

Solutions Architect Professional (SAP-C01)

Sample Exam Questions

ソリューションアーキテクト - プロフェッショナル (SAP-C01)

サンプル試験問題

- 1) ある企業には、個別のビジネスグループが所有する多数の AWS アカウントがあります。最近、当社のアカウントの 1 つが侵害されました。攻撃者は多数のインスタンスを起動し、そのアカウントに多額の請求が発生することになりました。

セキュリティ侵害の問題は解決されましたが、経営陣はソリューションアーキテクトに対し、すべてのアカウントで過剰な支出を防ぐソリューションを開発するよう依頼しました。各ビジネスグループは、AWS アカウントに対するフルコントロールを維持したいと考えています。

これらの要件を満たすためにソリューションアーキテクトが推奨すべきソリューションはどれですか。

- A. AWS 組織を使って各 AWS アカウントをマスターアカウントに追加する。ec2:instanceType 条件キーを使用するサービスコントロールポリシー (SCP) を作成して、各アカウントで高コストのインスタンスタイプが起動されないようにする。
- B. 新しいカスタマー管理 IAM ポリシーを、ec2:instanceType 条件キーを使用する各アカウントの IAM グループにアタッチして、高コストのインスタンスタイプの起動を防ぐ。既存のすべての IAM ユーザーをそれぞれのグループに配置する。
- C. 各 AWS アカウントで請求アラートを有効にする。アカウントが支出予算を超えた時点でアカウント管理者に Amazon SNS 通知を送信する Amazon CloudWatch アラームを作成する。
- D. 各アカウントで AWS Cost Explorer を有効にする。各アカウントの AWS Cost Explorer を定期的に確認して、支出が計画予算を超えないようにする。

Solutions Architect Professional (SAP-C01)

Sample Exam Questions

ソリューションアーキテクト - プロフェッショナル (SAP-C01)

サンプル試験問題

2) ある会社には複数の AWS アカウントがあります。同社は、オンプレミスの Active Directory (AD) と AWS SSO を統合し、AD ユーザーにすべてのアカウント間でインフラストラクチャを管理する最小限の権限を付与しました。

ソリューションアーキテクトは、すべての AWS アカウントで読み取り専用アクセスを必要とするサードパーティのモニタリングソリューションを統合する必要があります。モニタリングソリューションは、独自の AWS アカウントで実行されます。

モニタリングソリューションに必要な権限を与えるにはどうすればよいでしょうか。

- A. AWS SSO ディレクトリにユーザーを作成し、読み取り専用アクセス許可セットを割り当てる。モニタリングするすべての AWS アカウントを新しいユーザーに割り当てる。サードパーティのモニタリングソリューションにユーザー名とパスワードを提供する。
- B. 組織のマスターアカウントに AWS IAM ロールを作成する。サードパーティのモニタリングソリューションの AWS アカウントに、ロールを引き受けることを許可する。
- C. サードパーティのモニタリングソリューションの AWS アカウントを組織に招待する。すべての機能を有効にする。
- D. 信頼ポリシーにリストされているサードパーティのアカウントを使用して、サードパーティモニタリングソリューションの新しい AWS IAM ロールを定義する AWS CloudFormation テンプレートを作成する。スタックセットを使用することにより、リンクされているすべての AWS アカウントに IAM ロールを作成する。

Solutions Architect Professional (SAP-C01)

Sample Exam Questions

ソリューションアーキテクト - プロフェッショナル (SAP-C01)

サンプル試験問題

3) あるチームがパブリック Amazon S3 バケットでホストされる HTML フォームを構築しているところで、このフォームは、JavaScript を使用して Amazon API Gateway エンドポイントにデータをポストします。エンドポイントは AWS Lambda 関数と統合されています。このチームは API Gateway コンソールで各メソッドをテストし、有効な応答を受け取りました。

このフォームを API Gateway に成功的にポストし、有効な応答を受け取るには、どのステップの組み合わせを実行する必要がありますか。(2 つ選択)

- A. クロスオリジンリソース共有 (CORS) を許可するように S3 バケットを構成する。
- B. Amazon S3 ではなく Amazon EC2 でフォームをホストする。
- C. API Gateway の制限の引き上げをリクエストする。
- D. API Gateway でクロスオリジンリソース共有 (CORS) を有効にする。
- E. ウェブホスティング用の S3 バケットを構成する。

4) ある小売会社は、Amazon API Gateway、AWS Lambda、Amazon Cognito、および Amazon DynamoDB 上に構築されたサーバーレスモバイルアプリを実行しています。ホリデーシーズンのトラフィックが急増している間、断続的なシステム障害について苦情が報告されています。開発者は、API Gateway エンドポイントが有効と見られるリクエストに 502 Bad Gateway エラーを返していることに気づきました。

この問題の解決方法はどれですか。

Solutions Architect Professional (SAP-C01)

Sample Exam Questions

ソリューションアーキテクト - プロフェッショナル (SAP-C01)

サンプル試験問題

- A. Lambda 関数の同時実行制限を増やし、`ConcurrentExecutions` メトリクスが制限に近づくと Amazon CloudWatch から通知アラートが送信されるよう構成する。
- B. API Gateway エンドポイントで 1 秒あたりのトランザクション数の制限に関する通知アラートを構成し、必要に応じてこの制限を増やす Lambda 関数を作成する。
- C. 複数のリージョンの Amazon Cognito ユーザープールにユーザーをシャードして、ユーザー認証の待ち時間を短縮する。
- D. DynamoDB の強力な一貫性のある読み取りを使用して、クライアントアプリケーションに最新のデータが常に返されるようにする。

5) あるウェブホスティング会社は、すべての AWS リージョンですべてのアカウントの Amazon GuardDuty を有効にしました。システム管理者は、重大度の高いイベントに対して自動応答を作成する必要があります。

これはどうすれば実現できますか。

- A. プログラム方式で問題を解決する AWS Lambda 関数をトリガーする VPC フローログを通じてロールを作成する。
- B. プログラム方式で問題を解決する AWS Lambda 関数をトリガーする AWS CloudWatch イベントルールを作成する。
- C. プログラム方式で問題を解決する AWS Lambda 関数をトリガーするように AWS Trusted Advisor を構成する。

Solutions Architect Professional (SAP-C01)

Sample Exam Questions

ソリューションアーキテクト - プロフェッショナル (SAP-C01)

サンプル試験問題

D. プログラム方式で問題を解決する AWS Lambda 関数をトリガーするように AWS CloudTrail を構成する。

- 6) ある企業が Amazon ECS クラスターで新しいウェブサービスを立ち上げているところです。会社のポリシーに基づいて、クラスターインスタンスのセキュリティグループが、HTTPS (ポート 443) を除くすべての受信トラフィックをブロックする必要があります。クラスターは Amazon 100 EC2 インスタンスで構成されています。セキュリティエンジニアは、クラスターインスタンスの管理及び更新を担当します。セキュリティエンジニアリングチームは小人数であるため、管理作業を最小限に抑える必要があります。

これらの運用要件を満たすためには、サービスをどのように設計したらよいでしょうか。

- A. ユーザーデータスクリプトを使用して、クラスターインスタンスから SSH ポートを 2222 に変更する。ポート 2222 を経由し、SSH を使用して各インスタンスにログインする。
- B. ユーザーデータスクリプトを使用して、クラスターインスタンスで SSH ポートを 2222 に変更する。AWS Trusted Advisor を使用して、ポート 2222 上のクラスターインスタンスをリモート管理する。
- C. SSH キーペアがないクラスターインスタンスを起動する。Amazon EC2 Systems Manager Run Command を使用して、クラスターインスタンスをリモートで管理する。
- D. SSH キーペアがないクラスターインスタンスを起動する。AWS Trusted Advisor を使用して、クラスターインスタンスをリモート管理する。

- 7) ある会社には、運用ワークロード用と開発ワークロード用の 2 つの AWS アカウントがあります。開発チームとオペレーションチームが、ワークロードを作成および管理します。会社には、次の要件を満たすセキュリティ戦略が必要です。

Solutions Architect Professional (SAP-C01)

Sample Exam Questions

ソリューションアーキテクト - プロフェッショナル (SAP-C01)

サンプル試験問題

- 開発者は、開発アプリケーションインフラストラクチャを作成および削除する必要があります。
- オペレーターは、開発アプリケーションインフラストラクチャと運用アプリケーションインフラストラクチャの両方を作成および削除する必要があります。
- 開発者は、運用インフラストラクチャにアクセスすることができない必要があります。
- すべてのユーザーは、単一セットの AWS 認証情報が必要です。

これらの要件を満たす戦略は何ですか。

A. 開発アカウントで、次の手順を実行する。

- アプリケーションインフラストラクチャを作成および削除する機能を持つ開発 IAM グループを作成する。
- それぞれのオペレーターと開発者に対して IAM ユーザーを作成し、開発グループに割り当てる。

運用アカウントで、次の手順を実行する。

- アプリケーションインフラストラクチャを作成および削除する機能を持つオペレーション IAM グループを作成する。
- それぞれのオペレーターに対して IAM ユーザーを作成し、オペレーショングループに割り当てる。

B. 開発アカウントで、次の手順を実行する。

- アプリケーションインフラストラクチャを作成および削除する機能を持つ開発 IAM グループを作成する。
- それぞれの開発者に対して IAM ユーザーを作成し、開発グループに割り当てる。
- それぞれのオペレーターに対して IAM ユーザーを作成し、運用アカウントの開発グループとオペレーショングループに割り当てる。

運用アカウントで:

- アプリケーションインフラストラクチャを作成および削除する機能を持つオペレーション IAM グループを作成する。

Solutions Architect Professional (SAP-C01)

Sample Exam Questions

ソリューションアーキテクト - プロフェッショナル (SAP-C01)

サンプル試験問題

C. 開発アカウントで、次の手順を実行する。

- 運用アカウントでアプリケーションインフラストラクチャを作成および削除する機能を持つ共有 IAM ロールを作成する。
- アプリケーションインフラストラクチャを作成および削除する機能を持つ開発 IAM グループを作成する。
- 共有ロールを引き受ける機能を持つオペレーション IAM グループを作成する。
- それぞれの開発者に対して IAM ユーザーを作成し、開発グループに割り当てる。
- それぞれのオペレーターに対して IAM ユーザーを作成し、開発グループとオペレーショングループに割り当てる。

D. 開発アカウントで、次の手順を実行する。

- アプリケーションインフラストラクチャを作成および削除する機能を持つ開発 IAM グループを作成する。
- 運用アカウントで共有ロールを引き受ける機能を持つオペレーション IAM グループを作成する。
- それぞれの開発者に対して IAM ユーザーを作成し、開発グループに割り当てる。
- それぞれのオペレーターに対して IAM ユーザーを作成し、開発グループとオペレーショングループに割り当てる。

運用アカウントで:

- アプリケーションインフラストラクチャを作成および削除する機能を持つ共有 IAM ロールを作成する。
- 共有ロールに関する信頼ポリシーに開発アカウントを追加する。

8) ある企業では Apache Hadoop クラスタをデータセンターから AWS に移行しているところです。このクラスタは、60 台の VMware Linux 仮想マシン (VM) で構成されています。移行クラスタ中には、ダウンタイムを最小限に抑える必要があります。

Solutions Architect Professional (SAP-C01)

Sample Exam Questions

ソリューションアーキテクト - プロフェッショナル (SAP-C01)

サンプル試験問題

ダウンタイムを最小限に抑えるプロセスはどれですか。

- A. vCenter の AWS Management Portal を使用し、 Amazon EC2 インスタンスとして VM を AWS に移行する。
- B. AWS SMS を使用し、VM を AMI として AWS に移行する。AWS から移行された AMI の Amazon EC2 インスタンスとしてクラスターを起動する。
- C. VM の OVA ファイルを作成する。OVA ファイルを Amazon S3 にアップロードする。VM のインポート/エクスポートを使用して、OVA ファイルで AMI を作成する。AWS で AMI の Amazon EC2 インスタンスとしてクラスターを起動する。
- D. VM の HDFS データを、新しい Amazon Aurora データベースにエクスポートする。Amazon EC2 インスタンスで新しい Hadoop クラスターを起動する。新しいクラスターで Aurora データベースのデータを HDFS にインポートする。

- 9) あるソリューションアーキテクトは、ビッグデータアプリケーションのコストを削減する必要があります。アプリケーション環境は、Amazon Kinesis データストリームにイベントを送信する数百のデバイスで構成されています。各デバイスは、1 秒あたり 50 KB~450 KB のデータを送信します。シャードは、データを処理してその結果を Amazon S3 に保存する AWS Lambda 関数によってポーリングされます。

毎時間、AWS Lambda 関数は結果でデータについて特異点を識別し、これを Amazon SQS キューに配置する Amazon Athena クエリを実行します。2 つの EC2 インスタンスで構成された Amazon EC2 Auto Scaling グループはキューをモニタリングし特異点を処理する短い (約 30 秒) プロセスを実行しま

Solutions Architect Professional (SAP-C01)

Sample Exam Questions

ソリューションアーキテクト - プロフェッショナル (SAP-C01)

サンプル試験問題

す。デバイスは、1 時間に平均 10 個の特異値を送信します。

次の中で、コスト削減に最も適切な方法は何ですか。(2 つ選択)

- A. 同じインスタンスファミリーでより小さいインスタンスタイプを使用するように Auto Scaling グループの起動構成を変更する。
- B. Auto Scaling グループを、Amazon SQS キューに到着するメッセージによってトリガーされる AWS Lambda 関数に置き換える。
- C. 10 個のデバイスに対して 1 つのデータストリームシャードの比率に設定されるよう、デバイスとデータストリームを再構成する。
- D. 2 個のデバイスに対して 1 つのデータストリームシャードの比率に設定されるよう、デバイスとデータストリームを再構成する。
- E. Auto Scaling グループが望む容量を単一の EC2 インスタンスに変更する。

Solutions Architect Professional (SAP-C01)

Sample Exam Questions

ソリューションアーキテクト - プロフェッショナル (SAP-C01)

サンプル試験問題

10)ある会社は、ELB Application Load Balancer の背後にある Amazon EC2 インスタンスで e コマースアプリケーションを運用しています。インスタンスは、複数のアベイラビリティゾーンにまたがる Amazon EC2 Auto Scaling グループで実行されます。注文が成功に処理されたら、アプリケーションは注文紹介に対する販売手数料を支払う外部サードパーティ系列会社追跡システムに注文データを即時ポストします。成功的なマーケティングプロモーションの間、EC2 インスタンスの数が 2 から 20 に増加しました。アプリケーションは正常に動作し続けましたが、リクエスト率が増加したためサードパーティ系列会社過負荷となり、リクエストに失敗しました。

全体プロセスが負荷状態で正常に機能するために、次の中でどのような組み合わせのアーキテクチャ変更が必要ですか。(2 つ選択)

- A. **系列会社**を呼び出すコードを新しい AWS Lambda 関数に移動する。アプリケーションを変更して Lambda 関数を非同期的に呼び出す。
- B. **系列会社**を呼び出すコードを新しい AWS Lambda 関数に移動する。Amazon SQS キューに注文データを配置するようにアプリケーションを変更する。キューから Lambda 関数をトリガーする。
- C. 新しい AWS Lambda 関数のタイムアウトを延長する。
- D. 新しい AWS Lambda 関数の同時実行制限を調整する。
- E. 新しい AWS Lambda 関数のメモリを増やす。

Solutions Architect Professional (SAP-C01)

Sample Exam Questions

ソリューションアーキテクト - プロフェッショナル (SAP-C01)

サンプル試験問題

回答

- 1) C - [課金アラーム](#)を使用すると、経営陣はビジネスグループからコントロールを奪うことなく、過剰な支出に関するアラートを受け取ることができます。A と B は、各ビジネスグループがアカウントのコントロールを維持したいと考えており、これらのソリューションでは多数のインスタンス起動を防ぐことではないため、不正解です。D は手動プロセスであり、不正な支出が発見されるまでに時間がかかる可能性があります。
- 2) D - [AWS CloudFormation StackSets](#) なら、1 回の操作で複数のアカウントに IAM ロールをデプロイできます。A は、AWS SSO によって提供される認証情報が一時的なものであり、アプリケーションはアクセス権を失って再ログインする必要があるため、不正解です。B はマスターアカウントにのみアクセス権を付与します。C は、組織に属するアカウントは他のアカウントのアクセス許可を受け取らないため不正解です。
- 3) D、E - (D) 同じオリジンポリシーによりブラウザからエラーが発生しないようにするために、[CORS が必ず有効化される](#)必要があります。このためには、動的コンテンツを静的コンテンツと同じドメインから取得する必要があります。API Gateway は `[restapi-id].execute-api.amazonaws.com` 形式のドメインを使用しており、S3 バケットは `[bucketname].s3.website-[region].amazonaws.com` 形式を使用するため、CORS ヘッダーはこの制限を緩和するようにブラウザに対する API Gateway 応答と共に送信する必要があります。HTML フォームを[ウェブサイトエンドポイント](#)を通じて提供するには(E) が必要です。CORS ヘッダーが API エンドポイントからの動的応答によって返されるように構成する必要があるため、A は不正解です。S3 バケット用で CORS

Solutions Architect Professional (SAP-C01)

Sample Exam Questions

ソリューションアーキテクト - プロフェッショナル (SAP-C01)

サンプル試験問題

を構成することは役に立ちません。(B) は S3 バケットに比べて EC2 で実行されるウェブサーバーから静的ウェブページを提供することについて利点がないため、不正解です。API Gateway は 1 秒あたり 10,000 個の [デフォルトリージョンあたりの制限](#)があるため、(C) は不正解です。運営に必要な場合は、この制限を増やすことができます。

- 4) A – Lambda 関数が同時実行の制限を超えると、API Gateway によって [502 内部サーバーエラー](#)が断続的に返されます。この場合、API Gateway は [過多に多い要請に対する 429 エラー](#)を返すため、(B) は不正解です。(C) は、認証プロセス中ではなく API Gateway エンドポイントの呼び出す時にエラーが発生するため、不正解です。(D) は、古いデータにより無効なゲートウェイエラーが発生するわけではないため不正解です。
- 5) B – GuardDuty の調査結果は、Amazon SNS トピックおよび [CloudWatch Event](#) に送信できます。(A) と (D) は、VPC フローログや AWS CloudTrail の中でどちらも Lambda 関数を直接トリガーできないため、不正解です。(C) は、Trusted Advisor は推奨サービスであり、このシナリオには適していないため、不正解です。
- 6) C – [Amazon EC2 Systems Manager Run Command](#) の場合、インバウンドポートを開く必要はなく、これは全的にアウトバウンド HTTPS (デフォルトでセキュリティグループに対して開かれている) アウトバウンド HTTPS 上で完全に動作します。開かれる唯一の受信ポートが 443 であることが条件に明確に示されているため、(A) と (B) は除外されます。Trusted Advisor は管理機能を実行するた

Solutions Architect Professional (SAP-C01)

Sample Exam Questions

ソリューションアーキテクト - プロフェッショナル (SAP-C01)

サンプル試験問題

め、D が除外されます。

- 7) D - 正常に動作し要件を満たす回答はこれのみです。これは、ユーザーが制御する 2 つのアカウント間でクロスアカウントアクセスを許可するための[標準的なガイドライン](#)に従っています。(A) では、オペレーターに 2 セットの資格情報が必要となり、要件と合致しません。(B) は、IAM ユーザーを別のアカウントの IAM グループに追加できないため、適切ではありません。ロールは別のアカウントのリソースへのアクセスを付与できないため、(C) は適切ではありません。共有ロールが、そのロールが管理するリソースを持つアカウントに含まれている必要があります。
- 8) B - [AWS SMS](#) は各 VM を漸進的にアップロードするため、データセンタークラスターの実行中にサーバーをアップロードできます。データセンタークラスターは、すべての仮想マシンの最終増分同期の前のみシャットダウンする必要があります。(A) および (C) は、ダウンタイムを最小限に抑える要件を満たしていません。[vCenter および VM のインポート/エクスポートドキュメント](#)から：ほとんどの VM インポートのニーズについて AWS SMS を使用することが推奨します。AWS SMS は、インポートプロセスを自動化し (大規模の VM インフラストラクチャの移行ワークロードを減らし)、変化する VM の増分更新のサポートを追加し、インポートした VM をすぐに使用できる AMI に変換します。(D) は、ダウンタイムを最小限に抑えるという要件を満たしていません。
- 9) B、D - 1 時間あたりの平均コンピューティング使用量は約 300 秒 (10 イベント x 30 秒) です。A と E の両方ともコストを削減できますが、どちらも 1 時間あたり 3,300 秒以上使用されていない 1 つ以上の EC2 インスタンスについて支払う必要があります。B は、特異点を処理するために[必要な少](#)

Solutions Architect Professional (SAP-C01)

Sample Exam Questions

ソリューションアーキテクト - プロフェッショナル (SAP-C01)

サンプル試験問題

量のコンピューティング時間のみに支払をする必要があります。(C) と (D) の両方とも Kinesis Data Stream のシャード時間コストが削減されますが、(C) はデータ量が単一シャードの 1 MB/秒の制限を超えるため適切ではありません。

- 10) B、D - キュー (B) にメッセージを入れると、メインアプリケーションが系列会社に対する呼び出しから分離されます。そうすると、系列会社の容量減少によりメインアプリケーションを保護できるだけでなく、失敗した要請が自動的にキューに復帰されることができるようになります。同時実行の数を制限する (D) では系列会社のアプリケーション過負荷を防ぐことができます。(A) は、Lambda 関数を非同期的に呼び出すと EC2 インスタンスの負荷が軽減されますが、系列会社のアプリケーションへのリクエストの数は減らないため、不正解です。(C) は、Lambda 関数で外部呼び出しが戻るまで待機できる時間が長くなりますが、系列会社のアプリケーションの負荷を軽減しないため (まだ過負荷となる)、不正解です。(E) は、メモリを調整しても Lambda 関数と系列会社のアプリケーション間の相互作用には影響しないため不正解です。