aws training and certification

AWS 認定セキュリティ – 専門知識
AWS Certified Security – Specialty
(SCS-C01) 認定試験の質問例

1) ある企業が社内クラウドセキュリティポリシーにおいて、社内の VPC ～ KMS 間の通信はすべて AWS 内で行い、パブリックサービスエンドポイントを使用してはならないと定めています。

最も確実にこの要件を満たすには、どうすればよいですか (2 つ選択してください)。

A) `aws:sourceVpce` 条件を、社内の VPC エンドポイント ID を参照している AWS KMS キーポリシーに追加する。
B) VPC インターネットゲートウェイを VPC から削除し、仮想プライベートゲートウェイを VPC に追加することにより、パブリックインターネットに直接接続できないようにする。
C) AWS KMS に対する VPC エンドポイントを作成し、プライベート DNS を有効化する。
D) KMS のキーインポート機能を使用して、AWS KMS キーを VPN 上でセキュアに転送する。
E) `"aws:SourceIp": "10.0.0.0/16"` 条件を AWS KMS キーポリシーに追加する。

2) アプリケーションチームが、2 個のアプリケーションを使用するソリューションを設計しています。セキュリティチームは、アプリケーションのログを 2 か所に分けて格納したいと考えています。一方のアプリケーションでは、機密データを含むログが生成されるからです。

リスクと作業量を最小限に抑えつつ、これらの要件を満たすには、どうすればよいですか。

A) Amazon CloudWatch Logs を使用して、すべてのログを取得する。ログファイルを解析するための AWS Lambda 関数を作成する。機密データを別のログに移動する。
B) Amazon CloudWatch Logs を使用し、ロググループを 2 個作成する。それぞれのロググループを各アプリケーション用として使用する。必要に応じて、AWS IAM ポリシーを使用して、ロググループに対するアクセスを制御する。
C) 各ログを 1 個のファイルにまとめる。Amazon CloudWatch Logs を使用する。CloudWatch メトリクスフィルタを 2 個作成し、ログから機密データを除去する。
D) 機密データを含むログを Amazon EC2 インスタンスのローカルストレージに格納するロジックをアプリケーションに追加する。Amazon EC2 インスタンスにログインし、機密データを含むログをセキュアな場所に移動するバッチスクリプトを作成する。

3) セキュリティエンジニアが、3 層アプリケーションに対するセキュリティグループルールを設定する必要があります。

- **プレゼンテーション層 – Web 上でユーザーによってアクセスされます。セキュリティグループ `presentation-sg` によって保護されます。**
- **ロジック層 – RESTful API。プレゼンテーション層から HTTPS を使用してアクセスされます。セキュリティグループ `logic-sg` によって保護されます。**
- **データ層 – SQL Server データベース。ロジック層からポート 1433 経由でアクセスされます。セキュリティグループ `data-sg` によって保護されます。**

アプリケーションのセキュリティと機能を確保するには、セキュリティグループルールをどのように設定すればよいですか (3 つ選択してください)。

A) `presentation-sg`: 0.0.0.0/0 からのポート 80 および 443 経由でのアクセスを許可する。
B) `data-sg`: `presentation-sg` からのポート 1433 経由でのアクセスを許可する。
C) `data-sg`: `logic-sg` からのポート 1433 経由でのアクセスを許可する。
D) `presentation-sg`: `data-sg` からのポート 1433 経由でのアクセスを許可する。
E) `logic-sg`: `presentation-sg` からのポート 443 経由でのアクセスを許可する。
F) `logic-sg`: 0.0.0.0/0 からのポート 433 経由でのアクセスを許可する。

4) セキュリティエンジニアが、AWS 上で Web アプリケーションを開発している製品チームと共同作業を行っています。このアプリケーションでは、Amazon S3 を使用して静的コンテンツをホストし、Amazon API Gateway を使用して RESTful サービスを提供し、Amazon DynamoDB をバックエンドデータストアとして使用します。ユーザーは既に、SAML ID プロバイダを通じて公開されているディレクトリに登録されています。

ユーザーが認証を受けてこの Web アプリケーションにアクセスし、API を呼び出せるようにするには、セキュリティエンジニアはどうすればよいですか (3 つ選択してください)。

A) AWS Lambda を使用して、カスタム承認サービスを作成する。
B) Amazon Cognito で、属性を Amazon Cognito ユーザープール属性にマッピングするよう、SAML ID プロバイダを構成する。
C) Amazon Cognito ユーザープールを証明書利用者として追加するよう、SAML ID プロバイダを構成する。
D) ソーシャルログインプロバイダと統合するよう、Amazon Cognito ID プールを構成する。
E) ユーザーの E メールアドレスとパスワードを格納するよう、DynamoDB を更新する。
F) Amazon Cognito ユーザープールオーソライザーを使用するよう、API Gateway を更新する。

5) ある企業が、AWS 上で Web アプリケーションをホストしており、また Amazon S3 バケットを使用して画像を格納しています。各ユーザーがバケット内のオブジェクトを読み取れ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、パブリック読み取りアクセスを許可する次のバケットポリシーを作成しました。

```
{
   "ID":"Policy1502987489630",
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"Stmt1502987487640",
         "Action":[
            "s3:GetObject",
            "s3:GetObjectVersion"
         ],
         "Effect":"Allow",
         "Resource":"arn:aws:s3:::appbucket",
         "Principal":"*"
      }
   ]
}
```

しかし、オブジェクトを読み取ろうとすると、"Action does not apply to any resource(s) in statement." というエラーが通知されます。

このエラーを解消するには、どうすればよいですか。

A) PutBucketPolicy 権限を適用することによって、IAM 権限を変更する。
B) ポリシー名がバケット名と同じであるかどうかを調べる。同じでない場合、ポリシーをバケットと同じ名前にする。
C) `resource` セクションを `"arn:aws:s3:::appbucket/*"` に変更する。
D) `s3:ListBucket` アクションを追加する。

6) ある企業が、ある VPC 内にデータベースホストを配置し、アプリケーション層と Web 層が配置されている別の VPC に対する VPC ピアリングを構成することを決めました。しかし、アプリケーションサーバーからデータベースに接続できません。

この問題を解決するには、どうすればよいですか (2 つ選択してください)。

A) アプリケーションサーバーがプライベートサブネットとパブリックサブネットのどちらに配置されているかを確認する。
B) アプリケーションサーバーサブネットに対するルーティングテーブルを調べ、VPC ピアリング接続へのルートが設定されているかどうかを確認する。
C) データベースサブネットに対する NACL を調べ、インターネットからのトラフィックを許可するルールが設定されているかどうかを確認する。
D) データベースセキュリティグループを調べ、アプリケーションサーバーからのトラフィックを許可するルールが設定されているかどうかを確認する。
E) データベース VPC 内にインターネットゲートウェイがあるかどうかを確認する。

7) Amazon DynamoDB テーブルから項目を取得する新しい AWS Lambda 関数をセキュリティエンジニアがテストした際、この関数がデータを Amazon CloudWatch Logs にロギングしていないことに気付きました。

この Lambda 関数によって代行されるロールに、次のポリシーが割り当てられていました。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"Dynamo-1234567",
         "Action":[
            "dynamodb:GetItem"
         ],
         "Effect":"Allow",
         "Resource":"*"
      }
}
```

この関数が適切にロギングできるようにするには、どの最小権限ポリシーを追加すればよいですか。

A)
```
{
   "Sid":"Logging-12345",
   "Resource":"*",
   "Action":[
      "logs:*"
   ],
   "Effect":"Allow"
}
```

B)
```
{
   "Sid":"Logging-12345",
   "Resource":"*",
   "Action":[
      "logs:CreateLogStream"
   ],
   "Effect":"Allow"
}
```

C)
```
{
   "Sid":"Logging-12345",
   "Resource":"*",
   "Action":[
      "logs:CreateLogGroup",
      "logs:CreateLogStream",
      "logs:PutLogEvents"
   ],
   "Effect":"Allow"
}
```

D)
```
{
   "Sid":"Logging-12345",
   "Resource":"*",
   "Action":[
      "logs:CreateLogGroup",
      "logs:CreateLogStream",
      "logs:DeleteLogGroup",
      "logs:DeleteLogStream",
      "logs:getLogEvents",
      "logs:PutLogEvents"
   ],
   "Effect":"Allow"
}
```

8) ある企業が、Amazon S3 上にデータレイクを作成しようとしています。データは、機密データを含む数百万個の小規模ファイルから成ります。セキュリティチームは、このアーキテクチャに対して次の要件を定めています。

- **送信中データを暗号化しなければならない。**
- **格納データを暗号化しなければならない。**
- **バケットはプライベートでなければならない。バケットが誤ってパブリックになった場合、データは機密扱いのままでなければならない。**

これらの要件を満たすには、どうすればよいですか (2 つ選択してください)。

A) Amazon S3 バケットに対して AES-256 暗号化方式を有効化する。「Amazon S3 で管理されるキーを使用したサーバー側暗号化」(SSE-S3) を使用する。
B) S3 バケットに対してデフォルトの暗号化方式を有効化する。「AWS KMS で管理されるキーを使用したサーバー側暗号化」(SSE-KMS) を使用する。
C) `PutObject` リクエストの中に `aws:SecureTransport` が含まれていない場合に拒否するバケットポリシーを追加する。
D) `aws:SourceIp` を使用して、社内イントラネットからのアップロードとダウンロードだけを許可するバケットポリシーを追加する。
E) Amazon Macie を有効化して、データレイクの S3 バケットを監視し、バケットに変更が加えられた場合に対処する。

9) セキュリティエンジニアが、すべての企業アカウントにおけるすべての API 呼び出しが収集されていること、および API 呼び出しがオンライン状態でありすぐに 90 日間分析できることを確認する必要があります。コンプライアンス上の理由により、このデータは 7 年間復元可能でなければなりません。

拡張性と費用対効果の高い方法でこのデータ保持要件を満たすには、どうすればよいですか。

A) すべてのアカウントにおいて AWS CloudTrail ロギングを有効化し、バージョニングが有効化されている中央の Amazon S3 バケットにログを格納する。データを毎日 Amazon Glacier に移動し、90 日後にデータを失効させるライフサイクルポリシーを作成する。
B) すべてのアカウントにおいて AWS CloudTrail ロギングを有効化し、S3 バケットにログを格納する。7 年後に各バケット内のデータを失効させるライフサイクルポリシーを作成する。
C) すべてのアカウントにおいて AWS CloudTrail ロギングを有効化し、Amazon Glacier にログを格納する。7 年後にデータを失効させるライフサイクルポリシーを作成する。
D) すべてのアカウントにおいて AWS CloudTrail ロギングを有効化し、中央の Amazon S3 バケットにログを格納する。90 日経過したデータを Amazon Glacier に移動し、7 年後にデータを失効させるライフサイクルポリシーを作成する。

10) セキュリティエンジニアが、「あるユーザーのアクセスキーが GitHub 上で見つかった」という通知を受けました。セキュリティエンジニアは、このアクセスキーを使い続けることができないようにする必要があります。また、このアクセスキーが不正行為に使用されたかどうかを調べる必要があります。

これらのタスクを実行するには、どうすればよいですか。

A) このユーザーの IAM 権限を確認し、未承認リソースがあれば削除する。
B) このユーザーを削除する。すべてのリージョンにおける Amazon CloudWatch Logs を確認する。アクセスキーが不正使用されていた場合、報告する。
C) このユーザーのアクセスキーを削除またはローテートする。すべてのリージョンにおける AWS CloudTrail ログを確認する。未承認リソースがあれば削除する。
D) GitHub の投稿からアクセスキーを削除するよう、このユーザーに指示する。キーをローテートする。起動されたインスタンスがある場合、再展開する。

回答

1) A、C – IAM ポリシーに次の条件ステートメントを追加することにより、VPC エンドポイント経由でない AWS KMS へのアクセスを拒否できます。

```
"Condition":{
   "StringNotEquals":{
      "aws:sourceVpce":"vpce-0295a3caf8414c94a"
   }
}
```

[Enable Private DNS Name] オプションを選択した場合、標準の AWS KMS DNS ホスト名 (https://kms.<region>.amazonaws.com) が VPC エンドポイントに変換されます。

2) B – 各アプリケーションのログを特定の Amazon CloudWatch Logs ロググループに送信するよう、構成できます。

3) A、C、E – n 層アーキテクチャにおける各層のセキュリティグループは、そのセキュリティグループにトラフィックを送信するはずのセキュリティグループからのトラフィックだけを許可します。プレゼンテーション層は、インターネットからの HTTP トラフィックおよび HTTPS トラフィックを受け付けます。セキュリティグループはステートフルなので、受信ルールを設定するだけでかまいません。

4) B、C、F – Amazon Cognito が SAML アサーションを受信したとき、SAML 属性をユーザープール属性にマッピングできる必要があります。ID プロバイダから SAML アサーションを受信するよう Amazon Cognito を構成する際、その ID プロバイダは、Amazon Cognito を証明書利用者として追加するよう構成されている必要があります。Amazon API Gateway は、Amazon Cognito から渡される承認情報を認識できる必要があります。これは構成ステップです。

5) C – `resource` セクションは、処理タイプと一致している必要があります。末尾に /* を追加するよう、ARN を修正します。これはオブジェクト処理であるからです。https://aws.amazon.com/blogs/security/writing-iam-policies-how-to-grant-access-to-an-amazon-s3-bucket/

6) B、D – 各 VPC 内で、ピアリング接続を使用して相互にルーティングするよう、ルーティングテーブルを構成する必要があります。また、データベースに対するセキュリティグループに、「別の VPC 内のアプリケーションサーバーセキュリティグループからのリクエストを受け付ける」というルールを追加する必要があります。

7) C – Amazon CloudWatch Logs にロギングするために必要となる基本的な Lambda 権限は、`CreateLogGroup`、`CreateLogStream`、および `PutLogEvents` です。

8) B、C – KMS を使用してバケットを暗号化すれば、ディスクが盗まれた場合およびバケットがパブリックになった場合にデータが保護されます。AWS KMS キーを使用した場合、AWS の外部のユーザーに、そのキーに対する権限を与える必要があるからです。HTTPS を使用した場合、送信中データが保護されます。

9) D – データを Amazon Glacier に移動するライフサイクルポリシーを使用することにより、費用対効果の高い方法ですべての要件を満たしています。

10) C – アクセスキーが削除され、環境に対して不正行為がなされたかどうかが監査されます。

