse de que DNS privado esté desactivado para el endpoint.

E. En la VPC de la Cuenta B, verificar que la política del bucket S3 permita la acción s3:PutObjectAcl para uso entre cuentas. Luego, crear un endpoint de VPC tipo gateway para Amazon S3. Para el endpoint, crear una política de recursos que permita las acciones s3:GetObject, s3:ListBucket y s3:PutObject sobre el bucket S3.

177.- Un ingeniero de seguridad está diseñando una política IAM para un script que usará la CLI de AWS. Actualmente, el script asume un rol IAM al que están asociadas tres políticas administradas por AWS: AmazonEC2FullAccess, AmazonDynamoDBFullAccess, AmazonVPCFullAccess

El ingeniero de seguridad necesita construir una política IAM de mínimos privilegios que reemplace esas políticas administradas.

¿Qué solución cumplirá con estos requisitos de la manera más eficiente operativamente?

**A. En AWS CloudTrail, crear un trail para eventos de administración. Ejecutar el script con las políticas administradas existentes. Usar IAM Access Analyzer para generar una nueva política IAM basada en la actividad registrada en el trail. Reemplazar las políticas administradas por la nueva política generada.**

B. Eliminar las políticas administradas existentes del rol. Adjuntar el generador de políticas de IAM Access Analyzer al rol. Ejecutar el script. Ir a Access Analyzer y generar una política IAM de mínimos privilegios. Adjuntar la nueva política al rol.

C. Crear un analizador de cuenta en IAM Access Analyzer. Crear una regla de archivo (archive rule) con un filtro que revise si PrincipalArn coincide con el ARN del rol. Ejecutar el script. Eliminar las políticas administradas existentes del rol.

D. En AWS CloudTrail, crear un trail para eventos de administración. Eliminar las políticas administradas existentes del rol. Ejecutar el script. Buscar los errores de autorización en los eventos del trail asociados al script. Crear una política IAM nueva que incluya la acción y recurso que causó el fallo. Repetir el proceso hasta que el script funcione. Adjuntar la nueva política al rol.

178.- Un ingeniero de seguridad está diseñando una arquitectura en la nube para dar soporte a una aplicación. La aplicación se ejecuta en instancias de Amazon EC2 y procesa información sensible, incluidos números de tarjetas de crédito.

La aplicación enviará los números de tarjetas de crédito a un componente que se ejecuta en un entorno aislado. Este componente cifrará, almacenará y descifrará los números, y luego emitirá tokens para reemplazar los números en otras partes de la aplicación.

El componente que gestiona el proceso de tokenización se implementará en un conjunto separado de instancias EC2. Los demás componentes de la aplicación no deben poder almacenar ni acceder a los números de tarjetas de crédito.

¿Qué solución cumple con estos requisitos?

A. Usar instancias dedicadas de EC2 (Dedicated Instances) para el componente de tokenización de la aplicación.

B. Colocar las instancias EC2 que gestionan el proceso de tokenización en un grupo de ubicación de particiones (partition placement group).

C. Crear una VPC separada e implementar nuevas instancias EC2 en esa VPC para manejar la tokenización de datos.

**D. Implementar el código de tokenización en AWS Nitro Enclaves alojados en instancias EC2.**

179.- Una empresa tiene dos cuentas de AWS: la Cuenta A y la Cuenta B. La Cuenta A tiene un rol de IAM que los usuarios de IAM en la Cuenta B asumen cuando necesitan subir documentos sensibles a los buckets de Amazon S3 en la Cuenta A.

Un nuevo requisito establece que los usuarios solo pueden asumir el rol si están autenticados con MFA (autenticación multifactor). Un ingeniero de seguridad debe recomendar una solución que cumpla con este requisito con el menor riesgo y esfuerzo posible.

¿Qué solución debería recomendar el ingeniero de seguridad?

A. Agregar una condición aws:MultiFactorAuthPresent a la política de permisos del rol.

**B. Agregar una condición aws:MultiFactorAuthPresent a la política de confianza del rol.**

C. Agregar una condición aws:MultiFactorAuthPresent a la política de sesión.

D. Agregar una condición aws:MultiFactorAuthPresent a las políticas de los buckets de S3.

180.- Una empresa quiere recibir notificaciones por correo electrónico automáticas cuando se detecten claves de acceso de cuentas de desarrolladores de AWS en sitios de repositorios de código.

¿Qué solución proporcionará las notificaciones por correo electrónico requeridas?

**A. Crear una regla de Amazon EventBridge para enviar notificaciones por correo electrónico mediante Amazon SNS (Simple Notification Service) para hallazgos de Amazon GuardDuty del tipo UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS.**

B. Cambiar la información de contacto de tipo "Operaciones" de la cuenta de AWS a una dirección de correo electrónico distinta. Consultar periódicamente esta dirección de correo para revisar notificaciones.

C. Crear una regla de Amazon EventBridge que reaccione a eventos de AWS Health con un valor de "Risk" en la categoría de servicio. Configurar notificaciones por correo usando Amazon SNS.

D. Implementar un nuevo software de detección de anomalías. Ingerir los registros de AWS CloudTrail. Configurar la supervisión para eventos de tipo ConsoleLogin en la Consola de Administración de AWS. Configurar notificaciones por correo desde el software de detección de anomalías.

181.- Una empresa desplegó una instancia Amazon EC2 en una VPC en AWS. Una alerta reciente indica que la instancia EC2 está recibiendo una cantidad sospechosa de solicitudes a través de un puerto TCP abierto desde una fuente externa. El puerto TCP permanece abierto por períodos prolongados.

El equipo de seguridad de la empresa necesita detener toda la actividad hacia ese puerto desde la fuente externa para asegurarse de que la instancia EC2 no esté siendo comprometida. Sin embargo, la aplicación debe seguir estando disponible para otros usuarios.

¿Qué solución cumplirá con estos requisitos?

**A. Actualizar la ACL de red asociada a la subred de la instancia EC2. Agregar una declaración Deny para el puerto y las direcciones IP de origen.**

B. Actualizar el grupo de seguridad del interfaz de red elástica (ENI) de la instancia EC2 para eliminar el puerto de la lista de reglas de entrada.

C. Actualizar el grupo de seguridad del ENI de la instancia EC2 agregando una entrada Deny en la lista de entrada para el puerto y las direcciones IP de origen.

D. Crear una nueva ACL de red para la subred. Denegar todo el tráfico desde la instancia EC2 para evitar que se extraigan datos.

182.- Una empresa ha asegurado el usuario root de su cuenta de AWS siguiendo las mejores prácticas de AWS. También ha habilitado AWS CloudTrail, que está enviando sus registros a Amazon S3. Un ingeniero de seguridad quiere recibir una notificación en casi tiempo real si alguien utiliza las credenciales del usuario root para iniciar sesión en la Consola de administración de AWS.

¿Qué soluciones permitirán recibir esta notificación? (Elige dos opciones).

A. Usar AWS Trusted Advisor y sus evaluaciones de seguridad para la cuenta root. Configurar una regla de Amazon EventBridge que sea activada por la API de Trusted Advisor. Configurar la regla para que tenga como destino un tema de Amazon SNS. Suscribir los endpoints necesarios a ese tema para que reciban la notificación.

B. Usar AWS IAM Access Analyzer. Crear un filtro de métricas en Amazon CloudWatch Logs para evaluar las entradas del registro de Access Analyzer que detecten un inicio de sesión exitoso con la cuenta root. Crear una alarma de CloudWatch que monitoree si ha ocurrido un inicio de sesión con la cuenta root. Configurar la alarma para que notifique a un tema de Amazon SNS cuando entre en estado ALARM. Suscribir los endpoints necesarios al tema para que reciban la notificación.

**C. Configurar AWS CloudTrail para que envíe sus registros a Amazon CloudWatch Logs. Configurar un filtro de métricas en el grupo de logs de CloudWatch que utiliza CloudTrail para detectar registros de inicio de sesión exitosos con la cuenta root. Crear una alarma de Amazon CloudWatch que monitoree si ha ocurrido dicho inicio de sesión. Configurar la alarma para que notifique a un tema de Amazon SNS cuando entre en estado ALARM. Suscribir los endpoints necesarios al tema para recibir la notificación.**

D. Configurar AWS CloudTrail para que envíe notificaciones de registros a un tema de Amazon SNS. Crear una función de AWS Lambda que analice las notificaciones de CloudTrail en busca de actividad del usuario root e informe a otro tema de SNS con los endpoints que deben recibir la notificación. Suscribir la función Lambda al tema SNS que recibe las notificaciones de CloudTrail.

**E. Configurar una regla de Amazon EventBridge que se active cuando las llamadas a la API de Amazon CloudWatch registren un inicio de sesión exitoso con la cuenta root. Configurar la regla para que tenga como destino un tema de Amazon SNS. Suscribir los endpoints necesarios a ese tema para recibir la notificación.**

183.- Una empresa tiene cuentas de AWS que están organizadas dentro de una organización en AWS Organizations. Un ingeniero de seguridad necesita configurar AWS Security Hub en una cuenta dedicada exclusivamente al monitoreo de seguridad.

El ingeniero debe asegurarse de que Security Hub administre automáticamente todas las cuentas existentes y también las nuevas cuentas que se agreguen a la organización. Además, Security Hub debe recibir hallazgos desde todas las regiones de AWS.

¿Cuál combinación de acciones cumplirá estos requisitos con el menor esfuerzo operativo posible? (Elige dos opciones).

**A. Configurar una región de agregación de hallazgos en Security Hub. Enlazar las demás regiones a esta región de agregación.**

B. Crear una función de AWS Lambda que enrute eventos desde otras regiones hacia la cuenta dedicada de Security Hub. Crear una regla de Amazon EventBridge para invocar la función Lambda.

**C. Activar la opción para habilitar automáticamente cuentas en Security Hub.**

D. Crear una política de control de servicio (SCP) que deniegue el permiso securityhub:DisableSecurityHub. Asociar esta SCP a la cuenta raíz de la organización.

E. Configurar los servicios en otras regiones para que escriban eventos en un rastro de AWS CloudTrail a nivel de organización. Configurar Security Hub para que lea eventos desde ese rastro.

184.- Un ingeniero de seguridad está implementando una solución para permitir que los usuarios cifren objetos de Amazon S3 de forma transparente, sin necesidad de manejar directamente las claves. La solución debe ser altamente escalable y no requerir administración continua. Además, la organización debe poder eliminar inmediatamente las claves de cifrado.

¿Qué solución cumple con estos requisitos?

A. Usar AWS KMS con claves administradas por AWS y la API ScheduleKeyDeletion con PendingWindowInDays configurado en 0 para eliminar las claves si es necesario.

**B. Usar AWS KMS con material de clave importado y luego utilizar la API DeleteImportedKeyMaterial para eliminar el material de clave si es necesario.**

C. Usar AWS CloudHSM para almacenar las claves y luego usar la API de CloudHSM o la biblioteca PKCS11 para eliminarlas si es necesario.

D. Usar AWS Systems Manager Parameter Store para almacenar las claves y luego usar las operaciones de la API del servicio para eliminarlas si es necesario.

185.- Una empresa necesita implementar DNS Security Extensions (DNSSEC) para un subdominio específico. El subdominio ya está registrado en Amazon Route 53. Un ingeniero de seguridad ha habilitado la firma DNSSEC y ha creado una clave de firma de clave (KSK). Sin embargo, al intentar probar la configuración, el ingeniero recibe un error indicando una cadena de confianza rota.

¿Qué debe hacer el ingeniero de seguridad para resolver este error?

A. Reemplazar la KSK con una clave de firma de zona (ZSK).

B. Desactivar y luego volver a activar la KSK.

**C. Crear un registro Delegation Signer (DS) en la zona hospedada del dominio principal.**

D. Crear un registro Delegation Signer (DS) en el subdominio.

186.- Una empresa usó AWS Organizations para configurar un entorno con múltiples cuentas de AWS. Actualmente, la organización de la empresa tiene dos cuentas de AWS, pero se espera agregar más de 50 cuentas adicionales durante los próximos 12 meses. La empresa requiere que todas las cuentas actuales y futuras usen Amazon GuardDuty. Cada cuenta actual ya tiene GuardDuty activado. Actualmente, la empresa revisa los hallazgos de GuardDuty iniciando sesión en cada cuenta individualmente.

La empresa desea tener una vista centralizada de los hallazgos de GuardDuty de las cuentas existentes y de cualquier cuenta futura. Además, debe asegurarse de que GuardDuty se active automáticamente en cualquier nueva cuenta de AWS.

¿Qué solución cumplirá con estos requisitos?

A. Activar AWS Security Hub en la cuenta principal (management account) de la organización. Configurar GuardDuty dentro de esa cuenta para enviar todos los hallazgos a Security Hub.

**B. Crear una nueva cuenta de AWS dentro de la organización. Activar GuardDuty en esa cuenta. Designarla como cuenta administradora delegada para GuardDuty. Configurar GuardDuty para agregar las cuentas existentes como cuentas miembro. Seleccionar la opción para agregar automáticamente nuevas cuentas de AWS a la organización.**

C. Crear una nueva cuenta en la organización. Activar GuardDuty en esa cuenta. Activar AWS Security Hub en cada cuenta. Seleccionar la opción para agregar automáticamente nuevas cuentas de AWS a la organización.

D. Activar AWS Security Hub en la cuenta principal de la organización. Designar esa cuenta como administradora delegada de Security Hub. Agregar las cuentas existentes como cuentas miembro. Seleccionar la opción para agregar automáticamente nuevas cuentas a la organización. Enviar todos los hallazgos de Security Hub a la cuenta de GuardDuty de la organización.

187.- Una empresa quiere eliminar permanentemente todas las claves SSH de un subconjunto específico de sus instancias Amazon EC2 con Amazon Linux 2, las cuales están utilizando el mismo perfil de instancia IAM. Sin embargo, tres personas con cuentas de usuario IAM necesitarán acceder a estas instancias mediante sesiones SSH para realizar tareas críticas.

¿Cómo puede un ingeniero de seguridad proporcionar acceso y cumplir con estos requisitos?

A. Asignar una política IAM al perfil de instancia para permitir que las instancias EC2 sean gestionadas por AWS Systems Manager. Dar a las cuentas de usuario IAM los permisos necesarios para usar Systems Manager. Eliminar las claves SSH de las instancias EC2. Usar Systems Manager Inventory para seleccionar la instancia EC2 y conectarse.

B. Asignar una política IAM a las cuentas de usuario IAM para otorgarles permisos de uso de AWS Systems Manager Run Command. Eliminar las claves SSH de las instancias EC2. Usar Run Command para abrir una conexión SSH con la instancia EC2.

**C. Asignar una política IAM al perfil de instancia para permitir que las instancias EC2 sean gestionadas por AWS Systems Manager. Dar a las cuentas de usuario IAM permisos para usar Systems Manager. Eliminar las claves SSH de las instancias EC2. Usar Systems Manager Session Manager para seleccionar la instancia EC2 y conectarse.**

D. Asignar una política IAM a las cuentas de usuario IAM para permitirles usar el servicio EC2 desde la consola de administración de AWS. Eliminar las claves SSH de las instancias EC2. Conectarse a la instancia EC2 como ec2-user a través del método de cliente SSH de la consola de EC2 de AWS.

188.- Una empresa está almacenando datos en Amazon S3 Glacier. Un ingeniero de seguridad implementó una nueva política de Vault Lock para 10 TB de datos y ejecutó la operación initiate-vault-lock hace 12 horas. El equipo de auditoría identificó un error tipográfico en la política que está permitiendo acceso no intencionado al vault.

¿Cuál es la forma más rentable (cost-effective) de corregir este error?

**A. Invoque la operación abort-vault-lock, actualizar la política y luego volver a ejecutar initiate-vault-lock.**

B. Copiar los datos del vault a un nuevo bucket de S3. Eliminar el vault. Crear un nuevo vault con los datos.

C. Actualizar la política manteniendo el vault lock actual.

D. Actualizar la política y volver a ejecutar initiate-vault-lock para aplicar la nueva política.

189.- Una empresa utiliza HTTP Live Streaming (HLS) para transmitir contenido de video en vivo a suscriptores de pago mediante Amazon CloudFront. HLS divide el video en fragmentos para que el usuario pueda solicitar el fragmento adecuado según diferentes condiciones. Como los eventos de video duran varias horas, el video completo se compone de miles de fragmentos.

La URL del origen no se revela, y todos los usuarios están obligados a acceder mediante la URL de CloudFront. La empresa tiene una aplicación web que autentica a los usuarios de pago contra un repositorio interno, y ya dispone de un par de claves de CloudFront emitido.

¿Cuál es la forma más simple y MÁS efectiva de proteger el contenido?

A. Desarrollar la aplicación para usar el par de claves de CloudFront y generar URLs firmadas que los usuarios utilizarán para acceder al contenido.

**B. Desarrollar la aplicación para usar el par de claves de CloudFront y establecer cookies firmadas que los usuarios utilizarán para acceder al contenido.**

C. Desarrollar la aplicación para emitir un token de seguridad que Lambda@Edge recibirá para autenticar y autorizar el acceso al contenido.

D. Mantener la URL de CloudFront cifrada dentro de la aplicación y usar AWS

190.- Una empresa ejecuta sus cargas de trabajo en la región us-east-1. La empresa nunca ha desplegado recursos en otras regiones de AWS y no tiene recursos multi-región. Ahora necesita replicar sus cargas de trabajo e infraestructura en la región us-west-1.

Un ingeniero de seguridad debe implementar una solución que utilice AWS Secrets Manager para almacenar secretos en ambas regiones. La solución debe utilizar AWS Key Management Service (AWS KMS) para cifrar los secretos, minimizar la latencia y seguir funcionando incluso si solo una región está disponible.

El ingeniero de seguridad ya creó los secretos en us-east-1 usando Secrets Manager.

¿Qué debe hacer el ingeniero de seguridad a continuación para cumplir con los requisitos?

A. Cifrar los secretos en us-east-1 usando una clave KMS administrada por AWS. Replicar los secretos a us-west-1. Cifrar los secretos en us-west-1 usando una nueva clave KMS administrada por AWS en esa región.

B. Cifrar los secretos en us-east-1 usando una clave KMS administrada por AWS. Configurar los recursos en us-west-1 para que llamen al endpoint de Secrets Manager en us-east-1.

C. Cifrar los secretos en us-east-1 usando una clave KMS administrada por el cliente. Configurar los recursos en us-west-1 para que llamen al endpoint de Secrets Manager en us-east-1.

**D. Cifrar los secretos en us-east-1 usando una clave KMS administrada por el cliente. Replicar los secretos a us-west-1. Cifrar los secretos en us-west-1 usando la misma clave KMS administrada por el cliente desde us-east-1.**

191.- Una empresa opera una aplicación web que se ejecuta en instancias Amazon EC2. La aplicación escucha en los puertos 80 y 443. La empresa utiliza un Application Load Balancer (ALB) junto con AWS WAF para terminar la conexión SSL y reenviar el tráfico a las instancias de la aplicación solo por el puerto 80.

El ALB está en subredes públicas asociadas a una ACL de red llamada NACL1. Las instancias de la aplicación están en subredes privadas dedicadas, asociadas a la ACL de red NACL2. Una base de datos Amazon RDS para PostgreSQL, que usa el puerto 5432, está en una subred privada dedicada, asociada a la ACL de red NACL3. Actualmente, todas las ACLs de red permiten todo el tráfico de entrada y salida.

¿Qué conjunto de cambios en las ACLs de red aumentará la seguridad de la aplicación sin afectar su funcionamiento?

A. Hacer los siguientes cambios en NACL3:

Agregar una regla que permita tráfico entrante en el puerto 5432 desde NACL2.

Agregar una regla que permita tráfico saliente en los puertos 1024-65536 hacia NACL2.

Eliminar las reglas predeterminadas que permiten todo el tráfico de entrada y salida.

**B. Hacer los siguientes cambios en NACL3:**

**Agregar una regla que permita tráfico entrante en el puerto 5432 desde los bloques CIDR de las subredes de las instancias de la aplicación.**

**Agregar una regla que permita tráfico saliente en los puertos 1024-65536 hacia las subredes de las instancias de la aplicación.**

**Eliminar las reglas predeterminadas que permiten todo el tráfico de entrada y salida.**

C. Hacer los siguientes cambios en NACL2:

Agregar una regla que permita tráfico saliente en el puerto 5432 hacia los bloques CIDR de las subredes de RDS.

Eliminar las reglas predeterminadas que permiten todo el tráfico de entrada y salida.

D. Hacer los siguientes cambios en NACL2:

Agregar una regla que permita tráfico entrante en el puerto 5432 desde los bloques CIDR de las subredes de RDS.

Agregar una regla que permita tráfico saliente en el puerto 5432 hacia las subredes de RDS.

192.- AWS CloudTrail se está utilizando para monitorear llamadas a la API dentro de una organización. Una auditoría reveló que CloudTrail no está entregando los eventos a Amazon S3 como se esperaba.

¿Qué acciones iniciales se deben tomar para permitir la entrega de eventos de CloudTrail a S3? (Elige dos opciones).

**A. Verificar que la política del bucket de S3 permita a CloudTrail escribir objetos.**

B. Verificar que el rol de IAM utilizado por CloudTrail tenga acceso para escribir en Amazon CloudWatch Logs.

C. Eliminar cualquier política de ciclo de vida en el bucket de S3 que esté archivando objetos en S3 Glacier Flexible Retrieval.

**D. Verificar que el bucket de S3 definido en CloudTrail exista.**

E. Verificar que el prefijo del archivo de registro definido en CloudTrail exista en el bucket de S3.

193.- Una empresa tiene certificados públicos que son administrados por AWS Certificate Manager (ACM). Los certificados pueden ser certificados importados o certificados gestionados por ACM con métodos de validación mixtos. Un ingeniero de seguridad necesita diseñar una solución de monitoreo que envíe alertas por correo electrónico cuando un certificado esté próximo a vencer.

¿Cuál es la forma más eficiente operativamente de cumplir con este requisito?

A. Crear una función de AWS Lambda que liste todos los certificados y revise cada uno usando el SDK de AWS para obtener su información. Filtrar según el atributo NotAfter (fecha de expiración) y enviar una notificación por correo. Usar una expresión de programación de Amazon EventBridge para ejecutar la función Lambda diariamente.

B. Crear una alarma de Amazon CloudWatch. Agregar todos los ARN de certificados en el espacio de nombres AWS/CertificateManager a la métrica DaysToExpiry. Configurar la alarma para que envíe una notificación a un tema de Amazon SNS cuando el valor de DaysToExpiry sea menor o igual a 31.

C. Configurar AWS Security Hub. Activar el estándar AWS Foundational Security Best Practices con integración de ACM para enviar hallazgos. Crear y usar una acción personalizada que haga coincidir el patrón de eventos desde ACM usando el atributo NotBefore como fuente del evento. Crear un tema de Amazon SNS como destino.

**D. Crear una regla de Amazon EventBridge usando un patrón predefinido para ACM. Elegir el evento "ACM Certificate Approaching Expiration" como patrón de evento. Crear un tema de Amazon SNS como destino.**

194.- Un equipo de seguridad es responsable de revisar la actividad de llamadas a la API de AWS en el entorno en la nube para detectar violaciones de seguridad. Estos eventos deben registrarse y mantenerse en una ubicación centralizada, tanto para las regiones actuales como para las futuras de AWS.

¿Cuál es la forma más simple de cumplir con estos requisitos?

A. Activar las verificaciones de seguridad de AWS Trusted Advisor en la consola de AWS y reportar todos los incidentes de seguridad en todas las regiones.

B. Activar AWS CloudTrail creando registros (trails) individuales para cada región y especificar un único bucket de Amazon S3 para recibir los archivos de registro para su análisis posterior.

**C. Activar AWS CloudTrail creando un nuevo registro y aplicarlo a todas las regiones. Especificar un único bucket de Amazon S3 como ubicación de almacenamiento.**

D. Activar el registro en Amazon CloudWatch para todos los servicios de AWS en todas las regiones y agregarlos en un único bucket de Amazon S3 para su análisis posterior.

195.- Una empresa ejecuta una aplicación en instancias de Amazon EC2 dentro de un grupo de Auto Scaling. La aplicación almacena los registros (logs) localmente. Un ingeniero de seguridad notó que los registros se perdieron después de un evento de reducción de escala (scale-in). El ingeniero necesita recomendar una solución que garantice la durabilidad y disponibilidad de los datos de los registros. Todos los registros deben conservarse por al menos 1 año para fines de auditoría.

¿Qué debería recomendar el ingeniero de seguridad?

A. Dentro del ciclo de vida del Auto Scaling, agregar un hook para crear y adjuntar un volumen de Amazon Elastic Block Store (Amazon EBS) para logs cada vez que se cree una instancia EC2. Cuando la instancia se termine, el volumen EBS puede ser re-adjuntado a otra instancia para revisar los logs.

B. Crear un sistema de archivos Amazon Elastic File System (Amazon EFS) y agregar un comando en la sección de user data de la plantilla de lanzamiento del Auto Scaling para montar el sistema EFS al crear la instancia EC2. Configurar un proceso en la instancia que copie los logs una vez al día desde el volumen EBS a un directorio en EFS.

**C. Agregar un agente de Amazon CloudWatch en la AMI utilizada por el grupo de Auto Scaling. Configurar el agente para enviar los registros a Amazon CloudWatch Logs para su revisión.**

D. Dentro del ciclo de vida del Auto Scaling, agregar un lifecycle hook en la transición de estado terminación y alertar al equipo de ingeniería mediante una notificación a Amazon SNS. Configurar el hook para que permanezca en estado “Terminating:Wait” durante 1 hora para permitir la revisión manual de los logs de seguridad antes de la terminación de la instancia.

196.- Una empresa utiliza instancias Amazon EC2 para alojar servicios frontend detrás de un Application Load Balancer (ALB). Los volúmenes de Amazon EBS están conectados a las instancias EC2. Además, la empresa usa buckets de Amazon S3 para almacenar archivos grandes como imágenes y música.

La empresa ya ha implementado una arquitectura de seguridad en AWS para prevenir, identificar y aislar posibles ataques de ransomware. Ahora desea reducir aún más el riesgo.

Un ingeniero de seguridad debe desarrollar una solución de recuperación ante desastres (DR) que permita recuperar la operación normal si un atacante logra evadir los controles preventivos y de detección.

La solución debe cumplir con un RPO (Recovery Point Objective) de 1 hora.

¿Qué solución cumple con estos requisitos?

**A. Usar AWS Backup para crear copias de seguridad de las instancias EC2 y de los buckets S3 cada hora. Crear plantillas de AWS CloudFormation que repliquen los componentes actuales de la arquitectura. Usar AWS CodeCommit para almacenar esas plantillas junto con el código de configuración de la aplicación.**

B. Usar AWS Backup para respaldar los volúmenes EBS y los objetos S3 una vez al día. Usar Amazon Security Lake para centralizar los registros de AWS CloudTrail y los VPC Flow Logs. Utilizar los logs para respuestas automatizadas.

C. Usar Amazon Security Lake para centralizar los registros de AWS CloudTrail y VPC Flow Logs. Usar los logs para automatizar respuestas. Habilitar AWS Security Hub para centralizar los procedimientos de recuperación. Crear plantillas de CloudFormation para replicar la arquitectura existente. Almacenar las plantillas y la configuración en AWS CodeCommit.

D. Crear instantáneas EBS cada 4 horas. Activar Amazon GuardDuty Malware Protection. Crear automatizaciones para restaurar de inmediato la última instantánea de cualquier instancia EC2 que genere un hallazgo Execution:EC2/MaliciousFile en GuardDuty.

197.- Una empresa tiene una aplicación que se ejecuta en instancias de Amazon EC2 detrás de un Application Load Balancer (ALB). Las instancias están en un grupo de Auto Scaling de EC2 y están asociadas a volúmenes de Amazon EBS.

Un ingeniero de seguridad necesita preservar toda la evidencia forense de una de las instancias.

¿Qué orden de pasos debe seguir el ingeniero de seguridad para cumplir con este requisito?

A. Tomar una instantánea del volumen EBS de la instancia y almacenarla en un bucket de Amazon S3. Tomar una captura de la memoria de la instancia y almacenarla en un bucket de S3. Separar la instancia del grupo de Auto Scaling. Anular el registro de la instancia del ALB. Detener la instancia.

B. Tomar una captura de la memoria de la instancia y almacenarla en un bucket de Amazon S3. Detener la instancia. Tomar una instantánea del volumen EBS de la instancia y almacenarla en un bucket de S3. Separar la instancia del grupo de Auto Scaling. Anular el registro de la instancia del ALB.

**C. Separar la instancia del grupo de Auto Scaling. Anular el registro de la instancia del ALB. Tomar una instantánea del volumen EBS de la instancia y almacenarla en un bucket de Amazon S3. Tomar una captura de la memoria de la instancia y almacenarla en un bucket de S3. Detener la instancia.**

D. Separar la instancia del grupo de Auto Scaling. Anular el registro de la instancia del ALB. Detener la instancia. Tomar una captura de la memoria de la instancia y almacenarla en un bucket de Amazon S3. Tomar una instantánea del volumen EBS de la instancia y almacenarla en un bucket de S3.

198.- Un equipo de desarrollo quiere utilizar AWS Certificate Manager (ACM) para solicitar certificados públicos y así asegurar que los datos estén cifrados en tránsito. Los dominios que se utilizarán no están alojados actualmente en Amazon Route 53.

El equipo desea usar una solución administrada por AWS para distribución y almacenamiento en caché con el fin de optimizar las solicitudes a sus sistemas y ofrecer mejores puntos de presencia a los clientes. Esta solución de distribución usará un nombre de dominio principal personalizado, y también varios nombres de dominio alternativos. Los certificados deben renovarse automáticamente por un período de tiempo indefinido.

¿Qué combinación de pasos debe seguir el equipo para implementar esta arquitectura? (Elige tres opciones)

A. Solicitar un certificado en ACM en la región us-west-2. Agregar los nombres de dominio que el certificado debe proteger.

B. Enviar un correo electrónico a los administradores de los dominios para solicitar la validación de los dominios en ACM.

**C. Solicitar la validación de los dominios para ACM mediante DNS. Insertar registros CNAME en la zona DNS de cada dominio.**

D. Crear un Application Load Balancer para la solución de caché. Seleccionar el certificado recién solicitado en ACM para conexiones seguras.

**E. Crear una distribución de Amazon CloudFront para la solución de caché. Ingresar el CNAME principal como el nombre de origen. Ingresar los subdominios o nombres alternativos en la configuración de Alternate Domain Names. Seleccionar el certificado recién solicitado en ACM para conexiones seguras.**

F. Solicitar un certificado en ACM en la región us-east-1. Agregar los nombres de dominio que el certificado debe proteger.

199.- El ingeniero de seguridad de una empresa quiere recibir una alerta por correo electrónico cada vez que Amazon GuardDuty, AWS Identity and Access Management Access Analyzer o Amazon Macie generen un hallazgo de seguridad de alta severidad. La empresa usa AWS Control Tower para gobernar todas sus cuentas, y también utiliza AWS Security Hub con todas las integraciones de servicios de AWS habilitadas.

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

A. Configurar funciones separadas de AWS Lambda para GuardDuty, IAM Access Analyzer y Macie, que llamen a las API públicas de cada servicio para obtener los hallazgos de alta severidad. Usar Amazon SNS para enviar las alertas por correo electrónico. Crear una regla de Amazon EventBridge que invoque las funciones de forma programada.

**B. Crear una regla de Amazon EventBridge con un patrón que coincida con eventos de hallazgos de Security Hub con alta severidad. Configurar la regla para enviar los hallazgos a un tema de Amazon SNS como destino. Suscribir las direcciones de correo electrónico deseadas al tema de SNS.**

C. Crear una regla de Amazon EventBridge con un patrón que coincida con eventos de AWS Control Tower con alta severidad. Configurar la regla para enviar los hallazgos a un tema de SNS como destino. Suscribir las direcciones de correo electrónico deseadas al tema de SNS.

D. Hospedar una aplicación en Amazon EC2 para llamar a las APIs de GuardDuty, IAM Access Analyzer y Macie. Dentro de la aplicación, usar la API de SNS para obtener los hallazgos de alta severidad y enviarlos a un tema de SNS. Suscribir las direcciones de correo electrónico deseadas al tema de SNS.

200.- Una empresa aloja una aplicación en instancias de Amazon EC2. La aplicación también utiliza Amazon S3 y Amazon Simple Queue Service (Amazon SQS). La aplicación está detrás de un Application Load Balancer (ALB) y escala automáticamente mediante AWS Auto Scaling.

La política de seguridad de la empresa requiere el uso del principio de menor privilegio, el cual ya ha sido aplicado a todos los recursos de AWS existentes. Un ingeniero de seguridad necesita implementar conectividad privada a los servicios de AWS.

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

**A. Usar un punto de enlace VPC de tipo interface para Amazon SQS.**

B. Configurar una conexión a Amazon S3 mediante AWS Transit Gateway.

**C. Usar un punto de enlace VPC de tipo gateway para Amazon S3.**

D. Modificar el rol IAM asignado a las instancias EC2 en el grupo de Auto Scaling para permitir tráfico saliente hacia los puntos de enlace interface.

**E. Modificar las políticas de los endpoints VPC. Especificar los recursos de SQS y S3 que utiliza la aplicación.**

F. Configurar una conexión a Amazon S3 mediante AWS Firewall Manager.

201.- Un analista de seguridad intentó solucionar un problema relacionado con la monitorización de cambios sospechosos en los grupos de seguridad. Le informaron que existe una alarma de Amazon CloudWatch configurada para estos eventos de registros de AWS CloudTrail.

El analista probó la configuración haciendo un cambio en la configuración de un grupo de seguridad, pero no recibió ninguna alerta.

¿Cuál de los siguientes pasos de solución de problemas debería realizar el analista?

A. Asegurarse de que CloudTrail y el registro de acceso al bucket de S3 estén habilitados para la cuenta de AWS del analista.

**B. Verificar que se haya creado un filtro de métricas y que luego se haya asignado a una alarma. Revisar la acción de notificación de la alarma.**

C. Revisar los tableros (dashboards) de CloudWatch para asegurarse de que exista una métrica configurada con una dimensión adecuada para los cambios en los grupos de seguridad.

D. Verificar que la cuenta del analista esté asociada a una política IAM que incluya permisos para cloudwatch:GetMetricStatistics y cloudwatch:ListMetrics.

202.- Una API de Amazon API Gateway invoca una función de AWS Lambda que necesita interactuar con una plataforma de software como servicio (SaaS). En la plataforma SaaS se genera un token de cliente único para otorgar acceso a la función Lambda. Un ingeniero de seguridad necesita diseñar una solución que cifre el token de acceso en reposo y lo pase a la función Lambda en tiempo de ejecución.

¿Qué solución cumplirá con estos requisitos de la forma más rentable?

A. Almacenar el token de cliente como un secreto en AWS Secrets Manager. Usar el SDK de AWS para recuperar el secreto dentro de la función Lambda.

B. Configurar un autorizador Lambda basado en tokens en API Gateway.

**C. Almacenar el token de cliente como un parámetro SecureString en AWS Systems Manager Parameter Store. Usar el SDK de AWS para recuperar el valor del parámetro SecureString en la función Lambda.**

D. Usar AWS Key Management Service (AWS KMS) para cifrar el token de cliente. Pasar el token a la función Lambda en tiempo de ejecución mediante una variable de entorno.

203.- Una empresa está utilizando una distribución de Amazon CloudFront para entregar contenido desde dos orígenes. Uno de los orígenes es una aplicación dinámica alojada en instancias de Amazon EC2, y el otro es un bucket de Amazon S3 para archivos estáticos.

Un análisis de seguridad revela que las respuestas HTTPS de la aplicación no cumplen con el requisito de seguridad de incluir la cabecera HTTP X-Frame-Options, necesaria para prevenir ataques de tipo cross-site scripting relacionados con marcos (frames). Un ingeniero de seguridad debe asegurar que toda la pila cumpla con este requisito agregando la cabecera faltante en las respuestas.

¿Cuál solución cumplirá con estos requisitos?

**A. Crear una función Lambda@Edge. Incluir código para agregar la cabecera X-Frame-Options a la respuesta. Configurar la función para que se ejecute en el evento origin response de CloudFront.**

B. Crear una función Lambda@Edge. Incluir código para agregar la cabecera X-Frame-Options a la respuesta. Configurar la función para que se ejecute en el evento viewer request de CloudFront.

C. Actualizar la distribución de CloudFront agregando X-Frame-Options como cabecera personalizada en la configuración del origen.

D. Personalizar la aplicación alojada en EC2 para que agregue la cabecera X-Frame-Options en las respuestas que se devuelven a CloudFront.

204.- Una aplicación ha sido desarrollada con instancias de Amazon EC2 que recuperan mensajes desde Amazon SQS. Recientemente se hicieron cambios en IAM y ahora las instancias ya no pueden recuperar mensajes.

¿Qué acciones se deben tomar para solucionar el problema manteniendo el principio de privilegios mínimos? (Elige dos opciones).

A. Configurar y asignar un dispositivo MFA al rol utilizado por las instancias.

**B. Verificar que la política de recursos de SQS no deniegue explícitamente el acceso al rol usado por las instancias.**

C. Verificar que la clave de acceso asociada al rol usado por las instancias esté activa.

D. Adjuntar la política administrada AmazonSQSFullAccess al rol usado por las instancias.

**E. Verificar que el rol asociado a las instancias contenga políticas que permitan el acceso a la cola.**

205.- Una empresa tiene una clave administrada por el cliente en AWS Key Management Service (AWS KMS) con material de clave importado. La política de la empresa exige que todas las claves de cifrado se roten cada año.

¿Qué debe hacer un ingeniero de seguridad para cumplir con este requisito respecto a esta clave administrada por el cliente?

A. Habilitar la rotación automática de clave anualmente para la clave administrada por el cliente existente.

B. Usar la AWS CLI para crear una función de AWS Lambda que rote la clave administrada por el cliente existente cada año.

C. Importar nuevo material de clave en la clave administrada por el cliente existente. Rotar la clave manualmente.

**D. Crear una nueva clave administrada por el cliente. Importar nuevo material de clave en la nueva clave. Apuntar el alias de la clave a la nueva clave.**

206.- Una empresa del sector salud tiene múltiples cuentas de AWS dentro de una organización en AWS Organizations. La empresa utiliza buckets de Amazon S3 para almacenar información sensible de pacientes. Se necesita restringir que los usuarios puedan eliminar cualquier bucket de S3 en toda la organización.

¿Cuál es la solución MÁS escalable que cumple con estos requisitos?

A. Límites de permisos (Permissions boundaries) en AWS Identity and Access Management (IAM)

B. Políticas de bucket de S3 (S3 bucket policies)

C. Políticas de etiquetas (Tag policies)

**D. SCPs (Service Control Policies)**

207.- Una empresa necesita detectar accesos no autenticados a sus clústeres de Amazon Elastic Kubernetes Service (Amazon EKS). La solución debe funcionar sin requerir configuración adicional sobre el despliegue actual de EKS.

¿Qué solución cumplirá con estos requisitos con el mínimo esfuerzo operativo?

A. Instalar un complemento (add-on) de Amazon EKS de un proveedor de seguridad.

B. Habilitar AWS Security Hub y monitorear los hallazgos relacionados con Kubernetes.

C. Monitorear las métricas de Amazon CloudWatch Container Insights para Amazon EKS.

**D. Habilitar Amazon GuardDuty y usar la función de monitoreo de registros de auditoría de EKS .**

208.- Un ingeniero de seguridad está investigando una infección por malware que se ha propagado entre un conjunto de instancias de Amazon EC2. Un indicador clave del compromiso es el tráfico saliente por el puerto TCP 2905 hacia un conjunto de hosts de comando y control en internet.

El ingeniero de seguridad crea una regla en una ACL de red (network ACL) que deniega el tráfico saliente identificado. Aplica esta regla a la subred de las instancias EC2. Ahora, el ingeniero necesita identificar qué instancias EC2 están intentando comunicarse por el puerto TCP 2905.

¿Qué solución identificará las instancias afectadas con el MENOR esfuerzo operativo?

A. Crear un Network Access Scope en Amazon VPC Network Access Analyzer. Usar este scope para identificar las instancias EC2 que intentan enviar tráfico al puerto TCP 2905.

**B. Habilitar los VPC flow logs para la VPC donde están ubicadas las instancias EC2 afectadas. Configurar los logs para capturar el tráfico rechazado. Buscar en los logs registros REJECT que tengan como destino el puerto TCP 2905.**

C. Habilitar Amazon GuardDuty. Crear una lista IP personalizada en GuardDuty para generar hallazgos cuando una instancia EC2 intente comunicarse con alguno de los hosts de comando y control. Usar Amazon Detective para identificar las instancias EC2 que inician la comunicación.

D. Crear un firewall en AWS Network Firewall. Adjuntarlo a la subred de las instancias EC2. Crear una regla personalizada para identificar y registrar el tráfico del firewall en el puerto TCP 2905. Crear un filtro de métricas en Amazon CloudWatch Logs para identificar los registros del firewall que hagan referencia a tráfico en el puerto TCP 2905.

209.- Un ingeniero de seguridad utiliza Amazon Macie para escanear los buckets de Amazon S3 de una empresa en busca de datos sensibles. La empresa tiene muchos buckets de S3 y una gran cantidad de objetos almacenados en ellos. El ingeniero de seguridad debe identificar los buckets de S3 que contienen datos sensibles y realizar escaneos adicionales en esos buckets.

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

A. Configurar la replicación entre regiones (CRR) en los buckets de S3 para replicar los objetos a una segunda región de AWS. Configurar Macie en la segunda región para escanear los objetos replicados diariamente.

B. Crear una función de AWS Lambda como destino de eventos de S3 para los buckets. Configurar la función Lambda para iniciar un escaneo de Macie cuando se suba un objeto a un bucket de S3.

**C. Configurar el descubrimiento automatizado de Macie para que tome muestras continuamente de los datos en los buckets de S3. Realizar escaneos completos en los buckets donde Macie detecte datos sensibles.**

D. Configurar escaneos de Macie para que se ejecuten en los buckets de S3. Agregar los resultados de los escaneos en una tabla de Amazon DynamoDB y usar esa tabla para hacer consultas.

210.- Un ingeniero de seguridad de una gran empresa está gestionando una aplicación de procesamiento de datos que es utilizada por 1.500 empresas subsidiarias. Tanto la empresa matriz como sus subsidiarias utilizan AWS. La aplicación usa el puerto TCP 443 y se ejecuta en instancias de Amazon EC2 detrás de un Network Load Balancer (NLB). Por razones de cumplimiento, la aplicación debe ser accesible solo para las subsidiarias y no debe estar disponible en Internet público. Para cumplir con estos requisitos de acceso restringido, el ingeniero ha recibido los rangos de bloques CIDR públicos y privados de cada subsidiaria.

¿Qué solución debería implementar el ingeniero para aplicar las restricciones de acceso adecuadas a la aplicación?

A. Crear una NACL (lista de control de acceso a la red) para permitir el acceso por el puerto TCP 443 desde los 1.500 bloques CIDR de las subsidiarias. Asociar la NACL tanto al NLB como a las instancias EC2.

B. Crear un grupo de seguridad de AWS para permitir el acceso por el puerto TCP 443 desde los 1.500 bloques CIDR de las subsidiarias. Asociar el grupo de seguridad al NLB. Crear un segundo grupo de seguridad para las instancias EC2 que permita el acceso por el puerto TCP 443 desde el grupo de seguridad del NLB.

**C. Crear un servicio de endpoint de AWS PrivateLink en la cuenta de la empresa matriz, conectado al NLB. Crear un grupo de seguridad para las instancias que permita el acceso por el puerto TCP 443 desde el endpoint de AWS PrivateLink. Usar endpoints de interfaz de AWS PrivateLink en las 1.500 cuentas AWS de las subsidiarias para conectarse a la aplicación de procesamiento de datos.**

D. Crear un grupo de seguridad de AWS para permitir el acceso por el puerto TCP 443 desde los 1.500 bloques CIDR de las subsidiarias. Asociar el grupo de seguridad con las instancias EC2.

211.- Una empresa ejecuta cargas de trabajo en instancias Amazon EC2. La empresa necesita escanear continuamente esas instancias en busca de vulnerabilidades de software y exposición no intencionada a la red.

¿Qué solución cumplirá con estos requisitos?

**A. Usar Amazon Inspector. Configurar el modo de escaneo en escaneo híbrido.**

B. Usar Amazon GuardDuty. Habilitar la función de protección contra malware (Malware Protection).

C. Usar Amazon Inspector. Habilitar la función de protección contra malware (Malware Protection).

D. Usar Amazon GuardDuty. Habilitar la función de monitoreo en tiempo de ejecución (Runtime Monitoring).

212.- Una empresa tiene como requisito que ningún grupo de seguridad de Amazon EC2 permita acceso SSH desde el bloque CIDR 0.0.0.0/0. La empresa quiere monitorear el cumplimiento de este requisito en todo momento y recibir una notificación casi en tiempo real si algún grupo de seguridad no cumple con la política.

Un ingeniero de seguridad ya ha configurado AWS Config y utilizará la regla administrada restricted-ssh para monitorear los grupos de seguridad.

¿Qué debe hacer el ingeniero de seguridad a continuación para cumplir con estos requisitos?

A. Configurar AWS Config para que envíe sus capturas de configuración a un bucket de Amazon S3. Crear una función de AWS Lambda que se ejecute al producirse un evento PutObject en el bucket. Configurar la función Lambda para analizar la captura en busca de cambios de cumplimiento en la regla restricted-ssh. Configurar la función para enviar una notificación a un tema de Amazon SNS si se detecta un cambio.

**B. Configurar una regla de evento de Amazon EventBridge que se active con un evento de cambio de cumplimiento de AWS Config para la regla restricted-ssh. Configurar la regla para que tenga como destino un tema de Amazon SNS que enviará la notificación.**

C. Configurar AWS Config para que envíe todas sus notificaciones de cumplimiento a Amazon CloudWatch Logs. Configurar un filtro de métricas de CloudWatch Logs en el grupo de logs de AWS Config para buscar cambios en el cumplimiento de la regla restricted-ssh. Crear una alarma de CloudWatch sobre ese filtro para enviar una notificación a un tema de Amazon SNS si la alarma entra en estado ALARM.

D. Configurar una alarma de Amazon CloudWatch sobre la métrica de la regla restricted-ssh. Configurar la alarma para que envíe una notificación a un tema de Amazon SNS si la alarma entra en estado ALARM.

213.- Un ingeniero de seguridad descubre que las contraseñas de los usuarios de la empresa no tienen un largo mínimo requerido. La empresa está utilizando los siguientes dos proveedores de identidad (IdPs):

AWS Identity and Access Management (IAM) federado con Active Directory local

Amazon Cognito user pools que contienen la base de datos de usuarios para una aplicación en la nube de AWS desarrollada por la empresa

¿Qué combinación de acciones debe tomar el ingeniero de seguridad para implementar un largo mínimo requerido para las contraseñas? (Elige dos opciones).

A. Actualizar la política de longitud de contraseñas en la configuración de IAM.

**B. Actualizar la política de longitud de contraseñas en la configuración de Cognito.**

**C. Actualizar la política de longitud de contraseñas en la configuración de Active Directory local.**

D. Crear una SCP (Service Control Policy) en AWS Organizations y configurarla para exigir una longitud mínima de contraseña para IAM y Cognito.

E. Crear una política de IAM que incluya una condición de longitud mínima de contraseña y aplicarla a IAM y Cognito.

214.- Una empresa utiliza AWS Key Management Service (AWS KMS). Durante un intento de adjuntar un volumen cifrado de Amazon Elastic Block Store (Amazon EBS) a una instancia de Amazon EC2, la operación falla. La empresa descubre que una clave administrada por el cliente (CMK) se volvió inutilizable porque se eliminó el material de clave. La empresa necesita acceder a los datos que están en el volumen de EBS.

Un ingeniero de seguridad debe recomendar una solución para descifrar la clave de datos cifrada del volumen EBS. La solución también debe permitir adjuntar el volumen a la instancia EC2.

¿Qué solución cumplirá con estos requisitos?

A. Importar nuevo material de clave en la clave. Adjuntar el volumen de EBS.

B. Restaurar el volumen de EBS desde una snapshot tomada antes de que se eliminara el material de clave.

**C. Reimportar el mismo material de clave que originalmente se importó en la clave. Adjuntar el volumen de EBS.**

D. Crear una nueva clave. Importar nuevo material de clave. Adjuntar el volumen de EBS.

215.- Una empresa necesita analizar los registros de acceso (access logs) de un Application Load Balancer (ALB). El ALB dirige el tráfico al portal de inicio de sesión en línea de la empresa. Se requiere usar visualizaciones para identificar intentos de inicio de sesión por parte de bots, basándose en una lista de direcciones IP conocidas.

¿Qué solución cumplirá con estos requisitos?

A. Configurar el ALB para que envíe los registros directamente a Amazon CloudWatch Logs. Analizar y visualizar los registros usando CloudWatch Logs Insights.

B. Configurar el ALB para que envíe los registros directamente a Amazon Redshift. Analizar los registros usando consultas SQL. Visualizar los registros mediante informes personalizados.

C. Configurar el ALB para que envíe los registros directamente a Amazon OpenSearch Service. Analizar los registros mediante los paneles de OpenSearch. Visualizar los registros con dashboards personalizados.

**D. Configurar el ALB para que envíe los registros directamente a un bucket de Amazon S3. Analizar los registros usando Amazon Athena. Visualizar los datos con Amazon QuickSight.**

216.- Una empresa ejecuta un trabajo cron en una instancia de Amazon EC2 en un horario predefinido. Este trabajo cron llama a un script bash que cifra un archivo de 2 KB. Un ingeniero de seguridad crea una clave administrada por el cliente (CMK) en AWS Key Management Service (AWS KMS) con una política de clave. Tanto la política de la clave como el rol de la instancia EC2 tienen la configuración necesaria para este trabajo.

¿Qué proceso debe usar el script bash para cifrar el archivo?

**A. Usar el comando aws kms encrypt para cifrar el archivo utilizando la clave de KMS existente.**

B. Usar el comando aws kms create-grant para generar una concesión (grant) para la clave de KMS existente.

C. Usar el comando aws kms encrypt para generar una clave de datos. Usar la clave de datos en texto claro para cifrar el archivo.

D. Usar el comando aws kms generate-data-key para generar una clave de datos. Usar la clave de datos cifrada para cifrar el archivo.

217.- Un ingeniero de seguridad necesita analizar los registros de acceso del servidor web Apache, que están almacenados en un bucket de Amazon S3. Los registros fueron generados por instancias de Amazon EC2 que tienen instalado y configurado el agente de Amazon CloudWatch para reportar sus logs de acceso.

El ingeniero de seguridad necesita usar una consulta en Amazon Athena para analizar los registros. La consulta debe identificar las direcciones IP que intentaron acceder y fallaron al intentar acceder a contenido restringido del servidor ubicado en la ruta URL /admin. Además, la consulta debe identificar las URLs que esas IPs intentaron acceder.

¿Cuál consulta cumplirá con estos requisitos?

**A. SELECT client\_ip, client\_request FROM logs WHERE client\_request LIKE '%/admin%!’ AND server\_status = '403’**

B. SELECT client\_ip FROM logs WHERE client\_request CONTAINS '%/admin%’ AND server\_status = '401' GROUP BY client\_ip

C. SELECT DISTINCT (client\_ip), client\_request, client\_id FROM logs WHERE server status = ‘403’ LIMIT 1000

D. SELECT DISTINCT (client\_ip), client\_request FROM logs WHERE user\_id <> ‘admin’ AND server\_status = ‘401!’

218.- Una empresa utiliza Amazon Cognito como plataforma de identidad OAuth 2.0 para sus aplicaciones web y móviles. La empresa necesita registrar los intentos de inicio de sesión exitosos y fallidos, y también necesita consultar los datos sobre esos intentos.

¿Qué solución cumplirá con estos requisitos?

A. Configurar Cognito para enviar los registros de actividad del usuario a Amazon CloudWatch. Configurar Amazon EventBridge para invocar una función de AWS Lambda que exporte los registros a un bucket de Amazon S3. Usar Amazon Athena para consultar los registros por eventos con nombre SignUp y fuente de evento cognito-idp.amazonaws.com.

**B. Habilitar AWS CloudTrail para entregar registros a un bucket de Amazon S3. Usar Amazon Athena para consultar los registros por eventos con nombre InitiateAuth y fuente de evento cognito-idp.amazonaws.com.**

C. Configurar AWS CloudTrail para enviar los eventos de Cognito a Amazon CloudWatch para monitoreo. Consultar los registros de eventos por nombre SignUp y fuente de evento cognito-idp.amazonaws.com.

D. Configurar métricas de Amazon CloudWatch para monitorear e informar sobre los eventos de Cognito. Crear un panel de CloudWatch para las métricas proporcionadas. Mostrar los grupos de usuarios de Cognito por eventos con nombre InitiateAuth y fuente de evento cognito-idp.amazonaws.com.

219.- Un ingeniero de seguridad está configurando un trail de AWS CloudTrail para todas las regiones en una cuenta de AWS. Para mayor seguridad, los registros se almacenan usando cifrado del lado del servidor con claves administradas por AWS KMS (SSE-KMS) y tienen habilitada la validación de integridad de los logs.

Durante las pruebas de la solución, el ingeniero de seguridad descubre que los archivos de resumen (digest) se pueden leer, pero los archivos de logs no.

¿Cuál es la causa más probable?

A. Los archivos de logs fallaron la validación de integridad y automáticamente fueron marcados como no disponibles.

**B. La política de la clave KMS no otorga al usuario o rol IAM del ingeniero de seguridad permisos para descifrar con esa clave.**

C. El bucket está configurado para usar como predeterminado cifrado del lado del servidor con claves administradas por Amazon S3 (SSE-S3) y no permite archivos cifrados con SSE-KMS.

D. Una política IAM aplicada al usuario o rol del ingeniero de seguridad niega el acceso al prefijo “CloudTrail/” en el bucket de Amazon S3.

220.- Una empresa necesita desplegar de forma segura recursos y cargas de trabajo en varias cuentas de AWS. Las cuentas están dentro de una organización en AWS Organizations.

La empresa necesita usar AWS CloudFormation para gestionar la infraestructura como código (IaC) utilizando patrones arquitectónicos aprobados. Además, debe hacer cumplir requisitos de etiquetado y directrices específicas para la configuración y creación de recursos y cargas de trabajo.

¿Qué solución cumplirá con estos requisitos?

A. Usar políticas de pila de CloudFormation (stack policies) para evitar la creación de recursos que no cumplan con los requisitos de etiquetado o configuración. Usar reglas de Amazon EventBridge para detectar llamadas a la API que intenten crear recursos por fuera de CloudFormation.

B. Usar una canalización de AWS CodePipeline para probar y desplegar cargas de trabajo definidas como IaC mediante CloudFormation en las cuentas. Usar reglas de AWS Config para hacer cumplir los requisitos de etiquetado. Aplicar una SCP (Service Control Policy) para evitar la creación de recursos mal configurados en todas las Unidades Organizativas (OUs).

C. Crear un límite de permisos IAM (permissions boundary) para evitar la creación de recursos mal configurados mediante CloudFormation y hacer cumplir los requisitos de etiquetado. Aplicar este límite a todos los roles de las cuentas. Usar AWS Config para identificar recursos existentes que estén mal configurados.

**D. Usar AWS Service Catalogo junto con CloudFormation para gestionar el acceso a configuraciones arquitectónicas aprobadas. Proveer portafolios de Service Catalog a las cuentas dentro de la organización. Usar reglas de AWS Config para hacer cumplir los requisitos de etiquetado y otras políticas de configuración de recursos entre cuentas.**

221.- Una empresa está migrando sus aplicaciones basadas en Amazon EC2 para que usen Instance Metadata Service versión 2 (IMDSv2). Un ingeniero de seguridad necesita determinar si alguna de las instancias EC2 todavía está utilizando la versión 1 (IMDSv1) del servicio de metadatos.

¿Qué debería hacer el ingeniero de seguridad para confirmar que ya no se está usando el endpoint de IMDSv1?

A. Configurar registros en el agente de Amazon CloudWatch para IMDSv1 como parte del inicio de las instancias EC2. Crear un filtro de métricas y un panel en CloudWatch. Rastrear la métrica en el panel.

**B. Crear un panel en Amazon CloudWatch. Verificar que la métrica EC2:MetadataNoToken sea igual a cero en todas las instancias EC2. Monitorear el panel.**

C. Crear un grupo de seguridad que bloquee el acceso HTTP al endpoint de IMDSv1. Asociar este grupo de seguridad a todas las instancias EC2.

D. Configurar scripts de user data para todas las instancias EC2 que envíen información de registros a AWS CloudTrail cuando se use IMDSv1. Crear un filtro de métricas y un panel en Amazon CloudWatch. Rastrear la métrica en el panel.

222.- Una empresa está planificando crear una organización utilizando AWS Organizations. La empresa necesita integrar la gestión de usuarios con el proveedor de identidad externo (IdP) de la compañía. Además, necesita administrar de forma centralizada el acceso a todas sus cuentas de AWS y aplicaciones desde la cuenta de administración de la organización.

¿Qué solución cumplirá con estos requisitos?

A. Configurar AWS Directory Service con el IdP externo. Crear políticas de IAM y asociarlas con los usuarios del IdP externo.

**B. Habilitar AWS IAM Identity Center y usar el IdP externo como fuente de identidad. Crear conjuntos de permisos y asignaciones de cuentas usando IAM Identity Center.**

C. Configurar AWS Identity and Access Management (IAM) para usar el IdP externo como proveedor de identidad. Crear políticas de IAM y asociarlas con usuarios del IdP externo.

D. Habilitar Amazon Cognito en la cuenta de administración de la organización. Crear un pool de identidades y asociarlo con el IdP externo. Crear roles de IAM y asociarlos al pool de identidades.

223.- Una empresa utiliza Amazon Elastic Container Registry (Amazon ECR) como repositorio para sus aplicaciones en producción. Un ingeniero de seguridad debe implementar una solución automatizada que informe sobre cualquier vulnerabilidad detectada por el escaneo mejorado de ECR. La solución debe notificar los hallazgos de vulnerabilidades mediante un mensaje instantáneo en el canal de Slack de la empresa.

¿Cuál solución cumplirá con estos requisitos con la mayor eficiencia operativa?

**A. Activar los escaneos de Amazon Inspector para el repositorio de ECR. Crear un tema de Amazon SNS. Configurar un cliente de AWS Chatbot para Slack que consuma ese tema SNS. Crear una regla de Amazon EventBridge para los hallazgos de Amazon Inspector. Especificar el tema SNS como destino de la regla.**

B. Activar los escaneos de Amazon Inspector para el repositorio de ECR. Escribir un script que utilice comandos de la AWS CLI para obtener los hallazgos de escaneo de Amazon Inspector. Configurar el script para enviar los hallazgos a un endpoint de Slack. Lanzar una instancia EC2 para ejecutar el script.

C. Activar los escaneos de Amazon Inspector para el repositorio de ECR. Crear una máquina de estado de AWS Step Functions. Configurar un primer paso que llame a la operación ListFindings de Amazon Inspector. Crear un tema SNS con Slack como destino. Agregar un segundo paso en la máquina de estado para llamar a la operación Publish de SNS.

D. Activar los escaneos de AWS Security Hub para el repositorio de ECR. Crear una acción personalizada en Security Hub para los hallazgos. Definir una regla de Amazon EventBridge para esta acción. Configurar la regla para redirigir los hallazgos a un canal de Slack.

224.- Una empresa utiliza reglas de AWS Config para identificar buckets de Amazon S3 que no cumplen con la política de protección de datos de la empresa. Los buckets S3 están alojados en varias regiones de AWS y en varias cuentas de AWS. Las cuentas están organizadas dentro de una organización en AWS Organizations.

La empresa necesita una solución para corregir los buckets S3 no conformes ya existentes y también cualquier bucket S3 no conforme que se cree en el futuro.

¿Qué solución cumplirá con estos requisitos?

**A. Implementar un agregador de AWS Config con agregación de datos de recursos a nivel organizacional. Crear una función de AWS Lambda que responda a los hallazgos de AWS Config sobre buckets S3 no conformes, eliminando o reconfigurando dichos buckets.**

B. Implementar un agregador de AWS Config con agregación de datos de recursos a nivel organizacional. Crear una SCP (política de control de servicio) que contenga una instrucción Deny para evitar la creación de nuevos buckets S3 no conformes. Aplicar la SCP a todas las unidades organizativas (OUs) de la organización.

C. Implementar un agregador de AWS Config limitado solo a las cuentas y regiones que la empresa usa actualmente. Crear una función de AWS Lambda que responda a los hallazgos de AWS Config sobre buckets S3 no conformes, eliminando o reconfigurando dichos buckets.

D. Implementar un agregador de AWS Config limitado solo a las cuentas y regiones que la empresa usa actualmente. Crear una SCP que contenga una instrucción Deny para evitar la creación de nuevos buckets S3 no conformes. Aplicar la SCP a todas las OUs de la organización.

225.- El equipo de ingeniería de una empresa está desarrollando una nueva aplicación que crea concesiones (grants) de claves administradas por el cliente en AWS Key Management Service (AWS KMS) para los usuarios. Inmediatamente después de que se crea una concesión, los usuarios deben poder usar la clave KMS para cifrar una carga de 512 bytes. Durante las pruebas de carga, ocasionalmente ocurren errores AccessDeniedException cuando un usuario intenta usar la clave por primera vez para cifrar.

¿Qué solución debería recomendar el especialista en seguridad de la empresa para eliminar estos errores AccessDeniedException?

A. Indicar a los usuarios que implementen un mecanismo de reintento cada 2 minutos hasta que la llamada sea exitosa.

B. Indicar al equipo de ingeniería que reciba un grant token aleatorio de los usuarios y que llame a la operación CreateGrant, pasando ese grant token en la operación. Indicar a los usuarios que usen ese grant token en su llamada para cifrar.

C. Indicar al equipo de ingeniería que cree un nombre aleatorio para la concesión al llamar a la operación CreateGrant. Devolver ese nombre a los usuarios e indicarles que lo proporcionen como grant token en la llamada para cifrar.

**D. Indicar al equipo de ingeniería que pase el grant token devuelto en la respuesta de CreateGrant a los usuarios. Indicar a los usuarios que usen ese grant token en su llamada para cifrar.**

226.- Una empresa aloja su sitio web público en instancias de Amazon EC2 detrás de un Application Load Balancer (ALB). El sitio web está sufriendo un ataque DDoS global proveniente de una marca específica de dispositivos IoT, los cuales tienen un user agent único.

Un ingeniero de seguridad está creando una ACL web de AWS WAF y la asociará al ALB. El ingeniero debe implementar una regla dentro de la ACL que bloquee las solicitudes. La regla debe mitigar tanto el ataque actual como futuros ataques de estos dispositivos IoT, sin bloquear las solicitudes de clientes legítimos.

¿Qué declaración de regla cumplirá con estos requisitos?

A. Usar una regla de coincidencia de conjunto de IPs (IP set match rule) que incluya las direcciones IP de los dispositivos IoT extraídas del user agent.

B. Usar una regla de coincidencia geográfica (geographic match rule). Configurarla para bloquear los países donde se encuentran los dispositivos IoT.

C. Usar una regla basada en tasa (rate-based rule). Establecer un límite de tasa igual al número de solicitudes que provienen de los dispositivos IoT.

**D. Usar una regla de coincidencia de cadenas (string match rule) que incluya detalles de la marca del dispositivo IoT a partir del user agent.**

227.- Una empresa ha configurado un gateway VPC endpoint en una VPC. Solo las instancias de Amazon EC2 que se encuentran en una única subred dentro de la VPC pueden usar este endpoint. La empresa ha modificado la tabla de rutas de esa subred para enrutar el tráfico hacia Amazon S3 a través del gateway VPC endpoint. La VPC también tiene acceso a internet mediante un internet gateway.

Un ingeniero de seguridad intenta usar las credenciales del perfil de instancia desde una instancia EC2 para recuperar un objeto desde un bucket de S3, pero la solicitud falla. El ingeniero verifica que la instancia EC2 tiene un perfil de instancia IAM con los permisos correctos para acceder al bucket y recuperar objetos. También confirma que la política del bucket S3 permite el acceso correctamente. Además, verifica que el grupo de seguridad de la instancia EC2 y las listas de control de acceso a la red (ACLs) de la subred permiten la comunicación.

¿Qué más debería verificar el ingeniero de seguridad para determinar por qué está fallando la solicitud desde la instancia EC2?

A. Verificar que el grupo de seguridad de la instancia EC2 no tenga una regla implícita de denegación de entrada para Amazon S3.

B. Verificar que el grupo de seguridad del endpoint VPC no tenga una regla explícita de denegación de entrada para la instancia EC2.

C. Verificar que el internet gateway esté permitiendo tráfico hacia Amazon S3.

**D. Verificar que la política del endpoint VPC esté permitiendo el acceso a Amazon S3.**

228.- Un administrador de seguridad está restringiendo las capacidades de las cuentas root de la empresa. La empresa utiliza AWS Organizations con todas las funciones habilitadas.

La cuenta de administración se usa para propósitos de facturación y administración, pero no se usa para operaciones con recursos de AWS.

¿Cómo puede el administrador de seguridad restringir el uso de las cuentas root de los miembros de la organización?

A. Desactivar el uso de la cuenta root en la raíz de la organización. Habilitar autenticación multifactor (MFA) para la cuenta root de cada cuenta miembro.

B. Configurar políticas de usuario IAM para restringir las capacidades de la cuenta root en cada cuenta miembro.

**C. Crear una unidad organizativa (OU) en Organizations y adjuntar una SCP (política de control de servicio) que controle el uso de la cuenta root. Agregar todas las cuentas miembro a la nueva OU.**

D. Configurar AWS CloudTrail para integrarse con Amazon CloudWatch Logs. Crear un filtro de métricas para RootAccountUsage.

229.- Una empresa quiere comenzar a procesar datos sensibles en instancias de Amazon EC2. La empresa usará Amazon CloudWatch Logs para monitorear, almacenar y acceder a los archivos de registro de esas instancias EC2.

Los desarrolladores de la empresa usan CloudWatch Logs para la resolución de problemas. Un ingeniero de seguridad debe implementar una solución que impida que los desarrolladores vean los datos sensibles. La solución debe aplicarse automáticamente a cualquier nuevo grupo de logs que se cree en la cuenta en el futuro.

¿Qué solución cumplirá con estos requisitos?

**A. Crear una política de protección de datos a nivel de cuenta para CloudWatch Logs. Especificar los identificadores de datos apropiados en la política. Asegurarse de que los desarrolladores no tengan el permiso IAM logs:Unmask.**

B. Exportar los datos de CloudWatch Logs a un bucket de Amazon S3. Configurar Amazon Macie para hacer descubrimiento automatizado en el bucket. Crear un identificador de datos personalizado para los datos sensibles. Quitar el acceso de los desarrolladores a CloudWatch Logs. Otorgar permisos a los desarrolladores para ver los logs exportados en Amazon S3.

C. Exportar los datos de CloudWatch Logs a un bucket de Amazon S3. Configurar Amazon Macie para hacer descubrimiento automatizado en el bucket. Especificar identificadores de datos administrados apropiados. Quitar el acceso de los desarrolladores a CloudWatch Logs. Otorgar permisos a los desarrolladores para ver los logs exportados en Amazon S3.

D. Crear una política de protección de datos de CloudWatch Logs para cada grupo de logs. Especificar los identificadores de datos apropiados en la política. Asegurarse de que los desarrolladores no tengan el permiso IAM logs:Unmask.

230.- Un ingeniero de seguridad necesita implementar una solución para identificar cualquier dato sensible almacenado en un bucket de Amazon S3. La solución debe generar reportes sobre los datos sensibles encontrados en el bucket de S3 utilizando un tema existente de Amazon SNS (Simple Notification Service).

¿Cuál solución cumplirá con estos requisitos con el menor esfuerzo de implementación?

A. Habilitar AWS Config. Configurar AWS Config para monitorear datos sensibles en el bucket de S3 y enviar notificaciones al tema de SNS.

B. Crear una función de AWS Lambda para escanear el bucket de S3 en busca de datos sensibles que coincidan con un patrón. Programar la función Lambda para que envíe notificaciones al tema de SNS.

**C. Configurar Amazon Macie para usar identificadores de datos administrados que permitan identificar y clasificar datos sensibles. Crear una regla de Amazon EventBridge para enviar notificaciones al tema de SNS.**

D. Habilitar Amazon GuardDuty. Configurar los eventos de datos de S3 en AWS CloudTrail. Crear una alarma de Amazon CloudWatch que reaccione a los hallazgos de GuardDuty y envíe notificaciones al tema de SNS.

231.- Una empresa tiene una aplicación en instancias Amazon EC2 que almacena datos confidenciales de clientes. La empresa debe restringir el acceso a estos datos. Un ingeniero de seguridad necesita acceder de forma segura a las instancias que alojan la aplicación.

De acuerdo con la política de la empresa, los usuarios no deben abrir puertos de entrada, ni mantener hosts bastión, ni gestionar claves SSH para acceder a las instancias EC2.

El ingeniero de seguridad también quiere monitorizar, almacenar y acceder a todos los registros de actividad de las sesiones, y estos registros deben estar cifrados.

¿Qué solución cumplirá con estos requisitos?

A. Usar AWS Control Tower para conectarse a las instancias EC2. Configurar el registro de sesiones en Amazon CloudWatch. Seleccionar la opción para subir los registros de sesión y permitir solo grupos de logs en CloudWatch que estén cifrados.

B. Usar AWS Security Hub para conectarse a las instancias EC2. Configurar el registro de sesiones en Amazon CloudWatch. Seleccionar la opción para subir los registros de sesión y permitir solo grupos de logs en CloudWatch que estén cifrados.

C. Usar AWS Systems Manager Session Manager para conectarse a las instancias EC2. Configurar la monitorización en Amazon CloudWatch para grabar las sesiones. Seleccionar la opción de almacenar los registros de sesión en los grupos de logs de CloudWatch deseados.

**D. Usar AWS Systems Manager Session Manager para conectarse a las instancias EC2. Configurar el registro en Amazon CloudWatch. Seleccionar la opción para subir los registros de sesión y permitir solo grupos de logs cifrados en CloudWatch Logs.**

232.- Una empresa utiliza una organización en AWS Organizations para ayudar a separar sus instancias de Amazon EC2 y sus VPCs. La empresa tiene unidades organizativas (OUs) separadas para cargas de trabajo de desarrollo y de producción.

Un ingeniero de seguridad debe asegurarse de que solo las cuentas de AWS que están en la OU de producción puedan escribir los VPC Flow Logs en un bucket de Amazon S3. El ingeniero está configurando la política del bucket S3 con un elemento Condition para permitir la acción s3:PutObject para los VPC Flow Logs.

¿Cómo debe el ingeniero de seguridad configurar el elemento Condition para cumplir con estos requisitos?

A. Establecer el valor de la clave de condición aws:SourceOrgID como el ID de la organización.

**B. Establecer el valor de la clave de condición aws:SourceOrgPaths como la ruta de entidad de AWS Organizations de la OU de producción.**

C. Establecer el valor de la clave de condición aws:ResourceOrgID como el ID de la organización.

D. Establecer el valor de la clave de condición aws:ResourceOrgPaths como la ruta de entidad de AWS Organizations de la OU de producción.

233.- El agente de Amazon CloudWatch Logs está entregando correctamente los registros al servicio de CloudWatch Logs. Sin embargo, los registros dejan de enviarse después de que el flujo de logs ha estado activo durante un número específico de horas.

¿Qué pasos son necesarios para identificar la causa de este comportamiento? (Elige dos opciones).

**A. Asegurarse de que los permisos de los archivos monitoreados no hayan sido modificados, y que permitan al agente de CloudWatch Logs leer dichos archivos.**

**B. Verificar que las reglas de rotación de logs del sistema operativo sean compatibles con los requisitos de configuración del agente para transmisión continua.**

C. Configurar un productor de Amazon Kinesis para enviar primero los logs a Amazon Kinesis Streams.

D. Crear una métrica de CloudWatch Logs para aislar un valor que cambie al menos una vez durante el periodo anterior a que se detenga el envío de logs.

E. Usar AWS CloudFormation para crear y mantener dinámicamente el archivo de configuración del agente de CloudWatch Logs.

234.- Un ingeniero de seguridad ha diseñado una VPC para separar el tráfico privado del tráfico público. La VPC incluye dos zonas de disponibilidad. El ingeniero de seguridad ha aprovisionado cada zona de disponibilidad con una subred privada y una subred pública. Ha creado tres tablas de rutas para el entorno: una para las subredes públicas y dos para las subredes privadas (una por cada subred privada en cada zona de disponibilidad).

El ingeniero descubre que las cuatro subredes están intentando enrutar el tráfico a través del internet gateway que está adjunto a la VPC.

¿Qué combinación de pasos debe seguir el ingeniero de seguridad para corregir esta situación? (Elige dos opciones).

**A. Verificar que se ha aprovisionado un NAT gateway en la subred pública de cada zona de disponibilidad.**

B. Verificar que se ha aprovisionado un NAT gateway en la subred privada de cada zona de disponibilidad.

C. Modificar las tablas de rutas asociadas a cada subred pública. Crear una nueva ruta para destinos locales con el rango CIDR de la VPC.

**D. Modificar las tablas de rutas asociadas a cada subred privada. Crear una nueva ruta para el destino 0.0.0.0/0. Especificar el NAT gateway en la subred pública de la misma zona de disponibilidad como el destino de la ruta.**

E. Modificar las tablas de rutas asociadas a cada subred privada. Crear una nueva ruta para el destino 0.0.0.0/0. Especificar el internet gateway en la subred pública de la misma zona de disponibilidad como el destino de la ruta.

235.- Una empresa contrató a un consultor externo que necesita usar su laptop para acceder a las VPC de la empresa. Específicamente, el consultor necesita acceso a dos VPC que están conectadas por peering en la misma región de AWS. La empresa quiere otorgarle acceso solo a esas VPC, sin darle acceso innecesario a otros recursos de red.

¿Qué solución cumplirá con estos requisitos?

A. Crear un endpoint de AWS Site-to-Site VPN en la misma región que las VPC. Configurar el acceso mediante una subred y regla de autorización adecuadas.

B. Crear una cuenta de AWS. Usar la función de VPC sharing mediante AWS Resource Access Manager para permitir que el consultor acceda a las VPC.

**C. Crear un endpoint de AWS Client VPN en la misma región que las VPC. Configurar el acceso mediante una subred y regla de autorización adecuadas.**

D. Crear un endpoint de gateway VPC en la misma región que las VPC. Configurar el acceso mediante una subred y regla de autorización adecuadas.

236.- Una empresa utiliza AWS Organizations para gestionar una pequeña cantidad de cuentas de AWS. Sin embargo, planea agregar 1.000 cuentas más próximamente. La empresa permite que solo el equipo central de seguridad cree roles IAM para todas las cuentas y equipos. Los equipos de aplicaciones deben enviar solicitudes de creación de roles IAM al equipo de seguridad. Actualmente, el equipo de seguridad tiene un atraso de solicitudes y no puede revisarlas ni aprovisionar los roles con rapidez.

El equipo de seguridad debe crear un proceso que permita que los equipos de aplicaciones puedan aprovisionar sus propios roles IAM, pero que también limite el alcance de esos roles y evite la escalada de privilegios.

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

A. Crear un grupo de IAM para cada equipo de aplicación. Asociar políticas a cada grupo. Aprovisionar usuarios IAM para cada miembro del equipo de aplicación. Agregar los usuarios IAM al grupo correspondiente utilizando control de acceso basado en roles (RBAC).

B. Delegar en los líderes de equipo de las aplicaciones la capacidad de aprovisionar roles IAM para sus equipos. Realizar una revisión trimestral de los roles que hayan sido creados. Asegurarse de que los líderes de equipo hayan recibido la capacitación adecuada para revisar roles IAM.

C. Colocar cada cuenta de AWS en su propia unidad organizativa (OU). Agregar una SCP (política de control de servicios) a cada OU para permitir acceso solo a los servicios de AWS que los equipos necesiten usar. Incluir condiciones específicas en cada cuenta de equipo.

**D. Crear una SCP y una permisos boundary (límite de permisos) para los roles IAM. Agregar la SCP a la unidad organizativa raíz (root OU) para que solo se puedan crear nuevos roles IAM si tienen el límite de permisos adjunto.**

237.- Un desarrollador está recibiendo errores AccessDenied al ejecutar llamadas a la API de servicios de AWS desde su estación de trabajo. Anteriormente, el desarrollador configuró variables de entorno y archivos de configuración en la estación de trabajo para usar múltiples roles con otras cuentas de AWS.

Un ingeniero de seguridad necesita ayudar al desarrollador a configurar la autenticación. Se deben evaluar las credenciales actuales sin entrar en conflicto con otras credenciales que ya fueron configuradas en la estación de trabajo.

¿Dónde se deben configurar estas credenciales para cumplir con este requisito?

A. En el archivo de configuración local de AWS CLI

B. Como variables de entorno en la estación de trabajo local

**C. Como variables en las opciones de línea de comandos de AWS CLI**

D. En el archivo de configuración compartido de AWS

238.- Una empresa del sector médico recientemente completó una adquisición y heredó un entorno existente en AWS. La empresa tiene una auditoría próxima y está preocupada por el estado de cumplimiento normativo del entorno adquirido.

La empresa debe identificar información personal de salud (PHI) dentro de los buckets de Amazon S3 y también debe identificar los buckets S3 que sean accesibles públicamente. Necesitan prepararse para la auditoría recopilando evidencia dentro del entorno.

¿Qué combinación de pasos cumplirá con estos requisitos con el MENOR esfuerzo operativo? (Elige tres opciones)

**A. Habilitar Amazon Macie. Ejecutar un análisis bajo demanda de datos sensibles utilizando el identificador de datos administrado PERSONAL\_INFORMATION.**

B. Usar AWS Glue con la transformación Detect PII para identificar datos sensibles y enmascararlos.

**C. Habilitar AWS Audit Manager. Crear una evaluación utilizando un marco de cumplimiento compatible.**

D. Habilitar Amazon GuardDuty con protección para S3. Documentar cualquier hallazgo relacionado con accesos sospechosos a buckets S3.

**E. Habilitar AWS Security Hub. Usar el estándar AWS Foundational Security Best Practices. Revisar el panel de controles para obtener evidencia de errores en los controles de S3 Block Public Access.**

F. Habilitar AWS Config. Configurar la regla administrada s3-bucket-public-write-prohibited de AWS Config.

239.- Una empresa detecta que una de sus instancias de Amazon EC2 presenta repentinamente un uso elevado de CPU. La empresa no sabe si la instancia fue comprometida o si el sistema operativo está ejecutando tareas de limpieza en segundo plano.

¿Qué combinación de pasos debe realizar un ingeniero de seguridad antes de comenzar a investigar el problema? (Elige tres opciones).

A. Desactivar la protección contra terminación de la instancia EC2 si no ha sido desactivada.

**B. Activar la protección contra terminación de la instancia EC2 si no ha sido activada.**

**C. Tomar snapshots (copias de seguridad) de los volúmenes de datos de Amazon EBS que están adjuntos a la instancia EC2.**

D. Eliminar todos los snapshots de los volúmenes de datos de Amazon EBS que están adjuntos a la instancia EC2.

**E. Capturar los metadatos de la instancia EC2 y luego etiquetar la instancia como en cuarentena.**

F. Eliminar inmediatamente cualquier entrada en los metadatos de la instancia EC2 que contenga información sensible.

240.- Una empresa está implementando una solución personalizada de notificaciones para detectar intentos repetidos no autorizados de autenticación en bastion hosts. El ingeniero de seguridad de la empresa necesita implementar una solución que envíe una notificación cuando ocurran 5 intentos fallidos en un período de 5 minutos. La solución debe usar servicios nativos de AWS y notificar solo al administrador del sistema asignado al bastion host específico.

¿Qué solución cumplirá con estos requisitos?

A. Usar el agente de Amazon CloudWatch para recolectar los registros del sistema operativo. Usar Amazon EventBridge para configurar una alarma basada en un filtro de métricas para intentos fallidos de inicio de sesión. Enviar una alerta a Amazon SNS (Simple Notification Service) cuando se supere el umbral definido. Usar etiquetas (tags) de las instancias EC2 para determinar qué temas de SNS reciben las notificaciones.

B. Usar el agente de AWS Systems Manager para recolectar los registros del sistema operativo. Usar el documento AWS-ConfigureCloudWatch del comando Run Command de Systems Manager para configurar un evento de Amazon EventBridge basado en un filtro de métricas para intentos fallidos de inicio de sesión. Enviar una alerta a Amazon SNS cuando se supere el umbral definido. Usar filtros de mensajes de SNS para controlar quién recibe las notificaciones.

**C. Usar el agente de Amazon CloudWatch para recolectar los registros del sistema operativo. Crear una alarma de CloudWatch basada en un filtro de métricas para intentos fallidos de inicio de sesión. Enviar una alerta a Amazon SNS cuando se supere el umbral definido. Usar filtros de mensajes de SNS para controlar quién recibe las notificaciones.**

D. Usar el agente de AWS Systems Manager para recolectar los registros del sistema operativo. Usar el documento AWS-ConfigureCloudWatch del comando Run Command de Systems Manager para configurar una alarma de Amazon CloudWatch basada en un filtro de métricas para intentos fallidos de inicio de sesión. Enviar una alerta a Amazon SNS cuando se supere el umbral definido. Usar etiquetas de instancias EC2 para determinar qué temas de SNS reciben las notificaciones.

241.- Un sitio web de comercio electrónico estuvo inactivo durante una hora debido a un ataque DDoS. Los usuarios no pudieron conectarse al sitio web durante ese período. El equipo de seguridad de la empresa está preocupado por posibles ataques futuros y quiere estar preparado para estos eventos. La empresa necesita minimizar el tiempo de inactividad en su respuesta ante ataques similares en el futuro.

¿Qué pasos ayudarían a lograr esto? (Elige dos opciones).

A. Activar Amazon GuardDuty para monitorear automáticamente la actividad maliciosa y bloquear accesos no autorizados.

**B. Suscribirse a AWS Shield Advanced y contactar al soporte de AWS en caso de un ataque.**

C. Usar VPC Flow Logs para monitorear el tráfico de red y una función AWS Lambda para bloquear automáticamente la IP del atacante mediante grupos de seguridad.

D. Configurar una regla de Amazon EventBridge para monitorear en tiempo real los eventos de AWS CloudTrail, usar reglas de AWS Config para auditar la configuración y utilizar AWS Systems Manager para la remediación.

**E. Usar AWS WAF para crear reglas que respondan a este tipo de ataques.**

242.- Una cuenta de AWS tiene dos buckets de S3: bucket1 y bucket2. El bucket2 no tiene ninguna política definida, pero el bucket1 tiene la siguiente política de bucket:

Además, esta misma cuenta tiene un usuario IAM llamado “alice”, con la siguiente política IAM:

¿A qué buckets puede acceder el usuario “alice”?

A. Solo a bucket1

B. Solo a bucket2

**C. A ambos: bucket1 y bucket2**

D. A ninguno de los dos: ni bucket1 ni bucket2

243.- Una empresa planea crear buckets de Amazon S3 para almacenar datos de registros (logs). Todos los buckets tendrán habilitado el versionado y utilizarán la clase de almacenamiento S3 Standard.

Un ingeniero de seguridad necesita implementar una solución que proteja los objetos en los buckets S3 contra eliminación durante 90 días. La solución debe garantizar que ningún objeto pueda ser eliminado durante ese periodo, ni siquiera por un administrador o el usuario raíz de la cuenta de AWS.

¿Qué solución cumplirá con estos requisitos?

A. Habilitar S3 Object Lock en modo governance. Establecer una retención legal (legal hold) de 90 días.

B. Habilitar S3 Object Lock en modo governance. Establecer un período de retención de 90 días.

**C. Habilitar S3 Object Lock en modo compliance. Establecer un período de retención de 90 días.**

D. Crear una política de S3 Glacier Vault Lock que impida la eliminación durante 90 días.

244.- Una empresa ha utilizado funciones de AWS Lambda para construir una aplicación en AWS. El ingeniero de seguridad de la empresa implementó Amazon Inspector y activó el escaneo estándar de Lambda y el escaneo de código de Lambda.

El ingeniero de seguridad revisa la consola de Amazon Inspector y descubre que Amazon Inspector no está escaneando algunas funciones Lambda. El motivo proporcionado es que la elegibilidad para el escaneo expiró.

¿Qué debe hacer el ingeniero de seguridad para investigar la razón por la cual los escaneos están fallando?

A. Validar que la política administrada por AWS llamada AmazonInspector2ServiceRolePolicy otorgue permisos para acceder a Lambda.

B. Aumentar el valor del tiempo de espera (timeout) de las funciones Lambda para que los escaneos se completen exitosamente mientras se ejecuta el código.

C. Construir un runtime personalizado para las funciones Lambda no escaneadas e incluir el agente de Amazon Inspector en el runtime.

**D. Determinar si las funciones Lambda no escaneadas han sido invocadas en los últimos 90 días.**

245.- Un ingeniero de seguridad recibió una alerta de Amazon GuardDuty que indica un hallazgo relacionado con la instancia de Amazon EC2 que aloja el sitio web principal de la empresa. El hallazgo de GuardDuty dice:

UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.

El ingeniero de seguridad confirmó que un actor malicioso utilizó claves de acceso a la API destinadas para la instancia EC2 desde un país en el que la empresa no opera. El ingeniero necesita negar el acceso al actor malicioso.

¿Cuál es el primer paso que debe tomar el ingeniero de seguridad?

A. Abrir la consola de EC2 y eliminar cualquier grupo de seguridad que permita tráfico entrante desde 0.0.0.0/0.

B. Instalar el agente de AWS Systems Manager en la instancia EC2 y ejecutar un informe de inventario.

C. Instalar el agente de Amazon Inspector en el host y ejecutar una evaluación con el paquete de reglas CVE.

**D. Abrir la consola de IAM y revocar todas las sesiones IAM asociadas con el perfil de instancia.**

246.- Una empresa está probando procedimientos de respuesta ante incidentes para confinar destinos comprometidos. La empresa necesita confinar una instancia crítica de Amazon EC2 lo más rápido posible, manteniéndola en ejecución.

La instancia EC2 es el único recurso en una subred pública y tiene conexiones activas con otros recursos.

¿Qué solución permitirá confinar la instancia EC2 de forma INMEDIATA?

A. Crear un nuevo grupo de seguridad sin reglas de entrada ni de salida. Asociar ese nuevo grupo de seguridad a la instancia EC2.

B. Configurar el grupo de seguridad existente de la instancia EC2. Eliminar todas las reglas de entrada y salida del grupo de seguridad.

**C. Crear una nueva ACL de red con una única regla Deny para el tráfico de entrada y salida. Asociar la nueva ACL de red a la subred que contiene la instancia EC2.**

D. Crear una nueva VPC para aislamiento. Detener la instancia EC2. Crear una nueva AMI desde esa instancia. Usar la AMI para lanzar una nueva instancia EC2 en la nueva VPC.

247.- Una empresa necesita usar HTTPS al conectarse a sus aplicaciones web para cumplir con los requisitos de cumplimiento. Estas aplicaciones web se ejecutan en una Amazon VPC, en instancias de Amazon EC2 que están detrás de un Application Load Balancer (ALB). Un ingeniero de seguridad quiere asegurarse de que el load balancer solo acepte conexiones por el puerto 443, incluso si por error se configura un listener HTTP en el ALB.

¿Qué pasos de configuración debe seguir el ingeniero de seguridad para lograr este objetivo?

A. Crear un grupo de seguridad con una regla que deniegue las conexiones entrantes desde 0.0.0.0/0 en el puerto 80. Asociar este grupo de seguridad al ALB para sobrescribir reglas más permisivas del grupo de seguridad predeterminado del ALB.

B. Crear una ACL de red (network ACL) que deniegue conexiones entrantes desde 0.0.0.0/0 en el puerto 80. Asociar la ACL de red con el internet gateway de la VPC.

C. Crear una ACL de red que permita conexiones salientes solo hacia el rango de IPs de la VPC en el puerto 443. Asociar esta ACL de red con el internet gateway de la VPC.

**D. Crear un grupo de seguridad con una única regla de entrada que permita conexiones desde 0.0.0.0/0 en el puerto 443. Asegurarse de que este grupo de seguridad sea el único asociado al ALB.**

248.- Una agencia de consultoría necesita realizar una auditoría de seguridad en la cuenta de producción de AWS de una empresa. Varios consultores necesitan acceso a dicha cuenta. La agencia de consultoría ya tiene su propia cuenta de AWS.

La empresa requiere que todo acceso a la cuenta de producción use autenticación multifactor (MFA) y prohíbe el uso de credenciales de largo plazo.

¿Qué solución permitirá que la agencia de consultoría acceda cumpliendo con estos requisitos?

A. Crear un grupo de IAM. Crear un usuario IAM para cada consultor. Agregar cada usuario al grupo. Activar MFA para cada consultor.

B. Configurar Amazon Cognito en la cuenta de producción de la empresa para autenticar contra el proveedor de identidad (IdP) de la agencia de consultoría. Agregar MFA a un user pool de Cognito.

C. Crear un rol de IAM en la cuenta de AWS de la agencia de consultoría. Definir una política de confianza que requiera MFA. En la política de confianza, especificar la cuenta de producción de la empresa como principal. Asociar la política de confianza al rol.

**D. Crear un rol de IAM en la cuenta de producción de la empresa. Definir una política de confianza que requiera MFA. En la política de confianza, especificar la cuenta de AWS de la agencia de consultoría como principal. Asociar la política de confianza al rol.**

249.- Una empresa utiliza funciones de AWS Lambda para implementar la lógica de su aplicación. La empresa gestiona cientos de cuentas de AWS mediante una organización en AWS Organizations.

La empresa necesita implementar una solución para monitorear continuamente las funciones Lambda en busca de vulnerabilidades en todas las cuentas. La solución debe publicar los problemas detectados en un panel (dashboard). Las funciones Lambda que estén en fase de pruebas o desarrollo no deben aparecer en el panel.

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

A. Designar una cuenta administradora delegada de Amazon GuardDuty desde la cuenta principal de la organización. Usar el panel de resumen de GuardDuty para obtener una vista general de las funciones Lambda con vulnerabilidades.

**B. Designar una cuenta administradora delegada de Amazon Inspector desde la cuenta principal de la organización. Usar el panel de Amazon Inspector para obtener una vista general de las funciones Lambda con vulnerabilidades.**

**C. Aplicar etiquetas como "test" o "development" a todas las funciones Lambda que estén en prueba o desarrollo. Usar un filtro de supresión para ocultar los hallazgos que contengan estas etiquetas.**

D. Habilitar AWS Shield Advanced en la cuenta principal de la organización. Usar Amazon CloudWatch para construir un panel que muestre las funciones Lambda con vulnerabilidades.

E. Habilitar la Protección Lambda en GuardDuty para todas las cuentas. Activar automáticamente la Protección Lambda para cuentas nuevas. Aplicar una etiqueta a las funciones Lambda que estén en prueba o desarrollo, usando como clave GuardDutyExclusion y como valor LambdaStandardScanning.

250.- Una empresa tiene una organización en AWS Organizations que incluye cuentas dedicadas para cada una de sus unidades de negocio. La empresa está recolectando todos los logs de AWS CloudTrail de las cuentas en un único bucket de Amazon S3 ubicado en la cuenta principal (top-level). El equipo de gobernanza de TI tiene acceso a esta cuenta principal. Un ingeniero de seguridad necesita permitir que cada unidad de negocio acceda a sus propios logs de CloudTrail.

El ingeniero de seguridad crea un rol de IAM en la cuenta principal para cada una de las otras cuentas. Para cada rol, crea una política de IAM que otorga permisos de solo lectura a los objetos en el bucket de S3 con el prefijo correspondiente a los logs de esa unidad.

¿Qué acción debe tomar el ingeniero de seguridad en cada cuenta de unidad de negocio para permitir que un usuario IAM en esa cuenta pueda leer los logs?

**A. Adjuntar una política al usuario IAM que permita al usuario asumir el rol que fue creado en la cuenta principal. Especificar el ARN del rol en la política.**

B. Crear una SCP (política de control de servicio) que otorgue permisos a la cuenta principal.

C. Usar la cuenta raíz de la unidad de negocio para asumir el rol creado en la cuenta principal. Especificar el ARN del rol en la política.

D. Reenviar las credenciales del rol IAM de la cuenta principal al usuario IAM de la unidad de negocio.

251.- Una empresa ha configurado una organización en AWS Organizations para sus cuentas de AWS. AWS CloudTrail está habilitado en todas las regiones de AWS.

Un ingeniero de seguridad debe implementar una solución para evitar que CloudTrail sea deshabilitado.

¿Qué solución cumplirá con este requisito?

A. Habilitar la validación de integridad de archivos de registro de CloudTrail desde la cuenta de administración de la organización.

B. Habilitar el cifrado del lado del servidor con claves KMS (SSE-KMS) para los logs de CloudTrail. Crear una clave KMS y adjuntar una política a la clave para evitar que los logs sean descifrados.

**C. Crear una SCP (Service Control Policy) que incluya una regla explícita Deny para las acciones StopLogging y DeleteTrail. Adjuntar esta SCP a la unidad organizativa raíz (root OU).**

D. Crear políticas IAM para todos los usuarios de la empresa para evitar que ejecuten las acciones DescribeTrails y GetTrailStatus.

252.- Una empresa ejecuta su arquitectura de microservicios en contenedores Kubernetes en AWS, utilizando Amazon Elastic Kubernetes Service (Amazon EKS) y Amazon Aurora. La empresa tiene una organización en AWS Organizations para gestionar cientos de cuentas de AWS que alojan distintos microservicios.

La empresa necesita implementar una solución de monitoreo de logs para todos los recursos de AWS en todas las cuentas. La solución debe incluir detección automática de problemas relacionados con la seguridad.

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

**A. Designar una cuenta administradora de Amazon GuardDuty en la cuenta de administración de la organización. Habilitar GuardDuty en todas las cuentas. Activar la protección de EKS y la protección de RDS en la cuenta administradora de GuardDuty.**

B. Designar una cuenta de monitoreo. Compartir los logs de Amazon CloudWatch desde todas las cuentas con esa cuenta de monitoreo. Configurar Aurora para que publique todos los logs en CloudWatch. Usar Amazon Inspector en la cuenta de monitoreo para evaluar los logs de CloudWatch.

C. Crear un bucket central de Amazon S3 en la cuenta de administración de la organización. Configurar AWS CloudTrail en todas las cuentas de AWS para que envíen los registros a ese bucket. Configurar Aurora para que publique todos sus logs en CloudTrail. Usar Amazon Athena para consultar los registros en el bucket de S3 en busca de problemas de seguridad.

D. Designar una cuenta de monitoreo. Compartir los logs de Amazon CloudWatch desde todas las cuentas con esa cuenta. Suscribir un flujo de datos de Amazon Kinesis a los logs de CloudWatch. Crear funciones de AWS Lambda para procesar los registros del flujo y detectar problemas de seguridad.

253.- Un ingeniero de seguridad ha sido asignado para solucionar problemas de conectividad entrante a un servidor web. Este único servidor web no está recibiendo conexiones desde Internet, mientras que los demás servidores web están funcionando correctamente.

La arquitectura incluye listas de control de acceso a la red (network ACLs), grupos de seguridad (security groups) y un dispositivo de seguridad virtual. Además, el equipo de desarrollo ha implementado Application Load Balancers (ALB) para distribuir la carga entre todos los servidores web. Es un requisito que el tráfico entre los servidores web e Internet pase por el dispositivo de seguridad virtual.

El ingeniero de seguridad ha verificado lo siguiente:

Las reglas de los grupos de seguridad están correctas.

Las reglas de las network ACLs están correctas.

Las reglas del dispositivo de seguridad virtual están correctas.

¿Cuáles de los siguientes son otros elementos válidos que deberían revisarse en esta situación? (Elige dos opciones).

A. Verificar que la ruta 0.0.0.0/0 en la tabla de ruteo de la subred del servidor web apunte a un NAT Gateway.

B. Verificar qué grupo de seguridad está aplicado a la interfaz de red elástica (ENI) del servidor web en particular.

**C. Verificar que la ruta 0.0.0.0/0 en la tabla de ruteo de la subred del servidor web apunte al dispositivo de seguridad virtual.**

**D. Verificar los targets registrados en el ALB.**

E. Verificar que la ruta 0.0.0.0/0 en la subred pública apunte a un NAT Gateway.

254.- Una empresa tiene una política estricta que prohíbe el uso de las credenciales de root. El equipo de seguridad de la empresa quiere recibir una alerta lo antes posible cuando se utilicen las credenciales de root para iniciar sesión en la consola de administración de AWS.

¿Cómo debe actuar el equipo de seguridad para lograr este objetivo?

A. Usar AWS Lambda para consultar periódicamente AWS CloudTrail en busca de eventos de inicio de sesión en la consola y enviar alertas mediante Amazon Simple Notification Service (Amazon SNS).

**B. Usar Amazon EventBridge para monitorear los inicios de sesión en la consola y redirigirlos a Amazon Simple Notification Service (Amazon SNS).**

C. Usar Amazon Athena para consultar los registros de AWS IAM Identity Center y enviar alertas mediante Amazon SNS para eventos de inicio de sesión como root.

D. Configurar AWS Resource Access Manager para revisar los registros de acceso y enviar alertas mediante Amazon SNS.

255.- Una empresa quiere almacenar todos los objetos que contienen datos sensibles en un bucket de Amazon S3. La empresa usará cifrado del lado del servidor para cifrar el bucket de S3.

El equipo de operaciones de la empresa administra el acceso a los buckets de S3.

El equipo de seguridad administra el acceso a las claves de cifrado.

La empresa quiere separar las funciones de ambos equipos para asegurarse de que un error de configuración por parte de uno solo de los equipos no comprometa los datos otorgando acceso no autorizado a los datos en texto plano.

¿Qué solución cumplirá con este requisito?

A. Asegurar que el equipo de operaciones configure el cifrado predeterminado del bucket usando cifrado del lado del servidor con claves administradas por Amazon S3 (SSE-S3). Asegurar que el equipo de seguridad cree una política IAM que controle el acceso para usar las claves de cifrado.

**B. Asegurar que el equipo de operaciones cree una política de bucket que exija el uso de cifrado del lado del servidor con claves KMS (SSE-KMS) administradas por el cliente. Asegurar que el equipo de seguridad cree una política de claves que controle el acceso a dichas claves.**

C. Asegurar que el equipo de operaciones cree una política de bucket que exija el uso de cifrado del lado del servidor con claves administradas por Amazon S3 (SSE-S3). Asegurar que el equipo de seguridad cree una política IAM que controle el acceso a las claves de cifrado.

D. Asegurar que el equipo de operaciones cree una política de bucket que exija el uso de cifrado del lado del servidor con claves proporcionadas por el cliente (SSE-C). Asegurar que el equipo de seguridad almacene esas claves en AWS Key Management Service (AWS KMS). Asegurar que el equipo de seguridad cree una política de clave que controle el acceso a dichas claves.

256.- Un ingeniero de seguridad está diseñando controles de seguridad para un grupo de instancias de Amazon EC2 que ejecutan cargas de trabajo sensibles dentro de una VPC. El ingeniero necesita implementar una solución para detectar y mitigar vulnerabilidades de software en dichas instancias EC2.

¿Qué solución cumplirá con este requisito?

**A. Escanear las instancias EC2 usando Amazon Inspector. Aplicar parches de seguridad y actualizaciones mediante AWS Systems Manager Patch Manager.**

B. Instalar un firewall basado en host y software antivirus en cada instancia EC2. Usar AWS Systems Manager Run Command para actualizar el firewall y el antivirus.

C. Instalar el agente de Amazon CloudWatch en las instancias EC2. Habilitar el registro detallado (detailed logging). Usar Amazon EventBridge para revisar los registros de software en busca de anomalías.

D. Escanear las instancias EC2 usando Amazon GuardDuty Malware Protection. Aplicar parches de seguridad y actualizaciones mediante AWS Systems Manager Patch Manager.

257.- Una empresa almacena datos sensibles en AWS Secrets Manager. Un ingeniero de seguridad necesita diseñar una solución que genere una notificación por correo electrónico cuando ocurran llamadas anómalas a la API GetSecretValue. El ingeniero ya ha configurado una regla de Amazon EventBridge para todos los eventos de Secrets Manager que AWS CloudTrail entrega.

¿Qué solución cumplirá con estos requisitos?

A. Configurar CloudTrail como destino de la regla de EventBridge. Establecer un filtro de atributos sobre IncomingBytes y habilitar la detección de anomalías. Crear un tema de Amazon SNS. Configurar una alarma en CloudTrail que use el tema de SNS para enviar la notificación.

B. Configurar CloudTrail como destino de la regla de EventBridge. Establecer un filtro de atributos sobre IncomingBytes y habilitar la detección de anomalías. Crear una cola de Amazon SQS. Configurar una alarma en CloudTrail que use la cola de SQS para enviar la notificación.

**C. Configurar Amazon CloudWatch Logs como destino de la regla de EventBridge. Establecer un filtro de métricas sobre la métrica IncomingBytes y habilitar la detección de anomalías. Crear un tema de Amazon SNS. Configurar una alarma de CloudWatch que use ese tema de SNS para enviar la notificación.**

D. Configurar Amazon CloudWatch Logs como destino de la regla de EventBridge. Usar CloudWatch Logs Insights con sintaxis de consulta para buscar llamadas anómalas a la API GetSecretValue. Crear una cola de Amazon SQS. Configurar una alarma de CloudWatch que use la cola de SQS para enviar la notificación.

258.- Una empresa está utilizando AWS Organizations con la política de control de servicio (SCP) predeterminada. La empresa necesita restringir el uso de AWS para todas las cuentas que se encuentran en una unidad organizativa (OU) específica.

Excepto por algunos servicios globales permitidos, el uso de AWS debe ocurrir únicamente en la Región eu-west-1 para todas las cuentas dentro de esa OU. Un ingeniero de seguridad debe crear una SCP que aplique esta restricción tanto a las cuentas existentes como a las nuevas que se agreguen a la OU.

¿Qué SCP cumplirá con estos requisitos?

A.

B.

**C.**

D.

259.- Una empresa está planificando migrar sus aplicaciones a AWS en una sola región de AWS. Las aplicaciones de la empresa usarán una combinación de instancias Amazon EC2, balanceadores de carga de Elastic Load Balancing (ELB) y buckets de Amazon S3. La empresa desea completar la migración lo más rápido posible. Todas las aplicaciones deben cumplir con los siguientes requisitos:

Los datos deben estar cifrados en reposo.

Los datos deben estar cifrados en tránsito.

Los endpoints deben ser monitorizados ante tráfico de red anómalo.

¿Qué combinación de pasos debe tomar un ingeniero de seguridad para cumplir con estos requisitos con el menor esfuerzo posible? (Elige tres opciones):

A. Instalar el agente de Amazon Inspector en las instancias EC2 usando AWS Systems Manager Automation.

**B. Habilitar Amazon GuardDuty en todas las cuentas de AWS.**

C. Crear endpoints de VPC para Amazon EC2 y Amazon S3. Actualizar las tablas de rutas de la VPC para usar solo los endpoints seguros.

**D. Configurar AWS Certificate Manager (ACM). Configurar los balanceadores de carga para usar certificados de ACM.**

E. Usar AWS Key Management Service (AWS KMS) para la gestión de claves. Crear una política de bucket S3 que deniegue cualquier comando PutObject con una condición basada en x-amz-meta-side-encryption.

**F. Usar AWS Key Management Service (AWS KMS) para la gestión de claves. Crear una política de bucket S3 que deniegue cualquier comando PutObject que no incluya la condición x-amz-server-side-encryption.**

260.- Un ingeniero de seguridad está trabajando con un equipo de desarrollo para diseñar una aplicación de cadena de suministro que almacene datos sensibles de inventario en un bucket de Amazon S3. La aplicación utilizará una clave administrada por el cliente en AWS Key Management Service (AWS KMS) para cifrar los datos en S3.

Los datos de inventario en S3 se compartirán con cientos de proveedores, quienes usarán principales de AWS desde sus propias cuentas para acceder a los datos en S3. La lista de proveedores puede cambiar semanalmente. El ingeniero de seguridad necesita encontrar una solución que permita el acceso entre cuentas (cross-account).

¿Cuál es la forma más eficiente operativamente de gestionar el control de acceso a la clave administrada por el cliente?

**A. Usar concesiones de KMS para gestionar el acceso a la clave. Crear y revocar las concesiones de forma programada para controlar el acceso de los proveedores.**

B. Usar un rol de IAM para gestionar el acceso a la clave. Actualizar programáticamente las políticas del rol IAM para gestionar el acceso de los proveedores.

C. Usar políticas de claves KMS (key policies) para gestionar el acceso a la clave. Actualizar programáticamente las políticas de la clave KMS para gestionar el acceso de los proveedores.

D. Usar acceso delegado entre cuentas de AWS mediante roles IAM para gestionar el acceso a la clave. Actualizar programáticamente la política de confianza (trust policy) del rol para gestionar el acceso entre cuentas de los proveedores.

261.- Una empresa ejecuta una aplicación en un conjunto de instancias Amazon EC2 detrás de un Application Load Balancer (ALB). Un ingeniero de seguridad necesita proporcionar acceso seguro a la aplicación sin requerir el uso de una VPN.

Los usuarios deben poder acceder a la aplicación solo si cumplen ciertas condiciones de seguridad, incluyendo una postura de dispositivo específica (es decir, que el dispositivo cumpla ciertos requisitos de seguridad).

¿Qué solución cumplirá con estos requisitos?

A. Crear una ACL web de AWS WAF. Configurar una respuesta personalizada para bloquear el tráfico que no cumpla con la postura de dispositivo definida.

**B. Configurar AWS Verified Access. Agregar la aplicación creando un endpoint para el ALB.**

C. Configurar Amazon Verified Permissions. Usar una política PBAC (control de acceso basado en políticas) para realizar la autorización.

D. Configurar Amazon Verified Permissions. Agregar la aplicación creando un endpoint para el ALB.

262.- Una empresa necesita conservar los datos almacenados en los grupos de logs de Amazon CloudWatch Logs. La empresa debe retener estos datos durante 90 días. Además, debe recibir una notificación en AWS Security Hub cuando el período de retención de un grupo de logs no cumpla con este requisito.

¿Qué solución proporcionará la notificación adecuada?

A. Crear una acción personalizada en Security Hub para evaluar el período de retención de los grupos de logs.

B. Crear una política de protección de datos en CloudWatch Logs para evaluar el período de retención de los grupos de logs.

C. Crear una regla de automatización en Security Hub. Configurar la regla para evaluar el período de retención de los grupos de logs.

**D. Usar la regla administrada de AWS Config que evalúa el período de retención de los grupos de logs. Asegurarse de que la integración de AWS Config con Security Hub esté habilitada.**

263.- Una empresa necesita evitar que los objetos de Amazon S3 se compartan con identidades IAM externas a su organización en AWS Organizations. Un ingeniero de seguridad está creando y desplegando una SCP (Service Control Policy) para cumplir con este objetivo. La empresa ya ha habilitado la característica S3 Block Public Access en todos sus buckets de S3.

¿Qué debe hacer la SCP para cumplir con estos requisitos?

**A. Denegar la acción S3:\* con un elemento Condition que use el operador StringNotEquals, la clave aws:ResourceOrgID, y el valor ${aws:PrincipalOrgID}.**

B. Denegar la acción S3:PutAccountPublicAccessBlock con un elemento Condition que use el operador StringLike, la clave aws:PrincipalArn y los valores de los usuarios IAM externos.

C. Permitir la acción S3:\* con un elemento Condition que use el operador StringNotEquals, la clave aws:PrincipalOrgID, y el valor ${aws:PrincipalOrgID}.

D. Denegar la acción S3:\* con un elemento Condition que use el operador StringLike, la clave aws:PrincipalArn, y los valores de los usuarios IAM externos.

264.- Un ingeniero de seguridad está implementando un sistema de autenticación para un entorno con múltiples cuentas, utilizando acceso federado con SAML 2.0. El ingeniero ha configurado AWS IAM Identity Center como proveedor de identidad (IdP). También ha creado roles de IAM para otorgar acceso a las cuentas de AWS.

Un usuario federado reporta un error de autenticación al intentar iniciar sesión con el nuevo sistema.

¿Qué debe hacer el ingeniero de seguridad para solucionar este problema de la manera más eficiente operativamente?

**A. Revisar los registros del IdP SAML para identificar errores. Consultar AWS CloudTrail para verificar las llamadas a la API que hizo el usuario.**

B. Revisar los registros del IdP SAML para identificar errores. Usar el simulador de políticas de IAM para validar el acceso a los roles de IAM.

C. Usar el asesor de acceso de IAM (IAM Access Advisor) para revisar los accesos recientes a servicios. Usar el simulador de políticas de IAM para validar el acceso a los roles de IAM.

D. Volver a crear el IdP SAML en otra cuenta para confirmar el comportamiento que está experimentando el usuario.

265.- Una empresa almacena datos sensibles en un bucket de Amazon S3. La empresa cifra los datos en reposo utilizando cifrado del lado del servidor con claves administradas por Amazon S3 (SSE-S3).

Un ingeniero de seguridad debe evitar cualquier modificación a los datos en el bucket de S3.

¿Qué solución cumplirá con este requisito?

A. Configurar políticas del bucket de S3 para denegar los permisos DELETE y PUT de objetos.

**B. Configurar S3 Object Lock en modo de cumplimiento (compliance mode) con el versionado del bucket habilitado.**

C. Cambiar el cifrado del bucket de S3 para usar claves administradas por el cliente en AWS KMS.

D. Configurar el bucket de S3 con protección de eliminación mediante autenticación multifactor (MFA delete).

266.- Una empresa está desarrollando una nueva aplicación sin servidor (serverless) que utiliza funciones de AWS Lambda. La empresa usa AWS CloudFormation para desplegar las funciones Lambda.

Los desarrolladores están intentando depurar una función Lambda ya desplegada, pero no pueden hacerlo porque la función no está registrando su salida en Amazon CloudWatch Logs.

¿Qué combinación de pasos debería seguir un ingeniero de seguridad para resolver este problema? (Elige dos opciones).

**A. Verificar el rol definido en la plantilla de CloudFormation que se pasa a la función Lambda. Asegurarse de que dicho rol tenga una política de confianza que permita la acción sts:AssumeRole por parte del service principal lambda.amazonaws.com.**

**B. Verificar el rol de ejecución configurado en la plantilla de CloudFormation para la función Lambda. Asegurarse de que ese rol tenga los permisos necesarios para escribir en CloudWatch Logs.**

C. Verificar la configuración de la función Lambda en la plantilla de CloudFormation. Asegurarse de que la función tenga una configuración de trazabilidad de AWS X-Ray establecida en modo Active o PassThrough.

D. Verificar la política de recurso (resource policy) configurada en la plantilla de CloudFormation para la función Lambda. Asegurarse de que la política tenga los permisos necesarios para escribir en CloudWatch Logs.

E. Verificar el rol que los desarrolladores usan para depurar la función Lambda. Asegurarse de que ese rol tenga una política de confianza que permita la acción sts:AssumeRole por parte del service principal lambda.amazonaws.com.

267.- Una empresa utiliza una aplicación de colaboración. Un ingeniero de seguridad necesita configurar alertas automáticas desde AWS Security Hub en la región us-west-2 para esta aplicación. El ingeniero quiere recibir una alerta en un canal de la aplicación cada vez que Security Hub reciba un nuevo hallazgo.

El ingeniero crea una función de AWS Lambda para convertir el mensaje al formato que la aplicación requiere. Esta función Lambda también envía el mensaje a la API de la aplicación. Además, el ingeniero configura una regla de Amazon EventBridge que especifica la función Lambda como destino.

Después de implementar la regla de EventBridge, el canal comienza a recibir constantemente alertas desde Security Hub. Muchas de estas alertas provienen de Amazon Inspector y no requieren ninguna acción. El ingeniero de seguridad quiere detener las alertas de Amazon Inspector.

¿Qué solución cumplirá con este requisito con el menor esfuerzo operativo posible?

A. Actualizar el código de la función Lambda para detectar coincidencias de eventos provenientes de Amazon Inspector y suprimir esos hallazgos.

B. Crear una acción personalizada en Security Hub que envíe automáticamente los hallazgos de todos los servicios, excepto los de Amazon Inspector, al bus de eventos de EventBridge.

**C. Modificar el valor del atributo ProductArn en el patrón de eventos de la regla de EventBridge para usar: "anything-but": ["arn:aws:securityhub:us-west-2::product/aws/inspector"].**

D. Crear un tema de Amazon SNS para enviar mensajes a la aplicación. Establecer una política de filtro en las suscripciones del tema para rechazar cualquier mensaje que contenga la cadena product/aws/inspector.

268.- Una empresa tiene una organización en AWS Organizations, compuesta por múltiples unidades organizativas (OUs). La empresa debe evitar que los principales de IAM fuera de la organización accedan a los buckets de Amazon S3 de la organización. La solución no debe afectar el acceso existente que ya tienen las OUs a los buckets S3.

¿Qué solución cumplirá con estos requisitos?

A. Configurar S3 Block Public Access para todos los buckets de S3.

B. Configurar S3 Block Public Access para todas las cuentas de AWS.

C. Implementar una SCP que incluya la condición "aws:ResourceOrgPaths": "${aws:PrincipalOrgPaths}".

**D. Implementar una SCP que incluya la condición "aws:ResourceOrgID": "${aws:PrincipalOrgID}".**

269.- Una empresa necesita implementar gestión del ciclo de vida de datos para los snapshots de Amazon RDS. La empresa usará AWS Backup para administrar estos snapshots.

Se requiere retener los snapshots automatizados de RDS durante 5 años, y se usará Amazon S3 para el almacenamiento de archivo a largo plazo.

¿Qué solución cumplirá con estos requisitos?

A. Usar AWS Backup para aplicar una etiqueta de retención de 5 años a los snapshots de RDS.

B. Habilitar el versionado en el bucket de S3 que utiliza AWS Backup para los snapshots de RDS. Configurar un período de retención de 5 años.

C. Crear una política de ciclo de vida (Lifecycle) en S3. Incluir un período de retención de 5 años para el bucket de S3 que usa AWS Backup para los snapshots de RDS.

**D. Crear un plan de respaldo en AWS Backup. Configurar un período de retención de 5 años.**

270.- La política de seguridad de una empresa requiere que todas las instancias de Amazon EC2 usen el servicio de sincronización de hora de Amazon (Amazon Time Sync Service). Los trails de AWS CloudTrail están habilitados en todas las cuentas de AWS de la empresa. Los VPC Flow Logs están habilitados para todas las VPC.

Un ingeniero de seguridad debe identificar cualquier instancia EC2 que intente usar servidores NTP (Network Time Protocol) en internet.

¿Qué solución cumplirá con estos requisitos?

A. Monitorear los logs de CloudTrail en busca de llamadas a la API hacia servidores de hora no estándar.

B. Monitorear los logs de CloudTrail en busca de llamadas a la API hacia el servicio Amazon Time Sync.

**C. Monitorear los VPC Flow Logs en busca de tráfico hacia servidores de hora no estándar.**

D. Monitorear los VPC Flow Logs en busca de tráfico hacia el servicio Amazon Time Sync.

271.- Una empresa utiliza una estrategia de múltiples cuentas que emplea una organización en AWS Organizations con todas las funcionalidades habilitadas. La empresa ha activado el acceso confiable (trusted access) para AWS Account Management. Las nuevas cuentas se aprovisionan mediante AWS Control Tower Account Factory.

La empresa debe asegurarse de que todas las nuevas cuentas dentro de la organización se conviertan automáticamente en cuentas miembro de AWS Security Hub.

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

A. Habilitar Security Hub en la cuenta de administración de la organización. Crear un flujo de trabajo con AWS Step Functions. Crear una regla de Amazon EventBridge para invocar el flujo cuando ocurra un evento CreateAccount.

B. Habilitar Security Hub en la cuenta de administración de la organización. Esperar a que todas las nuevas cuentas se incorporen automáticamente.

C. Habilitar Security Hub en la cuenta de administración de la organización. Crear una función AWS Lambda para habilitar Security Hub en las nuevas cuentas. Invocar la función Lambda usando un evento del ciclo de vida de AWS Control Tower cuando se aprovisione una nueva cuenta.

**D. Usar la cuenta de administración de la organización para designar una cuenta delegada de Security Hub. En esa cuenta delegada, crear una política de configuración para habilitar Security Hub. Asociar la política de configuración a la raíz de la organización.**

272.- Una empresa utiliza Amazon Elastic Kubernetes Service (Amazon EKS) para ejecutar sus aplicaciones basadas en Kubernetes. La empresa utiliza Amazon GuardDuty para proteger dichas aplicaciones.

La protección para EKS está habilitada en GuardDuty. Sin embargo, la funcionalidad correspondiente no está monitoreando las aplicaciones basadas en Kubernetes.

¿Qué solución permitirá que GuardDuty comience a monitorear las aplicaciones de Kubernetes?

A. Habilitar los VPC Flow Logs para la VPC que aloja los clústeres de EKS.

B. Asignar la política administrada de AWS CloudWatchEventsFullAccess a los clústeres de EKS.

C. Asegurarse de que la política administrada de AWS AmazonGuardDutyFullAccess esté adjunta al rol de servicio de GuardDuty.

**D. Habilitar los logs del plano de control (control plane) en Amazon EKS. Asegurarse de que los logs se estén ingresando en Amazon CloudWatch.**

273.- Una empresa necesita registrar la actividad a nivel de objeto en sus buckets de Amazon S3. Además, necesita validar la integridad de los archivos de registro mediante una firma digital.

¿Qué solución cumplirá con estos requisitos?

**A. Crear un trail de AWS CloudTrail con la opción de validación de archivos de registro habilitada. Activar los eventos de datos y especificar Amazon S3 como tipo de evento de datos.**

B. Crear un nuevo bucket de S3 para almacenar los registros de acceso del servidor S3. Configurar los buckets existentes para enviar sus registros de acceso a este nuevo bucket.

C. Crear un grupo de logs de Amazon CloudWatch Logs. Configurar los buckets existentes para enviar sus registros de acceso del servidor S3 a este grupo.

D. Crear un nuevo bucket de S3 para los registros de acceso del servidor S3 con validación de archivos de registro habilitada. Activar los eventos de datos. Especificar Amazon S3 como tipo de evento de datos.

274.- Una empresa ha lanzado un nuevo sistema de gestión de cuentas basado en la web para un juego en línea. Los jugadores crean un nombre de usuario y una contraseña únicos para iniciar sesión en el sistema.

La empresa ha implementado una ACL web de AWS WAF para proteger el sistema. Esta ACL incluye el grupo de reglas administrado por AWS llamado core rule set (CRS), aplicado sobre el Application Load Balancer que sirve al sistema.

El equipo de seguridad de la empresa descubre que el sistema fue objetivo de un ataque de credential stuffing. Se usaron credenciales expuestas en otras brechas para intentar iniciar sesión en el sistema.

El equipo de seguridad debe implementar una solución que reduzca la posibilidad de un ataque exitoso de credential stuffing en el futuro, y que además minimice el impacto en los usuarios legítimos del sistema.

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

**A. Crear una métrica personalizada en Amazon CloudWatch para analizar la cantidad de respuestas de inicio de sesión exitosas desde una misma dirección IP.**

**B. Agregar el grupo de reglas administrado por AWS llamado account takeover prevention (ATP) a la ACL web. Configurar el grupo de reglas para que inspeccione las solicitudes de inicio de sesión al sistema. Bloquear cualquier solicitud que tenga la etiqueta awswaf:managed:aws:atp:signal:credential\_compromised.**

C. Configurar una acción predeterminada en la ACL web que exija a todos los usuarios resolver un CAPTCHA al iniciar sesión.

D. Implementar reglas en la ACL web basadas en IP para cualquier dirección IP que genere muchas respuestas de inicio de sesión exitosas. Bloquear las direcciones IP que generen muchos inicios de sesión exitosos.

E. Crear una respuesta personalizada de bloqueo que redirija a los usuarios a un flujo seguro dentro del sistema para restablecer su contraseña.

275.- Una empresa ejecuta cargas de trabajo en AWS. Estas cargas están distribuidas en cuentas separadas de AWS para desarrollo, pruebas y producción.

Todos los desarrolladores de la empresa pueden acceder a la cuenta de desarrollo. Un subconjunto de esos desarrolladores también puede acceder a las cuentas de pruebas y producción.

La empresa está gastando demasiado tiempo administrando credenciales individuales para cada desarrollador en cada entorno. Un ingeniero de seguridad debe implementar una solución más escalable, que permita a los desarrolladores acceder a recursos en múltiples cuentas, y que además minimice el uso compartido de credenciales.

¿Qué solución cumplirá con estos requisitos?

A. Usar AWS Identity and Access Management (IAM) Access Analyzer para identificar los permisos que los desarrolladores necesitan en cada cuenta. Configurar IAM Access Analyzer para aprovisionar automáticamente el acceso correcto para cada desarrollador.

B. Crear un flujo de trabajo en Amazon Simple Workflow Service (Amazon SWF). Indicar a los desarrolladores que usen ese flujo para solicitar acceso a otras cuentas cuando necesiten permisos adicionales.

**C. Crear roles de IAM en las cuentas de pruebas y producción. Agregar una política que permita la acción sts:AssumeRole a esos roles. Crear roles de IAM en la cuenta de desarrollo para los desarrolladores que deben acceder a pruebas y producción. Agregar estos roles a la política de confianza de los nuevos roles en pruebas y producción.**

D. Crear cuentas de servicio en los entornos de pruebas y producción. Entregar las claves de acceso de esas cuentas a los desarrolladores que necesiten acceso. Rotar las claves periódicamente.

276.- Una empresa opera una plataforma de software de código abierto expuesta a internet. Esta plataforma es legada y ya no recibe actualizaciones de seguridad. Funciona utilizando balanceo de carga con peso (weighted) de Amazon Route 53, enviando tráfico a dos instancias de Amazon EC2 que se conectan a un cluster de Amazon RDS.

Un informe reciente indica que esta plataforma es vulnerable a ataques de inyección SQL (SQL injection), y se han proporcionado ejemplos de estos ataques. El ingeniero de seguridad de la empresa debe proteger el sistema contra estos ataques en un plazo de 24 horas. La solución debe implicar el menor esfuerzo posible y mantener la operación normal durante la implementación.

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

**A. Crear un Application Load Balancer (ALB) con las instancias EC2 existentes como grupo de destino. Crear una ACL web de AWS WAF con reglas que protejan la aplicación de estos ataques y aplicarla al ALB. Probar que la vulnerabilidad ha sido mitigada, luego redirigir los registros de Route 53 para que apunten al ALB. Actualizar los grupos de seguridad de las instancias EC2 para evitar el acceso directo desde internet.**

B. Crear una distribución de Amazon CloudFront especificando una instancia EC2 como origen. Crear una ACL web de AWS WAF con reglas que protejan contra estos ataques y aplicarla a la distribución. Probar que la vulnerabilidad ha sido mitigada, luego redirigir los registros de Route 53 para que apunten a CloudFront.

C. Obtener el código fuente más reciente de la plataforma y realizar las actualizaciones necesarias. Probar el código actualizado para asegurarse de que la vulnerabilidad ha sido mitigada, luego desplegar la versión corregida en las instancias EC2.

D. Actualizar el grupo de seguridad de las instancias EC2 eliminando el acceso desde internet al puerto TCP usado por la base de datos SQL. Crear una ACL web de AWS WAF con reglas que protejan contra los ataques y aplicarla directamente a las instancias EC2. Probar que la vulnerabilidad ha sido mitigada y luego restaurar el grupo de seguridad a su configuración original.

277.- Una empresa ejecuta una aplicación que envía registros (logs) a un grupo de registros en Amazon CloudWatch Logs. Los correos electrónicos de los usuarios de la aplicación se incluyen en esos registros.

Los desarrolladores de la empresa necesitan ver los registros en CloudWatch Logs, pero un ingeniero de seguridad debe asegurarse de que los desarrolladores no puedan ver las direcciones de correo electrónico de los usuarios.

¿Qué solución cumplirá con este requisito?

A. Usar Amazon Macie para escanear el grupo de registros. Configurar Macie con un identificador de datos personalizado que utilice una expresión regular para detectar patrones de correos electrónicos. Activar el descubrimiento automático de datos en Macie.

B. Crear una clave de AWS Key Management Service (AWS KMS). Configurar el grupo de registros para que utilice esa clave para cifrar los registros. Configurar la política de la clave para denegar el acceso al rol IAM que los desarrolladores asumen para usar CloudWatch Logs.

C. Crear un filtro de suscripción para el grupo de registros. Configurar la suscripción para que envíe los datos de los registros a una función de AWS Lambda. Programar la función Lambda para que analice las entradas del log y oculte (enmascare) los valores que sean direcciones de correo electrónico.

**D. Configurar una política de protección de datos para el grupo de registros. Especificar el identificador de datos administrado por AWS llamado EmailAddress para el tipo de datos que se desea enmascarar. Activar la protección de datos para el grupo de registros.**

278.- Un ingeniero de seguridad está implementando una solución de registro de eventos para el entorno de AWS de una empresa. El ingeniero ha configurado un trail de AWS CloudTrail en la cuenta de AWS de la empresa. Los registros se almacenan en un bucket de Amazon S3 para que un proveedor de servicios externo los supervise. Este proveedor tiene un rol de IAM asignado para acceder al bucket S3.

La empresa requiere que todos los registros estén cifrados en reposo mediante una clave administrada por el cliente (CMK). El ingeniero de seguridad usa AWS Key Management Service (AWS KMS) para crear la clave y su política correspondiente. También configura CloudTrail para usar esa clave al cifrar los registros.

Cuando el ingeniero implementa esta configuración, el proveedor de servicios ya no puede leer los registros.

¿Qué debe hacer el ingeniero de seguridad para que el proveedor de servicios pueda leer los registros?

A. Asegurarse de que la política del bucket S3 permita el acceso del rol del proveedor de servicios para descifrar objetos.

**B. Agregar una declaración a la política de la clave para permitir que el rol del proveedor de servicios realice la acción kms:Decrypt sobre la clave.**

C. Agregar la política administrada de AWS AWSKeyManagementServicePowerUser al rol del proveedor de servicios.

D. Migrar la clave a AWS Certificate Manager (ACM) para crear un endpoint compartido de acceso a la clave.

279.- Una empresa ejecuta cargas de trabajo en instancias de Amazon EC2. La empresa necesita monitorear continuamente las instancias EC2 en busca de vulnerabilidades de software y mostrar los hallazgos en AWS Security Hub. No se deben instalar agentes en las instancias EC2.

¿Qué solución cumplirá con estos requisitos?

**A. Habilitar Amazon Inspector. Establecer el modo de escaneo en escaneo híbrido. Habilitar la integración de Amazon Inspector en Security Hub.**

B. Usar Security Hub para habilitar el estándar AWS Foundational Security Best Practices. Esperar a que Security Hub genere los hallazgos.

C. Habilitar Amazon GuardDuty. Iniciar escaneos de malware bajo demanda usando GuardDuty Malware Protection. Habilitar la integración de GuardDuty en Security Hub.

D. Usar reglas administradas de AWS Config para detectar vulnerabilidades de software en EC2. Asegurarse de que Security Hub tenga habilitada la integración con AWS Config.

280.- Una empresa ejecuta una aplicación de juegos en línea personalizada. La empresa utiliza Amazon Cognito para la autenticación y autorización de usuarios.

Un ingeniero de seguridad quiere usar AWS para implementar autorización de grano fino en los recursos de la aplicación personalizada. El ingeniero debe implementar una solución que use los atributos de usuario que ya existen en Cognito. La empresa ya configuró un grupo de usuarios (user pool) y un grupo de identidades (identity pool) en Cognito.

¿Qué solución cumplirá con estos requisitos?

A. Crear un conjunto de roles y políticas de IAM. Configurar el identity pool de Cognito para asignar los usuarios a los roles de IAM.

**B. Crear un almacén de políticas en Amazon Verified Permissions. Configurar Cognito como fuente de identidad. Mapear los tokens de acceso de Cognito al esquema de Verified Permissions.**

C. Crear permisos administrados por el cliente mediante AWS Resource Access Manager (AWS RAM). Configurar el identity pool de Cognito para asignar los usuarios a estos permisos administrados.

D. Crear un conjunto de usuarios de IAM y políticas de IAM. Configurar el user pool de Cognito para asignar los usuarios a los usuarios de IAM.

281.- Una empresa desea automatizar la creación de un informe de seguridad. La empresa tiene una función de AWS Lambda que recopila datos de hallazgos de Amazon Inspector almacenados en AWS Security Hub en la región us-west-2. Luego, la función Lambda debe generar un informe diario utilizando una programación con Amazon EventBridge.

Un ingeniero de seguridad descubre que la función Lambda no está logrando crear el informe. El ingeniero debe implementar una solución que corrija el problema y que además utilice permisos con el menor privilegio necesario.

¿Qué solución cumplirá con estos requisitos?

A. Crear una política basada en recursos que permita a Security Hub acceder al ARN de la función Lambda.  
**B. Adjuntar la política administrada AWSSecurityHubReadOnlyAccess al rol de ejecución de la función Lambda.**  
C. Otorgar al rol de ejecución de la función Lambda permisos de solo lectura para acceder a Amazon Inspector y Security Hub.  
D. Crear una política personalizada de IAM que otorgue permisos de Get\*, List\*, Batch\* y Describe\* en el recurso arn:aws:securityhub:us-west-2::product/aws/inspector/\*. Adjuntar la política al rol de ejecución de la función Lambda.

282.- Una empresa debe conservar copias de respaldo de sus instancias Amazon RDS y de los volúmenes de Amazon Elastic Block Store (Amazon EBS). Las copias de respaldo deben almacenarse en centros de datos situados a cientos de millas de distancia.

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

A. Configurar AWS Backup para crear las copias de respaldo según el programa necesario. En el plan de respaldo, especificar múltiples zonas de disponibilidad como destinos de respaldo.

B. Configurar Amazon Data Lifecycle Manager (DLM) para crear las copias de respaldo. Configurar la política de DLM para copiar los respaldos a un bucket de Amazon S3 y habilitar la replicación en dicho bucket.

**C. Configurar AWS Backup para crear las copias de respaldo según el programa necesario. Crear una bóveda de respaldo de destino en otra región de AWS. Configurar AWS Backup para copiar los respaldos a esa bóveda de destino.**

D. Configurar Amazon Data Lifecycle Manager (DLM) para crear las copias de respaldo. Crear una función de AWS Lambda que copie los respaldos a otra región de AWS. Usar Amazon EventBridge para invocar la función Lambda de forma programada.

283.- Un ingeniero de seguridad ha detectado una cantidad inusualmente alta de tráfico proveniente de una sola dirección IP al analizar los registros de acceso del Application Load Balancer.

¿Cómo puede el ingeniero limitar la cantidad de solicitudes desde esa IP sin bloquearla por completo?

A. Agregar una regla en el Application Load Balancer para enrutar el tráfico que provenga de la dirección IP en cuestión y mostrar una página web estática.

**B. Implementar una regla basada en tasa (rate-based rule) con AWS WAF.**

C. Utilizar AWS Shield para limitar la tasa de solicitudes originadas.

D. Implementar la función de geolocalización en Amazon Route 53

284.- Una empresa ejecuta cargas de trabajo distribuidas en cientos de instancias de Amazon EC2. Durante un incidente de seguridad reciente, una instancia de EC2 fue comprometida y ejecutó código malicioso hasta que la empresa la detuvo manualmente.

Ahora la empresa utiliza Amazon GuardDuty para detectar malware en las instancias de EC2. Un ingeniero de seguridad debe implementar una solución que responda de forma automática cuando GuardDuty determine que una instancia está infectada. La solución debe mitigar el incidente y cumplir con la guía de respuesta ante incidentes del AWS Well-Architected Framework.

¿Qué solución cumplirá con estos requisitos?

A. Configurar AWS Systems Manager Run Command para que se ejecute cuando GuardDuty detecte que una instancia está infectada. Usar Run Command para quitar todos los adaptadores de red del sistema operativo de la instancia comprometida y añadir la etiqueta “Infected” a la instancia.

B. Crear una función de AWS Lambda que se ejecute cuando GuardDuty detecte que una instancia está infectada. Programar la función Lambda para eliminar todas las interfaces de red elásticas asociadas a la instancia y añadir la etiqueta “Infected” a la instancia.

**C. Crear una función de AWS Lambda que se ejecute cuando GuardDuty detecte que una instancia está infectada. Programar la función Lambda para separar todos los volúmenes de Amazon Elastic Block Store (Amazon EBS) de la instancia, añadir la etiqueta “Infected” a los volúmenes EBS y, posteriormente, terminar la instancia.**

D. Definir una VPC independiente para aislar instancias de EC2 y un grupo de seguridad que no permita tráfico de red alguno. Crear una función de AWS Lambda que se ejecute cuando GuardDuty detecte que una instancia está infectada. Programar la función Lambda para mover la instancia a la VPC aislada y asignarle el grupo de seguridad.

285.- Una subred pública contiene dos instancias de Amazon EC2. La subred tiene una ACL de red personalizada. Un ingeniero de seguridad está diseñando una solución para mejorar la seguridad de la subred.

La solución debe permitir el tráfico saliente hacia un servicio de Internet que utiliza TLS por el puerto 443 y, además, denegar el tráfico entrante dirigido al puerto 3306 de MySQL.

¿Qué conjunto de reglas de ACL de red cumple con estos requisitos?

A. Usar la regla entrante 100 para permitir tráfico en el puerto TCP 443. Usar la regla entrante 200 para denegar tráfico en el puerto TCP 3306. Usar la regla saliente 100 para permitir tráfico en el puerto TCP 443.

**B. Usar la regla entrante 100 para denegar tráfico en el puerto TCP 3306. Usar la regla entrante 200 para permitir tráfico en el rango de puertos TCP 1024-65535. Usar la regla saliente 100 para permitir tráfico en el puerto TCP 443.**

C. Usar la regla entrante 100 para permitir tráfico en el rango de puertos TCP 1024-65535. Usar la regla entrante 200 para denegar tráfico en el puerto TCP 3306. Usar la regla saliente 100 para permitir tráfico en el puerto TCP 443.

D. Usar la regla entrante 100 para denegar tráfico en el puerto TCP 3306. Usar la regla entrante 200 para permitir tráfico en el puerto TCP 443. Usar la regla saliente 100 para permitir tráfico en el puerto TCP 443.

286.- Una empresa está investigando las acciones que realizó un rol de IAM. La empresa debe averiguar cuándo fue la última vez que el rol accedió a AWS Security Hub y cuándo fue la última vez que utilizó la acción DeleteInsight en Security Hub.

¿Qué solución proporcionará esta información?

A. Usar las comprobaciones de la categoría de seguridad en AWS Trusted Advisor. Buscar el rol y examinar las acciones realizadas.

**B. Usar la pestaña Access Advisor en AWS Identity and Access Management (IAM). Buscar Security Hub y las acciones realizadas.**

C. Usar AWS Identity and Access Management (IAM) para generar un informe de credenciales (credential report). Buscar actividad de Security Hub en el informe.

D. Crear un analyzer en AWS Identity and Access Management Access Analyzer. Examinar los hallazgos sobre las acciones del rol en Security Hub.

287.- Una empresa aloja su aplicación de microservicios en Amazon Elastic Kubernetes Service (Amazon EKS). La empresa ha configurado implementaciones continuas para actualizar la aplicación bajo demanda.

Un ingeniero de seguridad debe implementar una solución que proporcione detección automática de anomalías en los registros de la aplicación en tiempo casi real. Además, la solución debe enviar notificaciones sobre estas anomalías al equipo de seguridad.

¿Qué solución cumplirá con estos requisitos?

A. Configurar Amazon CloudWatch Container Insights para recopilar y agregar los registros de la aplicación en EKS. Crear una alarma de CloudWatch para supervisar las anomalías. Configurar la alarma para que ejecute una función de AWS Lambda que alerte al equipo de seguridad cuando se detecten anomalías.

**B. Configurar Amazon EKS para enviar los registros de la aplicación a Amazon CloudWatch. Crear una alarma de CloudWatch basada en un filtro de métricas del grupo de registros y especificar la detección de anomalías como tipo de umbral. Configurar la alarma para usar Amazon Simple Notification Service (Amazon SNS) y alertar al equipo de seguridad.**

C. Configurar Amazon EKS para exportar los registros a Amazon S3. Utilizar consultas de Amazon Athena para analizar los registros en busca de anomalías. Usar Amazon QuickSight para visualizar y supervisar las solicitudes de acceso de usuarios en busca de anomalías. Configurar notificaciones de Amazon SNS para alertar al equipo de seguridad.

D. Configurar AWS App Mesh para supervisar el tráfico hacia los microservicios en Amazon EKS. Integrar App Mesh con AWS CloudTrail para el registro. Utilizar Amazon Detective para analizar los registros en busca de anomalías y alertar al equipo de seguridad cuando se detecten.

288.- Una empresa está migrando cargas de trabajo en contenedores desde un centro de datos hacia clústeres de Amazon Elastic Container Service (Amazon ECS). La empresa debe implementar una solución para detectar amenazas potenciales en las cargas de trabajo y mejorar la postura de seguridad de los clústeres de contenedores.

¿Qué solución cumplirá con estos requisitos?

A. Configurar Amazon Inspector en la VPC donde se ejecutan los clústeres ECS.

**B. Habilitar Amazon GuardDuty Runtime Monitoring en los clústeres ECS.**

C. Auditar el acceso a la API de Amazon ECS usando los logs de Amazon CloudWatch para identificar accesos no autorizados.

D. Crear clústeres de contenedores en la misma VPC. Usar los VPC flow logs para monitorear

289.- Un ingeniero de seguridad necesita implementar una solución para determinar si las instancias Amazon EC2 de una empresa están siendo usadas para minar criptomonedas. La solución debe enviar notificaciones sobre actividades relacionadas con criptomonedas a un tema de Amazon Simple Notification Service (Amazon SNS).

¿Qué solución cumplirá con estos requisitos?

A. Crear reglas personalizadas de AWS Config usando una política personalizada de Guard. Configurar las reglas para detectar cuando una instancia EC2 consulta un nombre de dominio DNS asociado con actividades relacionadas con criptomonedas. Configurar AWS Config para enviar alertas al tema de SNS.

**B. Habilitar Amazon GuardDuty. Crear una regla en Amazon EventBridge para enviar alertas al tema de SNS cuando GuardDuty genere un hallazgo asociado con actividades relacionadas con criptomonedas.**

C. Habilitar Amazon Inspector. Crear una regla en Amazon EventBridge para enviar alertas al tema de SNS cuando Amazon Inspector genere un hallazgo asociado con actividades relacionadas con criptomonedas.

D. Habilitar los logs de flujo de VPC. Enviar los logs a un bucket de Amazon S3. Configurar una consulta en Amazon Athena para detectar cuando una instancia EC2 consulta un nombre de dominio DNS asociado con actividades relacionadas con criptomonedas. Configurar la consulta para que inicie alertas al tema de SNS.

290.- Una empresa controla el acceso de los usuarios mediante usuarios y grupos de IAM en varias cuentas de AWS dentro de una organización en AWS Organizations. La empresa utiliza un proveedor de identidad externo (IdP) para el inicio de sesión único (SSO) de su fuerza laboral.

La empresa necesita implementar una solución que proporcione un portal de administración único para acceder a las cuentas dentro de la organización. La solución debe admitir el IdP externo como fuente de federación.

¿Qué solución cumplirá con estos requisitos?

**A. Habilitar AWS IAM Identity Center. Especificar el IdP externo como fuente de identidad.**

B. Habilitar la federación con AWS Identity and Access Management (IAM). Especificar el IdP externo como fuente de identidad.

C. Migrar a Amazon Verified Permissions. Implementar acceso detallado a AWS mediante control de acceso basado en políticas (PBAC).

D. Migrar los usuarios a AWS Directory Service. Usar AWS Control Tower para centralizar la seguridad en toda la organización.

291.- Una empresa debe crear instantáneas anuales de los volúmenes de Amazon Elastic Block Store (Amazon EBS). La empresa debe conservar las instantáneas durante 10 años. Utilizará AWS Key Management Service (AWS KMS) para cifrar los volúmenes y las instantáneas de EBS.

Las claves de cifrado deben rotarse automáticamente cada año. Las instantáneas creadas en años anteriores deben seguir siendo legibles después de la rotación de las claves de cifrado.

¿Qué tipo de claves KMS debe usar la empresa para el cifrado y cumplir estos requisitos?

A. Claves KMS administradas por AWS asimétricas con material de clave creado por AWS KMS

**B. Claves KMS administradas por el cliente simétricas con material de clave creado por AWS KMS**

C. Claves KMS administradas por el cliente simétricas con material de clave importado de forma personalizada

D. Claves KMS administradas por AWS asimétricas con material de clave importado de forma personalizada

292.- Una empresa tiene cientos de cuentas de AWS y utiliza AWS Organizations. La empresa planea crear muchos roles y políticas de IAM diferentes para su equipo de producto, equipo de seguridad y equipo de plataforma. Algunas políticas de IAM se compartirán entre equipos.

Un ingeniero de seguridad necesita implementar una solución para agrupar lógicamente los roles de IAM de cada equipo. La solución debe permitir solo al equipo de plataforma delegar permisos de IAM a los servicios de AWS.

¿Qué solución cumple con estos requisitos?

**A. Configurar una ruta de IAM (IAM path) con los roles de cada equipo. Implementar una SCP que niegue el permiso iam:PassRole a todas las entidades, excepto a las que pertenecen a la ruta del equipo de plataforma.**

B. Aplicar etiquetas diferentes a los roles de IAM de cada equipo. Implementar una SCP que niegue el permiso sts:AssumeRole a todas las entidades, excepto a los roles del equipo de plataforma.

C. Aplicar etiquetas diferentes a las políticas de IAM de cada equipo. Implementar una SCP que niegue el permiso iam:PassRole a todas las entidades, excepto a las políticas del equipo de plataforma.

D. Configurar una ruta de IAM con los roles de cada equipo. Usar permissions boundaries de IAM para denegar el permiso sts:AssumeRole a los roles de los equipos de producto y de seguridad.

293.- Los desarrolladores de una empresa están utilizando URLs de funciones de AWS Lambda para invocar funciones directamente. La empresa debe asegurarse de que los desarrolladores no puedan configurar ni desplegar funciones sin autenticación en las cuentas de producción. La empresa quiere cumplir este requisito usando AWS Organizations, sin requerir trabajo adicional por parte de los desarrolladores.

¿Qué solución cumple con estos requisitos?

A. Requerir que los desarrolladores configuren todas las URLs de funciones para admitir CORS (compartición de recursos entre orígenes) cuando las funciones se llamen desde un dominio diferente.

B. Usar una cuenta delegada de administrador de AWS WAF para ver y bloquear el acceso no autenticado a las URLs de funciones en cuentas de producción, basándose en la unidad organizativa (OU) de las cuentas que utilizan las funciones.

C. Usar políticas de control de servicio (SCP) para permitir todas las acciones lambda:CreateFunctionUrlConfig y lambda:UpdateFunctionUrlConfig que tengan como valor de la clave de condición lambda:FunctionUrlAuthType el valor AWS\_IAM.

**D. Usar SCPs para denegar todas las acciones lambda:CreateFunctionUrlConfig y lambda:UpdateFunctionUrlConfig que tengan como valor de la clave de condición lambda:FunctionUrlAuthType el valor NONE.**

294.- Una empresa está implementando nuevos requisitos de cumplimiento para satisfacer las necesidades de sus clientes. Según estos nuevos requisitos, la empresa no debe usar instancias ni clústeres de bases de datos de Amazon RDS que no tengan cifrado en el almacenamiento subyacente.

La empresa necesita una solución que:

Genere una alerta por correo electrónico cuando se cree una instancia o clúster de base de datos sin cifrado.

Elimine automáticamente esa instancia o clúster sin cifrado.

¿Cuál solución cumplirá con estos requisitos de la manera más eficiente operativamente?

**A. Crear una regla administrada de AWS Config para detectar almacenamiento RDS sin cifrado. Configurar una acción de remediación automática que publique mensajes en un tema de Amazon SNS que incluya una función de AWS Lambda y un destino de correo electrónico como suscriptores. Configurar la función Lambda para eliminar el recurso sin cifrado.**

B. Crear una regla administrada de AWS Config para detectar almacenamiento RDS sin cifrado. Configurar una acción de remediación manual para invocar una función de AWS Lambda. Configurar la función Lambda para publicar mensajes en un tema de Amazon SNS y eliminar el recurso sin cifrado.

C. Crear una regla de Amazon EventBridge que evalúe patrones de eventos de RDS y se active con la creación de instancias o clústeres de bases de datos. Configurar la regla para publicar mensajes en un tema de Amazon SNS que incluya una función de AWS Lambda y un destino de correo electrónico como suscriptores. Configurar la función Lambda para eliminar el recurso sin cifrado.

D. Crear una regla de Amazon EventBridge que evalúe patrones de eventos de RDS y se active con la creación de instancias o clústeres de bases de datos. Configurar la regla para invocar una función de AWS Lambda. Configurar la función Lambda para publicar mensajes en un tema de Amazon SNS y eliminar el recurso sin cifrado.

295.- Un ingeniero de seguridad quiere evaluar los cambios de configuración realizados en un recurso específico de AWS para asegurarse de que cumpla con los estándares de cumplimiento. Sin embargo, le preocupa una situación en la que se realicen varios cambios de configuración en rápida sucesión. El ingeniero desea registrar solo la última configuración del recurso para reflejar el impacto acumulado del conjunto de cambios.

¿Cuál solución cumplirá con este requisito de la manera más eficiente operativamente?

A. Usar AWS CloudTrail para detectar los cambios de configuración filtrando llamadas a la API para monitorear los cambios. Usar la llamada a la API más reciente para reflejar el impacto acumulado de múltiples llamadas.

**B. Usar AWS Config para detectar los cambios de configuración y registrar la última configuración en caso de múltiples cambios.**

C. Usar Amazon CloudWatch para detectar los cambios de configuración filtrando llamadas a la API para monitorear los cambios. Usar la llamada a la API más reciente para reflejar el impacto acumulado de múltiples llamadas.

D. Usar AWS Cloud Map para detectar los cambios de configuración. Generar un informe de cambios desde AWS Cloud Map para rastrear el último estado usando una ventana de tiempo deslizante.

296.- Una empresa utiliza AWS Organizations para administrar una organización que consiste en tres Unidades Organizativas (OU) de trabajo: Producción, Desarrollo y Pruebas. La empresa usa plantillas de AWS CloudFormation para definir y desplegar la infraestructura de las cargas de trabajo en las cuentas de AWS asociadas a estas OUs. A cada OU se le han adjuntado diferentes Políticas de Control de Servicios (SCPs).

La empresa desplegó correctamente una actualización de una pila de CloudFormation en las cargas de trabajo de las OUs de Desarrollo y Pruebas. Sin embargo, al usar la misma plantilla de CloudFormation para desplegar la actualización en una cuenta dentro de la OU de Producción, la implementación falla. El mensaje de error indica permisos insuficientes en IAM.

¿Cuál debería ser el primer paso que debe tomar un ingeniero de seguridad para solucionar este problema?

**A. Revisar los registros de AWS CloudTrail en la cuenta de la OU de Producción. Buscar llamadas a la API fallidas provenientes de CloudFormation durante el intento de implementación.**

B. Eliminar todas las SCPs adjuntas a la OU de Producción. Volver a ejecutar la actualización de la pila de CloudFormation para determinar si las SCPs estaban bloqueando las llamadas a la API.

C. Confirmar que el rol utilizado por CloudFormation tenga los permisos suficientes para crear, actualizar y eliminar los recursos referenciados en la plantilla de CloudFormation.

D. Hacer que todas las SCPs adjuntas a la OU de Producción sean iguales a las SCPs de la OU de Pruebas.

297.- Una empresa aloja una aplicación web que captura y almacena datos sensibles en una tabla de Amazon DynamoDB. La empresa necesita implementar una solución que proporcione protección de datos de extremo a extremo y la capacidad de detectar cambios no autorizados en los datos.

¿Qué solución cumplirá con estos requisitos?

A. Usar una clave administrada por el cliente de AWS Key Management Service (AWS KMS). Cifrar los datos en reposo.

B. Usar AWS Private Certificate Authority. Cifrar los datos en tránsito.

**C. Usar el Cliente de Cifrado de DynamoDB. Usar cifrado del lado del cliente. Firmar los elementos de la tabla.**

D. Usar el SDK de cifrado de AWS. Usar cifrado del lado del cliente. Firmar los elementos de la tabla.

298.- Un ingeniero de seguridad ha creado un detector de Amazon GuardDuty en varias cuentas de AWS. Las cuentas pertenecen a una organización en AWS Organizations. El ingeniero de seguridad necesita una visibilidad centralizada de los hallazgos de seguridad provenientes de los detectores.

¿Qué solución cumplirá con este requisito?

A. Configurar Amazon CloudWatch Logs Insights.

B. Crear un panel de control (dashboard) en Amazon CloudWatch.

**C. Configurar integraciones con AWS Security Hub.**

D. Consultar los hallazgos usando Amazon Athena.

299.- Una empresa ejecuta cargas de trabajo en instancias Amazon EC2 dentro de VPCs. Las instancias EC2 realizan solicitudes a buckets de Amazon S3 a través de endpoints de VPC. La empresa utiliza AWS Organizations para gestionar sus cuentas de AWS.

La empresa necesita que las solicitudes realizadas por las instancias EC2 se originen desde la misma VPC para la cual se emitieron las credenciales de la instancia EC2.

¿Qué solución cumplirá con este requisito?

A. Implementar una SCP que incluya la acción S3:\* con la condición "aws:SourceVpc": "${aws:Ec2InstanceSourceVpc}".

B. Editar los endpoints de VPC para incluir la acción S3:\* con la condición "aws:Ec2InstanceSourcePrivateIPv4": "${aws:VpcSourceIp}".

C. Restringir todas las acciones en las políticas del bucket S3 utilizando la clave de condición aws:SourceVpce con el valor del endpoint de VPC permitido.

**D. Restringir todas las acciones en las políticas del bucket S3 utilizando la clave de condición aws:SourceVpc con el valor del ID de VPC permitido.**

300.- Una empresa utiliza Amazon Cognito para la autenticación de usuarios externos en una aplicación web. Los usuarios externos informan que ya no pueden iniciar sesión en la aplicación.

¿Cuál es el primer paso que debe tomar un ingeniero de seguridad para solucionar el problema?

A. Revisar los registros de AWS CloudTrail para identificar errores de autenticación relacionados con los usuarios de Cognito.

B. Usar AWS Identity and Access Management Access Analyzer para eliminar todos los roles y usuarios de IAM que no se estén utilizando.

**C. Revisar los cambios recientes en la configuración de Cognito, las políticas de IAM y las políticas de confianza de los roles para identificar posibles problemas.**

D. Escribir un script que utilice comandos de la CLI para restablecer todas las contraseñas de los usuarios en el grupo de usuarios de Cognito.

301.- Una empresa ejecuta su aplicación en AWS. Usuarios maliciosos aprovecharon un evento promocional reciente y crearon muchas cuentas falsas.

Actualmente, la aplicación utiliza Amazon CloudFront frente a una API de Amazon API Gateway. Las funciones de AWS Lambda gestionan los distintos endpoints de la API. El endpoint GET de registro se encuentra en la ruta /store/registration. El URI para enviar los detalles de una nueva cuenta está en /store/newaccount.

Un ingeniero de seguridad debe diseñar una solución que evite explotaciones similares en futuros eventos promocionales.

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

**A. Crear una ACL web de AWS WAF. Agregar el grupo de reglas AWSManagedRulesACFPRuleSet a la ACL web. Asociar la ACL web con la distribución de CloudFront.**

**B. Crear una ACL web de AWS WAF. Agregar una regla de límite de velocidad (rate limit) a la ACL web. Incluir una entrada RateBasedStatement que tenga un valor SearchString apuntando a /store/registration.**

C. Especificar /store/registration como la ruta de la página de registro. Especificar /store/newaccount como la ruta de creación de cuenta.

D. Habilitar AWS Shield Advanced para la cuenta que aloja la distribución de CloudFront. Configurar una mitigación personalizada específica de DNS que utilice el Shield Response Team (SRT) para /store/newaccount.

E. Habilitar Amazon GuardDuty para la cuenta que aloja la distribución de CloudFront. Habilitar la Protección Lambda para las funciones que responden a llamadas a /store/registration y /store/newaccount.

302.- Una empresa está investigando un aumento en su factura mensual de AWS. Descubre que actores maliciosos comprometieron algunas instancias de Amazon EC2 y usaron esas instancias para alojar páginas web como parte de una campaña masiva de phishing por correo electrónico.

Un ingeniero de seguridad debe implementar una solución para monitorear futuros aumentos de costos y así ayudar a detectar actividades maliciosas.

¿Qué solución ofrecerá a la empresa la detección más temprana posible de aumentos de costos?

A. Crear una regla de Amazon EventBridge que invoque una función de AWS Lambda cada hora. Programar la función Lambda para que descargue un informe de uso de AWS desde AWS Data Exports sobre el uso de todos los servicios. Programar también la función Lambda para analizar el informe y enviar una notificación cuando se detecten anomalías.

**B. Crear un monitor de costos en AWS Cost Anomaly Detection. Configurar una alerta individual para notificar a un tema de Amazon SNS cuando el porcentaje de costo supere un umbral definido.**

C. Revisar manualmente AWS Cost Explorer todos los días para detectar anomalías en los costos de meses anteriores. Revisar el uso de los servicios que muestren un aumento significativo.

D. Capturar los VPC flow logs de la VPC donde se ejecutan las instancias EC2. Usar una herramienta de análisis de red de terceros para analizar los registros de flujo y detectar anomalías de tráfico que puedan incrementar el costo.

303.- La política de seguridad de red de una empresa requiere cifrado para todos los datos en tránsito. La empresa debe cifrar los datos que se envían entre las instancias de Amazon EC2 y los volúmenes de Amazon Elastic Block Store (Amazon EBS).

¿Qué solución cumple con este requisito?

A. Configurar Amazon EC2 para habilitar el cifrado en las propiedades de la interfaz de red de EC2.

**B. Configurar Amazon EBS para habilitar el cifrado de volúmenes con AWS Key Management Service (AWS KMS) para datos en reposo.**

C. Configurar Amazon EBS para habilitar el cifrado TLS en las propiedades de configuración del volumen.

D. Configurar Amazon EC2 para habilitar el cifrado TLS con certificados almacenados en AWS Certificate Manager (ACM).

304.- Una empresa ejecuta una aplicación web en un conjunto de instancias de Amazon EC2 que forman parte de un grupo de Auto Scaling. Las instancias EC2 están en la misma subred de VPC que otras cargas de trabajo.

Un ingeniero de seguridad implementa un detector de Amazon GuardDuty en la misma región de AWS que las instancias EC2, y también configura la integración de AWS Security Hub con GuardDuty.

El ingeniero de seguridad necesita implementar una solución automatizada que detecte y responda adecuadamente a patrones de tráfico anómalos en la aplicación web. La solución debe cumplir con las mejores prácticas de AWS para la respuesta inicial a incidentes de seguridad y debe minimizar la interrupción de la aplicación web.

¿Qué solución cumplirá con estos requisitos?

A. Crear una regla de Amazon EventBridge que detecte hallazgos de GuardDuty con el tipo Behavior:EC2/TrafficVolumeUnusual. Configurar la regla para invocar una función de AWS Lambda que desactive las claves de acceso del perfil de instancia EC2.

**B. Crear una regla de Amazon EventBridge que invoque una función de AWS Lambda cuando GuardDuty detecte tráfico anómalo. Programar la función Lambda para desasociar la instancia identificada del grupo de Auto Scaling y aislarla usando un nuevo grupo de seguridad restringido.**

C. Crear una respuesta automatizada en Security Hub que actualice la ACL de red (network ACL) asociada a la subred de las instancias EC2. Configurar la respuesta para denegar tráfico desde la fuente que generó el tráfico anómalo detectado.

D. Crear un tema de Amazon SNS y suscribir el correo electrónico del ingeniero de seguridad a ese tema. Configurar GuardDuty para enviar todos los hallazgos al tema de SNS.

305.- Una empresa tiene una aplicación que necesita leer objetos desde un bucket de Amazon S3. La empresa configura una política de IAM y la adjunta a un rol de IAM que la aplicación utiliza. Sin embargo, cuando la aplicación intenta leer objetos del bucket S3, recibe errores de AccessDenied.

Un ingeniero de seguridad debe resolver este problema sin reducir la seguridad del bucket S3 ni de la aplicación.

¿Cuál solución cumplirá con estos requisitos?

A. Adjuntar una política de recursos (resource policy) al bucket S3 para otorgar acceso de lectura al rol.

B. Implementar una nueva versión de la aplicación en otra región de AWS y adjuntar el rol a la aplicación.

**C. Revisar la política de IAM utilizando AWS IAM Access Analyzer para asegurarse de que otorga los permisos adecuados. Validar que la aplicación esté asumiendo correctamente el rol.**

D. Asegurarse de que la función "Block Public Access" esté desactivada en el bucket S3. Revisar los registros de AWS CloudTrail para validar que la aplicación esté asumiendo correctamente el rol.

306.- Un ingeniero de seguridad está diseñando una solución que proporcione cifrado de extremo a extremo entre los clientes y los contenedores Docker que se ejecutan en Amazon Elastic Container Service (Amazon ECS). Esta solución también debe ser capaz de manejar patrones de tráfico volátiles.

¿Cuál solución ofrecería la mayor escalabilidad y la menor latencia?

A. Configurar un Network Load Balancer (NLB) para terminar el tráfico TLS y luego volver a cifrar el tráfico hacia los contenedores.

B. Configurar un Application Load Balancer (ALB) para terminar el tráfico TLS y luego volver a cifrar el tráfico hacia los contenedores.

**C. Configurar un Network Load Balancer con un listener TCP para pasar directamente el tráfico TLS hacia los contenedores.**

D. Configurar Amazon Route 53 con enrutamiento de respuesta multivalor (multivalue answer routing) para enviar el tráfico directamente a los contenedores.

307.- Una empresa tiene una gran cantidad de instancias de Amazon EC2 con Amazon Linux 2 que ejecutan una aplicación. Esta aplicación procesa datos sensibles y debe cumplir con los siguientes requisitos de conformidad:

No se pueden exponer los puertos de administración de acceso remoto a las instancias EC2, ni interna ni externamente.

Toda actividad de sesiones remotas debe registrarse en un log de auditoría.

Todo acceso remoto a las instancias EC2 debe ser autenticado y autorizado mediante AWS IAM Identity Center.

El equipo de DevOps de la empresa ocasionalmente necesita conectarse a alguna de las instancias EC2 para solucionar problemas.

¿Qué solución permitirá el acceso remoto a las instancias EC2 cumpliendo con los requisitos de conformidad?

A. Conceder acceso a la consola serial de EC2 a nivel de cuenta. Crear una política de IAM que permita a un rol del equipo DevOps acceder a la consola serial de EC2.

B. Habilitar EC2 Instance Connect en la AMI de las instancias EC2. Configurar las reglas de grupo de seguridad apropiadas. Conceder acceso a la consola EC2 al equipo DevOps para usar Instance Connect.

**C. Asignar un rol de instancia EC2 que permita el acceso a AWS Systems Manager. Crear una política de IAM que otorgue acceso a Session Manager de Systems Manager. Asignar esta política a un rol de IAM del equipo DevOps.**

D. Usar runbooks de AWS Systems Manager Automation para abrir puertos de acceso remoto en las instancias EC2. Adjuntar un rol a las instancias EC2 para permitir la ejecución de los runbooks.