1) Una empresa tiene muchas cuentas de AWS que pertenecen a grupos empresariales individuales. Una de las cuentas fue comprometida recientemente. El atacante lanzó un gran número de instancias, lo que dio lugar a una factura elevada para esa cuenta.

La interrupción de seguridad se resolvió, pero es necesario que un arquitecto de soluciones desarrolle una solución para evitar gastos excesivos en todas las cuentas. Cada grupo empresarial desea retener el control total de su cuenta de AWS.

¿Qué solución debería recomendar el arquitecto de soluciones para cumplir estos requisitos?

A) Utilizar AWS Organizations. Agregar cada cuenta de AWS a la cuenta de administración. Crear una política de control de servicios (SCP) que utilice la clave de condición ec2:instanceType para evitar el lanzamiento de tipos de instancias de alto costo en cada cuenta.
B) Adjuntar una nueva política de IAM administrada por el cliente a un grupo de IAM en cada cuenta. Crear una política para usar la clave de condición ec2:InstanceType a fin de evitar el lanzamiento de tipos de instancias de alto costo. Colocar todos los usuarios de IAM existentes en cada grupo.
C) Activar las alertas de facturación para cada cuenta de AWS. Crear alarmas de Amazon CloudWatch que envíen una notificación de Amazon Simple Notification Service (Amazon SNS) al administrador de la cuenta siempre que la cuenta supere un límite de gastos designado.
D) Activar AWS Cost Explorer en cada cuenta. Revisar los informes de Cost Explorer para cada cuenta con regularidad, para así asegurarse de que los gastos no superen la cantidad deseada.

2) Una empresa tiene varias cuentas de AWS en una organización en AWS Organizations. La empresa ha integrado el Active Directory que tiene en sus instalaciones con AWS Single Sign-On (AWS SSO) a fin de otorgar a los usuarios de Active Directory permisos de mínimo privilegio para administrar la infraestructura en todas las cuentas.

Un arquitecto de soluciones debe integrar una solución de monitoreo de terceros que requiera acceso de solo lectura en todas las cuentas de AWS. La solución de monitoreo se ejecutará en su propia cuenta de AWS.

¿Qué debe hacer el arquitecto de soluciones para otorgar los permisos requeridos a la solución de monitoreo?

A) Crear un usuario en un directorio de AWS SSO. Asignar al usuario un conjunto de permisos de solo lectura. Asignar al usuario todas las cuentas de AWS que necesiten monitoreo. Proporcionar a la solución de monitoreo de terceros el nombre de usuario y la contraseña.
B) Crear un rol de IAM en la cuenta de administración de la organización. Permitir que la cuenta de AWS de la solución de monitoreo de terceros asuma el rol.
C) Invitar a la cuenta de AWS de la solución de monitoreo de terceros a unirse a la organización. Habilitar todas las características.
D) Crear una plantilla de AWS CloudFormation que defina un nuevo rol de IAM para la solución de monitoreo de terceros. Especificar la cuenta de AWS de la solución de monitoreo de terceros en la política de confianza. Crear el rol de IAM en todas las cuentas de AWS vinculadas mediante stack sets.

3) Un equipo está creando un formulario HTML que está alojado en un Amazon S3 Bucket público. El formulario utiliza JavaScript para publicar datos en un punto de enlace de API de Amazon API Gateway. El punto de enlace de API está integrado en las funciones de AWS Lambda. El equipo ha probado cada método en la consola de API Gateway y ha recibido respuestas válidas.

¿Qué combinación de pasos debe realizar el equipo para que el formulario se publique con éxito en el punto de enlace de API y reciba una respuesta válida? (Seleccione DOS).

A) Configurar el S3 Bucket para permitir el intercambio de recursos de origen cruzado (CORS).
B) Alojar el formulario en Amazon EC2 en lugar de Amazon S3.
C) Solicitar un aumento de cuota para API Gateway.
D) Habilitar el intercambio de recursos de origen cruzado (CORS) en API Gateway.
E) Configurar el S3 Bucket para el alojamiento web.

4) Una empresa ejecuta una aplicación móvil sin servidor que utiliza Amazon API Gateway, las funciones de AWS Lambda, Amazon Cognito y Amazon DynamoDB. Durante grandes aumentos de tráfico, los usuarios informan errores intermitentes del sistema. El punto de enlace de API de API Gateway muestra errores de código de estado HTTP 502 (Bad Gateway) a solicitudes válidas.

¿Qué solución resolverá este problema?

A) Aumentar la cuota de concurrencia para las funciones de Lambda. Configurar Amazon CloudWatch para que envíe alertas de notificación cuando la métrica ConcurrentExecutions se acerque a la cuota.
B) Configurar alertas de notificación para la cuota de transacciones por segundo en el punto de enlace de API de API Gateway. Crear una función de Lambda que aumente la cuota cuando sea necesario.
C) Repartir los usuarios en grupos de usuarios de Amazon Cognito en varias regiones de AWS para reducir la latencia de la autenticación de usuarios.
D) Utilizar lecturas muy consistentes de DynamoDB para garantizar que la aplicación del cliente siempre reciba los datos más recientes.

5) Una empresa lanza un nuevo servicio web en un clúster de Amazon Elastic Container Service (Amazon ECS). El clúster consta de 100 instancias de Amazon EC2. La política de la empresa requiere que el grupo de seguridad de las instancias del clúster bloquee todo el tráfico entrante excepto HTTPS (puerto 443).

¿Qué solución cumplirá con estos requisitos?

A) Cambiar el puerto SSH a 2222 en las instancias del clúster mediante un script de datos del usuario. Iniciar sesión en cada instancia mediante el uso de SSH a través del puerto 2222.
B) Cambiar el puerto SSH a 2222 en las instancias del clúster mediante un script de datos del usuario. Utilizar AWS Trusted Advisor para administrar de forma remota las instancias del clúster a través del puerto 2222.
C) Lanzar las instancias del clúster sin pares de claves SSH. Utilizar AWS Systems Manager Run Command para administrar de forma remota las instancias del clúster.
D) Lanzar las instancias del clúster sin pares de claves SSH. Utilizar AWS Trusted Advisor para administrar de forma remota las instancias del clúster.

6) Una empresa tiene dos cuentas de AWS: una para cargas de trabajo de producción y otra para cargas de trabajo de desarrollo. Un equipo de desarrollo y un equipo de operaciones crean y administran estas cargas de trabajo. La empresa necesita una estrategia de seguridad que cumpla los siguientes requisitos:

- **Los desarrolladores deben crear y eliminar la infraestructura de aplicaciones de desarrollo.**
- **Los operadores deben crear y eliminar la infraestructura de aplicaciones de desarrollo y la de producción.**
- **Los desarrolladores no deben tener acceso a la infraestructura de producción.**
- **Todos los usuarios deben tener un conjunto único de credenciales de AWS.**

¿Qué estrategia cumplirá con estos requisitos?

A) En la cuenta de producción:
- Crear un grupo de IAM de operaciones que pueda crear y eliminar la infraestructura de aplicaciones.
- Crear un usuario de IAM para cada operador. Asignar estos usuarios al grupo de operaciones.

En la cuenta de desarrollo:
- Crear un grupo de IAM de desarrollo que pueda crear y eliminar la infraestructura de aplicaciones.
- Crear un usuario de IAM para cada operador y desarrollador. Asignar estos usuarios al grupo de desarrollo.

B) En la cuenta de producción:
- Crear un grupo de IAM de operaciones que pueda crear y eliminar la infraestructura de aplicaciones.

En la cuenta de desarrollo:
- Crear un grupo de IAM de desarrollo que pueda crear y eliminar la infraestructura de aplicaciones.
- Crear un usuario de IAM para cada desarrollador. Asignar estos usuarios al grupo de desarrollo.
- Crear un usuario de IAM para cada operador. Asignar estos usuarios al grupo de desarrollo y al grupo de operaciones en la cuenta de producción.

C) En la cuenta de desarrollo:
- Crear un rol de IAM compartido que pueda crear y eliminar la infraestructura de aplicaciones en la cuenta de producción.
- Crear un grupo de IAM de desarrollo que pueda crear y eliminar la infraestructura de aplicaciones.
- Crear un grupo de IAM de operaciones que pueda asumir el rol compartido.
- Crear un usuario de IAM para cada desarrollador. Asignar estos usuarios al grupo de desarrollo.
- Crear un usuario de IAM para cada operador. Asignar estos usuarios al grupo de desarrollo y al grupo de operaciones.

D) En la cuenta de producción:
- Crear un rol de IAM compartido que pueda crear y eliminar la infraestructura de aplicaciones.
- Agregar la cuenta de desarrollo a la política de confianza del rol compartido.

En la cuenta de desarrollo:
- Crear un grupo de IAM de desarrollo que pueda crear y eliminar la infraestructura de aplicaciones.
- Crear un grupo de IAM de operaciones con la capacidad de asumir el rol compartido en la cuenta de producción.
- Crear un usuario de IAM para cada desarrollador. Asignar estos usuarios al grupo de desarrollo.
- Crear un usuario de IAM para cada operador. Asignar estos usuarios al grupo de desarrollo y al grupo de operaciones.

7) Un arquitecto de soluciones necesita reducir los costos de una aplicación big data. El entorno de la aplicación consta de cientos de dispositivos que envían eventos a Amazon Kinesis Data Streams. El ID del dispositivo se utiliza como clave de partición, de modo que cada dispositivo recibe una partición diferente. Cada dispositivo envía entre 50 KB y 450 KB de datos por segundo. Una función de AWS Lambda obtiene las particiones, procesa los datos y almacena el resultado en Amazon S3.

Cada hora, otra función de Lambda ejecuta una consulta de Amazon Athena y compara con los datos de los resultados para identificar los valores atípicos. Esta función de Lambda coloca los valores atípicos en una cola de Amazon Simple Queue Service (Amazon SQS). Un grupo de Amazon EC2 Auto Scaling de dos instancias EC2 monitorea la cola y ejecuta un proceso de 30 segundos de duración para resolver los valores atípicos. Los dispositivos envían un promedio de 10 valores atípicos por hora.

¿Qué combinación de cambios en la aplicación reducirá MÁS los costos? (Seleccione DOS).

A) Cambiar la configuración de lanzamiento del grupo de Auto Scaling para utilizar tipos de instancias más pequeñas en la misma familia de instancias.
B) Reemplazar el grupo de Auto Scaling por una función de Lambda que se invoca cuando los mensajes llegan a la cola.
C) Volver a configurar los dispositivos y el flujo de datos para establecer una proporción de 10 dispositivos por cada partición de flujo de datos.
D) Volver a configurar los dispositivos y el flujo de datos para establecer una proporción de 2 dispositivos por cada partición de flujo de datos.
E) Cambiar la capacidad deseada del grupo de Auto Scaling a una sola instancia EC2.

8) Una empresa opera una aplicación de comercio electrónico en instancias de Amazon EC2 detrás de un Application Load Balancer. Las instancias se ejecutan en un grupo de Amazon EC2 Auto Scaling en varias zonas de disponibilidad. Después de que un pedido se haya procesado con éxito, la aplicación publica de forma inmediata los datos del pedido en un sistema externo de seguimiento de filiales de terceros que paga comisiones de ventas por referencias de pedidos.

Durante una promoción de marketing exitosa, el número de instancias EC2 aumentó de 2 a 20. La aplicación siguió funcionando correctamente durante este tiempo. Sin embargo, el aumento de la tasa de solicitudes saturó la filial del tercero y provocó solicitudes fallidas.

¿Qué combinación de cambios arquitectónicos debe realizar un arquitecto de soluciones para garantizar que todo el proceso funcione correctamente bajo carga? (Seleccione DOS).

A) Cambiar el código que llama a la filial por una nueva función de AWS Lambda. Modificar la aplicación para invocar la función de Lambda de forma asíncrona.
B) Cambiar el código que llama a la filial por una nueva función de AWS Lambda. Modificar la aplicación para colocar los datos del pedido en una cola de Amazon Simple Queue Service (Amazon SQS). Invocar la función de Lambda desde la cola.
C) Aumentar el tiempo de espera de la nueva función de AWS Lambda.
D) Reducir la concurrencia reservada de la nueva función de AWS Lambda.
E) Aumentar la memoria de la nueva función de AWS Lambda.

9) Una empresa creó una aplicación web de venta de entradas en línea en AWS. La aplicación está alojada en AWS App Runner y utiliza imágenes que se almacenan en un repositorio de Amazon Elastic Container Registry (Amazon ECR). La aplicación almacena datos en un clúster MySQL DB de Amazon Aurora. La empresa configuró un nombre de dominio en Amazon Route 53.

La empresa necesita implementar la aplicación en dos regiones de AWS en una configuración Active-Active.

¿Qué combinación de pasos cumplirá con estos requisitos con el MENOR cambio en la arquitectura? (Seleccione TRES).

A) Configurar Cross-Region Replication en la segunda región para las imágenes ECR.
B) Crear un punto de enlace de la VPC desde el repositorio de ECR en la segunda región.
C) Editar la configuración de App Runner y agregar un segundo destino de implementación a la segunda región.
D) Implementar App Runner en la segunda región. Configurar el enrutamiento basado en latencia de Route 53.
E) Cambiar la base de datos mediante tablas globales de Amazon DynamoDB en las dos regiones deseadas.
F) Utilizar una base de datos global de Aurora con una habilitación para el reenvío de escritura en la segunda región.

10) Una empresa implementó una aplicación web de varios niveles en la nube de AWS. La aplicación está compuesta por los siguientes niveles:

- **Un nivel web basado en Windows que se aloja en instancias de Amazon EC2 con direcciones IP elásticas**
- **Un nivel de aplicación basado en Linux que se aloja en instancias EC2 y que se ejecutan detrás de un Application Load Balancer (ALB) que utiliza enrutamiento basado en rutas**
- **Una base de datos MySQL que se ejecuta en una instancia EC2 de Linux**

Todas las instancias EC2 utilizan CPU x86 basadas en Intel. Un arquitecto de soluciones necesita modernizar la infraestructura para lograr un mejor rendimiento. La solución debe minimizar la sobrecarga operativa de la aplicación.

¿Qué combinación de acciones debe realizar el arquitecto de soluciones para cumplir con estos requisitos? (Seleccione DOS).

A) Ejecutar la base de datos MySQL en varias instancias EC2.
B) Colocar las instancias de nivel web detrás de un ALB.
C) Migrar la base de datos MySQL a Amazon Aurora Serverless.
D) Migrar todos los tipos de instancias EC2 a Graviton2.
E) Reemplazar el ALB para las instancias de nivel de aplicación por un equilibrador de carga administrado por la empresa.

Respuestas

1) C: las alarmas de facturación proporcionarán a la empresa alertas sobre gastos excesivos sin quitarle el control a ninguno de los grupos empresariales. Las opciones A y B son incorrectas porque cada grupo empresarial quiere retener el control de su cuenta. Estas opciones no impedirían el lanzamiento de una gran cantidad de instancias. La opción D es un proceso manual que no proporcionaría alertas inmediatas sobre gastos excesivos.

2) D: AWS CloudFormation StackSets puede implementar el rol de IAM en varias cuentas con una sola operación. La opción A es incorrecta porque las credenciales que proporciona AWS Single Sign-On (AWS SSO) son temporales. La aplicación perdería los permisos y tendría que volver a iniciar sesión. La opción B concedería acceso únicamente a la cuenta de administración. La opción C es incorrecta porque cuando una cuenta se une a una organización, la cuenta no recibe permisos para acceder a las demás cuentas de la organización.

3) D, E: el intercambio de recursos de origen cruzado (CORS) es una característica de seguridad del navegador que restringe las solicitudes HTTP que se inician desde scripts que se ejecutan en el navegador. Por lo general, se utiliza el CORS para crear aplicaciones web que accedan a las API alojadas en un dominio u origen diferente. Puede habilitar el CORS para permitir solicitudes a su API desde una aplicación web que esté alojada en un dominio diferente.
Por ejemplo, si su API está alojada en https://[api_id].execute-api.[region].amazonaws.com/ y quiere llamarla desde una aplicación web alojada en [bucketname].s3.website-[region], la API debe admitir el CORS. La opción E es necesaria para que se envíe el formulario HTML mediante un punto de enlace del sitio web.

La opción A es incorrecta porque el encabezado CORS debe configurarse para ser arrojado por la respuesta dinámica del punto de enlace de API. La configuración del CORS para el S3 Bucket no ayuda. La opción B es incorrecta porque no tiene ninguna ventaja servir una página web estática desde un servidor web que se ejecuta con Amazon EC2 en lugar de hacerlo desde un S3 Bucket. La opción C es incorrecta porque API Gateway tiene una cuota predeterminada de 10 000 solicitudes por segundo para cada región de AWS. Si es necesario, puede aumentar esta cuota.

4) A: Amazon API Gateway mostrará de forma intermitente los errores del código de estado HTTP 502 (Bad Gateway) si la función de AWS Lambda supera la cuota de concurrencia. La opción B es incorrecta porque, en este caso, API Gateway mostraría un error de código de estado 429 por exceso de solicitudes. La opción C es incorrecta porque los errores se producen durante las llamadas al punto de enlace de API de API Gateway, no durante el proceso de autenticación. La opción D es incorrecta porque los datos obsoletos no provocarían un error del tipo Bad Gateway.

5) C: AWS Systems Manager Run Command no requiere que se abran puertos de entrada. Run Command funciona completamente a través de HTTPS de salida, que está abierto de forma predeterminada para los grupos de seguridad. Las opciones A y B son incorrectas porque los requisitos indican que el único puerto de entrada que debe estar abierto es el 443. La opción D es incorrecta porque AWS Trusted Advisor no realiza esta función de administración.

6) D: la respuesta correcta sigue las pautas estándar para otorgar acceso cruzado entre dos cuentas que usted controla. La opción A no cumple con los requisitos porque requiere dos conjuntos de credenciales para los operadores. La opción B es incorrecta porque no puede agregar un usuario de IAM a un grupo de IAM en una cuenta diferente. La opción C es incorrecta porque un rol no puede otorgar acceso a los recursos de otra cuenta. El rol compartido debe estar en la misma cuenta con los recursos que administra.

7) B, D: la cantidad media de cómputo para abordar los valores atípicos cada hora es de 300 segundos (10 eventos de 30 segundos cada uno). La opción B es correcta porque con AWS Lambda solo paga por la pequeña cantidad de tiempo de cómputo que se requiere para procesar los valores atípicos. Si bien las opciones A y E reducirían los costos, ambas implican pagar por una o más instancias de Amazon EC2 que permanecerían sin uso durante 3300 segundos cada hora. Las opciones C y D reducen los costos de partición por hora del flujo de datos de Kinesis. Sin embargo, la opción C es incorrecta porque la cantidad de datos superaría la cuota de 1 MB/s de una sola partición.

8) B, D: en la opción B, el uso de una cola de Amazon Simple Queue Service (Amazon SQS) desconectará la aplicación principal de las llamadas al afiliado. Este cambio protegerá la aplicación principal de la capacidad reducida del afiliado. Además, las solicitudes fallidas pueden volver automáticamente a la cola. En la opción D, una reducción del número de invocaciones simultáneas evitará que la aplicación del afiliado se vea sobrepasada.

Si bien la opción A reducirá la carga en las instancias de Amazon EC2, esta solución no reducirá el número de solicitudes a la aplicación del afiliado. Aunque la opción C permitirá que la función de AWS Lambda espere más tiempo a que regrese la llamada externa, esta solución no reducirá la carga en la aplicación desbordada del afiliado. La opción E es incorrecta porque un aumento en la memoria no afectará la interacción entre la función de Lambda y el sistema de seguimiento de los afiliados.

9) A, D, F: AWS App Runner es un servicio totalmente administrado que los desarrolladores pueden utilizar para implementar con rapidez aplicaciones web en contenedores con imágenes que se almacenan en un repositorio de Amazon Elastic Container Registry (Amazon ECR). La opción A es correcta porque Cross-Region Replication hace una copia del repositorio en una segunda región de AWS. La opción D es correcta porque puede usar Route 53 para alojar el nombre de dominio personalizado y enrutar el tráfico a los recursos en varias regiones de AWS. La opción F es correcta porque las Amazon Aurora Global Databases se extienden a través de varias regiones y están diseñadas para aplicaciones distribuidas globalmente.

La opción B es incorrecta porque un punto de enlace de la VPC no proporcionará acceso a una imagen que esté almacenada en una región diferente. En la opción C, no existe tal configuración en App Runner. Aunque la opción E funcionaría, la introducción de Amazon DynamoDB requeriría más cambios en la arquitectura que el uso de una base de datos global de Aurora. La pregunta pide el menor cambio posible en la arquitectura.

10) B, C: en la opción B, al colocar el nivel web detrás de un Application Load Balancer (ALB), puede mejorar la disponibilidad y la escalabilidad del nivel web. El ALB sirve como el único punto de contacto para los clientes y distribuye el tráfico de aplicaciones entrante a las instancias de Amazon EC2. La opción C es correcta porque Amazon Aurora Serverless proporciona un alto rendimiento y una alta disponibilidad con una complejidad operativa reducida.

La opción A es incorrecta porque las instancias EC2 adicionales no minimizarán la sobrecarga operativa. Un servicio administrado sería una mejor opción. La opción D es incorrecta porque la aplicación incluye instancias de Windows, las cuales no están disponibles para Graviton2. La opción E es incorrecta porque un equilibrador de carga administrado por la empresa no minimizará la sobrecarga operativa.