1) Un'azienda dispone di molti account AWS che vengono assegnati ai singoli gruppi aziendali. Uno degli account è stato recentemente compromesso. L'aggressore ha lanciato un gran numero di istanze, con conseguente incremento in fattura per quell'account.

L'azienda ha affrontato la violazione della sicurezza, ma un Solutions Architect deve sviluppare una soluzione che prevenga spese eccessive in tutti gli account. Ogni gruppo aziendale vuole mantenere il pieno controllo del proprio account AWS.

Quale soluzione deve consigliare un Solutions Architect per soddisfare questi requisiti?

A) Utilizzare AWS Organizations. Aggiungere ogni account AWS all'account di gestione. Creare una policy di controllo dei servizi (SCP) che utilizzi la chiave di condizione ec2:instanceType per impedire l'avvio di tipi di istanza ad alto costo in ciascun account.
B) Collegare una nuova policy IAM gestita dal cliente a un gruppo IAM in ogni account. Configurare la policy per utilizzare la chiave di condizione ec2:instanceType per prevenire il lancio di tipi di istanze ad alto costo. Posizionare tutti gli utenti IAM esistenti in ciascun gruppo.
C) Attivare gli avvisi di fatturazione per ogni account AWS. Creare allarmi Amazon CloudWatch per inviare una notifica Amazon Simple Notification Service (Amazon SNS) all'amministratore dell'account ogni volta che l'account supera una soglia di spesa designata.
D) Attivare AWS Cost Explorer in ogni account. Esaminare regolarmente i report di Cost Explorer per ciascun account per essere certi che la spesa non superi l'importo desiderato.

2) Un'azienda dispone di più account AWS in un'organizzazione di AWS Organizations. L'azienda ha integrato il suo Active Directory on-premise con AWS Single Sign-On (AWS SSO) per concedere agli utenti di Active Directory autorizzazioni di privilegio minime per gestire l'infrastruttura su tutti gli account.

Un Solutions Architect deve integrare una soluzione di monitoraggio di terze parti che richiede l'accesso in sola lettura su tutti gli account AWS. La soluzione di monitoraggio verrà eseguita nel proprio account AWS.

Cosa deve fare il Solutions Architect per fornire la soluzione di monitoraggio con le autorizzazioni richieste?

A) Creare un utente in una directory AWS SSO. Assegnare all'utente un set di autorizzazioni in sola lettura. Assegnare all'utente tutti gli account AWS che devono essere monitorati. Fornire alla soluzione di monitoraggio di terze parti il nome utente e la password.
B) Creare un ruolo IAM nell'account di gestione dell'organizzazione. Consentire all'account AWS della soluzione di monitoraggio di terze parti di assumere il ruolo.
C) Invitare l'account AWS della soluzione di monitoraggio di terze parti ad aderire all'organizzazione. Abilitare tutte le funzionalità.
D) Creare un template AWS CloudFormation che definisca un nuovo ruolo IAM per la soluzione di monitoraggio di terze parti. Specificare l'account AWS della soluzione di monitoraggio di terze parti nella policy di attendibilità. Creare il ruolo IAM su tutti gli account AWS collegati utilizzando un set di stack.

© 2022, Amazon Web Services, Inc. o sue affiliate. Tutti i diritti riservati | aws.amazon.com

3) Un team sta costruendo un modulo HTML ospitato in un bucket Amazon S3 pubblico. Il modulo utilizza JavaScript per pubblicare dati su un endpoint API Amazon API Gateway. L'endpoint API è integrato con le funzioni AWS Lambda. Il team ha testato ogni metodo nella console API Gateway e ha ricevuto risposte valide.

Quale combinazione di passaggi deve completare il team affinché il modulo possa essere pubblicato correttamente nell'endpoint API e ricevere una risposta valida? (Seleziona DUE risposte.)

A) Configurare il bucket S3 per consentire cross-origin resource sharing (CORS).
B) Ospitare il modulo su Amazon EC2 anziché su Amazon S3.
C) Richiedere un aumento della quota per API Gateway.
D) Abilitare la Cross-Origin Resource Sharing (CORS) nell'API Gateway.
E) Configurare il bucket S3 per il web hosting.

4) Una società gestisce un'applicazione per dispositivi mobili serverless basata su Amazon API Gateway, funzioni AWS Lambda, Amazon Cognito e Amazon DynamoDB. Durante grandi picchi di traffico, gli utenti segnalano guasti intermittenti del sistema. L'endpoint API Gateway API restituisce errori con codice di stato HTTP 502 (gateway non valido) alle richieste valide.

Quale soluzione risolverà il problema?

A) Aumentare la quota di concorrenza per le funzioni Lambda. Configurare Amazon CloudWatch per l'invio di avvisi di notifica quando la metrica ConcurrentExecutions si avvicina alla quota.
B) Configurare gli avvisi di notifica per la quota di transazioni al secondo sull'endpoint API Gateway API. Creare una funzione Lambda che aumenterà la quota quando sarà raggiunta.
C) Condividere gli utenti con i pool di utenti Amazon Cognito in più regioni AWS per ridurre la latenza dell'autenticazione utente.
D) Utilizzare letture fortemente consistenti di DynamoDB per garantire che l'applicazione client riceva sempre i dati più recenti.

5) Un'azienda sta lanciando un nuovo servizio web su un cluster Amazon Elastic Container Service (Amazon ECS). Il cluster è composto da 100 istanze Amazon EC2. La policy aziendale richiede che il gruppo di sicurezza sulle istanze cluster blocchi tutto il traffico in entrata tranne il traffico HTTPS (porta 443).

Quale soluzione soddisfa questi requisiti?

A) Passare alla porta SSH 2222 sulle istanze cluster utilizzando uno script di dati utente. Accedere a ciascuna istanza utilizzando l'SSH sulla porta 2222.
B) Passare alla porta SSH 2222 sulle istanze cluster utilizzando uno script di dati utente. Usare AWS Trusted Advisor per gestire da remoto le istanze cluster sulla porta 2222.
C) Avviare le istanze cluster senza coppie di chiavi SSH. Utilizzare AWS Systems Manager Run Command per gestire da remoto le istanze cluster.
D) Avviare le istanze cluster senza coppie di chiavi SSH. Usare AWS Trusted Advisor per gestire in remoto le istanze cluster.

© 2022, Amazon Web Services, Inc. o sue affiliate. Tutti i diritti riservati | aws.amazon.com

6) Un'azienda ha due account AWS: uno per i carichi di lavoro di produzione e uno per i carichi di lavoro di sviluppo. Un team di sviluppo e un team operativo creano e gestiscono questi carichi di lavoro. L'azienda ha bisogno di una strategia di sicurezza che soddisfi i seguenti requisiti:

- **Gli sviluppatori devono creare ed eliminare l'infrastruttura delle applicazioni di sviluppo.**
- **Gli operatori devono creare ed eliminare l'infrastruttura delle applicazioni, sia di sviluppo che di produzione.**
- **Gli sviluppatori non devono avere accesso all'infrastruttura di produzione.**
- **Tutti gli utenti devono disporre di un unico set di credenziali AWS.**

Quale strategia soddisferà questi requisiti?

A) Nell'account di produzione:
- Istituire un gruppo IAM operativo in grado di creare ed eliminare l'infrastruttura delle applicazioni.
- Creare un utente IAM per ogni operatore. Assegnare questi utenti al gruppo operativo.

Nell'account di sviluppo:
- Creare un gruppo IAM di sviluppo in grado di creare ed eliminare l'infrastruttura dell'applicazione.
- Creare un utente IAM per ogni operatore e sviluppatore. Assegnare questi utenti al gruppo di sviluppo.

B) Nell'account di produzione:
- Istituire un gruppo IAM operativo in grado di creare ed eliminare l'infrastruttura delle applicazioni.

Nell'account di sviluppo:
- Creare un gruppo IAM di sviluppo in grado di creare ed eliminare l'infrastruttura dell'applicazione.
- Creare un utente IAM per ogni sviluppatore. Assegnare questi utenti al gruppo di sviluppo.
- Creare un utente IAM per ogni operatore. Assegnare questi utenti al gruppo di sviluppo e al gruppo operativo nell'account di produzione.

C) Nell'account di sviluppo:
- Creare un ruolo IAM condiviso in grado di creare ed eliminare l'infrastruttura dell'applicazione nell'account di produzione.
- Creare un gruppo IAM di sviluppo in grado di creare ed eliminare l'infrastruttura dell'applicazione.
- Creare un gruppo IAM delle operazioni in grado di assumere il ruolo condiviso.
- Creare un utente IAM per ogni sviluppatore. Assegnare questi utenti al gruppo di sviluppo.
- Creare un utente IAM per ogni operatore. Assegnare questi utenti al gruppo di sviluppo e al gruppo operativo.

D) Nell'account di produzione:
- Creare un ruolo IAM condiviso in grado di creare ed eliminare l'infrastruttura dell'applicazione.
- Aggiungere l'account di sviluppo alla policy di attendibilità per il ruolo condiviso.

Nell'account di sviluppo:
- Creare un gruppo IAM di sviluppo in grado di creare ed eliminare l'infrastruttura dell'applicazione.
- Creare un gruppo IAM operativo in grado di assumere il ruolo condiviso nell'account di produzione.
- Creare un utente IAM per ogni sviluppatore. Assegnare questi utenti al gruppo di sviluppo.
- Creare un utente IAM per ogni operatore. Assegnare questi utenti al gruppo di sviluppo e al gruppo operativo.

© 2022, Amazon Web Services, Inc. o sue affiliate. Tutti i diritti riservati | aws.amazon.com

7) Un Solutions Architect deve ridurre i costi per un'applicazione Big Data. L'ambiente dell'applicazione è costituito da centinaia di dispositivi che inviano eventi ad Amazon Kinesis Data Streams. L'ID dispositivo viene utilizzato come chiave di partizione, quindi ogni dispositivo ottiene uno shard separato. Ogni dispositivo invia tra 50 KB e 450 KB di dati al secondo. Una funzione AWS Lambda esegue il polling degli shard, elabora i dati e archivia il risultato in Amazon S3.

Ogni ora, un'altra funzione Lambda esegue una query di Amazon Athena sui dati dei risultati per identificare i valori anomali. Questa funzione Lambda inserisce i valori anomali in una coda Amazon Simple Queue Service (Amazon SQS). Un gruppo Amazon EC2 Auto Scaling composto da due istanze EC2 monitora la coda ed esegue un processo di 30 secondi per risolvere i valori anomali. I dispositivi inviano una media di 10 valori esterni ogni ora.

Quale combinazione di modifiche apportate all'applicazione riduce MAGGIORMENTE i costi? (Seleziona DUE risposte.)

A) Modificare la configurazione di avvio del gruppo Auto Scaling per utilizzare tipi di istanza più piccoli nella stessa famiglia di istanze.
B) Sostituire il gruppo Auto Scaling con una funzione Lambda che viene richiamata quando i messaggi arrivano nella coda.
C) Riconfigurare i dispositivi e il flusso dei dati per impostare un rapporto di 10 dispositivi e 1 shard di flusso di dati.
D) Riconfigurare i dispositivi e il flusso dei dati per impostare un rapporto di 2 dispositivi e 1 shard di flusso di dati.
E) Modificare la capacità desiderata del gruppo Auto Scaling in una singola istanza EC2.

8) Un'azienda gestisce un'applicazione di e-commerce su istanze Amazon EC2 su un Application Load Balancer. Le istanze vengono eseguite in un gruppo Amazon EC2 Auto Scaling in più zone di disponibilità. Dopo che un ordine è stato elaborato correttamente, l'applicazione pubblica immediatamente i dati dell'ordine su un sistema di tracciamento affiliato esterno di terze parti che paga le commissioni di vendita per i riferimenti degli ordini.

Durante una promozione di marketing di grande successo, il numero di istanze EC2 è aumentato da 2 a 20. In questo periodo, l'applicazione ha continuato a funzionare correttamente. Tuttavia, l'aumento del tasso di richieste ha sopraffatto l'affiliato di terze parti e ha provocato errori di richiesta.

Quale combinazione di modifiche architettoniche dovrebbe apportare un Solutions Architect per garantire che l'intero processo funzioni correttamente sotto sforzo? (Seleziona DUE risposte.)

A) Spostare il codice che chiama l'affiliato a una nuova funzione AWS Lambda. Modificare l'applicazione per richiamare la funzione Lambda in modo asincrono.
B) Spostare il codice che chiama l'affiliato a una nuova funzione AWS Lambda. Modificare l'applicazione per inserire i dati dell'ordine in una coda Amazon Simple Queue Service (Amazon SQS). Attivare la funzione Lambda dalla coda.
C) Aumentare il timeout della nuova funzione AWS Lambda.
D) Ridurre la concorrenza riservata della nuova funzione AWS Lambda.
E) Aumentare la memoria della nuova funzione AWS Lambda.

© 2022, Amazon Web Services, Inc. o sue affiliate. Tutti i diritti riservati | aws.amazon.com

9) Un'azienda ha creato un'applicazione web di biglietti online su AWS. L'applicazione è ospitata su AWS App Runner e utilizza immagini archiviate in un repository Amazon Elastic Container Registry (Amazon ECR). L'applicazione memorizza i dati in un cluster database Amazon Aurora MySQL. L'azienda ha creato un nome di dominio in Amazon Route 53.

L'azienda deve distribuire l'applicazione in due regioni AWS utilizzando una configurazione attivo-attivo.

Quale combinazione di passaggi soddisferà questi requisiti con la MINIMA modifica all'architettura? (Seleziona TRE risposte.)

A) Configurare la Cross-Region Replication sulla seconda regione per le immagini ECR.
B) Creare un endpoint VPC dal repository ECR nella seconda regione.
C) Modificare la configurazione di App Runner aggiungendo un secondo target di distribuzione alla seconda regione.
D) Distribuire App Runner nella seconda regione. Configurare il routing basato sulla latenza di Route 53.
E) Modificare il database utilizzando le tabelle globali di Amazon DynamoDB nelle due regioni desiderate.
F) Utilizzare un database globale Aurora con l'inoltro in scrittura abilitato nella seconda regione.

10) Un'azienda ha distribuito un'applicazione web a più livelli nel cloud AWS. L'applicazione è composta dai seguenti livelli:

- **Un livello web basato su Windows ospitato su istanze Amazon EC2 con indirizzi IP elastici**
- **Un livello di applicazione basato su Linux ospitato su istanze EC2 eseguite su un Application Load Balancer (ALB) che utilizza il routing basato su percorsi**
- **Un database MySQL eseguito su un'istanza EC2 Linux**

Tutte le istanze EC2 utilizzano CPU x86 basate su Intel. Un Solutions Architect deve modernizzare l'infrastruttura per ottenere prestazioni migliori. La soluzione deve ridurre al minimo il sovraccarico operativo dell'applicazione.

Quale combinazione di operazioni deve eseguire il Solutions Architect per soddisfare questi requisiti? (Seleziona DUE risposte.)

A) Eseguire il database MySQL su più istanze EC2.
B) Posizionare le istanze del livello web dietro un ALB.
C) Eseguire la migrazione del database MySQL ad Amazon Aurora Serverless.
D) Eseguire la migrazione di tutti i tipi di istanze EC2 a Graviton2.
E) Sostituire l'ALB per le istanze a livello di applicazione con un bilanciatore del carico gestito dall'azienda.

© 2022, Amazon Web Services, Inc. o sue affiliate. Tutti i diritti riservati | aws.amazon.com

Risposte

1) C: gli allarmi di fatturazione forniranno all'azienda avvisi su spese eccessive senza togliere il controllo a nessuno dei gruppi aziendali. Le opzioni A e B non sono corrette perché ogni gruppo aziendale desidera mantenere il controllo del proprio account. Queste opzioni non impedirebbero il lancio di un numero elevato di istanze. L'opzione D è un processo manuale che non fornirebbe avvisi immediati in merito a spese eccessive.

2) D: AWS CloudFormation StackSets può distribuire il ruolo IAM su più account con una singola operazione. L'opzione A non è corretta perché le credenziali fornite da AWS Single Sign-On (AWS SSO) sono temporanee. L'applicazione perderebbe le autorizzazioni e dovrebbe accedere nuovamente. L'opzione B consentirebbe l'accesso solo all'account di gestione. L'opzione C non è corretta perché quando entra a far parte di un'organizzazione, un account non riceve le autorizzazioni per accedere agli altri account dell'organizzazione.

3) D, E: Cross-Origin Resource Sharing (CORS) è una funzionalità di sicurezza del browser che limita le richieste HTTP avviate da script eseguiti nel browser. CORS è in genere richiesto per creare applicazioni web che accedono alle API ospitate su un dominio o un'origine differente. Puoi abilitare CORS per consentire le richieste alla tua API da un'applicazione web ospitata su un dominio differente. Ad esempio, se la tua API è ospitata su https://[api_id].execute-api.[region].amazonaws.com/ e desideri chiamare la tua API da un'applicazione web ospitata su [bucketname].s3.website-[region], la tua API deve supportare CORS. L'opzione E è necessaria per la visualizzazione del modulo HTML utilizzando un endpoint del sito web.

L'opzione A non è corretta perché l'intestazione CORS deve essere configurata per essere restituita dalla risposta dinamica dall'endpoint API. La configurazione di CORS per il bucket S3 non aiuta. L'opzione B non è corretta perché non vi è alcun vantaggio nel servire una pagina web statica da un server web in esecuzione su Amazon EC2 anziché da un bucket S3. L'opzione C non è corretta perché API Gateway ha una quota predefinita di 10.000 richieste al secondo per ciascuna regione AWS. Se necessario, è possibile aumentare questa quota.

4) A: Amazon API Gateway restituisce in modo intermittente errori con codice di stato HTTP 502 (gateway non valido) se la funzione AWS Lambda supera la quota di concorrenza. L'opzione B non è corretta perché, in questo caso, l'API Gateway restituisce un errore con codice di stato 429 dovuto alle troppe richieste. L'opzione C non è corretta perché gli errori si verificano durante le chiamate all'endpoint API Gateway API, non durante il processo di autenticazione. L'opzione D non è corretta perché i dati obsoleti non causerebbero un errore Gateway non valido.

5) C: AWS Systems Manager Run Command non richiede l'apertura di porte in ingresso. Run Command funziona interamente su HTTPS in uscita, che è aperto per impostazione predefinita per i gruppi di sicurezza. Le opzioni A e B non sono corrette perché i requisiti stabiliscono che l'unica porta in ingresso che dovrebbe essere aperta è la 443. L'opzione D non è corretta perché AWS Trusted Advisor non esegue questa funzione di gestione.

6) D: la risposta corretta segue le linee guida standard per la concessione dell'accesso tra account tra due account controllati dall'utente. L'opzione A non soddisfa i requisiti perché richiede due set di credenziali per gli operatori. L'opzione B non è corretta perché non è possibile aggiungere un utente IAM a un gruppo IAM in un account diverso. L'opzione C non è corretta perché un ruolo non può concedere l'accesso alle risorse di un altro account. Il ruolo condiviso deve trovarsi nello stesso account con le risorse gestite dal ruolo condiviso.

7) B, D: il tempo medio di elaborazione per risolvere i valori anomali ogni ora è di 300 secondi (10 eventi per 30 secondi ciascuno). L'opzione B è corretta perché con AWS Lambda paghi solo la piccola quantità di tempo di elaborazione necessaria per elaborare i valori esterni. Sebbene le opzioni A ed E riducano i costi, comportano entrambe il pagamento di una o più istanze Amazon EC2 che rimarrebbero inutilizzate per 3.300 secondi ogni ora. Le opzioni C e D riducono i costi relativi alle ore di frammento del flusso di dati Kinesis. Tuttavia, l'opzione C non è corretta perché la quantità di dati supererebbe la quota di 1 MB/s di un singolo shard.

© 2022, Amazon Web Services, Inc. o sue affiliate. Tutti i diritti riservati | aws.amazon.com

8) B, D: nell'opzione B, l'uso di una coda Amazon Simple Queue Service (Amazon SQS) separerà l'applicazione principale dalle chiamate all'affiliato. Questa modifica proteggerà l'applicazione principale dalla ridotta capacità dell'affiliato. Inoltre, le richieste non riuscite possono tornare automaticamente alla coda. Nell'opzione D, la riduzione del numero di invocazioni simultanee impedirà che la domanda di affiliazione venga sopraffatta.

Sebbene l'opzione A ridurrà il carico sulle istanze Amazon EC2, questa soluzione non ridurrà il numero di richieste all'applicazione di affiliazione. Sebbene l'opzione C consenta alla funzione AWS Lambda di attendere più a lungo il ritorno della chiamata esterna, questa soluzione non ridurrà il carico sull'applicazione di affiliazione sovraccaricata. L'opzione E non è corretta perché un aumento della memoria non avrà alcun effetto sull'interazione tra la funzione Lambda e il sistema di tracciamento degli affiliati.

9) A, D, F: AWS App Runner è un servizio completamente gestito che gli sviluppatori possono utilizzare per distribuire rapidamente applicazioni web containerizzate con immagini archiviate in un repository Amazon Elastic Container Registry (Amazon ECR). L'opzione A è corretta perché Cross-Region Replication crea una copia del repository in una seconda regione AWS. L'opzione D è corretta perché puoi utilizzare Route 53 per ospitare il nome di dominio personalizzato e per instradare il traffico verso le risorse in più regioni AWS. L'opzione F è corretta perché gli Amazon Aurora Global database si estendono su più regioni e sono progettati per applicazioni distribuite a livello globale.

L'opzione B non è corretta perché un endpoint VPC non fornirà l'accesso a un'immagine archiviata in una regione diversa. Nell'opzione C, tale configurazione non esiste in App Runner. Anche se l'opzione E funzionerebbe, l'introduzione di Amazon DynamoDB richiederebbe più modifiche all'architettura che l'uso di un database globale Aurora. La domanda chiede una modifica minima dell'architettura.

10) B, C: nell'opzione B, posizionando il livello web dietro un Application Load Balancer (ALB), è possibile migliorare la disponibilità e la scalabilità del livello web. L'ALB funge da unico punto di contatto per i clienti e distribuisce il traffico delle applicazioni in entrata alle istanze di Amazon EC2. L'opzione C è corretta perché Amazon Aurora Serverless offre prestazioni e disponibilità elevate con una complessità operativa ridotta.

L'opzione A non è corretta perché le istanze EC2 aggiuntive non ridurranno al minimo il sovraccarico operativo. Un servizio gestito sarebbe un'opzione migliore. L'opzione D non è corretta perché l'applicazione include istanze di Windows che non sono disponibili per Graviton2. L'opzione E non è corretta perché un bilanciatore del carico gestito dall'azienda non ridurrà al minimo il sovraccarico operativo.

© 2022, Amazon Web Services, Inc. o sue affiliate. Tutti i diritti riservati | aws.amazon.com