

あなたの会社にあるオンプレミス環境のコンテンツマネージメントシステムは以下のアーキテクチャを採用しています。

- アプリケーション層 - JBoss アプリケーションサーバー上で動作する Java コード
- データベース層 - Oracle RMAN バックアップユーティリティを使用して定期的に S3 にバックアップされる Oracle データベース
- 静的コンテンツ - iSCSI インターフェース経由でアプリケーションサーバにアタッチされた、Gateway Stored Volume の Storage Gateway に格納された 512GB のコンテンツ

AWS をベースとした災害対策戦略を想定した場合、最も優れた RTO を得られるのものはどれですか？

- EC2 に Oracle データベースおよび JBoss アプリサーバーをデプロイする。Amazon S3 から RMAN Oracle バックアップを復元する。Storage Gateway から静的コンテンツの EBS ボリュームを生成し、JBoss EC2 サーバーにアタッチする。
- RDS で Oracle データベースをデプロイする。EC2 に JBoss アプリサーバー をデプロイする。Amazon Glacier から RMAN Oracle バックアップを復元する。Storage Gateway から静的コンテンツの EBS ボリュームを生成し、JBoss EC2 サーバーにアタッチする。
- EC2 に Oracle データベースおよび JBoss アプリサーバーをデプロイする。Amazon S3 から RMAN Oracle バックアップを復元する。Amazon EC2 で稼働する AWS Storage Gateway を iSCSI ボリュームとして JBoss EC2 サーバーにアタッチして、静的コンテンツを復元する。
- EC2 に Oracle データベースおよび JBoss アプリサーバーをデプロイする。Amazon S3 から RMAN Oracle バックアップを復元する。Amazon EC2 で稼働する AWS Storage Gateway-VTL から静的コンテンツを復元する。

正解 = A

ある ERP アプリケーションが、1 つのリージョンで複数のアベイラビリティゾーンにまたがってデプロイされています。障害が発生した場合、RTO は 3 時間未満、RPO は 15 分である必要があります。お客様は、約 1.5 時間前にデータ破損が発生していたことに気づきました。このような種類の障害が発生したときにこの RTO と RPO を達成するために使用できるのは、どの DR 戦略ですか？

- 15 分ごとに Glacier に DB バックアップを保管すると共に、Amazon S3 に 5 分ごとのトランザクションログを保管する。
- 2 つのアベイラビリティゾーンの間で同期型データベースのマスター/スレーブレプリケーションを使用する。
- Amazon S3 への 1 時間ごとの DB バックアップ取得を行うと共に S3 に 5 分ごとのトランザクションログを保管する。

- D. Amazon EC2 のインスタンスストアボリュームへ 1 時間ごとに DB の バックアップ取得を行うと共に Amazon S3 に 5 分ごとのトランザクションログを保管する。

正解 = C

会社のマーケティング担当ディレクターから、"何気ない親切" と思われる善行を目にしたら 80 文字で要約して投稿できるモバイルアプリケーションを作成するように依頼されました。できるだけ幅広い種類のスマートフォン、ブラウザ、タブレットで動作するように、JavaScript でアプリケーションを記述することにしました。投稿された要約を保存するため、アプリケーションから Amazon DynamoDB にアクセスさせる必要があります。プロトタイプ of 初期テストでは、使用状況に大きなスパイクはないことが分かっています。このアプリケーションで最もコスト効率が高く、スケーラブルなアーキテクチャとなるのはどの選択肢ですか？

- A) EC2 インスタンス上で Security Token Service の Token Vending Machine (TVM) を使用して、JavaScript クライアント に対し一時的な認証情報を提供し、Amazon Identity and Access Management (IAM) ユーザーにマッピングされ、DynamoDB の入力および S3 への GET を許可する署名付き認証情報を提供する。ウェブサイトとして有効にした S3 バケットから モバイルアプリケーションを配信し、クライアントにより DynamoDB が更新される。
- B) Amazon、Google、または Facebook のようなウェブ認証プロバイダにアプリケーションを登録し、そのプロバイダ用の IAM ロールを作成し、IAM ロールには S3 への GET および DynamoDB の入力を許可する権限を設定する。ウェブサイトとして有効にした S3 バケットからモバイルアプリケーションを配信し、クライアントにより DynamoDB が更新される。
- C) Security Token Service の Token Vending Machine (TVM) を使用して、JavaScript クライアントに対し一時的な認証情報を提供し、IAM ユーザーにマッピングされ、DynamoDB の入力を許可する署名付き認証情報を提供する。負荷分散され、オートスケール設定された Apache EC2 インスタンスからモバイルアプリケーションを配信する。EC2 インスタンスは、DynamoDB の入力を許可する IAM ロールを設定し、サーバーにより DynamoDB が更新される。
- D) Amazon、Google、または Facebook のようなウェブ認証プロバイダに JavaScript アプリケーションを登録し、そのプロバイダ用の IAM ロールを作成し、IAM ロールに DynamoDB の入力を許可する権限を設定する。負荷分散され、オートスケール設定された Apache EC2 インスタンスからモバイルアプリケーションを配信する。EC2 インスタンスは、DynamoDB の入力を許可する IAM ロールを設定し、サーバーにより DynamoDB が更新される。

正解 = B

ユーザーにとって機密性の高い情報を取得して表示するウェブサイトを構築しています。サイトが受信するトラフィックの量はわかっている、上下しないと予想されます。このサイトでは、SSL を活用してクライアントとウェブサーバー間の通信を保護します。サイトの性質のゆえに、SSL プライベートキーのセキュリティについて非常に懸念しており、キーが誤って、または意図的に環境外に移動されることがないようにしたいと思っています。また、サイトで表示されるデータは暗号化された EBS ボリュームに保存されますが、ウェブサーバーのログに機密情報が含まれることも懸念しているため、自社の従業員以外には復号化できないようにログを保存する必要があります。すべての要件を満たすのは次のうちのどのアーキテクチャですか？

- A) Elastic Load Balancing を使用して、トラフィックを一連のウェブサーバーに分散する。SSL プライベートキーを保護するため、キーをロードバランサーにアップロードして、SSL トラフィックの負荷を軽減するようにロードバランサーを設定する。ウェブサーバーのログを、ランダムに生成された AES キーを使用して暗号化されているエフェメラルボリュームに書き込む。
- B) Elastic Load Balancing を使用して、トラフィックを一連のウェブサーバーに分散する。ロードバランサーで TCP ロードバランシングを使用して、起動時にプライベート Amazon S3 バケットからプライベートキーを取得するようにウェブサーバーを設定する。Amazon S3 サーバー側の暗号化を使用して、ウェブサーバーのログをプライベート Amazon S3 バケットに書き込む。
- C) Elastic Load Balancing を使用して、トラフィックを一連のウェブサーバーに分散する。TCP ロードバランシングを実行するようにロードバランサーを設定する。AWS CloudHSM を使用してウェブサーバー上で SSL トランザクションを処理し、Amazon S3 サーバー側の暗号化を使用して、ウェブサーバーのログをプライベート Amazon S3 バケットに書き込む。
- D) Elastic Load Balancing を使用して、トラフィックを一連のウェブサーバーに分散する。TCP ロードバランシングを実行するためにロードバランサーを設定する。AWS CloudHSM を使用してウェブサーバー上で SSL トランザクションを処理し、ウェブサーバーのログを、ランダムに生成された AES キーを使用して暗号化されているエフェメラルボリュームに書き込む。

正解 = D

あなたはファットクライアントアプリケーション向けのネットワーク接続を設計しています。このアプリケーションは、ビジネス旅行者向けに設計されており、ホテルの部屋、カフェ、公共の Wi-Fi ホットスポット、その他の場所などのインターネットから接続されています。このアプリケーションをインターネットで公開したくありません。

デプロイメントと運用コストを最小限に抑えながら上記の要件を満たすネットワーク設計はどれですか？

- A) AWS Direct Connect を導入し、VPC へのプライベートインターフェイスを準備する。パブリックサブネットを作成し、そこにアプリケーションサーバーを配置する。
- B) アプリケーションへのバックエンド接続の終端処理する SSL リスナーを使用した、Elastic Load Balancing を実装する。
- C) IPsec VPN 接続環境を構築し、ユーザーに設定情報の詳細を提供する。VPC にパブリックサブネットを作成し、そこにアプリケーションサーバーを配置する。
- D) VPC のパブリックサブネットで SSL VPN ソリューションを構築してから、すべてのユーザーのコンピュータに SSL VPN クライアントソフトウェアをインストールして設定する。VPC にプライベートサブネットを作成し、そこにアプリケーションサーバーを配置する。

正解 = D

あなたの会社は、中央ファイルサーバー経由で 900 GB のデータを共有している、オンプレミスのレガシーエンジニアリングアプリケーションをホストしています。エンジニアリングデータは、ファイルサイズがメガバイトから数ギガバイトで、数千個のファイルで構成されています。エンジニアは通常、1日に 5~10% のファイルを変更します。CTO はこのアプリケーションを AWS に移行したいと考えていますが、ユーザーのダウンタイムを最小限にするために週末に移行できることが条件です。計算によると、会社の既存の 45 Mbps インターネット接続を使用して 900 GB のデータを転送するには、最低 48 時間かかります。

AWS 上でアプリケーション環境を複製した後、与えられた時間内にデータを失うことなくアプリケーションのデータを AWS に移行するには、どうしたらよいですか？

- A) 大容量ファイルには複数のスレッドとマルチパートアップロードを使用して、週末にデータを Amazon S3 にコピーする。開発者と並行して作業し、複製されたアプリケーション環境を再設定して、Amazon S3 を利用してエンジニアリングファイルを提供する。

B) 移行の 1 週間前から Amazon S3 にエンジニアリングデータを同期する。金曜日の夜に最後の同期を実行して、同期が完了したら、データセット全体を AWS ファイルサーバーにコピーする。

C) 金曜日にエンジニアリングデータを 1 TB の USB ドライブにコピーし、土曜日に配送されるように USB ドライブを夜間便ですぐに AWS Import/Export に送付して、EBS ボリュームにインポートしてもらう。インポートされた EBS ボリュームを日曜日に AWS のファイルサーバーにマウントする。

D) AWS Storage Gateway の Gateway-Stored Volume を活用して、ボリュームを作成する。金曜日の夜にエンジニアリング データを Storage Gateway のボリュームにコピーする。データをコピーした後、ボリュームのスナップショットを実行し、EBS ボリュームとしてボリュームを復元して、日曜日に AWS のファイルサーバーにアタッチする。

正解 = B