AWS Certified SysOps Administrator - Associate
(SOA-C02) 試験問題サンプル

1) ある企業が、Amazon EC2 インスタンス上で Web アプリケーションをホストしています。ユーザーから、Web アプリケーションがときどき無応答状態になるという報告を受けました。Amazon CloudWatch メトリクスを調べたところ、無応答時の CPU 使用率が 100% になっていました。SysOps アドミニストレーターは、この問題を監視するためのソリューションを実装する必要があります。

この要件を満たすには、どうすればよいですか。

A. EC2 インスタンスに対する AWS CloudTrail イベントを監視するための CloudWatch アラームを作成する。
B. EC2 インスタンスの CPU 使用率に対する CloudWatch メトリクスを監視するための CloudWatch アラームを作成する。
C. EC2 インスタンスの CPU 使用率に対する CloudWatch メトリクスを監視するための Amazon Simple Notification Service (Amazon SNS) トピックを作成する。
D. Amazon Inspector を使用して CPU 使用率の異常値を検出することにより、EC2 インスタンス上に反復的評価検査を作成する。

2) ある企業が、アプリケーションに対して Amazon ElastiCache for Memcached を使用して、クエリ応答をキャッシュすることにより、応答速度を向上させています。ところが、アプリケーションのユーザーから応答速度が遅いという報告を受けました。SysOps アドミニストレーターは、Memcached のエビクション数に対する Amazon CloudWatch メトリクスの値が大きいことに気付きました。

この問題を解決するには、どうすればよいですか (2 つ選択してください)。

A. ElastiCache for Memcached の内容をフラッシュする。
B. ConnectionOverhead パラメータの値を大きくする。
C. クラスター内のノード数を増やす。
D. クラスター内のノードのサイズを大きくする。
E. クラスター内のノード数を減らす。

3) ある企業において、AWS Lambda 関数がこの企業のアカウントの VPC 内のリソースにアクセスできるようにする必要があります。また、この Lambda 関数は、インターネット経由でのみアクセス可能なサードパーティ製 API にアクセスする必要があります。

これらの要件を満たすには、どうすればよいですか。

A. Elastic IP アドレスを Lambda 関数にアタッチする。VPC のインターネットゲートウェイへのルートを構成する。
B. Lambda 関数を、VPC の仮想プライベートゲートウェイへのルートを持つプライベートサブネットに接続する。
C. Lambda 関数を、VPC のインターネットゲートウェイへのルートを持つパブリックサブネットに接続する。
D. Lambda 関数を、VPC のパブリックサブネット内の NAT ゲートウェイへのルートを持つプライベートサブネットに接続する。

4) ある企業が、Amazon EC2 インスタンスの大規模フリート上で、財務トランザクションを処理するアプリケーションを実行しています。また、Amazon Elastic File System (Amazon EFS) を使用して、EC2 インスタンス間でデータを共有しています。

この企業は、アプリケーションを別のアベイラビリティーゾーンに展開したいと考えています。この別のアベイラビリティーゾーン内には既に、新規サブネットおよびマウントターゲットを作成しています。ところが、SysOps アドミニストレーターがこの新規サブネット内で新しい EC2 インスタンスを起動したとき、EC2 インスタンスによってファイルシステムがマウントされません。

この問題の原因は何ですか。

A. EFS マウントターゲットがプライベートサブネット内に作成されている。
B. EC2 インスタンスに関連付けられている IAM ロールにおいて、efs:MountFileSystem アクションが許可されていない。
C. この別のアベイラビリティーゾーン内の Amazon EFS 用 VPC エンドポイントにトラフィックをルーティングするよう、ルーティングテーブルが構成されていない。
D. マウントターゲットに対するセキュリティグループにおいて、EC2 インスタンスによって使用されているセキュリティグループからの受信 NFS 接続が許可されていない。

5) ある企業が、AWS Organizations を使用して多数の AWS アカウントを作成および管理しています。この企業は、各アカウントに新規 IAM ロールを展開したいと考えています。

組織の各アカウントに新しいロールをデプロイするために、SysOps アドミニストレーターが実行すべきアクションはどれですか。

A. 新規 IAM ロールを各アカウントに追加するためのサービスコントロールポリシー (SCP) を組織内に作成する。
B. AWS CloudFormation 変更セットと、新規 IAM ロールを作成するためのテンプレートを組織に展開する。
C. AWS CloudFormation StackSets を使用して、新規 IAM ロールを作成するためのテンプレートを各アカウントに展開する。
D. AWS Config を使用して、新規 IAM ロールを各アカウントに追加するための組織ルールを作成する。

6) ある企業が、Amazon EC2 インスタンス上で数個の本番用ワークロードを実行しています。SysOps アドミニストレーターが、ある本番用 EC2 インスタンスがシステムヘルスチェックで不合格になったことに気付きました。そのため、そのインスタンスを手動で復旧しました。

SysOps アドミニストレーターは、EC2 インスタンスの復旧タスクを自動化したいと考えています。また、システムヘルスチェックで不合格になった場合には常に通知を受信したいと考えています。すべての本番用 EC2 インスタンスに対して、詳細モニタリングが有効化されています。

最も運用効率の高い方法でこれらの要件を満たすには、どうすればよいですか。

A. 各本番用 EC2 インスタンスに対して、Status Check Failed: System に対する Amazon CloudWatch アラームを作成する。EC2 インスタンスを復旧するよう、アラームアクションを設定する。Amazon Simple Notification Service (Amazon SNS) トピックにパブリッシュされるよう、アラーム通知を構成する。

B. 各本番用 EC2 インスタンス上で、ハートビート通知を中央監視サーバーに 1 分ごとに送信することによってシステムの健全性を監視するスクリプトを作成する。EC2 インスタンスからハートビートが送信されなくなった場合には、EC2 インスタンスをいったん停止して再開始し、通知を Amazon Simple Notification Service (Amazon SNS) トピックにパブリッシュするスクリプトを監視サーバー上で実行する。

C. 各本番用 EC2 インスタンス上で、cron ジョブを使用して高可用性エンドポイントに ping コマンドを送信するスクリプトを作成する。ネットワーク応答タイムアウトが検出された場合、EC2 インスタンスを再起動するコマンドを呼び出す。

D. 各本番用 EC2 インスタンス上で、ログを収集して Amazon CloudWatch Logs 内のロググループに送信するよう、Amazon CloudWatch エージェントを構成する。エラーを追跡するメトリクスフィルタに基づく CloudWatch アラームを作成する。EC2 インスタンスを再起動してメール通知を送信する AWS Lambda 関数を呼び出すよう、アラームを構成する。

7) ある企業が、AWS Organizations を使用して複数のアカウントを管理しています。本番用アカウントについて、現在および将来のすべての Amazon EC2 インスタンス上および Amazon Elastic File System (Amazon EFS) 上のすべてのデータが毎日バックアップされるよう、構成する必要があります。また、バックアップデータを 30 日間保持する必要があります。

最小限の作業量でこれらの要件を満たすには、どうすればよいですか。

A. AWS Backup でバックアッププランを作成する。リソース ID を使用してリソースを割り当てる。その際、本番用アカウントで動作しているすべての EC2 リソースおよび EFS リソースを選択する。新規リソースを含めるため、バックアッププランを毎日編集する。バックアッププランを、毎日実行するようにスケジューリングする。また、30 日後にバックアップデータを失効させるライフサイクルポリシーを適用する。
B. AWS Backup でバックアッププランを作成する。タグを使用してリソースを割り当てる。既存のすべての EC2 リソースおよび EFS リソースが正しくタグ付けされていることを確認する。正しいタグが付けられていない場合にはインスタンスおよびファイルシステムを作成しないというサービスコントロールポリシー (SCP) を、本番用アカウントの OU に適用する。バックアッププランを、毎日実行するようにスケジューリングする。また、30 日後にバックアップデータを失効させるライフサイクルポリシーを適用する。
C. Amazon Data Lifecycle Manager (Amazon DLM) でライフサイクルポリシーを作成する。リソース ID を使用してすべてのリソースを割り当てる。その際、本番用アカウントで動作しているすべての EC2 リソースおよび EFS リソースを選択する。新規リソースを含めるため、ライフサイクルポリシーを毎日編集する。スナップショットを毎日作成するよう、ライフサイクルポリシーをスケジューリングする。また、スナップショットの保持期間を 30 日に設定する。
D. Amazon Data Lifecycle Manager (Amazon DLM) でライフサイクルポリシーを作成する。タグを使用してすべてのリソースを割り当てる。既存のすべての EC2 リソースおよび EFS リソースが正しくタグ付けされていることを確認する。正しいタグが付けられていない場合にはリソースを作成しないというサービスコントロールポリシー (SCP) を適用する。スナップショットを毎日作成するよう、ライフサイクルポリシーをスケジューリングする。また、スナップショットの保持期間を 30 日に設定する。

8) ある企業が AWS CloudTrail を使用しています。この企業は、ログファイルが削除または修正されていないことを SysOps アドミニストレーターが簡単に検証できるようにしたいと考えています。

この要件を満たすには、どうすればよいですか。

A. ログファイルの暗号化に使用された AWS Key Management Service (AWS KMS) キーに対するアクセス権限を、SysOps アドミニストレーターに付与する。
B. トレイルの作成時または更新時の CloudTrail ログファイル整合性検査を有効化する。
C. ログファイルの格納先バケットに対する Amazon S3 サーバーアクセスロギングを有効化する。
D. ログファイルを別のバケットにレプリケートするよう、S3 バケットを構成する。

9) ある企業が、Amazon EC2 インスタンス上でカスタムデータベースを実行しています。このデータベースのデータは、Amazon Elastic Block Store (Amazon EBS) ボリュームに格納されています。SysOps アドミニストレーターは、この EBS ボリュームに対するバックアップ戦略を策定する必要があります。

この要件を満たすには、どうすればよいですか。

A. VolumeIdleTime メトリクスに対する Amazon CloudWatch アラームを作成する。EBS ボリュームのスナップショットを作成するためのアクションを作成する。
B. AWS Data Pipeline で、EBS ボリュームのスナップショットを定期的に作成するためのパイプラインを作成する。
C. EBS ボリュームのスナップショットを定期的に作成するための Amazon Data Lifecycle Manager (Amazon DLM) ポリシーを作成する。
D. EBS ボリュームのスナップショットを定期的に作成するための AWS DataSync タスクを作成する。

10) ある企業が、各部署用に多数の Amazon EC2 インスタンスを実行しています。この企業は、既存の AWS リソースのコストを部署別に追跡する必要があります。

この要件を満たすには、どうすればよいですか。

A. この企業のアカウントにおいて、AWS によって生成されるコスト配分タグをすべて有効化する。
B. Tag Editor を使用して、ユーザー定義タグをインスタンスに適用する。コスト配分に関してこれらのタグを有効化する。
C. EC2 使用率に対する AWS Pricing Calculator を定期的に実行するための AWS Lambda 関数をスケジューリングする。
D. AWS Trusted Advisor ダッシュボードを使用して、EC2 コストレポートをエクスポートする。

注: 2023 年 3 月 28 日以降、追って通知するまで AWS Certified SysOps Administrator - Associate 試験で試験ラボの出題がなくなります。今回の試験ラボの休止は一時的な措置であり、当社ではその間に試験ラボを評価し、受験者に最適なエクスペリエンスを提供するための改善を行います。この変更により、試験は 65 問の択一選択問題と複数選択問題で構成され、試験時間は 130 分となります。試験ページにある試験の準備リソースはすべて、この試験形式の変更後も引き続き有効です。

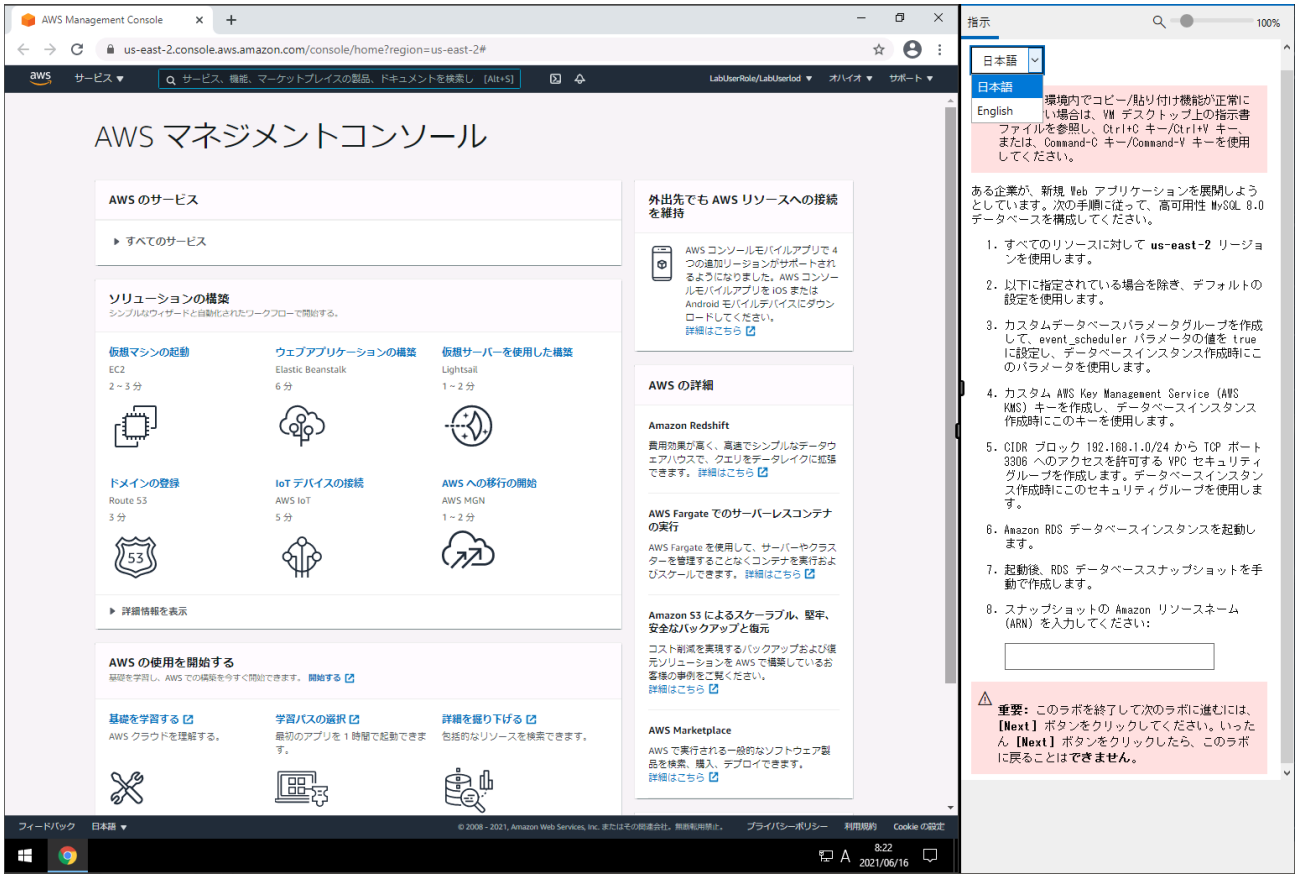
11) 試験ラボの例

ある企業が、新規 Web アプリケーションを展開しようとしています。次の手順に従って、高可用性 MySQL 8.0 データベースを構成してください。

1. すべてのリソースに **us-east-2** リージョンを使う。
2. 以下で指定された場合を除き、デフォルトの構成設定を使用する。
3. カスタムデータベースパラメータグループを作成して、**event_scheduler** パラメータの値を true に設定し、データベースインスタンス作成時にこのパラメータグループを使用します。
4. カスタム AWS Key Management Service (AWS KMS) キーを作成し、データベースインスタンス作成時にこのキーを使用します。
5. CIDR ブロック 192.168.1.0/24 から TCP ポート 3306 へのアクセスを許可する VPC セキュリティグループを作成します。データベースインスタンス作成時にこのセキュリティグループを使用します。
6. Amazon RDS データベースインスタンスを起動します。
7. 起動後、RDS データベーススナップショットを手動で作成します。

スナップショットの Amazon リソースネーム (ARN) を入力してください:_____

注: 次のスクリーンショットは、この試験ラボ例が試験中にどのように表示されるかを示したものです。



解答

1) B – Amazon CloudWatch を使用することにより、アプリケーションの監視に必要なデータとインサイトを得ることができます。Amazon EC2 から CloudWatch にメトリクスが送信されます。CPUUtilization メトリクスは、あるインスタンスに割り当てられている EC2 コンピュートユニットのうち、現在使用されている割合を示したものです。いずれか 1 個のインスタンスに対する CPUUtilization メトリクスを監視するための、CloudWatch アラームを作成できます。たとえば、5 分間の CPUUtilization メトリクスの平均値が 75% を上回った場合にメール通知を受信することができます。

2) C、D – Amazon ElastiCache for Memcached に対する Evictions メトリクスは、新規アイテム用のスペースを確保するためにキャッシュから削除された期限切れ前アイテムの数を示しています。クラスターでエビクションが発生している場合、一般に、処理できるデータ量を増やすため、スケールアップする (つまり、よりメモリ容量の大きいノードを使用する) かまたはスケールアウトする (つまり、クラスターにノードを追加する) する必要があります。

3) D – デフォルトでは、AWS Lambda 関数は、各種 AWS サービスおよびインターネットにアクセスできるセキュアな VPC 内で実行されます。この VPC は、Lambda によって所有されています。また、ユーザーアカウントのデフォルト VPC に接続されていません。ユーザーが Lambda 関数をユーザーアカウントの VPC に接続してプライベートリソースにアクセスしている場合、その VPC からアクセス権限を付与されない限り、その関数はインターネットにアクセスすることはできません。プライベートサブネットからインターネットにアクセスするには、Network Address Translation (NAT) が必要です。関数がインターネットにアクセスできるようにするには、送信トラフィックをパブリックサブネット内の NAT ゲートウェイにルーティングします。

4) D – マウントターゲットに関連付けるセキュリティグループにおいて、インスタンスによって使用されているセキュリティグループからの、TCP プロトコルを用いた NFS ポート経由の受信アクセスを許可する必要があります。

5) C – CloudFormation StackSets を使用することにより、複数のアカウントおよび複数の AWS リージョンにまたがるスタックを、1 回の操作で作成、更新、および削除できます。AWS Organizations 管理アカウントのユーザーは、サービス管理型権限を使用して、スタックセットを作成することができます。スタックセットは、組織内または特定の組織単位 (OU) 内のアカウントにスタックインスタンスを展開します。たとえば、AWS CloudFormation StackSets を使用して、中央 IAM ロールを組織内のすべてのアカウントに展開することができます。

6) A – Amazon CloudWatch アラームアクションを使用することにより、Amazon EC2 インスタンスを自動的に停止、削除、再起動、または復旧するためのアラームを作成できます。たとえば、物理ホストのハードウェアまたはソフトウェアに問題が発生した、ネットワーク接続が切断された、システムの電力供給が喪失した、などの理由によりインスタンスが正常に機能しなくなった場合、復旧アクションを自動開始して、インスタンスを別のハードウェアに移行することができます。また、復旧アクションの通知を受信するため、Amazon Simple Notification Service (Amazon SNS) トピックにパブリッシュされるよう、メッセージを構成することができます。

7) B – AWS Backup はフルマネージド型バックアップサービスです。AWS Backup を使用することにより、各種 AWS サービスのデータのバックアップ処理を簡単に集中管理および自動化できます。タグを使用したリソース割り当ては、複数のリソースをバックアップするためのシンプルで拡張性の高い方法です。指定したタグが付けられているリソースはすべて、バックアッププランに割り当てられます。タグポリシーは、AWS Organizations におけるサービスコントロールポリシー (SCP) の一種であり、組織のアカウントの各種リソースに付けるタグを標準化するうえで役立ちます。

8) B – AWS CloudTrail ログファイルの整合性を検査し、Amazon S3 バケットに配信された CloudTrail ログファイルがその後修正されたり削除されたりしていないかどうかを確認することができます。検査済みログファイルを使用すれば、ログファイル自体が修正されていないことや、特定のユーザー認証情報によって特定の API 処理が実行されたことを明言できます。また、CloudTrail ログファイルの整合性検査プロセスでは、ログファイルが削除または修正されたかどうかがユーザーに通知されます。ユーザーは、特定の期間にログファイルがアカウントに配信されたかされなかったかを明言するための、確固とした情報を得ることができます。トレイルを作成または更新する際、CloudTrail コンソールでログファイルの整合性検査を有効化できます。

9) C – Amazon Data Lifecycle Manager (Amazon DLM) を使用することにより、Amazon Elastic Block Store (Amazon EBS) スナップショットの作成、保持、および削除を自動化できます。ユーザーは、特定のタグを含めたライフサイクルポリシーを作成することにより、EBS ボリュームを指定したスケジュールに従ってバックアップし、バックアップデータを指定した期間保持することができます。たとえば、EBS ボリュームのスナップショットを毎日作成し、30 日間保持することができます。

10) B – ユーザー定義タグとは、ユーザーが手動で定義および作成し、リソースに適用するタグのことです。Tag Editor を使用することにより、すべてのリソースを検索し、それらのリソースにタグを適用することができます。コスト配分タグを使用して、AWS コストを詳細に追跡します。コスト配分タグを有効化すると、AWS によってそれらのタグが使用され、リソースコストが整理されます。これにより、AWS コストを簡単に分類および追跡できます。たとえば、部署別のコストを追跡する場合、"Department" という名前のタグを使用し、タグの値として部署名を指定することができます。

11) 試験ラボの解答:

カスタムデータベースパラメータグループを作成して、event_scheduler パラメータの値を true に設定し、データベースインスタンス作成時にこのパラメータを使用します。

i. https://console.amazonaws.com/rds/ にアクセスし、Amazon RDS コンソールを開きます。
ii. **[Resources]** セクションで **[Parameter groups]** を選択します。
iii. **[Create parameter group]** を選択します。
iv. **[Parameter group family]** の一覧で **[mysql8.0]** を選択します。
v. **[Group name]** ボックスに、新しいデータベースクラスターパラメータグループの名前（**「mysql80witheventscheduler」**）を入力します。
vi. **[Description]** ボックスに、この新しいデータベースクラスターパラメータグループの説明を入力します。
vii. **[Create]** を選択します。
viii. パラメータグループの一覧で、修正したいパラメータグループ（**mysql80witheventscheduler**）の横にあるチェックボックスをオンにします。
ix. **[Parameter group actions]** を選択し、**[Edit]** を選択します。
x. **[Filter parameters]** ボックスに**「event_s」**と入力します。これにより、**"event_scheduler"** パラメータだけがフィルタリングされます。
xi. **event_scheduler** パラメータに対するボックスを選択します。**[Values]** で、設定を **[ON]** に変更します。
xii. **[Save changes]** を選択します。

カスタム AWS Key Management Service (AWS KMS) キーを作成し、データベースインスタンス作成時にこのキーを使用します。

i. https://console.aws.amazon.com/kms にアクセスし、AWS KMS コンソールを開きます。
ii. ナビゲーションペインで **[Customer managed keys]** を選択します。
iii. **[Create key]** を選択します。
iv. 対称型 CMK を作成するため、**[Key type]** で **[Symmetric]** を選択します。
v. **[Next]** を選択します。
vi. CMK のエイリアスまたは表示名を入力します。このウォークスルーでは、**「mysqlDbKey」**という値を使用します。
vii. (オプション) CMK の説明を入力します。
viii. **[Next]** を選択します。
ix. (オプション) タグを追加するため、**[Add tag]** をクリックします。タグキーおよび任意のタグ値を入力します。複数のタグを CMK に追加するには、**[Add tag]** を選択します。
x. 完了したら、**[Next]** を選択します。
xi. この CMK を管理できる IAM ユーザーおよび IAM ロールを選択します。このウォークスルーでは、あなたの IAM ユーザーを使用します。
xii. **[Next]** を選択します。

xiii. この CMK を暗号化処理に使用できる、IAM ユーザーおよび IAM ロールを選択します。このウォークスルーでは、どちらも不要です。
xiv. **[Next]** を選択します。
xv. 選択内容に基づいて作成されたキーポリシードキュメントを確認します。このキーポリシードキュメントは編集可能です。
xvi. **[Finish]** を選択し、CMK を作成します。

CIDR ブロック 192.168.1.0/24 から TCP ポート 3306 へのアクセスを許可する **VPC セキュリティグループを作成し、データベースインスタンス作成時にこのセキュリティグループを使用します。**

i. https://console.aws.amazon.com/vpc/home にアクセスし、Amazon VPC コンソールを開きます。
ii. ナビゲーションペインで **[Security Groups]** を選択します。
iii. **[Create security group]** を選択します。
iv. セキュリティグループの名前（例えば**「mysqlAccessGroup」**）を入力し、次に、セキュリティグループの説明を入力します。
v. **[VPC]** で VPC の ID を選択します。
vi. **[Inbound rules]** で **[Add rule]** を選択します。
vii. **[Type]** を **[MYSQL/Aurora]** にします。
viii. **[Source]** を**「192.168.1.0/24」**にします。
ix. 下へスクロールし、**[Create security group]** を選択します。

Amazon RDS データベースインスタンスを起動します。

i. https://console.aws.amazon.com/rds/ にアクセスし、Amazon RDS コンソールを開きます。
ii. ナビゲーションペインで **[Databases]** を選択します。
iii. **[Create database]** を選択します。
iv. **[Create database]** ページで、**[Standard create]** オプションが選択されていることを確認します。次に、**[MySQL]** を選択します。
v. **[Templates]** セクションで **[Production]** を選択します。
vi. **[DB instance identifier]** セクションで**「mysqldemo」**という名前を入力します。
vii. **[Settings]** セクションで次の値を指定します。
    i. **[Master password]**
    ii. **[Confirm password]**: パスワードを再入力します。
viii. **[DB instance size]** セクションで次の値を指定します。
    iii. **[Burstable classes (includes t classes)]**
    iv. **[db.t3.micro]**
ix. **[Connectivity]** セクションの **[Virtual private cloud (VPC)]** で、既存の VPC を選択します。
x. **[Additional connectivity configuration]** メニューを展開し、次の値を指定します。
    v. **[Subnet group]** でデータベースサブネットグループを選択します。

vi. **[Public access]** で **[No]** を選択します。
vii. **[Existing VPC security groups]** で **[mysqlAccessGroup]** を選択します。
xi. デフォルトのセキュリティグループなど、他の既存セキュリティグループを削除するため、各セキュリティグループに対する **[X]** を選択します。
xii. **[Additional configuration]** セクションを展開します。
xiii. **[DB parameter group]** で **[mysql80witheventscheduler]** を選択します。
xiv. **[Master key]** で **[mysqlDbKey]** を選択します。
xv. **[Create database]** を選択し、RDS MySQL データベースインスタンスを作成します。

起動後、RDS データベーススナップショットを手動で作成します。

i. https://console.aws.amazon.com/rds/ にアクセスし、Amazon RDS コンソールを開きます。
ii. ナビゲーションペインで **[Databases]** を選択します。
iii. データベースインスタンスの一覧で、スナップショットを作成したいデータベースインスタンスを選択します。
iv. **[Actions]** を選択し、**[Take snapshot]** を選択します。
v. **[Take DB snapshot]** ウィンドウが開きます。
vi. **[Snapshot name]** ボックスにスナップショットの名前を入力します。このウォークスルーでは、**「mysqlsnapshot」**を使用します。
vii. **[Take snapshot]** を選択します。
viii. RDS コンソールのナビゲーションペインで、**[Snapshots]** を選択します。
ix. スナップショット名として **[mysqlsnapshot]** を選択します。
x. **[Details]** セクションで、ARN フィールドおよび ARN を確認します。

データベーススナップショットの ARN を入力してください:_____

