

1) Une entreprise exécute une application web à trois niveaux, destinée au public, dans un VPC sur plusieurs zones de disponibilité. Les instances Amazon EC2 pour le niveau Application qui s'exécutent dans des sous-réseaux privés doivent télécharger des correctifs logiciels depuis Internet. Toutefois, les instances EC2 ne peuvent pas être directement accessibles à partir d'Internet.

Quelles mesures doivent être prises pour permettre aux instances EC2 de télécharger les correctifs nécessaires ? (Sélectionnez DEUX réponses.)

- A) Configurer une passerelle NAT dans un sous-réseau public.
- B) Définir une table de routage personnalisée avec une route vers la passerelle NAT pour le trafic Internet et l'associer aux sous-réseaux privés pour le niveau Application.
- C) Attribuer des adresses IP Elastic aux instances EC2.
- D) Définir une table de routage personnalisée avec une route vers la passerelle Internet pour le trafic Internet et l'associer aux sous-réseaux privés pour le niveau Application.
- E) Configurer une instance NAT dans un sous-réseau privé.

2) Un architecte de solutions souhaite concevoir une solution permettant de réduire les coûts pour les instances Amazon EC2 qui n'ont pas besoin d'être exécutées pendant une période de fermeture de l'entreprise d'une durée de 2 semaines. stockent des données dans la mémoire des instances qui doivent être présentes lorsque les instances sont remises en route.

Quelle approche l'architecte de solutions doit-il recommander pour l'arrêt et la reprise des instances EC2 ?

- A) Modifier l'application pour stocker les données sur les volumes de stockage d'instance. Rattacher à nouveau les volumes lors de leur redémarrage.
- B) Réaliser un instantané des instances EC2 avant de les arrêter. Restaurer l'instantané après le redémarrage des instances.
- C) Exécuter les applications sur les instances EC2 activées pour la mise en veille prolongée. Mettre les instances en veille prolongée avant la fermeture de 2 semaines de l'entreprise.
- D) Noter la zone de disponibilité pour chaque instance EC2 avant de l'arrêter. Redémarrer les instances dans les mêmes zones de disponibilité après la fermeture de 2 semaines de l'entreprise.

3) Une entreprise envisage d'exécuter une application de surveillance sur une instance Amazon EC2 dans un VPC. Les connexions sont établies vers l'instance EC2 à l'aide de l'adresse IPv4 privée de l'instance. Un architecte de solutions doit concevoir une solution qui permettra de diriger rapidement le trafic vers une instance EC2 de secours si l'application échoue et devient inaccessible.

Quelle approche répondra à ces exigences ?

- A) Déployer un Application Load Balancer configuré avec un écouteur pour l'adresse IP privée et enregistrer l'instance EC2 principale auprès de l'équilibreur de charge. En cas d'échec, annuler l'enregistrement de l'instance et enregistrer l'instance EC2 de secours.
- B) Configurer un jeu d'options DHCP personnalisé. Configurer DHCP pour attribuer la même adresse IP privée à l'instance EC2 de secours lorsque l'instance EC2 principale échoue.
- C) Attacher une interface réseau Elastic secondaire à l'instance EC2 configurée avec l'adresse IP privée. Déplacer l'interface réseau vers l'instance EC2 de secours si l'instance EC2 principale devient inaccessible.
- D) Associer une adresse IP Elastic à l'interface réseau de l'instance EC2 principale. Dissocier l'adresse IP Elastic de l'instance principale en cas d'échec et l'associer à une instance EC2 de secours.

4) Une société spécialisée dans l'analytique envisage de proposer un service d'analytique web à ses utilisateurs. Le service exigera que les pages web des utilisateurs incluent un script JavaScript envoyant des requêtes GET authentifiées au compartiment Amazon S3 de l'entreprise.

Que doit faire l'architecte de solutions pour s'assurer que le script s'exécutera correctement ?

- A) Activer le partage des ressources cross-origine (CORS) sur le compartiment S3.
- B) Activer le contrôle de version S3 sur le compartiment S3.
- C) Fournir aux utilisateurs une URL signée pour le script.
- D) Configurer une politique de compartiment S3 autorisant les privilèges d'exécution publique.

5) L'équipe de sécurité d'une entreprise exige que toutes les données stockées dans le cloud soient chiffrées au repos en permanence à l'aide de clés de chiffrement stockées sur site.

Quelles options de chiffrement répondent à ces exigences ? (Sélectionnez DEUX réponses.)

- A) Utiliser le chiffrement côté serveur avec les clés de chiffrement gérées par Amazon S3 (SSE-S3).
- B) Utiliser le chiffrement côté serveur avec les clés gérées par AWS KMS (SSE-KMS).
- C) Utiliser le chiffrement côté serveur avec les clés de chiffrement fournies par le client (SSE-C).
- D) Utiliser le chiffrement côté client pour fournir un chiffrement au repos.
- E) Utiliser une fonction AWS Lambda invoquée par les événements Amazon S3 pour chiffrer les données à l'aide des clés du client.

6) Une entreprise utilise des instances réservées Amazon EC2 pour exécuter sa charge de travail de traitement des données. Réalisée la nuit, l'exécution de cette tâche prend généralement 7 heures et doit se terminer dans une plage horaire de 10 heures. L'entreprise prévoit des augmentations temporaires de la demande à la fin de chaque mois. Avec les ressources actuelles, l'exécution de la tâche va donc dépasser la plage horaire. Une fois démarrée, la tâche de traitement ne peut pas être interrompue. L'entreprise souhaite mettre en œuvre une solution qui permettrait d'augmenter la capacité des ressources de la manière la plus rentable possible.

Comment l'architecte de solutions peut-il parvenir à cet objectif ?

- A) Déployer des instances à la demande pendant les périodes de forte demande.
- B) Créer une deuxième réservation EC2 pour les instances supplémentaires.
- C) Déployer des instances Spot pendant les périodes de forte demande.
- D) Augmenter la taille des instances EC2 de la réservation EC2 pour prendre en charge l'augmentation de la charge de travail.

7) Une entreprise gère un système de vote en ligne pour une émission télévisée hebdomadaire en direct. Lors des diffusions, les utilisateurs soumettent des centaines de milliers de votes en quelques minutes à une flotte frontale d'instances Amazon EC2 exécutées dans un groupe Auto Scaling. Les instances EC2 écrivent les votes dans une base de données Amazon RDS. Toutefois, la base de données n'est pas en mesure de répondre aux demandes provenant des instances EC2. Un architecte de solutions doit concevoir une solution qui permette de traiter les votes de la manière la plus efficace possible et sans temps d'arrêt.

Quelle solution répond à ces conditions ?

- A) Migrer l'application frontale vers AWS Lambda. Utiliser Amazon API Gateway pour acheminer les demandes des utilisateurs vers les fonctions Lambda.
- B) Effectuer une mise à l'échelle horizontale de la base de données en la convertissant en déploiement multi-AZ. Configurer l'application frontale pour écrire à la fois sur les instances de base de données principales et secondaires.
- C) Configurer l'application frontale pour envoyer les votes vers une file d'attente Amazon Simple Queue Service (Amazon SQS). Mettre en service des instances de worker pour lire la file d'attente SQS et écrire les informations de vote dans la base de données.
- D) Utiliser Amazon EventBridge (Amazon CloudWatch Events) pour créer un événement planifié afin de réapprovisionner la base de données en instances plus grandes et optimisées en mémoire pendant les périodes de vote. À la fin du vote, réapprovisionner la base de données en instances plus petites.

8) Une entreprise possède une architecture d'application à deux niveaux qui s'exécute dans des sous-réseaux publics et privés. Les instances Amazon EC2 exécutant l'application web se trouvent dans le sous-réseau public et une instance EC2 de la base de données s'exécute sur le sous-réseau privé. Les instances de l'application web et la base de données s'exécutent dans une même zone de disponibilité (AZ).

Quelle combinaison d'étapes un architecte de solutions doit-il mettre en œuvre pour assurer la haute disponibilité de cette architecture ? (Sélectionnez DEUX réponses.)

- A) Créer de nouveaux sous-réseaux publics et privés dans la même zone de disponibilité.
- B) Créer un groupe Auto Scaling Amazon EC2 et un Application Load Balancer couvrant plusieurs zones de disponibilité pour les instances de l'application web.
- C) Ajouter les instances de l'application web existantes à un groupe Auto Scaling derrière un Application Load Balancer.
- D) Créer de nouveaux sous-réseaux publics et privés dans une nouvelle zone de disponibilité. Créer une base de données à l'aide d'une instance EC2 du sous-réseau public de la nouvelle zone de disponibilité. Migrer le contenu de l'ancienne base de données vers la nouvelle.
- E) Créer de nouveaux sous-réseaux publics et privés dans le même VPC, chacun dans une nouvelle zone de disponibilité. Créer une instance de bases de données multi-AZ Amazon RDS dans les sous-réseaux privés. Migrer le contenu de l'ancienne base de données vers la nouvelle instance de base de données.

9) Un site web exécute une application web personnalisée qui reçoit un pic de trafic chaque jour à midi. Les utilisateurs chargent quotidiennement de nouvelles images et de nouveaux contenus, mais se plaignent des délais d'attente. L'architecture utilise des groupes Auto Scaling Amazon EC2, et, au démarrage, l'application met systématiquement 1 minute à répondre aux demandes des utilisateurs.

De quelle façon un architecte de solutions doit-il repenser l'architecture pour mieux répondre à l'évolution du trafic ?

- A) Configurer un Network Load Balancer avec une configuration de démarrage lent.
- B) Configurer Amazon ElastiCache for Redis afin de décharger les instances EC2 des demandes directes.
- C) Configurer une politique de mise à l'échelle par étapes de l'Auto Scaling avec une condition de préchauffage des instances EC2.
- D) Configurer Amazon CloudFront pour utiliser un Application Load Balancer comme origine.

10) Une application exécutée sur AWS utilise un déploiement de cluster de bases de données multi-AZ Amazon Aurora pour sa base de données. Lors de l'évaluation des métriques de performance, un architecte de solutions découvre que les lectures de la base de données entraînent des I/O élevées et ajoutent de la latence aux demandes d'écriture sur la base de données.

Que doit faire l'architecte de solutions pour séparer les demandes de lecture des demandes d'écriture ?

- A) Activer la mise en cache en lecture directe sur la base de données Aurora.
- B) Mettre à jour l'application afin qu'elle lise à partir de l'instance de secours multi-AZ.
- C) Créer un réplica Aurora et modifier l'application afin qu'elle utilise les points de terminaison appropriés.
- D) Créer une deuxième base de données Aurora et la lier à la base de données principale en tant que réplica en lecture.

Réponses

- 1) A, B – Une [passerelle NAT](#) transfère le trafic des instances EC2 du sous-réseau privé vers Internet ou d'autres services AWS, puis renvoie la réponse aux instances. Après la création d'une passerelle NAT, les tables de routage des sous-réseaux privés doivent être mises à jour pour diriger le trafic Internet vers la passerelle NAT.
- 2) C – Les instances EC2 [mises en veille prolongée](#) enregistrent le contenu de la mémoire de l'instance sur un volume racine Amazon Elastic Block Store (Amazon EBS). Lorsque les instances redémarrent, le contenu de la mémoire de l'instance est rechargé.
- 3) C – Une [interface réseau Elastic secondaire](#) peut être ajoutée à une instance EC2. Les interfaces réseau principales ne peuvent pas être détachées d'une instance. Les interfaces réseau secondaires, quant à elles, peuvent être détachées et attachées à une instance EC2 différente.
- 4) A – Les navigateurs web bloquent l'exécution d'un script provenant d'un serveur dont le nom de domaine est différent de celui de la page web. [Amazon S3 peut être configuré avec CORS](#) pour envoyer des en-têtes HTTP autorisant l'exécution du script.
- 5) C, D – [Le chiffrement côté serveur avec des clés fournies par le client \(SSE-C\)](#) permet à Amazon S3 de chiffrer les objets côté serveur à l'aide d'une clé de chiffrement fournie dans la requête PUT. La même clé doit être fournie dans les requêtes GET pour qu'Amazon S3 déchiffre l'objet. Les clients ont également la possibilité de chiffrer les données côté client avant de les télécharger sur Amazon S3. Ils peuvent ensuite les déchiffrer après les avoir téléchargées. Les AWS software development kits (SDK) fournissent un client de chiffrement S3 qui simplifie le processus.
- 6) A – Bien que les [instances Spot](#) constituent l'option la moins coûteuse, elles ne conviennent pas aux tâches qui ne peuvent pas être interrompues ou qui doivent s'exécuter pendant une période donnée. La facturation des [instances à la demande](#) est basée sur le nombre de secondes pendant lesquelles elles s'exécutent.
- 7) C – [Découplez](#) l'ingestion des votes de la base de données pour permettre au système de vote de continuer à traiter les votes sans attendre les écritures dans la base de données. Ajoutez des workers dédiés pour lire les éléments de la [file d'attente SQS](#) et permettre la saisie des votes dans la base de données à un rythme contrôlable. Les votes seront ajoutés à la base de données dès que cette dernière pourra les traiter, mais aucun vote ne sera perdu.
- 8) B, E – Créez de nouveaux sous-réseaux dans une nouvelle zone de disponibilité (AZ) pour fournir un réseau redondant. Créez un [groupe Auto Scaling avec des instances dans deux zones de disponibilité derrière l'équilibreur de charge](#) afin de garantir la haute disponibilité de l'application web et la redistribution du trafic web entre les deux zones de disponibilité publiques. Créez une instance de base de données RDS dans les deux sous-réseaux privés pour rendre le [niveau de base de données hautement disponible](#) également.
- 9) C – La configuration actuelle met en service de nouvelles instances EC2 avant qu'elles ne soient en mesure de répondre aux transactions. Cela peut également entraîner un surdimensionnement des instances. Les [politiques de mise à l'échelle par étapes](#) vous permettent de spécifier le nombre de secondes nécessaires pour qu'une instance nouvellement lancée [se prépare](#). Une instance EC2 n'est pas comptée dans les métriques regroupées du groupe Auto Scaling tant que sa période de préparation, telle qu'elle est spécifiée, n'est pas arrivée à expiration. Lors de la mise à l'échelle horizontale, la logique Auto Scaling ne prend pas en compte les instances EC2 qui se préparent comme faisant partie de la capacité actuelle du groupe Auto Scaling. Par conséquent, plusieurs seuils d'alarme présents dans la plage d'un même ajustement par étape génèrent une activité de mise à l'échelle unique. Cela permet d'être sûr de ne pas ajouter plus d'instances que nécessaire.

AWS Certified Solutions Architect - Associate (SAA-C03)

Exemples de questions pour l'examen

10) C – Les [réplicas Aurora](#) permettent de décharger le trafic en lecture. Les réplicas Aurora partagent le même [stockage sous-jacent](#) que la base de données principale. Le temps de latence est ainsi généralement très faible. Les réplicas Aurora possèdent leurs propres points de terminaison. L'application devra donc être configurée pour diriger le trafic en lecture vers les nouveaux points de terminaison.