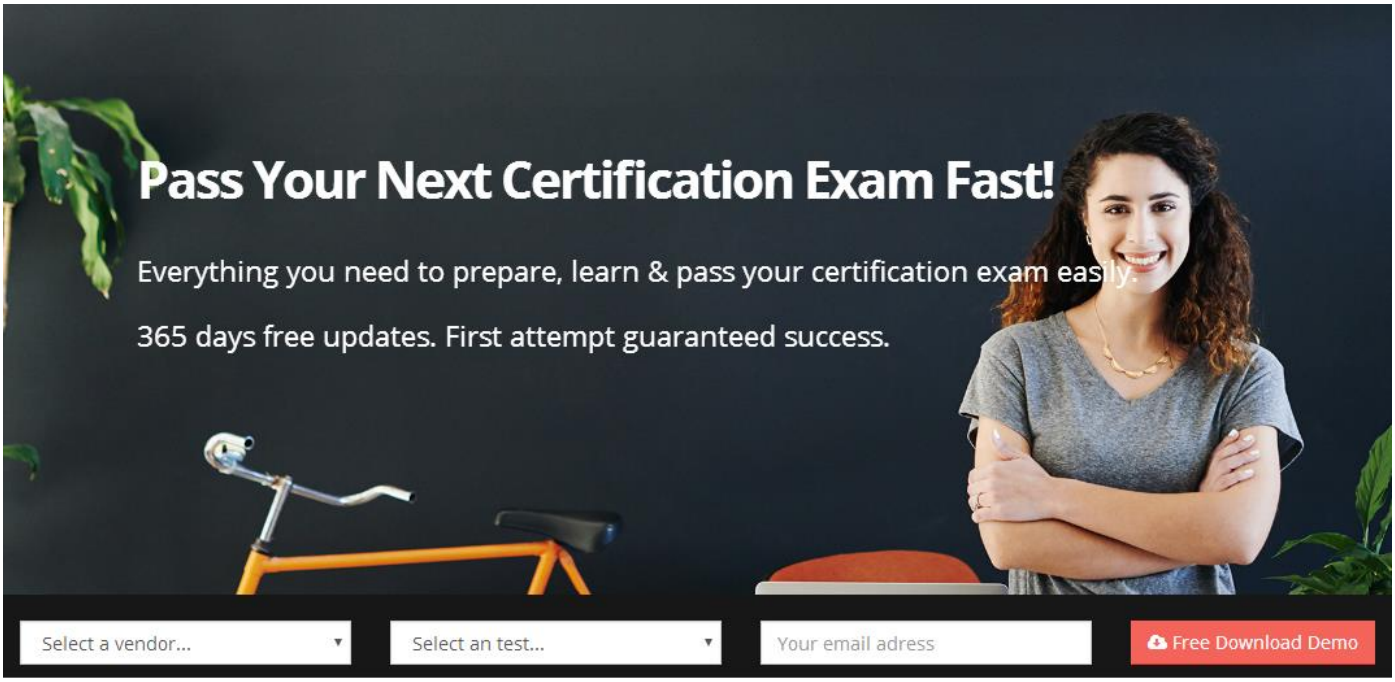
Exams4sures



Security & Privacy

Exams4sures respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

Instant Download

After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact Exams4sures.

365 Days Free Updates

Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.

Try Before Buy

Exams4sures offers free demo of each product. You can check out the interface, question quality and usability of our practice exams before you decide to buy.

48923+
Happy Clients

48923+
Shares

97846+
Downloads

9999+
Years in Business

http://www.exams4sures.com/

Everything you need to prepare, learn & pass your certification exam easily.

Exam : **AWS-Solutions-Architect-Professional-JPN**

Title : AWS Certified Solutions Architect - Professional (AWS-Solutions-Architect-Professional日本語版)

Vendor : Amazon

Version : DEMO

QUESTION NO: 1
ある企業には、アプリケーションのデータベースとして Amazon Aurora PostgreSQL DB クラスターを使用するアプリケーションがあります。DB クラスターには、1 つの小さなプライマリ インスタンスと 3 つの大きなレプリカ インスタンスが含まれています。アプリケーションは AWS Lambda 関数で実行されます。アプリケーションは、読み取り専用操作を実行するために、データベースのレプリカ インスタンスへの短期間の接続を多数作成します。
トラフィックが多い期間には、アプリケーションの信頼性が低下し、データベースは確立されている接続が多すぎると報告します。トラフィックが多い期間の頻度は予測できません。
どのソリューションがアプリケーションの信頼性を向上させますか?
A. Amazon RDS プロキシを使用して DB クラスターのプロキシを作成します。プロキシの読み取り専用エンドポイントを構成します。プロキシエンドポイントに接続するように Lambda 関数を更新します。
B. DB クラスターのパラメーターグループの max_connections 設定を増やします。DB クラスター内のすべてのインスタンスを再起動します。Lambda 関数を更新して DB クラスターエンドポイントに接続します。
C. DatabaseConnections メトリクスが max _connections 設定に近い場合に DB クラスターのインスタンス スケーリングが発生するように構成します。Lambda 関数を更新して、Aurora リーダーエンドポイントに接続します。
D. Amazon RDS プロキシを使用して DB クラスターのプロキシを作成します。プロキシ上で Aurora Data API の読み取り専用エンドポイントを設定します。プロキシエンドポイントに接続するように Lambda 関数を更新します。
Answer: A

QUESTION NO: 2
ある会社は、e コマース Web サイトのディザスター リカバリー (DR) ソリューションを構築する必要があります。ウェブアプリケーションは、一連の t3.large Amazon EC2 インスタンスでホストされ、Amazon RDS for MySQL DB インスタンスを使用します。EC2 インスタンスは、複数のアベイラビリティーゾーンにまたがる Auto Scaling グループにあります。
障害が発生した場合、Web アプリケーションは 30 秒の RPO と 10 分の R TO でセカンダリ環境にフェールオーバーする必要があります。
これらの要件を最も費用対効果の高い方法で満たすソリューションはどれですか?
A. Infrastructure as Code (IaC) を使用して、DR リージョンに新しいインフラストラクチャをプロビジョニングします。DB インスタンスのクロスリージョンリードレプリカを作成します。AWS Backup でバックアップ計画を設定して、EC2 インスタンスと DB インスタンスのクロスリージョンバックアップを作成します。EC2 インスタンスと DB インスタンスを 30 秒ごとに DR リージョンにバックアップする cron 式を作成します。最新の EC2 バックアップから EC2 インスタンスを復元します。Amazon Route 53 地理位置情報ルーティング ポリシーを使用して、災害時に DR リージョンに自動的にフェイルオーバーします。
B. Infrastructure as Code (IaC) を使用して、DR リージョンに新しいインフラストラクチャをプロビジョニングします。DB

インスタンスのクロスリージョンリードレプリカを作成します。EC2 インスタンスを DR リージョンに継続的にレプリケートするように AWS Elastic Disaster Recovery を設定します。DR リージョンの最小容量で EC2 インスタンスを実行する Amazon Route 53 フェイルオーバー ルーティング ポリシーを使用して、災害時に DR リージョンに自動的にフェイルオーバーします。Auto Scaling グループの必要な容量を増やします。

C. AWS Backup でバックアップ計画を設定して、EC2 インスタンスと DB インスタンスのクロスリージョン バックアップを作成します。EC2 インスタンスと DB インスタンスを 30 秒ごとに DR リージョンにバックアップする cron 式を作成します。Infrastructure as Code (IaC) を使用して、DR リージョンに新しいインフラストラクチャをプロビジョニングします。新しいインスタンスでバックアップ データを手動で復元します。Amazon Route 53 の単純なルーティング ポリシーを使用して、災害時に DR リージョンに自動的にフェイルオーバーします。

D. コードとしてのインフラストラクチャ (IaC) を使用して、DR リージョンに新しいインフラストラクチャをプロビジョニングします。Amazon Aurora グローバル データベースを作成します。EC2 インスタンスを DR リージョンに継続的にレプリケートするように AWS Elastic Disaster Recovery を設定します。DR リージョンで EC2 インスタンスの Auto Scaling グループをフルキャパシティで実行します。Amazon Route 53 フェイルオーバー ルーティング ポリシーを使用して、災害時に DR リージョンに自動的にフェイルオーバーします。

Answer: B

Explanation:

The company should use infrastructure as code (IaC) to provision the new infrastructure in the DR Region.

The company should create a cross-Region read replica for the DB instance. The company should set up AWS Elastic Disaster Recovery to continuously replicate the EC2 instances to the DR Region. The company should run the EC2 instances at the minimum capacity in the DR Region. The company should use an Amazon Route 53 failover routing policy to automatically fail over to the DR Region in the event of a disaster. The company should increase the desired capacity of the Auto Scaling group. This solution will meet the requirements most cost-effectively because AWS Elastic Disaster Recovery (AWS DRS) is a service that minimizes downtime and data loss with fast, reliable recovery of on-premises and cloud-based applications using affordable storage, minimal compute, and point-in-time recovery. AWS DRS enables RPOs of seconds and RTOs of minutes1.

AWS DRS continuously replicates data from the source servers to a staging area subnet in the DR Region, where it uses low-cost storage and minimal compute resources to maintain ongoing replication. In the event of a disaster, AWS DRS automatically converts the servers to boot and run natively on AWS and launches recovery instances on AWS within minutes2.

By using AWS DRS, the company can save costs by removing idle recovery site resources and paying for the full disaster recovery site only when needed. By creating a cross-Region read replica for the DB instance, the company can have a standby copy of its primary database in a different AWS Region3. By using infrastructure as code (IaC), the company can provision the new infrastructure in the DR Region in an automated and consistent way4.

By using an Amazon Route 53 failover routing policy, the company can route traffic to a resource that is healthy or to another resource when the first resource becomes unavailable.
The other options are not correct because:
Using AWS Backup to create cross-Region backups for the EC2 instances and the DB instance would not meet the RPO and RTO requirements. AWS Backup is a service that enables you to centralize and automate data protection across AWS services. You can use AWS Backup to back up your application data across AWS services in your account and across accounts. However, AWS Backup does not provide continuous replication or fast recovery; it creates backups at scheduled intervals and requires manual restoration. Creating backups every 30 seconds would also incur high costs and network bandwidth.
Creating an Amazon API Gateway Data API service integration with Amazon Redshift would not help with disaster recovery. The Data API is a feature that enables you to query your Amazon Redshift cluster using HTTP requests, without needing a persistent connection or a SQL client. It is useful for building applications that interact with Amazon Redshift, but not for replicating or recovering data.
Creating an AWS Data Exchange datashare by connecting AWS Data Exchange to the Redshift cluster would not help with disaster recovery. AWS Data Exchange is a service that makes it easy for AWS customers to exchange data in the cloud. You can use AWS Data Exchange to subscribe to a diverse selection of third-party data products or offer your own data products to other AWS customers. A datashare is a feature that enables you to share live and secure access to your Amazon Redshift data across your accounts or with third parties without copying or moving the underlying data. It is useful for sharing query results and views with other users, but not for replicating or recovering data.
References:
https://aws.amazon.com/disaster-recovery/
https://docs.aws.amazon.com/drs/latest/userguide/what-is-drs.html
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html#USER_ReadRepl.XR
https://aws.amazon.com/cloudformation/
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover.html
https://aws.amazon.com/backup/
https://docs.aws.amazon.com/redshift/latest/mgmt/data-api.html
https://aws.amazon.com/data-exchange/
https://docs.aws.amazon.com/redshift/latest/dg/datashare-overview.html

QUESTION NO: 3
ある企業は、レガシー アプリケーションを AWS
クラウドに移行しました。このアプリケーションは、3
つのアベイラビリティーゾーンに分散された 3 つの Amazon EC2
インスタンス上で実行されます。各アベイラビリティーゾーンには 1 つの EC2
インスタンスがあります。EC2 インスタンスは VPC の 3 つのプライベート
サブネットで実行されており、3 つのパブリック サブネットに関連付けられた Application Load Balancer (ALB) のターゲットとして設定されています。
アプリケーションはオンプレミス システムと通信する必要があります。会社の IP
アドレス範囲内の IP アドレスからのトラフィックのみがオンプレミス
システムへのアクセスを許可されます。会社のセキュリティ チームは、内部 IP

アドレス範囲から 1 つの IP アドレスのみをクラウドに持ち込んでいます。会社は、この IP アドレスを会社のファイアウォールの許可リストに追加しました。同社は、この IP アドレスに対して Elastic IP アドレスも作成しました。
ソリューション アーキテクトは、アプリケーションがオンプレミス システムと通信できるようにするソリューションを作成する必要があります。また、ソリューションは障害を自動的に軽減できなければなりません。
これらの要件を満たすソリューションはどれですか?
A. 各パブリック サブネットに 1 つずつ、3 つの NAT ゲートウェイを展開します。Elastic IP アドレスを NAT ゲートウェイに割り当てます。NAT ゲートウェイのヘルスチェックをオンにします。NAT ゲートウェイがヘルスチェックに失敗した場合は、NAT ゲートウェイを再作成し、新しい NAT ゲートウェイに Elastic IP アドレスを割り当てます。
B. ALB をネットワーク ロード バランサー (NLB) に置き換えます。Elastic IP アドレスを NLB に割り当てます。 NLB のヘルスチェックをオンにします。ヘルスチェックが失敗した場合は、NLB を別のサブネットに再デプロイします。
C. パブリック サブネットに単一の NAT ゲートウェイを展開します。Elastic IP アドレスを NAT ゲートウェイに割り当てます。
Amazon CloudWatch をカスタムメトリクスとともに使用して、NATゲートウェイを監視します。NAT ゲートウェイが異常な場合は、AWS Lambda 関数を呼び出して、別のサブネットに新しい NAT ゲートウェイを作成します。Elastic IP アドレスを新しい NAT ゲートウェイに割り当てます。
D. Elastic IP アドレスを ALB に割り当てます。Elastic IP アドレスを値として使用して、Amazon Route 53 の単純なレコードを作成します。Route 53 ヘルスチェックを作成します。ヘルスチェックが失敗した場合は、別のサブネットで ALB を再作成します。
Answer: C
Explanation:
to connect out from the private subnet you need an NAT gateway and since only one Elastic IP whitelisted on firewall its one NATGateway at time and if AZ failure happens Lambda creates a new NATGATEWAY in a different AZ using the Same Elastic IP ,dont be tempted to select D since application that needs to connect is on a private subnet whose outbound connections use the NATGateway Elastic IP

QUESTION NO: 4
金融会社がAmazonS3でデータレイクをホストしています。同社は、いくつかのサードパーティから毎晩SFTPを介して財務データレコードを受け取ります。同社は、VPCのパブリックサブネット内のAmazonEC2インスタンスで独自のSFTPサーバーを実行しています。ファイルがアップロードされた後、同じインスタンスで実行されるcronジョブによってデータレイクに移動されます。
SFTPサーバーは、Amazonルートを使用してDNSsftp.examWe.comからアクセスできます。
53。
SFTPソリューションの信頼性とスケーラビリティを向上させるためにソリューションアーキテクトは何をすべきですか？

A.EC2インスタンスをAutoScalingグループに移動します。
EC2インスタンスをApplicationLoad
Balancer（ALB）の背後に配置します。ルート53のDNSレコードsftp.example.comを更新して、ALBを指すようにします。
B.SFTPサーバーをAWS Transfer
forSFTPに移行します。ルートのDNSレコードsftp.example.comを更新します
53サーバーエンドポイントのホスト名を指します。
C.SFTPサーバーをAWS
StorageGatewayのファイルゲートウェイに移行します。ルート53のDNSレコードsflp.example.comを更新して、ファイルゲートウェイエンドポイントを指すようにします。
D.EC2インスタンスをネットワークロードバランサー（NLB）の背後に配置します。
NLBを指すようにRoute53のDNSレコードsftp.example.comを更新します。
Answer: B
Explanation:
https://aws.amazon.com/aws-transfer-family/faqs/
https://docs.aws.amazon.com/transfer/latest/userguide/what-is-aws-transfer-family.html
https://aws.amazon.com/about-aws/whats-new/2018/11/aws-transfer-for-sftp-fully-managed-sftp-for-s3/?nc1=h_

QUESTION NO: 5
ある大企業は、数百の AWS アカウントにデプロイされた VPC
でワークロードを実行しています。各 VPC
は、複数のアベイラビリティーゾーンにまたがるパブリックサブネットとプライベートサブネットで構成されます。NAT ゲートウェイはパブリック
サブネットに展開され、プライベート
サブネットからインターネットへの送信接続を可能にします。
ソリューションアーキテクトはハブアンドスポーク設計に取り組んでいます。スポーク
VPC 内のすべてのプライベート サブネットは、出力 VPC
経由でトラフィックをインターネットにルーティングする必要があります。ソリューションアーキテクトは、すでに中央の AWS アカウントの出力 VPC に NAT
ゲートウェイをデプロイしています。
これらの要件を満たすために、ソリューション設計者はどの追加手順を実行する必要がありますか?
A. 出力 VPC とスポーク VPC
の間にピアリング接続を作成します。インターネットへのアクセスを許可するために必要なルーティングを構成します。
B. トランジット ゲートウェイを作成し、既存の AWS アカウントと共有します。既存の
VPC をトランジット ゲートウェイに接続します。
インターネットへのアクセスを許可するために必要なルーティングを設定します。
C. すべてのアカウントにトランジット ゲートウェイを作成します。NAT
ゲートウェイをトランジット
ゲートウェイに接続します。インターネットへのアクセスを許可するために必要なルーティングを構成します。
D. エグレス VPC とスポーク VPC の間に AWS PrivateLink

接続を作成します。インターネットへのアクセスを許可するために必要なルーティングを構成します。

Answer: B

Explanation:

https://d1.awsstatic.com/architecture-diagrams/ArchitectureDiagrams/NAT-gateway-centralized-egress-ra.pdf?d

QUESTION NO: 6

ある企業は、Amazon RDS for Oracle データベースを別の AWS アカウントの RDS for PostgreSQL DB インスタンスに移行することを計画しています。ソリューション アーキテクトは、ダウンタイムを必要とせず、移行の完了に必要な時間を最小限に抑える移行戦略を設計する必要があります。移行戦略では、既存のすべてのデータと、移行中に作成される新しいデータをすべてレプリケートする必要があります。 ターゲット データベースは、移行プロセスの完了時にソース データベースと同一である必要があります。

現在、すべてのアプリケーションは、通信のエンドポイントとして Amazon Route 53 CNAME レコードを使用しています。 RDS for Oracle DB インスタンス RDS for Oracle DB インスタンスはプライベート サブネット内にあります。

これらの要件を満たすために、ソリューション設計者はどの手順の組み合わせを実行する必要がありますか? (3つ選択してください)

A. ターゲット アカウントで新しい RDS for PostgreSQL DB インスタンスを作成します。AWS Schema Conversion Tool (AWS SCT) を使用して、データベース スキーマをソース データベースからターゲット データベースに移行します。

B. AWS スキーマ変換ツール (AWS SCT) を使用して、ソース データベースのスキーマと初期データを使用して、ターゲット アカウントに新しい RDS for PostgreSQL DB インスタンスを作成します。

C. 2 つの AWS アカウントの VPC 間に VPC ピアリングを構成し、ターゲット アカウントから両方の DB インスタンスへの接続を提供します。ターゲット アカウントの VPC からデータベース ポートでのトラフィックを許可するように、各 DB インスタンスにアタッチされているセキュリティ グループを構成します。

D. ターゲット アカウントの VPC からの接続を提供するために、ソース DB インスタンスへのパブリック アクセスを一時的に許可します。各 DB インスタンスにアタッチされているセキュリティ グループを構成して、ターゲットの VPC からのデータベース ポートでのトラフィックを許可します。アカウント。

E. ターゲット アカウントで AWS Database Migration Service (AWS DMS) を使用して、ソース データベースからターゲット データベースへの全ロードと変更データ キャプチャ (CDC) 移行を実行します。移行が完了したら、CNAME レコードを変更します。ターゲット DB インスタンスのエンドポイントを指すようにする

F. ターゲット アカウントで AWS Database Migration Service (AWS DMS) を使用して、ソース データベースからターゲット データベースへの変更データ キャプチャ (CDC) 移行を実行します。移行が完了したら、CNAME レコードが、ターゲット DB インスタンスのエンドポイント。

Answer: A C E

QUESTION NO: 7
企業は、AWS Organizations の組織に AWS アカウントを持っています。同社は、Amazon EC2 の使用状況を指標として追跡したいと考えています。EC2 使用量が過去 30 日間の平均 EC2 使用量より 10% 以上高い場合、会社のアーキテクチャ
チームは毎日アラートを受け取る必要があります。
これらの要件を満たすソリューションはどれですか?
A. 組織の管理アカウントで AWS
予算を設定します。EC2実行時間の利用タイプを指定します。毎日の期間を指定します。AWS Cost Explorer から報告された過去 30 日間の平均使用量より 10%
多い予算額を設定します。使用量のしきい値に達した場合にアーキテクチャ
チームに通知するアラートを構成します。
B. 組織の管理アカウントで AWS Cost Anomaly Detection
を設定します。AWSサービスのモニタータイプを設定します。Amazon EC2のフィルターを適用します。使用量が過去 30 日間の平均使用量より 10%
多い場合にアーキテクチャ チームに通知するようにアラート
サブスクリプションを構成します。
C. 組織の管理アカウントで AWS Trusted Advisor を有効にします。EC2
の使用量が、報告された過去 30 日間の平均使用量より 10% 多い場合にアーキテクチャ
チームに通知するように、コスト最適化勧告アラートを構成します。
D. 組織の管理アカウントで Amazon Detective を設定します。Detective が 10%
を超える使用異常を特定した場合にアーキテクチャ チームに通知するように、EC2
使用異常アラートを構成します。
Answer: B
Explanation:
AWS Cost Anomaly Detection is a feature of the AWS Cost Management suite that leverages machine learning to enable continuous monitoring of your AWS costs and usage, allowing you to identify unexpected and abnormal spending1. You can create cost monitors that evaluate specific AWS services, member accounts, cost allocation tags, or cost categories based on your AWS account structure2. You can also configure alert subscriptions that notify you when a cost monitor detects an anomaly that meets your threshold2. In this case, you can create a cost monitor with a monitor type of AWS Service and apply a filter of Amazon EC2 to track the EC2 usage as a metric. You can then configure an alert subscription to notify the architecture team if the usage is 10% more than the average usage for the last 30 days, which is the anomaly detection period used by AWS Cost Anomaly Detection3.

QUESTION NO: 8
ある企業は AWS 上で多くのワークロードを実行し、AWS Organizations
を使用してアカウントを管理しています。ワークロードは Amazon EC2
でホストされます。AWSファーゲート。そしてAWSラムダ。ワークロードの中には、予測できない需要があるものもあります。アカウントは、ある月には高い使用量を記録し、別の月には低い使用量を記録します。
同社は今後 3 年間でコンピューティング
コストを最適化したいと考えています。ソリューション アーキテクトは
使用量を計算するための、組織全体の各アカウントの 6 か月の平均。
組織のすべてのコンピューティング使用量に対して最もコストを削減できるのはどのソリュ

ーションですか?
A. メンバー アカウントから最も一般的な EC2
インスタンスのサイズと数に一致する組織のリザーブド インスタンスを購入します。
B. 管理アカウント レベルの推奨事項を使用して、管理アカウントから組織の Compute Savings Plan を購入します。
C. 過去 6 か月のデータに基づいて、EC2 の使用率が高かった各メンバー
アカウントのリザーブド インスタンスを購入します。
D. 過去 6 か月の EC2 使用状況データに基づいて、管理アカウントからメンバー
アカウントごとに EC2 Instance Savings Plan を購入します。
Answer: B

QUESTION NO: 9
ソリューションアーキテクトは、Auto Scaling グループの Amazon EC2
インスタンスに運用ワークロードをデプロイしています。VPC アーキテクチャは、Auto Scaling グループがターゲットとしているサブネットを持つ 2
つのアベイラビリティーゾーン (AZ) にまたがっています。VPC
はオンプレミス環境に接続されており、接続は中断できません。Auto Scaling
グループの最大サイズは、サービス中のインスタンスが 20 です。VPC の IPv4
アドレス指定は次のとおりです。
VPCCIDR 10 0 0 0/23
AZ1 サブネット CIDR: 10 0 0 0724
AZ2 サブネット CIDR: 10.0.1 0724
導入後、リージョンで 3 番目の AZ が利用可能になりました。ソリューション
アーキテクトは、IPv4
アドレス空間を追加せず、サービスのダウンタイムも発生させずに新しい AZ
を採用したいと考えています。これらの要件を満たすソリューションはどれですか?
A. AZ2 サブネットのみを使用するように Auto Scaling グループを更新します。
以前のアドレス空間の半分を使用して、AZ1 サブネットを削除して再作成します。 新しい AZI サブネットも使用するように Auto Scaling グループを調整します。
インスタンスが正常な場合は、調整します。 Auto Scaling グループで AZ1
サブネットのみを使用する 現在の AZ2 サブネットを削除します 元の AZ1
サブネットのアドレス空間の後半を使用して新しい AZ2 サブネットを作成します 元の AZ2
サブネットのアドレス空間の半分を使用して新しい AZ3 サブネットを作成し、 3
つの新しいサブネットすべてをターゲットとする Auto Scaling グループ。
B. AZ1 サブネット内の EC2 インスタンスを終了します。ホール アドレス空間を使用して AZ1 サブネットを削除し、再作成します。この新しいサブネットを使用するように Auto Scaling グループを更新します。2 番目の AZ についてもこれを繰り返します。
AZ3 で新しいサブネットを定義します。次に、3
つの新しいサブネットすべてをターゲットにするように Auto Scaling
グループを更新します。
C. 同じ IPv4 アドレス空間を持つ新しい VPC を作成し、AZ ごとに 1 つずつ、3
つのサブネットを定義します。 新しい VPC
内の新しいサブネットをターゲットにするように既存の Auto Scaling
グループを更新します。

D. AZ2 サブネットのみを使用するように Auto Scaling グループを更新します。
以前のアドレス空間を停止するように AZ1 サブネットを更新します。 AZ1
サブネットも再び使用するように Auto Scaling
グループを調整します。インスタンスが正常な場合は、AZ1
サブネットのみを使用するように Auto Seating グループを調整します。現在の AZ2
サブネットを更新し、元の AZ1 サブネットのアドレス空間の後半を割り当てます。 元の
AZ2 サブネット アドレス空間の半分を使用して新しい AZ3 サブネットを作成し、3
つの新しいサブネットすべてをターゲットにするように Auto Scaling
グループを更新します。

Answer: A
Explanation:
https://repost.aws/knowledge-center/vpc-ip-address-range

QUESTION NO: 10
ある企業は、AWS でサービスとしてのソフトウェア (SaaS)
ソリューションをホストしています。このソリューションには、HTTPS
エンドポイントを提供する Amazon API Gateway API が含まれています。API
はコンピューティングに AWS Lambda 関数を使用します。Lambda 関数は、Amazon
Aurora Serverless VI データベースにデータを保存します。
同社は、AWS サーバーレス アプリケーション モデル (AWS SAM)
を使用してソリューションをデプロイしました。このソリューションは複数のアベイラビリティーゾーンにまたがり、災害復旧 (DR) 計画はありません。
ソリューションアーキテクトは、別の AWS リージョンでソリューションを回復できる DR 戦略を設計する必要があります。このソリューションの R TO は 5 分、RPO は 1 分です。
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は何をすべきでしょうか?

A. ターゲット リージョンに Aurora Serverless VI
データベースのリードレプリカを作成します。AWS SAM を使用して、ターゲット
リージョンにソリューションをデプロイするためのランブックを作成します。災害発生時にリードレプリカをプライマリに昇格させます。

B. Aurora Serverless VI データベースを、ソース リージョンとターゲット
リージョンにまたがる標準の Aurora MySQL グローバル データベースに変更します。AWS SAM を使用して、ターゲット
リージョンにソリューションをデプロイするためのランブックを作成します。

C. ターゲット リージョンに複数のライター インスタンスがある Aurora Serverless VI DB クラスターを作成します。
ターゲット リージョンでソリューションを起動します。2
つの地域ソリューションがアクティブ/パッシブ構成で動作するように構成します。

D. Aurora Serverless VI データベースを、ソース リージョンとターゲット
リージョンにまたがる標準の Aurora MySQL グローバル
データベースに変更します。ターゲット リージョンでソリューションを起動します。2
つの地域ソリューションがアクティブ/パッシブ構成で動作するように構成します。

Answer: D
Explanation: This option allows the solutions architect to use Aurora global database to replicate data across multiple AWS Regions with low latency and high availability1. By launching the solution in the target Region, the solutions architect can ensure that the API

Gateway, Lambda functions, and other resources are ready to serve traffic in case of a disaster in the source Region. By configuring the two Regional solutions to work in an active-passive configuration, the solutions architect can minimize costs and avoid data conflicts by having only one primary Region that accepts write operations and one secondary Region that serves as a standby2. The RTO and RPO requirements can be met by using Aurora global database, which supports sub-second failover times and near real-time replication1.
References:
Working with Amazon Aurora global database
Active-passive failover

QUESTION NO: 11
ある会社は、AWS Organizations の組織を使用して、何百もの AWS アカウントを管理しています。ソリューション アーキテクトは、Open Web Application Security Project (OWASP) のトップ 10 の Web アプリケーション脆弱性に対するベースライン保護を提供するソリューションに取り組んでいます。ソリューション アーキテクトは、組織内にデプロイされたすべての既存および新規の Amazon CloudFront ディストリビューションに AWS WAF を使用しています。ベースライン保護を提供するために、ソリューション アーキテクトはどの手順を組み合わせて実行する必要がありますか? (3 つ選択してください。)
A. すべてのアカウントで AWS Config を有効にします。
B. すべてのアカウントで Amazon GuardDuty を有効にします。
C. 組織のすべての機能を有効にします。
D. AWS Firewall Manager を使用して、すべての CloudFront ディストリビューションのすべてのアカウントに AWS WAF ルールをデプロイします。
E. AWS Shield Advanced を使用して、すべての CloudFront ディストリビューションのすべてのアカウントに AWS WAF ルールをデプロイします。
F. AWS Security Hub を使用して、すべての CloudFront ディストリビューションのすべてのアカウントに AWS WAF ルールをデプロイします。
Answer: C D E
Explanation:
Enabling all features for the organization will enable using AWS Firewall Manager to centrally configure and manage firewall rules across multiple AWS accounts1. Using AWS Firewall Manager to deploy AWS WAF rules in all accounts for all CloudFront distributions will enable providing baseline protection for the OWASP top 10 web application vulnerabilities2. AWS Firewall Manager supports AWS WAF rules that can help protect against common web exploits such as SQL injection and cross-site scripting3. Configuring redirection of HTTP requests to HTTPS requests in CloudFront will enable encrypting the data in transit using SSL/TLS.

QUESTION NO: 12
企業には、AWS Organizations に多数の AWS アカウントを持つ組織があります。ソリューション アーキテクトは、会社が組織内の AWS アカウントの共通セキュリティ グループ

ルールを管理する方法を改善する必要があります。
この会社には、各 AWS アカウントの許可リストに共通の IP CIDR
範囲のセットがあり、会社のオンプレミス
ネットワークとの間のアクセスを許可しています。
各アカウント内の開発者は、セキュリティ グループに新しい IP CIDR
範囲を追加する責任があります。セキュリティ チームには独自の AWS
アカウントがあります。現在、許可リストに変更が加えられると、セキュリティ
チームは他の AWS アカウントの所有者に通知します。
ソリューション アーキテクトは、CIDR
範囲の共通セットをすべてのアカウントに分散するソリューションを設計する必要があります。
運用上のオーバーヘッドが最も少なく、これらの要件を満たすソリューションはどれですか?
A. セキュリティ チームの AWS アカウントで Amazon Simple Notification Service (Amazon SNS) トピックを設定します。各 AWS アカウントに AWS Lambda
関数をデプロイします。SNS トピックがメッセージを受信するたびに実行するように Lambda 関数を設定します。IP
アドレスを入力として受け取り、それをアカウントのセキュリティ
グループのリストに追加するように Lambda 関数を設定します。SNS
トピックにメッセージを発行して変更を配布するようにセキュリティ チームに指示します。
B. 組織内の各 AWS アカウントで新しい顧客管理のプレフィックス
リストを作成します。各アカウントのプレフィックス リストにすべての内部 CIDR
範囲を入力します。各 AWS アカウントの所有者に通知して、セキュリティ
グループのアカウントで新しい顧客管理のプレフィックス リスト ID を許可します。各 AWS アカウント所有者と更新を共有するようにセキュリティ チームに指示します。
C. セキュリティ チームの AWS アカウントで新しい顧客管理のプレフィックス
リストを作成します。顧客管理のプレフィックス リストにすべての内部 CIDR
範囲を入力します。AWS Resource Access Manager
を使用して、顧客管理のプレフィックス リストを組織と共有します。各 AWS
アカウントの所有者に通知して、セキュリティ グループで新しい顧客管理のプレフィックス
リスト ID を許可します。
D. 組織内の各アカウントに IAM ロールを作成します。セキュリティ
グループを更新するアクセス許可を付与します。
セキュリティ チームの AWS アカウントに AWS Lambda
関数をデプロイします。入力として内部 IP
アドレスのリストを受け取り、各組織アカウントでロールを引き受け、IP
アドレスのリストを各アカウントのセキュリティ グループに追加するように Lambda
関数を設定します。
Answer: C
Explanation:
Create a new customer-managed prefix list in the security team's AWS account. Populate the customer-managed prefix list with all internal CIDR ranges. Share the customer-managed prefix list with the organization by using AWS Resource Access Manager. Notify the owner of each AWS account to allow the new customer-managed prefix list ID in their security groups.

This solution meets the requirements with the least amount of operational overhead as it requires the security team to create and maintain a single customer-managed prefix list, and share it with the organization using AWS Resource Access Manager. The owners of each AWS account are then responsible for allowing the prefix list in their security groups, which eliminates the need for the security team to manually notify each account owner when changes are made. This solution also eliminates the need for a separate AWS Lambda function in each account, reducing the overall complexity of the solution.

QUESTION NO: 13
ある会社は、AWS でサービスとしてのソフトウェア (SaaS)
ソリューションを構築しています。同社は、複数の AWS
リージョンと同じ本番アカウントで、AWS Lambda 統合を使用して Amazon API Gateway REST API をデプロイしました。
同社は段階的な価格設定を提供しており、顧客は 1 秒あたり特定の数の API
呼び出しを行う容量に対して支払うことができます。プレミアム レベルでは、1
秒あたり最大 3,000 回の呼び出しが提供され、顧客は一意の API
キーによって識別されます。さまざまな地域の複数のプレミアム
ティアのお客様が、使用のピーク時に複数の API メソッドから 429 Too Many Requests のエラー レスポンスを受け取ったと報告しています。ログは、Lambda
関数が呼び出されていないことを示しています。
これらの顧客のエラー メッセージの原因は何ですか?
A. Lambda 関数が同時実行制限に達しました。
B. Lambda 関数の同時実行のリージョン制限。
C. 会社は、1 秒あたりの呼び出し数が API Gateway アカウントの制限に達しました。
D. 会社は、1 秒あたりの呼び出し数が API
ゲートウェイのメソッドごとの既定の制限に達しました。
Answer: C
Explanation:
https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-request-throttling.html#apig-reques

QUESTION NO: 14
企業は顧客トランザクション データベースをオンプレミスから AWS
に移行する必要があります。データベースは、Linux サーバー上で実行される Oracle DB インスタンス上に存在します。新しいセキュリティ要件に従って、会社はデータベースのパスワードを毎年更新する必要があります。
運用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すか?
A. AWS Schema Conversion Tool (AWS SCT) を使用してデータベースを Amazon DynamoDB に変換します。
パスワードを AWS Systems Manager パラメータ ストアに保存します。Amazon CloudWatch アラームを作成して、毎年パスワードをローテーションするための AWS Lambda 関数を呼び出します。
B. データベースを Amazon RDS for Oracle に移行します。パスワードを AWS Secrets Manager に保存します。自動回転をオンにします。年間ローテーション

スケジュールを構成します。
C. データベースを Amazon EC2 インスタンスに移行します。AWS Systems Manager パラメータストアを使用して、AWS Lambda
関数を使用して接続文字列を維持し、年間スケジュールでローテーションします。
D. AWS スキーマ変換ツール (AWS SCT) を使用して、データベースを Amazon Neptune に移行します。Amazon CloudWatch
アラームを作成して、毎年パスワードをローテーションするための AWS Lambda
関数を呼び出します。
Answer: B

QUESTION NO: 15
ある会社がAWSクラウドでいくつかのプロジェクトを開発してホストしています。プロジェクトは、AWS組織の同じ組織の下にある複数のAWSアカウントにわたって開発されます。同社は、所有するプロジェクトにコストまたはクラウドインフラストラクチャを割り当てる必要があります。すべてのAWSアカウントを担当するチームは、いくつかのAmazonEC2インスタンスにコスト配分に使用されるプロジェクトタグがないことを発見しました。ソリューションアーキテクトは、問題を解決し、将来発生しないようにするために、どのアクションを実行する必要がありますか？ (3つ選択してください。)
A.各アカウントにAWS
Configルールを作成して、タグが欠落しているリソースを検索します。
B.Projectタグがない場合は、ec2：RunInstancesの拒否アクションを使用して組織内にSCPを作成します。
C.組織内のAmazon Inspectorを使用して、タグが欠落しているリソースを検索します。
D.Projectタグがない場合は、ec2：RunInstancesの拒否アクションを使用して各アカウントにIAMポリシーを作成します。
E.組織のAWS
Configアグリゲーターを作成して、Projectタグが欠落しているEC2インスタンスのリストを収集します。
F.AWS Security
Hubを使用して、Projectタグが欠落しているEC2インスタンスのリストを集約します。
Answer: A B E
Explanation:
https://docs.aws.amazon.com/config/latest/developerguide/config-rule-multi-account-deployment.html
https://docs.aws.amazon.com/config/latest/developerguide/aggregate-data.html
https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scps_examples_tagging.html

QUESTION NO: 16
企業は AWS クラウドでアプリケーションを実行しています。コア ビジネス
ロジックは、Auto Scaling グループ内の一連の Amazon EC2
インスタンスで実行されています。Application Load Balancer (ALB) は、トラフィックを EC2 インスタンスに分散します。Amazon Route 53 レコード api.example.com は ALB を指しています。
同社の開発チームは、ビジネス

ロジックを大幅に更新します。同社には、変更が展開された場合、テスト期間中に顧客の 10%
だけが新しいロジックを受け取ることができるという規則があります。お客様は、テスト期間中、同じバージョンのビジネス ロジックを使用する必要があります。
これらの要件を満たすために、会社は更新プログラムをどのように展開する必要がありますか?

A. 2 番目の ALB を作成し、新しいロジックを新しい Auto Scaling グループ内の一連の EC2 インスタンスにデプロイします。
トラフィックを EC2 インスタンスに分散するように ALB を構成します。Route 53 レコードを更新して加重ルーティングを使用し、レコードが両方の ALB を指すようにします。

B. ALB によって参照される 2 番目のターゲット グループを作成します。この新しいターゲット グループの EC2 インスタンスに新しいロジックをデプロイします。重み付けされたターゲット グループを使用するように ALB リスナー ルールを更新します。ALB ターゲット グループの粘着性を構成します。

C. Auto Scaling グループの新しい起動設定を作成します。AutoScalingRollingUpdate ポリシーを使用するように起動設定を指定し、MaxBatchSize オプションを 10 に設定します。Auto Scaling グループの起動設定を置き換えます。変更をデプロイします。

D. ALB によって参照される 2 番目の Auto Scaling グループを作成します。この新しい Auto Scaling グループの一連の EC2 インスタンスに新しいロジックをデプロイします。ALB ルーティング アルゴリズムを最小未処理要求 (LOR) に変更します。ALB セッション スティッキを構成します。

Answer: B

Explanation:

The company should create a second target group that is referenced by the ALB. The company should deploy the new logic to EC2 instances in this new target group. The company should update the ALB listener rule to use weighted target groups. The company should configure ALB target group stickiness. This solution will meet the requirements because weighted target groups are a feature that enables you to distribute traffic across multiple target groups using a single listener rule. You can specify a weight for each target group, which determines the percentage of requests that are routed to that target group. For example, if you specify two target groups, each with a weight of 10, each target group receives half the requests1. By creating a second target group and deploying the new logic to EC2 instances in this new target group, the company can have two versions of its business logic running in parallel. By updating the ALB listener rule to use weighted target groups, the company can control how much traffic is sent to each version. By configuring ALB target group stickiness, the company can ensure that a customer uses the same version of the business logic during the testing window. Target group stickiness is a feature that enables you to bind a user's session to a specific target within a target group for the duration of the session2.

The other options are not correct because:

Creating a second ALB and deploying the new logic to a set of EC2 instances in a new Auto Scaling group would not be as cost-effective or simple as using weighted target groups. A second ALB would incur additional charges and require more configuration and

management. Updating the Route 53 record to use weighted routing would not ensure that a customer uses the same version of the business logic during the testing window, as DNS caching could affect how requests are routed.
Creating a new launch configuration for the Auto Scaling group and replacing it on the Auto Scaling group would not allow for gradual traffic shifting between versions. A launch configuration is a template that an Auto Scaling group uses to launch EC2 instances. You can specify information such as the AMI ID, instance type, key pair, security groups, and block device mapping for your instances3.
However, replacing the launch configuration on an Auto Scaling group would affect all instances in that group, not just 10% of customers.
Creating a second Auto Scaling group and changing the ALB routing algorithm to least outstanding requests (LOR) would not allow for controlled traffic shifting between versions. A second Auto Scaling group would require more configuration and management. The LOR routing algorithm is a feature that enables you to route traffic based on how quickly targets respond to requests. The load balancer selects a target from the target group with the fewest outstanding requests4. However, this algorithm does not take into account customer sessions or weights.
References:
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-listeners.html#listener-
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/sticky-sessions.html
https://docs.aws.amazon.com/autoscaling/ec2/userguide/LaunchConfiguration.html
https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-target-groups.html#rou

QUESTION NO: 17
企業は、us-east-1 リージョンの Amazon RDS for MySQL DB
インスタンスにデータベースをデプロイしました。
同社は、ヨーロッパの顧客がデータを利用できるようにする必要があります。ヨーロッパの顧客は、米国 (US)
の顧客と同じデータにアクセスできる必要があり、アプリケーションの待ち時間が長くなったり、データが古くなったりすることは許されません。ヨーロッパの顧客と米国の顧客は、データベースに書き込む必要があります。顧客の両方のグループは、リアルタイムで他のグループからの更新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すか?
A. RDS for MySQL DB インスタンスの Amazon Aurora MySQL
レプリカを作成します。RDS DB
インスタンスへのアプリケーションの書き込みを一時停止します。Aurora
レプリカをスタンドアロン DB
クラスターに昇格させます。アプリケーションを再構成して、Aurora
データベースを使用し、書き込みを再開します。eu-west-1 をセカンダリ リージョンとして
06クラスター。DB クラスターで書き込み転送を有効にします。アプリケーションを eu-west-1 にデプロイします。eu-west-1 で Aurora MySQL
エンドポイントを使用するようにアプリケーションを設定します。
B. RDS for MySQL DB インスタンスの eu-west-1 にクロスリージョン

レプリカを追加します。書き込みクエリをプライマリ DB
インスタンスにレプリケートするようにレプリカを設定します。アプリケーションを eu-west-1 にデプロイします。eu-west-1 で RDS for MySQL
エンドポイントを使用するようにアプリケーションを構成します。
C. 最新のスナップショットを RDS for MySQL DB インスタンスから eu-west-1 にコピーします。スナップショットから eu-west-1 に新しい RDS for MySQL DB
インスタンスを作成します。us-east-1 から eu-west-1 への MySQL
論理レプリケーションを構成します。DB
クラスターで書き込み転送を有効にします。アプリケーションを eu-west-1 にデプロイします。
eu-west-1 で RDS for MySQL
エンドポイントを使用するようにアプリケーションを構成します。
D. RDS for MySQL DB インスタンスを Amazon Aurora MySQL DB
クラスターに変換します。eu-west-1 をセカンダリリージョンとして DB
クラスターに追加します。DB
クラスターで書き込み転送を有効にします。アプリケーションを eu-west-1 にデプロイします。eu-west-1 で Aurora MySQL
エンドポイントを使用するようにアプリケーションを設定します。
Answer: D
Explanation:
The company should use AWS Amplify to create a static website for uploads of media files. The company should use Amplify Hosting to serve the website through Amazon CloudFront. The company should use Amazon S3 to store the uploaded media files. The company should use Amazon Cognito to authenticate users.
This solution will meet the requirements with the least operational overhead because AWS Amplify is a complete solution that lets frontend web and mobile developers easily build, ship, and host full-stack applications on AWS, with the flexibility to leverage the breadth of AWS services as use cases evolve. No cloud expertise needed1. By using AWS Amplify, the company can refactor the application to a serverless architecture that reduces operational complexity and costs. AWS Amplify offers the following features and benefits:
Amplify Studio: A visual interface that enables you to build and deploy a full-stack app quickly, including frontend UI and backend.
Amplify CLI: A local toolchain that enables you to configure and manage an app backend with just a few commands.
Amplify Libraries: Open-source client libraries that enable you to build cloud-powered mobile and web apps.
Amplify UI Components: Open-source design system with cloud-connected components for building feature-rich apps fast.
Amplify Hosting: Fully managed CI/CD and hosting for fast, secure, and reliable static and server-side rendered apps.
By using AWS Amplify to create a static website for uploads of media files, the company can leverage Amplify Studio to visually build a pixel-perfect UI and connect it to a cloud backend in clicks. By using Amplify Hosting to serve the website through Amazon CloudFront, the company can easily deploy its web app or website to the fast, secure, and reliable AWS content delivery network (CDN), with hundreds of points of presence globally. By using

Amazon S3 to store the uploaded media files, the company can benefit from a highly scalable, durable, and cost-effective object storage service that can handle any amount of data2. By using Amazon Cognito to authenticate users, the company can add user sign-up, sign-in, and access control to its web app with a fully managed service that scales to support millions of users3.
The other options are not correct because:
Using AWS Application Migration Service to migrate the application server to Amazon EC2 instances would not refactor the application or accelerate development. AWS Application Migration Service (AWS MGN) is a service that enables you to migrate physical servers, virtual machines (VMs), or cloud servers from any source infrastructure to AWS without requiring agents or specialized tools. However, this would not address the challenges of overutilization and data uploads failures. It would also not reduce operational overhead or costs compared to a serverless architecture.
Creating a static website for uploads of media files and using AWS AppSync to create an API would not be as simple or fast as using AWS Amplify. AWS AppSync is a service that enables you to create flexible APIs for securely accessing, manipulating, and combining data from one or more data sources.
However, this would require more configuration and management than using Amplify Studio and Amplify Hosting. It would also not provide authentication features like Amazon Cognito.
Setting up AWS IAM Identity Center (AWS Single Sign-On) to give users the ability to sign in to the application would not be as suitable as using Amazon Cognito. AWS Single Sign-On (AWS SSO) is a service that enables you to centrally manage SSO access and user permissions across multiple AWS accounts and business applications. However, this service is designed for enterprise customers who need to manage access for employees or partners across multiple resources. It is not intended for authenticating end users of web or mobile apps.
References:
https://aws.amazon.com/amplify/
https://aws.amazon.com/s3/
https://aws.amazon.com/cognito/
https://aws.amazon.com/mgn/
https://aws.amazon.com/appsync/
https://aws.amazon.com/single-sign-on/

QUESTION NO: 18
ある会社は、カスタム
アプリケーションから画像をアップロードする機能をユーザーに提供します。アップロード プロセスは、画像を処理して Amazon S3 バケットに保存する AWS Lambda
関数を呼び出します。アプリケーションは、特定の関数バージョン ARN を使用して
Lambda 関数を呼び出します。
Lambda
関数は、環境変数を使用して画像処理パラメーターを受け入れます。同社は、最適な画像処理出力を実現するために、Lambda 関数の環境変数を調整することがよくあります。
同社はさまざまなパラメーターをテストし、結果を検証した後、更新された環境変数を使用して新しい関数バージョンを公開します。この更新プロセスでは、新しい関数バージョンの ARN を呼び出すために、カスタム

アプリケーションを頻繁に変更する必要もあります。これらの変更により、ユーザーの中断が発生します。
ソリューション
アーキテクトは、このプロセスを簡素化して、ユーザーへの混乱を最小限に抑える必要があります。
運用上のオーバーヘッドが最も少なく、これらの要件を満たすソリューションはどれですか？

A. 発行された Lambda 関数のバージョンの環境変数を直接変更します。SLATEST バージョンを使用して、画像処理パラメーターをテストします。

B. 画像処理パラメータを格納する Amazon DynamoDB テーブルを作成します。Lambda 関数を変更して、DynamoDB テーブルから画像処理パラメーターを取得します。

C. Lambda 関数内で画像処理パラメーターを直接コーディングし、環境変数を削除します。会社がパラメーターを更新するときに、新しい関数バージョンを公開します。

D. Lambda 関数のエイリアスを作成します。関数エイリアス ARN を使用するようにクライアント アプリケーションを変更します。
会社がテストを終了したら、関数の新しいバージョンを指すように Lambda エイリアスを再構成します。

Answer: D

Explanation:

A Lambda function alias allows you to point to a specific version of a function and also can be updated to point to a new version of the function without modifying the client application. This way, the company can test different versions of the function with different environment variables and, once the optimal parameters are found, update the alias to point to the new version, without the need to update the client application.

By using this approach, the company can simplify the process of updating the environment variables, minimize disruption to users, and reduce the operational overhead.

Reference:

AWS Lambda documentation: https://aws.amazon.com/lambda/

AWS Lambda Aliases documentation: https://docs.aws.amazon.com/lambda/latest/dg/aliases-intro.html AWS Lambda versioning and aliases documentation: https://aws.amazon.com/blogs/compute/versioning-aliases-in-aws-lambda/

QUESTION NO: 19

大手給与会社は最近、小規模な人材派遣会社と合併しました。現在、統合された会社には複数のビジネスユニットがあり、それぞれが独自の既存の AWS アカウントを持っています。
ソリューションアーキテクトは、企業がすべての AWS アカウントの請求およびアクセスポリシーを一元管理できることを確認する必要があります。ソリューションアーキテクトは、集中管理アカウントから会社のすべてのメンバーアカウントに招待を送信することにより、AWS Organizations を構成します。
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は次に何をすべきでしょうか？

A. 各メンバー アカウントに OrganizationAccountAccess IAM グループを作成します。各管理者に必要な IAM ロールを含めます。

B. 各メンバー アカウントに OrganizationAccountAccessPolicy IAM

ポリシーを作成します。クロスアカウント アクセスを使用して、メンバー
アカウントを管理アカウントに接続します。
C. 各メンバー アカウントに OrganizationAccountAccessRole IAM
ロールを作成します。管理アカウントに IAM
ロールを引き受けるアクセス許可を付与します。
D. 管理アカウントに OrganizationAccountAccessRole IAM
ロールを作成します。AdministratorAccess AWS 管理ポリシーを IAM
ロールにアタッチします。各メンバー アカウントの管理者に IAM ロールを割り当てます。
Answer: C

QUESTION NO: 20
ある企業は、Amazon EC2 インスタンスのフリートに分散型インメモリ
データベースをデプロイしています。フリートは、1 つのプライマリ ノードと 8
つのワーカー ノードで構成されます。プライマリ
ノードは、クラスターの健全性の監視、ユーザー リクエストの受け入れ、ユーザー
リクエストのワーカー
ノードへの分散、集約応答のクライアントへの送信を担当します。ワーカー
ノードは相互に通信してデータ パーティションを複製します。
同社は、最大のパフォーマンスを達成するために、ネットワーク遅延を可能な限り低く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. パーティション配置グループでメモリ最適化された EC2 インスタンスを起動します。
B. パーティション配置グループでコンピューティングに最適化された EC2
インスタンスを起動します。
C. クラスター配置グループでメモリ最適化された EC2 インスタンスを起動します。
D. スプレッド配置グループでコンピューティングに最適化された EC2
インスタンスを起動します。
Answer: C

QUESTION NO: 21
ソフトウェア会社は、開発プロセスの一環として、プル
リクエストをテストするための短期間のテスト環境を作成する必要があります。各テスト環境は、Auto Scaling グループ内の単一の Amazon EC2 インスタンスで構成されます。
テスト環境は、テスト結果を報告するために中央サーバーと通信できる必要があります。中央サーバーはオンプレミスのデータセンターにあります。ソリューション
アーキテクトは、企業が手動介入なしでテスト環境を作成および削除できるようにソリューションを実装する必要があります。同社は、オンプレミス ネットワークへの VPN
接続を備えたトランジット ゲートウェイを作成しました。
運用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すか?
A. トランジットゲートウェイのアタッチメントと関連するルーティング設定を含む AWS CloudFormation テンプレートを作成します。このテンプレートを含む CloudFormation スタック セットを作成します。CloudFormation StackSets を使用して、アカウント内の各 VPC に新しいスタックをデプロイします。テスト環境ごとに新しい VPC
をデプロイします。

B. テスト環境用に単一の VPC を作成します。トランジット
ゲートウェイのアタッチメントと関連するルーティング構成を含めます。AWS
CloudFormation を使用して、すべてのテスト環境を VPC にデプロイします。
C. テスト用に AWS Organizations に新しい OU を作成します。VPC、必要なネットワーク
リソース、トランジット ゲートウェイ
アタッチメント、および関連するルーティング設定を含む AWS CloudFormation
テンプレートを作成します。このテンプレートを含む CloudFormation スタック
セットを作成します。01.1 のテストで各アカウントにデプロイするには CloudFormation
StackSet を使用します。テスト環境ごとに新しいアカウントを作成します。
D. テスト環境 EC2 インスタンスを Docker イメージに変換します。AWS CloudFormation
を使用して、新しい VPC で Amazon Elastic Kubernetes Service (Amazon EKS)
クラスターを設定し、トランジットゲートウェイアタッチメントを作成し、関連するルーティング設定を作成します。Kubernetes
を使用して、テスト環境のデプロイメントとライフサイクルを管理します。
Answer: B
Explanation: This option allows the company to use a single VPC to host multiple test environments that are isolated from each other by using different subnets and security groups1. By including a transit gateway attachment and related routing configurations, the company can enable the test environments to communicate with the central server in the on-premises data center through a VPN connection2. By using AWS CloudFormation to deploy all test environments into the VPC, the company can automate the creation and deletion of test environments without any manual intervention3. This option also minimizes the operational overhead by reducing the number of VPCs, accounts, and resources that need to be managed.
References:
Working with VPCs and subnets
Working with transit gateways
Working with AWS CloudFormation stacks

QUESTION NO: 22
会社は、Source という名前の AWS
アカウントにアプリケーションを持っています。アカウントは AWS Organizations
の組織にあります。アプリケーションの 1 つは AWS Lambda 関数を使用し、在庫データを
Amazon Aurora データベースに保存します。アプリケーションは、デプロイ
パッケージを使用して Lambda 関数をデプロイします。同社は、Aurora
の自動バックアップを構成しています。
この会社は、Lambda 関数と Aurora データベースを、Target という名前の新しい AWS
アカウントに移行したいと考えています。アプリケーションは重要なデータを処理するため、会社はダウンタイム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すか?
A. ソース アカウントから Lambda 関数デプロイ
パッケージをダウンロードします。デプロイ パッケージを使用して、Target
アカウントで新しい Lambda 関数を作成します。自動化された Aurora DB
クラスターのスナップショットを Target アカウントと共有します。
B. ソース アカウントから Lambda 関数デプロイ

パッケージをダウンロードします。デプロイ パッケージを使用して、Target アカウントで新しい Lambda 関数を作成する AWS Resource Access Manager (AWS RAM) を使用して、Aurora DB クラスターを Target アカウントと共有します。Aurora DB クラスターのクローンを作成するアクセス許可をターゲット アカウントに付与します。

C. AWS Resource Access Manager (AWS RAM) を使用して、Lambda 関数と Aurora DB クラスターをターゲット アカウントと共有します。Aurora DB クラスターのクローンを作成するアクセス許可をターゲット アカウントに付与します。

D. AWS Resource Access Manager (AWS RAM) を使用して、Lambda 関数をターゲット アカウントと共有します。自動化された Aurora DB クラスターのスナップショットを Target アカウントと共有します。

Answer: C

Explanation:

This solution uses a combination of AWS Resource Access Manager (RAM) and automated backups to migrate the Lambda functions and the Aurora database to the Target account while minimizing downtime. In this solution, the Lambda function deployment package is downloaded from the Source account and used to create new Lambda functions in the Target account. The Aurora DB cluster is shared with the Target account using AWS RAM and the Target account is granted permission to clone the Aurora DB cluster, allowing for a new copy of the Aurora database to be created in the Target account. This approach allows for the data to be migrated to the Target account while minimizing downtime, as the Target account can use the cloned Aurora database while the original Aurora database continues to be used in the Source account.

QUESTION NO: 23

ある企業は、Amazon EC2 Auto Scaling グループへのアプリケーションの CI/CD に AWS CodePipeline を使用しています。すべての AWS リソースは AWS CloudFormation テンプレートで定義されます。アプリケーションアーティファクトは Amazon S3 バケットに保存され、インスタンスユーザーデータスクリプトを使用して Auto Scaling グループにデプロイされます。

アプリケーションがより複雑になるにつれて、CloudFormation テンプレートの最近のリソース変更により、計画外のダウンタイムが発生しました。

ソリューションアーキテクトは、テンプレートの変更によってダウンタイムが発生する可能性を減らすために、CI/CD パイプラインをどのように改善する必要がありますか?

A. デプロイメント実行時に CloudFormation エラー状態を検出して報告するようにデプロイメント スクリプトを調整します。本番環境への変更を承認する前に、テスト チームが非本番環境で実行するためのテスト計画を作成します。

B. テスト環境で AWS CodeBuild を使用して自動テストを実装します。CloudFormation 変更セットを使用して、デプロイ前に変更を評価します。AWS CodeDeploy を使用してブルー/グリーン デプロイメント パターンを活用し、必要に応じて評価と変更を元に戻すことができるようにします。

C. 統合開発環境 (IDE) のプラグインを使用してテンプレートにエラーがないか確認し、AWS CLI を使用してテンプレートが正しいことを検証します。デプロイメント コードを調整して、エラー状態をチェックし、エラーに関する通知を生成します。本番環境

への変更を承認する前に、テスト環境にデプロイし、手動テスト計画を実行します。
D. AWS CodeDeploy と CloudFormation での Blue/Green デプロイ
パターンを使用して、ユーザー データ デプロイ
スクリプトを置き換えます。オペレーターに実行中のインスタンスにログインさせ、手動のテスト計画を実行して、アプリケーションが期待どおりに実行されていることを確認します。
Answer: B

QUESTION NO: 24
企業には、データ層が単一の AWS
リージョンにデプロイされている重要なアプリケーションがあります。データ層は、Amazon DynamoDB テーブルと Amazon Aurora MySQL DB クラスターを使用します。現在の Aurora MySQL エンジンのバージョンは、グローバル
データベースをサポートしています。アプリケーション層は、すでに 2
つのリージョンにデプロイされています。
会社のポリシーでは、重要なアプリケーションにはアプリケーション層コンポーネントとデータ層コンポーネントが 2
つのリージョンにデプロイされている必要があると規定されています。RTO と RPO
は、それぞれ数分以内にする必要があります。ソリューション
アーキテクトは、データ層を会社のポリシーに準拠させるためのソリューションを推奨する必要があります。
これらの要件を満たすのは、どのステップの組み合わせですか？（2つ選んでください。）
A. Aurora MySQL DB クラスターに別のリージョンを追加する
B. Aurora MySQL DB クラスターの各テーブルに別のリージョンを追加します。
C. DynamoDB テーブルと Aurora MySQL DB
クラスターのスケジュールされたクロスリージョン バックアップを設定する
D. 別のリージョンを構成に追加して、既存の DynamoDB テーブルをグローバル
テーブルに変換します。
E. Amazon Route 53 Application Recovery Controller
を使用して、データベースのバックアップとセカンダリ
リージョンへのリカバリを自動化する
Answer: A D
Explanation:
The company should use Amazon Aurora global database and Amazon DynamoDB global table to deploy the data tier components across two Regions. Amazon Aurora global database is a feature that allows a single Aurora database to span multiple AWS Regions, enabling low-latency global reads and fast recovery from Region-wide outages1. Amazon DynamoDB global table is a feature that allows a single DynamoDB table to span multiple AWS Regions, enabling low-latency global reads and writes and fast recovery from Region-wide outages2.
References:
https://aws.amazon.com/rds/aurora/global-database/
https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/globaltables_HowItWorks.html
https://aws.amazon.com/route53/application-recovery-controller/

QUESTION NO: 25
ある企業は AWS
クラウドで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、AWS Lambda 関数と、プライマリ コンピューティングとして AWS Fargate テクノロジーで実行される Amazon Elastic Container Service (Amazon ECS)
コンテナを使用します。アプリケーションの負荷は不規則です。アプリケーションが長期間使用されないと、トラフィックが突然大幅に増加または減少します。このアプリケーションは書き込み負荷が高く、データを Amazon Aurora MySQL
データベースに保存します。データベースは、負荷を処理できない Amazon RDS
メモリに最適化された DB インスタンス上で実行されます。
トラフィックの突然の大幅な変化に企業が対処する最も費用対効果の高い方法は何ですか?
A. データベースにリードレプリカを追加します。Instance Savings Plan と RDS リザーブドインスタンスを購入します。
B. データベースを Aurora マルチマスター DB クラスターに移行します。Instance Savings Plan を購入します。
C. データベースを Aurora グローバル データベースに移行します。Compute Savings Plan と RDS リザーブド インスタンスを購入します。
D. データベースを Aurora Serverless v1 に移行します。Compute Savings Plan を購入します。
Answer: D

QUESTION NO: 26
グローバルオフィスを持つ企業は、単一のAWSリージョンへの単一の1 Gbps AWS DirectConnect接続を持っています。
会社のオンプレミスネットワークは、接続を使用してAWSクラウド内の会社のリソースと通信します。接続には、単一のVPCに接続する単一のプライベート仮想インターフェイスがあります。
ソリューションアーキテクトは、同じリージョンに冗長なDirectConnect接続を追加するソリューションを実装する必要があります。このソリューションは、会社が他の地域に拡大するのと同じダイレクトコネクト接続のペアを介して他の地域への接続も提供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.ダイレクトコネクトゲートウェイをプロビジョニングします。既存の接続から既存のプライベート仮想インターフェイスを削除します。
2番目の直接接続接続を作成します。各接続で新しいプライベート仮想インターレースを作成し、両方のプライベート仮想インターフェイスをDirectConnectゲートウェイに接続します。 DirectConnectゲートウェイを単一のVPCに接続します。
B.既存のプライベート仮想インターフェイスを保持します。
2番目の直接接続接続を作成します。新しい接続で新しいプライベート仮想インターフェイスを作成し、新しいプライベート仮想インターフェイスを単一のVPCに接続します。
C.既存のプライベート仮想インターフェイスを保持します。
2番目の直接接続接続を作成します。新しい接続で新しいパブリック仮想インターフェイスを作成し、新しいパブリック仮想インターフェイスを単一のVPCに接続します。
D.トランジットゲートウェイをプロビジョニングします。既存の接続から既存のプライベー

ト仮想インターフェイスを削除します。
2番目の直接接続接続を作成します。接続ごとに新しいプライベート仮想インターフェイスを作成し、両方のプライベート仮想インターフェイスをトランジットゲートウェイに接続します。トランジットゲートウェイを単一のVPCに関連付けます。

Answer: A

Explanation:
A Direct Connect gateway is a globally available resource. You can create the Direct Connect gateway in any Region and access it from all other Regions. The following describe scenarios where you can use a Direct Connect gateway.
https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways-intro.html

QUESTION NO: 27

ある企業は、AWS クラウドの Amazon EC2
インスタンスでアプリケーションを実行しています。アプリケーションは、データ層としてレプリカ セットを持つ MongoDB データベースを使用しています。MongoDB
データベースは、会社のオンプレミス
データセンターのシステムにインストールされており、データセンター環境への AWS Direct Connect 接続を通じてアクセスできます。
ソリューションアーキテクトは、オンプレミスの MongoDB データベースを Amazon DocumentDB (MongoDB 互換性あり) に移行する必要があります。
ソリューションアーキテクトは、この移行を実行するためにどの戦略を選択する必要がありますか?

A. EC2 インスタンスのフリートを作成します。EC2 インスタンスに MongoDB Community Edition
をインストールし、データベースを作成します。オンプレミスのデータセンターで実行されているデータベースを使用して、継続的な同期レプリケーションを構成します。

B. AWS Database Migration Service (AWS DMS) レプリケーション
インスタンスを作成します。変更データ キャプチャ (CDC) を使用して、オンプレミスの MongoDB データベースのソース エンドポイントを作成します。Amazon DocumentDB
データベースのターゲットエンドポイントを作成します。DMS
移行タスクを作成して実行します。

C. AWS Data Pipeline を使用してデータ移行パイプラインを作成します。オンプレミスの MongoDB データベースと Amazon DocumentDB データベースのデータ
ノードを定義します。データ
パイプラインを実行するスケジュールされたタスクを作成します。

D. AWS Glue クローラーを使用して、オンプレミスの MongoDB
データベースのソースエンドポイントを作成します。MongoDB データベースと Amazon DocumentDB データベースの間で継続的な非同期レプリケーションを設定します。

Answer: B

Explanation:
https://aws.amazon.com/getting-started/hands-on/move-to-managed/migrate-mongodb-to-documentdb/

QUESTION NO: 28

ソリューション アーキテクトは、既存の VPC の DNS 戦略を決定しています。VPC は、10.24.34.0/24 CIDR ブロック。VPC は、DNS に Amazon Route 53 リゾルバーも使用します。新しい要件では、DNS クエリでプライベート ホスト ゾーンを使用することが義務付けられています。さらに、パブリック IP アドレスを持つインスタンスは、対応するパブリック ホスト名を受け取る必要があります。
VPC
内でドメイン名が正しく解決されることを保証するために、これらの要件を満たすソリューションはどれですか?

A. プライベートホストゾーンを作成します。VPC のenableDnsSupport 属性とenableDnsHostnames 属性を有効にします。VPC DHCP オプション セットを更新して、domain-name-servers-10.24.34.2 を含めます。

B. プライベートホストゾーンを作成します。プライベートホストゾーンを VPC に関連付けます。VPC のenableDnsSupport 属性とenableDnsHostnames 属性を有効にします。新しい VPC DHCP オプション セットを作成し、domain-name-servers=AmazonProvidedDNS を設定します。新しい DHCP オプション セットを VPC に関連付けます。

C. VPC のenableDnsSupport 属性を非アクティブ化します。VPC のenableDnsHostnames 属性をアクティブ化します。新しい VPC DHCP オプション セットを作成し、domain-name-servers=10.24.34.2 を構成します。
新しい DHCP オプション セットを VPC に関連付けます。

D. プライベートホストゾーンを作成します。プライベートホストゾーンを VPC に関連付けます。VPC のenableDnsSupport 属性を有効にします。VPC のenableDnsHostnames 属性を非アクティブ化します。VPC DHCP オプション セットを更新して、domain-name-servers=AmazonProvidedDNS を含めます。

Answer: B

Explanation: This option allows the solutions architect to use a private hosted zone to host DNS records that are only accessible within the VPC1. By associating the private hosted zone with the VPC, the solutions architect can ensure that DNS queries from the VPC are routed to the private hosted zone2. By activating the enableDnsSupport attribute and the enableDnsHostnames attribute for the VPC, the solutions architect can enable DNS resolution and hostname assignment for instances in the VPC3. By creating a new VPC DHCP options set, and configuring domain-name-servers=AmazonProvidedDNS, the solutions architect can use Amazon-provided DNS servers to resolve DNS queries from instances in the VPC4. By associating the new DHCP options set with the VPC, the solutions architect can apply the DNS settings to all instances in the VPC5.
References:
What is Amazon Route 53 Resolver?
Associating a private hosted zone with your VPC
Using DNS with your VPC
DHCP options sets
Modifying your DHCP options

QUESTION NO: 29
ある企業は、数千の Amazon EC2

インスタンスで構成されるワークロードを実行しています。ワークロードは、複数のパブリック サブネットとプライベート サブネットを含む VPC
で実行されています。パブリックサブネットには、
0.0.0.0/0 を既存のインターネット ゲートウェイに接続します。プライベート
サブネットには、既存の NAT ゲートウェイへの 0.0.0.0/0 のルートがあります。
ソリューションアーキテクトは、IPv6 を使用するために EC2
インスタンス全体を移行する必要があります。プライベート サブネットにある EC2
インスタンスには、パブリック インターネットからアクセスできません。
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は何をすべきでしょうか?
A. 既存の VPC を更新し、カスタム IPv6 CIDR ブロックを VPC
およびすべてのサブネットに関連付けます。
すべての VPC ルート テーブルを更新し、::/0 のルートをインターネット
ゲートウェイに追加します。
B. 既存の VPC を更新し、Amazon が提供する IPv6 CIDR ブロックを VPC
およびすべてのサブネットに関連付けます。すべてのプライベート サブネットの VPC
ルート テーブルを更新し、::/0 のルートを NAT ゲートウェイに追加します。
C. 既存の VPC を更新し、Amazon が提供する IPv6 CIDR ブロックを VPC
およびすべてのサブネットに関連付けます。下り専用のインターネットゲートウェイを作成します。すべてのプライベート サブネットの VPC ルート テーブルを更新し、::/0
のルートを出力専用インターネット ゲートウェイに追加します。
D. 既存の VPC を更新し、カスタム IPv6 CIDR ブロックを VPC
およびすべてのサブネットに関連付けます。新しい NAT ゲートウェイを作成し、IPv6
サポートを有効にします。すべてのプライベート サブネットの VPC ルート
テーブルを更新し、::/0 のルートを IPv6 対応 NAT ゲートウェイに追加します。
Answer: C

QUESTION NO: 30
ある会社が、Amazon RDS
forMySQLデータベースを使用してデータを保存する重要なアプリケーションを実行しています。 RDS DBインスタンスは、マルチAZモードでデプロイされます。
最近のRDSデータベースフェイルオーバーテストにより、アプリケーションが40秒停止しました。ソリューションアーキテクトは、停止時間を20秒未満に短縮するソリューションを設計する必要があります。
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はどの手順の組み合わせを実行する必要がありますか？（3つ選択してください。）
A.データベースの前でMemcachedにAmazonElastiCacheを使用する
B.データベースの前でRedisにAmazonElastiCacheを使用します。
C.データベースの前でRDSプロキシを使用する
D.データベースをAmazon AuroraMySQLに移行します
E.AmazonAuroraレプリカを作成する
F.MySQL読み取りレプリカのRDSを作成します
Answer: C D E
Explanation:
Migrate the database to Amazon Aurora MySQL. - Create an Amazon Aurora Replica. - Us

e RDS Proxy in front of the database. - These options are correct because they address the requirement of reducing the failover time to less than 20 seconds. Migrating to Amazon Aurora MySQL and creating an Aurora replica can reduce the failover time to less than 20 seconds. Aurora has a built-in, fault-tolerant storage system that can automatically detect and repair failures. Additionally, Aurora has a feature called "Aurora Global Database" which allows you to create read-only replicas across multiple AWS regions which can further help to reduce the failover time. Creating an Aurora replica can also help to reduce the failover time as it can take over as the primary DB instance in case of a failure. Using RDS proxy can also help to reduce the failover time as it can route the queries to the healthy DB instance, it also helps to balance the load across multiple DB instances.

QUESTION NO: 31
ある企業は、Application Load Balancer (ALB) の背後にある Amazon EC2
インスタンスでイントラネット Web
アプリケーションをホストしています。現在、ユーザーは内部ユーザー
データベースに対してアプリケーションを認証します。
会社は、既存の AWS Directory Service for Microsoft Active Directory
ディレクトリを使用して、アプリケーションに対してユーザーを認証する必要があります。
ディレクトリ内のアカウントを持つすべてのユーザーは、アプリケーションにアクセスできる必要があります。
これらの要件を満たすソリューションはどれですか?
A. ディレクトリに新しいアプリ クライアントを作成します。ALB のリスナー
ルールを作成します。リスナールールのauthenticate-oidcアクションを指定します。Active Directory サービスの適切な発行者、クライアント ID
とシークレット、エンドポイントの詳細を使用してリスナー ルールを構成します。ALB
が提供するコールバック URL を使用して新しいアプリ クライアントを構成します。
B. Amazon Cognito
ユーザープールを設定します。ディレクトリからのメタデータを持つフェデレーション ID
プロバイダー (IdP) を使用してユーザー
プールを構成します。アプリクライアントを作成します。アプリクライアントをユーザープールに関連付けます。ALB のリスナー ルールを作成します。リスナー
ルールの認証認識アクションを指定します。
ユーザー プールとアプリ クライアントを使用するようにリスナー ルールを構成します。
C. ディレクトリを新しい 1AM ID プロバイダー (IdP) として追加します。SAML 2.0
フェデレーションのエンティティ タイプを持つ新しい 1AM ロールを作成します。ALB
へのアクセスを許可するロール ポリシーを構成します。新しいロールを IdP
のデフォルトの認証済みユーザー ロールとして構成します。ALB のリスナー
ルールを作成します。リスナールールのauthenticate-oidcアクションを指定します。
D. AWS 1AM ID センター (AWS シングル サインオン) を有効にします。SAML
を使用する外部 ID プロバイダー (IdP)
としてディレクトリを構成します。自動プロビジョニング方式を使用します。SAML 2.0
フェデレーションのエンティティ タイプを持つ新しい 1AM ロールを作成します。ALB
へのアクセスを許可するロール ポリシーを構成します。
新しいロールをすべてのグループにアタッチします。ALB のリスナー
ルールを作成します。リスナー ルールの認証認識アクションを指定します。

Answer: A
Explanation:
The correct solution is to use the authenticate-oidc action for the ALB listener rule and configure it with the details of the AWS Directory Service for Microsoft Active Directory directory. This way, the ALB can use OpenID Connect (OIDC) to authenticate users against the directory and grant them access to the intranet web application. The app client in the directory is used to register the ALB as an OIDC client and provide the necessary credentials and endpoints. The callback URL is the URL that the ALB redirects the user to after a successful authentication. This solution does not require any additional services or roles, and it leverages the existing directory accounts for all users.
The other solutions are incorrect because they either use the wrong action for the ALB listener rule, or they involve unnecessary or incompatible services or roles. For example:
Solution B is incorrect because it uses Amazon Cognito user pool, which is a separate user directory service that does not integrate with AWS Directory Service for Microsoft Active Directory. To use this solution, the company would have to migrate or synchronize their users from the directory to the user pool, which is not required by the question. Moreover, the authenticate-cognito action for the ALB listener rule only works with Amazon Cognito user pools, not with federated identity providers (IdPs) that have metadata from the directory.
Solution C is incorrect because it uses IAM as an identity provider (IdP), which is not compatible with AWS Directory Service for Microsoft Active Directory. IAM can only be used as an IdP for web identity federation, which allows users to sign in with social media or other third-party IdPs, not with Active Directory. Moreover, the authenticate-oidc action for the ALB listener rule requires an OIDC IdP, not a SAML 2.0 federation IdP, which is what IAM provides.
Solution D is incorrect because it uses AWS IAM Identity Center (AWS Single Sign-On), which is a service that simplifies the management of SSO access to multiple AWS accounts and business applications. This service is not needed for the scenario in the question, which only involves a single intranet web application. Moreover, the authenticate-cognito action for the ALB listener rule does not work with external IdPs that use SAML, such as AWS IAM Identity Center.
References:
Authenticate users using an Application Load Balancer
What is AWS Directory Service for Microsoft Active Directory?
Using OpenID Connect for user authentication

QUESTION NO: 32
ある企業は、Web サイトをオンプレミスのデータセンターから AWS に移行したいと考えています。同時に、可用性とコスト効率を向上させるために、Web サイトをコンテナ化されたマイクロサービス
ベースのアーキテクチャに移行したいと考えています。会社のセキュリティ
ポリシーでは、最小限の特権を使用して、ベスト プラクティスに従って特権とネットワーク アクセス許可を構成する必要があると規定しています。
ソリューションアーキテクトは、セキュリティ要件を満たすコンテナ化されたアーキテクチャを作成し、アプリケーションを Amazon ECS
クラスターにデプロイする必要があります。

導入後に要件を満たすにはどのような手順が必要ですか? (2つお選びください。)
A. ブリッジ ネットワーク モードを使用してタスクを作成します。
B. awsvpc ネットワーク モードを使用してタスクを作成します。
C. セキュリティ グループを Amazon EC2 インスタンスに適用し、EC2 インスタンスの IAM ロールを使用して他のリソースにアクセスします。
D. セキュリティ グループをタスクに適用し、起動時に IAM 認証情報をコンテナに渡して他のリソースにアクセスします。
E. セキュリティ グループをタスクに適用し、タスクの IAM ロールを使用して他のリソースにアクセスします。
Answer: B E
Explanation: The awsvpc network mode provides each task with its own elastic network interface (ENI) and a primary private IP address1. By using this network mode, the solutions architect can isolate the tasks from each other and apply security groups to the tasks directly2. This way, the solutions architect can control the inbound and outbound traffic at the task level and enforce the least privilege principle3. IAM roles for tasks allow the solutions architect to assign permissions to each task separately, so that they can access other AWS resources that they need4. By using IAM roles for tasks, the solutions architect can avoid passing IAM credentials into the container at launch time, which is less secure and more prone to errors5.
References:
awsvpc network mode
Task networking with the awsvpc network mode
Security groups for your VPC
IAM roles for tasks
Best practices for managing AWS access keys

QUESTION NO: 33
ある会社はスマートビークルを製造しています。同社は、カスタム アプリケーションを使用して車両データを収集しています。車両は MQTT プロトコルを使用してアプリケーションに接続します。
会社は 5 分間隔でデータを処理します。その後、同社は車両テレマティクス データをオンプレミス ストレージにコピーします。カスタム アプリケーションは、このデータを分析して異常を検出します。
データを送信する車両の数は常に増加しています。新しい車両は大量のデータを生成します。オンプレミスのストレージ ソリューションは、ピーク時のトラフィックに合わせて拡張できず、データ損失につながります。同社は、ソリューションを最新化し、ソリューションを AWS に移行して、スケーリングの課題を解決する必要があります。
運用上のオーバーヘッドが最も少なく、これらの要件を満たすソリューションはどれですか?
A. AWS IOT Greengrass を使用して、車両データを Amazon Managed Streaming for Apache Kafka (Amazon MSK) に送信します。Amazon S3 にデータを保存する Apache Kafka アプリケーションを作成します。Amazon SageMaker で事前トレーニング済みのモデルを使用して、異常を検出します。
B. AWS IOT Core を使用して車両データを受信します。Amazon S3 にデータを保存する

Amazon Kinesis Data Firehose
配信ストリームにデータをルーティングするルールを設定します。配信ストリームから読み取って異常を検出する Amazon Kinesis Data Analytics アプリケーションを作成します。
C. AWS IOT FleetWise を使用して車両データを収集します。データを Amazon Kinesis データ ストリームに送信します。
Amazon Kinesis Data Firehose 配信ストリームを使用して、データを Amazon S3 に保存します。AWS Glue の組み込みの機械学習変換を使用して、異常を検出します。
D. Amazon MQ for RabbitMQ を使用して車両データを収集します。データを Amazon Kinesis Data Firehose 配信ストリームに送信して、データを Amazon S3 に保存します。Amazon Lookout for Metrics を使用して異常を検出します。
Answer: B
Explanation:
Using AWS IoT Core to receive the vehicle data will enable connecting the smart vehicles to the cloud using the MQTT protocol1. AWS IoT Core is a platform that enables you to connect devices to AWS Services and other devices, secure data and interactions, process and act upon device data, and enable applications to interact with devices even when they are offline2. Configuring rules to route data to an Amazon Kinesis Data Firehose delivery stream that stores the data in Amazon S3 will enable processing and storing the vehicle data in a scalable and reliable way3. Amazon Kinesis Data Firehose is a fully managed service that delivers real-time streaming data to destinations such as Amazon S3. Creating an Amazon Kinesis Data Analytics application that reads from the delivery stream to detect anomalies will enable analyzing the vehicle data using SQL queries or Apache Flink applications. Amazon Kinesis Data Analytics is a fully managed service that enables you to process and analyze streaming data using SQL or Java.

QUESTION NO: 34
ある企業が、静的コンテンツをホストする新しい Web サイトを設計しています。この Web サイトにより、ユーザーは大きなファイルをアップロードおよびダウンロードできます。会社の要件に従って、すべてのデータは転送中および保管中に暗号化する必要があります。ソリューション アーキテクトは、Amazon S3 と Amazon CloudFront を使用してソリューションを構築しています。
暗号化の要件を満たすのは、どの手順の組み合わせですか? (3 つ選択してください。)
A. Web アプリケーションが使用する S3 バケットの S3 サーバー側暗号化をオンにします。
B. S3 ACL の読み取りおよび書き込み操作用に、"aws:SecureTransport": "true" のポリシー属性を追加します。
C. Web アプリケーションが使用する S3 バケットで暗号化されていない操作を拒否するバケット ポリシーを作成します。
D. AWS KMS キー (SSE-KMS) によるサーバー側の暗号化を使用して、CloudFront で保存時の暗号化を構成します。
E. CloudFront で HTTP リクエストの HTTPS リクエストへのリダイレクトを設定します。
F. Web アプリケーションが使用する S3 バケットの署名付き URL の作成で RequireSSL オプションを使用します。
Answer: A C E
Explanation:

Turning on S3 server-side encryption for the S3 bucket that the web application uses will enable encrypting the data at rest using Amazon S3 managed keys (SSE-S3)1. Creating a bucket policy that denies any unencrypted operations in the S3 bucket that the web application uses will enable enforcing encryption for all requests to the bucket2. Configuring redirection of HTTP requests to HTTPS requests in CloudFront will enable encrypting the data in transit using SSL/TLS3.

QUESTION NO: 35
ある企業はインフラストラクチャを AWS
クラウドに移行しています。企業は、さまざまなプロジェクトのさまざまな規制基準に準拠する必要があります。会社はマルチアカウント環境を必要としています。
ソリューションアーキテクトは、ベースラインインフラストラクチャを準備する必要があります。このソリューションは、管理とセキュリティの一貫したベースラインを提供する必要がありますが、さまざまな AWS
アカウント内のさまざまなコンプライアンス要件に柔軟に対応できる必要があります。このソリューションは、既存のオンプレミスの Active Directory フェデレーション サービス (AD FS) サーバーと統合する必要もあります。
運用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すか?
A. AWS Organizations
で組織を作成します。すべてのアカウントにわたる最小特権アクセス用の単一の SCP
を作成します。すべてのアカウントに対して単一の OU を作成します。オンプレミスの AD FS サーバーとのフェデレーション用に IAM ID
プロバイダーを構成します。ログ生成サービスが中央アカウントにログ
イベントを送信するための定義済みプロセスを使用して中央ログ
アカウントを構成します。すべてのアカウントの適合パックを使用して、中央アカウントで AWS Config を有効にします。
B. AWS Organizations で組織を作成します。組織で AWS Control Tower
を有効にします。SCP に含まれるコントロール (ガードレール)
を確認します。追加が必要な領域については、AWS Config
を確認してください。必要に応じて OUS を追加します。AWS IAM Identity Center (AWS Single Sign-On) をオンプレミスの AD FS サーバーに接続します。
C. AWS Organizations で組織を作成します。最小限の特権アクセス用の SCP
を作成します。OU 構造を作成し、それを使用して AWS
アカウントをグループ化します。AWS IAM Identity Center (AWS Single Sign-On)
をオンプレミスの AD FS
サーバーに接続します。ログ生成サービスが中央アカウントにログ
イベントを送信するための定義済みプロセスを使用して中央ログ
アカウントを構成します。アグリゲーターと適合パックを使用して、中央アカウントで AWS Config を有効にします。
D. AWS Organizations で組織を作成します。組織で AWS Control Tower
を有効にします。SCP に含まれるコントロール (ガードレール)
を確認します。追加が必要な領域については、AWS Config
を確認してください。オンプレミスの AD FS サーバーとのフェデレーション用に IAM ID
プロバイダーを構成します。

Answer: B