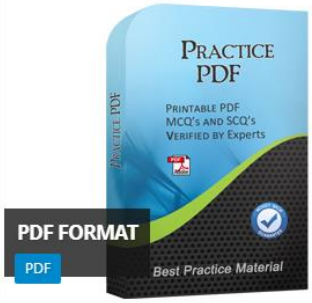
ActualVCE

- 24/7 customer support, Secure shopping site
- Free One year updates to match real exam scenarios
- If you failed your exam after buying our products we will refund the full amount back to you.

Download Demo

- Online Tool, Convenient, easy to study.
- Instant Online Access
- Supports All Web Browsers
- Practice Online Anytime
- Test History and Performance Review
- Supports Windows / Mac / Android / iOS, etc.

- Installable Software Application
- Simulates Real Exam Environment
- Builds Exam Confidence
- Supports MS Operating System
- Two Modes For Practice
- Practice Offline Anytime



- Printable PDF Format
- Prepared by IT Experts
- Instant Access to Download
- Study Anywhere, Anytime
- 365 Days Free Updates
- Free PDF Demo Available

Security & Privacy

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

365 Days Free Updates

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

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 ActualVCE.

Try Before Buy

ActualVCE 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.

http://www.actualvce.com/

Believable Exam Dumps Questions grant you ensured success by your first attempt - ActualVCE

Exam : **SCS-C02-JPN**

Title : AWS Certified Security - Specialty (SCS-C02日本語版)

Vendor : Amazon

Version : DEMO

QUESTION NO: 1
ある企業は、AWS Organizations 内の組織に AWS
アカウントを保有しています。この企業は、本番環境、サポート環境、テスト環境のアカウントで Amazon GuardDuty
を有効化しています。重要なワークロードは本番環境アカウントで実行し、ログはサポート環境アカウントの Amazon S3 バケットに一元的に保存しています。
セキュリティエンジニアは、本番環境アカウントとS3バケットのセキュリティ検出結果を「高」レベルに引き上げ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、重大度が「高」の検出結果を自動的に「重大」レベルに引き上げる必要があります。
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. すべてのアカウントでAWS Security Hubを有効にします。Security Hub管理者アカウントで、GuardDuty統合を有効にします。本番環境アカウントとS3バケットの検出結果を優先する自動化ルールを作成します。
B. すべてのアカウントでAWS Security Hubを有効にします。Security Hub管理者アカウントで、GuardDuty統合を有効にします。Amazon EventBridgeを使用して、本番環境アカウントとS3バケットの検出結果を昇格させるカスタムルールを作成します。
C. GuardDuty 管理者アカウントを使用して、本番環境アカウントと S3 バケットを含む脅威リストを設定します。Amazon EventBridge と Amazon Simple Notification Service (Amazon SNS)
を使用して、脅威リストからの検出結果を上位に表示します。
D. GuardDuty 管理者アカウントを使用して、S3 バケットを含むサポートアカウントの S3 保護を有効にします。本番環境アカウントと S3 バケットの検出結果を昇格するように GuardDuty を設定します。
Answer: A

QUESTION NO: 2
ある会社には 1 つの AWS アカウントがあり、Amazon EC2
インスタンスを使用してアプリケーション
コードをテストしています。この会社は最近、インスタンスが侵害されたことを発見しました。インスタンスはマルウェアを配信していました。インスタンスを分析した結果、インスタンスは 35 日前に侵害されたことが判明しました。
セキュリティ
エンジニアは、重大度の高い検出結果について、電子メール配信リストを通じて侵害されたインスタンスについて会社のセキュリティ
チームに自動的に通知する継続的な監視ソリューションを実装する必要があります。セキュリティ エンジニアは、できるだけ早く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ために、セキュリティ
エンジニアはどのような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. AWS アカウントで AWS Security Hub を有効にします。
B. AWS アカウントで Amazon GuardDuty を有効にします。
C. Amazon Simple Notification Service (Amazon SNS)
トピックを作成します。セキュリティチームのメール配信リストをトピックに登録します。

D. Amazon Simple Queue Service (Amazon SQS)
キューを作成します。セキュリティチームのメール配信リストをキューに登録します。
E. 重大度の高い GuardDuty の検出結果に対して Amazon EventBridge (Amazon CloudWatch Events)
ルールを作成します。トピックにメッセージを公開するようにルールを設定します。
F. 重大度の高い Security Hub の検出結果に対して Amazon EventBridge (Amazon CloudWatch Events)
ルールを作成します。メッセージをキューに公開するようにルールを設定します。
Answer: B,C,E

QUESTION NO: 3
セキュリティエンジニアは、会社の Amazon EC2
インスタンスが暗号通貨のマイニングに使用されているかどうかを判断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、暗号通貨関連のアクティビティの通知を Amazon Simple Notification Service (Amazon SNS)
トピックに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しょうか?
A. Guard カスタムポリシーを使用して AWS Config カスタムルールを作成します。EC2
インスタンスが暗号通貨関連のアクティビティに関連付けられた DNS
ドメイン名をクエリしたときにそれを検出するように AWS Config
ルールを設定します。SNS トピックへのアラートを開始するように AWS Config
を設定します。
B. Amazon GuardDuty を有効にします。GuardDuty
が暗号通貨関連のアクティビティに関連する検出結果を作成したときに SNS
トピックにアラートを送信する Amazon EventBridge ルールを作成します。
C. Amazon Inspector を有効にします。Amazon Inspector
が暗号通貨関連のアクティビティに関連する検出結果を作成したときに SNS
トピックにアラートを送信する Amazon EventBridge ルールを作成します。
D. VPC フローログを有効にします。フローログを Amazon S3
バケットに送信します。Amazon Athena でクエリを設定し、EC2
インスタンスが暗号通貨関連のアクティビティに関連付けられた DNS
ドメイン名をクエリしたときにそれを検出します。SNS
トピックへのアラートを開始するように Athena クエリを設定します。
Answer: B
Explanation:
Enable Amazon GuardDuty:
GuardDuty is a threat detection service that natively supports detecting cryptocurrency mining activity on Amazon EC2 instances.
Enable GuardDuty for the account and all AWS Regions to ensure comprehensive coverage.
Monitor GuardDuty Findings:
GuardDuty generates findings for activities associated with cryptocurrency mining (e.g., unauthorized mining, DNS queries to known mining domains).
Create an EventBridge Rule:
Define an EventBridge rule that triggers on specific GuardDuty findings related to

cryptocurrency activity.
Configure the rule to send notifications to an Amazon SNS topic.
Example Rule:
{
"Source":
["aws.guardduty"],
"DetailType":
["GuardDuty Finding"],
"Detail": {
"type":
["CryptoCurrency:EC2/BitcoinTool.B"]
}
}
Advantages of GuardDuty:
Automated Threat Detection: Requires no additional setup or custom rules.
Near-Real-Time Alerts: Delivers findings and notifications with minimal delay.
Amazon GuardDuty Documentation
Creating EventBridge Rules for GuardDuty Findings

QUESTION NO: 4
Web
アプリケーションを使用すると、ユーザーはログインしてメンバーシップの有効性を確認し、Amazon S3
バケットに保存されている成果物を参照できます。ユーザーがオブジェクトをダウンロードしようとすると、アプリケーションはオブジェクトへのアクセス許可を確認し、example com などのカスタム
ドメイン名からユーザーがオブジェクトをダウンロードできるようにする必要があります。セキュリティ エンジニアがこの機能を実行する最も安全な方法は何ですか?
A. バケット ACL
を使用してオブジェクトへの読み取り専用アクセスを設定します。設定された時間が経過したらアクセスを削除します。
B. ユーザーに S3 バケットへの読み取りアクセス権を付与する IAM
ポリシーを実装します。
C. S3 署名済み URL を作成し、アプリケーションを通じてユーザーに S3 署名済み URL を提供します。
D. Amazon CloudFront 署名付き URL を作成します。アプリケーションを通じてユーザーに CloudFront 署名付き URL を提供します。
Answer: D
Explanation:
For this scenario you would need to set up static website hosting because a custom domain name is listed as a requirement. "Amazon S3 website endpoints do not support HTTPS or access points. If you want to use HTTPS, you can use Amazon CloudFront to serve a static website hosted on Amazon S3." This is not secure.
https://docs.aws.amazon.com/AmazonS3/latest/userguide/website-hosting-custom-domain-walkthrough.html CloudFront signed URLs allow much more fine-grained control as well as

HTTPS access with custom domain names:https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-signed-urls.html

QUESTION NO: 5
Amazon CloudFront で SSL 証明書を使用する場合に有効な設定は次のどれですか? (3 つ選択)
A. デフォルトの AWS Certificate Manager 証明書
B. AWS KMS に保存されたカスタム SSL 証明書
C. デフォルトの CloudFront 証明書
D. AWS Certificate Manager に保存されているカスタム SSL 証明書
E. AWS Secrets Manager に保存されているデフォルトの SSL 証明書
F. AWS IAM に保存されたカスタム SSL 証明書
Answer: A,B,C
Explanation:
The key length for an RSA certificate that you use with CloudFront is 2048 bits, even though ACM supports larger keys. If you use an imported certificate with CloudFront, your key length must be 1024 or 2048 bits and cannot exceed 2048 bits. You must import the certificate in the US East (N. Virginia) Region. You must have permission to use and importthe SSL/TLS certificate
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cnames-and-https-requirements.html

QUESTION NO: 6
セキュリティエンジニアは、既存の証跡の AWS CloudTrail ログファイルプレフィックスを更新するように求められています。CloudTrail コンソールで変更を保存しようとすると、セキュリティエンジニアは次のエラーメッセージを受け取ります:
「バケットポリシーに問題があります。」セキュリティエンジニアが変更を保存できるようにするにはどうすればよいでしょうか?
A.
更新されたログファイルプレフィックスを使用して新しい証跡を作成し、元の証跡を削除します。Amazon S3 コンソールで既存のバケットポリシーを新しいログファイルプレフィックスで更新し、CloudTrail コンソールでログファイルプレフィックスを更新します。
B. Amazon S3 コンソールで既存のバケットポリシーを更新して、セキュリティエンジニアのプリンシパルが PutBucketPolicy を実行できるようにし、CloudTrail コンソールでログファイルのプレフィックスを更新します。
C. Amazon S3 コンソールで既存のバケットポリシーを新しいログファイルプレフィックスで更新し、CloudTrail コンソールでログファイルプレフィックスを更新します。
D. Amazon S3 コンソールで既存のバケットポリシーを更新して、セキュリティエンジニアのプリンシパル

が GetBucketPolicy を実行できるようにし、CloudTrail
コンソールでログファイルのプレフィックスを更新します。

Answer: C

Explanation:

The correct answer is C. Update the existing bucket policy in the Amazon S3 console with the new log file prefix, and then update the log file prefix in the CloudTrail console.

According to the AWS documentation1, a bucket policy is a resource-based policy that you can use to grant access permissions to your Amazon S3 bucket and the objects in it. Only the bucket owner can associate a policy with a bucket. The permissions attached to the bucket apply to all of the objects in the bucket that are owned by the bucket owner.

When you create a trail in CloudTrail, you can specify an existing S3 bucket or create a new one to store your log files. CloudTrail automatically creates a bucket policy for your S3 bucket that grants CloudTrail write-only access to deliver log files to your bucket. The bucket policy also grants read-only access to AWS services that you can use to view and analyze your log data, such as Amazon Athena, Amazon CloudWatch Logs, and Amazon QuickSight.

If you want to update the log file prefix for an existing trail, you must also update the existing bucket policy in the S3 console with the new log file prefix. The log file prefix is part of the resource ARN that identifies the objects in your bucket that CloudTrail canaccess. If you don't update the bucket policy with the new log file prefix, CloudTrail will not be able to deliver log files to your bucket, and you will receive an error message when you try to save the change in the CloudTrail console.

The other options are incorrect because:

A . Creating a new trail with the updated log file prefix, and then deleting the original trail is not necessary and may cause data loss or inconsistency. You can simply update the existing trail and its associated bucket policy with the new log file prefix.

B . Updating the existing bucket policy in the S3 console to allow the Security Engineer's Principal to perform PutBucketPolicy is not relevant to this issue. The PutBucketPolicy action allows you to create or replace a policy on a bucket, but it does not affect CloudTrail's ability to deliver log files to your bucket. You still need to update the existing bucket policy with the new log file prefix.

D . Updating the existing bucket policy in the S3 console to allow the Security Engineer's Principal to perform GetBucketPolicy is not relevant to this issue. The GetBucketPolicy action allows you to retrieve a policy on a bucket, but it does not affect CloudTrail's ability to deliver log files to your bucket. You still need to update the existing bucket policy with the new log file prefix.

References:

1:Using bucket policies - Amazon Simple Storage Service

QUESTION NO: 7

ある会社のアプリケーション チームは、内部アプリケーションを、単一の IAM
リージョン内の Amazon EC2 インスタンス、IAM Lambda 関数、および Amazon S3
バケットで構成される新しい IAM
アーキテクチャに置き換えたいと考えています。アーキテクチャのレビュー後、セキュリティ チームは、アプリケーション ネットワーク トラフィックがいかなる時点でもパブリック インターネットを通過できないようにすることを義務付けました。セキュリティ

チームは、インターネット ゲートウェイ、NAT
ゲートウェイ、および出力専用ゲートウェイの作成を制限するために、会社の組織の IAM 組織に SCP をすでに配置しています。
これらの要件を満たすために、アプリケーション
チームはどの組み合わせの手順を実行する必要がありますか? (3 つ選択してください。)
A. アプリケーションの VPC に対するフルアクセスポリシーを持つ S3 エンドポイントを作成します。
B. S3 バケットの S3 アクセス ポイントを作成します。ネットワーク オリジンを VPC に制限するポリシーを含めます。
C. Lambda 関数を起動します。ブロックパブリックアクセス構成を有効にします。
D. S3 エンドポイントを宛先とするポート 443 経由の送信ルールを持つセキュリティ グループを作成します。
セキュリティ グループを EC2 インスタンスに関連付けます。
E. ポート 443 経由の送信ルールと S3 アクセス ポイントの送信先を持つセキュリティ グループを作成します。セキュリティ グループを EC2 インスタンスに関連付けます。
F. VPC で Lambda 関数を起動します。
Answer: A,D,F

QUESTION NO: 8
セキュリティエンジニアは、企業が Amazon S3 バケットに保存するデータに対して、Write-Once-Read-Many (WORM) モデルを実装する必要があります。同社は、すべての S3 バケットに S3 標準ストレージ クラスを使用しています。セキュリティ エンジニアは、AWS アカウントの root ユーザーを含むどのユーザーもオブジェクトを上書きしたり削除したりできない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すか?
A. コンプライアンス モードで S3 オブジェクト ロックを有効にして新しい S3 バケットを作成します。オブジェクトを S3 バケットに配置します。
B. S3 Glacier Vault Lock を使用して、新しい S3 バケットに Vault Lock ポリシーをアタッチします。Vault ロック プロセスが完了するまで 24 時間待ちます。オブジェクトを S3 バケットに配置します。
C. ガバナンス モードで S3 オブジェクト ロックを有効にして新しい S3 バケットを作成します。オブジェクトを S3 バケットに配置します。
D. ガバナンス モードで S3 オブジェクト ロックを有効にして新しい S3 バケットを作成します。S3 バケットに法的ホールドを追加します。オブジェクトを S3 バケットに配置します。
Answer: A

QUESTION NO: 9
ある企業は、AWS Organizations 内の組織内に AWS アカウントを持っています。この企業は、組織内のすべてのアカウントのすべての Amazon EC2 インスタンスに企業ソフトウェア パッケージをインストールする必要があります。
中央アカウントは、EC2 インスタンスの基本 AMI を提供します。同社では、ソフトウェア インベントリとパッチ適用操作に AWS Systems Manager を使用しています。

セキュリティ エンジニアは、必要なソフトウェアがインストールされていない EC2 インスタンスを検出するソリューションを実装する必要があります。また、ソフトウェアが存在しない場合は、ソリューションによってソフトウェアが自動的にインストールされる必要があります。
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. 必要なソフトウェアが事前にインストールされた新しい AMI を提供します。AMI に必要なソフトウェアがあることを示すタグを AMI に適用します。インスタンスにタグ付けされた AMI がある場合にのみ新しい EC2 インスタンスを起動できるように SCP を構成します。既存のすべての EC2 インスタンスにタグを付けます。
B. Systems Manager Patch Manager でカスタム パッチ ベースラインを設定します。必要なソフトウェアのパッケージ名を承認済みパッケージ リストに追加します。新しいパッチ ベースラインをすべての EC2 インスタンスに関連付けます。ソフトウェア デプロイメントのメンテナンス ウィンドウを設定します。
C. AWS Config を一元的に有効にします。すべてのアカウントに対して ec2-managedinstance-applications-required AWS Config ルールを設定します。AWS Config イベントに反応する Amazon EventBridge ルールを作成します。Systems Manager Run Command を使用して必要なソフトウェアをインストールする AWS Lambda 関数を呼び出すように EventBridge ルールを設定します。
D. 必要なソフトウェア用の新しい Systems Manager Distributor パッケージを作成します。ダウンロード場所を指定します。異なるアカウント内のすべての EC2 インスタンスを選択します。Systems Manager Run Command を使用してソフトウェアをインストールします。
Answer: C
Explanation:
Utilizing AWS Config with a custom AWS Config rule (ec2-managedinstance-applications-required) enables detection of EC2 instances lacking the required software across all accounts in an organization. By creating an Amazon EventBridge rule that triggers on AWS Config events, and configuring it to invoke an AWS Lambda function, automated actions can be taken to ensure compliance. The Lambda function can leverage AWS Systems Manager Run Command to install the necessary software on non-compliant instances. This approach ensures continuous compliance and automated remediation, aligning with best practices for cloud security and management.

QUESTION NO: 10
ある企業が本番環境アプリケーションをホストするAWSアカウントを保有しています。Amazon GuardDutyがアカウントでImpact IAMUser/AnomalousBehaviorの検出を検知したというメール通知を受け取りました。セキュリティエンジニアは、このセキュリティインシデントに関する調査プレイブックを実行し、アプリケーションに影響を与えずに情報を収集・分析する必要があります。
これらの要件を最も迅速に満たすソリューションはどれでしょうか?
A.
読み取り専用認証情報を使用してAWSアカウントにログインします。GuardDutyの検出結果で、使用された1AM認証情報の詳細を確認します。1AMコンソールを使用して、1AMプリン

シパルにDenyAllポリシーを追加します。
B. 読み取り専用の認証情報を使用して AWS アカウントにログインします。GuardDuty の検出結果を確認して、どの API 呼び出しが検出結果を開始したかを判断します。Amazon Detective を使用してコンテキスト内の API 呼び出しを確認します。
C.
管理者の認証情報を使用してAWSアカウントにログインします。GuardDutyの検出結果で、使用された1AMの認証情報の詳細を確認します。1AMコンソールを使用して、DenyAllポリシーを
午前1時の校長。
D. 読み取り専用の認証情報を使用して AWS アカウントにログインします。GuardDuty の検出結果を確認して、どの API 呼び出しが検出結果を開始したかを判断します。AWS CloudTrail Insights と AWS CloudTrail Lake を使用して、コンテキスト内の API 呼び出しを確認します。
Answer: B

QUESTION NO: 11
ある企業では、個人識別情報（PLL）を処理するアプリケーションを運用しています。このアプリケーションは、Application Load Balancer（ALB）の背後にあるAmazon EC2インスタンス上で稼働しています。企業のセキュリティポリシーでは、PLLが平文で漏洩する可能性を回避するため、転送中のデータは常に暗号化することが義務付けられています。
セキュリティ
エンジニアは、これらの要件を満たすためにどのソリューションを使用できますか? (2つ選択)
A.
既存のALB上のクライアントからのSSLを終了します。ALBからEC2インスタンスへの接続にはHTTPSを使用します。
B. 既存の ALB をネットワーク ロード バランサー (NLB) に置き換えます。NLB で、クライアント接続を受信するための SSL リスナーと TCP パススルーを構成します。EC2 インスタンス上の NLB からの HTTPS トラフィックを終了します。
C.
既存のALBをネットワークロードバランサー（NLB）に置き換えます。NLBで、クライアント接続を受信するためのTCPパススルーを設定します。EC2インスタンスのNLBからのSSLを終了します。
D. クライアント接続を受信するために TCP パススルーを備えたネットワーク ロード バランサー (NLB) を構成します。既存の ALB で SSL を終了します。
E. クライアント接続を受信するために、TLS リスナーを使用してネットワーク ロード バランサー (NLB) を構成します。NLB が EC2 インスタンスに到達できるように、既存の ALB で TCP パススルーを構成します。EC2 インスタンス上の ALB からの SSL を終了します。
Answer: A,B

QUESTION NO: 12

ある企業は、Amazon Elastic Kubernetes Service (Amazon EKS)
クラスターへの認証されていないアクセスを検出する必要があります。既存の EKS
デプロイメントに追加の設定を必要としないソリューションが必要です。
最も少ない運用労力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. セキュリティベンダーの Amazon EKS アドオンをインストールします。
B. AWS Security Hub を有効にします。Kubernetes の検出結果を監視します。
C. Amazon EKS の Amazon CloudWatch Container Insights メトリクスを監視します。
D. Amazon GuardDuty を有効にします。EKS 監査ログモニタリングを使用します。
Answer: D

QUESTION NO: 13
ある企業は、Amazon EC2
インスタンスで機密データの処理を開始したいと考えています。同社は Amazon
CloudWatch Logs を使用して、EC2 インスタンスからのログ
ファイルを監視、保存、アクセスする予定です。
同社の開発者はトラブルシューティングに CloudWatch Logs
を使用しています。セキュリティ
エンジニアは、開発者が機密データを閲覧できないようにするソリューションを実装する必要があります。このソリューションは、今後アカウントに作成される新しいログ
グループに自動的に適用される必要があります。
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. CloudWatch Logs
アカウント全体のデータ保護ポリシーを作成します。ポリシーに適切なデータ識別子を指定します。開発者に logs:Unmask 1AM 権限がないことを確認します。
B. CloudWatch Logs データを Amazon S3 バケットにエクスポートします。S3 バケットで Amazon Macie を使用して自動検出を設定します。機密データのカスタム
データ識別子を作成します。開発者の CloudWatch Logs
へのアクセスを削除します。開発者に Amazon S3 にエクスポートされたログ
データを表示する権限を付与します。
C. CloudWatch Logs データを Amazon S3 バケットにエクスポートします。S3 バケットで Amazon Macie
を使用して自動検出を設定します。適切な管理データ識別子を指定します。開発者の CloudWatch Logs へのアクセスを削除します。開発者に、Amazon S3
にエクスポートされたログデータを表示する権限を付与します。
D. 各ロググループに対して CloudWatch Logs
データ保護ポリシーを作成します。ポリシーに適切なデータ識別子を指定します。開発者に logsiUnmask 1AM 権限がないことを確認します。
Answer: A
Explanation:
Create an Account-Wide Data Protection Policy:
Use AWS CloudWatch Logs account-level data protection policies to prevent sensitive data exposure.
Define the policy with appropriate AWS managed data identifiers or custom identifiers specific to the company's sensitive data.

Apply the policy across all log groups in the account, ensuring coverage for both existing and future log groups.
Restrict Developer Access to Unmasked Data:
Explicitly deny thelogs:UnmaskIAM permission to developers. This prevents developers from accessing unmasked sensitive data in log entries.
Automatic Policy Application:
Account-wide data protection policies automatically apply to new log groups created in the future, ensuring scalability and compliance without manual intervention.
Testing and Verification:
Test the policy with sample log entries containing sensitive data to ensure proper masking.
Verify that developers can troubleshoot logs without exposing sensitive information.
AWS CloudWatch Logs Data Protection Documentation
AWS Identity and Access Management Permissions for CloudWatch Logs

QUESTION NO: 14
企業は規制に準拠するために、TOG データ
アーカイブを数年間保持する必要があります。TOG
データは使用されなくなりましたが、保持する必要があります。これらの要件を満たす最も安全でコスト効率の高いソリューションは何ですか?
A. データをAmazon S3にアーカイブし、制限バケットポリシーを適用してs3 DeleteOotect APIを拒否します。
B. データをAmazon S3 Glacierにアーカイブし、Vault Lockポリシーを適用する
C. データを Amazon S3 にアーカイブし、2 番目の IAM リージョンの 2
番目のバケットに複製します。S3 標準 - 低頻度アクセス (S3 標準 - 1A
) ストレージクラスを選択し、制限付きバケットポリシーを適用して s3 DeleteObject API を拒否します。
D. ログデータを 16 T8 Amazon Elastic Block Store (Amazon EBS)
ボリュームに移行し、EBS ボリュームのスナップショットを作成します。
Answer: B
Explanation:
To securely and cost-effectively retain log data archives for several years, the company should do the following:
Archive the data to Amazon S3 Glacier and apply a Vault Lock policy. This allows the company to use a low-cost storage class that is designed for long-term archival of data that is rarely accessed. It also allows the company to enforce compliance controls on their S3 Glacier vault by locking a vault access policy that cannot be changed.

QUESTION NO: 15
ある会社が、us-east-1 リージョンで Amazon Elastic Block Store (Amazon EBS)
ボリュームを持つ Amazon EC2
インスタンスを起動しました。ボリュームは、会社のセキュリティチームが作成した AWS Key Management Service (AWS KMS)
カスタマー管理キーで暗号化されています。セキュリティチームは 1AM
キーポリシーを作成し、そのポリシーをキーに割り当てました。また、セキュリティチームは 1AM

インスタンスプロファイルを作成し、そのプロファイルをインスタンスに割り当てました。EC2
インスタンスは起動せず、保留状態からシャットダウン状態、終了状態へと遷移します。セキュリティエンジニアは、この問題のトラブルシューティングを行うために、どの組み合わせの手順を実行する必要がありますか? (2 つ選択してください)

A. KMS キーポリシーで、aws SourceIP
条件キーを使用してキーへのアクセスを禁止する拒否ステートメントが指定されていることを確認します。範囲に、EBS ボリュームに関連付けられている EC2 インスタンスの IP アドレスが含まれていることを確認します。

B.
EBSボリュームに関連付けられているKMSキーが対称キータイプに設定されていることを確認します。

C. EBSボリュームに関連付けられているKMSキーが有効状態であることを確認します。

D.
インスタンスプロファイルに関連付けられているEC2ロールに、EBSボリュームを持つEC2インスタンスを起動するための正しい1AMインスタンスポリシーがあることを確認します。

E.
EBSボリュームに関連付けられたキーの有効期限が切れておらず、ローテーションする必要があることを確認します。

Answer: C,D

Explanation:
To troubleshoot the issue of an EC2 instance failing to start and transitioning to a terminated state when it has an EBS volume encrypted with an AWS KMS customer managed key, a security engineer should take the following steps:
C . Verify that the KMS key that is associated with the EBS volume is in the Enabled state. If the key is not enabled, it will not function properly and could cause the EC2 instance to fail.
D . Verify that the EC2 role that is associated with the instance profile has the correct IAM instance policy to launch an EC2 instance with the EBS volume. If the instance does not have the necessary permissions, it may not be able to mount the volume and could cause the instance to fail.
Therefore, options C and D are the correct answers.
Reference:
[1] "Amazon EBS encryption uses AWS KMS keys when creating encrypted volumes ...".

QUESTION NO: 16
ある会社では、AWS Key Management Service (AWS KMS)
を使用しています。暗号化された Amazon Elastic Block Store (Amazon EBS) ボリュームを Amazon EC2
インスタンスに接続しようとしましたが、接続に失敗しました。会社は、キーのキーマテリアルが削除されたために、顧客管理キーが使用できなくなっていることを発見しました。会社には、EBS ボリュームにあるデータが必要です。
セキュリティ エンジニアは、EBS ボリュームの暗号化されたデータ
キーを復号化するソリューションを推奨する必要があります。また、ソリューションではボリュームを EC2 インスタンスにアタッチ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. 新しいキーマテリアルをキーにインポートします。EBS ボリュームを接続します。
B. キーマテリアルを削除する前に作成されたスナップショットから EBS ボリュームを復元します。
C. キーに最初にインポートされたものと同じキー マテリアルを再インポートします。EBS ボリュームをアタッチします。
D. 新しいキーを作成します。新しいキーマテリアルをインポートします。EBS ボリュームを接続します。
Answer: B
Explanation:
Understanding the Key Material Deletion:
Once the key material for a customer managed KMS key is deleted, the key becomes permanently unusable.
Restoring from a Snapshot (Option B):
If the EBS volume was previously backed up with a snapshot, you can create a new volume from the snapshot.
This new volume will use a different key for encryption, enabling access to the data.
Other Options Are Invalid:
Reimporting key material (Option C) or importing new key material (Options A and D) does not restore the ability to decrypt data encrypted with the original key material.
Best Practices:
Always ensure snapshots are taken and stored securely to protect against key loss.
Restoring EBS Volumes from Snapshots
KMS Key Management Best Practices

QUESTION NO: 17
ある企業は、AWS アカウント内のリソースを監視するために AWS CloudTrail と Amazon CloudWatch を使用しています。
同社の開発者は過去 3 か月間、アカウントで 1AM ロールを使用してきました。
セキュリティ エンジニアは、ロールに添付された顧客管理の 1AM ポリシーを調整して、ロールが最小限の権限アクセスを提供するようにする必要があります。
最も少ない労力でこの要件を満たすソリューションはどれでしょうか?
A. ロールに AWS 1AM Access Analyzer ポリシー生成を実装します。
B. ロールに AWS 1AM Access Analyzer ポリシー検証を実装します。
C. CloudWatch ログを検索して、ロールが呼び出したアクションを特定し、権限を評価します。
D. AWS Trusted Advisor を使用して、ロールに割り当てられたポリシーを AWS のベストプラクティスと比較します。
Answer: A

QUESTION NO: 18
ある会社には、IAM 組織内に 2 つの IAM アカウントがあります。アカウント 1 では、サービスにリンクされたロールを使用して Amazon EC2 Auto Scaling が起動されます。アカウント 2 では、Amazon EBS ボリュームが IAM KMS キーで暗号化されています。セキュリティエンジニアは、サービスにリンクされたロールが

これらの暗号化されたボリュームを使用してインスタンスを起動できることを確認する必要があります。セキュリティエンジニアは、両方のアカウントでどの組み合わせの手順を実行する必要がありますか? (2 つ選択してください。)

A. キーポリシーを使用して、アカウント 1 がアカウント 2 の KMS キーにアクセスできるようにします。

B. Account-1 のサービスにリンクされたロールに、CreateGrant アクションを許可する IAM ポリシーをアタッチします。

DescnbeKey、Encrypt、GenerateDataKey、Decrypt、および ReEncrypt

C. CreateGrant、DescnbeKey Encrypt、GenerateDataKey Decrypt、および ReEncrypt アクションを使用して、サービスにリンクされたロールの KMS 付与を作成します。

D. KMS アクションを使用して EC2 インスタンスにアタッチされたロールに IAM ポリシーをアタッチし、KMS キーポリシーで Account-1 を許可します。

E. EC2 インスタンスを起動しているユーザーに IAM ポリシーをアタッチし、ユーザーが Account-2 の KMS キーポリシーにアクセスできるようにします。

Answer: C,D

Explanation:

because these are the steps that can ensure that the service-linked role can launch instances with encrypted volumes. A service-linked role is a type of IAM role that is linked to an AWS service and allows the service to perform actions on your behalf. A KMS grant is a mechanism that allows you to delegate permissions to use a customer master key (CMK) to a principal such as a service-linked role.A KMS grant specifies the actions that the principal can perform, such as encrypting and decrypting data. By creating a KMS grant for the service-linked role with the specified actions, you can allow the service-linked role to use the CMK in Account-2 to launch instances with encrypted volumes. By attaching an IAM policy to the role attached to the EC2 instances with KMS actions and then allowing Account-1 in the KMS key policy, you can also enable cross-account access to the CMK and allow the EC2 instances to use the encrypted volumes. The other options are either incorrect or unnecessary for meeting the requirement.

QUESTION NO: 19

ある企業では最近セキュリティ監査を実施し、監査人が複数の潜在的な脅威を特定しました。これらの潜在的な脅威は、DNS アクセスのピーク、異常なインスタンス トラフィック、異常なネットワーク インターフェイス トラフィック、異常な Amazon S3 API 呼び出しなどの使用パターンの変化を引き起こす可能性があります。脅威はさまざまなソースから発生する可能性があり、いつでも発生する可能性があります。企業は、システムを継続的に監視し、これらすべての侵入する脅威をほぼリアルタイムで特定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. AWS CloudTrail ログ、VPC フロー ログ、および DNS ログを有効にします。Amazon CloudWatch Logs を使用して、これらのログを一元的なアカウントから管理します。

B. AWS CloudTrail ログ、VPC フロー ログ、および DNS ログを有効にします。Amazon Macie を使用して、一元化されたアカウントからこれらのログを監視します。

C. 一元化されたアカウントから Amazon GuardDuty を有効にします。GuardDuty を使用して、AWS CloudTrail ログ、VPC フロー ログ、DNS ログを管理します。

D. 一元化されたアカウントから Amazon Inspector を有効にします。Amazon Inspector を使用して、AWS CloudTrail ログ、VPC フロー ログ、DNS ログを管理します。

Answer: C

Explanation:

Q: Which data sources does GuardDuty analyze? GuardDuty analyzes CloudTrail management event logs, CloudTrail S3 data event logs, VPC Flow Logs, DNS query logs, and Amazon EKS audit logs. GuardDuty can also scan EBS volume data for possible malware when GuardDuty Malware Protection is enabled and identifies suspicious behavior indicative of malicious software in EC2 instance or container workloads. The service is optimized to consume large data volumes for near real-time processing of security detections. GuardDuty gives you access to built-in detection techniques developed and optimized for the cloud, which are maintained and continuously improved upon by GuardDuty engineering.

QUESTION NO: 20

ある会社が、複数のAmazon EC2インスタンスでホストされる、非常に回復力の高いアプリケーションを開発しています。アプリケーションは、機密性の高いユーザーデータをAmazon RDSテーブルに保存します。アプリケーションは

* アプリケーションの災害復旧計画に別の IAM リージョンへの移行を含めます。
* 暗号化キー管理イベントの完全な監査証跡を提供する
* 会社の管理者のみがキーを管理できるようにします。
* アプリケーション層暗号化を使用して保存データを保護

セキュリティ

エンジニアが暗号化キー管理のオプションを評価しています。このような状況で、セキュリティ エンジニアが暗号化キー管理に IAM KMS ではなく IAM CloudHSM を選択すべきなのはなぜでしょうか。

A. CloudHSM によって生成されるキー管理イベント ログは、IAM KMS よりもはるかに広範囲にわたります。

B. CloudHSM では、会社のサポートスタッフのみが暗号化キーを管理できますが、IAM KMS では IAM スタッフがキーを管理できます。

C. CloudHSM によって生成された暗号文は、IAM KMS によって生成された暗号文よりも、ブルートフォース復号化攻撃に対してより強力な保護を提供します。

D. CloudHSMはキーを別のリージョンにコピーする機能を提供しますが、IAM KMSは

Answer: B

Explanation:

CloudHSM allows full control of your keys such including Symmetric (AES), Asymmetric (RSA), Sha-256, SHA 512, Hash Based, Digital Signatures (RSA). On the other hand, AWS Key Management Service is a multi-tenant key storage that is owned and managed byAWS1.

References: 1: What are the differences between AWS Cloud HSM and KMS?

QUESTION NO: 21

システムエンジニアは、アプリケーションチームが QA ワークフローを通じて提供したいくつかのカスタムビルドイメージからコンテナをデプロイ

しました。システムエンジニアは、ターゲットプラットフォームとして Fargate 起動タイプを指定した Amazon Elastic Container Service (Amazon ECS) を使用しました。システムエンジニアは、すべてのコンテナから既存の Amazon CloudWatch ロググループにログを収集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?

A. LogConfiguration プロパティで awslogs-group と awslogs-region のパラメータを指定して、awslogs ログ ドライバーをオンにします。

B. コンテナインスタンスにCloudWatchエージェントをダウンロードして設定する

C. Fluent Bit と FluentO を DaemonSet として設定し、Amazon CloudWatch Logs にログを送信します。

D. togs CreateLogGroupアクションを含む1AMポリシーを構成し、コンテナインスタンスにポリシーを割り当てます。

Answer: A

Explanation:

The AWS documentation states that you can use the awslogs log driver to send log information to CloudWatch Logs. To use this method, you specify the parameters for awslogs-group and awslogs-region in the LogConfiguration property of the container definition. This method is the easiest way to send logs to CloudWatch Logs.

References: : Amazon Elastic Container Service Developer Guide

QUESTION NO: 22

ある会社では、外部の ID プロバイダーを使用して、さまざまな IAM アカウントへのフェデレーションを許可しています。会社のセキュリティ エンジニアは、1 週間前に本番環境の Amazon EC2 インスタンスを終了したフェデレーション ユーザーを特定する必要があります。

セキュリティ エンジニアがフェデレーション ユーザーを識別する最も速い方法は何ですか?

A. Amazon S3 バケット内の IAM CloudTrail イベント履歴ログを確認し、TerminateInstances イベントを探して、ロールセッション名からフェデレーションユーザーを識別します。

B. TerminateInstances イベントの IAM CloudTrail イベント履歴をフィルタリングし、引き受けた IAM ロールを特定します。CloudTrail の AssumeRoleWithSAML イベント呼び出しを確認して、対応するユーザー名を特定します。

C. IAM CloudTrail ログで TerminateInstances イベントを検索し、イベントの時間をメモします。すべてのフェデレーション ロールの IAM アクセス アドバイザー タブを確認します。最終アクセス時間は、インスタンスが終了した時間と一致する必要があります。

D. Amazon Athena を使用して、Amazon S3 バケットに保存されている IAM CloudTrail ログに対して SQL クエリを実行し、TerminateInstances イベントでフィルタリングします。対応するロールを識別し、別のクエリを実行して、ユーザー名の AssumeRoleWithWebIdentity イベントをフィルタリングします。

Answer: B

Explanation:
The fastest way to identify the federated user who terminated a production Amazon EC2 instance is to filter the IAM CloudTrail event history for the TerminateInstances event and identify the assumed IAM role. Then, review the AssumeRoleWithSAML event call in CloudTrail to identify the corresponding username. This method does not require any additional tools or queries, and it directly links the IAM role with the federated user.
Option A is incorrect because the role session name may not be the same as the federated user name, and it may not be unique or descriptive enough to identify the user.
Option C is incorrect because the IAM Access Advisor tab only shows when a role was last accessed, not by whom or for what purpose. It also does not show the specific time of access, only the date.
Option D is incorrect because using Amazon Athena to run SQL queries on the IAM CloudTrail logs is not the fastest way to identify the federated user, as it requires creating a table schema and running multiple queries. It also assumes that the federation is done using web identity providers, not SAML providers, as indicated by the AssumeRoleWithWebIdentity event. References:
AWS Identity and Access Management
Logging AWS STS API Calls with AWS CloudTrail
[Using Amazon Athena to Query S3 Data for CloudTrail Analysis]

QUESTION NO: 23
ある企業は、Amazon EC2 インスタンスで公開 Web サイトをホストしています。HTTPS トラフィックは Web サイトにアクセスできる必要があります。同社は Web サーバーの管理に SSH を使用しています。
Web サイトはサブネット 10.0.1.0/24 上にあります。管理サブネットは 192.168.100.0/24 です。セキュリティ エンジニアは、EC2 インスタンスのセキュリティ グループを作成する必要があります。
最も安全な方法でこれらの要件を満たすために、セキュリティ エンジニアはどの手順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. ソース 0.0.0.0/0 からのポート 22 を許可します。
B. ソース 0.0.0.0/0 からのポート 443 を許可します。
C. 192.168.100.0/24 からのポート 22 を許可します。
D. 10.0.1.0/24 からのポート 22 を許可します。
E. 10.0.1.0/24 からのポート 443 を許可します。
Answer: B,C
Explanation:
The correct answer is B and C.
B . Allow port 443 from source 0.0.0.0/0.
This is correct because port 443 is used for HTTPS traffic, which must be able to access the website from any source IP address.
C . Allow port 22 from 192.168.100.0/24.
This is correct because port 22 is used for SSH, which is the management protocol for the web server. The management subnet is 192.168.100.0/24, so only this subnet should be allowed to access port 22.
A . Allow port 22 from source 0.0.0.0/0.

This is incorrect because it would allow anyone to access port 22, which is a security risk. SSH should be restricted to the management subnet only.
D . Allow port 22 from 10.0.1.0/24.
This is incorrect because it would allow the website subnet to access port 22, which is unnecessary and a security risk. SSH should be restricted to the management subnet only.
E . Allow port 443 from 10.0.1.0/24.
This is incorrect because it would limit the HTTPS traffic to the website subnet only, which defeats the purpose of having a public website.

QUESTION NO: 24
ある会社のエンジニアリング チームは、ユーザーに対して AWS Key Management Service (AWS KMS)
カスタマー管理キー付与を作成する新しいアプリケーションを開発しています。付与の作成後すぐに、ユーザーは KMS キーを使用して 512
バイトのペイロードを暗号化できる必要があります。負荷テスト中、ユーザーが最初にキーを使用して暗号化しようとすると、AccessDeniedException エラーがときどき発生します。これらの AccessDeniedException
エラーを排除するために、会社のセキュリティ専門家はどのソリューションを推奨すべきでしょうか?
A. 通話が成功するまで 2
分ごとに再試行メカニズムを実装するようにユーザーに指示します。
B. エンジニアリング
チームに、ユーザーからランダムな許可トークンを取得し、その許可トークンを操作に渡して CreateGrant
操作を呼び出すように指示します。ユーザーには、暗号化の呼び出しでその許可トークンを使用するように指示します。
C. CreateGrant 操作を呼び出すときに、エンジニアリング
チームに許可のランダムな名前を作成するように指示します。その名前をユーザーに返し、暗号化の呼び出しで許可トークンとしてその名前を提供するように指示します。
D. CreateGrant 応答で返された許可トークンをユーザーに渡すようにエンジニアリング
チームに指示します。ユーザーには、暗号化の呼び出しでその許可トークンを使用するように指示します。
Answer: D
Explanation:
Understand the Issue:
KMS grants are created using theCreateGrantoperation.
The grant might not propagate immediately for use, leading toAccessDeniedExceptionerrors.
Use Grant Tokens for Immediate Access:
When a grant is created, AWS KMS provides a grant token in the response.
This grant token can be used immediately, even before the grant is fully propagated.
Implement Solution:
Pass the grant token returned byCreateGrantto the users.
Ensure users include the grant token in their requests to encrypt data.
AWS KMS Grant Tokens Documentation
Troubleshooting KMS AccessDenied Errors

QUESTION NO: 25
AWS Organizations を使用する企業は、AWS 1AM Identity Center (AWS Single Sign-On) を使用して AWS
アカウントへのアクセスを管理しています。セキュリティエンジニアは、1AM Identity Center
でカスタム権限セットを作成しています。企業は、権限セットを複数のアカウントで使用します。権限セットには、AWS
管理ポリシーと顧客管理ポリシーが添付されています。セキュリティエンジニアは完全な管理権限を持ち、管理アカウントで操作しています。
セキュリティ エンジニアが、複数のアカウントにアクセスできる 1AM Identity Center
ユーザーに権限セットを割り当てようとすると、割り当ては失敗します。
この障害を解決するためにセキュリティ エンジニアは何をすべきでしょうか?
A.
権限セットが割り当てられているすべてのアカウントに顧客管理ポリシーを作成します。各アカウントで顧客管理ポリシーに同じ名前と同じ権限を付与します。
B. 権限セットから AWS
管理ポリシーまたはカスタマー管理ポリシーのいずれかを削除します。
削除されたポリシーを含む 2
番目の権限セットを作成します。権限セットをユーザーに個別に適用します。
C. AWS
管理ポリシーとカスタマー管理ポリシーのロジックを評価します。デプロイ前に、アクセス許可セット内のポリシーの競合を解決します。
D.
ユーザーに新しい権限セットを追加しないでください。代わりに、ユーザーの既存の権限セットを編集して、AWS 管理ポリシーとカスタマー管理ポリシーを含めます。
Answer: A
Explanation:
https://docs.aws.amazon.com/singlesignon/latest/userguide/howtocmp.html
"Before you assign your permission set with IAM policies, you must prepare your member account. The name of an IAM policy in your member account must be a case-sensitive match to name of the policy in your management account. IAM Identity Center fails to assign the permission set if the policy doesn't exist in your member account."

QUESTION NO: 26
コンサルタント会社が、ある企業の本番環境AWSアカウントのセキュリティ監査を実施する必要があります。複数のコンサルタントがアカウントにアクセスする必要があります。コンサルタント会社は既に独自のAWSアカウントを保有しています。
同社は、本番環境アカウントへのすべてのアクセスに多要素認証（MFA）を義務付けています。また、長期間有効な認証情報の使用も禁止しています。
これらの要件を満たすアクセスをコンサルタント機関に提供するソリューションはどれですか?
A.
午前1時グループを作成します。コンサルタントごとに午前1時ユーザーを作成します。各ユーザーをグループに追加します。コンサルタントごとにMFAを有効にします。

B. 会社の本番環境アカウントで Amazon Cognito を設定し、コンサルタント会社の ID プロバイダー (IdP) に対して認証します。Cognito ユーザープールに MFA を追加します。
C.
コンサルタント会社のAWSアカウントに1AMロールを作成します。MFAを要求する信頼ポリシーを定義します。
信頼ポリシーで、会社の本番環境アカウントをプリンシパルとして指定します。信頼ポリシーをロールにアタッチします。
D. 会社の本番環境アカウントに 1AM ロールを作成します。MFA を要求する信頼ポリシーを定義します。信頼ポリシーでは、コンサルタント会社の AWS アカウントをプリンシパルとして指定します。信頼ポリシーをロールにアタッチします。
Answer: D

QUESTION NO: 27
ある企業がコラボレーションアプリケーションを使用しています。セキュリティエンジニアは、us-west-2リージョンのAWS Security Hubからアプリケーションに自動アラートを設定する必要があります。セキュリティエンジニアは、Security Hubが新しい検出結果を受信するたびに、アプリケーション内のチャネルでアラートを受信したいと考えています。
セキュリティエンジニアは、メッセージをアプリケーションに必要な形式に変換するAWS Lambda関数を作成します。このLambda関数は、メッセージをアプリケーションのAPIに送信します。セキュリティエンジニアは、Lambda関数をターゲットとして指定するAmazon EventBridgeルールを設定します。
EventBridge ルールが実装されると、チャネルは Security Hub から継続的にアラートを受信するようになります。
アラートの多くはAmazon Inspectorのアラートであり、対応は必要ありません。セキュリティエンジニアはAmazon Inspectorのアラートを停止したいと考えています。
最も少ない運用労力でこの要件を満たすソリューションはどれでしょうか?
A. アプリケーションにメッセージを送信するためのAmazon Simple Notification Service (Amazon SNS)トピックを作成します。トピックサブスクリプションにフィルターポリシーを設定し、製品名を含むメッセージを拒否します。
/aws/inspector 文字列。
B. Lambda 関数コードを更新して、Amazon Inspector からのイベントのパターン一致を見つけ、検出結果を抑制します。
C. Amazon Inspector を除くすべてのサービスからの検出結果を EventBridge イベントバスに自動的に送信する Security Hub カスタム アクションを作成します。
D. EventBridge ルールのイベント パターン内の ProductArn 属性の値を "anything- but": ["arn:aws:securityhub:us-west-2::product/aws/inspector"] に変更します。
Answer: D
Comprehensive and Detailed Explanation From Exact Extract:
The most operationally efficient solution is to modify the EventBridge rule's event pattern using the anything-but operator on the ProductArn attribute. This effectively filters out all

findings generated by Amazon Inspector, allowing all other findings to trigger alerts as intended-without modifying Lambda code or managing additional services like SNS. This technique aligns with Logging and Monitoring best practices to reduce noise from security alerts and improve response efficiency by filtering at the event rule level.

QUESTION NO: 28
企業は、AWS CloudFormation
テンプレートからリソースをデプロイするには、セキュリティのベストプラクティスに従う必要があります。CloudFormation
テンプレートは、機密性の高いデータベース認証情報を構成できる必要があります。
同社はすでに AWS Key Management Service (AWS KMS) と AWS Secrets Manager を使用しています。
どのソリューションが要件を満たすでしょうか?
A. CloudFormation テンプレートの動的参照を使用して、Secrets Manager のデータベース認証情報を参照します。
B. CloudFormation
テンプレートのパラメータを使用してデータベース認証情報を参照します。AWS KMS を使用して CloudFormation テンプレートを暗号化します。
C. CloudFormation テンプレートの SecureString パラメーターを使用して、Secrets Manager のデータベース認証情報を参照します。
D. CloudFormation テンプレートの SecureString パラメータを使用して、AWS KMS の暗号化された値を参照します。
Answer: A
Explanation:
Option A: This option meets the requirements of following security best practices and configuring sensitive database credentials in the CloudFormation template. A dynamic reference is a way to specify external values that are stored and managed in other services,such as Secrets Manager, in the stack templates1. When using a dynamic reference, CloudFormation retrieves the value of the specified reference when necessary during stack and change set operations1. Dynamic references can be used for certain resources that support them, such as AWS::RDS::DBInstance1. By using a dynamic reference to reference the database credentials in Secrets Manager, the company can leverage the existing integration between these services and avoid hardcoding the secret information in the template. Secrets Manager is a service that helps you protect secrets needed to access your applications, services, and IT resources2. Secrets Manager enables you to rotate, manage,and retrieve database credentials, API keys, and other secrets throughout theirlifecycle2.

QUESTION NO: 29
セキュリティエンジニアは、パブリックサブネット上の Amazon EC2
インスタンスが、既知の悪意のあるボットである特定の IP アドレスからの SFTP
ブルートフォース攻撃を受けているというアラートを受け取りました。セキュリティエンジニアは、悪意のあるボットをブロックするために何をすべきでしょうか?
A.
パブリックVPCセキュリティグループに拒否ルールを追加して、悪意のあるIPをブロックし

ます。
B. 悪意のあるIPをIAM WAFバックアドレスに追加する
C. Linux
iptablesまたはWindowsファイアウォールを設定して、悪意のあるIPからのトラフィックをブロックします。
D. Amazon Route
53のホストゾーンを変更し、悪意のあるIPのDNSシンクホールを作成します。
Answer: D
Explanation:
what the Security Engineer should do to block the malicious bot. SFTP is a protocol that allows secure file transfer over SSH. EC2 is a service that provides virtual servers in the cloud. A public subnet is a subnet that has a route to an internet gateway, which allows it to communicate with the internet. A brute force attack is a type of attack that tries to guess passwords or keys by trying many possible combinations. A malicious bot is a software program that performs automated tasks for malicious purposes. Route 53 is a service that provides DNS resolution and domain name registration. A DNS sinkhole is a technique that redirects malicious or unwanted traffic to a different destination, such as a black hole server or a honeypot. By modifying the hosted zone in Route 53 and creating a DNS sinkhole for the malicious IP, the Security Engineer can block the malicious bot from reaching the EC2 instance on the public subnet. The other options are either ineffective or inappropriate for blocking the malicious bot.

QUESTION NO: 30
セキュリティエンジニアは、VPCフローログと関連するIAMロールを設定し、すべてのVPCトラフィックをAmazon CloudWatch
Logsのロググループに記録するようにしました。10分待っても、ロググループにログは表示されませんでした。セキュリティエンジニアは、トラフィックがVPCに送信されていることを確認しました。
追加のデバッグを行った後、セキュリティ エンジニアは問題を VPC フロー
ログに関連付けられているロールに切り分けます。
ログが CloudWatch Logs に表示されない理由は何でしょうか?
A. ロールに logs:GetLogEvents 権限が付与されていません。
B. セキュリティ エンジニアには、ロールを引き受ける権限がありません。
C. プリンシパル vpc-flow-logs.amazonaws.com
には、ロールを引き受ける権限がありません。
D. ロールには、CloudWatch Logs ストリームにタグを付ける権限がありません。
Answer: C

QUESTION NO: 31
ある企業はセキュリティ体制を評価しています。同社は過去に、特定のホストとホストヘッダーの組み合わせで、同社のビジネスに影響を与える問題を確認していました。同社は、これらの問題を軽減するための最初のステップとして、AWS WAF ウェブ ACL
を設定しました。
企業は、問題のあるアクティビティを監視するために、AWS WAF ウェブ ACL
のログ分析ソリューションを作成する必要があります。同社は、すべての AWS WAF

ログを中央の場所で処理したいと考えています。企業は、特定のホストに基づいてリクエストをフィルタリングする機能を備えている必要があります。
セキュリティ エンジニアは、AWS WAF ウェブ ACL のアクセス
ログの有効化を開始します。
これらの要件を最大限の運用効率で満たすために、セキュリティ
エンジニアは次に何をすべきでしょうか?

A. アクセスログの保存先としてAmazon Redshiftを指定します。Amazon Athena Redshift コネクタをデプロイします。Athena を使用して Amazon Redshift からデータをクエリし、ホストごとにログをフィルタリングします。

B. アクセスログの保存先として Amazon CloudWatch を指定します。Amazon CloudWatch Logs Insights を使用して、ホストごとにログをフィルタリングするクエリを設計します。

C. アクセスログの保存先として Amazon CloudWatch を指定します。CloudWatch ログを Amazon S3 バケットにエクスポートします。Amazon Athena を使用してログをクエリし、ホストごとにログをフィルタリングします。

D. アクセスログの保存先として Amazon CloudWatch を指定します。Amazon Redshift Spectrum を使用してログをクエリし、ホストごとにログをフィルタリングします。

Answer: C

Explanation:

The correct answer is C. Specify Amazon CloudWatch as the destination for the access logs. Export the CloudWatch logs to an Amazon S3 bucket. Use Amazon Athena to query the logs and to filter the logs by host.

According to the AWS documentation1, AWS WAF offers logging for the traffic that your web ACLs analyze. The logs include information such as the time that AWS WAF received the request from your protected AWS resource, detailed information about the request, and the action setting for the rule that the request matched. You can send yourlogs to an Amazon CloudWatch Logs log group, an Amazon Simple Storage Service (Amazon S3) bucket, or an Amazon Kinesis Data Firehose.

To create a log analysis solution for the AWS WAF web ACLs, you can use Amazon Athena, which is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL2. You can use Athena to query and filter the AWS WAF logs by host or any other criteria. Athena is serverless, so there is no infrastructure to manage, and you pay only for the queries that you run.

To use Athena with AWS WAF logs, you need to export the CloudWatch logs to an S3 bucket.You can do this by creating a subscription filter that sends your log events to a Kinesis Data Firehose delivery stream, which then delivers the data to an S3 bucket3.Alternatively, you can use AWS DMS to migrate your CloudWatch logs to S34.

After you have exported your CloudWatch logs to S3, you can create a table in Athena that points to your S3 bucket and use the AWS service log format that matches your log schema5. For example, if you are using format for your AWS WAF logs, you can use the AWSSerDe serde. Then you can run SQL queries on your Athena table and filter the results by host or any other field in your log data.

Therefore, this solution meets the requirements of creating a log analysis solution for the AWS WAF web ACLs with the most operational efficiency. This solution does not require setting up any additional infrastructure or services, and it leverages the existing capabilities of CloudWatch, S3, and Athena.

The other options are incorrect because:
A . Specifying Amazon Redshift as the destination for the access logs is not possible, because AWS WAF does not support sending logs directly to Redshift. You would need to use an intermediate service such as Kinesis Data Firehose or AWS DMS to load the data from CloudWatch or S3 to Redshift.Deploying the Amazon Athena Redshift connector is not necessary, because you can query Redshift data directly from Athena without using a connector6. This solution would also incur additional costs and operational overhead of managing a Redshift cluster.
B . Specifying Amazon CloudWatch as the destination for the access logs is possible, but using Amazon CloudWatch Logs Insights to design a query to filter the logs by host is not efficient or scalable.CloudWatch Logs Insights is a feature that enables you to interactively search and analyze your log data in CloudWatch Logs7.However, CloudWatch Logs Insights has somelimitations, such as a maximum query duration of 20 minutes, a maximum of 20 log groups per query, and a maximum retention period of 24 months8. These limitations may affect your ability to perform complex and long-running analysis on your AWS WAF logs.
D . Specifying Amazon CloudWatch as the destination for the access logs is possible, but using Amazon Redshift Spectrum to query the logs and filter them by host is not efficient or cost-effective.Redshift Spectrum is a feature of Amazon Redshift that enables you to run queries against exabytes of data in S3 without loading or transforming any data9. However, Redshift Spectrum requires a Redshift cluster to process the queries, which adds additional costs and operational overhead.Redshift Spectrum also charges you based on the number ofbytes scanned by each query, which can be expensive if you have large volumes of log data10.
References:
1:Logging AWS WAF web ACL traffic - AmazonWeb Services2:What Is Amazon Athena? - Amazon Athena3:Streaming CloudWatch Logs Data to Amazon S3 - Amazon CloudWatch Logs4:Migrate data from CloudWatch Logs using AWS Database Migration Service - AWS Database Migration Service5:Querying AWS service logs - Amazon Athena6:Querying data from Amazon Redshift - Amazon Athena7:Analyzing log data with CloudWatch LogsInsights - Amazon CloudWatch Logs8:CloudWatch Logs Insights quotas - Amazon CloudWatch9:Querying external data using Amazon Redshift Spectrum - Amazon Redshift10:Amazon Redshift Spectrum pricing - Amazon Redshift

QUESTION NO: 32
ある企業には、IAM でホストされている一連の EC2 インスタンスがあります。EC2 インスタンスには、重要な情報を保存するために使用される EBS ボリュームがあります。EBS ボリュームの高可用性を確保するために、ビジネス継続性が求められています。どうすればこれを実現できるでしょうか。
A. EBSボリュームのライフサイクルポリシーを使用する
B. EBSスナップショットを使用する
C. EBSボリュームレプリケーションを使用する
D. EBSボリューム暗号化を使用する
Answer: B
Explanation:

Data stored in Amazon EBS volumes is redundantly stored in multiple physical locations as part of normal operation of those services and at no additional charge. However, Amazon EBS replication is stored within the same availability zone, not across multiple zones; therefore, it is highly recommended that you conduct regular snapshots to Amazon S3 for long-term data durability Option A is invalid because there is no lifecycle policy for EBS volumes Option C is invalid because there is no EBS volume replication Option D is invalid because EBS volume encryption will not ensure business continuity For information on security for Compute Resources, please visit the below URL:https://d1.awsstatic.com/whitepapers/Security/Security_Compute_Services_Whitepaper.pdf

QUESTION NO: 33
ある会社には小売店があり、顧客の領収書のスキャンコピーを Amazon S3 に保存するソリューションを設計しています。ファイルは PDF 形式で 100 KB ～ 5 MB になります。小売店ごとに固有の暗号化キーが必要です。オブジェクトごとに固有のキーで暗号化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. 各小売店専用の AWS Key Management Service (AWS KMS) カスタマー管理キーを作成します。S3 Put オペレーションを使用してオブジェクトを Amazon S3 にアップロードします。AWS KMS キー (SSE-KMS) を使用したサーバー側暗号化と、店舗のキーのキー ID を指定します。
B. 各小売店ごとに毎日新しい AWS Key Management Service (AWS KMS) カスタマー管理キーを作成します。KMS 暗号化操作を使用してオブジェクトを暗号化します。次に、オブジェクトを Amazon S3 にアップロードします。
C. 各小売店に対して毎日 AWS Key Management Service (AWS KMS) GenerateDataKey オペレーションを実行し、データキーとクライアント側の暗号化を使用してオブジェクトを暗号化します。次に、オブジェクトを Amazon S3 にアップロードします。
D. AWS Key Management Service (AWS KMS) ImportKeyMaterial オペレーションを使用して、小売店ごとに毎日新しいキーマテリアルを AWS KMS にインポートします。顧客管理キーと KMS Encrypt オペレーションを使用してオブジェクトを暗号化し、オブジェクトを Amazon S3 にアップロードします。
Answer: A
Explanation:
To meet the requirements of storing scanned copies of customer receipts on Amazon S3, where files will be between 100 KB and 5 MB in PDF format, each retail store must have a unique encryption key, and each object must be encrypted with a unique key, the most appropriate solution would be to create a dedicated AWS Key Management Service (AWS KMS) customer managed key for each retail store. Then, use the S3 Put operation to upload the objects to Amazon S3, specifying server-side encryption with AWS KMS keys (SSE-KMS) and the key ID of the store's key.
References: : Amazon S3 - Amazon Web Services : AWS Key Management Service - Amazon Web Services : Amazon S3 - Amazon Web Services : AWS Key Management Service - Amazon Web Services

QUESTION NO: 34
ある会社では、Amazon Elastic Kubernetes Service (Amazon EKS)
クラスターを使用して、Kubernetes
ベースのアプリケーションを実行しています。この会社では、Amazon GuardDuty
を使用してアプリケーションを保護しています。GuardDuty では EKS
保護が有効になっています。ただし、対応する GuardDuty 機能は、Kubernetes
ベースのアプリケーションを監視していません。
A. EKS クラスターをホストする VPC の VPC フローログを有効にします。
B. CloudWatchEventsFullAccess AWS 管理ポリシーを EKS クラスターに割り当てます。
C. AmazonGuardDutyFullAccess AWS 管理ポリシーが GuardDuty
サービスロールにアタッチされていることを確認します。
D. Amazon EKS でコントロールプレーンログを有効にします。ログが Amazon CloudWatch
に取り込まれることを確認します。
Answer: D
Explanation:
Comprehensive Detailed Explanation with all AWS References
To enable GuardDuty to monitor Kubernetes-based applications:
Enable Control Plane Logs:
GuardDuty uses control plane logs to detect malicious or unauthorized activity in Amazon EKS.
Enable EKS control plane logs (API, audit, authenticator) and ingest them into CloudWatch.
Reference:
Incorrect Options:
A:VPC flow logs are used for network traffic analysis, not specific to EKS protection.
B:CloudWatchEventsFullAccess is unrelated to EKS or GuardDuty functionality.
C:The GuardDuty service role already has required permissions when EKS Protection is enabled.

QUESTION NO: 35
ある会社が新しいアプリケーション スタックを設計しています。設計には、Amazon EC2
インスタンスでホストされる Web サーバーとバックエンド
サーバーが含まれています。また、設計には Amazon Aurora MySQL DB
クラスターも含まれています。
EC2 インスタンスは、起動テンプレートを使用する Auto Scaling グループです。Web
レイヤーとバックエンド レイヤーの EC2 インスタンスは、Amazon Elastic Block Store
(Amazon EBS)
ボリュームによってサポートされています。保存時に暗号化されるレイヤーはありません。
セキュリティ エンジニアが保存時の暗号化を実装する必要があります。
どの手順の組み合わせがこれらの要件を満たしますか? (2 つ選択してください。)
A. 暗号化を有効にするには、ターゲット AWS リージョンの EBS
デフォルト暗号化設定を変更します。Auto Scaling
グループインスタンスの更新を使用します。
B. ウェブレイヤーとバックエンドレイヤーの起動テンプレートを変更して、アタッチされた
EBS ボリュームに AWS Certificate Manager (ACM) 暗号化を追加します。Auto Scaling
グループインスタンスの更新を使用します。

C. 既存の DB クラスターのスナップショットから、新しい AWS Key Management Service (AWS KMS) 暗号化 DB クラスターを作成します。
D. 既存の DB クラスターに AWS Key Management Service (AWS KMS) 暗号化を適用します。
E. 既存の DB クラスターに AWS Certificate Manager (ACM) 暗号化を適用します。
Answer: A,C
Explanation:
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Overview.Encryption.html
https://aws.amazon.com/premiumsupport/knowledge-center/ebs-automatic-encryption/ To implement encryption at rest for both the EC2 instances and the Aurora DB cluster, the following steps are required:
For the EC2 instances, modify the EBS default encryption settings in the target AWS Region to enable encryption. This will ensure that any new EBS volumes created in that Region are encrypted by default using an AWS managed key. Alternatively, you can specify a customer managed key when creating new EBS volumes.For more information, see Amazon EBS encryption.
Use an Auto Scaling group instance refresh to replace the existing EC2 instances with new ones that have encrypted EBS volumes attached. An instance refresh is a feature that helps you update all instances in an Auto Scaling group in a rolling fashion without the need to manage the instance replacement process manually. For more information, see Replacing Auto Scaling instances based on an instance refresh.
For the Aurora DB cluster, create a new AWS Key Management Service (AWS KMS) encrypted DB cluster from a snapshot of the existing DB cluster. You can use either an AWS managed key or a customer managed key to encrypt the new DB cluster. You cannot enable or disable encryption for an existing DB cluster, so you have to create a new one from a snapshot.For more information, see Encrypting Amazon Aurora resources.
The other options are incorrect because they either do not enable encryption at rest for the resources (B, D), or they use the wrong service for encryption (E).
Verified References:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html
https://docs.aws.amazon.com/autoscaling/ec2/userguide/asg-instance-refresh.html
https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/Overview.Encryption.html