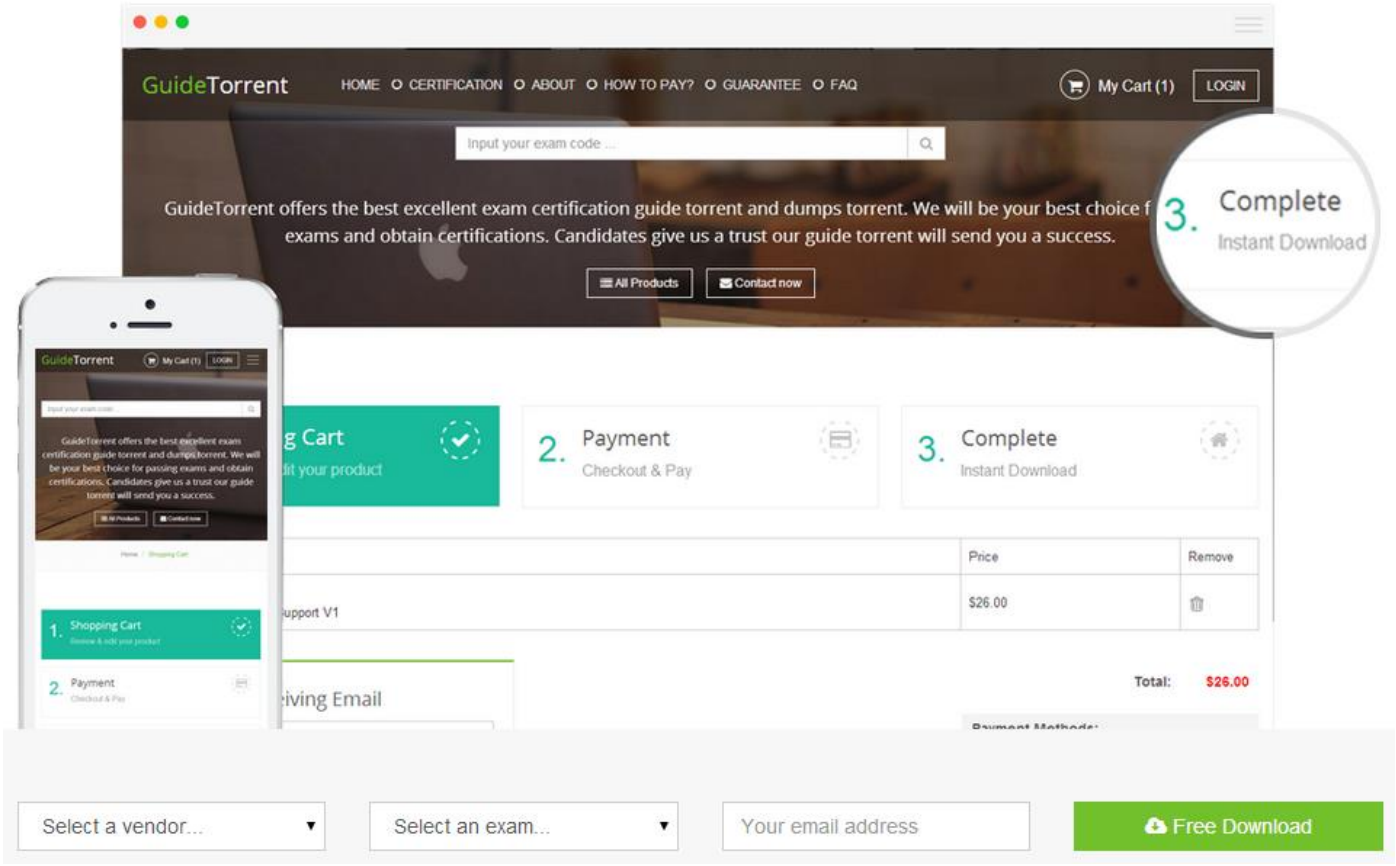
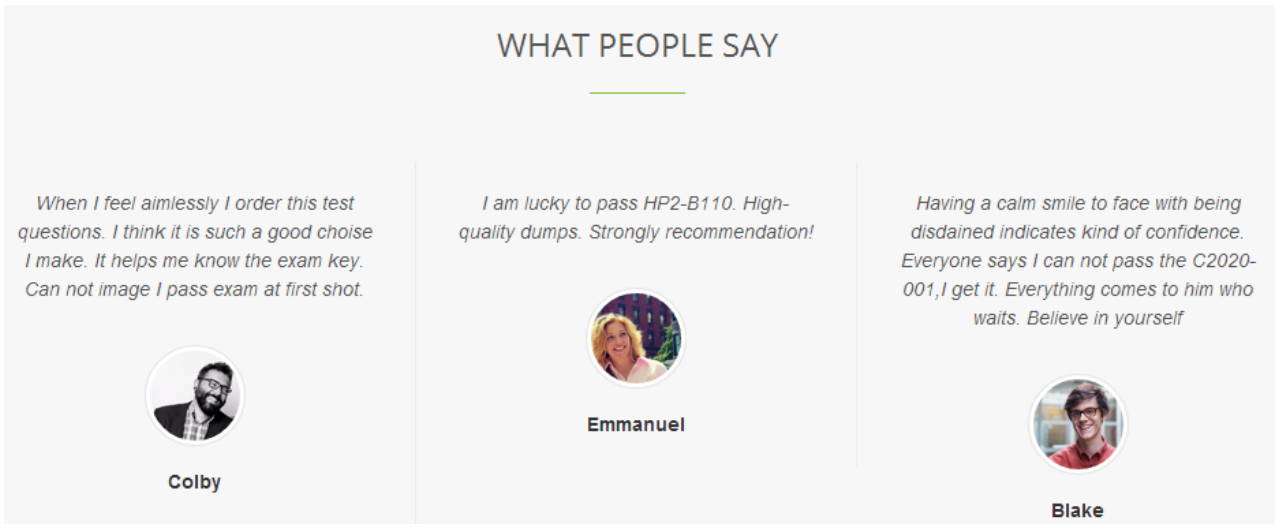
GuideTorrent





http://www.guidetorrent.com

The best excellent exam certification guide torrent and dumps torrent provider

Exam : **SOA-C02-JPN**

Title : AWS Certified SysOps Administrator - Associate (SOA-C02日本語版)

Vendor : Amazon

Version : DEMO

QUESTION NO: 1
SysOps 管理者がアプリケーションをテストしています。マットは 5 つの Amazon EC2 インスタンスでホストされています。アプリケーション ロード バランサー (ALB) の背後にある Auto Scaling グループでインスタンスが実行されています。SysOps 管理者は、トラブルシューティングを行って、Auto Scaling グループがスケールアウトする前に、高い CPU 使用率の根本原因を見つける必要があります。
これらの要件を満たすために、SysOps 管理者はどのアクションを実行する必要がありますか?
A. インスタンスのスケールイン保護を有効にします。
B. インスタンスをスタンバイ状態にします。
C. ALB からリスナーを削除します
D. Launch および Terminate プロセス タイプを一時停止します。
Answer: D
Explanation:
You can put an instance that is in the InService state into the Standby state, update or troubleshoot the instance, and then return the instance to service. Instances that are on standby are still part of the Auto Scaling group, but they do not actively handle load balancer traffic.
https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-enter-exit-standby.html

QUESTION NO: 2
ある企業は、Application Load Balancer の背後にある Amazon EC2 インスタンスで Web サイトをホストしています。
同社は Amazon Route 53 を使用して DNS を管理しており、ドメインのゾーン頂点を Web サイトにポイントしたいと考えています。
これらの要件を満たすにはどのタイプのレコードを使用する必要がありますか?
A. ドメインのゾーン頂点のAAAAレコード
B. ドメインのゾーン頂点のAレコード
C. ドメインのゾーン頂点のCNAMEレコード
D. ドメインのゾーン頂点のエイリアスレコード
Answer: D
Explanation:
Route 53 supports redirection of zone apex to the ALB via alias.
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing- alias-non-alias.html
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-elb-load-balancer.html

QUESTION NO: 3
ある企業は、VPCと自社のオンプレミスデータセンターでコンピューティングリソースを運用しています。VPCとオンプレミスデータセンターの間には、既にAWS Direct Connect接続が確立されています。
SysOps 管理者は、VPC 内の Amazon EC2

インスタンスがオンプレミスデータセンター内のホストの DNS
名を解決できることを確認する必要があります。
継続的なメンテナンスを最小限に抑えながらこの要件を満たすソリューションはどれでしょうか?

A. Amazon Route 53
プライベートホストゾーンを作成します。オンプレミスデータセンター内のホストのホスト名と IP アドレスをゾーンに入力します。

B. Amazon Route 53 Resolver
のアウトバウンドエンドポイントを作成します。転送が必要なドメイン名に対応するオンプレミス DNS サーバーの IP アドレスを追加します。

C. Amazon Route 53 Resolver で逆引きDNSクエリの転送ルールを設定します。VPC の enableDnsHostnames 属性を true に設定します。

D. オンプレミスホストのホスト名と IP アドレスを各 EC2 インスタンスの /etc/hosts ファイルに追加します。

Answer: B

Explanation:
By creating an Amazon Route 53 Resolver outbound endpoint and configuring forwarding rules to send DNS queries to the on-premises DNS servers, EC2 instances in the VPC can dynamically resolve hostnames in the on-premises data center. This solution leverages AWS managed DNS forwarding and minimizes ongoing maintenance compared to manually maintaining DNS records or host file configurations.

QUESTION NO: 4
オンコールエンジニアのチームは、トラブルシューティングやコマンド実行のために、プライベートサブネット内の Amazon EC2 インスタンスに頻繁に接続する必要があります。
インスタンスでは、AWS が提供する最新の Windows Amazon マシンイメージ (AMI) または Amazon Linux AMI のいずれかが使用されます。
チームには、認可用のIAMロールが既に存在します。SysOps管理者は、このロールにIAM権限を付与することで、チームにインスタンスへのアクセスを提供する必要があります。
どのソリューションがこの要件を満たすでしょうか?

A. インスタンスで ssm:StartSession アクションを許可するステートメントを IAM ロールポリシーに追加します。
引き受けた IAM ロールを使用して、AWS Systems Manager Session Manager を使用してインスタンスに接続するようにチームに指示します。

B. 各インスタンスに Elastic IP アドレスとセキュリティ グループを関連付けます。
エンジニアの IP アドレスをセキュリティ グループの受信ルールに追加します。
チームがインスタンスに接続できるように、IAM ロール ポリシーに ec2:AuthorizeSecurityGroupIngress アクションを許可するステートメントを追加します。

C. EC2 インスタンスを使用して要塞ホストを作成し、要塞ホストを VPC に関連付けます。
1AM ロール ポリシーにステートメントを追加して、要塞ホストで ec2:CreateVpnConnection アクションを許可します。
チームに、要塞ホスト
エンドポイントを使用してインスタンスに接続するように指示します。

D. インターネットに接続されたネットワーク ロード バランサーを作成します。
2つのリスナーを使用します。ポート22をLinuxインスタンスのターゲットグループに転送し

ます。
ポート 3389 を Windows インスタンスのターゲット グループに転送します。
チームがインスタンスに接続できるように、IAM ロール ポリシーに ec2:CreateRoute アクションを許可するステートメントを追加します。
Answer: A
Explanation:
https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager.html

QUESTION NO: 5
SysOps 管理者は、Amazon EC2 Auto Scaling グループに Amazon EC2 スポットインスタンスの新しいフリートをプロビジョニングする必要があります。Auto Scaling
グループでは、さまざまなインスタンスタイプが使用されます。構成されたフリートは、起動されるインスタンスの数に対して最も可用性の高いプールから取得する必要があります。これらの要件を満たすソリューションはどれでしょうか?
A. Auto Scalingグループの最大容量までスポットインスタンスを起動します
B. 多様化された戦略を使用してスポットインスタンスを起動します。
C. 容量最適化戦略を使用してスポットインスタンスを起動します。
D.
スポットインスタンスアドバイザーを使用して、最適なスポット割り当て戦略を決定します。
Answer: D
Explanation:
The Spot Instance advisor helps you determine pools with the least chance of interruption and provides the savings you get over on-demand rates.
https://aws.amazon.com/ec2/spot/instance-advisor/

QUESTION NO: 6
ある企業は、Auto Scaling グループ内の Amazon EC2 インスタンスで Web サイトを運営しています。
ウェブサイトのトラフィックが増加すると、ソフトウェアをインストールする長時間実行されるユーザー データ
スクリプトが原因で、追加のインスタンスが使用可能になるまでに数分かかることがあります。
SysOps
管理者は、新しいインスタンスが使用可能になるまでに必要な時間を短縮する必要があります。
この要件を満たすために SysOps
管理者はどのようなアクションを実行する必要がありますか?
A.
トラフィックが増加する前にインスタンスが追加されるように、スケーリングしきい値を下げます。
B. Auto Scaling グループの最大容量の 100%
をカバーするためにリザーブドインスタンスを購入します。
C. Auto Scaling

グループを更新して、ストレージ最適化インスタンスタイプを持つインスタンスを起動します。
D. EC2 Image Builder を使用して、ソフトウェアが事前にインストールされた Amazon Machine Image (AMI) を準備します。
Answer: C

QUESTION NO: 7
ある企業には、接続された Amazon Elastic Block Store (Amazon EBS) ボリュームに対して多くのファイルを読み書きする Linux Amazon EC2 スポット インスタンスのクラスターがあります。EC2 インスタンスは頻繁に起動および停止されます。EC2 インスタンスの起動時のプロセスの一部として、EBS ボリュームがスナップショットから復元されます。スナップショットから復元された EBS ボリュームの初期パフォーマンスが予想より低くなります。会社のワークロードには、接続された EBS ボリューム上のプロビジョニングされた IOPS のほぼすべてが必要です。EBS ボリュームのパフォーマンスが低すぎる場合、EC2 インスタンスはワークロードをサポートできません。SysOps 管理者は、EBS ボリュームがスナップショットから復元されたときに期待されるパフォーマンスを確実に提供できるようにするソリューションを実装する必要があります。
これらの要件を満たすソリューションはどれですか?
A. 使用されるスナップショットで高速スナップショット リストア (FSR) を構成します。
B. 各スナップショットを暗号化されていない EBS ボリュームに復元します。パフォーマンスが安定したら、EBS ボリュームを暗号化します。
C. スナップショットを復元する前に、EBS ボリュームを XFS ファイル システムとしてフォーマットします。
D. Linux 先読みバッファを 1 MiB に増やします。
Answer: A

QUESTION NO: 8
ある企業は、メッセージ形式のファイルを処理するためのデータ取り込みパイプラインを実装しました。フロントエンドアプリケーションはユーザー入力を受け取り、Amazon S3 に保存します。バックエンドアプリケーションは Amazon EC2 インスタンスを使用して、Amazon S3 にアップロードされたオブジェクトを処理します。この企業は最近、顧客トラフィックの大幅な増加を経験しました。フロントエンドアプリケーションが一度に送信するメッセージの数がバックエンドアプリケーションの処理能力を超え、一部のメッセージが失われる問題が発生しています。
最も少ない運用上の労力でこの問題を解決するには、どのアクションを実行する必要がありますか?
A. バックエンドアプリケーションを一連の AWS Lambda 関数として再開発します。
B. バックエンドアプリケーションを置き換えるために Amazon Kinesis データストリームを実装します。
C. Application Load Balancer を実装して、バックエンド アプリケーション

インスタンス全体にメッセージ トラフィックを分散します。
D. フロントエンドコンポーネントとバックエンドコンポーネント間に Amazon Simple Queue Service (Amazon SQS) キューを実装します。
Answer: D
Explanation:
Implementing an Amazon SQS queue between the frontend and backend decouples the processing pipeline. The queue can buffer messages, allowing the backend to process them at its own pace, and preventing message loss during traffic spikes. This solution requires minimal operational effort and can be integrated with the existing architecture without a major redesign.

QUESTION NO: 9
ある企業は、自社のアプリケーションに災害対策（DR）を実装する必要があります。アプリケーションの本番環境は、Auto Scaling グループ内の Amazon EC2 インスタンスと、3 つのリードレプリカを持つ Amazon RDS データベースで構成されています。
DR環境では、Auto Scalingグループ内の単一のEC2インスタンスと、クロスリージョンリードレプリカを1つ使用しています。DNS解決にはAmazon Route 53を使用しています。
SysOps管理者はDRプロセスを自動化する必要があります。ただし、DNSレコードの更新というフェイルオーバーの最終ステップについては、SysOps管理者が手動で制御する必要があります。
最も少ないダウンタイムでこれらの要件を満たすソリューションはどれでしょうか?
A. Auto Scaling グループの EC2 インスタンス数を増やす AWS CloudFormation テンプレートを作成します。3 つの RDS リードレプリカを追加する AWS Systems Manager Run Command ドキュメントを作成します。Route 53 の DNS レコードを更新します。
B. 適切な数のEC2インスタンスを含む新しいAuto Scalingグループをデプロイする AWS CloudFormationテンプレートを作成します。このCloudFormationテンプレートを使用して、新しいRDS DBインスタンスと必要なリードレプリカをデプロイします。DR環境がトラフィックをサポートする準備ができたら、Route 53 DNSレコードを更新するコマンドを送信します。
C. Auto Scaling グループの EC2 インスタンス数を増やし、3 つの RDS リードレプリカを追加し、データベースをフェイルオーバーする AWS Systems Manager Automation ランブックを作成します。DR 環境がトラフィックをサポートできる状態になったら、Route 53 の DNS レコードを更新するコマンドを送信します。
D. Auto Scaling グループの EC2 インスタンス数を増やし、3 つの RDS リードレプリカを追加し、データベースをフェイルオーバーする AWS Systems Manager Run Command ドキュメントを作成します。Route 53 の DNS レコードを更新します。
Answer: C
Explanation:
An AWS Systems Manager Automation runbook can orchestrate the multi-step DR actions - scale the ASG, add replicas, and promote/fail over the DB - quickly and repeatably. You keep manual control by triggering the final Route 53 update only after the runbook finishes preparing the DR site. This yields minimal downtime with controlled DNS cutover.

QUESTION NO: 10
SysOps管理者は、Amazon
CloudFrontディストリビューションのキャッシュヒット率が10%未満であることに気づきました。SysOps管理者は、ディストリビューションのキャッシュヒット率を向上させ、ネットワークパフォーマンスを改善し、オリジンの負荷を軽減する必要があります。
これらの要件を満たすために、SysOps
管理者はどのようなアクションの組み合わせを実行する必要がありますか?
（2つ選択してください。）
A. 必要な AWS リージョンに対して CloudFront Origin Shield を有効にします。
B. ビューアー プロトコル ポリシーを HTTPS のみを使用するように変更します。
C.
2つ目のオリジンを追加します。両方のオリジンを含むオリジングループを作成します。CloudFront オリジンフェイルオーバーを有効にします。
D. キャッシュ動作設定でオブジェクトの自動圧縮をオンにします。
E. キャッシュ動作設定で CloudFront TTL 値を増やします。
Answer: AE
Explanation:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/origin-shield.html

QUESTION NO: 11
AWSマネージドVPN接続をセットアップする際、SysOps管理者はAWSにカスタマーゲートウェイリソースを作成します。カスタマーゲートウェイデバイスは、その前にNATゲートウェイがあるデータセンターにあります。
カスタマーゲートウェイリソースを作成するには、どのアドレスを使用する必要がありますか？
A.カスタマーゲートウェイデバイスのプライベートIPアドレス
B.カスタマーゲートウェイデバイスの前にあるNATデバイスのMACアドレス
C.カスタマーゲートウェイデバイスのパブリックIPアドレス
D.カスタマーゲートウェイデバイスの前にあるNATデバイスのパブリックIPアドレス
Answer: D
Explanation:
If your customer gateway device is behind a network address translation (NAT) device, use the IP address of your NAT device.
https://docs.aws.amazon.com/vpn/latest/s2svpn/cgw-options.html

QUESTION NO: 12
SysOps 管理者は、プライベート Amazon S3 バケットのオブジェクトを、AWS
アカウントを持たないユーザーグループと安全に共有したいと考えています。
この要件を満たす最も運用効率の高いソリューションは何ですか?
A. ユーザーの IP アドレスからのオブジェクトのダウンロードのみを許可する S3
バケットポリシーをアタッチします。
B.
オブジェクトへのアクセス権を持つIAMロールを作成します。ユーザーにロールを引き受け

るよう指示します。
C.
オブジェクトへのアクセス権を持つIAMユーザーを作成します。認証情報をユーザーと共有します。
D. オブジェクトの署名付きURLを生成します。このURLをユーザーと共有します。
Answer: D
Explanation:
https://docs.aws.amazon.com/AmazonS3/latest/userguide/ShareObjectPreSignedURL.html

QUESTION NO: 13
企業は、AWS Organizations を使用して AWS
上の一連のアカウントを管理します。同社のセキュリティ チームは、ネイティブ AWS
サービスを使用して、Center for Internet Security (CIS) の AWS Foundations Benchmark
に対してすべての AWS アカウントを定期的にスキャンしたいと考えています。
これらの要件を満たす最も運用効率の高い方法は何ですか?
A. 中央セキュリティ アカウントを AWS Security Hub
管理者アカウントとして指定します。Security Hub
管理者アカウントから招待を送信し、メンバー
アカウントからの招待を受け入れるスクリプトを作成します。新しいアカウントが作成されるたびにスクリプトを実行します。
CIS AWS Foundations Benchmark スキャンを実行するように Security Hub を設定します。
B. Amazon Inspector を使用して、すべてのアカウントに対して CIS AWS Foundations
ベンチマークを実行します。
C. 中央セキュリティアカウントを Amazon GuardDuty
管理者アカウントとして指定します。GuardDuty
管理者アカウントから招待を送信し、メンバー
アカウントからの招待を受け入れるスクリプトを作成します。新しいアカウントが作成されるたびにスクリプトを実行します。
CIS AWS Foundations Benchmark スキャンを実行するように GuardDuty を構成します。
D. AWS Security Hub
管理者アカウントを指定します。組織内の新しいアカウントを構成して、自動的にメンバーアカウントになるようにします。CIS AWS Foundations ベンチマーク
スキャンを有効にします。
Answer: D

QUESTION NO: 14
Amazon EC2 インスタンス上でデータ分析アプリケーションが実行中です。SysOps
管理者は、Amazon CloudWatch
エージェントによって収集されるメトリクスにカスタムディメンションを追加する必要があります。
SysOps 管理者はどのようにしてこの要件を満たすことができますか?
A. Amazon CloudWatch
エージェントを使用してディメンションを抽出し、メトリクスを収集するためのカスタム
シェル スクリプトを作成します。

B. 必要なカスタムディメンションを評価し、メトリクスを Amazon Simple Notification Service (Amazon SNS) に送信するための Amazon EventBridge (Amazon CloudWatch Events) ルールを作成します。
C. AWS CloudTrail からメトリクスを収集し、Amazon CloudWatch Logs グループに送信する AWS Lambda 関数を作成します。
D. メトリクスを収集するには、Amazon CloudWatch エージェント設定ファイルに append_dimensions フィールドを作成します。
Answer: D
Explanation:
In custom metrics, the --dimensions parameter is common. A dimension further clarifies what the metric is and what data it stores. You can have up to 30 dimensions assigned to one metric, and each dimension is defined by a name and value pair.
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/publishingMetrics.html

QUESTION NO: 15
ある企業は、単一の AWS リージョンで数百の Amazon EC2 インスタンスを実行しています。各 EC2 インスタンスには、2 つの接続された 1 GiB 汎用 SSD (gp2) Amazon Elastic Block Store (Amazon EBS) ボリュームがあります。重要なワークロードが、EBS ボリュームで利用可能なすべての IOPS 容量を使用しています。
会社のポリシーによると、会社は、会社のアプリケーションが適切に機能することを検証するための長い受け入れテストを完了することなく、インスタンス タイプまたは EBS ボリューム タイプを変更することはできません。SysOps 管理者は、EBS ボリュームの I/O パフォーマンスをできるだけ早く向上させる必要があります。
これらの要件を満たすために、SysOps 管理者はどのアクションを実行する必要がありますか?
A. 1 GiB EBS ボリュームのサイズを増やします。
B. 各 EC2 インスタンスに 2 つのエラスティック ネットワーク インターフェイスを追加します。
C. リージョン内の EBS ボリュームで Transfer Acceleration をオンにします。
D. すべての EC2 インスタンスをクラスター配置グループに追加します。
Answer: A
Explanation:
With Amazon EBS Elastic Volumes, you can increase the volume size, change the volume type, or adjust the performance of your EBS volumes. If your instance supports Elastic Volumes, you can do so without detaching the volume or restarting the instance. This enables you to continue using your application while the changes take effect.
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-modify-volume.html They have Elastic Volumes in place (per the question) and that's exactly why it is specified in the question. As others have mentioned, increasing the volume size increases IOPS, up to the volume type max. For gp2, you can have a volume size of 1 GiB - 16 TiB with a max IOPS of 16,000 for the 16 TiB volume size.
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-volume-types.html

QUESTION NO: 16

ある企業が顧客の売上データを分析しています。顧客が会社のAmazon S3バケットの1つにファイルをアップロードすると、Amazonリソースネーム（ARN）オブジェクトを含むAmazon Simple Queue Service（Amazon SQS）キューにメッセージがポストされます。Amazon EC2インスタンス上で実行されるアプリケーションがキューをポーリングし、メッセージを処理します。処理時間はファイルのサイズによって異なります。
顧客からファイルの処理に遅延が発生しているとの報告を受けています。SysOps管理者は、最初のステップとしてAmazon EC2 Auto Scalingを設定することにしました。SysOps管理者は、既存のEC2インスタンスをベースにしたAmazon Machine Image（AMI）を作成します。また、AMIを参照する起動テンプレートも作成します。
応答時間を改善するために、SysOps 管理者は Auto Scaling ポリシーをどのように構成する必要がありますか?

A. 起動テンプレートにいくつかの異なるインスタンス サイズを追加します。キュー内のメッセージ数に基づいてインスタンスのサイズを選択するには、approximateNumberOfMessagesVisible メトリックに基づいて Auto Scaling ポリシーを作成します。

B. キュー内の遅延されたメッセージの数に基づいてインスタンスの数をスケーリングするための approximateNumberOfMessagesDelayed メトリックに基づく Auto Scaling ポリシーを作成します。

C. Auto Scaling グループの ASGAverageCPUUtilization メトリックと GroupPendingInstances メトリックに基づいてカスタムメトリックを作成します。アプリケーションを変更してメトリクスを計算し、1 分ごとに Amazon CloudWatch にメトリクスを投稿します。このメトリックに基づいて Auto Scaling ポリシーを作成し、インスタンスの数をスケーリングします。

D. approximateNumberOfMessagesVisible メトリックと Auto Scaling グループ内の InService 状態のインスタンスの数に基づいてカスタムメトリックを作成します。アプリケーションを変更してメトリクスを計算し、1 分ごとに Amazon CloudWatch にメトリクスを投稿します。このメトリックに基づいて Auto Scaling ポリシーを作成し、インスタンスの数をスケーリングします。

Answer: D

Explanation:
When there are delays in processing files due to a high volume of messages in the queue, adding more instances using Auto Scaling can help to reduce the processing time. The ApproximateNumberOfMessagesVisible metric is a good indicator of the workload on the EC2 instances. By creating an Auto Scaling policy based on this metric, the number of instances can be scaled up or down depending on the number of messages in the queue.
https://docs.aws.amazon.com/autoscaling/ec2/userguide/ec2-auto-scaling-target-tracking-metric- math.html#metric-math-sqs-queue-backlog

QUESTION NO: 17
企業は、Amazon Aurora MySQL DB

クラスターにデータベースをデプロイすることを計画しています。データベースには、デモンストレーション環境用のデータが格納されます。データは毎日リセットする必要があります。
これらの要件を満たす最も運用効率の高いソリューションは何ですか?
A. データが入力された後、DB クラスターの手動スナップショットを作成します。毎日 AWS Lambda 関数を呼び出す Amazon EventBridge (Amazon CloudWatch Events) ルールを作成します。スナップショットを復元してから、以前の DB クラスターを削除する機能を設定します。
B. DB クラスターの作成中にバックトラック機能を有効にします。48 時間のターゲット バックトラック ウィンドウを指定します。毎日 AWS Lambda 関数を呼び出す Amazon EventBridge (Amazon CloudWatch Events) ルールを作成します。バックトラック操作を実行するように関数を構成します。
C. データが取り込まれた後、DB クラスターの手動スナップショットを Amazon S3 バケットにエクスポートします。毎日 AWS Lambda 関数を呼び出す Amazon EventBridge (Amazon CloudWatch Events) ルールを作成します。Amazon S3 からスナップショットを復元する機能を設定します。
D. DB クラスターのバックアップ保持期間を 2 日に設定します。毎日 AWS Lambda 関数を呼び出す Amazon EventBridge (Amazon CloudWatch Events) ルールを作成します。DB クラスターを特定の時点に復元してから、以前の DB クラスターを削除する機能を設定します。
Answer: B
Explanation:
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Managing .Ba cktrack.html

QUESTION NO: 18
会社には、AWSのすべてのリソースが設定されたポリシーに従ってタグ付けされなければならないという新しい要件があります。
ポリシーに準拠していないすべてのリソースを適用し、継続的に特定するには、どのAWS サービスを使用する必要がありますか？
A.AWS CloudTrail
B.Amazon Inspector
C.AWSConfig
D.AWS Systems Manager
Answer: C
Explanation:
https://aws.amazon.com/config

QUESTION NO: 19
ある会社が、ポイントインタイムリカバリ、バックトラッキング、および自動バックアップが有効になっているAmazon Aurora MySQLDBクラスターを使用しています。
SysOps管理者は、過去72時間以内にDBクラスターを特定のリカバリポイントにロールバックできる必要があります。復元は、同じ実動DBクラスターで完了する必要があります。
これらの要件を満たすソリューションはどれですか？

A.Auroraレプリカを作成します。レプリカをプロモートして、プライマリDBインスタンスを置き換えます。
B.AWS Lambda関数を作成して、既存のDBクラスターに自動バックアップを復元します。
C.バックトラッキングを使用して、既存のDBクラスターを目的のリカバリポイントに巻き戻します。
D.ポイントインタイムリカバリを使用して、既存のDBクラスタを目的のリカバリポイントに復元します。
Answer: C
Explanation:

Resolution

Note: If you receive errors when running AWS Command Line Interface (AWS CLI) commands, make sure that you're using the most recent version of the AWS CLI.

Amazon Aurora backs-up your cluster volume's changes automatically and continuously. The back-ups are retained for the length of your backup retention period. This continuous backup also means that you are able to restore your data to a new cluster, to any point in time within the retention period specified. This avoids the need for a lengthy binlog roll-forward process. Because you create a new cluster, there is no impact to performance or interruption to your original database.

When you initiate a clone, snapshot, or point in time restore, Amazon RDS calls the following APIs on your behalf:

- Either RestoreDBClusterFromSnapshot or RestoreDBClusterToPointInTime. This creates a new cluster and restores volume from Amazon Simple Storage Service (Amazon S3). This can take up to two hours to complete. This is because when you restore data to an Aurora cluster, all of the data must be brought in parallel from Amazon S3 to the six copies on your three AZs.
- Cluster storage volume cloning is a variation of RestoreDBClusterToPointInTime. It uses the copy-on-write protocol, and usually completes in a few minutes.

Reference:
https://aws.amazon.com/premiumsupport/knowledge-center/aurora-mysql-slow-snapshot-restore/
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/AuroraMySQL.Managing.Ba cktrack.html

QUESTION NO: 20
ある企業は、Amazon
EC2インスタンス上で稼働するビジネスクリティカルなアプリケーションをサポートしています。このアプリケーションは、オンプレミスデータセンターで稼働するサービスからデータを受信しています。エンドユーザーから、データ更新に関連する断続的な問題が報告されています。これらの問題は、AWSとオンプレミスデータセンター間の利用可能なネットワーク帯域幅の変動が原因で発生しています。
SysOps 管理者は、アプリケーション スタックへの変更を最小限に抑えながら、ユーザーエクスペリエンスとアプリケーションのパフォーマンスを向上させる必要があります。
これらの要件を満たしながら、最もパフォーマンスが向上するソリューションはどれでしょうか?
A. サービスを AWS に移行し、自動スケーリングを実装します。

B. Amazon S3 Transfer Acceleration を使用するようにサービスを変更します。
C. オンプレミスのデータセンターとの AWS Direct Connect 接続を設定します。
D. AWS Storage Gateway を使用してデータを AWS に移動します。
Answer: A
Explanation:
https://docs.aws.amazon.com/AmazonS3/latest/userguide/transfer-acceleration.html

QUESTION NO: 21
SysOps 管理者は、カスタムネットワーク ACL を活用したパブリックサブネットとプライベートサブネットを持つ VPC のトラブルシューティングを行っています。プライベートサブネット内のインスタンスはインターネットにアクセスできません。パブリックサブネットにはインターネットゲートウェイが接続されています。プライベートサブネットには、同じくパブリックサブネットに接続された NAT ゲートウェイへのルートがあります。Amazon EC2 インスタンスは、VPC のデフォルトのセキュリティグループに関連付けられています。
このシナリオで問題が発生する原因は何でしょうか?
A.
プライベートサブネット上に、すべての送信トラフィックを拒否するように設定されたネットワーク ACL があります。
B. VPC のプライベートサブネットに NAT ゲートウェイがデプロイされていません。
C. VPC のデフォルトのセキュリティグループは、EC2 インスタンスへのすべての受信トラフィックをブロックします。
D. VPC のデフォルトのセキュリティグループは、EC2 インスタンスからのすべての送信トラフィックをブロックします。
Answer: A
Explanation:
Network ACLs (Access Control Lists) are stateless and operate at the subnet level. If there is a network ACL on the private subnet that is configured to deny all outbound traffic, it would prevent instances in the private subnet from accessing the internet through the NAT gateway .

QUESTION NO: 22
ある会社には、MySQLを実行するAmazonEC2インスタンスで構成されるデータベース層を持つWebアプリケーションがあります。
SysOps管理者は、潜在的なデータ損失と、データベース障害が発生した場合の回復に必要な時間を最小限に抑える必要があります。
これらの要件を満たす最も運用効率の高いソリューションは何ですか？
A.StatusCheckFailed_SystemメトリクスのAmazon CloudWatchアラームを作成して、EC2インスタンスを停止および開始するAWSLambda関数を呼び出します。
B.MySQL Multi-AZDBインスタンス用のAmazonRDSを作成します。 Amazon S3に保存されているMySQLネイティブバックアップを使用して、データを新しいデータベースに復元します。 Webアプリケーションの接続文字列を更新します。
C.リードレプリカを使用してMySQL Single-

AZDBインスタンス用のAmazonRDSを作成します。 Amazon S3に保存されているMySQLネイティブバックアップを使用して、データを新しいデータベースに復元します。 Webアプリケーションの接続文字列を更新します。

D.Amazon Data Lifecycle Manager（Amazon DLM）を使用して、Amazon Elastic Block Store（Amazon EBS）ボリュームのスナップショットを1時間ごとに取得します。 EC2インスタンスに障害が発生した場合は、スナップショットからEBSボリュームを復元します。

Answer: D

Explanation:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/snapshot-lifecycle.html

QUESTION NO: 23

アプリケーションは、Amazon Aurora PostgreSQL マルチAZ DB クラスター上で稼働するデータベースにアクセスします。アプリケーションのユーザー数が増加し、負荷が増加しています。SysOps 管理者は、データベースユーザー接続をプールして共有することで、アプリケーションのパフォーマンスを向上させる必要があります。

どのソリューションがこの要件を満たすでしょうか?

A. DB クラスターの IOPS を増やします。

B. Amazon RDS Proxy を使用してプロキシを設定します。プロキシを DB クラスターに関連付けます。

C. DBクラスターで拡張モニタリングを有効にします。ログをAmazon CloudWatchに移動します。

D. DB クラスターで Performance Insights を 35 日間有効にします。

Answer: B

Explanation:

Amazon RDS Proxy pools and reuses database connections for Aurora PostgreSQL, reducing overhead from frequent opens/closes and letting many application clients share fewer backend connections - directly improving performance under increased load.

QUESTION NO: 24

ある企業では、メモリを大量に消費するアプリケーションをElastic Load Balancer（ELB）の背後にあるAmazon EC2インスタンス群で実行しています。これらのインスタンスはAuto Scalingグループで実行されています。SysOps管理者は、アプリケーションに接続するユーザー数に応じてアプリケーションがスケールできることを確認する必要があります。

これらの要件を満たすソリューションはどれでしょうか?

A. ELB から生成される ActiveConnectionCount Amazon CloudWatch メトリックに基づいてアプリケーションをスケーリングするスケーリングポリシーを作成します。

B. ELB から生成される mem_used Amazon CloudWatch メトリックに基づいてアプリケーションをスケーリングするスケーリングポリシーを作成します。

C. 追加の接続をサポートするために、Auto Scaling グループ内の EC2

インスタンスの数を増やすスケジュールされたスケーリングポリシーを作成します。
D. 接続ユーザー数をカスタム Amazon CloudWatch
メトリクスとして公開するためのスクリプトを ELB
に作成してデプロイします。このメトリクスを使用するスケーリングポリシーを作成します
。
Answer: A

QUESTION NO: 25
ある企業がAmazon
EC2インスタンス上で開発アプリケーションを実行しています。このアプリケーションは、デフォルトの暗号化が有効になっているターゲットAmazon
S3バケットに、サイズ1GBのファイル50万個をアップロードします。EC2インスタンスは
、S3バケットがデプロイされているAWSリージョンと同じリージョンにあります。
同社では、アプリケーションソフトウェアに組み込まれているパフォーマンスログを使用しています。ログを見ると、アプリケーションがS3バケットへのファイルの書き込みを常に待機していることがわかります。SysOps管理者は、アプリケーションのスループットパフォーマンスを改善する必要があります。SysOps管理者は、EC2インスタンスのネットワークが制限されていないことを確認しています。
S3 アップロードのパフォーマンスを向上させるために、SysOps
管理者は何をすべきでしょうか?
A. S3 バケットで S3 Transfer Acceleration を有効にします。
B. S3
書き込み操作を分割し、複数のバケットプレフィックスを使用してアイテムを並列に書き込みます。
C. Amazon S3 用の AWS PrivateLink を設定します。S3 バケットの暗号化をオフにします。
D. リージョンでAWS Global
Acceleratorを設定します。S3バケットの暗号化をオフにします。
Answer: B

QUESTION NO: 26
ある企業は、マイクロサービスベースのアプリケーションをホストするために、Amazon Elastic Kubernetes Service (Amazon ECS) 上に Kubernetes
クラスターを実装しました。同社は来月、アプリケーションのトラフィックが大幅に増加すると予想しており、リクエスト数の急増によるアプリケーションのクラッシュを回避したいと考えています。
管理オーバーヘッドを最小限に抑えながらこれらの要件を満たすソリューションはどれでしょうか?
A.
2つ目のEKSクラスターを作成します。2つのクラスター間でワークロードを負荷分散します
。
B. Kubernetes Horizontal Pod Autoscaler を実装します。目標の CPU 使用率を設定します。
C. 翌月、アプリケーションを Amazon EKS から Amazon EC2
に移行します。月末にアプリケーションを Amazon EKS に戻します。
D. Kubernetes Vertical Pod Autoscaler を実装します。目標の CPU 使用率を設定します。

Answer: B
Explanation:
The Kubernetes Horizontal Pod Autoscaler (HPA) is designed to automatically scale the number of pods in a deployment or replica set based on observed CPU or memory utilization. In this scenario, the company wants to prevent the application from crashing due to high request traffic.
The HPA can dynamically adjust the number of pods based on CPU utilization, ensuring that the application can handle increased traffic while avoiding overloading the system.

QUESTION NO: 27
ある企業は、インポートされたキーマテリアルを含む AWS KMS カスタマーマスターキー (CMK) を使用しています。同社は、データを暗号化するために Java アプリケーション内でエイリアスによって CMK を参照します。CMK は 6 か月ごとにローテーションする必要があります。
キーをローテーションするプロセスは何ですか?
A. CMK の自動キー ローテーションを有効にし、6 か月の期間を指定します。
B. 新しいインポートされたマテリアルを使用して新しい CMK を作成し、新しい CMK を指すようにキー エイリアスを更新します。
C. 現在のキー マテリアルを削除し、新しいマテリアルを既存の CMK にインポートします。
D. 既存のキー マテリアルのコピーをバックアップとして新しい CMK にインポートし、6 か月のローテーション スケジュールを設定します。
Answer: B
Explanation:
If you choose to import keys to AWS KMS or asymmetric keys or use a custom key store, you can manually rotate them by creating a new KMS key and mapping an existing key alias from the old KMS key to the new KMS key.
https://aws.amazon.com/kms/faqs/

QUESTION NO: 28
SysOps管理者は、Ubuntuを実行する数百のAmazon EC2インスタンスにデプロイされたカスタムアプリケーションからログファイルの内容を収集する必要があります。ログファイルはAmazon CloudWatch Logsに保存する必要があります。
SysOps 管理者は、運用オーバーヘッドを最小限に抑えながらアプリケーション ログ ファイルをどのように収集すればよいでしょうか?
A. 各 EC2 インスタンスで syslogd サービスを設定し、アプリケーション ログ ファイルを収集して CloudWatch Logs に送信します。
B. Amazon Linux パッケージマネージャーを使用して、各 EC2 インスタンスに CloudWatch エージェントをインストールします。各エージェントがアプリケーションログファイルを収集するように設定します。
C. AWS Systems Manager を使用して、各 EC2 インスタンスに CloudWatch エージェントをインストールします。CloudWatch 設定ウィザードを使用して、各インスタンスにエージェント設定を作成します。各エージェントがアプリケーションログファイルを収集するように設定します。
D. CloudWatch エージェントの設定を AWS Systems Manager

パラメータストアに保存します。Systems Manager を使用して、各 EC2 インスタンスに CloudWatch
エージェントをインストールします。各エージェントがアプリケーションログファイルを収集するように設定します。

Answer: D

Explanation:

The most operationally efficient method is to centralize the CloudWatch agent configuration so that it can be deployed and managed uniformly across all instances. By storing the CloudWatch agent configuration in AWS Systems Manager Parameter Store, you can centrally manage and update the configuration for the agents. Then, using AWS Systems Manager, you can install the CloudWatch agent on each EC2 instance (even though they are running Ubuntu) without manually configuring each one.

QUESTION NO: 29

ある企業の公開ウェブサイトで最近問題が発生しました。一部のリンクをクリックするとウェブページが欠落し、他のリンクでは正しくないウェブページが表示されるという問題が発生していました。アプリケーションインフラストラクチャは正常に動作しており、プロビジョニングされたリソースもすべて正常でした。アプリケーションログとダッシュボードにはエラーは表示されず、監視アラームも発生していませんでした。システム管理者は、エンドユーザーから問題が報告されるまで、問題に気付いていませんでした。
同社は今後、このような問題がないかウェブサイトを積極的に監視し、できるだけ早く解決策を実施する必要があります。
最も少ない運用オーバーヘッドでこれらの要件を満たすソリューションはどれでしょうか?

A. 問題が発生したときにアプリケーション ログにカスタム
エラーが表示されるようにアプリケーションを書き換えます。
ログを自動的に解析してエラーを検出します。
問題が検出された場合にアラートを提供するための Amazon CloudWatch
アラームを作成します。

B. ウェブサイトをテストするための AWS Lambda 関数を作成します。
エラーが検出されたときに Amazon CloudWatch カスタムメトリックを発行するように Lambda 関数を設定します。
問題が検出された場合にアラートを提供するように CloudWatch アラームを設定します。

C. Amazon CloudWatch Synthetics カナリアを作成します。
CloudWatch Synthetics Recorder
プラグインを使用して、カナリア実行用のスクリプトを生成します。
要件に応じてカナリアを構成します。
問題が検出された場合に警告を提供するアラームを作成します。

D. Amazon CloudWatch コンソールで、Application Insights をオンにします。
問題が検出された場合にアラートを提供するための CloudWatch アラームを作成します。

Answer: C

Explanation:

Canaries are scripts written in Node.js or Python.
They create Lambda functions in your account that use Node.js or Python as a framework.
Canaries work over both HTTP and HTTPS protocols. which makes it possible for you to continually verify your customer experience even when you don't have any customer traffic

on your applications. By using canaries, you can discover issues before your customers do.
https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch_Synthetics_Ca naries.html

QUESTION NO: 30
ある企業のアプリケーションは、Application Load Balancer (ALB) の背後にある Amazon EC2 インスタンス上で実行されています。同社は、HTTPCode_Target_5XX_Count メトリクスを監視するために Amazon CloudWatch アラームを設定しています。アプリケーションは営業時間中に数日おきにクラッシュします。このクラッシュにより CloudWatch アラームがトリガーされ、サービスが中断されます。クラッシュの原因はアプリケーションのメモリリークです。開発者が問題の解決に取り組んでいる間、SysOps管理者は一時的な解決策を実装する必要があります。この解決策では、EC2インスタンスを毎日自動的に再起動し、営業時間中のアプリケーションの中断を最小限に抑える必要があります。
これらの要件を満たすソリューションはどれでしょうか?
A. 営業時間外に実行するようにスケジュールされた Amazon EventBridge ルールを作成します。EC2 インスタンスで StartInstances オペレーションを呼び出すようにルールを設定します。
B. AWS Systems Manager を使用して、営業時間外の毎日のメンテナンスウィンドウを作成します。EC2インスタンスをターゲットとして登録します。AWS-RestartEC2Instance ランブックをメンテナンスウィンドウに割り当てます。
C. EC2インスタンスのStatusCheckFailed_Systemメトリクスを監視するための追加のCloudWatchアラームを設定します。追加アラームに対して、インスタンスを再起動するためのEC2アクションを設定します。
D. アプリケーションがクラッシュするたびにトリガーされる追加の CloudWatch アラームを設定します。追加のアラームに対して EC2 アクションを設定し、EC2 インスタンス上のアプリケーションを再起動します。
Answer: B
Explanation:
Using AWS Systems Manager to create a daily maintenance window outside of business hours allows you to schedule a reboot of the EC2 instances with minimal disruption. By registering the instances as targets and assigning the AWS-RestartEC2Instance runbook, the instances will be automatically rebooted during off-peak hours, which helps mitigate the memory leak issue temporarily while preserving application availability during business hours.

QUESTION NO: 31
ある企業が、Auto Scaling グループに属する Linux ベースの Amazon EC2 インスタンス群にデプロイされたサービスを開発しました。このサービスは、アプリケーションコードのエラーが原因で、予期せず障害が発生することがあります。同社のエンジニアリングチームは、サービス障害の根本原因の解決には数週間かかる可能性があると判断しました。
SysOps 管理者は、いずれかの EC2

インスタンスでサービスがクラッシュした場合に回復を自動化するソリューションを作成する必要があります。
どのソリューションがこの要件を満たしますか? (2 つ選択してください。)
A. EC2インスタンスにAmazon CloudWatchエージェントをインストールします。CloudWatchエージェントを設定してサービスを監視します。サービスのヘルスチェックが失敗した場合に再起動するようにCloudWatchアクションを設定します。
B. EC2インスタンスにタグを付けます。AWS Systems Manager Session Managerを使用してタグ付けされたEC2インスタンスにログインし、サービスを再起動するAWS Lambda関数を作成します。Lambda関数を5分ごとに実行するようにスケジュールします。
C. EC2インスタンスにタグを付けます。AWS Systems Manager State Managerを使用して、AWS-RunShellScriptドキュメントを使用する関連付けを作成します。関連付けコマンドには、サービスが実行中かどうかを確認し、実行されていない場合はサービスを開始するスクリプトを設定します。ターゲットには、EC2インスタンスのタグを指定します。関連付けは5分ごとに実行されるようにスケジュールします。
D. Auto Scaling グループの起動テンプレートに指定されている EC2 ユーザーデータを更新し、5 分ごとに cron スケジュールで実行されるスクリプトを追加します。このスクリプトは、サービスが実行中かどうかを確認し、実行されていない場合はサービスを起動するように設定してください。更新した起動テンプレートを使用して、Auto Scaling グループ内のすべての EC2 インスタンスを再デプロイします。
E. Auto Scaling グループの起動テンプレートに指定されている EC2 ユーザーデータを更新し、起動時にサービスが実行されるようにします。更新された起動テンプレートを使用して、Auto Scaling グループ内のすべての EC2 インスタンスを再デプロイします。
Answer: AE

QUESTION NO: 32
ある企業のVPCは、AWSサイト間VPNを介してオンプレミスデータセンターに接続しています。この企業は、example.comへのDNSクエリをデータセンター内のDNSサーバーに送信するために、VPC内のAmazon EC2インスタンスを必要としています。
これらの要件を満たすソリューションはどれでしょうか?
A. Amazon Route 53 Resolver のインバウンドエンドポイントを作成します。オンプレミス DNS サーバーに条件付き転送ルールを作成し、example.com への DNS リクエストをインバウンドエンドポイントに転送します。
B. Amazon Route 53 リゾルバーのインバウンドエンドポイントを作成します。リゾルバーに、example.com へのすべてのクエリをオンプレミスの DNS サーバーに送信する転送ルールを作成します。このルールを VPC に関連付けます。
C. Amazon Route 53 Resolver のアウトバウンドエンドポイントを作成します。オンプレミス DNS サーバーに条件付き転送ルールを作成し、example.com への DNS

リクエストをアウトバウンドエンドポイントに転送します。
D. Amazon Route 53
リゾルバーのアウトバウンドエンドポイントを作成します。リゾルバーに、example.com へのすべてのクエリをオンプレミスの DNS
サーバーに送信する転送ルールを作成します。このルールを VPC に関連付けます。
Answer: D
Explanation:
To allow EC2 instances in the VPC to resolve DNS queries using on-premises DNS servers over an AWS Site-to-Site VPN, you need to configure an Amazon Route 53 Resolver outbound endpoint. This enables DNS queries to be forwarded from AWS to external DNS servers, such as those in an on-premises data center.
1. Create a Route 53 Resolver outbound endpoint ?This allows the VPC to send DNS queries to on-premises DNS servers.
2. Configure a forwarding rule ?The rule ensures that all queries for example.com are directed to the on-premises DNS servers.
3. Associate the rule with the VPC ?This ensures that the EC2 instances in the VPC use the resolver for DNS resolution.

QUESTION NO: 33
ある企業には、www.example.com 用の既存のパブリック Web アプリケーションがあります。Application Load Balancer (ALB) は、単一の HTTP 80 リスナーで構成されています。SysOps 管理者は、www.example.com へのすべての Web リクエストがクライアントと ALB 間で暗号化されていることを確認する必要があります。SysOps 管理者は、AWS Certificate Manager (ACM) で www.example.com のパブリック証明書をすでにリクエストし、検証しています。アプリケーションの既存のユーザーは、接続先のエンドポイントを変更する必要はありません。
これらの要件を満たすために、SysOps 管理者はどのような追加の手順を実行する必要がありますか?
A. ポート 443 で HTTPS 用の追加 ALB リスナーを作成します。すべてのトラフィックをターゲット グループに転送するようにデフォルトのアクションを設定します。www example.com 用に作成された ACM 証明書をデフォルトの SSL 証明書として指定します。
B. ポート 443 で HTTPS 用の追加 ALB リスナーを作成します。すべてのトラフィックをターゲット グループに転送するようにデフォルトのアクションを設定します。www.example.com 用に作成された ACM 証明書をデフォルトの SSL 証明書として指定します。ポート 80 の元の HTTP リスナーを削除します。
C. HTTP ポート 80 リスナーの ALB デフォルト ルールを変更します。リスナーにルールを作成し、ホスト www example com のすべてのトラフィックをターゲット グループに転送します。www.example.com 用に作成された ACM 証明書をデフォルトの SSL 証明書として指定します。
D. HTTP ポート 80 リスナーの ALB デフォルト ルールを変更して、ポート 443 の HTTPS にリダイレクトします。ポート 443 に追加の HTTPS リスナーを作成します。すべてのトラフィックをターゲット グループに転送するようにデフォルト アクションを設定します。www example.com

用に作成された ACM 証明書をデフォルトの SSL 証明書として指定します。
Answer: D

QUESTION NO: 34
会社は、会社のアカウントの Amazon S3
バケット内のデータの公開を禁止するために、セキュリティ
ポリシーを更新します。この要件を満たすために、SysOps
管理者は何をする必要がありますか?
A. アカウント レベルから S3 Block Public Access をオンにします。
B. Amazon EventBridge (Amazon CloudWatch Events) ルールを作成して、すべての S3 オブジェクトがプライベートであることを強制します。
C. Amazon Inspector を使用して S3 バケットを検索し、パブリック S3
バケットが見つかった場合は S3 ACL を自動的にリセットします。
D. S3 Object Lambda を使用して S3 ACL を調べ、パブリック S3 ACL
をプライベートに変更します。
Answer: A
Explanation:
Using Amazon S3 Block Public Access as a centralized way to limit public access. Block Public Access settings override bucket policies and object permissions. Be sure to enable Block Public Access for all accounts and buckets that you don't want publicly accessible.

QUESTION NO: 35
ある企業が2つのアプリケーションを接続しようとしています。1つのアプリケーションは、ホスト名がhost1.onprem
privateであるオンプレミスデータセンターで実行されています。もう1つのアプリケーションは、ホスト名がhost1.awscloud privateであるAmazon
EC2インスタンスで実行されています。オンプレミスネットワークとAWSの間には、AWSサイト間VPN接続が確立されています。
データセンターで実行されるアプリケーションは、EC2インスタンスで実行されるアプリケーションに接続しようとしますが、DNS解決に失敗します。SysOps管理者は、オンプレミスとAWSリソース間のDNS解決を実装する必要があります。
オンプレミスのアプリケーションが EC2
インスタンスのホスト名を解決できるようにするソリューションはどれですか?
A. onprem.private ホストゾーンの転送ルールを使用して、Amazon Route 53
インバウンドリゾルバーエンドポイントを設定します。リゾルバーを EC2 インスタンスの VPC に関連付けます。オンプレミス DNS リゾルバーを設定して、onprem.private の DNS クエリをインバウンドリゾルバーエンドポイントに転送します。
B. Amazon Route 53 のインバウンドリゾルバエンドポイントを設定します。リゾルバを EC2 インスタンスの VPC に関連付けます。オンプレミスの DNS
リゾルバを設定して、awscloud.private の DNS
クエリをインバウンドリゾルバエンドポイントに転送します。
C. onprem.private ホストゾーンの転送ルールを使用して、Amazon Route 53
アウトバウンドリゾルバーエンドポイントを設定します。リゾルバーを EC2
インスタンスの AWS リージョンに関連付けます。
オンプレミスの DNS リゾルバーを構成して、onprem.private DNS クエリをアウトバウンド

リゾルバー エンドポイントに転送します。
D. Amazon Route 53 アウトバウンドリゾルバエンドポイントを設定します。リゾルバを EC2 インスタンスの AWS リージョンに関連付けます。オンプレミス DNS リゾルバを設定して、awscloud.private の DNS クエリをアウトバウンドリゾルバエンドポイントに転送します。
Answer: B
Explanation:
Route 53 resolver provides resolution for AWS resources and on-prem dns NS provides resolution for on-prem resources. When DNS NS gets a dns query for AWS resources, it forwards it to Route 53 resolver.