AWS CERTIFICATION / SOA-C03

1問ずつ深く考える 100問問題集

AWS Certified CloudOps Engineer - Associate
本番相当・本番より難しい・複合難問

問題の直後に改ページ	全選択肢を個別解説	公式ガイド v1.1 対応

作成基準日 2026-07-14

この問題集の使い方

昼休みや短い休憩で、1回に1-3問を解く前提です。選択肢を決めたら、必ず「なぜ他の選択肢ではないか」を一言で説明してから改ページしてください。解説は、正解だけでなく、誤答が正解へ変わる条件まで含めています。

手順	すること
1	問題文の制約を「必須」「望ましい」「禁止」に分ける。
2	各選択肢が落とす条件を探し、最後まで残る構成を選ぶ。
3	改ページして、判断過程と「正解になり得る条件」を照合する。

出題配分

分野	問数	公式配分
Domain 1 監視・ログ・分析・修復・性能最適化	22	22%
Domain 2 信頼性・事業継続	22	22%
Domain 3 デプロイ・プロビジョニング・自動化	22	22%
Domain 4 セキュリティ・コンプライアンス	16	16%
Domain 5 ネットワーク・コンテンツ配信	18	18%

範囲と版

AWS公式試験ガイド（SOA-C03）Version 1.1、2026年6月1日公開の改訂内容を基準にしています。現行名称はAWS Certified CloudOps Engineer - Associateです。問題はAWS認定試験の実問題ではなく、公開された出題範囲とAWS公式ドキュメントをもとに作成した独自問題です。

問題一覧

問題 001 | Domain 1 / 監視・性能 | 本番相当 | 複数選択（5つから2つ選択）

問題 1 プライベートサブネットのCloudWatchエージェント

ある決済会社は、3つのプライベートサブネットに合計60台のAmazon EC2 Linuxインスタンスを配置しています。インスタンスにはパブリックIPv4アドレスがなく、NATゲートウェイもありません。SSM AgentとCloudWatchエージェントはAMIに導入済みで、ssm、ssmmessages（および既存リージョンで必要なec2messages）のインターフェイスVPCエンドポイントを通じてSystems Managerのマネージドノードとして稼働しています。

運用チームは、標準のEC2メトリクスに加えて、OSのメモリ・ディスク使用率、/var/log/settlement/*.log、および複数のワーカープロセスを生成するsettlementdのCPU使用率・メモリ使用量・プロセス数を収集したいと考えています。エージェント設定はSystems Manager Parameter Storeで一元管理し、Run Commandで全インスタンスへ展開します。インスタンスへ長期アクセスキーを置かず、インターネット経路も追加せず、実行時権限は最小限にする必要があります。

要件を満たすために実施すべき対応はどれですか。（2つ選択）

選択肢

A EC2詳細モニタリングを有効化し、CloudWatch Logsの旧エージェントを導入する。settlementdの各PIDをディメンションとして詳細モニタリングへ登録し、ログファイルも同じエージェントで送信する。

B CloudWatchエージェント設定のmetrics_collectedにprocstatとOSメトリクスを、logsに対象ファイルを定義する。設定をAmazonCloudWatch-で始まるParameter Storeパラメータに保存し、各インスタンスのIAMロールにCloudWatchAgentServerPolicy相当の送信・取得権限を付与する。

C 各インスタンスのIAMロールにCloudWatchAgentAdminPolicyを付与する。これにより、実行中のエージェント自身がParameter Storeの設定を更新でき、すべてのサーバーで設定が自動的に同期される。

D CloudWatchメトリクス用のmonitoringとCloudWatch Logs用のlogsのインターフェイスVPCエンドポイントを作成し、プライベートDNSとTCP 443の到達性を確保する。既存のSystems Manager用エンドポイントは、Run CommandとParameter Storeからの設定取得に使用する。

E CloudWatch用のインターフェイスVPCエンドポイントだけを作成する。CloudWatch LogsとParameter Storeへの通信もCloudWatchのエンドポイントへ自動的に集約されるため、ほかのエンドポイントは不要である。

ここでいったん止める | 解答と解説は次ページ

問題 001 正解・解説 本番相当

問題 1の正解・解説

1. 正解

B、D

2. 問題文の重要な条件

- 標準EC2メトリクスだけでなく、ゲストOSのメモリ・ディスク、ログファイル、特定プロセスの状態を収集する。
- settlementdはワーカーを生成するため、固定した1つのPIDではなく、名前や実行ファイルなどで継続的にプロセスを選択する必要がある。
- 設定はParameter Storeに置き、Systems Managerで多数のインスタンスへ展開する。
- NATもパブリックIPも追加できない。CloudWatch、CloudWatch Logs、Systems Managerへプライベートに到達させる必要がある。
- 長期アクセスキーを保存せず、エージェントの実行ロールに設定更新権限を与えない。

3. 正解へ至る判断過程

まず、EC2が標準で送信するメトリクスと、ゲストOS内部でしか取得できない情報を分けます。メモリ使用率、ファイルシステム使用率、任意ログ、プロセス別メトリクスはCloudWatchエージェントの領域です。特定プロセスの監視にはprocstatプラグインを使用し、pid_file、exe、patternのいずれか適切な方式で対象を選びます。

次に、認証と接続経路を分けます。認証にはEC2インスタンスプロファイルを使い、メトリクス・ログ送信と、指定したParameter Storeパラメータの読取りだけを許可します。CloudWatchAgentServerPolicyはAmazonCloudWatch-*パラメータへのssm:GetParameterを含むため、問題文の命名なら適合します。一方、通信経路としてはCloudWatchメトリクス、CloudWatch Logs、Systems Managerは別サービスです。したがって、既存SSMエンドポイントに加えてmonitoringとlogsのインターフェイスエンドポイントが必要です。

4. 正解が要件を満たす理由

Bは、1つのCloudWatchエージェントでOSメトリクス、procstatメトリクス、ログを収集でき、Parameter Storeの共通設定を各サーバーが取得できます。インスタンスロールの一時認証情報を使うため、アクセスキーの配布も不要です。ServerPolicy相当の権限に限定すれば、実行サーバーは設定を読み取ってテレメトリを送信できますが、設定を書き換える必要はありません。

Dは、インターネット経路を設けずに各サービスへHTTPS接続させます。VPCエンドポイントのプライベートDNS、エンドポイントのセキュリティグループ、インスタンス側のアウトバウンド経路を揃えることで、通常のAWSサービスDNS名を変更せずにエージェントを動かせます。

5. 各不正解選択肢が不適切な理由

- **A:** EC2詳細モニタリングは標準EC2メトリクスの送信間隔を主に1分へ短縮する機能で、ゲストOSのメモリや任意プロセスを自動収集しません。旧CloudWatch Logsエージェントはログ送信用であり、procstatによるプロセスメトリクス収集をまとめて担う構成ではありません。
- **C:** CloudWatchAgentAdminPolicyにはParameter StoreへのPutParameterが含まれます。設定を作成・保存する管理主体には使えますが、各本番サーバーへ配ると実行時権限が過大です。また、この権限を付けただけで設定の変更が各エージェントへ自動配信されるわけでもありません。
- **E:** CloudWatchメトリクスのサービスエンドポイントはCloudWatch LogsやSystems ManagerのAPIエンドポイントを兼ねません。メトリクス送信だけ成功し、ログ送信や設定取得が失敗する構成になります。

6. 各不正解選択肢が正解になり得る条件

- **Aが適切になる条件:** CPU、ネットワーク、ディスクI/OなどEC2標準メトリクスの1分粒度だけが必要で、OSメモリ、プロセス、統合ログ収集が不要な場合です。既存の旧ログエージェントを保守する短期的事情がある場合にも限定的には成立します。
- **Cが適切になる条件:** 設定生成専用の管理用インスタンスやCIジョブがParameter StoreへCloudWatchエージェント設定を書き込む場合です。その主体に限ってAdmin相当を与え、監視対象サーバーにはServer相当だけを与えます。
- **Eが適切になる条件:** メトリクスだけを送信し、ログ収集もParameter StoreもSystems Managerも使わない場合です。ログやSSMへは別途NATやプロキシ経由で到達できる場合も、CloudWatch用エンドポイントだけを追加する判断自体はあり得ます。

7. 今後使える判断基準

監視問題では、**何を収集するか、誰の権限で送るか、どのネットワーク経路を通るか**を別々に確認します。EC2標準メトリクスにメモリ・ファイルシステム・プロセスは含まれません。Parameter Storeへ設定を書き込む管理者と、設定を読み取る監視対象サーバーも分離します。また、PrivateLinkでは「AWS全体への1個のエンドポイント」ではなく、原則としてサービスごとのエンドポイントが必要です。

8. 関連サービスとの比較

- **EC2詳細モニタリング:** EC2標準メトリクスを細かい粒度で得る用途。ゲストOS内部の任意情報は収集しません。
- **CloudWatchエージェント:** EC2、オンプレミス、コンテナ環境からOS・アプリケーションのメトリクス、ログ、トレースを収集します。
- **Systems Manager State Manager / Run Command:** エージェントのインストールや設定適用を多数ノードへ実行する手段です。テレメトリの保存先そのものではありません。
- **Parameter Store:** 共有設定の保管に向きます。実行ノードには通常GetParameterだけを許可します。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4

問題 002 | Domain 2 / 信頼性・BC | 本番相当 | 四択（1つ選択）

問題 2 CPUではなく「1台あたりの仕事量」を追う

あるチケット販売会社は、Application Load Balancer（ALB）の背後にあるEC2 Auto ScalingグループでWeb APIを実行している。リクエストごとの処理量はほぼ一定だが、レスポンス待ちの大半は外部決済APIへのI/Oであり、CPU使用率は負荷と比例しない。負荷試験の結果、ターゲット1台あたりの平均リクエスト数が毎分900件を超える状態が続くと、p95レイテンシーがSLOを超えることが分かった。

運用チームは、通常時の余剰インスタンスを抑えながら、トラフィックの増減に応じてこの比率を自動的に維持したい。段階ごとの増減台数を継続的に調整する運用は避けたい。最も適切な構成はどれか。

選択肢

A ALBRequestCountPerTarget を使用し、目標値を負荷試験で得た安全な値に設定したターゲット追跡スケーリングポリシーを作成する。適切なデフォルトインスタンスウォームアップも設定する

B Auto Scalingグループの平均CPU使用率が50%を超えたら2台追加し、30%を下回ったら1台削除するステップスケーリングを設定する

C 過去1週間の最大同時接続数に合わせて最小キャパシティを固定し、ALBのスロースタートだけを有効にする

D 毎時のリクエスト数を予測する予測スケーリングだけを設定し、動的スケーリングは設定しない

ここでいったん止める | 解答と解説は次ページ

問題 002 正解・解説 本番相当

問題 2の正解・解説

1. 正解

A

2. 問題文の重要な条件

- CPU使用率と負荷が比例しない。
- 1ターゲットあたりのリクエスト数とレイテンシーの関係が負荷試験で分かっている。
- 余剰容量とポリシー調整の運用負荷を抑えたい。

3. 正解へ至る判断過程

まず「何台にするか」ではなく、増減に対してほぼ反比例する利用率・スループット指標があるかを見る。本問では、ALB配下のターゲットが増えるほど ALBRequestCountPerTarget が下がり、減るほど上がるため、ターゲット追跡に適した指標である。CPUは外部I/O待ちのため需要の代理指標として弱い。

4. 正解が要件を満たす理由

ターゲット追跡は、指定した目標値の付近にメトリクスを維持するよう、Auto Scalingグループの容量を自動調整する。ALBRequestCountPerTarget は定義済みメトリクスとして利用できる。デフォルトインスタンスウォームアップを実際の初期化時間に合わせれば、起動直後のインスタンスを早く容量に数えて過剰な連続スケールアウトを起こすことも抑えられる。

5. 各不正解選択肢が不適切な理由

- B：CPUが需要と比例しないので、必要なときにアラームが上がらず、逆にCPUだけが上がったときに不要な増設をする可能性がある。
- C：最大負荷への固定は可用性には寄与するが、通常時の余剰容量を抑える要件に反する。ALBのスロースタートは容量自体を増減しない。
- D：予測外の販売開始や外部要因に反応できない。予測スケーリング単独では、実負荷に対する即時の補正手段がない。

6. 各不正解選択肢が正解になり得る条件

- B：CPUが処理量と強く相関し、しきい値超過の大きさごとに増減台数を明示したい場合。
- C：負荷が常に最大に近く、コストより絶対的な即時容量を優先する場合。
- D：負荷が極めて規則的で、予測からの外れを別の仕組みで吸収できる場合。

7. 今後使える判断基準

ターゲット追跡では「容量を2倍にすると、対象メトリクスがおおむね半分になるか」を確認する。CPU、1台あたりのリクエスト数、バックログ÷稼働台数など、容量に応じて変化する平均指標が向く。総リクエスト数のように、台数を増やしても値が変わらない指標をそのまま使わない。

8. 関連サービスとの比較

ターゲット追跡は目標状態を指定する方式、ステップスケーリングはアラーム超過幅ごとの動作を指定する方式である。予測スケーリングは履歴から将来容量を先回りして用意し、スケジュール済みアクションは既知の時刻に容量を変更する。ALBのスロースタートやヘルスチェック猶予期間は、スケーリング方式そのものではない。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3

問題 003 | Domain 3 / 展開・自動化 | 本番相当 | 四択（1つ選択）

問題 3 Change Setで本番更新の影響を見極める

ある企業は、CloudFormationスタックで本番のRDS DBインスタンス、Application Load Balancer、Auto Scalingグループ、IAMロールを管理しています。次のリリースでは、RDSの識別子、起動テンプレートのAMI、ALBリスナー設定、IAMポリシーを同時に変更する予定です。RDSのプロパティ変更によっては、インプレース更新ではなくリソース置換となり、停止やデータ保護の計画が必要です。

変更管理委員会は、次の要件を示しました。

- 本番リソースを変更する前に、追加・変更・削除される論理リソースと、置換の有無を確認する。
- テンプレートとパラメータの候補を複数比較し、承認しなかった候補は実行しない。
- 承認後に、確認した内容を使ってCloudFormationから更新する。
- 構文確認だけで安全と判断せず、実行時のサービス制約などで更新が失敗し得ることも考慮する。
- 確認のためだけに本番と同規模の複製環境を常時維持しない。

最も適切な手順はどれですか。

選択肢

A 本番スタックに対して更新タイプのChange Setを作成し、リソースごとのAction、Replacement、変更前後のプロパティなどを確認する。必要なら別のテンプレートまたはパラメータで複数のChange Setを作り、承認した1つだけを実行する。Change Setの作成成功は更新成功の保証ではないため、バックアップとロールバック計画も維持する。

B validate-templateでテンプレートを検証し、成功したらupdate-stackで直接更新する。テンプレート検証は、既存リソースとの差分、置換、サービスクォータ、カスタムリソースの実行結果まで検査するため、別の事前確認は不要である。

C スタックのドリフト検出を実行し、IN_SYNCなら更新によるリソース置換は発生しないと判断して直接更新する。ドリフト検出は新旧テンプレートの差分と将来の更新動作を表示する。

D 現在のテンプレートから別名の検証スタックを毎回作成し、その作成が成功したら本番を直接更新する。検証スタックの作成結果だけで、既存本番リソースに対する更新・置換動作も完全に再現できる。

ここでいったん止める | 解答と解説は次ページ

問題 003 正解・解説 本番相当

問題 3の正解・解説

1. 正解

A

2. 問題文の重要な条件

- 本番へ変更を適用する前に、追加・変更・削除と置換の可能性を確認する。
- テンプレートだけでなく、パラメータ変更も比較対象である。
- 複数候補を作り、承認された候補だけを実行する。
- プレビューは必要だが、プレビュー成功をデプロイ成功の保証とはみなさない。
- 検証環境の新規作成ではなく、既存スタックに対する更新影響を確認する。

3. 正解へ至る判断過程

要件の中心は「既存スタックへ提案する変更を、適用前に確認する」ことです。この目的に直接対応するのがCloudFormation Change Setです。CloudFormationは現在のスタックと、提出した新しいテンプレートまたはパラメータを比較し、どの論理リソースへどの操作を行う予定かをChange Setに示します。RDSのような重要リソースでは、Replacementやプロパティレベルの差分を確認してから実行判断を行います。

Change Setを作成した段階では本番リソースは変更されません。複数案を作り、不要なChange Setを削除し、承認したものをExecuteChangeSetで適用できます。ただし、作成時の検証で一般的な構文・競合・一部クォータ問題を検出できても、実行時のカスタムリソース処理、刻々と変化するクォータや容量、サービス固有条件まで成功を保証するものではありません。

4. 正解が要件を満たす理由

Aは、レビューと実行を分離します。委員会は本番スタックを変えずに、リソースの追加・変更・削除・条件付き変更・置換を確認できます。パラメータだけを変えた案も別のChange Setとして比較可能です。承認済みChange Setを実行することで、レビュー対象と実際のCloudFormation更新を結び付けられます。また、Change Setの限界を認識してバックアップやロールバック計画を残すため、RDS置換を含む本番運用としても妥当です。

5. 各不正解選択肢が不適切な理由

- **B:** validate-templateはテンプレートの基本的な妥当性確認に使えますが、既存スタックとの更新差分や置換を承認用に提示する機能ではありません。直接更新すると、レビュー前にリソース変更が始まります。実行時の全サービス制約を保証するという説明も誤りです。
- **C:** ドリフト検出は、現在の実リソースが現在のテンプレートから外れているかを調べる機能です。次のテンプレートによる将来の追加・削除・置換をプレビューするものではありません。IN_SYNCでも、次の変更が置換を要求することはあります。
- **D:** 新規スタックの作成テストは、テンプレートが新規環境で作れるかを確かめる補助策です。しかし、既存物理リソースに対する更新と新規作成ではCloudFormationの動作が異なり、RDS置換やデータ保持への影響を完全には再現しません。毎回の同規模環境にも費用と時間がかかります。

6. 各不正解選択肢が正解になり得る条件

- **Bが適切になる条件:** 開発環境の小さな変更など、承認前プレビューを要求せず、速度を優先して直接更新できる場合です。それでもvalidate-templateだけで本番安全性が保証されるとは考えません。
- **Cが適切になる条件:** 調査目的が「コンソールやCLIで手動変更された既存リソースを特定すること」であり、新しいテンプレートの更新影響を確認することではない場合です。

- **Dが適切になる条件:** 新規環境の再現性、統合テスト、アプリケーション動作確認を行う場合です。これはChange Setによる本番更新プレビューを補完しますが、代替にはなりません。

7. 今後使える判断基準

CloudFormationの事前確認は、**構文ならvalidate-template、実状態と現テンプレートの差ならドリフト検出、新テンプレートを既存スタックへ適用した差ならChange Set**と分けます。Change SetでReplacement=Trueまたは条件付き置換が見えた重要リソースは、停止、バックアップ、DeletionPolicy、スタックポリシーも併せて確認します。プレビューはリスクを可視化しますが、実行成功の保証ではありません。

8. 関連サービスとの比較

- **Change Set:** 既存スタックまたは新規スタックへ提案する変更を、実行前に一覧化します。
- **ドリフト検出:** 現行テンプレートの期待値と、現在の実リソース状態を比較します。
- **直接更新:** Change Setのレビュー段階を省き、送信した変更を直ちに適用します。
- **スタックポリシー:** スタック更新時に重要リソースへ許可する更新アクションを制限します。Change Setの可視化とは役割が異なります。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3

問題 004 | Domain 5 / ネットワーク | 本番相当 | 四択（1つ選択）

問題 4 NATゲートウェイ障害とAZ依存

ある会社は、3つのアベイラビリティーゾーン（AZ）にまたがるプライベートサブネットでEC2インスタンスを実行している。各インスタンスは、OS更新と外部のSaaS APIへのHTTPS通信のためにインターネットへの送信接続を必要とする。現在はAZ-aのパブリックサブネットにNATゲートウェイを1つだけ配置し、全プライベートサブネットのデフォルトルートをそのNATゲートウェイへ向けている。

AZ-aで障害が発生した際、残りのAZのアプリケーション自体は稼働を続けたが、外部APIへ接続できなくなった。会社はAZ障害への耐性を高めると同時に、通常時のAZ間データ転送料も抑えたい。EC2インスタンスへのパブリックIPv4アドレスの付与は禁止されている。最適な変更はどれか。

選択肢

A AZ-aのNATゲートウェイにElastic IPアドレスを2つ関連付け、接続数の上限を増やす。

B NATゲートウェイを廃止し、各プライベートサブネットのデフォルトルートをインターネットゲートウェイへ向ける。

C 各AZのパブリックサブネットにNATゲートウェイを配置し、各プライベートサブネットを同じAZのNATゲートウェイへルーティングする。

D AZ-aにNATインスタンスのAuto Scalingグループを作成し、既存のNATゲートウェイを置き換える。

ここでいったん止める | 解答と解説は次ページ

問題 004 正解・解説 本番相当

問題 4の正解・解説

1. 正解

C

2. 問題文の重要な条件

3AZで稼働していること、AZ-aの障害でも送信通信を継続すること、通常時のAZ間転送料を抑えること、そして各EC2へパブリックIPv4を付与できないことが重要である。

3. 正解へ至る判断過程

NATゲートウェイは配置先AZのリソースである。単一AZのNATゲートウェイを全AZから共用すると、そのAZが送信経路の単一障害点になり、他AZからの通常通信にはAZ間転送も生じる。各AZにNATゲートウェイを置き、同一AZ内で経路を完結させれば、可用性と転送コストの両条件を満たす。

4. 正解が要件を満たす理由

AZごとに独立した送信経路を持つため、1AZの障害が他AZのNAT経路へ波及しない。プライベートサブネットから同じAZのNATゲートウェイを使用するので、平常時の不要なAZ間転送も避けられる。

5. 各不正解選択肢が不適切な理由

A: 追加のElastic IPは同一宛先への同時接続数拡張には役立つが、NATゲートウェイのAZ依存を解消しない。
B: インターネットゲートウェイはプライベートIPv4を変換しない。パブリックIPv4を持たないEC2は、この経路だけではインターネットへ出られない。
C: 正解肢のため対象外。
D: NATインスタンスを同じAZだけで実行すれば単一AZ障害は残り、パッチ適用・フェイルオーバー・帯域管理の運用負荷も増える。

6. 各不正解選択肢が正解になり得る条件

Aは、可用性ではなく同一宛先へのポート枯渇だけが問題なら候補になる。Bは、EC2にパブリックIPv4を付与でき、直接公開してもよい場合に限られる。Dは、NATゲートウェイが提供しない特殊なパケット処理が必要で、複数AZ化と運用を会社が引き受けられる場合に候補になる。

7. 今後使える判断基準

「複数AZのプライベートサブネットからIPv4で外へ出る」「AZ障害に耐える」「AZ間転送を減らす」が揃ったら、NATゲートウェイをAZごとに置き、同一AZへルーティングする。

8. 関連サービスとの比較

NATゲートウェイはIPv4の送信通信に使う。IPv6の送信専用ならegress-onlyインターネットゲートウェイ、S3やDynamoDBだけなら追加料金のないゲートウェイVPCエンドポイント、対応AWSサービスへの非公開接続ならインターフェイスVPCエンドポイントも比較する。

公式確認先 AWS公式 1 / AWS公式 2

問題 005 | Domain 4 / セキュリティ | 複合難問 | 複数選択（5つから2つ選択）

問題 5 委任先管理者に二重の上限を設ける

AWS Organizations配下の各開発アカウントでは、アカウント管理者がアプリケーション用IAMロールを作成し、業務に応じたポリシーを付与する。中央セキュリティチームは次を同時に満たしたい。

1. どのメンバーアカウントでも、CloudTrail停止やOrganizations離脱など組織として禁止した操作は、ローカル管理者にも許可しない。
2. 開発アカウントの管理者が作る特定のワークロードロールは、誤ってAdministratorAccessを付けても、事前定義したサービスとアクションの範囲を越えられない。

ローカル管理者が日々の最小権限ポリシーを変更できる柔軟性は残す。選ぶべき対策を2つ選べ。

選択肢

A	すべてのワークロードロールへ読み取り専用のIAMポリシーだけを付与し、将来の変更は中央チームが代行する。
B	禁止操作を明示的にDenyするSCPを対象OUへ関連付ける。
C	CloudTrailバケットのリソースポリシーだけでOrganizations離脱も拒否する。
D	ワークロードロール作成時に中央定義のpermissions boundaryを必須とし、そのboundaryを外す権限をローカル管理者へ与えない。
E	各利用者のSTSセッション時間を1時間へ短縮する。

ここでいったん止める | 解答と解説は次ページ

問題 005 正解・解説 複合難問

問題 5の正解・解説

1. 正解

B、D

2. 問題文の重要な条件

組織全体の絶対的な禁止と、特定ロールに対する委任可能な最大権限は別要件である。ローカル管理者には境界内でポリシーを変える自由を残す。

3. 正解へ至る判断過程

SCPはメンバーアカウント内のプリンシパルが得られる最大権限を組織階層から制限し、明示的Denyはローカルの Allowで覆せない。Permissions boundaryは、そのIAMユーザーまたはロールにアイデンティティポリシーで付与できる最大範囲を定める。両者をそれぞれの層へ使う。

4. 正解が要件を満たす理由

Bでアカウント管理者を含む組織的な禁止を強制し、Dで委任作成ロールだけの上限を細かく設定できる。ローカル管理者はboundaryの内側なら業務ポリシーを更新できる。

5. 各不正解選択肢が不適切な理由

A: 柔軟性を失い、中央チームが全変更のボトルネックになる。付与済みポリシーだけでは、管理者による追加を防げない。
B: 正解肢のため対象外。
C: S3バケットへの操作は制御できても、Organizations APIや他サービスの禁止を一つのバケットポリシーでは強制できない。
D: 正解肢のため対象外。
E: 認証情報の有効時間を短くするだけで、許可されるアクションの上限を変えない。

6. 各不正解選択肢が正解になり得る条件

Aは権限変更が極めて少なく中央統制を優先する小規模環境なら運用案になる。Cはログバケットへの削除・上書き・外部アクセスを守る一要素として必要である。Eは漏えい時のセッション悪用時間を短くしたい場合に有効である。

7. 今後使える判断基準

SCPは組織・OU・アカウントの最大権限、permissions boundaryは特定IAM主体の委任上限、identity policyは実際に与える権限である。境界やSCPは単独で権限を付与しない。

8. 関連サービスとの比較

リソースポリシーは対象リソース側からプリンシパルを許可・拒否する。Session policyはAssumeRole時の一時セッションをさらに絞る。最終的な権限はAllowの積集合と、どこかにある明示的Denyを評価して決まる。

公式確認先 AWS公式 1 / AWS公式 2

問題 006 | Domain 1 / 監視・性能 | 本番相当 | 四択（1つ選択）

問題 6 エラー率で動かすAuto Scalingアラーム

あるAPIサービスはApplication Load Balancer（ALB）配下のEC2 Auto Scalingグループで稼働しています。通常は毎分数万件のリクエストがありますが、深夜には数分間リクエストが0件になることがあります。運用チームは、ALBのHTTPCode_Target_5XX_Countを固定件数で監視しているため、トラフィックが多い時間だけ過剰にスケールアウトする問題を抱えています。

要件は次のとおりです。

- 5XXの**割合**が2%を超えた状態が、直近3分のうち2分で発生した場合にステップスケーリングでスケールアウトする。
- リクエストが0件で両方のメトリクスが発行されない時間を障害とは扱わず、空のグループを不要にスケールアウトしない。
- 1分だけの一過性エラーではスケールしない。
- 新しいカスタムメトリクスをアプリケーションから発行する運用は避ける。

最も適切な構成はどれですか。

選択肢

A 同じ1分間のHTTPCode_Target_5XX_CountのSumをRequestCountのSumで割り100を掛けるMetric Math式を作り、その式を返す時系列だけをアラーム対象にする。期間1分、評価期間3、Datapoints to alarmを2、しきい値を2%とし、欠落データをnotBreachingとしてステップスケーリングポリシーを関連付ける。

B HTTPCode_Target_5XX_Countの合計が毎分100件を超えたら発報するアラームを作る。期間1分、評価期間3、Datapoints to alarmを2、欠落データをbreachingにし、ステップスケーリングポリシーを関連付ける。

C HTTPCode_Target_5XX_CountにCloudWatch Anomaly Detectionバンドを設定し、上限バンドを超えたらAuto Scalingアクションを直接実行する。欠落データはignoreにする。

D RequestCountをFILL(m1, REPEAT)で補完し、最新の非ゼロ値を分母として5XX率を計算する。期間1分で1回でも2%を超えたらターゲット追跡スケーリングを実行する。

ここでいったん止める | 解答と解説は次ページ

問題 006 正解・解説 本番相当

問題 6の正解・解説

1. 正解

A

2. 問題文の重要な条件

- エラー件数ではなく、トラフィック量で正規化した5XX率を使う。
- 3分中2分というM out of N評価が必要である。
- 無通信時の欠落は正常であり、スケールアウトの根拠にしない。
- 既存のALBメトリクスだけで実現し、カスタムメトリクスの発行を避ける。
- 実行したいのは異常検知の通知ではなく、ステップスケーリングである。

3. 正解へ至る判断過程

固定件数の5XXはリクエスト総数が増えるほど大きくなるため、まずMetric Mathで100 × 5XX / RequestCountを計算します。次に「3分のうち2分」をEvaluationPeriods=3、DatapointsToAlarm=2で表します。深夜にリクエストがなく式のデータポイントが欠落することは障害ではないため、TreatMissingData=notBreachingが要件に合います。最後に、そのMetric Mathアラームへステップスケーリングポリシーを関連付けます。

4. 正解が要件を満たす理由

Aは、負荷の大小に左右されにくいエラー率を既存メトリクスから計算します。M out of Nにより1分だけの異常を除外しつつ、3分連続を待たず2回の悪化で対応できます。欠落を非違反として扱うため、0トラフィック時に欠落だけを理由としてALARMになりません。Metric Math式をアラームの戻り値にし、元メトリクスは計算入力として扱うことで、追加のメトリクス発行も不要です。

5. 各不正解選択肢が不適切な理由

- **B:** 固定100件では、同じエラー率でも総リクエスト数により評価が変わります。また、正常な無通信をbreachingにすると、深夜の欠落だけでスケールアウトする危険があります。
- **C:** Anomaly Detectionは過去のパターンから動的なしきい値を作る用途で、明示された2%というSLO条件をそのまま表すものではありません。さらに、異常検知モデルをしきい値に使うアラームはAuto Scalingアクションを持てません。
- **D:** 0トラフィック後にも古いRequestCountを分母として反復すると、異なる時点の件数を混ぜて実在しないエラー率を作る可能性があります。1データポイントで反応するため一過性エラーを除外できず、ステップスケーリングという指定にも一致しません。

6. 各不正解選択肢が正解になり得る条件

- **Bが適切になる条件:** 毎分のリクエスト量がほぼ一定で、利用者影響がエラー率ではなく「失敗した絶対件数」で定義され、メトリクス欠落自体を障害として扱う場合です。
- **Cが適切になる条件:** 日次・週次パターンがあり、静的なしきい値を決めにくい指標の異常をSNS通知や調査開始に使う場合です。Auto Scalingアクションが不要なら有力です。
- **Dが適切になる条件:** 本来連続して発行されるゲージ値が一時的に欠落し、「直前値を維持する」ことに業務上の意味がある場合です。疎なメトリクスをターゲット追跡に使う際にFILL(..., REPEAT)が役立つことはあります。

7. 今後使える判断基準

比率の問題では、分子・分母のSumを同一期間で揃え、分母0と欠落の意味を先に決めます。M out of Nは「感度」と「一過性ノイズ耐性」を両立させる手段です。欠落データは一律に悪いものではなく、**常時発行されるはずのメトリクスならbreaching、イベント発生時だけ出るメトリクスや無通信が正常ならnotBreaching**を基本に検討します。

8. 関連サービスとの比較

- **Metric Math:** 複数の既存メトリクスから比率・合計・条件式を作り、ダッシュボードやアラームに利用します。
- **Anomaly Detection:** 周期性を含む通常範囲を学習します。固定SLOの判定とは目的が異なり、異常検知アラームはAuto Scalingアクションに制約があります。
- **ステップスケーリング:** しきい値からの超過量に応じて増減幅を変えられます。
- **ターゲット追跡:** 指標を目標値付近に維持するようCloudWatchアラームをサービス側が管理します。単発の障害率に対する段階的増強とは設計意図が異なります。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4

問題 007 | Domain 2 / 信頼性・BC | 本番より難しい | 四択（1つ選択）

問題 7 段階表どおりにワーカーを増やす

ある映像変換システムでは、Amazon SQSキューからEC2ワーカーがジョブを取得する。ジョブの平均処理時間は一定ではなく、CPU使用率もジョブ種別によって大きく異なる。運用部門は負荷試験と費用承認の結果から、ApproximateNumberOfMessagesVisible ÷ InServiceワーカー数 をカスタムメトリクスとして発行し、次の増設表を厳密に適用することにした。

- 100超〜300以下：2台追加
- 300超〜800以下：6台追加
- 800超：現在容量を100%増加

また、低下時には別の段階表で縮小し、起動後8分間は新規ワーカーを次の縮小判断の計算から保護したい。承認済みの増減表を変更せず、アラーム超過の大きさに応じて自動化する方法として最も適切なものはどれか。

選択肢

A	バックログ/ワーカー数を100に維持するターゲット追跡ポリシーを1つだけ設定する
B	カスタムメトリクスに対するCloudWatchアラームと、超過幅ごとに絶対台数・割合の調整値を定義したステップスケーリングポリシーを設定し、インスタンスウォームアップを8分にする
C	しきい値100を超えたら6台追加するシンプルスケーリングを設定し、クールダウンを8分にする
D	キューのメッセージ到着時刻をEventBridgeで集計し、1時間ごとのスケジュール済みアクションとして希望容量を書き換える

ここでいったん止める | 解答と解説は次ページ

問題 007 正解・解説 本番より難しい

問題 7の正解・解説

1. 正解

B

2. 問題文の重要な条件

- CPUではなく、キューのバックログを容量で割った指標が需要を表す。
- 超過幅に応じた増減台数・割合が承認済みで、表どおりの動作が必要。
- 起動後8分のワーカーを縮小判断から外したい。

3. 正解へ至る判断過程

目標値を保つだけならターゲット追跡も有力だが、本問は「どの超過幅で何台または何%増やすか」を明示している。これはステップ調整の要件そのものである。新規インスタンスが安定するまでの期間は、ステップスケーリングのインスタンスウォームアップで扱う。

4. 正解が要件を満たす理由

ステップスケーリングは、CloudWatchアラームのしきい値からどの程度離れたかに応じて、複数のスケーリング調整を選べる。ChangeInCapacity と PercentChangeInCapacity などを使い分けられるため、2台、6台、100%増加という表現を実装できる。ウォームアップ中の容量を考慮して重複した増減を抑えられる。

5. 各不正解選択肢が不適切な理由

- A：SQSワーカーの一般的な自動調整としては妥当だが、Auto Scalingが必要容量を計算するため、承認済みの段階表どおりの調整を保証しない。
- C：シンプルスケーリングは1回の調整とクールダウンを基本とし、超過幅ごとの3段階を表現できない。
- D：不規則に到着する実際のバックログではなく時刻で動くため、急増にも処理時間の変化にも追従しない。

6. 各不正解選択肢が正解になり得る条件

- A：段階表への拘束がなく、バックログ/台数を一定に保つことが目的なら、より少ない調整で運用できる。
- C：1個のしきい値と1個の調整値で十分な単純なワークロード。
- D：処理量と実行時刻が事前に確定している定期バッチ。

7. 今後使える判断基準

「目標を維持したい」ならターゲット追跡、「超過幅ごとの操作表を実装したい」ならステップスケーリングである。SQSでは総バックログだけでなく、バックログを処理能力または稼働台数で割った指標の方が、必要容量との比例関係を作りやすい。

8. 関連サービスとの比較

シンプルスケーリングはクールダウン中に次の動作を待ちやすい。ステップスケーリングとターゲット追跡はインスタンス単位のウォームアップを利用する。予測スケーリングは将来の規則的な負荷を先回りするもので、キューに既に溜まったジョブへの段階対応とは役割が異なる。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3

問題 008 | Domain 3 / 展開・自動化 | 本番より難しい | 四択（1つ選択）

問題 8 ドリフトを整理して既存リソースをインポートする

あるチームは、CloudFormationスタックでWebシステムを管理しています。インシデント対応中、スタック管理下のセキュリティグループへ運用担当者が許可済み社内CIDRを手動追加しました。この変更は恒久的に残すことが承認されています。一方、監査ログ用S3バケットは過去にコンソールから作成されており、どのCloudFormationスタックにも属していません。バケット名は固定で、大量のログと既存のバケットポリシー・暗号化・ライフサイクル設定を保持しています。

チームは次の状態を目指しています。

- セキュリティグループの手動変更を把握し、テンプレートの期待状態へ正式に取り込む。
- S3バケットを削除・再作成せず、既存スタックの管理対象にする。
- インポート中に、既存スタックのほかのリソースを作成・削除・変更しない。
- インポート後に、テンプレート記述と実バケット設定の差を確認する。

最も適切な手順はどれですか。

選択肢

A スタックのドリフト検出を実行する。DRIFTEDになればCloudFormationが実リソースを読み取り、セキュリティグループの変更をテンプレートへ自動追記し、同じアカウントの未管理S3バケットも自動的にスタックへ追加する。

B まずドリフト検出で変更箇所を特定し、承認済みセキュリティグループ設定をdesired stateとしてテンプレートへ反映する。actual state、previous deployment state、desired stateを比較するdrift-aware Change Setを作成・確認して実行し、物理ルールを変更せずドリフト状態を整合させる。次に、実バケットの構成を記述しDeletionPolicy: Retainを付けたS3リソースを含むスタック全体のテンプレートを用意し、バケット名を識別子として別のIMPORT Change Setを実行する。完了後に再度ドリフト検出する。

C S3バケットをテンプレートへ追加し、通常のUPDATE Change Setを実行する。CloudFormationは同名バケットを検出すると新規作成を省略し、自動的に既存バケットの所有権をスタックへ移す。

D インポート用テンプレートで、既存のセキュリティグループを新しい論理IDとして、S3バケットと同時に指定する。元の論理IDを削除すれば、同じ物理セキュリティグループを新しい論理IDへインポートでき、ドリフトも同時に解消する。

ここでいったん止める | 解答と解説は次ページ

問題 008 正解・解説 本番より難しい

問題 8の正解・解説

1. 正解

B

2. 問題文の重要な条件

- 手動変更されたセキュリティグループは、すでにこのスタックの管理対象である。
- 手動変更は消すのではなく、承認済みの期待状態としてテンプレートへ採用する。
- S3バケットは実在し、未管理で、データを保持したままインポートする。
- 手動インポートでは、インポート対象リソースにDeletionPolicyと物理リソース識別子が必要である。
- インポート操作中は、ほかのリソース作成・削除・プロパティ変更を混在させられない。
- CloudFormationはインポート時にテンプレートと実際の全プロパティ一致までは検証しないため、完了後のドリフト確認が重要である。

3. 正解へ至る判断過程

最初に「既存スタック管理下のリソース」と「スタック外のリソース」を分けます。セキュリティグループはすでにCloudFormation管理下なので、新たにインポートする対象ではありません。ドリフト検出でテンプレートと実設定の差を確認し、実設定を正とする承認があるため、テンプレート側へ社内CIDRを追加します。drift-aware Change Setはactual、previous deployment、desiredの3状態を比較し、desiredをactualに合わせたプロパティについては物理リソースを変更せずドリフト状態をリセットできます。これにより既存ルールを重複作成する通常更新の問題を避けます。

S3バケットは未管理なのでResource Importを使います。インポート用テンプレートには既存のスタックリソースをすべて保持したうえで、実バケットを表す論理リソースを追加します。手動インポート対象にはDeletionPolicyが必要であり、保護意図が明確なRetainが適します。バケット名を識別子として実物と論理IDを対応付け、IMPORT Change Setを実行します。この操作ではほかの構成変更を同時に行わず、完了後にドリフト検出で記述漏れを確認します。

4. 正解が要件を満たす理由

Bは、drift-aware Change Setによる既存ドリフトの採用と、IMPORT Change Setによる未管理リソースの取り込みを別の安全な操作として扱います。セキュリティグループのactual stateを正式なdesired stateへ反映するので、物理ルールを削除・再作成せず、将来の更新で承認済みルールが意図せず消されにくくなります。S3バケットは物理IDを保ったままスタックへ関連付けられるため、ログのコピーやバケット再作成が不要です。インポート後のドリフト検出は、CloudFormationがインポート時に検証しない実プロパティとの差を発見する手段になります。

5. 各不正解選択肢が不適切な理由

- **A:** ドリフト検出は差を報告する機能であり、実状態をテンプレートへ自動反映したり、未管理リソースを自動発見してインポートしたりしません。解消方法は運用者が選びます。
- **C:** 通常のスタック更新で未管理のS3バケットを追加すると、CloudFormationは新規作成を試みます。同名バケットが既に存在すれば作成に失敗するので、IMPORT操作が必要です。
- **D:** セキュリティグループはすでに同じスタックの元論理IDに属しています。同じ物理リソースを別の論理IDや複数スタックへ重複インポートできません。また、インポート操作では既存リソースの削除やプロパティ変更を混在させられません。

6. 各不正解選択肢が正解になり得る条件

- **Aが適切になる条件:** 「自動修復」ではなく、手動変更の有無と差分を一覧化することだけが目的の場合です。結果に基づくテンプレート修正または実リソース修正は別途行います。
- **Cが適切になる条件:** テンプレートへ追加する物理リソースがまだ存在せず、CloudFormationに新規作成させたい場合です。
- **Dが適切になる条件:** あるリソースを別スタックへ移動する場合、元スタックでDeletionPolicy: Retainを設定してテンプレートから安全に外し、どのスタックにも属さない状態にした後、別操作で移動先へインポートする方法はあります。同時重複管理はできません。

7. 今後使える判断基準

ドリフト検出は差の発見、drift-aware Change Setはactual/previous/desiredの3者比較とドリフト調整、Resource Importは既存の未管理リソースと論理IDの関連付けです。インポート時は対象タイプのサポート、識別子、DeletionPolicy、他スタック未所属を確認します。インポートは実構成との完全一致を保証しないため、直後のドリフト検出を習慣にします。

8. 関連サービスとの比較

- **Resource Import:** 既存の物理リソースを削除せずCloudFormation管理へ取り込みます。
- **ドリフト検出:** テンプレートに明示された期待値と現在値の差を報告します。未対応タイプはNOT_CHECKEDになります。
- **従来のChange Set / drift-aware Change Set:** 従来型はpreviousとdesiredを比較し、drift-aware型はactualも含む3者を比較してドリフト上書き・採用の影響を示します。どちらも未管理の同名リソースを自動インポートしません。
- **DeletionPolicy: Retain:** スタックから論理リソースを外したりスタックを削除したりするとき、物理リソースを保持します。通常の更新置換を制御するUpdateReplacePolicyとは役割が異なります。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4 / AWS公式 5

問題 009 | Domain 5 / ネットワーク | 本番相当 | 四択（1つ選択）

問題 9 戻り通信だけ失敗するネットワークACL

インターネット向けApplication Load Balancer（ALB）が、プライベートサブネットのEC2へTCP 8080で転送している。セキュリティグループは、ALBでインターネットからの443を許可し、EC2ではALBのセキュリティグループから8080を許可している。新しいネットワークACLを適用した直後から、ALBのターゲットが断続的にunhealthyになった。ネットワークACLは、ALBサブネットへの受信443と、EC2サブネットへの受信8080だけを許可し、その他を拒否している。

セキュリティグループを広げず、最小限の変更で通信を復旧するにはどうすべきか。

選択肢

A ALBサブネットのACLでは、クライアント向けエフェメラルポートの送信、EC2向けTCP 8080の送信、EC2からのエフェメラルポートの受信を必要なCIDRに限定して許可する。EC2サブネットのACLでは、ALBからのTCP 8080の受信とALB向けエフェメラルポートの送信を許可する。

B EC2のセキュリティグループへ、クライアントの全IPv4アドレスからTCP 8080を許可する。

C ALBをNetwork Load Balancerへ置き換え、クライアントIPをEC2まで保持する。

D 両サブネットのルートテーブルに、相互のCIDRを宛先とするローカルルートを追加する。

ここでいったん止める | 解答と解説は次ページ

問題 009 正解・解説 本番相当

問題 9の正解・解説

1. 正解

A

2. 問題文の重要な条件

問題はネットワークACL適用直後に始まり、セキュリティグループの受信元は適切である。ACLは要求先の受信ポートだけを許可し、ALBからEC2への8080送信と、両接続の戻り通信に使われるエフェメラルポートを許可していない。

3. 正解へ至る判断過程

セキュリティグループはステートフルなので、許可された接続の戻り通信は自動的に許可される。一方、ネットワークACLはステートレスであり、要求と応答を別々に許可する必要がある。クライアント->ALBとALB->ターゲットは別のTCP接続であるため、それぞれについて宛先ポートへの要求と要求元エフェメラルポートへの応答を許可する。

4. 正解が要件を満たす理由

ALB側の8080送信を追加し、両接続のエフェメラルポートを必要な方向とCIDRに限定して許可すれば、既存のセキュリティグループ境界を保ったまま、ステートレスACLによる要求・応答の破棄を解消できる。ヘルスチェックポートがトラフィックポートと異なる場合は、そのポートも同様に許可する。

5. 各不正解選択肢が不適切な理由

A: 正解肢のため対象外。
B: ALB経由だけに限定していたEC2の境界を不要に広げるうえ、ACLで応答が拒否される原因は残る。
C: ロードバランサーの種類を変えても、ステートレスACLで双方向を許可する必要は変わらない。
D: VPC内CIDRには自動的にlocalルートが存在する。ACLによる拒否をルート追加では直せない。

6. 各不正解選択肢が正解になり得る条件

Bは、ALBを介さずEC2へ直接接続させる明確な要件がある場合だけ検討する。Cは、静的IP、TCP/UDP、超低遅延、送信元IP保持などNLB固有の要件がある場合に適する。Dは、接続先が別VPCやオンプレミスで、実際に経路が欠けている場合に必要となる。

7. 今後使える判断基準

SGが正しく、ACL変更後に片方向・断続的なTCP失敗が起きたら、「ACLはステートレス」「ロードバランサーはクライアント側とターゲット側で別接続」「要求先ポートと戻り側エフェメラルポートの両方」を確認する。

8. 関連サービスとの比較

セキュリティグループはENI単位のステートフル制御、ネットワークACLはサブネット単位のステートレス制御である。VPC Flow LogsのREJECTはACLやSGの調査に役立つが、どちらのルールが原因かを直接断定するものではない。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3

問題 010 | Domain 4 / セキュリティ | 本番相当 | 四択（1つ選択）

問題 10 意図しない外部公開を継続検出する

セキュリティアカウントから、組織内全アカウントのS3バケット、IAMロール、KMSキー、SQSキューなどについて、リソースポリシーが組織外のプリンシパルへアクセスを許していないか継続的に確認したい。許可済みの自組織を信頼ゾーンとして定義し、新たな外部アクセスが生まれたときにFindingとして検出したい。脆弱性スキャンや機密データ内容の検査ではない。

最適なサービスはどれか。

選択肢

A	AWS IAM Access Analyzerを組織の信頼ゾーンで構成し、委任管理者から外部アクセスFindingを集約する。
B	Amazon Inspectorで全EC2のCVEスキャンを有効にする。
C	Amazon MacieでS3の機密データ検出ジョブだけを実行する。
D	IAM Policy Simulatorで各リソースポリシーを週次に手入力して検証する。

ここでいったん止める | 解答と解説は次ページ

問題 010 正解・解説 本番相当

問題 10の正解・解説

1. 正解

A

2. 問題文の重要な条件

対象はリソースポリシーによる組織外アクセス、信頼ゾーンとの差分、継続的Finding、マルチアカウント集約である。

3. 正解へ至る判断過程

IAM Access Analyzerのexternal access analyzerは、数学的解析を用いて、定義したzone of trust外からアクセス可能な対応リソースを検出する。Organizationsと委任管理者を使い、組織を信頼範囲にできる。

4. 正解が要件を満たす理由

新規・変更されたリソースポリシーを継続評価し、意図しない外部プリンシパルへの経路をFindingとして可視化できる。CVEやデータ内容を読む必要はない。

5. 各不正解選択肢が不適切な理由

A: 正解肢のため対象外。
B: Inspectorはワークロードやコンテナイメージ等の脆弱性を評価し、リソースポリシーの外部共有を主目的にしない。
C: MacieはS3内の機密データ発見とS3セキュリティ評価であり、IAMロールやKMSキー等を横断した外部アクセス解析ではない。

D: 手作業で継続性と網羅性に欠け、信頼ゾーン外の経路を組織規模で自動Finding化しない。

6. 各不正解選択肢が正解になり得る条件

BはCVE・ネットワーク到達性を含む脆弱性管理、Cは個人情報や認証情報などS3内データの分類、Dは特定主体の特定APIが許可されるかを個別に再現する場合に適する。

7. 今後使える判断基準

「誰がアクセスできるか、特に信頼境界の外」はAccess Analyzer。「中に何が入っているか」はMacie。「ソフトウェアに何の脆弱性があるか」はInspectorと読む。

8. 関連サービスとの比較

AWS Configは設定がルールへ適合するか、Security Hubは複数サービスのFinding集約、CloudTrailは実際に行われたAPI操作を記録する。Access Analyzerはアクセス可能性そのものの解析を担う。

公式確認先 AWS公式 1 / AWS公式 2

問題 011 | Domain 1 / 監視・性能 | 本番より難しい | 四択（1つ選択）

問題 11 複合アラームによる通知抑制

あるSaaS企業では、1つのリージョンにある注文処理基盤を20個のCloudWatchメトリクスアラームで監視しています。データベース接続枯渇が起きると、APIレイテンシ、キュー滞留、ワーカーエラーなど多数のアラームが同時にALARMになり、同じ当番担当者へ大量の通知が届きます。一方、週2回のデプロイ中は数分間これらのしきい値を超えることが予想されます。

運用チームは次の動作を求めています。

- 通常時は、APIレイテンシ悪化とキュー滞留の両方が起きた場合だけ、重大インシデント用SNSトピックへ1件通知する。
- デプロイ開始アラームがALARMになっている間は重大通知を抑制する。
- デプロイ開始イベントと各メトリクスの発報順が数十秒前後することがあるため、抑制アラームがALARMへ遷移するまで待つ猶予を設ける。
- デプロイ終了直後のメトリクス安定化中も5分間は通知を抑制する。
- 個々のメトリクスアラームはトラブルシューティング用に残すが、そのSNSアクションを毎回手動で無効化しない。

最小の運用負荷で要件を満たす構成はどれですか。

選択肢

A APIレイテンシとキュー滞留の各アラームから同じSNSトピックへ通知する。デプロイ時はEventBridge Schedulerで両アラームのアクションを無効化し、終了5分後に有効化する。

B ALARM(ApiLatency) AND ALARM(QueueBacklog)をルールに持つ複合アラームを作り、重大SNSアクションは複合アラームだけに設定する。デプロイ中アラームをActionsSuppressorに指定し、適切なWaitPeriodと300秒のExtensionPeriodを設定する。

C ALARM(ApiLatency) OR ALARM(QueueBacklog) OR ALARM(DeploymentInProgress)の複合アラームを作成し、デプロイ中アラームがALARMなら複合アラームをINSUFFICIENT_DATAへ変更するLambda関数を起動する。

D 20個のアラームをCloudWatchダッシュボードへ配置し、SNSではなくContributor Insightsルールで同時発生数を集計する。同時に2個以上発生したときだけ通知する。

ここでいったん止める | 解答と解説は次ページ

問題 011 正解・解説 本番より難しい

問題 11の正解・解説

1. 正解

B

2. 問題文の重要な条件

- 重大通知の条件はAPIレイテンシ**かつ**キュー滞留であり、論理積が必要である。
- 元のアラームは可視性のため残すが、ページング通知を集約したい。
- 計画デプロイ中は設定を削除・変更せずアクションだけを抑制したい。
- 抑制開始の競合を吸収する待機時間と、抑制解除後5分の延長時間が必要である。
- 手動操作や独自Lambdaによる状態操作を避けたい。

3. 正解へ至る判断過程

複数アラームの状態を論理式でまとめる要件なので、まず複合アラームを選びます。重大通知を複合アラームに集約し、元のアラームは診断用に維持します。次に、計画作業中だけアクションを止める要件には複合アラームのアクション抑制を使います。ActionsSuppressorWaitPeriodは複合アラームが発報条件に入ってから抑制アラームがALARMになるまで待つ時間、ActionsSuppressorExtensionPeriodは抑制アラームがALARMを離れた後も抑制を継続する時間です。後者を300秒にすれば終了後5分を表現できます。

4. 正解が要件を満たす理由

BではANDルールにより、片方だけの軽微な悪化で重大通知を送りません。ページングアクションを複合アラームだけに置けば、相関した事象を1つの運用シグナルにできます。ActionsSuppressorはアラーム自体の定義や状態評価を消さずにアクションを抑制するため、デプロイ中も元アラームの履歴と状態は観測できます。Wait Periodがイベント順序のずれを吸収し、Extension Periodが終了直後の揺れを吸収します。

5. 各不正解選択肢が不適切な理由

- **A:** 2つの元アラームが別々に通知するためAND条件にも通知集約にもなりません。スケジュールと実際のデプロイ時刻がずれると誤抑制・誤通知が起こり、アクション有効化に失敗する運用リスクも残ります。
- **C:** ORは片方の異常やデプロイ開始だけでも複合アラームを発報させます。また、利用者がLambdaからCloudWatchアラームを任意にINSUFFICIENT_DATA状態へ遷移させ続ける設計は、標準のアクション抑制より複雑で、状態評価との競合も生みます。
- **D:** Contributor Insightsはログから高カーディナリティの上位寄与者などを分析する機能で、CloudWatchアラーム状態を論理結合する機能ではありません。ダッシュボードも可視化であって通知条件の相関を実装しません。

6. 各不正解選択肢が正解になり得る条件

- **Aが適切になる条件:** 各症状を独立した担当チームへ通知する必要があり、計画停止の開始・終了時刻が厳密に固定され、アラームアクションの一括制御を確実に自動化できる場合です。
- **Cが適切になる条件:** 標準抑制では表せない外部承認や複雑な業務状態に基づいて、通知先や処理そのものをLambdaで制御する場合です。その場合もアラーム状態を偽装するより、通知経路側を制御します。
- **Dが適切になる条件:** 目的がログ中のクライアントIP、テナントID、エラーコードなどの上位寄与者を継続集計することで、アラーム相関やページングが不要な場合です。

7. 今後使える判断基準

多数の症状アラームから1件の運用判断を作るときは複合アラームを検討します。ANDは誤検知削減、ORはどれか1つでも重大な場合、NOTは既知状態の除外に使えます。計画作業の抑制では、**抑制開始前の競合をWait Period、終了後の余韻をExtension Period**として読み分けます。抑制は評価を止めるのではなく、アクションを止める機能です。

8. 関連サービスとの比較

- **複合アラーム:** 他のアラーム状態を論理結合し、通知ノイズを減らします。メトリクス自体を直接評価するものではありません。
- **アクション抑制:** 計画作業や既知障害中に複合アラームのアクションを一時抑制します。
- **EventBridge / Scheduler:** 時刻やイベントを契機に処理を起動します。固定時刻の作業には使えますが、アラーム相関の代替ではありません。
- **Contributor Insights:** 構造化ログからTop-N寄与者やユニーク寄与者数を求める分析機能です。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3

問題 012 | Domain 2 / 信頼性・BC | 本番相当 | 四択（1つ選択）

問題 12 履歴のない月末バッチを時刻どおりに

金融会社は、新しい月次集計アプリケーションをEC2 Auto Scalingグループへ移行する。毎月最終営業日の02:00に上流システムから一括ファイルが届き、02:10には40台すべてが処理可能でなければならない。インスタンスの起動と初期化には平均8分かかる。処理は04:00までに終わり、04:30以降は4台へ戻せる。実行日と時刻は業務カレンダーで3か月先まで確定しているが、このAuto Scalingグループには十分な負荷履歴がない。

費用を抑え、初回実行から確実に容量を用意する方法はどれか。

選択肢

A	CPU使用率60%のターゲット追跡だけを設定し、最小4、最大40にする
B	予測スケーリングをForecast and scaleモードで有効にし、履歴が蓄積するまで最大容量を40にする
C	業務カレンダーに従って01:50に希望容量40、04:30に希望容量4へ変更するスケジュール済みアクションを登録する
D	40台分の停止済みインスタンスをAuto Scalingグループ外に保持し、02:00に手動で起動してアタッチする

ここでいったん止める | 解答と解説は次ページ

問題 012 正解・解説 本番相当

問題 12の正解・解説

1. 正解

C

2. 問題文の重要な条件

- 日時と必要台数が事前に確定している。
- 初回から間に合わせる必要がある。
- 予測に使える履歴がない。
- 終了後は速やかに縮小してよい。

3. 正解へ至る判断過程

既知の時刻に既知の容量が必要なら、実負荷を観測してから反応する必要はない。起動時間を逆算したスケジュール済みアクションで希望容量を上げ、終了後に戻すのが直接的である。予測スケーリングは履歴から日次・週次パターンを予測するため、履歴のない初回と特殊な営業日カレンダーには不向きである。

4. 正解が要件を満たす理由

スケジュール済みスケーリングは、特定日時または繰り返しスケジュールで最小・最大・希望容量を変更できる。本問では01:50に増やすことで、8分の初期化を含めても02:00前後に40台を用意できる。04:30の縮小により常時40台を維持する費用も避けられる。

5. 各不正解選択肢が不適切な理由

- A：CPUが上がってから起動するため、02:10の期限に間に合わない可能性が高い。
- B：十分な履歴がなく、最終営業日という不規則なカレンダーも単純な日次・週次パターンではない。
- D：手動作業とグループ外インスタンスの管理が必要で、失敗時の再現性や監査性が低い。

6. 各不正解選択肢が正解になり得る条件

- A：起動時間が非常に短く、到着量も不確実で、処理開始後の自動追従を優先する場合。
- B：十分な履歴があり、負荷が日次・週次の繰り返しとして予測可能な場合。
- D：Auto Scalingを利用できない特殊なライセンス制約があり、手順化された人手運用を受容する場合。

7. 今後使える判断基準

「時刻と台数が既知」ならスケジュール、「時刻は規則的だが台数が履歴から変動」なら予測、「発生時刻も量も不明」なら動的スケーリングを中心に考える。初期化時間がある場合は、必要時刻ではなく、その時間だけ前倒しして容量を増やす。

8. 関連サービスとの比較

予測スケーリングは日次・週次の繰り返しから将来容量を予測する。ターゲット追跡とステップスケーリングは現在のメトリクスに反応する。ウォームプールは不規則な急増に対する起動遅延を短縮するが、既知の台数を既知の時刻に用意する本問ではスケジュール済みアクションの方が単純である。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3

問題 013 | Domain 3 / 展開・自動化 | 本番相当 | 四択（1つ選択）

問題 13 ロールバックとTermination Protectionの境界

ある本番CloudFormationルートスタックは、ネットワークとアプリケーションのNested Stackを含んでいます。過去に運用者がルートスタックを誤って削除しかけたため、スタック階層全体の偶発的なDeleteStackを防ぐ必要があります。一方、通常のスタック更新は継続し、更新中にリソース作成や変更が失敗した場合は、部分的な変更を残さず直前の安定状態へ自動的にロールバックさせたいと考えています。

将来、特定のデータベースについて更新時の置換まで防ぐ必要が生じた場合は、それも別の制御として追加できる構成にします。要件を最も正確に満たす設定はどれですか。

選択肢

A 各Nested Stackへ個別にTermination Protectionを有効化し、ルートスタックではロールバックを無効化する。これにより子スタックの更新・置換もすべて禁止され、失敗時は自動的に元へ戻る。

B データベースへDeletionPolicy: Retainだけを設定する。これによりルートスタックのDeleteStack自体が拒否され、Nested Stackやその他のリソースも削除されない。

C ルートスタックでTermination Protectionを有効化し、更新の自動ロールバックは既定どおり有効のままにする。Termination Protectionは明示的なスタック削除を防ぐ制御であり、通常更新や更新ロールバックを止めない。特定リソースの更新・置換を防ぐ必要があれば、別途スタックポリシーを使用する。

D ルートスタックでTermination Protectionを有効化し、すべての作成・更新でdisable-rollbackを指定する。Termination Protectionが失敗した変更を元へ戻すため、ロールバックを無効化しても部分更新は残らない。

ここでいったん止める | 解答と解説は次ページ

問題 013 正解・解説 本番相当

問題 13の正解・解説

1. 正解

C

2. 問題文の重要な条件

- 防ぎたいのは、運用者によるルートスタック全体の偶発的な削除である。
- Nested Stackを含むため、Termination Protectionはルートで管理する。
- 通常の更新は許可する。
- 更新失敗時は部分状態を残さず、自動ロールバックさせる。
- Termination Protection、ロールバック無効化、DeletionPolicy、スタックポリシーの目的を混同しない。

3. 正解へ至る判断過程

最初に、保護する操作を特定します。Termination Protectionは、保護されたスタックへの明示的な削除要求を拒否する機能です。ルートスタックで有効化するとNested Stackへも設定が伝わり、Nested Stack側で個別に有効・無効を変更しません。ただし、スタック更新の一部としてCloudFormationがリソースやNested Stackを削除・置換することまでは防ぎません。

次に、失敗時の挙動を分けます。ロールバックを有効のままにすれば、更新失敗時にCloudFormationは更新前の安定状態へ戻そうとします。disable-rollbackまたは「正常にプロビジョニングされたリソースを保持」は、失敗した作成を調査するため部分状態を残す用途であり、本番の自動復旧要件とは逆です。重要DBの更新を防ぐなら、スタック更新操作を制限するスタックポリシーを別に使います。

4. 正解が要件を満たす理由

Cでは、誤操作によるDeleteStackはTermination Protectionで拒否されます。保護をルートに設定することで子スタック階層も対象になります。一方、デプロイは通常どおり実行でき、更新失敗時は既定の自動ロールバックが働きます。スタック全体の削除防止と、個別リソースの更新防止を別々の制御にしているため、必要以上に正常なデプロイを止めません。

5. 各不正解選択肢が不適切な理由

- **A:** Nested StackのTermination Protectionは子スタックから個別変更できず、ルートで設定します。ロールバックを無効化すると失敗時に部分状態を保持するので、「自動的に元へ戻る」とも矛盾します。Termination Protectionは更新全般を禁止しません。
- **B:** DeletionPolicy: Retainは、その論理リソースが削除対象になったとき物理DBなどを保持する属性です。スタックへの削除要求そのものを拒否せず、ほかのリソースやNested Stackを保護しません。
- **D:** Termination Protectionはロールバックエンジンではありません。ロールバックを無効化した操作が失敗すると、成功済みリソースを含む部分状態をトラブルシューティング用に残すため、本問の自動復元要件を満たしません。

6. 各不正解選択肢が正解になり得る条件

- **Aが適切になる条件:** 適切になる部分は「スタック階層を削除から守る」という目的ですが、実際にはルートでTermination Protectionを設定します。失敗した状態を調査したい場合だけ、対象操作でロールバック無効化を検討します。
- **Bが適切になる条件:** スタック自体の削除は許可しつつ、データを持つS3、RDS、EBSなど特定の物理リソースだけを残したい場合です。

- **Dが適切になる条件:** 開発・調査環境の新規作成で、失敗原因を確認するため成功済みリソースを意図的に保持したい場合です。調査後の修復または削除手順が必要です。

7. 今後使える判断基準

Termination Protectionはスタック削除API、ロールバック設定は作成・更新失敗時、DeletionPolicyは論理リソース削除時の物理リソース、スタックポリシーは更新時のリソース操作を制御します。似た「保護」という言葉でも対象操作が違います。UPDATE_ROLLBACK_FAILEDになった場合は原因を修正してContinueUpdateRollbackを使い、スキップしたリソースは次回更新前にテンプレートと整合させます。

8. 関連サービスとの比較

- **Termination Protection:** 明示的なスタック削除を拒否します。Nested Stackではルートから設定します。
- **Stack failure options / disable rollback:** 失敗時に成功済みリソースを保持して調査するか、元へ戻すかを制御します。
- **スタックポリシー:** 更新時に特定リソースへ許可する更新アクションを制限します。
- **DeletionPolicy / UpdateReplacePolicy:** 削除または置換される物理リソースの保持・スナップショット動作を指定します。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4

問題 014 | Domain 5 / ネットワーク | 本番より難しい | 四択（1つ選択）

問題 14 インターフェイスエンドポイントの名前解決

会社はインターネット接続を持たないVPCのプライベートサブネットでEC2を運用している。Systems Managerのために必要なインターフェイスVPCエンドポイントを作成し、エンドポイントのセキュリティグループではEC2サブネットからのHTTPSを許可した。VPCではDNS resolutionとDNS hostnamesを有効にしている。しかしEC2上のSSM Agentは、ssm.<region>.amazonaws.comへ接続できないと記録している。名前を引くとパブリックIPアドレスが返る。独自DNSサーバーは使用していない。

最小の変更で、標準のAWSサービス名を変えずに非公開接続させる方法はどれか。

選択肢

A	プライベートサブネットにNATゲートウェイへのデフォルトルートを追加する。
B	EC2の/etc/hostsへ、エンドポイントENIのIPアドレスを固定登録する。
C	インターフェイスエンドポイントをゲートウェイエンドポイントへ変更する。
D	各インターフェイスエンドポイントでPrivate DNSを有効にし、必要なエンドポイント一式が同じVPCにあることを確認する。

ここでいったん止める | 解答と解説は次ページ

問題 014 正解・解説 本番より難しい

問題 14の正解・解説

1. 正解

D

2. 問題文の重要な条件

VPCのDNS機能は有効、独自DNSはなく、エンドポイントのSGも許可済みだが、標準サービス名がパブリックIPへ解決されている。これは経路より名前解決の問題を示す。

3. 正解へ至る判断過程

インターフェイスエンドポイントのPrivate DNSを有効にすると、サービスの標準リージョナルDNS名がVPC内ではエンドポイントENIのプライベートIPへ解決される。Systems Managerは機能に応じてSSM、SSM Messagesなど複数の接続先を使うため、必要なエンドポイントが揃っていることも確認する。

4. 正解が要件を満たす理由

アプリケーションやAgent側のURLを変更せず、通信をAWS PrivateLink経由へ切り替えられる。NATやインターネットゲートウェイを追加しないため、非公開接続という制約も維持する。

5. 各不正解選択肢が不適切な理由

A: 接続自体は可能になり得るが、インターネットを経由しないという設計目的を崩し、NAT料金も発生する。
B: エンドポイントENIのアドレス変更やAZ追加に弱く、マネージドDNSを使うべき構成を手作業にする。
C: Systems Managerはゲートウェイエンドポイントの対象ではない。
D: 正解肢のため対象外。

6. 各不正解選択肢が正解になり得る条件

Aは、PrivateLink非対応の外部サービスにも接続が必要なら候補になる。Bは短時間の診断には使えても恒久策にはしない。CはS3またはDynamoDBへVPC内から接続し、ゲートウェイエンドポイントの制約で足りる場合に適する。

7. 今後使える判断基準

「インターフェイスエンドポイントを作ったのに標準名がパブリックIPを返す」なら、Private DNS、VPC DNS属性、必要エンドポイント、エンドポイントSGの順で調べる。

8. 関連サービスとの比較

インターフェイスエンドポイントはENIとPrivate DNSを使い、多くのAWSサービスに対応する。S3/DynamoDBのゲートウェイエンドポイントはルートテーブルへ経路を追加し、時間料金やデータ処理料金がない一方、利用経路に制約がある。

公式確認先 AWS公式 1 / AWS公式 2

問題 015 | Domain 4 / セキュリティ | 本番より難しい | 四択（1つ選択）

問題 15 別アカウントのKMSキーで復号できない

ログ保管アカウントのS3バケットは、同アカウントのカスタマーマネージドKMSキーで暗号化されている。分析アカウントのAuditRoleには、対象バケットのGetObjectとKMSキーARNに対するkms:Decryptを許可するIAMポリシーを付与した。しかしS3オブジェクト取得時にKMSのAccessDeniedとなる。S3バケットポリシーはAuditRoleの読み取りを既に許可し、明示的Denyはない。

最小権限で修正するにはどうすべきか。

選択肢

A	分析アカウントのデフォルトAWS管理KMSキーを、ログ保管アカウントと共有する。
B	S3オブジェクトをSSE-S3へ暗号化し直し、KMSを使用しない。
C	AuditRoleへkms:*をResource *で追加する。
D	ログ保管アカウント側のKMSキーポリシーで分析アカウントまたはAuditRoleへ必要な復号権限を許可し、分析アカウント側IAM許可と組み合わせる。

ここでいったん止める | 解答と解説は次ページ

問題 015 正解・解説 本番より難しい

問題 15の正解・解説

1. 正解

D

2. 問題文の重要な条件

KMSキーと呼び出しロールが別アカウントで、IAM側だけは許可済み。S3認可は通るがKMSで拒否されている。

3. 正解へ至る判断過程

KMSのクロスアカウント利用には、キー所有アカウントのkey policyによる外部アカウント/主体への許可と、呼び出し元アカウントのIAM policyによる委任の両方が必要である。片側だけのAllowでは成立しない。

4. 正解が要件を満たす理由

対象キー、対象ロール、kms:Decryptなど必要操作へ絞って二つのポリシーを揃えられる。暗号化方式を弱めたり、全KMS操作へ広げたりせずに済む。

5. 各不正解選択肢が不適切な理由

A: AWS管理KMSキーは一般に任意のクロスアカウント共有用にキーポリシーを編集できず、問題の対象キーとも異なる。
B: 機能要件を落とす不要な再暗号化で、最小変更ではない。
C: 呼び出し側IAMを広げても、キー側policyがクロスアカウント利用を認めなければ無効であり、過剰権限でもある。
D: 正解肢のため対象外。

6. 各不正解選択肢が正解になり得る条件

Bは顧客管理キーによる監査・分離が不要でSSE-S3で十分な新規設計なら選択肢になり得る。Cの広い権限は限定された緊急診断でも避け、操作とキーを特定する。Aは同一アカウント内でAWS管理キーを使う通常用途に限る。

7. 今後使える判断基準

クロスアカウントKMSは「キー所有側key policy」と「呼び出し側IAM policy」の二面を見る。S3許可があっても、暗号化オブジェクトではKMS許可が別途必要である。

8. 関連サービスとの比較

S3 bucket policyはオブジェクトへのアクセス、KMS key policyはデータキー復号を制御する。SCPやpermissions boundaryのDeny/上限も両方のAllowより優先して最終権限へ影響する。

公式確認先 AWS公式 1 / AWS公式 2

問題 016 | Domain 1 / 監視・性能 | 複合難問 | 複数選択（5つから2つ選択）

問題 16 Organizations全体のクロスアカウント監視

ある企業はAWS Organizationsで120のAWSアカウントを管理しており、毎月複数の新規アカウントが追加されます。ワークロードは東京と大阪の両リージョンに分散し、各アプリケーションチームは自分のアカウント内でCloudWatchメトリクス、CloudWatch Logs、X-Rayトレースを保持しています。中央SREチームは専用の監視アカウントから、次の操作を行いたいと考えています。

- アカウント境界を越えてメトリクス、ログ、トレースを検索・可視化する。
- 東京と大阪の主要指標を1つのCloudWatchダッシュボードで比較する。
- テレメトリを別ストレージへ複製せず、ソースアカウントに保持したまま参照する。
- 監視アカウントへ業務リソース全般の読取り権限を与えない。
- 指定したOUへ追加された新規アカウントも、個別の手作業を最小限にして監視対象へ加える。

要件を満たすために実施すべき対応はどれですか。（2つ選択）

選択肢

A 各対象リージョンの監視アカウントにCloudWatch Observability Access Manager（OAM）のsinkを作成し、Organizationsの組織IDまたはOUを条件とするsinkポリシーを設定する。ソースアカウントには、共有するメトリクス、ログ、トレースを選択したlinkを作成する仕組みを組織単位で展開する。

B 管理アカウントにマルチリージョンのCloudTrail組織証跡を作成し、CloudWatch Logsへ配信する。監視アカウントは、そのロググループを共有されれば各アカウントのアプリケーションメトリクスとX-Rayトレースも自動的に参照できる。

C 全ソースアカウントでCloudWatch Metric Streamsを有効にし、Firehoseで監視アカウントのS3バケットへ配信する。ログはサブスクリプションフィルターで複製し、X-Rayトレースは毎分のLambdaでエクスポートして、監視アカウントへデータを集約する。

D 監視アカウントから各ソースアカウントのOrganizationAccountAccessRoleを引き受け、CloudWatch、Logs、X-Rayに加えて全AWSサービスの読取り権限を利用する。ダッシュボード閲覧時にLambdaが各アカウントへ順番にAssumeRoleする。

E OAMのlinkとsinkはリージョナルであることを前提に各リージョンで構成し、監視アカウントにクロスアカウント・クロスリージョンのCloudWatchダッシュボードを作成する。ウィジェットでソースアカウントとリージョンを指定し、必要に応じて同じ監視アカウントから各リージョンの共有ログやトレースを調査する。

ここでいったん止める | 解答と解説は次ページ

問題 016 正解・解説 複合難問

問題 16の正解・解説

1. 正解

A、E

2. 問題文の重要な条件

- メトリクスだけでなく、CloudWatch LogsとX-Rayトレースもアカウント横断で扱う。
- データを中央へコピーせず、ソースアカウントのテレメトリを共有する。
- 東京・大阪という複数リージョンを1つの運用ビューへまとめる。
- 監視専用の最小権限とし、業務リソース全般への読取りを許可しない。
- アカウント数が増え続けるため、OrganizationsまたはOU単位のオンボーディングが必要である。

3. 正解へ至る判断過程

まず、中央へデータを再取り込みせずにCloudWatchのテレメトリを共有する要件から、OAMを基盤とするCloudWatchクロスアカウントオブザーバビリティを選びます。監視アカウント側にsink、各ソースアカウント側にlinkを作り、両側が許可したテレメトリ種別だけを共有します。Organizationsを利用すれば、個別アカウントIDを列挙する方式より新規アカウントを取り込みやすくなります。

次にリージョン境界を確認します。OAMのsinkとlinkはリージョナルなので東京用と大阪用の構成が必要です。一方、CloudWatchダッシュボードのウィジェットにはアカウントとリージョンを指定できるため、監視アカウントの1つのダッシュボードへ両リージョンの主要メトリクスを並べられます。

4. 正解が要件を満たす理由

Aにより、監視アカウントは共有された観測データを自アカウントのデータに近い操作感で検索・可視化できます。共有対象はメトリクス、ログ、トレースなどから選択でき、一般的な業務リソースの読取りロールを渡す必要がありません。OrganizationsまたはOUを許可するsinkポリシーと組織展開されたlinkにより、アカウント追加時の作業を減らせます。

Eは、リージョナルな共有構成と、クロスリージョン表示という別の層を正しく組み合わせています。ダッシュボードは東京と大阪を同時表示し、詳細調査では対象リージョンにリンクされたログ・トレースを監視アカウントから利用できます。

5. 各不正解選択肢が不適切な理由

- **B:** CloudTrailはAWS APIやアカウントアクティビティの監査証跡です。組織証跡を作っても、アプリケーションのCloudWatchメトリクスやX-Rayトレースが共有されるわけではありません。
- **C:** 技術的に個別の転送パイプラインを構築できる部分はありますが、データを複製しないという要件に反します。メトリクス、ログ、トレースごとの転送・再取込み・失敗処理・保存費用も発生し、OAMより運用負荷が大きくなります。
- **D:** AWS Organizationsで新規アカウント作成時に用いられる管理ロールを中央監視の常用経路にすると、監視に不要な広い権限を持たせます。逐次AssumeRoleと独自集約Lambdaも、CloudWatchのネイティブな横断検索やダッシュボードより複雑です。

6. 各不正解選択肢が正解になり得る条件

- **Bが適切になる条件:** 目的がIAM変更、EC2操作、KMS操作などのAPI監査を全アカウントから中央収集することで、アプリケーションテレメトリの横断監視が不要な場合です。

- **Cが適切になる条件:** SIEMや独自時系列基盤へデータを恒久的に集約する必要があり、変換、長期保管、AWS外への配信が要件で、複製コストとパイプライン運用を許容できる場合です。
- **Dが適切になる条件:** 一時的な調査でCloudWatch以外の多数のAWSリソース設定まで確認する必要があり、厳格に限定した監査ロールを各アカウントで引き受ける場合です。それでも広い管理用ロールの流用は避けます。

7. 今後使える判断基準

クロスアカウント監視では、**閲覧を共有するのか、データを転送・複製するのか**を最初に分けます。OAMは同一リージョン内のテレメトリ共有、Metric Streamsやサブスクリプションは別基盤への継続配信です。複数リージョンでは「リージョンごとの共有構成」と「ダッシュボード上の横断表示」を別々に設計します。Organizations連携は、新規アカウントが増える環境で個別ID管理を減らす重要な条件です。

8. 関連サービスとの比較

- **CloudWatchクロスアカウントオブザーバビリティ（OAM）:** メトリクス、ログ、トレースなどをソースに保持したまま監視アカウントから利用します。
- **クロスアカウント・クロスリージョンダッシュボード:** 複数アカウント・リージョンのウィジェットを1つの画面へ配置します。共有権限の土台は別途必要です。
- **CloudWatch Metric Streams:** メトリクスをFirehoseなどへ低遅延で継続配信する用途です。ログやトレースの共有機能ではありません。
- **CloudTrail組織証跡:** 全アカウントのAPI監査イベントを中央化します。性能・アプリケーション監視とは目的が異なります。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4

問題 017 | Domain 2 / 信頼性・BC | 本番より難しい | 四択（1つ選択）

問題 17 先回りと想定外への追従を両立する

動画配信サービスのトランスコード受付APIは、9か月にわたり平日18時と週末昼に同じような負荷上昇を繰り返している。EC2インスタンスが利用可能になるまで12分かかるため、現在のターゲット追跡だけでは上昇直後に短時間のスロットリングが発生する。一方、スポーツ中継の延長などにより、予測を30〜50%上回る日もある。運用チームは、平常パターンには負荷上昇前から備え、予測外の増加にも自動対応し、固定スケジュールを毎週修正する作業は避けたい。

最も適切なスケーリング構成はどれか。

選択肢

A	12分前に最大容量まで増やすスケジュール済みアクションだけを、平日と週末でそれぞれ作成する
B	ターゲット追跡を削除し、予測スケーリングをForecast onlyモードで設定する
C	最小容量を過去9か月の最大必要台数へ引き上げ、スケーリングポリシーをすべて削除する
D	予測スケーリングで反復パターンに先回りし、ターゲット追跡も併用して予測外の実負荷を補正する。必要に応じてスケジューリングバッファまたは十分な前倒し時間を設定する

ここでいったん止める | 解答と解説は次ページ

問題 017 正解・解説 本番より難しい

問題 17の正解・解説

1. 正解

D

2. 問題文の重要な条件

- 十分な履歴と日次・週次パターンがある。
- 起動に12分かかるため、反応型だけでは遅い。
- 予測を上回る日があり、予測だけでも不足する。
- 固定スケジュールの保守を減らしたい。

3. 正解へ至る判断過程

規則的な部分は予測スケーリングで先回りできる。しかし、予測は保証ではなく、突発的な上振れには実測値に反応する動的スケーリングが必要である。AWSも予測スケーリングと動的スケーリングを組み合わせる構成を示している。

4. 正解が要件を満たす理由

予測スケーリングは履歴から将来の需要を推定し、予測した時刻より前に容量を用意できる。ターゲット追跡は実際の利用率・スループットが目標を超えた際に追加容量を要求する。この組み合わせにより、通常の山では起動遅延を隠し、延長戦などの外れ値では反応型ポリシーが補完する。

5. 各不正解選択肢が不適切な理由

- A：最大容量までの固定増設は過剰になりやすく、試合予定や季節変化のたびに保守が必要。
- B：Forecast onlyは予測を表示するだけで容量を変更しない。さらにターゲット追跡を削除すると上振れへ対応できない。
- C：性能は満たしやすいが、常時最大規模を維持するため費用要件を無視している。

6. 各不正解選択肢が正解になり得る条件

- A：容量が時刻ごとに契約で固定され、負荷履歴より業務予定表の方が正確な場合。
- B：本番投入前に予測精度だけを評価し、まだ自動変更を許可しない検証段階。
- C：数分の容量不足も許されず、最大負荷用の常時確保費用を受容する場合。

7. 今後使える判断基準

予測スケーリングは「先回り」、動的スケーリングは「現実との差分補正」と考える。起動に時間がかかり、履歴に反復性があるときは併用価値が高い。Forecast onlyは観察用、Forecast and scaleが実際の容量変更を行う。

8. 関連サービスとの比較

スケジュール済みアクションは時刻と容量を人が決める。予測スケーリングは履歴から必要容量を決める。ウォームプールは起動工程を短縮する別の手段で、需要予測そのものは行わない。必要なら、予測＋動的スケーリングにウォームプールを追加することもできる。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3

問題 018 | Domain 3 / 展開・自動化 | 複合難問 | 複数選択（5つから2つ選択）

問題 18 Nested StackとSecret更新の境界を設計する

ある企業は、1つのルートスタックからNetworkChild、DataChild、AppChildの3つのNested Stackを作成しています。各子テンプレートはバージョン付きのS3オブジェクトURLで参照され、ルートスタックがパラメータを渡します。DataChild内のRDS DBインスタンスは、Secrets Managerのシークレットから次のようなバージョン指定なしのDynamic Referenceでマスターパスワードを取得しています。

{{resolve:secretsmanager:prod/db:SecretString:password}}

次のリリースではAppChildだけを変更します。SREチームはスタック階層全体の変更を事前確認し、子スタックを独立運用してルートとの整合性を失うことを避けたいと考えています。また、DBシークレットをSecrets Manager側で手動ローテーションしたところ、シークレットのAWSCURRENTは新しくなりましたが、RDSには古いマスターパスワードが残っています。CloudFormationで更新する場合の正しい挙動も運用手順へ明記する必要があります。

要件を満たす記述はどれですか。（2つ選択）

選択肢

A AppChildの物理子スタックへ直接UpdateStackを実行する。子スタックは独立したスタックなので、ルートスタックのテンプレートや次回更新と無関係に永続的な管理境界として扱える。

B AppChildの新しいTemplateURLまたは入力パラメータをルートテンプレートへ反映し、ルートスタックからNested Stackを含むChange Setを作成する。CLIでは必要に応じて--include-nested-stacksを使用し、階層内の差分を確認してルートChange Setから実行する。CloudFormationは階層を確認するが、実際のリソース変更は差分があるNested Stack内だけで行われる。

C Secrets Managerでシークレット値を変更した時点で、CloudFormationがDynamic Referenceの変更イベントを受信し、テンプレートが不変でも直ちにRDSへ新しいパスワードを設定する。スタック操作は不要である。

D 通常のローテーションに追従しやすいよう、Dynamic Referenceはversion-idやversion-stageを固定しない。Secrets Managerの値だけを変更してもCloudFormationは再取得しないため、CloudFormationからRDSへ新値を適用するなら、DataChild内のDynamic Referenceを含むRDSリソースに実際の変更を加え、ルートからスタック更新を実行して新しいAWSCURRENTを解決させる。

E DataChildのOutputsへ解決済みパスワードを出力し、ルートからAppChildへ平文パラメータとして渡す。これによりルート更新のたびに必ずシークレットが再解決され、Change Setとスタックイベントにも値を表示して確認できる。

ここでいったん止める | 解答と解説は次ページ

問題 018 正解・解説 複合難問

問題 18の正解・解説

1. 正解

B、D

2. 問題文の重要な条件

- 3つの子スタックはルートスタックがAWS::CloudFormation::Stackリソースとして所有する。
- Appだけを変更し、変更のないNetwork・Dataへ不要な更新を行わない。
- Change SetでNested Stack階層の差を確認し、実行境界をルートへ揃える。
- Dynamic ReferenceはバージョンAWSCURRENTを参照する。
- Secrets Managerの値だけを変えてもCloudFormationスタック更新は自動起動しない。
- シークレットの解決済み値をテンプレート、Outputs、ログへ露出させない。

3. 正解へ至る判断過程

まずNested Stackの所有境界を確認します。子スタックはルートテンプレート内のリソースであり、更新は原則としてルートから開始します。新しいAppテンプレートURLまたはパラメータをルートへ反映し、Nested Stackを含むChange Setを作れば、階層内の予定変更をたどれます。CLIでは--include-nested-stacksが必要で、作成された子Change Setの実行・削除もルートChange Setを起点に行います。ルート更新時にはCloudFormationが各Nested Stackを確認しますが、実際には対応するテンプレートに差分があるリソースだけを更新します。

次にDynamic Referenceの「参照先の値」と「CloudFormationの更新契機」を分けます。バージョンなし参照は解決時点のAWSCURRENTを使いますが、Secrets Managerで値が変わったこと自体はスタック更新を起動しません。CloudFormationは、Dynamic Referenceを含むリソースを作成または変更するときに値を取得します。したがってCloudFormationからRDSへ新値を渡すには、そのRDSリソースに実際の変更を生じさせたスタック更新が必要です。

4. 正解が要件を満たす理由

Bは、ルートを唯一のデプロイ境界として保ちながら、App子スタックだけを更新します。階層Change Setにより、親パラメータ変更が子へ及ぼす影響や、子内部の追加・変更・置換も実行前に確認できます。

Dは、シークレットのバージョンをテンプレートへ固定せず、ローテーション時のAWSCURRENTを参照できる形を維持します。同時に「シークレット変更だけではCloudFormationは何もしない」という重要な制約を正しく扱っています。なお、Secrets ManagerのRDS向け自動ローテーションを使用する場合はローテーション処理自身がDB資格情報も更新できるため、CloudFormation更新に依存しない運用も検討できます。

5. 各不正解選択肢が不適切な理由

- **A:** Nested Stackを直接更新すると、ルートテンプレートが表す期待状態と実子スタックがずれ、後続のルート更新やロールバックを複雑にします。AWSはNested Stackの更新をルートから開始するよう案内しています。
- **C:** Dynamic ReferenceはSecrets Manager変更イベントに追従して自動的に対象リソースを更新する監視機能ではありません。シークレット値だけの変更では、CloudFormationは新値を取得せず、RDSもCloudFormation経由では更新されません。
- **E:** Dynamic Referenceの目的は解決済みシークレットをCloudFormationのテンプレートやログへ残さないことです。秘密値をOutputや通常パラメータへ渡す設計は漏えいリスクを増やします。また、secure dynamic referenceの解決値を確認用に表示する発想自体が不適切です。

6. 各不正解選択肢が正解になり得る条件

- **Aが適切になる条件:** 対象がNested Stackではなく、ライフサイクルと所有者を完全に分離した独立スタックである場合です。独立スタック間の値共有にはExport/ImportValueやパラメータストアなどを検討します。
- **Cが適切になる条件:** Secrets Managerの自動ローテーションLambdaが、シークレットだけでなくRDS上のパスワードもローテーション手順の一部として更新する構成なら、DBはCloudFormation更新なしで新資格情報へ移行できます。ただし、それはDynamic Referenceが自動更新した結果ではありません。
- **Eが適切になる条件:** 子スタックから非機密のARN、サブネットID、エンドポイントなどをOutputsで親へ返す場合です。解決済み秘密値は対象にしません。

7. 今後使える判断基準

Nested Stackは、**テンプレート再利用の単位であって、親から独立して更新する運用単位ではない**と整理します。変更はルートから開始し、変更された子だけが更新されます。Dynamic Referenceは「テンプレートへ秘密を書かない解決方式」であり、「参照先の変更を監視してリソースを自動更新する方式」ではありません。参照値、解決時点、ローテーション実行主体を分けて判断します。

8. 関連サービスとの比較

- **Nested Stack:** 同じライフサイクルの大規模テンプレートを、再利用可能な子テンプレートへ分割します。
- **Cross-stack reference:** 独立スタック間でOutputsをExportしFn::ImportValueで参照します。更新・削除の結合に注意が必要です。
- **Secrets Manager Dynamic Reference:** CloudFormationが作成・更新時に秘密を解決し、テンプレートへの平文埋込みを避けます。
- **Secrets Manager自動ローテーション:** ローテーション関数がシークレットと対象サービス側資格情報の両方を段階的に変更します。Dynamic Referenceの再解決とは別の仕組みです。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4

問題 019 | Domain 5 / ネットワーク | 本番相当 | 四択（1つ選択）

問題 19 VPCピアリングの推移的ルーティング

共有サービスVPCを中心に、20個のアプリケーションVPCが同一リージョンで稼働している。各アプリケーションVPCは共有サービスVPCとのVPCピアリングを持ち、CIDRは重複していない。新要件として、アプリケーションVPC同士もプライベートIPで通信する必要が生じた。運用担当者は、共有サービスVPCを経由するルートを各VPCへ追加したが通信できない。将来はVPCが50個まで増える予定で、接続とルート管理を簡素化したい。

最適な対応はどれか。

選択肢

A	共有サービスVPCでIP forwardingを有効にし、既存のピアリングをそのまま使う。
B	各VPCをAWS Transit Gatewayへアタッチし、Transit Gatewayルートテーブルで到達性を制御する。
C	各アプリケーションVPCの間にフルメッシュのVPCピアリングを追加する。
D	共有サービスVPCにNATゲートウェイを配置し、各VPCのプライベートCIDRをNAT経由へ向ける。

ここでいったん止める | 解答と解説は次ページ

問題 019 正解・解説 本番相当

問題 19の正解・解説

1. 正解

B

2. 問題文の重要な条件

VPCピアリングを中継して通信しようとしていること、20から50 VPCへ増えること、ルート管理を簡素化しつつ到達性を制御したいことが中心である。

3. 正解へ至る判断過程

VPCピアリングは推移的ルーティングをサポートしないため、A-共有、共有-Bという2本の接続だけではA-B間を中継できない。Transit Gatewayは多数のVPCをハブへ集約し、ルートテーブルの関連付けと伝播で分離や共有を管理できる。

4. 正解が要件を満たす理由

VPC数に比例したアタッチメントでハブ・アンド・スポークを構成でき、50 VPCでもフルメッシュより管理対象を大幅に減らせる。Transit Gatewayルートテーブルを分ければ、環境ごとの通信許可も表現できる。

5. 各不正解選択肢が不適切な理由

A: VPC側でIP forwardingを有効にしても、ピアリング自体の非推移性は変わらない。
B: 正解肢のため対象外。
C: 技術的には直接通信できるが、接続数とルートが二次関数的に増え、50 VPCという将来要件に不向きである。
D: NATゲートウェイはVPC間の推移的ルーターではなく、プライベートCIDR間接続の解決策ではない。

6. 各不正解選択肢が正解になり得る条件

Cは、VPCがごく少数で、高帯域の直接接続を安価に保ちたい場合に有力である。AはEC2ルーターやセキュリティアプライアンスを意図的に中継させる別設計なら一部必要だが、ピアリングの制約は別途回避する必要がある。Dはインターネットへのipv4送信変換に使う。

7. 今後使える判断基準

少数・1対1・低コストならVPCピアリング、多数VPC・推移的接続・集中ルート制御ならTransit Gatewayと判断する。

8. 関連サービスとの比較

AWS PrivateLinkはサービス提供側を一方向に公開し、利用側にサービスCIDR全体を見せたくない場合に適する。Transit Gatewayはネットワーク間の広い到達性、VPCピアリングは2 VPC間の直接到達性を提供する。

公式確認先 AWS公式 1 / AWS公式 2

問題 020 | Domain 4 / セキュリティ | 本番より難しい | 四択（1つ選択）

問題 20 短命な暗号化権限をサービスへ委任する

バックアップサービスが、数時間だけカスタマーマネージドKMSキーを使用して大量のリソースを暗号化する。ジョブごとに利用主体と許可操作を限定し、ジョブ完了後は権限を失効させたい。中央チームは、短命なジョブのたびに長大なkey policyを編集して反映・復元することを避けたい。サービス統合が一時的な暗号化権限を代理作成できるようにする必要もある。

最適な仕組みはどれか。

選択肢

A	キーエイリアスをジョブごとに付け替え、終了後に削除する。
B	必要な暗号操作と制約を持つAWS KMS grantを作成し、完了後にretireまたはrevokeする。key policyでは必要なCreateGrantを条件付きで許可する。
C	KMSキーを毎回無効化し、ジョブ開始時だけ有効化する。
D	全サービスプリンシパルへkms:*を許可する単一のIAMポリシーを作る。

ここでいったん止める | 解答と解説は次ページ

問題 020 正解・解説 本番より難しい

問題 20の正解・解説

1. 正解

B

2. 問題文の重要な条件

権限は一時的、ジョブ単位で主体と操作を限定、完了後に失効、key policyの頻繁な編集を避け、AWSサービス統合が関与する。

3. 正解へ至る判断過程

KMS grantは特定grantee principalへ暗号操作等を委任する独立した認可手段で、作成後にretire/revokeできる。AWSサービスは利用者に代わってgrantを作ることがあり、kms:GrantIsForAWSResourceなどの条件でCreateGrantを絞れる。

4. 正解が要件を満たす理由

恒久ポリシーをジョブごとに書き換えず、必要最小限の操作とencryption context等の制約を持つ短命権限を管理できる。終了時のrevokeにより明示的に失効できる。

5. 各不正解選択肢が不適切な理由

A: aliasはキーを識別しやすくする名前であり、利用権限を付与・失効させる仕組みではない。
B: 正解肢のため対象外。
C: キー全体を無効化すると同じキーを使う他ワークロードも停止し、主体別の権限制御にならない。
D: 恒久的かつ過剰で、ジョブ単位の失効・制約を満たさない。

6. 各不正解選択肢が正解になり得る条件

Aはアプリケーションから論理名でキーを参照し、ローテーションや切替を容易にする場合に使う。Cはキー利用を緊急に全面停止するインシデント対応で使う。Dが正解になる通常条件はなく、必ず主体・キー・操作を絞る。

7. 今後使える判断基準

恒久的な基本アクセスはkey/IAM policy、一時的・サービス統合・取り消し可能な委任はKMS grantを検討する。grantもkey policy等と合わせて評価される。

8. 関連サービスとの比較

STSは一時的なAWS認証情報、KMS grantは特定KMSキーへの一時的な認可手段である。両者は似た「短命」でも、認証情報とキー利用権限という対象が異なる。

公式確認先 AWS公式 1 / AWS公式 2

問題 021 | Domain 1 / 監視・性能 | 本番相当 | 四択（1つ選択）

問題 21 CloudWatch Logs分析機能の使い分け

あるマルチテナント型Webサービスは、JSON形式のアプリケーションログを20個のCloudWatch Logsロググループへ出力しています。各イベントにはtenantId、requestId、durationMs、responseBytes、errorCodeが含まれます。運用チームには、性質の異なる次の3つの要件があります。

1. 障害調査時だけ、過去48時間の複数ロググループを対象に特定requestIdの処理経路を検索し、durationMsのp95をその場で集計したい。
2. 毎日のダッシュボードで、転送バイト数に最も寄与した上位20テナントとユニークなテナント数を継続的に確認したい。
3. errorCode="PAYMENT_TIMEOUT"が5分間に10件を超えたらCloudWatchアラームを発報したい。

検索結果全体を別の分析基盤へ常時転送せず、各要件に最も適したCloudWatchの機能を使う構成はどれですか。

選択肢

A 1にはメトリクスフィルター、2にはLogs Insights、3にはContributor Insightsを使用する。すべてのルールは障害発生時にだけ有効化する。

B 1〜3のすべてをLogs Insightsのスケジュール済みクエリだけで実装する。クエリ結果を直接Auto Scalingアクションと SNSアクションへ関連付ける。

C 1にはCloudWatch Logs Insights、2にはContributor Insights、3にはログイベントをカスタムメトリクスへ変換するメトリクスフィルターと、そのメトリクスを評価するCloudWatchアラームを使用する。

D 1にはContributor Insights、2には各tenantIdをディメンションにしたメトリクスフィルター、3にはLogs Insightsを使用する。高カーディナリティでもディメンション数に関係なく固定料金になる。

ここでいったん止める | 解答と解説は次ページ

問題 021 正解・解説 本番相当

問題 21の正解・解説

1. 正解

C

2. 問題文の重要な条件

- 1は事前定義しない一時的な検索・集計であり、複数ロググループと過去範囲を横断する。
- 2はtenantIdという高カーディナリティの寄与者を順位付けし、継続レポートにする。
- 3は固定パターンの発生回数を時系列メトリクスにし、しきい値アラームを作る。
- ログ全体を外部へ継続転送する要件ではない。
- 同じ「ログ分析」でも、調査、Top-N分析、リアルタイムなメトリクス化で適切な機能が異なる。

3. 正解へ至る判断過程

要件を処理のタイミングで分類します。過去ログへ任意のクエリを実行する1はLogs Insightsです。構造化フィールドを抽出し、filter、stats、パーセンタイル関数などで対話的に調べられます。継続的にログを評価して上位寄与者を求める2はContributor Insightsです。tenantIdを寄与者キー、responseBytesを集計値としてTop-Nやユニーク寄与者を可視化できます。固定文字列・JSONパターンを到着時に数値へ変換し、通常のCloudWatchアラームで評価する3はメトリクスフィルターです。

4. 正解が要件を満たす理由

Cは、オンデマンド調査にだけクエリコストを使い、日常のTop-N分析は専用ルールで継続生成し、即時アラームに必要な固定信号だけをカスタムメトリクス化します。tenantIdごとに大量のカスタムメトリクスを作らずに高カーディナリティ分析を行える点も、コストと運用負荷の両方に合います。

5. 各不正解選択肢が不適切な理由

- **A:** メトリクスフィルターはログ到着時に既知パターンを数値化する機能で、過去48時間から任意のrequestIdをたどる調査には向きません。Logs InsightsはTop-Nを一時的に求められますが、継続的な高カーディナリティ寄与者レポートにはContributor Insightsが適します。Contributor Insightsは固定エラー数を通常メトリクスへ変換する第一選択でもありません。
- **B:** Logs Insightsは対話的・定期的な分析に使えますが、3つの用途を1種類へ統一すると、固定パターンの継続アラームやTop-Nレポートの標準機能を活かせません。「クエリ結果をそのまま任意のCloudWatchアラームアクションへ関連付ける」という説明も、メトリクスフィルターで作ったメトリクスを評価する構成と同一ではありません。
- **D:** Contributor Insightsは単一リクエストの自由な追跡より、寄与者の集計向けです。tenantIdをメトリクスディメンション化するとテナントごとにカスタムメトリクスが増え、想定外の高コストを招きます。Logs Insightsはログ到着ごとに固定アラーム信号を生成するメトリクスフィルターの代替ではありません。

6. 各不正解選択肢が正解になり得る条件

- **Aが適切になる条件:** 1が「既知のエラー文字列を数える」、2が障害時の一時的なTop-N確認、3が上位クライアントやホストの継続分析という、各要件の性質が選択肢の機能に合うよう入れ替わった場合です。
- **Bが適切になる条件:** すべてがオンデマンドまたは定時のレポートで、分単位のアラームや継続的なContributorレポートが不要な場合です。保存したLogs Insightsクエリで分析を標準化できます。
- **Dが適切になる条件:** 寄与者の種類が少なく固定され、カスタムメトリクス数と費用を厳密に管理できる場合は、ディメンション別メトリクスが有用です。個別イベントの検索は別途Logs Insightsで行います。

7. 今後使える判断基準

CloudWatch Logsの設問では、**過去へ自由に問い合わせるならLogs Insights、継続的にTop-N寄与者を求めるならContributor Insights、到着した既知パターンをアラーム可能な数値へ変えるならメトリクスフィルター**と整理します。高カーディナリティな値を安易にメトリクスディメンションへすると、時系列数とコストが増える点も確認します。

8. 関連サービスとの比較

- **Logs Insights:** 複数ロググループを対象に、フィルター、集計、並べ替え、パーセンタイルなどを対話的に実行します。
- **Contributor Insights:** ログからTop-N寄与者、ユニーク寄与者数、使用量の時系列を作ります。
- **メトリクスフィルター:** 一致するログイベントをCloudWatchカスタムメトリクスへ変換し、通常のダッシュボードやアラームに使います。
- **サブスクリプションフィルター:** ログイベントをKinesis、Firehose、Lambdaなどへストリーミングする機能で、今回の内部分析だけなら必須ではありません。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4

問題 022 | Domain 2 / 信頼性・BC | 本番より難しい | 四択（1つ選択）

問題 22 18分の初期化をスケールアウト時から追い出す

保険会社の見積もりアプリケーションはEC2 Auto Scalingグループで稼働している。新しいインスタンスは、OS起動後に12GBのルールデータを取得し、ローカル索引を生成してからでなければトラフィックを処理できず、初期化に18分かかる。負荷急増の時刻は予測できず、追加容量は2分以内に使える必要がある。通常は2台で足りるため、ピーク用8台を常時 InService にしておく費用は認められない。初期化が終わっていないインスタンスをALBへ登録してはならない。

最も適切な構成はどれか。

選択肢

A Auto Scalingグループに停止済み（または要件を満たす場合は休止済み）のウォームプールを作成し、ライフサイクルフック中にルール取得と索引生成を完了させてからウォームプールへ移す。スケールアウト時は初期化済みインスタンスをプールから InService にする

B 起動ライフサイクルフックだけを設定し、スケールアウト要求が発生してから18分の初期化を開始する。ハートビートタイムアウトを30分にする

C ヘルスチェック猶予期間を20分へ延長し、ユーザーデータによる初期化の成否にかかわらず起動直後にALBへ登録する

D 予測スケーリングだけを有効にし、過去の平均時刻の18分前に新規インスタンスを起動する

ここでいったん止める | 解答と解説は次ページ

問題 022 正解・解説 本番より難しい

問題 22の正解・解説

1. 正解

A

2. 問題文の重要な条件

- 起動後の初期化が18分と長い。
- 急増時刻は予測不能だが、2分以内に容量が必要。
- 常時稼働の過剰プロビジョニングは不可。
- 初期化完了前にトラフィックを受けてはならない。

3. 正解へ至る判断過程

スケールアウトの検知を速くしても、検知後に18分の初期化が必要なら2分の目標は達成できない。したがって、初期化を需要発生前に済ませた容量を、稼働費用を抑えた状態で保持する必要がある。これはウォームプールの用途である。

4. 正解が要件を満たす理由

ウォームプールは、長い起動・初期化時間を持つアプリケーションで、停止または休止状態などの事前初期化済みインスタンスをAuto Scalingグループに用意する。ライフサイクルフックを使えば、初期化中に待機させ、完了を通知してからプールへ移せる。需要発生時は新規作成より短時間で InService に移行でき、常時8台を稼働するより計算費用を抑えられる。

5. 各不正解選択肢が不適切な理由

- B：未初期化インスタンスへの配信は防げるが、需要発生後に18分待つため2分の目標を満たさない。
- C：猶予期間は異常判定を遅らせるだけで初期化を速めない。起動直後の登録は未準備ターゲットへ配信する危険がある。
- D：急増時刻を予測できないという条件に反し、平均時刻から外れた需要に弱い。

6. 各不正解選択肢が正解になり得る条件

- B：初期化時間より長いスケールアウト猶予があり、準備完了まで確実に待機させることだけが目的の場合。
- C：アプリケーション自身が準備完了までヘルスチェックを失敗させ、猶予期間中の早期置換だけを避けたい場合。ただし準備前の配信はしない構成が前提。
- D：十分な履歴があり、急増が日次・週次パターンに強く従う場合。

7. 今後使える判断基準

起動時間が許容スケールアウト時間を超え、負荷時刻を予測できないならウォームプールを検討する。ライフサイクルフックは「状態遷移を待たせて処理する」機能であり、それだけでは処理時間そのものを短縮しない。

8. 関連サービスとの比較

ウォームプールは初期化済み容量を低コスト状態で保持する。起動テンプレートやEC2 Image Builderで初期化物をAMIへ焼き込めるなら、そちらで起動時間自体を短縮できる。スケジュール・予測スケーリングは需要時刻を先読みする方式で、予測不能な急増への保証にはならない。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3

問題 023 | Domain 3 / 展開・自動化 | 本番より難しい | 四択（1つ選択）

問題 23 EC2の初期化完了をCloudFormationへ通知する

あるチームはCloudFormationで、EC2インスタンスAppServerと、そのアプリケーションを社内サービスカタログへ登録するカスタムリソースServiceRegistrationを作成しています。AppServerのUser Dataは、パッケージ導入、設定取得、DBスキーマ移行、サービス起動、/health確認を順に実行し、通常8〜12分かかります。

現在、ServiceRegistrationにDependsOn: AppServerを指定しています。しかし、EC2インスタンスがrunningとなりCloudFormation上で作成完了になった直後、User Dataが終わる前に登録処理が始まり、ヘルスチェック失敗でスタックがロールバックします。

要件は次のとおりです。

- CloudFormationがAppServer自体を作成完了とする前に、User Dataとヘルスチェックの成功を待つ。
- 初期化が失敗した場合は失敗を通知し、15分でタイムアウトしてスタックをロールバックする。
- EC2向けにAWSが推奨する方式を使い、別の待機用CloudFormationリソースと署名済み待機URLを増やさない。
- 後続リソースは、アプリケーション準備完了後にだけ作成する。

最も適切な構成はどれですか。

選択肢

A DependsOn: AppServerを維持し、User Dataの末尾へsleep 900を追加する。DependsOnはEC2のUser Dataプロセス終了まで監視するため、十分な待機時間を設定すればよい。

B AWS::CloudFormation::WaitConditionHandleとWaitConditionを追加し、User Dataがヘルスチェック後に署名済みURLへSUCCESSを送る。ServiceRegistrationをWaitConditionへ依存させる。この方式は動作するが、EC2向けにCreationPolicyを使わず別の同期リソースを増やす。

C AppServerへCreationPolicyと15分のResourceSignalを付けるが、User Dataは完了メッセージをCloudWatch Logsへ書くだけにする。CloudFormationはログを自動検出して成功シグナルへ変換する。

D AppServerへCreationPolicyのResourceSignalを設定し、Timeout: PT15M、Count: 1とする。User Dataは各初期化処理とヘルスチェック後に、終了コードを渡してcfn-signalをAppServer論理IDへ送る。ServiceRegistrationはAppServerの完了に依存させる。

ここでいったん止める | 解答と解説は次ページ

問題 023 正解・解説 本番より難しい

問題 23の正解・解説

1. 正解

D

2. 問題文の重要な条件

- EC2 API上の起動完了と、ゲストOS内のアプリケーション準備完了は異なる。
- DependsOnはCloudFormationリソースの操作順序を制御するが、User Dataの任意処理を自動監視しない。
- EC2リソース自身のCREATE_COMPLETEをシグナル受信まで遅らせる必要がある。
- 成功だけでなく、スクリプト失敗をCloudFormationへ伝える。
- タイムアウトは15分で、失敗時にスタックをロールバックする。
- EC2/Auto ScalingにはWaitConditionよりCreationPolicyが推奨される。

3. 正解へ至る判断過程

DependsOnは、指定したリソースがCloudFormation上で作成完了になってから後続を作る機能です。しかし通常のEC2リソース作成完了は、User Dataによるアプリケーション初期化完了を意味しません。そこでAppServerの作成完了条件自体へシグナル待ちを追加します。

EC2インスタンスにCreationPolicy.ResourceSignalを指定すると、CloudFormationは必要数の成功シグナルを受けるまで、そのEC2リソースを作成完了にしません。User Dataの最後でcfn-signal --exit-codeなどを使い、初期化コマンドとヘルスチェックの終了状態を送ります。失敗シグナルまたはPT15Mのタイムアウトはリソース作成失敗となり、ロールバックへ進みます。後続はEC2の完了へ依存するため、別の待機リソースなしで正しい順序になります。

4. 正解が要件を満たす理由

Dは、EC2のライフサイクルとゲスト内の準備状態をCloudFormationのシグナルで結びます。Count: 1は1台の成功、Timeout: PT15Mは最大待機時間を表します。cfn-signalへ実際の終了コードを渡せば、途中処理の失敗を成功として隠しません。ServiceRegistrationの明示的DependsOnまたはRefなどの暗黙依存は、シグナル後のAppServer CREATE_COMPLETEまで待つので、未準備の登録を防げます。

5. 各不正解選択肢が不適切な理由

- **A:** DependsOnが待つのはCloudFormation上のリソース作成であり、User Dataプロセスの終了ではありません。User Data内のsleepはEC2のCREATE_COMPLETE判定を遅らせず、障害時にも固定時間後に成功扱いとなり得ます。
- **B:** WaitConditionとHandleを正しく接続し、後続をWaitConditionへ依存させれば同期自体は可能です。しかし本問はEC2リソース自身の準備完了を表し、別リソースと署名済みURLを増やさない要件です。AWSもEC2とAuto ScalingにはCreationPolicyを推奨しています。
- **C:** CreationPolicyはCloudWatch Logsを監視しません。指定数の有効なリソースシグナルが届かなければ、処理が成功してログへ出力されてもタイムアウトします。

6. 各不正解選択肢が正解になり得る条件

- **Aが適切になる条件:** 先行リソースについてCloudFormation API上の作成完了だけを待てばよく、ゲスト内・外部システムの準備状態を待つ必要がない場合です。DependsOnは並列作成を明示的に直列化する用途に使います。

- **Bが適切になる条件:** EC2やAuto Scaling以外の外部設定処理、複数システムからの任意シグナル、待機結果データの受取りなど、独立した同期ポイントを表したい場合です。更新ごとに新しいWaitConditionHandleを使い、古いシグナルの再利用を避けます。
- **Cが適切になる条件:** ログ出力に加えて、User Dataがcfn-signalまたはSignalResource APIでCreationPolicyへ明示的に結果を送るよう修正した場合です。

7. 今後使える判断基準

DependsOnは順序、CreationPolicyはリソース作成の準備完了シグナル、WaitConditionは独立した汎用同期ポイントです。EC2/Auto Scalingのブートストラップ完了にはCreationPolicyとcfn-signalを優先します。更新時のAuto ScalingローリングでシグナルをWaitOnResourceSignalsとPauseTimeを検討します。

8. 関連サービスとの比較

- **DependsOn:** CloudFormationリソース間の作成・更新・削除順序を明示します。アプリケーションヘルスの意味は持ちません。
- **CreationPolicy:** EC2、Auto Scalingなどの作成完了を、指定数のシグナルまで保留します。
- **WaitCondition / WaitConditionHandle:** 署名済みURLまたはSignalResourceを使う汎用待機リソースです。
- **cfn-init / cfn-signal:** cfn-initはメタデータに従ってOSを構成し、cfn-signalはその結果をCloudFormationへ通知します。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4

問題 024 | Domain 5 / ネットワーク | 本番より難しい | 複数選択（5つから2つ選択）

問題 24 ハイブリッドDNSを双方向にする

会社はSite-to-Site VPNでオンプレミスとAWSを接続している。AWS側にはaws.internalのRoute 53プライベートホストゾーン、オンプレミス側にはcorp.internalのDNSゾーンがある。次の両方を実現する必要がある。

1. オンプレミスの端末からaws.internalを解決する。
2. VPC内のEC2からcorp.internalを解決する。

DNSサーバーをEC2で運用せず、可用性のあるマネージド構成にしたい。実施すべきことを2つ選べ。

選択肢

A	VPC DHCPオプションセットで、オンプレミスDNSだけを全VPCのネームサーバーに指定する。
B	複数AZにRoute 53 Resolverインバウンドエンドポイントを作成し、オンプレミスDNSからそのIPへaws.internalを条件付き転送する。
C	Route 53のパブリックホストゾーンにaws.internalを複製する。
D	オンプレミスにRoute 53 Resolver DNS Firewallを配置する。
E	複数AZにRoute 53 Resolverアウトバウンドエンドポイントを作成し、corp.internalの転送ルールをオンプレミスDNSへ向けて対象VPCへ関連付ける。

ここでいったん止める | 解答と解説は次ページ

問題 024 正解・解説 本番より難しい

問題 24の正解・解説

1. 正解

B、E

2. 問題文の重要な条件

DNS解決は双方向であり、ゾーンはAWSのプライベートホストゾーンとオンプレミスに分かれている。VPNは既にあり、EC2上のDNS運用を避け、複数AZで可用性を確保したい。

3. 正解へ至る判断過程

オンプレミスからVPC Resolverへ入る方向にはインバウンドエンドポイントを使う。VPCからオンプレミスDNSへ出る方向にはアウトバウンドエンドポイントと転送ルールを使う。方向の名前を、問い合わせを開始する場所ではなくVPC Resolverから見た入出力として整理する。

4. 正解が要件を満たす理由

BによりオンプレミスDNSがAWSのプライベート名前空間へ問い合わせでき、EによりVPC Resolverがcorp.internalだけをオンプレミスへ転送できる。両エンドポイントを複数AZへ置けば、個別DNSサーバーを管理せず可用性を持たせられる。

5. 各不正解選択肢が不適切な理由

A: AmazonProvidedDNSを外すとAWS内部名やプライベートホストゾーンの解決を損ないやすく、双方向転送を明示的に実現しない。
B: 正解肢のため対象外。
C: 内部名とプライベートIPを公開DNSへ載せる設計となり、情報公開と名前空間の要件に反する。
D: DNS FirewallはVPCからのDNSクエリをドメインリストで制御する機能であり、オンプレミスに配置するDNS転送装置ではない。
E: 正解肢のため対象外。

6. 各不正解選択肢が正解になり得る条件

Aは、組織のDNSへ全問い合わせを送る設計を十分に検証し、そのDNSがAWS名も適切に転送できる限定環境なら採り得る。Cは公開すべきドメインと公開アドレスの場合に使う。DはVPCからマルウェアや不許可ドメインへの名前解決を制御する場合に使う。

7. 今後使える判断基準

オンプレミスからAWSの名前を引くならResolver inbound、AWSからオンプレミスの名前を引くならResolver outbound + rule、と方向を固定して覚える。

8. 関連サービスとの比較

プライベートホストゾーンは関連付けたVPC内の権威DNSを提供する。Resolverエンドポイントはハイブリッド間の問い合わせ経路、Resolverルールは特定サフィックスの転送先、DNS Firewallは問い合わせ内容の許可・拒否を担う。

公式確認先 AWS公式 1 / AWS公式 2

問題 025 | Domain 4 / セキュリティ | 本番相当 | 四択（1つ選択）

問題 25 データベース認証情報を自動更新する

複数AZのRDSデータベースをECSサービスから利用している。現在は接続パスワードを暗号化した環境変数としてタスク定義へ保存しており、90日ごとの変更時に全サービスを手作業で更新している。監査では、秘密値をコードやタスク定義から分離し、自動ローテーションし、取得操作をCloudTrailで追跡することが求められた。アプリケーションはAWS SDKから実行時に秘密を取得できる。

最も運用負荷の低い構成はどれか。

選択肢

A Systems Manager Parameter StoreのStringパラメーターへ平文で保存し、EventBridge Schedulerで名前だけ変更する。

B S3オブジェクトへパスワードを保存し、バケットのバージョニングで90日ごとに戻す。

C AWS Secrets Managerへ認証情報を保存し、RDS向けローテーションを構成する。ECSタスクロールへ対象secretの取得と必要なKMS復号だけを許可する。

D IAMユーザーのアクセスキーをデータベースパスワードとして利用し、毎週ローテーションする。

ここでいったん止める | 解答と解説は次ページ

問題 025 正解・解説 本番相当

問題 25の正解・解説

1. 正解

C

2. 問題文の重要な条件

RDSパスワード、コード/タスク定義からの分離、自動ローテーション、監査、実行時取得、運用負荷削減が求められる。

3. 正解へ至る判断過程

Secrets Managerはsecretの暗号化保存、バージョン管理、RDS等に対するローテーション、APIアクセス監査を統合する。タスクロールへsecret ARN単位で許可すれば、配布用の長期認証情報も不要である。

4. 正解が要件を満たす理由

ローテーションワークフローによりDB側とsecret側を整合させ、アプリケーションは実行時に現行値を取得できる。CloudTrailでSecrets Manager API呼び出しを監査できる。

5. 各不正解選択肢が不適切な理由

A: Stringは平文であり、名前変更だけではDBパスワード更新と同期しない。Parameter Store単独の標準機能はSecrets Managerの管理ローテーションと同じではない。
B: S3は汎用オブジェクト保存で、DB認証情報ローテーションを安全に協調しない。
C: 正解肢のため対象外。
D: IAMアクセスキーとDBパスワードは別の認証情報であり、流用できない。

6. 各不正解選択肢が正解になり得る条件

AでもSecureStringは、ローテーション不要の設定値・秘密や低コストな階層設定に適する。Bは秘密ではない大きな設定ファイルの版管理に使える。Dではなく RDS IAM database authenticationは、対応エンジンで短命トークンを使う設計なら比較対象になる。

7. 今後使える判断基準

自動ローテーションが中心ならSecrets Manager。ローテーション不要の設定階層やSecureStringならParameter Store。実行環境にはタスク/インスタンスロールを使い、秘密の配布先を増やさない。

8. 関連サービスとの比較

Secrets Managerはsecret lifecycle、KMSは保存値の暗号鍵と復号認可、IAMは誰が取得APIを呼べるかを担う。三層のどれか一つだけでは完全な秘密管理にならない。

公式確認先 AWS公式 1 / AWS公式 2

問題 026 | Domain 1 / 監視・性能 | 本番より難しい | 四択（1つ選択）

問題 26 CloudTrail組織証跡と選択的データイベント

ある金融企業はAWS Organizations配下に90のAWSアカウントを持ち、セキュリティアカウントをCloudTrailの委任管理者にする予定です。監査部門は、全リージョン・全アカウントについてIAM、KMS、EC2、VPCなどのコントロールプレーン操作を長期保管したいと考えています。一方、S3オブジェクトアクセスは件数と費用が非常に大きいため、機密データ用としてARNが確定している5個のバケットへのGetObjectだけを記録対象にします。

さらに、通常のベースラインから外れたAuthorizeSecurityGroupIngressなどの書込みAPI呼出し数の急増、および管理APIのエラー率上昇をCloudTrailの標準機能で検出したいという要件があります。ログはログアーカイブ用S3バケットへ集約し、一般のメンバーアカウントが証跡を変更できない構成にします。アカウント追加時の作業も最小限にする必要があります。

最も適切な構成はどれですか。

選択肢

A 各リージョンのCloudTrailイベント履歴を監視アカウントから定期取得し、90日を超える分だけS3へコピーする。イベント履歴には管理イベント、S3オブジェクトデータイベント、Insightsイベントが既定で含まれるため、証跡は作成しない。

B 全リージョン対応のCloudTrail組織証跡を作り、読取り・書込みの管理イベントだけを記録する。S3のGetObjectはバケット設定を読み取る管理イベントなので、追加のイベントセレクターは不要である。

C StackSetsで各メンバーアカウントに個別証跡を作成し、全S3バケットのデータイベントを記録する。CloudTrail InsightsはS3データイベントだけに有効化し、そこから管理API呼出しの異常も検出する。

D 委任管理者から全リージョン対応のCloudTrail組織証跡を作成し、読取り・書込み管理イベントを記録する。高度なイベントセレクターで指定した5バケットのS3オブジェクトGetObjectデータイベントだけを含め、必要な管理イベントのAPIコール率・APIエラー率についてCloudTrail Insightsを有効化し、ログアーカイブ用S3バケットへ配信する。

ここでいったん止める | 解答と解説は次ページ

問題 026 正解・解説 本番より難しい

問題 26の正解・解説

1. 正解

D

2. 問題文の重要な条件

- 全アカウント・全リージョンへ一貫した証跡を自動適用する。
- IAM、KMS、EC2、VPCなどのコントロールプレーン操作は管理イベントとして読取り・書込みとも記録する。
- S3 GetObjectはオブジェクトレベルのデータイベントであり、既定では証跡に含まれない。
- データイベント費用を抑えるため、5バケットとGetObjectへ対象を限定する。
- APIコール率とAPIエラー率のベースライン異常をCloudTrail Insightsで検出する。
- CloudTrail委任管理者を使い、メンバーアカウントが組織証跡を変更できないようにする。

3. 正解へ至る判断過程

最初にスコープから組織証跡を選びます。組織証跡はOrganizationsの全メンバーアカウントへ適用され、新規アカウントも取り込めます。次にイベント分類を行います。IAMポリシー変更、セキュリティグループ変更、KMSキー設定などは管理イベントですが、S3オブジェクトに対するGetObjectはデータイベントです。そのため、管理イベントを包括的に有効化したうえで、高度なイベントセレクターによりresources.type、対象ARN、eventNameなどを使って必要なS3データイベントだけを選びます。

最後に異常検知を追加します。管理イベントの書込みAPIコール率を分析するには、証跡が書込み管理イベントを記録し、該当するInsightsタイプを有効化している必要があります。APIエラー率は読み取りまたは書込みの管理イベントを基に分析できます。これらを組織証跡と同じ統制下で有効化します。

4. 正解が要件を満たす理由

Dは、中央管理、全リージョン、全アカウント、新規アカウント自動適用という運用要件を組織証跡で満たします。管理イベントとS3データイベントを正しく分離し、高度なイベントセレクターで高額になりやすいデータイベントを必要なバケット・操作へ限定します。CloudTrail Insightsは通常のAPI活動を継続分析してコール率・エラー率の異常をInsightsイベントとして記録します。委任管理者は組織証跡を管理できますが、リソースの所有は管理アカウントに残り、メンバーアカウントは組織証跡を削除・変更できません。

5. 各不正解選択肢が不適切な理由

- **A:** イベント履歴は各アカウント・リージョンの過去90日間の管理イベントを調査する機能で、長期の組織集約証跡ではありません。データイベントやInsightsイベントがすべて既定で含まれるわけでもありません。
- **B:** S3バケット自体の作成やポリシー変更は管理イベントですが、オブジェクトのGetObjectはデータイベントです。管理イベントだけの証跡では必要な閲覧監査が欠落します。
- **C:** 個別証跡は組織証跡より展開・変更管理が複雑です。全バケットのデータイベント記録は費用制約に反します。また、S3データイベントのInsightsを有効化しただけで、管理APIの異常を分析できるわけではありません。分析対象カテゴリのイベントを記録して対応するInsightsを有効にする必要があります。

6. 各不正解選択肢が正解になり得る条件

- **Aが適切になる条件:** 単一アカウント・単一リージョンで、直近90日以内の管理イベントを一時的に検索するだけで、継続配信・長期保管・データイベントが不要な場合です。

- **Bが適切になる条件:** オブジェクトレベルの読取り監査が不要で、コントロールプレーン操作だけを記録すればよい場合です。その場合でもInsights要件があれば別途有効化します。
- **Cが適切になる条件:** Organizationsを使えない独立アカウント群、またはアカウントごとに異なる証跡所有・保存先・イベント選択が必須の場合です。すべてのS3オブジェクト操作を監査する規制要件があり、費用を許容できる場合には全データイベント記録も成立します。

7. 今後使える判断基準

CloudTrailでは、まず**管理イベント＝リソース設定・コントロールプレーン、データイベント＝リソース内部への高頻度操作**と分類します。データイベントは既定で記録されず、量が多いため対象リソースやイベント名を絞ります。組織全体なら個別証跡より組織証跡を優先します。Insightsは「元となる対象イベントを記録していること」が前提で、コール率とエラー率では必要な読取り・書込みカテゴリが異なります。

8. 関連サービスとの比較

- **CloudTrailイベント履歴:** 直近90日の管理イベントをリージョン単位で検索する簡易機能です。
- **CloudTrail証跡:** イベントをS3へ継続配信し、必要に応じてCloudWatch LogsやEventBridgeと連携します。
- **CloudTrail Lake:** イベントデータストアへ取り込み、SQLで長期分析する用途です。S3ログ保管を主要件とする証跡とは課金・検索モデルが異なります。
- **AWS Config:** リソース構成の履歴と準拠状態を追跡します。誰がどのAPIを呼んだかを記録するCloudTrailとは補完関係です。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4 / AWS公式 5

問題 027 | Domain 2 / 信頼性・BC | 本番より難しい | 四択（1つ選択）

問題 27 20台を止めずにAMIを段階更新する

ある社内APIはALB配下のAuto Scalingグループ20台で稼働している。セキュリティ更新済みAMIを指す新しい起動テンプレートへ切り替える必要がある。更新中も少なくとも18台は正常にサービスを提供し続けなければならない。最初の2台を置換した時点で15分停止し、合成監視と業務メトリクスを確認してから残りを進めたい。新AMIのヘルスチェックが失敗した場合は以前の構成へ自動的に戻し、すでに新しい起動テンプレート版で動くインスタンスは不要に再作成したくない。

追加の常設環境を作らずに要件を満たす方法はどれか。

選択肢

A	起動テンプレートのデフォルトバージョンだけを変更し、各インスタンスを運用担当者が2台ずつ手動終了する
B	希望する起動テンプレートを指定してインスタンス更新を開始し、最小正常率90%、10%のチェックポイント、チェックポイント遅延15分、自動ロールバック、Skip matchingを設定する
C	Auto Scalingグループの希望容量を0にしてから新しい起動テンプレートへ変更し、20へ戻す
D	AWS Backupで全EC2インスタンスのAMIを取得し、新AMIのAuto Scalingグループを別に20台作成してDNS TTL満了後に切り替える

ここでいったん止める | 解答と解説は次ページ

問題 027 正解・解説 本番より難しい

問題 27の正解・解説

1. 正解

B

2. 問題文の重要な条件

- 20台中18台以上、すなわち90%以上を正常に維持する。
- 2台置換後に検証のため停止したい。
- 失敗時の自動ロールバックが必要。
- 既に一致するインスタンスは置換不要。
- 常設の別環境は避ける。

3. 正解へ至る判断過程

Auto Scalingのインスタンス更新は、希望構成へ段階的に置換するための機能である。20台の10%は2台であり、最小正常率90%は18台維持に対応する。チェックポイント、遅延、自動ロールバック、Skip matchingが問題文の各要件に一対一で対応する。

4. 正解が要件を満たす理由

インスタンス更新では、最小正常率により同時にサービスから外せる割合を制御できる。チェックポイントで更新を段階停止し、EventBridge通知などと組み合わせて検証できる。自動ロールバックは失敗時に以前の構成へ戻し、Skip matchingは既に希望構成と一致するインスタンスを置換対象から外す。

5. 各不正解選択肢が不適切な理由

- A：手動終了ではチェックポイントや自動ロールバックがなく、誤って18台未満にする危険もある。
- C：全停止となり、可用性要件を完全に違反する。
- D：ブルー/グリーンとしては成立し得るが、追加20台分の環境とDNS切替運用が必要で、「追加の常設環境を作らない」要件に対して過剰である。AWS Backupはローリング更新の制御機能でもない。

6. 各不正解選択肢が正解になり得る条件

- A：少数の非本番インスタンスで、停止と手動復旧を許容できる場合。
- C：完全停止可能な保守時間があり、更新速度を最優先する場合。
- D：新旧環境を同時に動かして即時にトラフィックを戻す厳格なブルー/グリーン要件があり、追加費用を受容する場合。

7. 今後使える判断基準

起動テンプレートやAMIをグループ内で段階置換するならインスタンス更新を第一候補にする。可用性は最小/最大正常率、段階検証はチェックポイント、安定待ちはインスタンスウォームアップとBake time、失敗復旧はロールバックで表現する。

8. 関連サービスとの比較

インスタンス更新は同一Auto Scalingグループ内のローリング置換である。CodeDeployや別グループを使うブルー/グリーンは新旧環境を並行稼働できるが、追加容量とトラフィック切替の設計が必要。CloudFormationの更新ポリシーでもローリング更新は可能だが、既存グループの運用機能としてはインスタンス更新のチェックポイントやSkip matchingが直接的である。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3

問題 028 | Domain 3 / 展開・自動化 | 本番相当 | 四択（1つ選択）

問題 28 Organizations向けStackSetsの権限モデル

ある企業は、すべての機能を有効にしたAWS Organizationsで300のメンバーアカウントを管理しています。セキュリティ基盤チームは、指定した2つのOUに属する全アカウントの東京・大阪リージョンへ、共通のIAMロール、AWS Config設定、通知用SNSトピックをCloudFormation StackSetsで展開します。今後OUへ追加・移動される新規アカウントにも同じスタックを自動展開し、OUから外れたときのスタック保持・削除方針も設定したいと考えています。

次の条件があります。

- 対象は同じOrganization内のアカウントだけである。
- 各メンバーアカウントへStackSets用の実行ロールを手作業で事前作成・保守したくない。
- 日常のStackSet操作は、管理アカウントではなく登録済みの委任管理者アカウントから行う。
- OUへのアカウント追加を検知する独自Lambdaは作らない。

最も適切な構成はどれですか。

選択肢

A Organizationsの管理アカウントでCloudFormation StackSetsのTrusted Accessを有効化し、セキュリティアカウントを委任管理者として登録する。Service-managed permissionsのStackSetで対象OUとリージョンを指定し、Automatic deploymentを有効化する。必要なサービスリンクロールと対象アカウント側ロールはCloudFormationに作成させる。

B Self-managed permissionsのStackSetを委任管理者に作り、管理アカウントにAWSCloudFormationStackSetAdministrationRoleだけを作成する。Trusted Accessを有効化すれば、Self-managedでもCloudFormationが全対象アカウントのAWSCloudFormationStackSetExecutionRoleとOU自動展開を管理する。

C Trusted Accessを有効化せずService-managed permissionsを選択し、各対象アカウントにAWSCloudFormationStackSetExecutionRoleを手動作成する。Service-managedはOrganizations外のアカウントも同じStackSetで対象にできる。

D 各対象アカウントにSelf-managed用の管理・実行ロールを作成し、OUをStackSetのターゲットに指定してAutomatic deploymentを有効化する。Self-managed permissionsにはOUの追加・削除へ自動追従する標準機能がある。

ここでいったん止める | 解答と解説は次ページ

問題 028 正解・解説 本番相当

問題 28の正解・解説

1. 正解

A

2. 問題文の重要な条件

- AWS Organizationsの全機能が有効で、対象は同じ組織内に限定される。
- アカウントIDの個別列挙ではなくOUを対象にする。
- 新規・移動アカウントへ自動展開する。
- StackSets用IAMロールを各アカウントで手動管理しない。
- 委任管理者アカウントから日常運用する。
- Service-managed permissionsにはTrusted Accessが前提である。

3. 正解へ至る判断過程

権限モデルは、対象アカウントの所属とロール管理要件で選びます。Service-managed permissionsはOrganizations内のアカウント・OUを対象とし、CloudFormationとOrganizationsのTrusted Accessを使って必要なロールを作成・管理します。Automatic deploymentを有効にすると、対象OUへのアカウント追加、削除、OU間移動を契機にスタックインスタンスを自動作成・削除できます。

Trusted Accessの有効化と委任管理者登録は同じ操作ではありません。まず管理アカウント側でTrusted Accessを有効化し、その後、組織内のメンバーアカウントを委任管理者に登録できます。委任管理者から作成・管理したService-managed StackSetでも、組織上の操作は管理アカウントの権限関係を通じて実行されます。

4. 正解が要件を満たす理由

Aは、同じOrganization内の多数アカウント、OU単位の対象指定、新規アカウント自動展開、手動実行ロール不要という条件をすべて満たします。管理アカウントにはAWSServiceRoleForCloudFormationStackSetsOrgAdmin、対象メンバーにはAWSServiceRoleForCloudFormationStackSetsOrgMemberなどの必要なロールがサービス連携により用意されます。Automatic deploymentでは、OUからアカウントが外れた場合にスタックと関連リソースを削除するか、保持するかも選択できます。

5. 各不正解選択肢が不適切な理由

- **B:** Self-managed permissionsでは、管理側のAWSCloudFormationStackSetAdministrationRoleと対象側のAWSCloudFormationStackSetExecutionRoleを利用者が作成・保守します。Trusted Accessを有効にしてもSelf-managedのロール管理やOU自動展開がService-managedへ変わるわけではありません。
- **C:** Service-managed permissionsにはOrganizationsの全機能とTrusted Accessが必要です。対象アカウント側へSelf-managed用実行ロールを手動作成するモデルでもありません。また、Service-managedの対象は同じOrganization内に限定され、組織外アカウントへは展開できません。
- **D:** Self-managed permissionsはアカウントIDと必要ロールを利用者が管理するモデルです。Service-managedにあるou-baseのAutomatic deploymentを標準機能としてそのまま利用できません。また、管理ロールは通常ターゲットごとではなくStackSet管理アカウント側に置きます。

6. 各不正解選択肢が正解になり得る条件

- **Bが適切になる条件:** 対象アカウント側に実行ロールも正しく作成し、自動OU追従を要求せず、明示したアカウントへSelf-managedで展開する場合です。権限ポリシーを独自に細かく管理したいケースがあります。
- **Cが適切になる条件:** Trusted Accessを有効化したうえで、対象を同じOrganization内に限定し、手動のSelf-managed実行ロールを前提から外せばService-managedの構成になります。組織外を対象にするならSelf-managedを選びます。
- **Dが適切になる条件:** Organizationsを利用していない、または別Organization・独立アカウントも対象で、各対象に信頼済み実行ロールを準備し、アカウント追加を独自プロセスで管理する場合です。

7. 今後使える判断基準

同一OrganizationsのOU、新規アカウント自動展開、ロール自動管理ならService-managed。組織外を含む、または管理・実行ロールを自分で厳密に設計するならSelf-managedが基本です。Trusted AccessはService-managedを成立させる組織連携であり、Self-managed用Execution Roleの代名詞ではありません。委任管理者登録もTrusted Access有効化後の別ステップです。

8. 関連サービスとの比較

- **Service-managed permissions:** Organizationsと連携し、OUターゲット、サービス管理ロール、Automatic deploymentを利用できます。
- **Self-managed permissions:** 管理アカウントと対象アカウント間の信頼ロールを利用者が作成し、Organizations外にも展開できます。
- **Delegated administrator:** 管理アカウント以外のメンバーアカウントからService-managed StackSetsを運用できるようにします。
- **Automatic deployment:** 対象OUのアカウント追加・削除・移動にスタックインスタンスを追従させます。StackSet単位で設定します。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4 / AWS公式 5

問題 029 | Domain 5 / ネットワーク | 本番相当 | 四択（1つ選択）

問題 29 リージョン障害時だけ切り替えるDNS

企業のWeb APIは東京リージョンのALBをプライマリ、大阪リージョンのALBを待機系としている。通常は全トラフィックを東京へ送り、東京のALBまたは配下ターゲットが利用不能になった場合だけ大阪へ切り替えたい。クライアントは単一の独自ドメインを使用する。DNSレコードはルートドメイン（zone apex）に置く必要があり、運用担当者は固定IPを管理したくない。

最適なRoute 53構成はどれか。

選択肢

A	2つのCNAMEレコードを作成し、東京をMulti-Value Answer、大阪をSimpleに設定する。
B	2つのレイテンシーベースAliasレコードを作成し、両方の重みを0にする。
C	ALBを参照するPrimary/SecondaryのフェイルオーバーAliasレコードを作成し、Evaluate Target Healthを有効にする。
D	東京を重み100、大阪を重み0とするWeightedレコードだけを作成し、ヘルスチェックを関連付けない。

ここでいったん止める | 解答と解説は次ページ

問題 029 正解・解説 本番相当

問題 29の正解・解説

1. 正解

C

2. 問題文の重要な条件

通常は東京だけ、障害時だけ大阪、zone apex、ALB、固定IP管理不要という条件がある。これはトラフィック分散ではなくactive-passiveである。

3. 正解へ至る判断過程

Route 53のフェイルオーバールーティングはPrimaryが正常な間はPrimaryを返し、異常時にSecondaryを返す。Aliasはzone apexで利用でき、ALBのDNS名を参照できる。Evaluate Target HealthによりAlias先のALBの状態をルーティング判断へ反映できる。

4. 正解が要件を満たす理由

固定IPやCNAMEをzone apexへ置く必要がなく、東京から大阪へのactive-passive切り替えをDNSレベルで自動化できる。ALB配下の正常性も考慮できる。

5. 各不正解選択肢が不適切な理由

A: zone apexにCNAMEは置けず、Multi-Value AnswerはPrimary/Secondaryの厳密なフェイルオーバー用途ではない。
B: レイテンシーベースは正常な複数リージョンから低遅延な宛先を選ぶため、通常時に東京だけという条件を直接表さない。
C: 正解肢のため対象外。
D: Weight 0はフェイルオーバーの代替ではなく、ヘルスチェックがなければ東京障害を検出して大阪へ切り替える保証がない。

6. 各不正解選択肢が正解になり得る条件

AのMulti-Value Answerは複数の正常なIPを最大8件返す簡易分散に向く。Bは利用者ごとの遅延を最小化するactive-activeに向く。DのWeightedは段階リリースや比率分散に向き、各レコードへヘルスチェックを付ければ異常宛先を除外できる。

7. 今後使える判断基準

「平常時は一方だけ、障害時だけもう一方」はFailover。「両方を比率で使う」はWeighted。「利用者から近い正常リージョン」はLatencyと読む。

8. 関連サービスとの比較

Route 53はDNS応答を切り替えるためTTLの影響を受ける。Global Acceleratorは静的Anycast IPと高速なエンドポイント切り替えを提供し、DNSキャッシュの影響を抑えたいTCP/UDPワークロードで比較対象になる。

公式確認先 AWS公式 1 / AWS公式 2

問題 030 | Domain 4 / セキュリティ | 本番相当 | 四択（1つ選択）

問題 30 ALB証明書を手作業なしで更新する

インターネット向けALBでapi.example.comを公開している。会社は公開TLS証明書をAWSで管理し、期限切れ前の更新作業を自動化したい。DNSはRoute 53で管理され、ドメイン所有権の検証レコードを継続保持できる。EC2へ秘密鍵を配布せず、ALBリスナーでTLSを終端する。

最適な方法はどれか。

選択肢

A	ACMで公開証明書をDNS検証により発行し、ALBのHTTPSリスナーへ関連付け、検証CNAMEを削除せず保持する。
B	EC2上で自己署名証明書を毎月作成し、ALBへ秘密鍵をコピーする。
C	ACM Private CAで公開インターネット用証明書を発行し、ブラウザへCA証明書を手動配布する。
D	IAM server certificateへ証明書をアップロードし、EventBridgeで期限だけ通知する。

ここでいったん止める | 解答と解説は次ページ

問題 030 正解・解説 本番相当

問題 30の正解・解説

1. 正解

A

2. 問題文の重要な条件

公開ドメイン、ALB終端、Route 53、DNS検証を維持可能、自動更新、秘密鍵をEC2へ配らないという条件である。

3. 正解へ至る判断過程

ACMの公開証明書を統合サービスで使用し、DNS検証レコードが存在し続け、証明書が使用中などの条件を満たせばACMが更新を管理する。ALBへ直接関連付けられ、秘密鍵の輸出・配布は不要である。

4. 正解が要件を満たす理由

公開ブラウザが信頼する証明書を使い、検証と更新の運用をAWSへ委ねられる。Route 53なら検証CNAME作成も容易である。

5. 各不正解選択肢が不適切な理由

A: 正解肢のため対象外。
B: 公開クライアントに信頼されず、秘密鍵配布と毎月作業が増える。
C: Private CAは社内PKI向けで、一般ブラウザが既定で信頼する公開証明書ではない。
D: アップロード証明書の期限通知だけでは自動更新・再配置を実現しない。

6. 各不正解選択肢が正解になり得る条件

Bは閉じたテスト環境、Cは企業管理端末・内部サービスの私設PKI、Dは古いAWSサービスとの互換要件で既存証明書を使う限定場面に当てはまる。通常のALB公開証明書にはACMを使う。

7. 今後使える判断基準

ALB/CloudFront/API GatewayなどACM統合先の公開TLSは、ACM公開証明書 + DNS検証を第一候補にする。検証レコードを消すと管理更新を妨げる。

8. 関連サービスとの比較

ACMは証明書ライフサイクル、Route 53はDNS所有権検証、ALBはTLS終端を担う。Secrets ManagerやParameter Storeへ秘密鍵を自前保存する必要はない。

公式確認先 AWS公式 1 / AWS公式 2

問題 031 | Domain 1 / 監視・性能 | 複合難問 | 四択（1つ選択）

問題 31 EventBridgeとSSM Automationによる自動修復

ある企業では、本番VPCのEC2セキュリティグループに対して、TCP 22または3389を0.0.0.0/0へ開放する変更を禁止しています。ただし、アプリケーション用ポートの公開や、承認済み社内CIDRからの管理アクセスは許可されています。CloudTrailはすでに有効であり、セキュリティグループの変更イベントを記録しています。

過去に、緊急作業者が誤ってSSHを全世界へ開放し、定時のコンプライアンススキャンまで20分間残存しました。運用チームは、AuthorizeSecurityGroupIngressの該当変更をほぼリアルタイムに検出し、サーバーレスなAWSマネージド機能で自動的に取り消したいと考えています。次の条件があります。

- 変更イベントに含まれるセキュリティグループIDと許可ルールを修復処理へ渡す。
- 修復前に現在のルールを再確認し、すでに人手で削除済みでも安全に終了する。
- EventBridgeでは同じイベントが複数回届く可能性を考慮する。
- 修復処理には、対象セキュリティグループの参照と該当Ingressルールの削除だけを許可する。
- 常駐LambdaやEC2インスタンスを新たに運用しない。

最も適切な構成はどれですか。

選択肢

A CloudTrail経由のAuthorizeSecurityGroupIngressを一致させるEventBridgeルールを作成し、Systems Manager Automationのカスタムランブックをターゲットにする。入力トランスフォーマーでイベントの識別情報をランブックへ渡し、ランブックで現在状態を確認して該当ルールだけを取り消す。AutomationAssumeRoleには必要なEC2参照・取消し権限だけを付与し、処理を冪等にする。

B AWS Configのセキュリティグループ用マネージドルールを24時間ごとに評価し、非準拠時にSystems Manager Automationでセキュリティグループ全体を削除する。Configが同じ評価を再実行しないよう、修復再試行は無効にする。

C CloudTrailログをCloudWatch Logsへ配信し、メトリクスフィルターとアラームで検出する。アラームアクションとしてSystems Manager Run Commandを全EC2インスタンスへ実行し、OSのiptablesからTCP 22と3389を拒否する。

D EventBridge Schedulerを1分間隔で起動し、Systems Manager Run Commandで管理用インスタンスからすべてのセキュリティグループを走査する。違反があれば管理者権限のインスタンスプロファイルを使ってセキュリティグループを既定状態へ戻す。

ここでいったん止める | 解答と解説は次ページ

問題 031 正解・解説 複合難問

問題 31の正解・解説

1. 正解

A

2. 問題文の重要な条件

- 変更発生からほぼリアルタイムに動作し、定時走査を待たない。
- CloudTrailイベントの内容を利用し、変更された対象だけを修復する。
- Lambdaや管理サーバーを常駐させず、EventBridgeからSSM Automationを直接起動する。
- 再配信や競合を前提に、現在状態を確認する冪等な処理にする。
- Automation用IAMロールを最小権限にする。
- 許可されているIngressまで削除しない。

3. 正解へ至る判断過程

検出源はすでにCloudTrailに記録されるAPI呼出しなので、EventBridgeの「AWS API Call via CloudTrail」イベントパターンでeventSourceとeventNameを絞ります。イベントのrequestParametersなどから対象を取り出すには入力トランスフォーマーを使えます。修復先としてSSM Automationランブックは EventBridgeの直接ターゲットにできるため、中継Lambdaは不要です。

ランブックでは、渡されたグループIDとルールを再取得し、禁止条件に一致して現在も存在する場合だけRevokeSecurityGroupIngressまたはセキュリティグループルールIDによる取消しを行います。同じイベントの再配信や人手による先行削除があっても、存在しなければ成功扱いで終了させます。EventBridgeがAutomationを開始するロールと、AutomationがEC2 APIを実行するAutomationAssumeRoleも役割を分けて制限します。

4. 正解が要件を満たす理由

Aはイベント駆動なので定時スキャンより露出時間を短くできます。入力トランスフォーマーにより、ランブックはイベント全体または必要なフィールドをパラメータとして受け取れます。Automationには条件分岐、AWS API実行、スクリプト、失敗処理を組み込めるため、現在状態の検証と限定的な取消しを1つの監査可能なワークフローにできます。実行履歴もSystems Managerに残り、常駐コードのパッチ運用が不要です。

5. 各不正解選択肢が不適切な理由

- **B:** 24時間評価では「ほぼリアルタイム」を満たしません。セキュリティグループ全体の削除は、許可されたアプリケーションルールまで失わせ、関連リソースがある場合の影響も大きすぎます。Config自動修復は有力ですが、問題文の即時イベントと限定修復には合いません。
- **C:** OSファイアウォールを変更しても、VPCレベルの禁止設定そのものは残り、EC2以外のENIや将来のインスタンスにも適切に対応できません。アラームからRun Commandを全台へ実行するのは対象範囲も過大です。
- **D:** 走査用インスタンスの運用が新たに必要で、1分ごとの全件API走査は非効率です。管理者権限と「既定状態へ戻す」処理は最小権限・最小変更にも反します。

6. 各不正解選択肢が正解になり得る条件

- **Bが適切になる条件:** 既存リソースも含めた継続的な準拠評価が主目的で、数十分から1日の検出遅延を許容し、非準拠ルールだけを安全に直すConfig自動修復ランブックを用意できる場合です。

- **Cが適切になる条件:** ネットワークACLやセキュリティグループを変更できず、EC2ゲストOS内部の防御を緊急に追加すること自体が要件で、対象インスタンスをタグで厳密に選べる場合です。
- **Dが適切になる条件:** イベントとして取得できない外部状態を定期ポーリングする必要があり、管理ノードの保守を許容する場合です。それでもIAMは必要な読取り・変更へ限定します。

7. 今後使える判断基準

修復設計では、**検出イベント、オーケストレーター、実際に変更する権限**を分離します。CloudTrail APIイベントが使えるならEventBridge、複数ステップのAWS API修復ならSSM Automationが基本候補です。イベント駆動システムは重複・順序ずれ・遅延を前提にし、「望ましい状態なら何もしない」冪等性を持たせます。自動修復はリソース全体ではなく違反部分だけを変更します。

8. 関連サービスとの比較

- **EventBridgeルール:** イベントパターンに一致した変更を低遅延でターゲットへ渡します。
- **EventBridge Scheduler:** 特定時刻・間隔での実行に向き、変更イベントそのものへの即応とは異なります。
- **SSM Automation:** AWS API操作や分岐を含むランブックを実行し、実行履歴とIAMロールを管理できます。
- **SSM Run Command:** マネージドノード上でコマンドを実行します。AWSコントロールプレーンの設定修復ではAutomationのほうが自然です。
- **AWS Config自動修復:** 構成準拠の継続評価と修復に向き、イベント駆動修復を補完できます。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4

問題 032 | Domain 2 / 信頼性・BC | 本番相当 | 四択（1つ選択）

問題 32 ALBでは異常なのにEC2が置換されない

Webアプリケーションは、ALBにアタッチされたEC2 Auto Scalingグループで稼働している。あるインスタンスでアプリケーションプロセスが停止し、ALBの /health は連続してHTTP 500を返すようになった。ALBはそのターゲットを unhealthy としてトラフィックから外したが、30分経過してもAuto Scalingグループはインスタンスを置換しなかった。EC2のシステムステータスチェックとインスタンスステータスチェックはどちらも合格している。調査すると、Auto Scalingグループのヘルスチェックタイプはec2だけであった。

アプリケーション異常のインスタンスを自動置換しつつ、正常な起動直後のインスタンスを早まって置換しないための変更はどれか。

選択肢

A	Route 53のヘルスチェックを各EC2インスタンスのパブリックIPへ作成し、失敗時にDNSレコードを削除する
B	ALBの登録解除の遅延を0秒にし、ターゲットが異常になったら直ちに接続を切断する
C	Auto ScalingグループでElastic Load Balancingヘルスチェックを有効にし、アプリケーションの実際の初期化時間に合うヘルスチェック猶予期間を設定する
D	HealthyHostCount を使うターゲット追跡スケーリングを設定し、正常ターゲット数が減ったら希望容量を増やす

ここでいったん止める | 解答と解説は次ページ

問題 032 正解・解説 本番相当

問題 32の正解・解説

1. 正解

C

2. 問題文の重要な条件

- ALBはアプリケーション異常を検出済みである。
- EC2基盤のステータスチェックは正常である。
- Auto Scalingグループは EC2ヘルスチェックしか評価していない。
- 起動直後の誤置換も防ぎたい。

3. 正解へ至る判断過程

ALBが異常ターゲットを外すことと、Auto ScalingがEC2を異常と判定して置換することは別である。Auto Scalingグループで ELBヘルスチェックを有効にすると、ALBが報告した異常をAuto Scalingが取り込み、置換対象にできる。起動処理中の一時的な失敗は猶予期間で扱う。

4. 正解が要件を満たす理由

ELBヘルスチェックを有効にしたAuto Scalingグループは、ロードバランサーが登録済みインスタンスを Unhealthy と報告すると、次の定期チェックでインスタンスを異常とマークし、置換する。ヘルスチェック猶予期間を正しく設定すれば、アプリケーションが準備中の間はその判定を猶予できる。

5. 各不正解選択肢が不適切な理由

- A：ALBが既にターゲット単位でヘルスチェックしており、Route 53を各インスタンスに重ねてもAuto Scalingの置換判定にはならない。
- B：登録解除の遅延は既存接続のドレイニングを制御する機能であり、異常インスタンスの置換を開始しない。
- D：正常台数低下を契機に別のインスタンスを追加できる可能性はあるが、異常インスタンス自体を確実に終了・置換する正しいヘルス判定ではない。また HealthyHostCount はターゲット追跡に適した定義済み利用率メトリクスではない。

6. 各不正解選択肢が正解になり得る条件

- A：ロードバランサーを使わず、DNSで独立エンドポイント間をフェイルオーバーする場合。
- B：デプロイやスケールイン時に長時間接続をどれだけ待つかを調整したい場合。
- D：置換とは別に、正常ターゲット数不足をカスタムアラームとステップスケーリングで一時補完する設計を採る場合。

7. 今後使える判断基準

「ALBが配信を止める」と「Auto Scalingが置換する」を区別する。EC2ヘルスチェックは基盤障害、ELBヘルスチェックはアプリケーション経路の障害を検出する。アプリ異常で自己修復させたいなら、Auto Scaling側でELBヘルスチェックを明示的に有効にする。

8. 関連サービスとの比較

ALBヘルスチェックはターゲットグループ内の配信可否を決める。Route 53ヘルスチェックはDNS応答でエンドポイントを選ぶ。Auto Scalingヘルスチェックはインスタンスの維持・置換に使われる。ヘルスチェック猶予期間は新規インスタンスへの異常判定を遅らせ、登録解除の遅延は終了するターゲットの既存接続を待つ。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3

問題 033 | Domain 3 / 展開・自動化 | 複合難問 | 複数選択（5つから2つ選択）

問題 33 委任管理者の権限境界

ある企業はAWS Organizationsで300のアカウントを管理している。CloudFormation StackSetsを用いて、Prod OUの全アカウント・2リージョンへ監査用IAMロールとAWS Config設定を配布し、今後Prod OUへ追加されるアカウントにも自動展開したい。組織の管理アカウントは日常運用に使用せず、専用のプラットフォームアカウントをCloudFormation StackSetsの委任管理者として登録する方針である。

セキュリティ部門は、委任後の権限範囲を誤認しないこと、メンバーアカウントへ手作業で実行ロールを作らないこと、Sandbox OUにはスタックインスタンスを作らないことを要求している。テンプレートはマクロやネストされたスタックを含まない。

この設計について正しい対応または説明を2つ選べ。

選択肢

A	管理アカウントで委任管理者を登録するとき、CloudFormationの登録APIへProd OUを指定すれば、委任管理者のStackSets権限そのものをそのOUだけに技術的に制限できる
B	管理アカウントでStackSetsとOrganizationsのtrusted accessを有効化し、プラットフォームアカウントを委任管理者に登録する。委任管理者からservice-managed permissionsのStackSetを作成し、Prod OUをターゲットとしてautomatic deploymentを有効化する
C	新規アカウントへのOU連動自動展開を行うにはself-managed permissionsが必須であり、各メンバーアカウントにAWSCloudFormationStackSetExecutionRoleを手作業で作成する
D	service-managed permissionsを使えば、委任管理者のStackSetテンプレートでマクロ、Transform、ネストされたスタックを制限なく利用できる
E	委任管理者は組織内の任意アカウントへStackSetを展開できる強い権限を持ち、管理アカウント側から対象OUだけに委任範囲を狭めることはできない。そのため、委任管理者へのアクセス、変更承認、CloudTrail監査を組織全体へ展開可能な権限として統制する

ここでいったん止める | 解答と解説は次ページ

問題 033 正解・解説 複合難問

問題 33の正解・解説

1. 正解

B、E

2. 問題文の重要な条件

- OrganizationsのOUをターゲットとし、新規アカウントにも自動展開する。
- メンバーアカウントの実行ロールを手動管理しない。
- 管理アカウントではなく委任管理者から日常運用する。
- 実際の展開対象はProd OUだが、委任管理者として付与される権限範囲は別に評価する。
- service-managed permissionsで非対応となるテンプレート機能も把握する。

3. 正解へ至る判断過程

OU連動と自動展開、ロール自動作成からservice-managed permissionsを選ぶ。この方式では、管理アカウントでtrusted accessを有効化し、必要ならメンバーアカウントを委任管理者として登録する。StackSetのターゲットにProd OUを選べば、現在および将来の所属アカウントへautomatic deploymentできる。

ただし、「そのStackSetがProdを対象にすること」と「委任管理者の権限がProdだけに限定されること」は同じではない。CloudFormationの委任管理者は組織全体の任意アカウントへ展開でき、管理アカウントから特定OUや特定StackSet操作だけに委任を狭められない。したがって、高権限主体として運用統制する。

4. 正解が要件を満たす理由

Bはtrusted accessによりCloudFormationが必要なservice-linked roleとターゲットアカウント側の実行ロールを管理するため、手作業のロール配布を不要にする。OUターゲットとautomatic deploymentは、新規アカウント追加への追随を満たす。Eは委任管理者の実際の権限範囲を正しく表し、Sandboxへ展開しないことを単なる技術的委任範囲と誤認せず、アクセス制御・承認・監査で守る設計につながる。

5. 各不正解選択肢が不適切な理由

A: 委任管理者登録で対象OUを指定して権限を限定する機能はない。StackSet操作時にターゲットOUを選べても、委任管理者自身の組織内展開権限はそれより広い。
B: 正解肢のため対象外。
C: OU連動のautomatic deploymentはservice-managed permissionsの機能である。self-managedでは管理・実行ロールを利用者が用意し、アカウントを明示的に扱う運用になる。
D: service-managed permissionsのStackSetsはネストされたスタックをサポートせず、マクロやTransformを含むテンプレートにも制約がある。
E: 正解肢のため対象外。

6. 各不正解選択肢が正解になり得る条件

A: 委任ではなく、社内のCI/CDロールが呼べる独自パイプラインをIAM条件や承認でProd用操作へ限定する設計なら、運用上の対象範囲を狭められる。ただしStackSets委任管理者のサービス上の範囲が変わるわけではない。
C: Organizationsに属さない外部アカウントや、trusted accessを使えない環境へ展開し、管理・実行ロールを明示的に管理する必要がある場合はself-managed permissionsが適する。
D: 単一アカウントの通常のCloudFormationスタックで、必要なCapabilitiesを承認し、サポートされるマクロやネストされたスタックを使う場合なら利用できる。

7. 今後使える判断基準

StackSetsでは、実際のターゲット、権限モデル、管理主体を分けて読む。OU自動追随とロール自動管理はservice-managed、Organizations外を含む明示アカウントと自前ロールはself-managedが基本である。委任管理者は「管理アカウントを使わずに済む低権限ロール」ではなく、組織全体へ展開可能な強い主体として扱う。

8. 関連サービスとの比較

Organizationsのtrusted accessはStackSetsが組織構造と必要なロールを利用するための連携である。委任管理者は日常管理をメンバーアカウントへ移す。SCPはメンバーアカウントの利用可能な最大権限を制御できるが、StackSets委任登録時に特定OUだけを選ぶ機能の代わりにはならない。CloudTrailは誰がどのStackSet操作を行ったかの監査を補完する。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4

問題 034 | Domain 5 / ネットワーク | 本番相当 | 四択（1つ選択）

問題 34 5%だけ新環境へ流すDNSカナリア

同一リージョンに、現行版と新版のAPIをそれぞれ別のALBで稼働させている。運用チームは、同じホスト名を使用したまま新版へ約5%のDNSトラフィックを送り、24時間監視した後に比率を段階的に上げたい。どちらかのALBが異常な場合は、その宛先をDNS応答から除外したい。クライアント実装の変更はできず、セッション固定性は要件ではない。

最も運用負荷の低い構成はどれか。

選択肢

A	2つのWeighted Aliasレコードを重み95と5で作成し、それぞれのターゲットヘルスを評価する。
B	2つのFailover AliasレコードをPrimaryとSecondaryで作成し、TTLを同じにする。
C	2つのGeolocationレコードを作成し、同じ地域を割り当てる。
D	ALBのリスナールールで送信元IPの末尾5%を新版へ転送する。

ここでいったん止める | 解答と解説は次ページ

問題 034 正解・解説 本番相当

問題 34の正解・解説

1. 正解

A

2. 問題文の重要な条件

同一名で95対5の比率、段階変更、異常宛先の除外が必要である。地域や低遅延ではなく、意図した比率でのカナリアである。

3. 正解へ至る判断過程

Weightedルーティングは同じ名前・型の複数レコードへ相対的な重みを付けられる。AliasでALBを参照し、Evaluate Target Healthを有効にすれば、異常なALBを応答対象から外せる。

4. 正解が要件を満たす理由

重みの更新だけで5%から段階的に増やせる。クライアントやアプリケーションを変更せず、ALBの可用性もDNS判断へ反映できる。

5. 各不正解選択肢が不適切な理由

A: 正解肢のため対象外。
B: Failoverは正常時にPrimaryへ寄せるactive-passiveであり、5%を継続的に流す目的と異なる。
C: Geolocationは利用者の位置で振り分けるため、全体の5%を保証しない。同一地域の重複指定も目的に合わない。
D: ALBルールの条件だけで「IP末尾5%」という比率分散は提供されず、送信元IP分布にも偏りがある。

6. 各不正解選択肢が正解になり得る条件

Bは待機系へ障害時だけ切り替える場合、Cは法令・言語・地域別コンテンツで宛先を変える場合に適する。Dはヘッダー、パス、ホスト名など明示的な条件で同じALBのターゲットグループを分ける場合に有効である。

7. 今後使える判断基準

比率を数値で操作するならWeighted。DNSベースの比率は各問い合わせに対する確率であり、少数クライアントや長いDNSキャッシュでは実測比率が厳密な5%にならない点も押さえる。

8. 関連サービスとの比較

ALBのweighted target groupsでも比率分散でき、DNSキャッシュの影響を受けにくい。同一ALB内のリリースならALB、別リージョン・別ALBをDNSで段階移行するならRoute 53 Weightedを比較する。

公式確認先 AWS公式 1 / AWS公式 2

問題 035 | Domain 4 / セキュリティ | 本番より難しい | 四択（1つ選択）

問題 35 許可リージョン外の操作を組織で拒否する

規制により、メンバーアカウントのリージョナルリソースは東京と大阪でだけ作成できる。IAM、Route 53、CloudFront、Organizationsなど必要なグローバルサービスの操作は継続させる。各アカウント管理者がローカルIAMポリシーを変更してもこの制約を回避できないようにし、新規アカウントへも自動適用したい。

最適な実装はどれか。

選択肢

A	各IAMユーザーのコンソール設定で既定リージョンを東京にする。
B	AWS Config aggregatorで許可外リージョンのリソースを表示し、月次で削除する。
C	各アカウントのAdministratorAccessポリシーをコピーして、東京と大阪だけを記述する。
D	aws:RequestedRegionを使い、必要なグローバルサービス操作をNotAction等で除外するRegion-deny SCP（またはControl TowerのRegion deny control）を対象OUへ適用する。

ここでいったん止める | 解答と解説は次ページ

問題 035 正解・解説 本番より難しい

問題 35の正解・解説

1. 正解

D

2. 問題文の重要な条件

組織全体で予防的に強制し、ローカル管理者が回避できず、新規アカウントへ継承し、グローバルサービスは壊さない必要がある。

3. 正解へ至る判断過程

OUのSCPは配下アカウントへ継承され、明示的DenyをローカルIAMのAllowで覆せない。aws:RequestedRegionで許可外リージョンを拒否しつつ、IAM等のグローバルサービスに必要な操作を慎重に除外する。

4. 正解が要件を満たす理由

リソース作成前にAPIを拒否する予防的統制であり、新規アカウントもOUへ配置すれば対象になる。Control Tower利用時は管理されたRegion deny controlで同じ目的を実装できる。

5. 各不正解選択肢が不適切な理由

A: UIの既定値であり、CLI/APIや利用者変更を禁止しない。
B: 検出的で、規制違反リソースが一時的に作成される。Aggregator自体は削除を強制しない。
C: すべての主体・新規ポリシーへ確実に適用されず、管理者が別Allowを作成できる。
D: 正解肢のため対象外。

6. 各不正解選択肢が正解になり得る条件

Aは利便性向上、Bは既存リソースの可視化と補助的な是正、Cは個別職務ロールの権限付与には使える。いずれも組織の非回避な最大権限にはSCPを代替しない。

7. 今後使える判断基準

リージョン制約はグローバルサービス例外が落とし穴である。aws:RequestedRegionのDenyだけを単純適用せず、グローバルなAPIとリージョン別副作用を確認する。

8. 関連サービスとの比較

SCP/Control Tower preventive controlは作成を拒否、Config ruleは作成後の非準拠検出、conformance packは複数ルールと是正を組織展開する。予防と検出を併用すると強い。

公式確認先 AWS公式 1 / AWS公式 2

問題 036 | Domain 1 / 監視・性能 | 本番より難しい | 四択（1つ選択）

問題 36 MPI基盤の配置とEFA

ある研究機関は、64台のEC2インスタンスでMPIベースの流体解析を実行します。各反復で全ノード間の小さなメッセージ交換が頻繁に発生し、現在は計算時間より通信待ち時間が支配的です。アプリケーションはLibfabricを利用でき、候補インスタンスタイプはElastic Fabric Adapter（EFA）をサポートしています。

解析ジョブはチェックポイントから再実行できるため、単一アベイラビリティーゾーン障害への耐性よりも、ジョブ実行中の低レイテンシーと高いノード間スループットを優先します。インスタンスにパブリックIPは不要です。セキュリティ部門は、必要な通信だけを許可しつつ、EFAのOS-bypass機能を正しく動作させるよう求めています。

最も適切な構成はどれですか。

選択肢

A 64台を複数アベイラビリティーゾーンにまたがるパーティションプレイスメントグループへ配置し、ENAを有効化する。各パーティションを別AZへ固定して障害分離を最大化する。

B 64台を同一アベイラビリティーゾーンかつ同一サブネットのクラスタープレイスメントグループへ配置し、EFA対応AMI、EFAドライバー、Libfabricを使用する。EFAに関連付けるセキュリティグループで、そのセキュリティグループ自身を送信元・宛先とする全インバウンド・アウトバウンド通信を許可する。

C 64台をラックレベルのスプレッドプレイスメントグループへ配置し、EFAを有効化する。各インスタンスを別の基盤ハードウェアへ分散すれば、同時に最大の帯域幅も得られる。

D 64台を同一AZのクラスタープレイスメントグループへ配置するが、EFAは使わずENA Expressだけを有効化する。TCP単一フロー性能が向上するため、LibfabricのOS-bypassと同等のMPI性能になる。

ここでいったん止める | 解答と解説は次ページ

問題 036 正解・解説 本番より難しい

問題 36の正解・解説

1. 正解

B

2. 問題文の重要な条件

- MPIの反復ごとに密結合ノード間通信があり、低レイテンシーが主要目的である。
- Libfabricを利用でき、インスタンスタイプもEFA対応である。
- AZ障害耐性より、単一ジョブの性能を優先できる。
- 64台という規模は小規模なスプレッド配置に向かない。
- EFAのOS-bypassを使うには、ドライバーだけでなくセキュリティグループの自己参照通信も満たす必要がある。

3. 正解へ至る判断過程

まずワークロードを「密結合HPC」と分類します。クラスタープレイスメントグループは同一AZの高い二分帯域幅を持つネットワークセグメントへインスタンスを近接配置し、低レイテンシー・高スループットを狙う方式です。次に、従来のIPネットワーキングを提供するENAと、SRDおよびOS-bypassを提供するEFAを区別します。MPIアプリケーションがLibfabricを使えるのでEFAの利点を活かせます。

最後に実装条件を確認します。EFA対応インスタンス、対応AMIまたはドライバー、Libfabricが必要です。EFAトラフィックはルーティングできずAZやVPCを越えないため、通信ノードを同じサブネットへ配置します。OS-bypass通信を有効にするには、EFAが属するセキュリティグループで同じセキュリティグループからの全トラフィックを双方向に許可します。この自己参照許可はインターネットへの全開放ではありません。

4. 正解が要件を満たす理由

Bは、クラスタープレイスメントグループで物理的ネットワーク配置を最適化し、EFAでカーネルのネットワークスタックを迂回する低遅延通信を提供します。SRDによる信頼性と輻輳制御も密結合HPCに適します。単一AZという可用性上のトレードオフはありますが、問題文ではチェックポイント再実行が可能で性能を優先すると明示されています。自己参照セキュリティグループにより、クラスターノード間だけでEFA通信を成立させられます。

5. 各不正解選択肢が不適切な理由

- **A:** パーティションプレイスメントグループは、Kafka、Cassandra、Hadoopのような大規模分散ワークロードで相関障害を隔離する目的に適します。AZやパーティションをまたぐ配置は、各反復で全ノードが同期するMPIの最低レイテンシー要件と相反します。ENAにもEFAのOS-bypassはありません。
- **C:** スプレッドプレイスメントグループは少数の重要インスタンスを別ハードウェアへ厳格に分散する方式で、密結合性能を最大化する配置ではありません。ラックレベルのスプレッドには1AZあたりの実行インスタンス数制限があり、64台の単一クラスター用途にも合いません。
- **D:** ENA ExpressはSRDによりTCP/UDPの単一フロー帯域やテールレイテンシーを改善できますが、EFAのLibfabric OS-bypassインターフェイスと同一ではありません。アプリケーションがEFAを活用できる密結合MPIでは、EFAを外す理由がありません。

6. 各不正解選択肢が正解になり得る条件

- **Aが適切になる条件:** ノードが疎結合で、レプリケーションを持つ分散データ基盤についてラック・パーティション障害の影響範囲を限定することが、通信レイテンシーより重要な場合です。

- **Cが適切になる条件:** ごく少数のクリティカルなインスタンスを別ハードウェアへ分離し、同時障害を避けたい場合です。例えば小規模なアクティブ・スタンバイ構成が該当します。
- **Dが適切になる条件:** アプリケーションが通常のTCP/UDPしか利用せずLibfabricへ対応できない、またはインスタンスがEFA非対応で、同一リージョン内の単一フロー性能を改善したい場合です。

7. 今後使える判断基準

プレイスメントグループは、**性能ならcluster、少数ノードの相関障害分離ならspread、大規模分散システムの障害ドメイン分割ならpartition**と整理します。ENAは高性能な通常IPネットワーク、EFAは密結合HPC・分散学習向けのOS-bypassです。クラスタープレイスメントグループは単一AZの性能を得る代わりに、AZ障害耐性を失う点まで含めて判断します。

8. 関連サービスとの比較

- **ENA:** SR-IOVを使う拡張ネットワーキングで、通常のIP通信を高帯域・低CPU負荷で提供します。
- **ENA Express:** SRDを通常のTCP/UDPへ適用し、対応通信の単一フロー帯域やテールレイテンシーを改善します。
- **EFA:** ENA機能に加えてLibfabricから利用するOS-bypassを備え、MPIや分散MLに適します。
- **Capacity Reservation:** クラスタープレイスメントグループ内の起動キャパシティ確保に利用できますが、ネットワーク方式そのものではありません。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4

問題 037 | Domain 2 / 信頼性・BC | 本番相当 | 四択（1つ選択）

問題 37 プライベートIPの装置をDNSフェイルオーバーする

企業のVPC内には、AWSサービスではない仮想アプライアンスが2つあり、いずれもプライベートIPだけを持つ。社内クライアントはRoute 53プライベートホストゾーンの proxy.corp.example を利用する。通常はプライマリだけへ接続し、プライマリのアプリケーション処理が5分以上失敗した場合にセカンダリへ切り替えたい。

Route 53のヘルスチェッカーはVPC内のプライベートIPへ直接到達できない。既に、VPC内の合成監視から送られる標準解像度のCloudWatchメトリクスと、そのメトリクスに基づくアラームがある。公開IPを付与せず、DNSフェイルオーバーを構成する最も適切な方法はどれか。

選択肢

A	プライベートIPを直接監視するHTTP Route 53ヘルスチェックを作成し、プライマリのAレコードだけに関連付ける
B	2つのプライベートIPを単一のシンプルルーティングAレコードに登録し、TTLを短くする
C	マルチバリュー回答ルーティングで2つのIPを常に返し、クライアント側の接続タイムアウトだけに任せる
D	CloudWatchアラームのデータストリームを監視するRoute 53ヘルスチェックを作成し、プライベートホストゾーンにプライマリ/セカンダリのフェイルオーバーレコードを構成する

ここでいったん止める　解答と解説は次ページ

問題 037 正解・解説 本番相当

問題 37の正解・解説

1. 正解

D

2. 問題文の重要な条件

- エンドポイントはプライベートIPのみで、Route 53ヘルスチェッカーから直接到達できない。
- 既にVPC内からの合成監視とCloudWatchメトリクスがある。
- active/passiveで切り替えたい。
- 公開IPを付けられない。

3. 正解へ至る判断過程

Route 53の外部ヘルスチェッカーでプライベートIPを直接監視するのではなく、VPC内から観測した状態をCloudWatchへ出し、そのデータストリームをRoute 53ヘルスチェックに評価させる。トラフィック方針はactive/passiveなので、プライマリとセカンダリのフェイルオーバーレコードを使う。

4. 正解が要件を満たす理由

Route 53はCloudWatchアラームが監視するメトリクスのデータストリームを基にヘルスチェック状態を決められる。これにより、外部から直接到達できないVPC内エンドポイントも、内部合成監視の結果でDNSフェイルオーバーできる。フェイルオーバールーティングはプライマリが異常なときにセカンダリを返すactive/passive用途に合う。

5. 各不正解選択肢が不適切な理由

- A：Route 53のヘルスチェッカーはVPC外にあり、公開到達性のないプライベートIPを直接確認できない。
- B：シンプルルーティングではヘルスに基づくactive/passive切替にならず、短いTTLだけでは異常IPを除外できない。
- C：両方を返すactive/active寄りの方式であり、プライマリ優先とサーバー側の一元的な切替要件を満たさない。

6. 各不正解選択肢が正解になり得る条件

- A：エンドポイントにRoute 53ヘルスチェッカーから到達できる公開IPまたは公開FQDNがある場合。
- B：単一の健全なエンドポイントしかなく、フェイルオーバーを必要としない場合。
- C：各クライアントが複数IPの再試行を正しく実装し、両系を通常時から利用する場合。

7. 今後使える判断基準

プライベートエンドポイントのDNSヘルス判定では、直接到達性を最初に確認する。到達できないなら、CloudWatchメトリクス/アラームを監視するヘルスチェックを使う。ELBのエイリアスターゲットであれば Evaluate Target Health という別の選択肢もある。

8. 関連サービスとの比較

フェイルオーバールーティングはactive/passive、マルチバリュー回答や重み付け・レイテンシールーティングは複数の正常リソースを利用するactive/activeに使える。Evaluate Target Health はALB/NLBなどエイリアス先のAWSリソースの状態を評価する。本問のような任意のプライベートIPでは、内部監視結果をCloudWatch経由で渡す。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3

問題 038 | Domain 3 / 展開・自動化 | 本番相当 | 四択（1つ選択）

問題 38 CDKアセットをCIから展開する

開発チームはAWS CDK v2で、Lambda関数のローカルソースコードとECS用Dockerイメージを含むアプリケーションを定義している。CIパイプラインから開発・本番の2アカウント、各2リージョンへ展開する。プルリクエストでは生成されるCloudFormationの差分とIAM変更を確認し、本番ではCloudFormationのスタック履歴、ロールバック、ドリフト検出を維持したい。

現在、cdk synthは成功するが、最初の本番リージョンへのcdk deployでアセット用バケットまたはECRリポジトリが見つからないというエラーになる。開発者端末から本番へ直接アップロードすることは許可されない。

最も適切な対応はどれか。

選択肢

A cdk synthが成功しているためbootstrapは不要である。生成されたテンプレートだけを各リージョンのCloudFormationへ直接渡し、ローカルアセット参照はCloudFormationが開発者端末から取得するよう設定する

B CI用の信頼と最小権限を設計したうえで、展開対象の各アカウント・リージョンを現行のCDK bootstrap templateでbootstrapする。CIでテスト、cdk synth、cdk diffを行い、承認後にアセットをbootstrap資源へ発行してcdk deployでCloudFormationスタックを更新する

C LambdaコードとDockerイメージをテンプレート本文へBase64で埋め込み、CloudFormationのテンプレートサイズ上限を引き上げる。これにより全環境を1回だけbootstrapすればよい

D 本番でもcdk deploy --hotswapだけを使い、LambdaとECSをCloudFormationの外側で直接更新する。高速なためスタックテンプレートとの差分やドリフトは発生しない

ここでいったん止める | 解答と解説は次ページ

問題 038 正解・解説 本番相当

問題 38の正解・解説

1. 正解

B

2. 問題文の重要な条件

- LambdaソースとDockerイメージというCDK assetがある。
- 展開先は複数アカウント・複数リージョンであり、環境ごとのbootstrapが必要である。
- CIだけが本番へ発行・展開する。
- PRでテンプレートとIAM差分を確認する。
- 本番の実変更はCloudFormation管理下に置き、履歴・ロールバック・ドリフト検出を保つ。

3. 正解へ至る判断過程

cdk synthはCDKアプリケーションからcloud assemblyとCloudFormationテンプレートを生成する処理であり、展開先にアセット保管先があることを保証しない。ファイルassetにはS3、Docker image assetにはECRなどのbootstrap資源と、デプロイ用ロールが必要になる。そのため、CIから展開する各環境をbootstrapし、信頼するCI主体と権限を明示する。

レビューではテスト、synth、diffを行い、生成物とセキュリティに影響する差分を確認する。承認後のdeployでアセットを発行し、CloudFormationを介して更新する。

4. 正解が要件を満たす理由

Bは各アカウント・リージョンにCDKToolkit bootstrap stackを作り、アセット保管先とCDKが使用するデプロイロールを準備する。CIだけを信頼する構成にすれば、開発者端末へ本番資格情報を渡さずに済む。cdk diffで事前確認し、通常のcdk deployを使用することで最終的なインフラ状態はCloudFormationスタックに記録される。

5. 各不正解選択肢が不適切な理由

A: CloudFormationはCIや開発者端末のローカルパスからassetを取得できない。synth成功と展開環境のbootstrap済みは別条件である。
B: 正解肢のため対象外。
C: DockerイメージをCloudFormation本文へ埋め込む方式はなく、大きなLambda assetもテンプレート上限と再利用性の点で不適切である。bootstrapは原則として対象環境ごとに必要である。
D: hotswapはCloudFormationの外で直接変更する開発高速化機能であり、スタック状態との意図的な差異を生み得る。本番でCloudFormation履歴とロールバックを維持する要件に反する。

6. 各不正解選択肢が正解になり得る条件

A: 外部assetを一切含まず、テンプレートがすでにS3 URIやECR digestなど展開先から参照可能な不変成果物だけを指し、CloudFormationを別パイプラインで直接展開する場合はCDK deployを使わない選択もできる。
C: ごく小さなインラインLambdaコードをCloudFormationの対応プロパティへ記述する単純な検証用途なら、S3 assetを使わずに済む場合がある。Docker imageには当てはまらない。
D: 個人の開発環境で反復速度を優先し、後で通常deployによりCloudFormationへ同期する前提ならhotswapを利用できる。

7. 今後使える判断基準

CDKでは、constructを評価するsynth、展開済み状態との差を見るdiff、環境側の共通資源を作るbootstrap、asset発行とCloudFormation更新を行うdeployを区別する。ローカルファイルやDocker imageを含むなら、テンプレートだけを渡して終わりではない。bootstrapの信頼設定は本番へ到達できる主体を決めるため、管理者権限を無条件に与えない。

8. 関連サービスとの比較

CDKは最終的にCloudFormationテンプレートとasset manifestなどを含むcloud assemblyを合成する。CloudFormationがリソースライフサイクルを管理し、S3/ECRはassetを保持する。SAMもサーバーレスassetのパッケージ・展開を支援するが、CDKアプリ全体のbootstrap資源を自動的に代替するわけではない。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4

問題 039 | Domain 5 / ネットワーク | 本番より難しい | 四択（1つ選択）

問題 39 更新した静的ファイルが古いまま見える

S3をオリジンとするCloudFrontディストリビューションでWebアセットを配信している。デプロイ時に/app.jsを同じキーで上書きしたところ、一部のエッジロケーションでは旧版が数時間返り続けた。オリジンのオブジェクトは正しく更新されている。今回は数分以内に新版へ統一し、今後は緊急デプロイのたびにディストリビューション全体を無効化するコストと運用を避けたい。アセット名をビルド時に変更することは可能である。

最適な対応はどれか。

選択肢

A	S3 Transfer Accelerationを有効にし、同じ/app.jsを再アップロードする。
B	CloudFrontのPrice ClassをAllへ変更し、全エッジへ即時複製させる。
C	S3の整合性が落ち着くまで待ち、CloudFrontのMinimum TTLを増やす。
D	今回は/app.jsを対象にinvalidatonを実行し、以後は内容ハッシュを含む版付きファイル名と適切なCache-Controlを使う。

ここでいったん止める | 解答と解説は次ページ

問題 039 正解・解説 本番より難しい

問題 39の正解・解説

1. 正解

D

2. 問題文の重要な条件

CloudFrontキャッシュだけが古く、今回は急いで統一する必要がある。一方で今後の全体invalidatonを避けられ、ファイル名を変更できる。

3. 正解へ至る判断過程

現在キャッシュ済みの同一キーを早く追い出すには対象パスのinvalidatonが直接的である。将来はapp.<hash>.jsのような版付きキーにすれば、新版は別オブジェクトとして取得され、旧版を長くキャッシュしても問題にならない。HTML側だけ短いTTLで更新する設計が一般的である。

4. 正解が要件を満たす理由

対象を限定したinvalidatonで今回の影響を短くし、以後はキャッシュの利点を維持しながらデプロイごとの無効化をほぼ不要にできる。Cache-ControlによりブラウザとCloudFrontのTTLも意図的に制御できる。

5. 各不正解選択肢が不適切な理由

A: Transfer AccelerationはS3への長距離転送を高速化する機能で、CloudFrontの既存キャッシュを削除しない。
B: Price Classは使用するエッジ地域を制限する料金設定であり、キャッシュ更新機構ではない。
C: S3は更新後も強い読み取り整合性を提供する。Minimum TTLを増やすと古いキャッシュをさらに長く保持する。
D: 正解肢のため対象外。

6. 各不正解選択肢が正解になり得る条件

Aは遠隔拠点からS3へ大容量を直接アップロードする遅延が問題なら候補になる。Bは配信地域と料金の最適化に使う。Cの長いTTLは内容不変の版付きアセットでキャッシュヒット率を上げる場合に有効である。

7. 今後使える判断基準

同じキーの緊急更新は限定invalidaton、継続的な静的アセット配信は版付きキー + 長いTTL、頻繁に変わる入口HTMLは短いTTL、と役割を分ける。

8. 関連サービスとの比較

CloudFront invalidatonはエッジキャッシュを期限前に削除する。S3 Lifecycleは保存クラス移行・期限切れ、Transfer AccelerationはS3への転送経路、Origin Shieldはオリジン負荷軽減であり、古いキーの即時更新とは目的が異なる。

公式確認先 AWS公式 1 / AWS公式 2

問題 040 | Domain 4 / セキュリティ | 本番より難しい | 四択（1つ選択）

問題 40 複数ルールと是正を全アカウントへ配る

企業はOrganizationsの80アカウントに対し、S3暗号化、EBS暗号化、必須タグ、セキュリティグループの公開禁止など20個のAWS Config ruleと、承認済みのSystems Manager Automationによる一部自動是正を同じパラメーターで配布したい。各メンバーアカウントがルールや是正設定を変更できないようにし、中央から版を更新する。全リージョンの結果は別途一画面で参照したい。

最適な中核機能はどれか。

選択肢

A	Config aggregatorだけを作成し、集約先から各メンバーへルールを自動生成する。
B	OrganizationsのAWS Config organization conformance packとして、ルールとremediation actionsを一つのテンプレートで展開する。可視化にはConfig aggregatorを併用する。
C	20個のCloudWatch Alarmを管理アカウントだけに作成する。
D	SCPに20個のConfig rule名を記述し、非準拠リソースを自動削除させる。

ここでいったん止める | 解答と解説は次ページ

問題 040 正解・解説 本番より難しい

問題 40の正解・解説

1. 正解

B

2. 問題文の重要な条件

複数のConfig rulesと是正を一単位で、組織全体へ中央展開・更新し、メンバー変更を防ぎたい。集約表示も必要だが配布とは別である。

3. 正解へ至る判断過程

Organization conformance packは複数のConfig rulesとremediation actionsをテンプレートで組織配布する。メンバー側で基盤ルールを変更できない。Config aggregatorは構成・準拠結果を集めるが、ルールを配布しないため併用する。

4. 正解が要件を満たす理由

一つの版管理された定義から80アカウントへ同じ統制を展開し、更新・除外も中央管理できる。Aggregatorを追加すればマルチアカウント・マルチリージョンの結果を参照できる。

5. 各不正解選択肢が不適切な理由

A: Aggregatorは読み取り集約であり、source accountsへrulesやremediationを作成しない。
B: 正解肢のため対象外。
C: CloudWatch AlarmはConfig rule群と組織的な是正展開を代替しない。
D: SCPはAPI権限の最大範囲を制限するもので、Config ruleを実行・自動削除するエンジンではない。

6. 各不正解選択肢が正解になり得る条件

Aは既に各所へConfig rulesがあり、中央可視化だけが必要なら正解になる。Cは数値メトリクスのしきい値通知、Dは特定APIを事前に禁止する予防統制に適する。

7. 今後使える判断基準

単一チェックはConfig rule、ルール + 是正の束はconformance pack、結果の中央参照はaggregator。似た名称でも「配る」と「集める」を混同しない。

8. 関連サービスとの比較

Control Tower detective controlsもConfigを利用するものがあるが、独自の統制セットをテンプレート化して組織展開する一般機能はorganization conformance packである。Security Hub standardsはセキュリティFindingの標準評価・集約に向く。

公式確認先 AWS公式 1 / AWS公式 2

問題 041 | Domain 1 / 監視・性能 | 本番相当 | 四択（1つ選択）

問題 41 EBSキュー増大のボトルネック判定

ある企業は、NitroベースのEC2インスタンス上でトランザクションデータベースを運用しています。データボリュームはgp3で、8,000 IOPSと500 MiB/sをプロビジョニングしています。ボリュームはスナップショットから作成したものではなく、初期化遅延はありません。平常時のVolumeQueueLengthは2〜4ですが、日中のバッチ処理とオンライン処理が重なる2時間だけ20を超え、VolumeAvgReadLatencyとアプリケーションのp99応答時間が悪化します。

運用チームが同じ時間帯のCloudWatchメトリクスを確認したところ、次の状況でした。

- VolumeIOPSExceededCheckとVolumeThroughputExceededCheckはいずれも0である。
- 実際のボリュームIOPSは8,000未満で、ボリュームのプロビジョンドIOPSには達していない。
- EC2インスタンスのEBSByteBalance%は徐々に低下して0%になり、その時点から遅延が顕著になる。
- CPUUtilizationは35%前後で、メモリにも余裕がある。
- 現在のインスタンスサイズはEBS最適化帯域を一定時間バーストできるが、ベースライン帯域は日中の持続トラフィックより低い。

データベースのストレージ方式を大きく変更せず、最も直接的にボトルネックを解消する対応はどれですか。

選択肢

A gp3のプロビジョンドIOPSを16,000、スループットを1,000 MiB/sへ増やす。VolumeQueueLengthが高いので、ボリューム側の性能不足と判断する。

B ボリュームを同じIOPSのio2 Block Expressへ変更する。平均レイテンシーが低いボリュームタイプへ変更すれば、インスタンスのEBS帯域制限にも影響されなくなる。

C 持続時のEBSベースライン帯域が現在の読書き量を上回るEC2インスタンスサイズへ変更する。ボリューム側の超過チェックとインスタンス側のEBSByteBalance%を併せて監視し、gp3の設定はまず維持する。

D EC2詳細モニタリングを有効化し、VolumeQueueLengthが8を超えたらSNS通知する。詳細モニタリングによりEBSボリュームメトリクスが5分から1分粒度になり、キューも自動的に短縮される。

ここでいったん止める | 解答と解説は次ページ

問題 041 正解・解説 本番相当

問題 41の正解・解説

1. 正解

C

2. 問題文の重要な条件

- ボリュームのIOPS・スループット超過チェックは0で、ボリュームのプロビジョンドIOPSにも未達である。
- EBSByteBalance%が0%へ低下した時点と性能悪化が一致している。
- インスタンスはEBS帯域をバーストできるが、持続時ベースラインが不足している。
- CPU・メモリではなく、EC2とEBSの間の帯域が制約である。
- キュー長は原因そのものではなく、処理しきれないI/Oが待機している結果である。
- ストレージ方式の大幅な変更を避けたい。

3. 正解へ至る判断過程

EBS性能は、ボリュームに設定した性能と、アタッチ先EC2インスタンスが提供できるEBS最適化性能の小さい方に制約されます。したがって、キュー長だけを見てボリュームを増強してはいけません。本問ではVolumeIOPSExceededCheck=0、VolumeThroughputExceededCheck=0で、実IOPSもプロビジョンド値未満です。一方、インスタンスのEBSスループットクレジットを示すEBSByteBalance%が0になった時点で遅延が増えています。ボトルネックはボリュームではなく、インスタンスの持続EBS帯域です。

SSDボリュームでは、目安として利用可能な1,000 IOPSにつきキュー深度1程度から観察・調整しますが、最適値はI/Oサイズとレイテンシー要件で変わります。8,000 IOPSに対して20超というキューは待ちが増えている兆候ではあっても、どの層が上限かは超過メトリクスとインスタンス仕様で確定します。

4. 正解が要件を満たす理由

Cは、日中2時間の持続トラフィックをバーストクレジットへ依存せず処理できるインスタンスへ変更します。CPUやメモリ目的ではないため、候補サイズのEBSベースライン帯域・IOPS上限を確認して選ぶことが重要です。既存gp3はまだ自身の上限に達していないので、まずそのまま利用でき、データ移行も不要です。変更後もボリューム側の超過チェック、レイテンシー、キュー長と、インスタンス側のEBS性能を併せて確認すれば、過不足を検証できます。

5. 各不正解選択肢が不適切な理由

- **A:** ボリュームは現在の8,000 IOPS・500 MiB/s上限を超過していません。インスタンス側の帯域が先に詰まっているため、ボリュームへ追加性能を購入しても利用できず、費用だけ増える可能性が高いです。
- **B:** io2 Block Expressは低レイテンシーと高いプロビジョンドIOPSが必要なワークロードに適しますが、EC2インスタンスのEBS性能上限を迂回しません。アタッチ先が転送できる集約性能を超えれば、ボリュームタイプを変えても同じ層で制限されます。
- **D:** EBSボリュームのCloudWatchメトリクスは自動的に1分間隔で提供され、EC2詳細モニタリングを有効にしなくても本問の観測はできます。通知は検出には役立ちますが、帯域不足を解消しません。

6. 各不正解選択肢が正解になり得る条件

- **Aが適切になる条件:** VolumeIOPSExceededCheckまたはVolumeThroughputExceededCheckが1になり、インスタンス側には十分なEBS帯域があり、ワークロードがボリューム設定値へ到達している場合です。I/Oサイズに応じてIOPSとスループットのどちらを増やすか決めます。

- **Bが適切になる条件:** インスタンス側に十分な余裕があり、gp3の単一桁ミリ秒より低い一貫したレイテンシー、高IOPS、より高い耐久性がデータベース要件として必要な場合です。
- **Dが適切になる条件:** 目的がEC2標準メトリクスを5分から1分粒度へ変更して、CPUなどの短いスパイクを検出することで、性能修復は別に行う場合です。EBSメトリクスの収集粒度を変える手段としては扱いません。

7. 今後使える判断基準

EBSの遅延では、**ボリューム上限、EC2のEBS最適化上限、I/O特性、初期化状態**を順番に確認します。VolumeQueueLengthが高いことだけでは「IOPSを増やす」が答えになりません。IOPS超過、スループット超過、平均レイテンシー、I/Oサイズ、インスタンスのEBSクレジットまたはベースライン仕様を突き合わせます。EBS性能は「ボリューム合計」と「インスタンス上限」の小さい方で決まる、と覚えると判断しやすくなります。

8. 関連サービスとの比較

- **gp3:** 容量、IOPS、スループットを独立して設定できる汎用SSDです。一般的なトランザクション処理に費用対効果があります。
- **io2 Block Express:** 非常に高いIOPS、低く一貫したレイテンシー、高耐久性を必要とする重要データベース向けです。
- **st1:** 大きな連続I/Oのスループットを重視するHDDで、小さなランダムI/Oやブートボリュームには適しません。
- **CloudWatch AgentのEBS NVMe詳細統計:** Nitroインスタンスでは、OS側から高解像度のI/O統計を収集し、キューやレイテンシーの詳細分析を補完できます。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4

問題 042 | Domain 2 / 信頼性・BC | 複合難問 | 四択（1つ選択）

問題 42 誤検知では切り替えない、多リージョンの非常スイッチ

決済会社は、2つのAWSリージョンに同一アプリケーションを配置し、通常はプライマリだけへトラフィックを送る。障害検知は複数の監視系で行うが、外部依存先の一時障害をリージョン障害と誤認する可能性があるため、リージョン間フェイルオーバーはインシデント責任者の承認後にだけ実行する。さらに、操作ミスで両リージョンを同時にトラフィック対象外にすることを防ぎたい。

復旧操作は、障害リージョンの通常のAWSコントロールプレーンに依存せず、訓練時にも同じ手順をAPIで実行できる必要がある。最も適切な構成はどれか。

選択肢

A Amazon Application Recovery Controller（ARC）のルーティングコントロールを各リージョン用に作成し、ルーティングコントロールへルスチェックをRoute 53レコードに関連付ける。少なくとも一方をオンに保つ安全ルールを設定し、承認後にARCのデータプレーンAPIで状態を変更する

B 各リージョンのALBに通常のRoute 53 HTTPヘルスチェックを設定し、失敗を検知したら自動フェイルオーバーさせる

C Global Acceleratorのエンドポイントヘルスチェックだけを使い、異常と判断したリージョンのトラフィックダイヤルを障害リージョン内のLambdaから0にする

D CloudFormationでRoute 53レコードのプライマリ/セカンダリを入れ替える変更セットを作り、障害のたびに障害リージョンでスタック更新する

ここでいったん止める | 解答と解説は次ページ

問題 042 正解・解説 複合難問

問題 42の正解・解説

1. 正解

A

2. 問題文の重要な条件

- 自動検知ではなく、人の承認で切り替える。
- 両リージョンを同時に無効化する誤操作を防ぐ。
- 障害リージョンの通常コントロールプレーンに依存しない。
- APIで反復可能な訓練・実行が必要。

3. 正解へ至る判断過程

ARCルーティングコントロールは、アプリケーション監視とは別のオン/オフスイッチとしてRoute 53のDNSフェイルオーバーを制御する。安全ルールで許されない状態遷移を拒否でき、信頼性を重視したデータプレーンエンドポイントから操作できる。これは手動承認型のフェイルオーバーに合致する。

4. 正解が要件を満たす理由

ルーティングコントロールヘルスチェックは、実エンドポイントを測定する通常のヘルスチェックではなく、ルーティングコントロールの状態をDNSへ反映する。ARCの安全ルールにより、例えば「少なくとも一方のセルはオン」というガードを設定できる。運用チームは承認後にCLI/SDKで高信頼なARCデータプレーンへ接続して切り替えられる。

5. 各不正解選択肢が不適切な理由

- B：監視失敗で自動切替するため、人の承認を必須とする要件に反する。一時的な依存先障害で誤切替する懸念も残る。
- C：自動ヘルス判定が主となり、障害リージョン内Lambdaへの依存も生じる。両系を無効化しない安全ルールの要件も満たさない。
- D：DNS設定のコントロールプレーン変更であり、障害リージョンでの実行に依存する。非常時に変更セットを作る運用も遅く、誤操作防止の専用ガードがない。

6. 各不正解選択肢が正解になり得る条件

- B：アプリケーションのヘルスが単純で誤検知リスクが低く、自動active/passive切替を求める場合。
- C：固定Anycast IPと高速なエンドポイント切替が必要で、Global Acceleratorの自動ヘルスルーティングを受け入れる場合。
- D：計画済みの通常変更としてDNS構成そのものを更新し、緊急復旧のデータプレーン要件がない場合。

7. 今後使える判断基準

通常のRoute 53ヘルスチェックは「状態を測って自動で除外」、ARCルーティングコントロールは「運用判断でトラフィックを明示的に切り替える」。誤切替の影響が大きく、安全な手動スイッチと高可用な制御面を求めるならARCを検討する。

8. 関連サービスとの比較

ARCルーティングコントロールはDNSレコードに関連付けたヘルスチェックをオン/オフする。安全ルールはルーティングコントロールの不正な組み合わせを防ぐ。ARC Region switchは、DNSだけでなくAuto ScalingやAuroraなど複数の復旧手順をワークフローとして順序制御する別機能である。Global AcceleratorはDNSキャッシュを介さずエンドポイントへトラフィックを振り分けるが、本問の承認・安全ルール要件とは異なる。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3

問題 043 | Domain 3 / 展開・自動化 | 本番より難しい | 四択（1つ選択）

問題 43 組織内で共有するTransit Gateway

ネットワークアカウントにある1つのAWS Transit Gatewayを、同じAWS Organizations配下のApplication OUに所属する40アカウントから利用させる。新規アカウントがOUへ追加されたときも共有対象へ含めたい。外部組織のアカウントへの共有は禁止する。Transit Gatewayの所有権とルート管理はネットワークチームに残し、アプリケーションアカウントには自身のVPCをアタッチするために必要な操作だけを許可する。長期アクセスキーや、ネットワークアカウントの管理ロールを各チームへ渡してはならない。

最も適切な構成はどれか。

選択肢

A OrganizationsでApplication OUを作成すればTransit Gatewayは自動的にOUへ共有されるため、AWS RAMの設定や利用者側IAM権限は不要である

B 各アプリケーションアカウントへネットワークアカウントの管理ロールをAssumeRoleさせ、Transit Gatewayをアカウントごとに複製する。VPC peeringで複製したTransit Gateway同士を接続する

C AWS RAMのOrganizations連携を有効化し、ネットワークアカウントでTransit Gatewayのresource shareを作成してApplication OUをprincipalに指定する。外部principalを許可せず、適切なRAM managed permissionを選び、各利用アカウントのIAM主体には共有資源を利用してVPCアタッチメントを作る最小権限を別途付与する

D Transit Gatewayへ手書きのリソースベースポリシーを付ければ、全リージョン・全アカウントから自動利用できる。共有先IAMの明示許可は不要であり、所有権も共有先へ移る

ここでいったん止める | 解答と解説は次ページ

問題 043 正解・解説 本番より難しい

問題 43の正解・解説

1. 正解

C

2. 問題文の重要な条件

- サポートされた単一リソースを複数アカウントで利用し、複製しない。
- 同じOrganizations内のOUを単位に共有し、新規アカウントへ追随する。
- 外部principalを禁止する。
- 所有権と中央管理はネットワークアカウントに残す。
- 共有の成立と、利用者IAMの操作許可を分ける。
- AWS RAMはリージョナルサービスである。

3. 正解へ至る判断過程

Transit GatewayはAWS RAMで共有できる資源である。同一組織・OUへ継続的に共有するため、RAMとOrganizationsの共有を有効化し、OUをresource shareのprincipalにする。外部共有を無効化し、リソースタイプに適したRAM permissionで共有先が行える操作範囲を定義する。

ただしresource shareだけでは、各アプリケーションのIAM principalがAPIを呼ぶidentity-based permissionまで自動付与されない。利用アカウント側で必要なEC2/Transit Gatewayアタッチメント操作を最小権限で許可する。

4. 正解が要件を満たす理由

CはTransit Gatewayを中央所有のまま再利用し、OUへの共有によりアカウント列挙を減らす。組織内共有を有効化した環境では、外部共有のような個別招待受諾を省きやすい。allowExternalPrincipals=false相当の設定とIAM条件を組み合わせれば、組織外共有を防げる。ネットワークチームはTransit Gatewayとルートを管理し、利用者にはVPC接続に必要な範囲だけを与えられる。

5. 各不正解選択肢が不適切な理由

A: OU所属だけでは資源は共有されない。RAM resource shareと、利用するIAM主体への権限が必要である。
B: Transit Gatewayの複製は要件に反し、管理ロール共有も過大権限である。Transit Gateway同士をVPC peeringのように扱う説明も不適切である。
C: 正解肢のため対象外。
D: RAM対応資源の共有を任意の手書きポリシーだけで一般化できない。RAMはリージョナルで、共有により所有権が移転するわけでも、利用者IAM評価が不要になるわけでもない。

6. 各不正解選択肢が正解になり得る条件

A: OUをprincipalとして設定済みのRAM resource shareが存在し、利用者IAMも別途整っているなら、新規アカウントのOU所属により共有対象へ加える運用ができる。
B: 共有非対応資源を各アカウントが独立所有することが規制上必須で、中央テンプレートから複製する設計なら、StackSets等で個別作成する場合がある。
D: リソースサービスが独自のリソースベースポリシーによるクロスアカウントアクセスを正式にサポートし、その方式が要件に合う場合はRAM以外を選べる。それでもidentity-based permissionとの評価は確認する。

7. 今後使える判断基準

RAMの問題では、まず対象がshareable resource typeかを確認し、所有者、consumer、principal、permissionを分ける。同一組織ならOrganizations連携とOU共有、外部なら招待受諾の有無を確認する。resource shareはIAMユーザーへ無条件の操作権限を配る仕組みではない。

8. 関連サービスとの比較

RAMは1つの対応資源をアカウント境界越しに利用させる。StackSetsは同じ構成の資源を各アカウントへ複製する。AssumeRoleは別アカウントの権限で操作する手段であり、資源共有そのものではない。VPC peeringはVPC間接続で、Transit Gatewayの組織的な共有管理とは異なる。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4

問題 044 | Domain 5 / ネットワーク | 本番より難しい | 四択（1つ選択）

問題 44 公開S3バケットを閉じたままCloudFront配信

企業はS3バケット内の機密性のあるダウンロード資料をCloudFrontだけから配信したい。S3 Block Public Accessは維持し、利用者がS3 URLへ直接アクセスすることを禁止する。オリジンのオブジェクトはSSE-KMSで暗号化され、今後も最新の署名方式と細かなバケットポリシー制御を利用したい。CloudFrontでは署名付きURLによる視聴者制御も行う。

最適なオリジンアクセス構成はどれか。

選択肢

A S3静的ウェブサイトエンドポイントをCloudFrontのカスタムオリジンにし、バケットをpublic-readにする。

B Origin Access Control（OAC）を作成してCloudFrontディストリビューションへ関連付け、CloudFrontサービスプリンシパルをディストリビューションARNで制限するバケットポリシーと必要なKMS許可を設定する。

C S3バケットにインターフェイスVPCエンドポイントを作成し、そのエンドポイントのIPだけをCloudFrontで許可する。

D CloudFrontのビューワープロトコルポリシーをHTTPS Onlyにするだけで、S3 Block Public Accessを解除する。

ここでいったん止める | 解答と解説は次ページ

問題 044 正解・解説 本番より難しい

問題 44の正解・解説

1. 正解

B

2. 問題文の重要な条件

S3を非公開に維持し、CloudFrontだけへ許可し、直接URLを拒否する。SSE-KMSと最新の署名方式、ディストリビューション単位の制限も求めている。

3. 正解へ至る判断過程

OACはCloudFrontからS3オリジンへのリクエストをSigV4で署名し、OAIより広い機能を提供する。バケットポリシーのAWS:SourceArnで特定ディストリビューションに限定し、SSE-KMSのキー側にもCloudFrontが復号できる条件付き許可を加える。

4. 正解が要件を満たす理由

S3 Block Public Accessを保ったままCloudFront経由だけを許可できる。視聴者側の署名付きURLは「誰がCloudFrontへアクセスできるか」、OACは「CloudFrontが非公開S3へアクセスできるか」を別々に制御する。

5. 各不正解選択肢が不適切な理由

A: S3 website endpointではOACを使えず、public-readは直接アクセス禁止に反する。
B: 正解肢のため対象外。
C: CloudFrontのマネージドエッジから顧客VPC内の通常のS3インターフェイスエンドポイントを経由させる構成ではない。
D: HTTPSは転送中暗号化であり、オリジン認可を提供しない。Block Public Access解除も要件違反である。

6. 各不正解選択肢が正解になり得る条件

Aは公開静的WebサイトでS3 website固有のリダイレクト機能が必要な場合に限り検討する。CのS3 VPCエンドポイントはVPCやオンプレミスからS3へ私的に接続する場合に使う。DのHTTPS Onlyは視聴者通信の暗号化要件には必要だが、単独ではアクセス制御にならない。

7. 今後使える判断基準

非公開S3をCloudFrontだけに見せるならOAC + バケットポリシー。利用者認可は署名付きURL/Cookie、オリジン認可はOAC、と層を分けて考える。

8. 関連サービスとの比較

OAIは従来方式で、OACが推奨される。OACはS3 REST endpoint向けであり、S3 website endpointはカスタムオリジンとして扱う。AWS WAFはL7リクエスト検査、署名付きURLはコンテンツ利用者の期限付き認可を担う。

公式確認先 AWS公式 1 / AWS公式 2

問題 045 | Domain 4 / セキュリティ | 複合難問 | 四択（1つ選択）

問題 45 Control Towerの統制を作成経路に合わせる

AWS Control Towerで管理する開発OUでは、すべてのS3バケットをCloudFormationから作成している。セキュリティチームは、テンプレートが暗号化要件を満たさない場合にリソース作成そのものを失敗させたい。一方、コンソールやSDKから直接作られた既存リソースも別途検出し、ダッシュボードで非準拠を確認したい。SCPでS3の全作成を禁止するほど強い制約は望まない。

最適なControl Tower controlsの組み合わせ方を説明している選択肢はどれか。

選択肢

A	Detective controlだけでCloudFormationのpre-create処理を失敗させ、直接API作成も同時に拒否する。
B	Proactive controlを有効にすれば、コンソール・SDK・Terraformを含むすべての作成経路を必ず拒否できるため、他のcontrolは不要である。
C	CloudFormation hookに基づくProactive controlで非準拠なstack操作を拒否し、Configに基づくDetective controlで直接作成を含む既存リソースの非準拠を検出する。
D	Mandatory controlを無効化してから、同じ要件をCloudWatch Logs metric filterで実装する。

ここでいったん止める | 解答と解説は次ページ

問題 045 正解・解説 複合難問

問題 45の正解・解説

1. 正解

C

2. 問題文の重要な条件

CloudFormation経由では作成前に止めたいが、直接API等で作られたリソースは検出したい。作成経路が二つあり、予防と検出を組み合わせる必要がある。

3. 正解へ至る判断過程

Control Towerのproactive controlはCloudFormation hookのpreCreate/preUpdateでテンプレートを評価し、非準拠stack操作を失敗させる。一方、direct APIや他IaC経路を必ず止めるものではない。Detective controlは既存構成の非準拠を検出するので補完できる。

4. 正解が要件を満たす理由

主要な作成経路では違反を未然に防ぎ、迂回経路や既存リソースは継続的に可視化できる。S3作成そのものを全面拒否せず、暗号化条件だけを統制する。

5. 各不正解選択肢が不適切な理由

A: Detective controlは違反検出が主で、CloudFormation hookとして作成前に拒否するものではない。
B: Proactive controlの適用対象はCloudFormation stack operationsであり、直接サービスAPI等を網羅しない。
C: 正解肢のため対象外。
D: Mandatory controlはlanding zone運用に必要で任意無効化する前提ではなく、ログフィルターは構成統制を代替しない。

6. 各不正解選択肢が正解になり得る条件

Aのdetectiveだけでよいのは作成後検出で足りる場合。Bは組織が作成経路をCloudFormationへ完全に限定し、別のpreventive controlで迂回も禁止している場合に近づく。Dのmetric filterは特定APIイベントの通知には使える。

7. 今後使える判断基準

Control Towerではbehaviorを読む。PreventiveはSCP/RCP等でAPIを拒否、ProactiveはCloudFormation作成前評価、Detectiveは作成後の準拠検出である。

8. 関連サービスとの比較

Guidance（mandatory、strongly recommended、elective）は推奨度で、behavior（preventive、detective、proactive）は動作方式である。二つの分類軸を混同しない。

公式確認先 AWS公式 1 / AWS公式 2

問題 046 | Domain 1 / 監視・性能 | 本番より難しい | 四択（1つ選択）

問題 46 S3リクエスト急増とKMSスロットリング

あるIoT基盤は、同一リージョンのコンテナ群からAmazon S3の汎用バケットへ、平均20 KiBのオブジェクトを大量にPUTしています。すべての新規オブジェクトは、1つのカスタマーマネージドKMSキーを使うSSE-KMSで暗号化します。通常は毎秒2,000 PUTですが、毎時0分に多数の端末が同期し、30秒以内に毎秒25,000 PUTへ急増します。オブジェクトキーはすべてingest/yyyy/mm/dd/hh/の同じ時刻プレフィックスへ集中します。

負荷試験では、S3クライアントに一時的なHTTP 503 Slow Downが発生し、同時刻にAWS KMSのGenerateDataKeyでThrottlingExceptionも記録されました。クライアントは即時に1回だけ再試行します。セキュリティ部門はカスタマーマネージドKMSキーの利用継続を要求しています。送信元とS3は同じリージョンで、長距離ネットワーク転送はボトルネックではありません。

暗号化要件を維持しながら、性能とリクエスト費用を改善する最も適切な対応はどれですか。

選択肢

A オブジェクト名を連番からUUIDへ変更するが、同じ時刻プレフィックス、同じ急激な開始レート、同じKMS設定を維持する。S3はキー名がランダムならKMS呼出しも自動的に分散する。

B 10個のカスタマーマネージドKMSキーを作り、オブジェクトごとにラウンドロビンする。KMSの暗号化APIクォータはキー単位なので、キー数に比例してアカウントの毎秒クォータも増える。

C S3 Transfer Accelerationを有効化し、20 KiBの各オブジェクトをマルチパートアップロードに変更する。エッジロケーションを経由すれば、S3のプレフィックス拡張とKMSクォータの両方を回避できる。

D S3 Bucket Keyを有効化してS3からKMSへのリクエスト数と費用を減らす。書込みを複数プレフィックスへ分散し、可能なら開始レートを段階的に上げる。AWS SDKの指数バックオフ付き再試行を使用し、残るKMS需要がクォータを超えるならService Quotasで引上げを申請する。S3リクエストメトリクスの5xxも監視する。

ここでいったん止める | 解答と解説は次ページ

問題 046 正解・解説 本番より難しい

問題 46の正解・解説

1. 正解

D

2. 問題文の重要な条件

- 小さなPUTが短時間に12倍以上へ急増し、同じプレフィックスへ集中する。
- S3の503とKMSのスロットリングが同時に観測され、ボトルネックが2層ある。
- SSE-KMSとカスタマーマネージドキーを維持する必要がある。
- 同一リージョンなので、WAN経路短縮は主要因ではない。
- クライアントの即時1回再試行は、段階的なS3内部スケーリングや一時スロットリングへの耐性が低い。
- 性能だけでなくKMSリクエスト費用も改善したい。

3. 正解へ至る判断過程

まず、S3の503 Slow DownとKMSのThrottlingExceptionを別々の制約として扱います。S3は高いリクエストレートへ自動的にスケールしますが、急激な新規レートへ内部最適化している間は一時的な503が起こり得ます。複数プレフィックスへリクエストを分け、負荷を可能な範囲で徐々に増やし、指数バックオフと十分な再試行を実装するのが適切です。

次にSSE-KMSです。S3 Bucket Keyを有効にすると、S3が時限的なバケットレベルキーを使用するため、個々のオブジェクト処理でS3からKMSへ送られるリクエストを大幅に減らせます。これによりKMSコストとスロットリング圧力の両方が下がります。それでもアカウント・リージョンの共有暗号オペレーションクォータを超えるなら、実測に基づいてクォータ引上げを申請します。

4. 正解が要件を満たす理由

Dは、S3側とKMS側の両方へ対策します。プレフィックス分散と段階的なランプアップはS3の並列スケールを活かし、SDKのバックオフは一時的な503を吸収します。Bucket Keyは暗号化をSSE-KMSのまま維持し、元のカスタマーマネージドキーでバケットレベルキーを保護しつつ、KMSへの直接リクエスト頻度を削減します。CloudWatchのS3リクエストメトリクスを有効にすれば、プレフィックスなどのフィルターごとに5xx、レイテンシー、リクエスト数を確認できます。

5. 各不正解選択肢が不適切な理由

- **A:** 現在のS3は高リクエスト性能のためにランダムなキー名を必須としません。UUID化だけでは、同一プレフィックスへの急激な25,000 PUT、再試行不足、S3からKMSへの呼出し数を解決しません。S3キーの分散とKMSクォータは別問題です。
- **B:** 対称KMSキーに対する暗号オペレーションのリクエストクォータは、通常、アカウントとリージョンで共有されます。キーを増やすだけで共有クォータが10倍になるわけではなく、キー管理・ポリシー・ローテーションの負荷を増やします。
- **C:** Transfer Accelerationは遠距離クライアントからS3への転送をAWSエッジネットワークで高速化する用途です。同一リージョンの小オブジェクト大量PUTには適合せず、S3内部のリクエストスケーリングやKMS APIクォータも回避しません。20 KiBをマルチパート化するとリクエスト数と複雑性がかえって増えます。

6. 各不正解選択肢が正解になり得る条件

- **Aが適切になる条件:** 特定のキーへ同時PUTして競合している、またはアプリケーション上のホットキーを分散する必要がある場合です。UUID化は一意性にも役立ちますが、KMS対策は別途必要です。

- **Bが適切になる条件:** テナント分離、異なるキーポリシー、独立した失効・監査境界が必要で、性能ではなく暗号鍵の分離が目的の場合です。クォータはキーを増やす前に対象リージョンのKMS仕様を確認します。
- **Cが適切になる条件:** 世界各地のクライアントから大きなオブジェクトをアップロードし、インターネット経路の距離と変動が主要ボトルネックである場合です。大容量オブジェクトのマルチパートアップロードは並列性と再試行効率を改善します。

7. 今後使える判断基準

S3性能問題では、**リクエストレート、オブジェクトサイズ、プレフィックス、クライアント並列性、再試行、暗号化先サービス**を確認します。503 Slow DownはS3の一時スケーリング、KMS ThrottlingはKMSの共有クォータとして分離して診断します。SSE-KMS大量アクセスで費用・スロットリングが問題ならBucket Keyを第一候補にし、複数KMSキーへの分散が共有クォータを増やすとは考えません。

8. 関連サービスとの比較

- **S3 Bucket Key:** SSE-KMSのKMSリクエスト数と費用を大幅に減らします。暗号化方式をSSE-S3へ変更する機能ではありません。
- **S3 Transfer Acceleration:** 遠距離クライアントのインターネット転送を高速化します。リクエストレートやKMSクォータの対策ではありません。
- **CloudFront:** 読取りのキャッシュやエッジ配信には有効ですが、新規小オブジェクトの高頻度PUT取り込みとは主目的が異なります。
- **S3リクエストメトリクス / Storage Lens詳細ステータスコード:** 5xxや503の傾向、プレフィックス別の問題を特定する観測手段です。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4 / AWS公式 5

問題 047 | Domain 2 / 信頼性・BC | 本番相当 | 四択（1つ選択）

問題 47 読み取り性能ではなくAZ障害からの自動復旧

受注管理システムはAmazon RDS for MySQLのSingle-AZ DBインスタンスを使用している。処理の80%は更新であり、読み取り負荷には余裕がある。事業部は、DBインスタンスまたはアベイラビリティーゾーン障害時の手作業をなくし、同じリージョン内で数分程度に自動復旧したい。直前にコミットされたトランザクションの損失は認められない。アプリケーションの接続先を平常時と障害時で手動変更したくなく、必要以上の読み取り用インスタンス費用も避けたい。

最も適切な変更はどれか。

選択肢

A	同じAZにRDSリードレプリカを1台作り、障害時に手動昇格して接続文字列を変更する
B	RDSを1台のスタンバイを持つMulti-AZ DBインスタンス配置へ変更し、既存のDBエンドポイントを利用し続ける
C	1日1回の自動バックアップと、15分ごとのEBSスナップショットを設定する
D	1つのライターと2つの読み取り可能なスタンバイを持つMulti-AZ DBクラスターへ必ず移行する

ここでいったん止める | 解答と解説は次ページ

問題 047 正解・解説 本番相当

問題 47の正解・解説

1. 正解

B

2. 問題文の重要な条件

- 同一リージョン内のAZ/インスタンス障害対策。
- 自動フェイルオーバー、コミット済みデータ損失不可。
- 読み取りスケールは不要。
- 接続先の手動変更と不要な費用を避ける。

3. 正解へ至る判断過程

これは読み取り性能ではなく高可用性の要件である。RDS Multi-AZ DBインスタンス配置は、別AZのスタンバイへ同期的に複製し、障害時にRDSが自動フェイルオーバーする。スタンバイは読み取りに使えないが、本問では読み取り容量を必要としていないため問題にならない。

4. 正解が要件を満たす理由

Multi-AZ DBインスタンス配置では、プライマリと別AZのスタンバイが同一DBエンドポイントを共有する。計画保守やインフラ障害時にRDSがスタンバイへ自動切替するため、手動昇格や接続文字列の変更を避けられる。読み取り用に2台を追加するMulti-AZ DBクラスターより、本問の要件に対して費用を抑えやすい。

5. 各不正解選択肢が不適切な理由

- A：同じAZではAZ障害を耐えられず、非同期レプリケーション、手動昇格、接続変更によりRPO/RTOと運用要件を満たさない。
- C：バックアップは復元可能性を提供するが、数分の自動フェイルオーバーにはならない。RDSの基盤EBSを利用者が個別スナップショットする設計でもない。
- D：高可用性は満たすが、2つの読み取り可能なスタンバイの費用と機能が不要で、最適解ではない。

6. 各不正解選択肢が正解になり得る条件

- A：読み取りスケールが主目的で、非同期遅延と手動昇格を許容する場合。AZ耐障害性が必要なら別AZに置く。
- C：RTOが数時間で、費用最小のバックアップ/リストア戦略を採る場合。
- D：同時に読み取りスループットを増やし、3AZにまたがる2台の読み取り可能なフェイルオーバー先を必要とする場合。

7. 今後使える判断基準

RDSでは「Multi-AZ＝高可用性」「リードレプリカ＝読み取りスケール/非同期DR」を起点に考える。Multi-AZ DBインスタンスのスタンバイは読み取り不可、Multi-AZ DBクラスターの2台のスタンバイは読み取り可能という違いも条件に使う。

8. 関連サービスとの比較

Multi-AZ DBインスタンスは1ライター＋1非読取スタンバイ、Multi-AZ DBクラスターは1ライター＋2読取可能インスタンスを3AZに配置する。リードレプリカは非同期で、通常は読み取り分散に使い、昇格時は独立DBとなる。スナップショット/PITRは新しいDBを復元する方式で、稼働中のエンドポイントの自動引継ぎではない。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3

問題 048 | Domain 3 / 展開・自動化 | 本番より難しい | 四択（1つ選択）

問題 48 制約付きセルフサービス製品

中央クラウドチームは、データ分析環境をCloudFormationテンプレートとして標準化した。20のメンバーアカウントにいる研究者が、承認済みバージョンをセルフサービスで起動・更新・終了できるようにしたい。ただし研究者自身にはEC2、IAM、S3を直接作成できる広い権限を付与しない。起動時に選べるEC2インスタンスタイプは小・中規模だけに限定し、CostCenterとDataClassは中央が定めた候補から選ばせてタグとして適用する。製品バージョンと利用可能な対象者は中央管理し、Organizations内のアカウントへ再利用可能な形で配布する。

最も適切な構成はどれか。

選択肢

A 研究者へcloudformation:*、ec2:*、iam:PassRoleを付与し、テンプレートURLを共有する。パラメータ制限とタグ規則は利用手順書だけで強制する

B Service Catalogに製品を登録し、portfolioへ関連付けるが、launch constraintは設定しない。研究者自身のIAM権限でCloudFormationを実行させ、instance type制限はCloudWatch alarmで事後検出する

C CloudFormation StackSetsで全アカウントへ同じ分析環境を一律作成する。研究者ごとの起動・更新・終了や選択可能パラメータはStackSet operation preferencesだけで制御する

D AWS Service CatalogでCloudFormation製品とバージョンをportfolioへ登録し、最小権限のlaunch roleをlaunch constraintとして設定する。template constraintで許可パラメータを絞り、TagOptionsで承認済みタグ値を提示し、portfolioをOrganizations内の対象アカウントへ共有して利用者アクセスを関連付ける

ここでいったん止める | 解答と解説は次ページ

問題 048 正解・解説 本番より難しい

問題 48の正解・解説

1. 正解

D

2. 問題文の重要な条件

- 承認済みCloudFormation製品を利用者が自分でライフサイクル管理する。
- 利用者へ基盤サービスの広い作成権限を与えない。
- 起動パラメータ値を事前制約する。
- 中央定義のタグ分類を選択・適用させる。
- 製品バージョン、portfolio、対象者を中央管理し、複数アカウントへ共有する。

3. 正解へ至る判断過程

一律配布ではなく、統制されたセルフサービスが主目的なのでService Catalogを選ぶ。製品をportfolioに入れ、launch constraintのIAM roleをService Catalogが引き受けて資源を作る。利用者は製品操作権限を持てばよく、EC2等の作成権限を直接持つ必要がない。

次に、template constraintでCloudFormationパラメータの許容範囲を狭める。TagOptionsを製品またはportfolioへ関連付け、起動時に中央承認済みのタグ値を選べるようにする。portfolio共有で複数アカウントへ製品と統制を配布する。

4. 正解が要件を満たす理由

Dは製品バージョンを中央で公開しつつ、研究者にprovisioned productの起動・更新・終了を委ねられる。launch roleが実資源を作るため、研究者へ基盤サービスの広い権限を付けずに済む。template constraintは許容instance typeなどを起動前に制限し、TagOptionsはタグ分類の候補を管理する。portfolio単位の共有とprincipal関連付けにより、対象アカウント・利用者を統制できる。

5. 各不正解選択肢が不適切な理由

A: 利用者権限が過大で、手順書はAPI上の強制にならない。任意テンプレートやIAM roleのPassRoleによる権限昇格にも注意が必要になる。
B: launch constraintがなければ、利用者は製品テンプレートが作る各AWS資源への権限を自分で持つ必要があり、最小権限要件を満たしにくい。CloudWatch alarmは不許可パラメータの事前制約ではない。
C: StackSetsは中央から複数アカウント・リージョンへ一律構成を展開する用途であり、利用者ごとのオンデマンド製品カタログとパラメータ選択を提供しない。
D: 正解肢のため対象外。

6. 各不正解選択肢が正解になり得る条件

A: 専用のCI/CD service roleだけが審査済みテンプレートを展開し、利用者に直接権限を与えず、パイプライン側でパラメータとタグを検証する場合はCloudFormation直接展開でも統制できる。
B: 製品が利用者の既存権限だけで安全に作成でき、launch roleを使わないことが明示要件ならService Catalogを権限なしカタログとして利用する場合がある。
C: セキュリティエージェントや監査設定のように、利用者の選択なしで全アカウントへ必ず同じベースラインを置く場合はStackSetsが適する。

7. 今後使える判断基準

中央強制の一律展開はStackSets、利用者が承認済み製品を選ぶ統制セルフサービスはService Catalogで考える。Service Catalogでは、誰に見せるかはportfolio、何を作るかはproduct/version、何の権限で作るかはlaunch constraint、何を選べるかはtemplate constraint、タグ候補はTagOptionsへ分解する。

8. 関連サービスとの比較

launch constraintは実行IAM role、template constraintはパラメータ規則であり、互いの代替ではない。TagOptionsはタグ分類候補を製品・portfolioへ関連付ける。AWS Organizations共有は配布範囲を広げるが、各利用者へのService Catalogアクセス許可やlaunch roleの設計まで自動的に不要にするものではない。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4

問題 049 | Domain 5 / ネットワーク | 本番相当 | 四択（1つ選択）

問題 49 固定IPが必要なTCP/UDPサービス

ゲーム会社は、東京とシドニーのNetwork Load Balancer（NLB）でTCPとUDPのリアルタイムサービスをactive-active運用している。世界各地の企業ネットワークから接続されるため、顧客のファイアウォールへ登録できる少数の固定Anycast IPが必要である。障害時は正常なリージョンへ短時間で振り替え、可能な限りAWSグローバルネットワークを利用してジッターを減らしたい。HTTPキャッシュは不要である。

最適なサービスはどれか。

選択肢

A	Amazon CloudFrontでNLBをカスタムオリジンにし、TTLを0にする。
B	Route 53 Weightedレコードを作成し、各リージョン/AZのNLB静的IP（必要ならインターネット向けNLBへ割り当てたElastic IP）を顧客へ許可リスト登録する。
C	AWS Global Acceleratorを作成し、両リージョンのNLBをエンドポイントとしてヘルスチェックとトラフィックダイヤルを設定する。
D	各NLBの前にApplication Load Balancerを置き、Elastic IPを関連付ける。

ここでいったん止める | 解答と解説は次ページ

問題 049 正解・解説 本番相当

問題 49の正解・解説

1. 正解

C

2. 問題文の重要な条件

TCPとUDP、固定Anycast IP、複数リージョン、速い障害切り替え、AWSバックボーン、キャッシュ不要である。

3. 正解へ至る判断過程

Global Acceleratorは静的Anycast IPを提供し、最寄りのAWSエッジからAWSネットワークへ取り込み、正常なリージョナルエンドポイントへTCP/UDPを転送する。エンドポイントのヘルスとトラフィックダイヤルにより段階配分や障害切り替えもできる。

4. 正解が要件を満たす理由

顧客は少数の固定IPだけを許可すればよく、DNS TTLに依存せずエンドポイントを切り替えられる。HTTP以外のTCP/UDPに対応し、インターネットを長距離横断する区間を減らせる。

5. 各不正解選択肢が不適切な理由

A: CloudFrontは主にHTTP/HTTPSコンテンツ配信で、任意のUDPサービスを中継しない。
B: NLBは有効化したAZごとに静的IPを持てるが、顧客はリージョン/AZごとの複数IPを管理する必要がある。これは少数のグローバルAnycast IPという要件を満たさず、DNS切り替えもキャッシュとTTLに依存し、最寄りエッジからAWSグローバルネットワークへ取り込む経路最適化も提供しない。
C: 正解肢のため対象外。
D: ALBはElastic IPを直接関連付けられず、UDPも扱わない。

6. 各不正解選択肢が正解になり得る条件

AはHTTP/HTTPSのキャッシュ、エッジ処理、WAF連携が中心なら適する。Bはリージョン/AZごとの静的IP数を許容でき、DNSベースの比率分散とTTL依存の切り替えで十分なら選択になり得る。Dではなく NLBを直接使う構成は、単一リージョンで静的IPとTCP/UDPが必要な場合に適する。

7. 今後使える判断基準

動的Webコンテンツのエッジキャッシュは CloudFront、固定Anycast IP + TCP/UDP + 高速なリージョン切り替えは Global Acceleratorと判断する。

8. 関連サービスとの比較

Route 53はDNSポリシーで宛先名を返す。NLBはAZごとの静的IPを提供し、インターネット向けならAZごとにElastic IPを割り当てられる。Global Acceleratorは少数のグローバル静的Anycast IPとネットワーク層の固定入口を提供する。CloudFrontはHTTP層でキャッシュ・オリジン保護・エッジ機能を提供する。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4

問題 050 | Domain 4 / セキュリティ | 本番相当 | 四択（1つ選択）

問題 50 多数のセキュリティFindingを一か所で正規化する

Organizations配下でGuardDuty、Inspector、Macie、Configを有効にしている。SOCは各サービスのコンソールを巡回せず、セキュリティ標準への準拠状況とFindingを一つの管理アカウントへ集約し、重要度やワークフローステータスを統一形式で扱いたい。集約したFindingをEventBridgeへ送り、チケット作成も自動化する。脅威検出エンジンそのものを一つへ置き換える意図はない。

中核にすべきサービスはどれか。

選択肢

A	AWS Security Hubを委任管理者で構成し、リージョン集約と統合サービスを有効にする。
B	GuardDutyだけを有効にし、MacieとInspectorのFindingをGuardDutyへ直接インポートする。
C	CloudTrail Lakeに全FindingのJSONを手動アップロードする。
D	Trusted AdvisorのSecurity checksだけを組織ビューで確認する。

ここでいったん止める | 解答と解説は次ページ

問題 050 正解・解説 本番相当

問題 50の正解・解説

1. 正解

A

2. 問題文の重要な条件

複数の検出サービス、統一形式、組織集約、セキュリティ標準、ワークフロー状態、EventBridge連携が必要である。

3. 正解へ至る判断過程

Security HubはASFF形式でAWSおよび対応製品のFindingを受け取り、標準コントロールの結果も統合する。Organizationsの委任管理者とcross-Region aggregationを使い、SOCの集約点にできる。

4. 正解が要件を満たす理由

検出元サービスを残したまま、Findingの正規化・優先順位付け・ワークフロー管理・EventBridge配信を一元化できる。

5. 各不正解選択肢が不適切な理由

A: 正解肢のため対象外。
B: GuardDutyは脅威検出サービスで、任意のInspector/Macie Findingを統一管理するハブではない。
C: CloudTrail LakeはAWSアクティビティやイベントの分析基盤であり、Security Hubの標準・ワークフローをそのまま提供しない。
D: Trusted Advisorは推奨チェックを提供するが、各検出サービスのFinding正規化・集約を担わない。

6. 各不正解選択肢が正解になり得る条件

BはAWSアカウントやワークロードの不審活動検出が単独要件なら中核になる。CはAPI操作や特定イベントの長期SQL分析、Dはコスト・性能・サービス制限を含むベストプラクティス確認に適する。

7. 今後使える判断基準

Findingを「作る」サービス（GuardDuty/Inspector/Macie/Config）と、「集めて標準化する」Security Hubを分けて考える。

8. 関連サービスとの比較

EventBridgeはFinding発生後のルーティング、Security Hubは集約と状態管理、Systems Manager Automation/Lambdaは是正処理を担う。ハブだけでは自動修復は完結しない。

公式確認先 AWS公式 1 / AWS公式 2

問題 051 | Domain 1 / 監視・性能 | 複合難問 | 四択（1つ選択）

問題 51 EFSとFSx for Lustreの性能設計

あるメディア企業には、同じVPC内で動作する性質の異なる2つのLinuxワークロードがあります。

ワークロード1：Web配信基盤
3つのアベイラビリティーゾーンにまたがるEC2 Auto Scalingグループが、共有のPOSIXファイルシステムへ画像、設定、ユーザー生成コンテンツを保存します。多数の小さなファイルとメタデータ操作があり、1回の操作レイテンシーを重視します。保存量は3 TiBで、平常時のスループットは20 MiB/sですが、予告しにくいキャンペーン時には数時間だけ600 MiB/sへ上昇します。現在のEFSはBursting throughputを使用しており、繁忙時にBurstCreditBalanceがほぼ0になっています。AZ障害が起きても、残るAZのWebサーバーから同じデータを利用できることが必要です。

ワークロード2：夜間映像解析
毎晩、150台のEC2インスタンスがS3にある60 TiBの映像を、共有POSIX名前空間から高い並列スループットで数時間処理します。作業用ファイルはジョブ終了後に不要で、ファイルサーバー障害時にはS3の原本からジョブを再実行できます。結果だけをS3へ永続化します。ジョブ実行時以外の固定費を抑えたいと考えています。

プロトコル変更を最小限にし、可用性、レイテンシー、並列性能、費用をすべて満たす最も適切な構成はどれですか。

選択肢

A Web配信基盤には、各AZにマウントターゲットを持つRegional EFSをGeneral Purpose performance modeとElastic throughputで使用する。夜間解析にはS3データリポジトリとリンクしたFSx for Lustre Scratchファイルシステムをジョブごとに使用し、結果をS3へエクスポートして削除する。

B 2つのワークロードを1つのRegional EFSへ統合し、Max I/O performance modeと、両者のピーク合計を満たすProvisioned throughputを常時設定する。Max I/OはGeneral Purposeより全操作のレイテンシーが低く、Elastic throughputと同時利用できる。

C Web配信基盤をOne Zone EFSのGeneral Purpose performance modeとElastic throughputへ移し、3AZのEC2から同じマウントターゲットへ接続する。夜間解析にはFSx for Lustre Persistentを常時稼働させ、毎晩S3から全データをコピーする。

D Web配信と夜間解析の両方を、S3にリンクした1つのFSx for Lustre Scratchファイルシステムへ移行する。Scratchはデータを複製するためRegional EFSと同等のAZ耐障害性があり、Webの小規模メタデータ処理にも常に最低レイテンシーを提供する。

ここでいったん止める | 解答と解説は次ページ

問題 051 正解・解説 複合難問

問題 51の正解・解説

1. 正解

A

2. 問題文の重要な条件

- Webは3AZから同じ永続データを利用し、AZ障害後も継続する必要がある。
- Webは小さなファイルとメタデータ操作が多く、低い1操作レイテンシーを重視する。
- Webの平均対ピーク比は小さく、ピーク時刻と必要スループットを予測しにくい。
- 現行EFSのBursting throughputはクレジット枯渇が実測されている。
- 夜間解析はS3原本から再作成できる一時データで、非常に高い並列ファイルI/Oが必要である。
- 夜間解析の結果はS3に残し、ジョブ外の固定費を抑えたい。

3. 正解へ至る判断過程

2つのワークロードを同じ「共有POSIX」とだけ見ず、耐久性とI/O特性で分けます。Web配信基盤には、複数AZにデータを保存するRegional EFSと、各利用AZのマウントターゲットが適します。General Purpose performance modeは低い1操作レイテンシーを提供し、現在は多くのEFS用途で推奨されます。スループットは予測困難で平均がピークの約3%なので、自動的に上下するElastic throughputが適します。

映像解析は、S3データを多数ノードから高並列に処理する典型的なFSx for Lustre用途です。作業領域の損失を許容し、再実行できるため、複製を持つPersistentではなく費用対効果の高いScratchを選べます。S3とのデータリポジトリ関連付けによりオブジェクトをファイルとして処理し、必要な結果をS3へ書き戻してからファイルシステムを削除できます。

4. 正解が要件を満たす理由

AのRegional EFSは複数AZにデータを冗長保存し、各AZのローカルマウントターゲットを使うことでAZ間転送料と余分なレイテンシーを避けます。Elastic throughputはクレジット残高やファイルシステム容量に依存してピークが制限されるBurstingの問題を解消し、負荷に応じた利用量ベースの特性を持ちます。

FSx for Lustre Scratchは処理負荷の高い短期ワークロード向けで、高い集約スループットとS3統合を提供します。Scratchは非複製というリスクがありますが、問題文では原本がS3にあり再実行可能です。ワークロードごとに耐久性へ支払う場所を分けるため、すべてを高価な永続・プロビジョンド性能へ寄せるより要件と費用が一致します。

5. 各不正解選択肢が不適切な理由

- **B:** Max I/Oは高い並列性と引換えにGeneral Purposeより高い1操作レイテンシーを持つ従来世代のモードで、小ファイルWeb処理には不利です。Max I/OはElastic throughputと組み合わせられません。また、夜間のピーク合計へProvisioned throughputを常時設定すると、平均利用が低いWebと夜間だけの解析に固定費が過大です。
- **C:** One Zone EFSは単一AZにデータを保存し、マウントターゲットも1つです。別AZからアクセスはできますが、AZ障害後も同じデータを利用する要件を満たさず、AZ間転送費と追加レイテンシーも生じます。Persistent Lustreは作業データの複製・ファイルサーバー置換が必要な場合に有用ですが、再作成可能な夜間ジョブへ常時稼働させると費用要件に劣ります。
- **D:** FSx for Lustre Scratchはデータを複製せず、ファイルサーバーやディスク障害で一部データを失う可能性があります。Regional EFSと同等の複数AZ耐久性はありません。一時HPC用の単一AZファイルシステムへWebの永続コンテンツを統合するのは、可用性と耐久性の要件に反します。

6. 各不正解選択肢が正解になり得る条件

- **Bが適切になる条件:** 既存のMax I/Oファイルシステムで極めて高い並列処理が必要で、多少高いメタデータレイテンシーを許容し、必要スループットが常時予測可能な場合にはProvisioned throughputが候補になります。ただし新規設計ではGeneral Purposeの最新性能と制約を先に評価します。
- **Cが適切になる条件:** Webデータを別リージョンやバックアップから復元でき、単一AZ障害による停止を許容してストレージ費用を優先する場合はOne Zone EFSが候補です。解析結果や途中状態を失えず、長期にLustreを使う場合はPersistentが適します。
- **Dが適切になる条件:** 対象がすべて再作成可能な一時的HPCデータで、単一AZ・ジョブ単位の利用だけであり、永続Webコンテンツを置かない場合です。Scratchの障害時再実行を運用として受け入れます。

7. 今後使える判断基準

共有ファイルストレージは、**プロトコル、AZ耐障害性、1操作レイテンシー、集約スループット、データの再作成可否**で選びます。EFS内では、低レイテンシーのGeneral Purposeを基本とし、予測困難なスパイクにはElastic、容量比例の安定した利用にはBursting、容量に対して高い一定性能が必要ならProvisionedを検討します。S3データを多数ノードで一時的に処理するHPCではFSx for Lustre、損失許容ならScratch、長期保持・複製が必要ならPersistentです。

8. 関連サービスとの比較

- **Regional EFS:** 複数AZにまたがるマネージドNFSで、可変台数のLinuxコンピュートから永続共有データを利用する用途に適します。
- **One Zone EFS:** 単一AZ保存で費用を抑えますが、AZ障害耐性が必要なデータには向きません。
- **FSx for Lustre Scratch:** 非複製の短期・処理集約型ストレージです。S3に原本があるHPCやML処理に適します。
- **FSx for Lustre Persistent:** データを複製し、障害ファイルサーバーを置換する長期ワークロード向けです。
- **AWS DataSync:** NFSやオブジェクトストレージ間の移行・定期転送には有効ですが、実行中HPCへLustre性能を提供するサービスではありません。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4 / AWS公式 5

問題 052 | Domain 2 / 信頼性・BC | 本番より難しい | 四択（1つ選択）

問題 52 RDS PostgreSQLの互換性を保ったまま3AZ化する

分析ダッシュボードと業務更新を同じAmazon RDS for PostgreSQLで処理している。アプリケーションはRDS PostgreSQL固有の検証済み拡張に依存しており、今期中のAuroraへの移行は承認されていない。現在のMulti-AZ DBインスタンス配置はAZ障害に自動フェイルオーバーできるが、スタンバイが読み取りに使えず、月末はライターのCPUが読み取りクエリで逼迫する。

要件は、同一リージョンの3つのAZにまたがり、ライター障害時はRDSが自動昇格し、平常時には2台を読み取りに利用できることである。アプリケーションでリードレプリカ昇格手順を実装したくない。最も適切な構成はどれか。

選択肢

A	現在のMulti-AZ DBインスタンス配置を維持し、スタンバイのエンドポイントへ分析クエリを送る
B	Single-AZのプライマリと、異なる2AZの通常リードレプリカを作成し、障害時は最も遅延の小さいレプリカをLambdaで昇格する
C	RDS for PostgreSQLのMulti-AZ DBクラスターへ移行し、クラスターのリーダーエンドポイントへ分析読み取りを送り、ライター障害時の自動フェイルオーバーを利用する
D	Aurora PostgreSQLクラスターへ移行し、互換性試験を省略して既存拡張をそのまま導入する

ここでいったん止める | 解答と解説は次ページ

問題 052 正解・解説 本番より難しい

問題 52の正解・解説

1. 正解

C

2. 問題文の重要な条件

- Aurora移行は禁止され、RDS PostgreSQL互換性を維持する。
- 3AZ、2台の平常時読み取り、RDS管理の自動フェイルオーバーが必要。
- アプリケーションによる昇格自動化は避ける。

3. 正解へ至る判断過程

従来のMulti-AZ DBインスタンスはスタンバイを読み取りに使えない。一方、RDS Multi-AZ DBクラスターは、3AZにライター1台と読み取り可能な2台を配置し、そのリーダーが自動フェイルオーバー先にもなる。エンジンをRDS PostgreSQLのまま維持できる点も重要である。

4. 正解が要件を満たす理由

Multi-AZ DBクラスターは半同期の高可用性配置で、2台の読み取り可能なDBインスタンスを持つ。読み取りクエリをリーダーエンドポイントへ分散しながら、ライター障害時は最新の変更レコードを持つリーダーをRDSが選んで昇格する。通常リードレプリカの手動昇格ロジックをアプリケーションに持たせる必要がない。

5. 各不正解選択肢が不適切な理由

- A：Multi-AZ DBインスタンスのスタンバイはユーザー接続を受け付けず、読み取りスケールに使えない。
- B：読み取り性能は得られるが、レプリケーションは非同期で、昇格と接続切替を自作する必要がある。クラスター管理の自動フェイルオーバー要件に劣る。
- D：Aurora移行が承認されておらず、拡張の互換性試験省略は移行制約を無視する。

6. 各不正解選択肢が正解になり得る条件

- A：読み取り負荷がなく、1台の非読取スタンバイによる高可用性だけで十分な場合。
- B：リージョンをまたぐDRや、クラスターが対応しないエンジン/バージョンで読み取りを増やし、手動昇格を許容する場合。
- D：Aurora互換性を十分に検証し、Auroraのストレージ/フェイルオーバー特性を必要とする場合。

7. 今後使える判断基準

「スタンバイを読めるか」をMulti-AZの種類ごとに確認する。RDS Multi-AZ DBインスタンスの1台のスタンバイは読めず、Multi-AZ DBクラスターの2台は読める。通常リードレプリカは読み取りに使えるが、同じ自動HA単位ではない。

8. 関連サービスとの比較

Auroraも複数AZのリーダーと自動フェイルオーバーを提供するが、エンジン互換性・移行検証は別問題である。RDS ProxyをMulti-AZ DBクラスターと組み合わせると接続プールとフェイルオーバー時の接続影響をさらに抑えられるが、読み取り容量そのものを作るのはDBクラスターである。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3

問題 053 | Domain 3 / 展開・自動化 | 複合難問 | 四択（1つ選択）

問題 53 組織ベースラインからネストを外す

ある企業はCDKで作成した運用ベースラインを、AWS OrganizationsのWorkloads OUにある120アカウント・3リージョンへ配布し、OUへ追加される新規アカウントにも自動展開したい。現在のCDKアプリケーションは、親スタックから複数のネストされたCloudFormationスタックを作成し、カスタムTransformも使用している。Lambdaコードassetも含む。組織の管理アカウントではtrusted accessが有効で、専用アカウントがStackSets委任管理者である。

試行時、service-managed permissionsのStackSetはテンプレート機能の制約で作成できなかった。チームはOU自動展開を維持し、CIで生成物を固定・審査し、失敗許容数と同時実行数を抑えた段階展開を行いたい。メンバーアカウントにself-managed用IAMロールを手作業で配布することは避ける。

最も適切な再設計はどれか。

選択肢

A CDK構成を、service-managed StackSetsでサポートされるフラットなCloudFormationテンプレートへ分割または再構成し、カスタムTransformとネストされたスタックへの依存を除く。CIでsynthし、assetを対象リージョンから参照可能な不変成果物として発行した後、OUを対象とするservice-managed StackSetをautomatic deploymentと保守的なoperation preferencesで更新する

B 現在の親テンプレートをそのままservice-managed StackSetへ渡し、CAPABILITY_AUTO_EXPANDを指定する。StackSetsではこの指定によりネストされたスタック、任意マクロ、ローカルCDK assetが自動的に展開される

C self-managed permissionsへ変更すればOU所属変更を自動追跡でき、管理・実行ロールもCloudFormationが全アカウントへ自動作成するため、現在のテンプレートを無変更で利用できる

D Service CatalogでportfolioをOUへ共有する。portfolioを共有した時点で各アカウントに製品が自動プロビジョニングされ、StackSetsと同じautomatic deploymentおよび失敗許容制御が得られる

ここでいったん止める | 解答と解説は次ページ

問題 053 正解・解説 複合難問

問題 53の正解・解説

1. 正解

A

2. 問題文の重要な条件

- OUへの現在・将来のアカウント自動展開を維持する。
- 手作業のself-managed実行ロールを避けるためservice-managed permissionsが必要である。
- 現行テンプレートのネストされたスタック、マクロ/Transformがservice-managed StackSetsの制約に抵触している。
- CDKのLambda assetは、対象環境から取得可能な場所へ事前発行する必要がある。
- CI審査とStackSet operation preferencesによる段階展開が必要である。

3. 正解へ至る判断過程

まずOU自動追随とロール自動管理という譲れない条件からservice-managed permissionsを残す。すると、非対応のテンプレート機能を回避する側へ設計を変える必要がある。ネスト構造をフラット化するか、独立したサポート対象テンプレートへ分割し、TransformをCI側で処理済みの静的テンプレートへ置き換える。

次に、CDK assetはテンプレート内のローカルパスではないため、CIでハッシュ化された成果物をS3等へ発行し、各対象リージョンから取得可能な参照をテンプレートへ持たせる。最後にStackSetのfailure tolerance、max concurrency、リージョン順序などを保守的に設定して展開する。

4. 正解が要件を満たす理由

Aはservice-managed StackSetsの制約にテンプレートを合わせるため、OUターゲットとautomatic deploymentを維持できる。CIでsynth、静的解析、承認、asset発行を済ませれば、展開時に開発者端末や未処理マクロへ依存しない。operation preferencesで一度に影響するアカウント数と失敗許容を抑え、組織全体への変更リスクを管理できる。

5. 各不正解選択肢が不適切な理由

A: 正解肢のため対象外。
B: service-managed StackSetsの非対応機能はCapabilities指定だけでは解消しない。CloudFormationはローカルassetを自動取得できない。
C: self-managed permissionsでは利用者が管理アカウントとターゲットアカウントのIAMロールを用意・維持する。service-managedのようなOrganizations OU automatic deploymentを同じ形では提供しない。
D: portfolio共有は製品を利用可能にする配布であり、共有しただけで製品を全アカウントへ自動起動しない。StackSet operation preferencesの代替にもならない。

6. 各不正解選択肢が正解になり得る条件

B: 通常の単一アカウントCloudFormationスタックで、使用するTransformがサポートされ、必要なCapabilitiesを明示承認し、asset参照も解決済みならマクロ展開を利用できる。
C: Organizations外の明示アカウントへ展開し、ターゲットロールを中央で事前配布・管理でき、OU自動追随が不要ならself-managed permissionsが候補になる。
D: 利用者が承認済み製品を必要なときに選んで起動するセルフサービスが目的ならService Catalog portfolio共有が適する。

7. 今後使える判断基準

機能制約に遭遇したら、権限モデルを変えて必須要件を失う前に、テンプレートをサポート範囲へ変換できるかを検討する。StackSetsでは、OU自動展開、ロール管理、テンプレート機能、asset配置、同時実行・失敗許容を別々に確認する。CDKが生成することと、StackSetsがその生成物を受理・取得できることは同義ではない。

8. 関連サービスとの比較

CDKはテンプレートとasset manifestを生成する開発レイヤー、CloudFormationは1スタックの状態管理、StackSetsは複数アカウント・リージョンへの反復展開である。Service Catalogは承認済み製品のセルフサービス、RAMは既存共有資源の共同利用を担い、どちらも組織ベースラインの自動プロビジョニングをそのまま置き換えない。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4 / AWS公式 5

問題 054 | Domain 5 / ネットワーク | 本番より難しい | 四択（1つ選択）

問題 54 重複CIDRの顧客へ一つのサービスだけ公開する

企業はサービス提供VPCのTCP 8443 APIを、複数の顧客AWSアカウントから非公開に利用させたい。顧客VPCのCIDRは互いに重複しており、将来さらに増える。顧客からAPIへの接続だけを許可し、VPC間の一般的な相互到達性や推移的ルーティングは与えたくない。顧客は標準の社内DNS名を使い、インターネットゲートウェイやNATを経由しない。提供側は許可したAWSプリンシパルだけが接続を作成できるようにしたい。

最も拡張性が高く、要件に合う構成はどれか。

選択肢

A	APIをNetwork Load Balancerの背後に置いてVPC endpoint serviceとして公開し、顧客はinterface VPC endpointを作成する。Allowed principals、acceptance設定、検証済みprivate DNS nameを構成する。
B	すべての顧客VPCと提供VPCをVPC peeringし、重複CIDRごとにNATゲートウェイで変換する。
C	顧客VPCを一つのTransit Gatewayへ接続し、全顧客ルートを相互伝播させる。
D	APIをインターネット向けApplication Load Balancerで公開し、顧客のNAT Gateway Elastic IPだけをセキュリティグループで許可する。

ここでいったん止める | 解答と解説は次ページ

問題 054 正解・解説 本番より難しい

問題 54の正解・解説

1. 正解

A

2. 問題文の重要な条件

顧客CIDRが重複し、サービス単位の一方向アクセスだけを許可し、フルメッシュ到達性を避け、インターネットを使わず、接続作成主体を制限したい。

3. 正解へ至る判断過程

AWS PrivateLinkのendpoint serviceは、提供側NLBへ顧客のinterface endpointから私的に接続させる。VPCのCIDR全体をルーティングしないため、顧客同士や提供VPCとのCIDR重複を接続モデルへ持ち込まず、サービス単位の公開にできる。

4. 正解が要件を満たす理由

Allowed principalsでendpoint作成可能なアカウント・ロールを制限し、必要なら接続要求を承認できる。Private DNS nameを検証して関連付ければ、顧客は提供側が指定した名前をinterface endpointのプライベートIPへ解決できる。

5. 各不正解選択肢が不適切な理由

A: 正解肢のため対象外。
B: VPC peeringは重複CIDR間で利用できず、顧客数に応じて接続とルートが増える。NAT Gatewayを一般的なpeeringの重複解消装置として挟む設計でもない。
C: Transit Gatewayは広いネットワーク到達性に向くが、重複CIDRのルーティングと顧客間の分離が難しく、本問の「一つのサービスだけ」に対して過大である。
D: 技術的には公開APIをIP制限できるが、インターネット非経由の要件に反し、顧客ごとのEIP管理も増える。

6. 各不正解選択肢が正解になり得る条件

Bは少数の非重複CIDR VPC間で双方向の広い到達性が必要なら低コストで有力になる。Cは多数VPCを集中接続し、ルートテーブルでネットワーク間の到達性を管理する場合に適する。Dは公開サービスで、固定送信元IPの許可リストとインターネット経由を受容できる場合に選べる。

7. 今後使える判断基準

多数のconsumer VPCへ「ネットワークではなく特定サービスだけ」を公開し、CIDR重複や一方向性が条件に出たらPrivateLinkを第一候補にする。

8. 関連サービスとの比較

VPC peeringは2 VPC間の直接ルーティング、Transit Gatewayは多数ネットワークのハブ、PrivateLinkはNLB/GWLB等を介したservice-orientedな私的公開である。AWS RAMは対応リソースを共有するが、任意APIの通信経路そのものを提供しない。

公式確認先 AWS公式 1 / AWS公式 2

問題 055 | Domain 4 / セキュリティ | 本番相当 | 四択（1つ選択）

問題 55 S3内の個人情報を発見して優先順位を付ける

データレイクには数千のS3バケットがあり、どのバケットに氏名、住所、クレジットカード番号、認証情報が含まれるか把握できていない。組織のセキュリティアカウントからメンバーアカウントを管理し、まずS3の公開・暗号化・共有状態を可視化したうえで、選択したバケットをサンプリングまたは定期ジョブで内容分類したい。EC2の脆弱性やAPIの不審挙動ではない。

最適なサービスはどれか。

選択肢

A	Amazon Inspector
B	Amazon GuardDuty Malware Protection
C	IAM Access Analyzerのpolicy generation
D	Amazon Macieを委任管理者として有効にし、S3 inventoryとsensitive data discovery jobsを構成する。

ここでいったん止める | 解答と解説は次ページ

問題 055 正解・解説 本番相当

問題 55の正解・解説

1. 正解

D

2. 問題文の重要な条件

対象はS3、バケットのセキュリティ状態とオブジェクト内容の機密データ分類、マルチアカウント、定期・選択的ジョブである。

3. 正解へ至る判断過程

MacieはS3バケットのinventoryとセキュリティ評価を提供し、managed/custom data identifiersを使ってオブジェクト内の機密データを発見する。Organizationsの委任管理者でメンバーを集中管理できる。

4. 正解が要件を満たす理由

公開状態などから優先順位を付け、対象を絞ったclassification jobで費用を制御しながら個人情報・認証情報等をFinding化できる。

5. 各不正解選択肢が不適切な理由

A: InspectorはEC2/ECR/Lambda等の脆弱性管理で、S3オブジェクト内容を分類しない。
B: GuardDuty Malware Protectionは悪性ファイル検出の文脈で、PII分類とバケットinventoryの代替ではない。
C: Access Analyzer policy generationはCloudTrail活動から最小権限policyを作る補助で、S3内容を読む分類器ではない。
D: 正解肢のため対象外。

6. 各不正解選択肢が正解になり得る条件

AはCVE優先順位付け、Bはアップロード等に含まれるマルウェア検出、Cは実利用に基づくIAM policyの縮小で正解になり得る。

7. 今後使える判断基準

S3の中身が機密かはMacie、不審な利用はGuardDuty、外部へ許可されているかはAccess Analyzer、ソフトウェア脆弱性はInspector。

8. 関連サービスとの比較

S3 Inventoryはオブジェクトメタデータ一覧で内容分類をしない。Macie inventoryはバケット姿勢の可視化、discovery jobはオブジェクト内容の検査という二段階で考える。

公式確認先 AWS公式 1 / AWS公式 2

問題 056 | Domain 1 / 監視・性能 | 本番相当 | 四択（1つ選択）

問題 56 RDS遅延の二つの層

ある会社は、実行計画分析に対応するバージョンのAmazon Aurora PostgreSQL DBインスタンスを約50台運用している。数日に一度、アプリケーションの応答時間が10分ほど悪化するが、1分間隔の CPUUtilization の平均値は40%未満である。DBAは、遅延時に「どのSQLがDB負荷を生み、どの待機イベントやロックが支配的だったか」を複数DBにまたがって調査し、SQL実行計画も確認したい。運用チームは同時に、OSのメモリ、ファイルシステム、プロセス別CPUを最短1秒粒度で確認したい。DBホストへエージェントを手動導入することはできない。2026年8月以降も同じ監視画面と保持方針を継続でき、調査のための自作ETLを最小化する必要がある。

最も適切な構成はどれか。

選択肢

A すべてのDBで従来のPerformance Insightsを7日保持で有効化し、CloudWatchの基本RDSメトリクスを1分粒度で併用する。OSプロセスはRDSイベントサブスクリプションから推定する

B CloudWatch Database InsightsのAdvanced modeを対象DBで有効化し、DB負荷、Top SQL、待機、ロックおよび実行計画を分析する。加えてRDS Enhanced Monitoringを1秒粒度で有効化し、OSレベルの情報をCloudWatch Logsへ配信する

C RDS Enhanced Monitoringだけを1秒粒度で有効化し、RDSOSMetricsロググループをCloudWatch Logs Insightsで検索してSQL、待機イベント、ロックツリーまで復元する

D Database InsightsのStandard modeを使用し、各DBホストにCloudWatch agentをインストールしてOSプロセスとメモリを収集する

ここでいったん止める | 解答と解説は次ページ

問題 056 正解・解説 本番相当

問題 56の正解・解説

1. 正解

B

2. 問題文の重要な条件

- 平均CPUでは説明できないDB遅延であり、SQL、待機イベント、ロック、実行計画まで必要である。
- 約50台を横断して調べるため、DB単体のメトリクス表示だけでは運用負荷が高い。
- OSプロセス、メモリ、ファイルシステムを最短1秒粒度で確認したい。
- RDSの基盤ホストには利用者がエージェントを導入できない。
- 2026年7月31日に従来のPerformance Insightsコンソール体験が終了することを踏まえ、8月以降も継続可能でなければならない。

3. 正解へ至る判断過程

まず、DB負荷の内訳とOS資源の内訳は別の観測層であると整理する。Database InsightsはDB Loadを中心にSQL・待機を関連付け、Advanced modeではフリート表示や対応エンジンのロック分析・実行計画分析を提供する。一方、Enhanced MonitoringはRDSが基盤OSからCPU、メモリ、プロセス、ファイルシステムなどを取得し、最短1秒粒度でCloudWatch Logsへ送る。二つを併用することで、DBセッションの待機とOS資源枯渇を同じ時間軸で検証できる。

4. 正解が要件を満たす理由

Database Insights Advanced modeは、標準のRDSメトリクスだけでは分からないDB Load、Top SQL、待機の寄与を可視化し、フリート規模の監視と深い診断を両立する。対応するPostgreSQLではロックツリーや実行計画の分析にも進める。Enhanced Monitoringは利用者によるホストアクセスを必要とせず、RDSサービスがOSメトリクスを収集する。したがって、SQL層とOS層の両方を、独自の収集基盤を構築せずに満たす。

5. 各不正解選択肢が不適切な理由

A: Performance Insightsだけに新規運用を固定すると、2026年7月31日以降のコンソール移行を考慮できない。基本CloudWatchメトリクスにはプロセス別CPUやOSメモリがなく、RDSイベントからも推定できない。
B: 正解肢のため対象外。
C: Enhanced MonitoringはOSを観測する機能であり、SQL別DB負荷、DB待機イベント、ロックツリーを復元する機能ではない。

D: Standard modeはAdvanced modeのフリート表示や高度なロック・実行計画分析を満たさない。また、利用者はRDS基盤ホストへCloudWatch agentをインストールできない。

6. 各不正解選択肢が正解になり得る条件

A: 2026年7月以前の短期調査で、SQL別負荷だけが必要でOS詳細や長期継続が不要なら、既存Performance Insightsを利用する判断には妥当性がある。
C: SQLではなく、スワップ、OSプロセス、ディスクI/OなどのOS資源だけが調査対象なら適切である。
D: 高度なロック分析が不要でStandard modeの範囲で足り、対象が自己管理EC2上のDBであれば、CloudWatch agentによるOS収集を組み合わせられる。

7. 今後使える判断基準

RDSの遅延では、まず「DBセッションが何を待つか」と「OSが何を消費しているか」を分ける。前者はDatabase Insights、後者の詳細はEnhanced Monitoring、サービス全体のしきい値監視はCloudWatch標準メトリクスを中心に選ぶ。平均CPUが低いことは、ロック待ちやI/O待ちがない証拠にはならない。

8. 関連サービスとの比較

CloudWatch標準RDSメトリクスはアラームと長期傾向に向く。Enhanced MonitoringはOSの詳細をCloudWatch Logsへ送り、Database InsightsはDB LoadとSQL・待機の原因分析に向く。RDSイベントサブスクリプションはフェイルオーバーや設定変更などのライフサイクル通知であり、性能プロファイラではない。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4 / AWS公式 5

問題 057 | Domain 2 / 信頼性・BC | 複合難問 | 四択（1つ選択）

問題 57 計画切替は無損失、災害切替は秒単位RPO

SaaS企業は東京リージョンのAurora PostgreSQLクラスターを使用している。大阪リージョンには読み取りトラフィックも一部送って、DR費用を有効活用したい。リージョン障害時の目標はRTO 5分以内、RPO 10秒以内である。四半期ごとのDR訓練では両リージョンが正常な状態で計画的にプライマリを入れ替え、その際のデータ損失は0でなければならない。実障害時は、複製遅延相当のわずかなデータ損失を許容する。

また、切替後にアプリケーションのDB接続文字列を毎回編集する運用は避けたい。最も適切な構成はどれか。

選択肢

A 東京のクラスターで1日1回スナップショットを取得して大阪へコピーし、障害時に復元する。計画訓練でも同じ復元手順を使う

B 東京のAuroraクラスター内に別AZのAurora Replicaを追加し、大阪リージョンへの構成は作らない

C 大阪にDBインスタンスを持たないheadlessのAurora Global Databaseセカンダリだけを作り、障害を検知してからDBインスタンスを追加する

D DBインスタンスを含む大阪のセカンダリクラスターをAurora Global Databaseとして構成し、rds.global_db_rpo を10秒に設定してRPO遅延を監視する。アプリケーションはグローバルライターエンドポイントを使用し、DNSキャッシュTTLを5秒程度にする。計画訓練ではswitchover、実障害ではmanaged failoverを使い、訓練でRTOを実測する

ここでいったん止める | 解答と解説は次ページ

問題 057 正解・解説 複合難問

問題 57の正解・解説

1. 正解

D

2. 問題文の重要な条件

- クロスリージョンでRTO 5分、RPO 10秒。
- セカンダリで平常時の読み取りも行う。
- 計画切替はRPO 0、実障害は非同期遅延を許容。
- 接続文字列の手動変更を避ける。

3. 正解へ至る判断過程

Aurora Global Databaseは、プライマリから別リージョンのセカンダリへ非同期にストレージレベルで複製し、セカンダリを読み取りに使える。正常時の計画切替では同期を待つswitchover、障害時はデータ損失の可能性を受け入れるfailoverを使い分ける。厳密なRPO上限には rds.global_db_rpo とRPO遅延メトリクスを使い、接続切替はグローバルライターエンドポイントと短いDNSキャッシュTTLの両方で閉じる。

4. 正解が要件を満たす理由

rds.global_db_rpo=10 はユーザーDBのRPO遅延が上限を超えないよう追跡し、超過時にはプライマリのコミットを待機させ得るため、可用性・書き込み性能との交換条件も明示できる。switchoverはセカンダリを同期してから役割を交換するためRPO 0で、managed failoverは複製済みの最新地点へ昇格する。グローバルライターエンドポイントは昇格後のライターへ更新され、5秒程度のDNSキャッシュTTLと切替訓練によって5分RTOを運用上検証できる。セカンダリにDBインスタンスがあるため、平常時の読み取りにも使える。

5. 各不正解選択肢が不適切な理由

- A：日次スナップショットではRPOが最大24時間程度となり、復元にも5分を大きく超える可能性が高い。
- B：同一リージョン内のAZ障害には有効だが、東京リージョン全体の障害を大阪で復旧できない。
- C：ストレージは同期されても、headlessセカンダリには昇格対象のDBインスタンスがない。切替前に追加が必要で、平常時読み取りもできずRTO 5分を危険にする。

6. 各不正解選択肢が正解になり得る条件

- A：RTOが数時間、RPOが1日でよく、DR費用を最小化するバックアップ/リストア戦略。
- B：リージョン障害を対象とせず、AZ/インスタンス障害だけに備える場合。
- C：平常時のセカンダリ計算費用を最小化し、DBインスタンス追加を含む長いRTOを受容するパイロットライト寄りの構成。

7. 今後使える判断基準

Aurora Global Databaseでは、正常な計画変更はswitchover、予期しない停止はfailoverと区別する。前者は同期してRPO 0、後者は非同期複製遅延による非ゼロRPOを持ち得る。数値でRPO上限を要求されたら rds.global_db_rpo、RPO遅延監視、コミット待機の影響まで確認する。接続先の抽象化だけでRTOが確定するわけではなく、クライアント側DNSキャッシュと切替訓練も必要である。

8. 関連サービスとの比較

通常のRDSクロスリージョンリードレプリカもDRに使えるが、昇格は独立DB化と接続切替を伴い、Aurora Global Databaseほど統合されたリージョン切替ではない。DynamoDB global tablesは各リージョンで書き込み可能なmulti-activeで、単一ライターのAurora Global Databaseとは書き込みモデルが異なる。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3

問題 058 | Domain 3 / 展開・自動化 | 本番より難しい | 四択（1つ選択）

問題 58 中央AMIを「共有」ではなく各アカウントへ配る

ある企業は、セキュリティ専用アカウントでLinuxのゴールデンAMIを毎月作成し、検査に合格したイメージだけを20個のワークロードアカウントへ配布している。ワークロードは東京とシンガポールの2リージョンで稼働する。現在は担当者がAMIを手動コピーしているため、コピー漏れ、暗号化キーの選択誤り、起動テンプレートのAMI ID更新漏れが発生している。

新しい仕組みには次の要件がある。

- OS更新、エージェント導入、構成検査を再現可能なパイプラインにする。
- 配布先アカウントが、それぞれのリージョンにあるAMIコピーを所有する。中央アカウントのAMIを削除しても、既に配布したAMIから起動できなければならない。
- EBSスナップショットは暗号化し、配布先でも指定したカスタマーマネージドKMSキーを使用する。
- 昇格対象のビルドを配布したとき、配布先のEC2起動テンプレートに新しいAMIを参照するバージョンを作成できるようにする。
- 長期アクセスキーと、毎月の手動コピーをなくす。

最も適切な構成はどれか。

選択肢

A EC2 Image Builderでビルド・テストコンポーネントを含むイメージパイプラインを作成する。配布設定で対象アカウントとリージョンへのAMIコピー、および対象の起動テンプレートを指定する。各配布先にEC2ImageBuilderDistributionCrossAccountRoleと必要最小限の権限を用意し、送信元・配布先リージョンのKMSキーポリシーとロール権限を構成する

B Image Builderで中央アカウントにだけAMIを作成し、AWS OrganizationsのOUへ起動権限を付与する。中央KMSキーを全アカウントに共有し、各起動テンプレートは中央AMIのIDを固定して参照する

C Systems Manager Automationで各アカウントの実行時に中央AMIを手動選択し、暗号化されたAMIを暗号化解除してから各リージョンへコピーする。コピー先ではAWS管理のEBSキーを必ず使用する

D 最新AMIのIDを中央アカウントのParameter Storeに保存し、各EC2インスタンスのユーザーデータが起動時にその値を読み取って、自分自身のルートボリュームへ更新内容を適用する

ここでいったん止める | 解答と解説は次ページ

問題 058 正解・解説 本番より難しい

問題 58の正解・解説

1. 正解

A

2. 問題文の重要な条件

- 配布先アカウント自身がAMIコピーを所有する必要があり、中央AMIへの依存を残せない。
- 2リージョン、20アカウントへ継続的に配布するため、手動コピーでは運用負荷と不整合が大きい。
- 暗号化AMIのクロスアカウント配布では、AMIの権限だけでなくKMSと配布用IAMロールも成立させる必要がある。
- 起動テンプレートの新しいバージョンまで一貫して生成したい。

3. 正解へ至る判断過程

まず「中央AMIを利用させる共有」か「配布先が所有するコピー」かを分ける。本問は中央アカウントから独立した所有権を求めるので、起動権限の共有だけでは不足する。次に、継続的なビルド、テスト、複数アカウント・リージョンへのコピー、起動テンプレート更新を一つのイメージ供給工程として扱えるかを見る。Image Builderのパイプラインと配布設定がこの組み合わせに合う。

4. 正解が要件を満たす理由

Image Builderはレシピ、ビルドコンポーネント、テストコンポーネントを使ってAMI作成を再現できる。配布設定では、出力AMIを指定した配布先アカウントとリージョンへコピーでき、配布先はそのコピーを所有する。launchTemplateConfigurationsを指定すると、新しいAMI IDを含む起動テンプレートバージョンも作成できる。

暗号化AMIのクロスアカウント配布では、配布先の EC2ImageBuilderDistributionCrossAccountRole が送信元と配布先のKMSキーへ必要な操作を行えること、送信元キーポリシーが配布先を許可することなどが必要である。これらをIaCで各アカウントへ展開すれば、長期アクセスキーを使わずに定期配布できる。なお、起動テンプレートのデフォルトバージョンを自動変更するかは昇格方針に合わせて設定し、本番承認前に勝手に切り替えない設計にする。

5. 各不正解選択肢が不適切な理由

- B：OUへの起動権限付与は共有であり、配布先がAMIコピーを所有しない。中央AMIや中央KMSキーへの依存も残り、中央AMI削除後も使えるという条件を満たさない。
- C：暗号化スナップショットから非暗号化コピーを作成することはできない。「暗号化解除してコピー」という前提が誤っている。さらに、毎回の手動選択とAWS管理キー固定は、指定した配布先カスタマーマネージドキーという要件に反する。
- D：Parameter StoreはAMI IDを配布する補助手段にはなるが、別アカウント・別リージョンへAMIを作成・所有させない。起動後の自己更新はゴールデンAMIの再現性を崩し、起動時間と失敗点も増やす。

6. 各不正解選択肢が正解になり得る条件

- B：中央アカウントがAMIを継続保有し、利用側は起動するだけでよく、コピー費用と各アカウントのAMI管理を減らしたい場合。
- C：一度限りの例外移行で、Automation runbookに承認済みコピー手順と適切なKMS再暗号化を実装する場合。ただし非暗号化にはできない。
- D：同一アカウント・リージョン内で、起動テンプレートやIaCが最新AMI IDをParameter Storeから解決するだけなら有効である。インスタンス内でOS更新を行う用途とは分ける。

7. 今後使える判断基準

AMI配布では、最初に「共有元が所有し続ける」か「利用先がコピーを所有する」かを確認する。暗号化された成果物をクロスアカウントで扱う問題では、リソース共有権限だけでなく、KMSキーポリシー、利用側IAM権限、サービスが引き受けるロールの3点を必ず点検する。

8. 関連サービスとの比較

EC2 Image Builderは継続的なイメージ製造・テスト・配布に向く。EC2のAMI共有はコピーを作らず利用権限を付ける方式で、AMIコピーはコピー先に独立したイメージを作る。Systems Manager AutomationでもAMI作成やコピー手順は組めるが、標準化された継続パイプラインとしてはImage Builderの方が運用項目を減らせる。Parameter StoreにAMI IDを発行する方法は、配布後の参照先発見には使えるが、イメージ自体を配布する機能ではない。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4

問題 059 | Domain 5 / ネットワーク | 複合難問 | 四択（1つ選択）

問題 59 集中ファイアウォールで戻り経路がずれる

企業は複数のスポークVPCをTransit Gatewayへ接続し、検査VPCのAWS Network Firewallを経由してVPC間通信を検査している。各AZにFirewall endpointを配置した。負荷試験では一部の長時間TCPセッションだけが切断され、ログから要求と応答が異なるAZのFirewall endpointを通過する非対称ルーティングが疑われた。Network Firewallはステートフルルールを使用している。検査を迂回せず、AZ障害にも耐え、セッションの往復を同じ検査経路へ維持したい。

最適な変更はどれか。

選択肢

A	すべてのスポークVPCで送信元/送信先チェックを無効にする。
B	Network Firewallのステートフルルールをすべてステートレスルールへ変える。
C	Transit Gatewayを廃止し、全スポーク間をVPCピアリングのフルメッシュにする。
D	検査VPCのTransit Gatewayアタッチメントでappliance modeを有効にし、Transit Gatewayルートテーブルで往路・復路をFirewall経由にする。

ここでいったん止める | 解答と解説は次ページ

問題 059 正解・解説 複合難問

問題 59の正解・解説

1. 正解

D

2. 問題文の重要な条件

Transit Gateway経由の集中検査、複数AZ、ステートフルFirewall、要求と応答のAZずれ、検査を迂回できないという条件である。

3. 正解へ至る判断過程

ステートフル装置は同じフローの双方向を同じ装置で見る必要がある。Transit Gatewayのappliance modeは、フローの存続中に同じAZのアタッチメントENIを使用するようセッションアフィニティを保つ。加えてTGWルートテーブルで両方向を検査VPCへ向ける。

4. 正解が要件を満たす理由

Firewall endpointごとの状態が往復で一致し、非対称経路による破棄を防げる。各AZのendpointを使う設計を維持するため、単一AZへ集約せず可用性も保てる。

5. 各不正解選択肢が不適切な理由

A: source/destination checkはEC2がルーターとして転送する場合の設定で、TGWのAZアフィニティを直さない。
B: 状態を捨てれば一部症状は変わり得るが、必要なステートフル検査能力を失い、要件を満たさない。
C: 接続管理が増大し、集中検査経路も失う。ピアリングは推移的ではない。
D: 正解肢のため対象外。

6. 各不正解選択肢が正解になり得る条件

AはEC2ベースのNAT・ルーター・ファイアウォールを自ら構成する場合に必要になる。Bは各パケットを独立評価するL3/L4の単純な stateless 制御だけで足りる場合に採り得る。Cは少数VPC間を直接・低コストで接続し、集中検査が不要なら候補になる。

7. 今後使える判断基準

TGW + ステートフルアプライアンス + 複数AZで断続的なセッション切断なら、appliance modeと往復ルートの対称性を確認する。

8. 関連サービスとの比較

Network Firewallはマネージドなネットワーク検査、AWS WAFはHTTPリクエスト検査、セキュリティグループはENI単位の許可制御である。Transit Gateway appliance modeは検査ルールそのものではなく、ステートフル装置へ対称に届ける経路機能である。

公式確認先 AWS公式 1 / AWS公式 2

問題 060 | Domain 4 / セキュリティ | 本番より難しい | 四択（1つ選択）

問題 60 GuardDuty Findingから隔離まで自動化する

GuardDutyが、踏み台EC2から暗号資産マイニング関連IPへの通信をHigh severityで検出した。会社は今後、同種Findingが発生したら数分以内にインシデント用セキュリティグループへENIを切り替え、スナップショットと証跡を取得し、SOCへ通知したい。ただしLow/Medium Findingでは自動隔離せず、担当者承認を残す。手動巡回は避けたい。

最適な実装はどれか。

選択肢

A	GuardDutyのtrusted IP listへ検出IPを追加し、Findingを自動的に非表示にする。
B	GuardDuty FindingをEventBridge ruleでseverity/typeにより選別し、Systems Manager Automation runbookまたはLambdaへ渡して隔離・証拠保全・通知を実行する。
C	GuardDutyを無効にし、Network ACLで全送信通信を拒否する。
D	Security Hubのワークフローステータスを RESOLVEDへ変えるだけで、EC2を自動停止させる。

ここでいったん止める | 解答と解説は次ページ

問題 060 正解・解説 本番より難しい

問題 60の正解・解説

1. 正解

B

2. 問題文の重要な条件

Highだけを数分で自動隔離し、複数の是正・証拠保全・通知を行い、低重要度は人手判断へ残す。イベント駆動が必要である。

3. 正解へ至る判断過程

GuardDutyはFindingをEventBridgeへ発行する。ルールでseverityやfinding typeを絞り、Automation runbook/Lambdaで定型手順を実行すれば、検出と是正を疎結合に自動化できる。

4. 正解が要件を満たす理由

重大度ごとの分岐、実行履歴、SNS/チケット連携、承認ステップを設計できる。GuardDuty自体へ隔離ロジックを詰め込まず、再利用可能なrunbookにできる。

5. 各不正解選択肢が不適切な理由

A: 悪性IPをtrusted扱いすると検出を抑制し、逆効果である。
B: 正解肢のため対象外。
C: 検出能力と必要な正当通信を失い、重大度別対応にならない。
D: Findingの状態変更はリソースへの是正操作ではない。

6. 各不正解選択肢が正解になり得る条件

Aは自社の既知スキャナー等、真に信頼できるIPによる誤検出を抑える場合だけ使う。Cの広い送信拒否は隔離SG/NACLとして一時的に利用できる。Dは調査・修復済みFindingのワークフロー整理に使う。

7. 今後使える判断基準

Findingから自動処理はEventBridgeで選別し、Lambda/Automationで実行する。検出サービス、イベントルーター、是正エンジンを分ける。

8. 関連サービスとの比較

GuardDutyは挙動・ログから脅威を検出、Inspectorは脆弱性を継続スキャン、Security HubはFindingを集約、Systems Manager Automationは運用手順を実行する。

公式確認先 AWS公式 1 / AWS公式 2

問題 061 | Domain 1 / 監視・性能 | 本番より難しい | 四択（1つ選択）

問題 61 接続急増と容量逼迫を分ける

API GatewayとAWS Lambdaで構成した注文APIが、RDS for MySQLのMulti-AZ DBインスタンスへ接続している。キャンペーン開始時、Lambdaの同時実行数が急増すると、DBのCPUより先に接続数と接続確立時間が上昇し、Too many connections が発生する。トランザクションの70%は書き込みを含み、セッション状態に依存するSQLは一部だけである。また、監査データの増加によって FreeStorageSpace が毎月低下している。アプリケーションのDBエンジン変更は許可されず、停止を伴う計画増強を毎月行うことも避けたい。読み取りの結果整合性と既存のMulti-AZ可用性は維持する。

運用変更とアプリケーション改修を最小限にして、二つのボトルネックに対処する最適な方法はどれか。

選択肢

A 読み取りレプリカを2台追加し、LambdaからすべてのSELECTをラウンドロビンする。空き容量アラームが発報するたびにソースDBとレプリカのストレージを手動で増やす

B DBインスタンスをメモリ最適化の最大クラスへ変更し、Lambdaの予約済み同時実行数をキャンペーン最大値に固定する。ストレージは現状のまま維持する

C RDS Proxyを導入して接続をプールし、DatabaseConnections、Proxyの借用待ち、接続ピン留めを監視する。RDSストレージオートスケーリングに十分な最大ストレージしきい値を設定し、FreeStorageSpaceも継続監視する

D Amazon Aurora Serverless v2へ移行して最小・最大ACUを設定し、Aurora Replica Auto Scalingとストレージの自動拡張に全面的に委ねる

ここでいったん止める | 解答と解説は次ページ

問題 061 正解・解説 本番より難しい

問題 61の正解・解説

1. 正解

C

2. 問題文の重要な条件

- CPU飽和ではなく、Lambdaの短時間の接続急増が先に障害を起こしている。
- 70%が書き込みであり、単純な読み取り分散だけでは主負荷を解決しない。
- DBエンジン変更は禁止されている。
- 容量増加への運用介入を減らしつつ、Multi-AZを維持する。
- 一部にセッション状態依存SQLがあるため、Proxyのピン留めも観測する必要がある。

3. 正解へ至る判断過程

接続枯渇とストレージ枯渇は原因が異なるため、一つのスケール機能でまとめて扱わない。短命かつ多数のLambda接続にはRDS Proxyの接続プールが適する。ただし、セッション状態の変更などで接続がピン留めされると多重化の効果が落ちるため、Proxyメトリクスとアプリケーション SQLを確認する。ストレージ側はRDSストレージオートスケーリングを有効にし、最大値と空き容量アラームを併用する。

4. 正解が要件を満たす理由

RDS Proxyはクライアント接続を受け、再利用可能なDB接続プールへ多重化するため、Lambdaの接続急増によるDBのメモリ・接続確立負荷を抑える。既存MySQLとMulti-AZを維持でき、障害時の接続復旧にも寄与する。ストレージオートスケーリングは空き容量が少ない状態を検知して割り当てストレージを増やすので、毎月の手動変更を減らせる。最大ストレージ値を適切に設定し、到達前に通知する監視は残すべきである。

5. 各不正解選択肢が不適切な理由

A: 読み取りレプリカは読み取り負荷には有効だが、書き込み主体の接続ストームを直接プールしない。RDSの通常の読み取りレプリカは需要に応じて自動で増減せず、すべてのSELECTを送るとレプリケーション遅延による整合性要件にも注意が要る。手動容量変更も要件に反する。
B: 大きなDBクラスは許容接続数を増やし得るが、接続生成の急増を吸収する設計ではない。常時最大クラスと過大な予約済み同時実行はコストが高く、ストレージ枯渇を解決しない。
C: 正解肢のため対象外。
D: 技術的には伸縮性が高いが、DBエンジン変更禁止という移行制約を満たさない。移行検証と停止・互換性確認も必要になる。

6. 各不正解選択肢が正解になり得る条件

A: 負荷の大部分が結果整合性を許容する読み取りで、アプリケーションがリーダー用エンドポイントを明示的に使える場合は有効である。
B: 接続数が安定しており、CPU・メモリ・ネットワーク帯域が継続的に不足し、短期的な垂直スケールが許容される場合は候補になる。
D: Aurora互換性が確認済みでエンジン移行が許可され、計算資源の変動も含めて自動伸縮させたい新規構築なら有力である。

7. 今後使える判断基準

RDSで DatabaseConnections が先に限界へ達するなら接続管理、CPUやI/Oが先ならDBクラス・ストレージ性能、FreeStorageSpaceなら容量管理を検討する。ProxyはSQL処理能力そのものやストレージ容量を増やさない。読み取りレプリカは接続プールでも書き込みスケール機能でもない。

8. 関連サービスとの比較

RDS Proxyは接続の多重化とフェイルオーバー時の接続回復、読み取りレプリカは読み取り分散、ストレージオートスケーリングは容量拡張を担当する。Multi-AZは主に可用性のための同期スタンバイであり、通常は読み取りスケール先として扱わない。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4

問題 062 | Domain 2 / 信頼性・BC | 本番相当 | 四択（1つ選択）

問題 62 昨日までのピークが当てにならない DynamoDB

新しいWebhook受信サービスは、受信イベントをAmazon DynamoDBへ書き込む。通常は1時間に数分しか書き込みがないが、提携先のキャンペーン開始時刻は事前通知されず、数十秒で直近ピークの10〜20倍へ増えることがある。夜間はほぼゼロになる。初月は信頼できるトラフィック履歴がなく、書き込みのスロットリングはイベント消失につながるため避けたい。一方、想定最大値の書き込みキャパシティを24時間プロビジョニングする費用は認められず、容量計画の運用も最小化したい。

最も適切なDynamoDBの容量設定はどれか。

選択肢

A オンデマンドキャパシティモードを使用する。直前ピークの2倍を30分以内に超える可能性があるため、想定ピークまでWarmThroughputを事前に引き上げ、テーブル/アカウントのクォータと任意の最大スループット上限が必要値を下回らないことを確認する

B プロビジョンドモードで最小値を通常負荷、最大値を想定最大負荷とし、ターゲット使用率70%のAuto Scalingだけに任せる

C プロビジョンドモードで想定最大書き込み容量を常時割り当て、Auto Scalingを無効にする

D 読み取り用にDynamoDB Accelerator（DAX）クラスターを作成し、テーブルの書き込み容量は通常負荷に固定する

ここでいったん止める | 解答と解説は次ページ

問題 062 正解・解説 本番相当

問題 62の正解・解説

1. 正解

A

2. 問題文の重要な条件

- 書き込みの時刻と規模が予測不能で、短時間に急増する。
- ほぼゼロの時間が長い。
- スロットリングを避けたいが、最大容量の常時費用は不可。
- 容量運用を最小化したい。

3. 正解へ至る判断過程

プロビジョンドAuto Scalingは実際の消費量をCloudWatchで観測してから容量を変更するため、秒単位の未知の急増には追随が遅れる場合がある。変動が大きくアイドル時間も長いワークロードでは、リクエスト単位で支払い、容量計画を減らせるオンデマンドが適する。ただしオンデマンドも「無限に瞬時」ではない。直前ピークの2倍を30分以内に超える10〜20倍スパイクには、事前にWarmThroughputを想定値まで引き上げる。

4. 正解が要件を満たす理由

オンデマンドモードは、利用者が通常のRCU/WCUを指定せず、需要に応じてDynamoDBが処理能力を調整する。WarmThroughputは急増前に処理可能な初期スループットを引き上げるもので、最大スループット設定は増強ではなく、利用量と費用を抑える上限である。予測不能、ゼロ付近まで落ちる、バッチ的に急増するというパターンで、高いプロビジョンド容量を常時維持するより費用と運用負荷を抑えやすい。

5. 各不正解選択肢が不適切な理由

- B：Auto Scalingはメトリクス超過を検知して更新するまで数分かかり得るため、数十秒の未知のスパイクでは初動をスロットリングする可能性がある。
- C：性能は確保しやすいが、ほぼゼロの時間にも最大容量へ課金され、費用要件に反する。
- D：DAXは読み取りキャッシュであり、テーブルへの書き込みキャパシティ不足を解消しない。

6. 各不正解選択肢が正解になり得る条件

- B：負荷が比較的滑らかで予測可能、一定のベースラインがあり、プロビジョンド容量の単価を活かしたい場合。
- C：負荷が常時高く一定で、スロットリング防止を最優先し、予約済みの一定容量が最も経済的な場合。
- D：読み取り中心で、同じキーへの低レイテンシー読み取りをキャッシュしたい場合。

7. 今後使える判断基準

DynamoDBでは「変動の幅」「立ち上がり速度」「ゼロ近くの時間」「容量運用の許容度」を見る。予測不能でスパイクとアイドルが大きいならオンデマンドが第一候補だが、直前ピークの2倍を短時間で超えるならWarmThroughputを事前設定する。最大スループットは急増対策ではなく制限であり、安定した基礎負荷があるならプロビジョンド＋Auto Scalingも比較する。

8. 関連サービスとの比較

DynamoDB Auto ScalingはApplication Auto Scalingのターゲット追跡でプロビジョンドRCU/WCUを変更する。オンデマンドは通常の容量計画を減らし、WarmThroughputは新しい急増前の処理能力を準備する。最大スループットはオンデマンド利用量のガードレールである。DAXは読み取りレイテンシーと読み取り負荷を下げるキャッシュで、書き込みの容量モードとは別の判断である。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4

問題 063 | Domain 3 / 展開・自動化 | 本番相当 | 四択（1つ選択）

問題 63 パッチの「承認」と「展開リング」を分ける

ある企業はAWS Organizations配下の35アカウント、3リージョンで、Amazon LinuxとWindows Serverを合わせて約1,800台運用している。すべてSystems Managerのマネージドノードである。これまではアカウントごとにMaintenance Windowを作成していたが、設定差異と更新漏れが増えている。

セキュリティ部門は、OSごとに承認ルールの異なるカスタムパッチベースラインを使用し、毎日コンプライアンスをスキャンしたい。インストールは、PatchRing=canary のノードへ水曜日、PatchRing=production のノードへ翌日曜日に行う。各リングでは同時実行率とエラーしきい値を制御し、必要な場合だけ再起動する。対象OUやリージョンが増えても、各アカウントへ同じ設定を手作業で追加したくない。

最も運用負荷が低く、要件を満たす構成はどれか。

選択肢

A 各OSのAWS管理パッチベースラインをデフォルトに設定し、全ノードを同じMaintenance Windowへ登録する。canaryとproductionの違いは、担当者が実行時に対象インスタンスIDを選び分ける

B Systems Manager Quick Setupで、Organizationsの対象OU・リージョンを指定したPatch Managerパッチポリシーをリングごとに作成する。ノードタグで対象を分け、OS別カスタムベースライン、スキャンとインストールの各スケジュール、再起動方針、同時実行率、エラーしきい値、ログ保存先を設定する

C State Managerで AWS-GatherSoftwareInventory を毎日実行し、見つかった更新プログラムをEventBridgeからLambdaで各ノードへ直接インストールする

D AWS ConfigのEC2関連マネージドルールを全アカウントへ展開し、非準拠になったインスタンスをAuto Scalingのインスタンス更新で置き換える

ここでいったん止める | 解答と解説は次ページ

問題 063 正解・解説 本番相当

問題 63の正解・解説

1. 正解

B

2. 問題文の重要な条件

- 多数のアカウントとリージョンをOrganizations単位で一元設定したい。
- 日次スキャンと週次インストールは別スケジュールである。
- canaryとproductionで対象と実行日を分離する。
- OSごとの承認ルール、再起動、同時実行率、失敗停止条件が必要である。

3. 正解へ至る判断過程

個々のノードでパッチを実行できるかではなく、組織全体へ同じ運用ポリシーをどう展開するかが焦点である。Maintenance WindowやState Manager associationは一つのアカウント・リージョン単位で構成すると数が増える。Quick Setupのパッチポリシーは、OrganizationsのOUと複数リージョンを対象に、スキャン、インストール、ベースライン、レート制御をまとめて定義できる。異なる展開日を持つリングは、タグ対象の異なるポリシーとして分ける。

4. 正解が要件を満たす理由

パッチポリシーは、OSタイプごとにAWS管理またはカスタムパッチベースラインを選択でき、スキャンとインストールに別のcronまたはrateスケジュールを設定できる。Organizations全体または選択OU・リージョンへ展開でき、ノードタグによる対象指定、再起動オプション、同時実行とエラーしきい値も設定できる。canaryとproductionを別ポリシーにすれば、同じ承認ルールを使いながら時間差で展開できる。

プライベート接続だけを使うノードでは、Systems Manager用エンドポイントに加え、Quick Setupが作成するパッチポリシー用S3バケットをS3エンドポイントポリシーとノードロールが読み取れることも確認する。ここを見落とすと、ポリシー自体は配布されても実行時にベースライン情報を取得できない。

5. 各不正解選択肢が不適切な理由

- A：手動のインスタンス選択はリングの誤選択を招き、多数のアカウント・リージョンで設定を一元化できない。AWS管理ベースライン固定もOS別の独自承認ルールを満たさない。
- C：Inventoryはソフトウェア情報を収集する機能で、パッチ承認ルールや依存関係を評価してインストールする仕組みではない。独自Lambdaは再起動、失敗停止、OS差異の実装負荷が大きい。
- D：AWS Configは構成評価に向くが、ゲストOSのパッチベースラインに従ったインストールを代替しない。状態を評価せず全インスタンスを置き換えると、非Auto Scalingノードや状態保持サーバーにも適用できない。

6. 各不正解選択肢が正解になり得る条件

- A：単一アカウント・リージョンの小規模環境で、全ノードを同一日程・同一ベースラインで更新する場合。
- C：Inventory結果に基づく独自ソフトウェアの配布など、Patch Managerが扱わないアプリケーション更新を個別ロジックで行う場合。
- D：完全にイミュータブルなAuto Scalingワークロードで、パッチ済みAMIを作成後、インスタンス更新により全台を置き換える方針の場合。

7. 今後使える判断基準

パッチ問題では「何を承認するか」をパッチベースライン、「誰にいつ適用するか」をポリシー・タグ・スケジュール、「どの速度で止めるか」を同時実行率とエラーしきい値として分解する。複数アカウント・リージョンへ同じ運用を展開するなら、まずQuick Setupの組織向けパッチポリシーを検討する。

8. 関連サービスとの比較

Patch Managerはパッチの選定、スキャン、インストール、コンプライアンスを扱う。Maintenance Windowsはパッチ以外を含む中断可能な作業を決められた時間枠で実行する。State Managerは望ましい構成を継続的に再適用し、Inventoryはノード内のメタデータを収集する。イミュータブル運用ではImage BuilderとEC2 Auto Scalingインスタンス更新が代替になり得るが、状態保持ノードを含む混在フリートではPatch Managerの方が直接的である。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4

問題 064 | Domain 5 / ネットワーク | 本番相当 | 四択（1つ選択）

問題 64 在宅勤務者ごとのVPCアクセス

300人の運用担当者が自宅や出張先から、VPC内の管理ポータルとプライベートIPのEC2へ接続する必要がある。端末の送信元IPは変動する。会社のSAML IdPでユーザーを認証し、グループごとに到達可能なVPCネットワークを分け、退職者の証明書を個別管理する負担を減らしたい。拠点間の常時接続ではなく、ユーザーが必要なときだけ接続する方式が求められる。

最適な構成はどれか。

選択肢

A	各自宅ルーターとAWS間にSite-to-Site VPNを作成し、静的ルートを配布する。
B	AWS Client VPN endpointを複数AZのサブネットへ関連付け、SAMLフェデレーション認証とグループ別authorization ruleを設定する。
C	各EC2へElastic IPを付与し、セキュリティグループで利用者の現在IPを毎日更新する。
D	AWS PrivateLink endpoint serviceを作成し、利用者PCへインターフェイスエンドポイントを作る。

ここでいったん止める | 解答と解説は次ページ

問題 064 正解・解説 本番相当

問題 64の正解・解説

1. 正解

B

2. 問題文の重要な条件

個人端末からのオンデマンド接続、変動IP、SAML IdP、グループ別認可、300人規模、複数AZの可用性が必要である。

3. 正解へ至る判断過程

AWS Client VPNはマネージドなクライアントVPNで、SAMLフェデレーション認証と接続先ネットワーク単位のauthorization ruleを利用できる。サブネット関連付けを複数AZに置けば、単一AZ依存も避けられる。

4. 正解が要件を満たす理由

利用者はOpenVPN互換クライアントなどから必要時に接続し、認証ライフサイクルは既存IdPへ寄せられる。ユーザーグループごとの認可をAWS側で表現でき、利用者の公衆IPを許可リスト管理する必要がない。

5. 各不正解選択肢が不適切な理由

A: Site-to-Site VPNは拠点ネットワーク間の常時接続向けで、300台の変動する個人端末には運用負荷が大きい。
B: 正解肢のため対象外。
C: 管理面をインターネットへ公開し、日々のIP更新が必要で、最小公開の要件に反する。
D: PrivateLinkはVPC内のサービスを他VPCへ非公開公開する機能で、一般の利用者PCへエンドポイントを作るリモートアクセスVPNではない。

6. 各不正解選択肢が正解になり得る条件

Aは固定した拠点ネットワークをVPCへ接続する場合に適する。Cは公開Webサービスで厳格な別認証・WAF等があり、管理面ではない場合に限る。Dは別VPCの利用者へ特定サービスだけを一方向に公開したい場合に有力である。

7. 今後使える判断基準

「人・端末が必要時に入る」はClient VPN、「拠点ネットワーク同士」はSite-to-Site VPN、「VPC間で特定サービスだけ見せる」はPrivateLinkと整理する。

8. 関連サービスとの比較

Client VPNのauthenticationは本人確認、authorization ruleは接続後に到達できるCIDRの制御である。セキュリティグループやルートも別途必要であり、認証だけで通信が成立するわけではない。

公式確認先 AWS公式 1 / AWS公式 2

問題 065 | Domain 4 / セキュリティ | 本番より難しい | 四択（1つ選択）

問題 65 稼働中・イメージ・関数のCVEを継続評価する

組織はEC2、ECRのコンテナイメージ、Lambda関数を多数運用している。SOCは既知CVEと意図しないネットワーク露出を継続的に評価し、悪用可能性や修正済みバージョンを考慮して優先順位を付けたい。S3の個人情報分類や実際の不審API活動ではない。各開発チームが個別の脆弱性スキャナーサーバーを保守することも避けたい。

最適なサービスはどれか。

選択肢

A	Amazon Macie
B	AWS CloudTrail Insights
C	Amazon InspectorをOrganizationsの委任管理者から有効化し、対象リソースタイプの継続スキャンを管理する。
D	Route 53 Resolver DNS Firewall

ここでいったん止める | 解答と解説は次ページ

問題 065 正解・解説 本番より難しい

問題 65の正解・解説

1. 正解

C

2. 問題文の重要な条件

EC2/ECR/Lambda、CVE、ネットワーク露出、継続評価、修正とリスクによる優先順位、組織集中管理である。

3. 正解へ至る判断過程

Inspectorは対応するcompute workloadとcontainer images、Lambdaを継続スキャンし、vulnerability findingsを生成する。Organizationsでアカウントとリソースタイプを集中管理できる。

4. 正解が要件を満たす理由

スキャナー基盤を自前運用せず、新CVEやリソース変更に追随する継続評価と修復情報を得られる。EC2のnetwork reachabilityもFindingの文脈へ利用できる。

5. 各不正解選択肢が不適切な理由

A: MacieはS3機密データ分類である。
B: CloudTrail Insightsは通常と異なるAPI呼び出し率等を検出し、パッケージCVEをスキャンしない。
C: 正解肢のため対象外。
D: DNS Firewallはドメイン問い合わせの制御で、コードやパッケージ脆弱性を評価しない。

6. 各不正解選択肢が正解になり得る条件

Aはデータ分類、Bは異常な管理API活動、Dは悪性ドメインへのDNSアクセス予防で正解になる。

7. 今後使える判断基準

CVE・パッケージ・イメージ・関数はInspector。実際の侵害兆候はGuardDuty。機密データはMacie。役割名ではなく入力データとFindingの種類で選ぶ。

8. 関連サービスとの比較

ECR basic/enhanced scanningのうち、Inspector連携のenhanced scanningは継続・拡張された脆弱性評価を提供する。Security HubへInspector Findingを統合すればSOCの一元管理が可能になる。

公式確認先 AWS公式 1 / AWS公式 2

問題 066 | Domain 1 / 監視・性能 | 本番相当 | 四択（1つ選択）

問題 66 節約提案を性能要件に合わせる

ある組織は、200台のEC2インスタンスと複数のAuto Scalingグループを運用している。財務部門は月額費用を15%削減したいが、決済ワークロードでは月末のメモリ使用量とネットワークPPSが通常日の数倍になる。現在はCPUメトリクスしか収集しておらず、直近14日間だけを見ると多くのインスタンスが過剰に見える。Savings Plansによる割引も既に適用されている。運用部門は、割引後の節約見込みを優先順位付けしながら、月末ピークを含む性能リスクを明示して段階的にサイズ変更したい。

最も適切な進め方はどれか。

選択肢

A Cost ExplorerのRightsizing RecommendationsをCPUだけで適用し、節約額が最大のインスタンスから直ちに停止または縮小する

B Trusted Advisorの低使用率EC2チェックを唯一の根拠にし、月末前に全対象を1サイズ縮小する

C CloudWatchの平均CPUが20%未満のインスタンスに対し、同一ファミリー内で最小のサイズを固定的に選ぶ。Savings Plansのコミットメントは性能余力として扱う

D Compute Optimizerを有効化し、CloudWatch agentでメモリメトリクスも収集する。十分なルックバック期間、CPU・メモリのヘッドルームとインスタンスファミリー設定を調整し、Savings estimation modeまたはCost Optimization Hub連携による割引後節約額と性能リスクを比較して、検証後に段階適用する

ここでいったん止める | 解答と解説は次ページ

問題 066 正解・解説 本番相当

問題 66の正解・解説

1. 正解

D

2. 問題文の重要な条件

- CPU以外にメモリとネットワークPPSが制約になり得る。
- 14日では月末ピークを含まず、観測期間の偏りがある。
- 既存割引後の実質的な節約見込みで優先順位を付けたい。
- 決済系なので、費用削減だけでなく性能リスクと余力を明示する必要がある。
- 200台を一括変更せず段階適用したい。

3. 正解へ至る判断過程

まず観測データを要件に合わせる。EC2のゲストOSメモリは標準EC2メトリクスに含まれないため、CloudWatch agentなどで収集してCompute Optimizerに利用させる。次に、月末を含むルックバック期間とヘッドルームを設定し、CPU、メモリ、EBS、ネットワーク帯域・PPSなどを考慮した性能リスクを比較する。最後に、割引を反映したSavings opportunityを使って候補を順位付けし、代表ワークロードで検証してから展開する。

4. 正解が要件を満たす理由

Compute Optimizerは現行構成と推奨構成について複数のリソース仕様から性能リスクを算出し、rightsizing preferenceでルックバック、CPUしきい値・ヘッドルーム、メモリヘッドルーム、対象ファミリーを調整できる。Savings estimation modeやCost Optimization Hubのデータを用いると、On-Demand定価だけでなく適用済み割引を踏まえた節約見込みを比較できる。提案は自動的な安全保証ではないため、段階検証を組み合わせることも要件に合う。

5. 各不正解選択肢が不適切な理由

A: CPUだけかつピークを含まない観測から即時変更すると、メモリやPPSのボトルネックを見落とす。停止はrightsizingとは異なる影響を持つ。
B: Trusted Advisorは有用な入口だが、月末ピーク、メモリ、詳細な性能リスクとカスタムヘッドルームを十分に反映する唯一の根拠にはならない。
C: 平均CPUだけではバーストや他資源を評価できない。Savings Plansは料金コミットメントであり、インスタンスの性能余力ではない。
D: 正解肢のため対象外。

6. 各不正解選択肢が正解になり得る条件

A: 非本番の中断可能な環境で、CPU以外の制約がないと実測済みであり、停止候補を迅速に洗い出す場合には有効である。
B: 小規模で低リスクの環境に対する一次スクリーニングなら、Trusted Advisorのチェックを使える。
C: 単一CPU制約の均質なバッチで、最大値や処理時間も別途検証済みなら、単純な同一ファミリー縮小が候補になる。

7. 今後使える判断基準

rightsizingでは「観測期間がピークを含むか」「標準メトリクスにない資源を収集したか」「推奨先の性能リスク」「実際の割引後コスト」を確認する。低い平均CPUだけで縮小を決めない。推奨は意思決定材料であり、変更前の負荷試験や段階展開を省略する理由にはならない。

8. 関連サービスとの比較

Compute Optimizerは利用率からリソース構成を推奨する。Cost ExplorerとCost Optimization Hubは費用の可視化・最適化機会の集約に強く、Trusted Advisorは広いベストプラクティスチェックを提供する。CloudWatchは元となる運用メトリクスと変更後検証を担う。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4

問題 067 | Domain 2 / 信頼性・BC | 本番より難しい | 四択（1つ選択）

問題 67 両リージョンで書ける買い物かご

世界向けECサイトは、東京とフランクフルトの両リージョンでAPIをactive/active稼働させる。買い物かごはDynamoDBに保存し、通常はユーザーをホームリージョンへ固定するが、一方のリージョン障害時はもう一方で直ちに読み書きを継続したい。アプリケーションは同じユーザーの同時更新を条件付き書き込みと冪等キーで抑えられ、リージョン間で1秒程度の一時的な不一致を許容する。目標は、リージョン障害時のRTOをほぼ0、RPOを低く保ち、自作レプリケーションの運用を避けることである。

最も適切な構成はどれか。

選択肢

A 東京のDynamoDBテーブルだけを使用し、フランクフルトAPIからは東京のリージョナルエンドポイントを呼び出す

B Multi-Region eventual consistency（MREC）のDynamoDB global tableを作成し、各APIはローカルレプリカへ読み書きする。ReplicationLatency などを監視し、アプリケーションのリージョンアフィニティと競合回避を維持する

C 東京のDynamoDBから毎分エクスポートし、フランクフルトで新しいテーブルへインポートする

D 各リージョンに独立テーブルを作り、DAXクラスター同士が更新を複製するよう設定する

ここでいったん止める | 解答と解説は次ページ

問題 067 正解・解説 本番より難しい

問題 67の正解・解説

1. 正解

B

2. 問題文の重要な条件

- 2リージョンの両方が通常時から読み書きするactive/active。
- 一時的な不一致を許容し、アプリ側で同時更新を抑制できる。
- リージョン障害時はほぼ即時に継続したい。
- 自作の複製処理を避ける。

3. 正解へ至る判断過程

DynamoDB global tablesはmulti-Region、multi-activeで、各レプリカが読み書きを受け付け、自動的に更新を複製する。強いリージョン間整合性が要求されず、短い一時的不一致を許容するためMRECが要件に合う。競合の可能性は、ユーザーのリージョンアフィニティや冪等性で抑える。

4. 正解が要件を満たす理由

各リージョンのアプリケーションはローカルDynamoDBエンドポイントへ低レイテンシーでアクセスできる。一方が停止しても、もう一方のレプリカは既に書き込み可能であるため、DBの昇格処理が不要でRTOを極小化できる。複製はマネージドで、ReplicationLatency や保留件数をCloudWatchで監視できる。

5. 各不正解選択肢が不適切な理由

- A：東京リージョンが単一障害点となり、フランクフルトからのレイテンシーも増える。
- C：毎分のバッチ処理ではRPO/RTOが大きく、切替可能な継続レプリカにもならない。
- D：DAXは各テーブルの読み取りキャッシュであり、独立テーブル間のレプリケーション機能ではない。

6. 各不正解選択肢が正解になり得る条件

- A：単一リージョン障害を対象外とし、強い単一書き込み地点を最優先する場合。
- C：分析用の時点データを低頻度で複製し、オンラインDRを必要としない場合。
- D：各リージョンの独立データに対して、ローカルの読み取りキャッシュだけを高速化する場合。

7. 今後使える判断基準

即時のmulti-Region書き込み継続には、「フェイルオーバー時に昇格が必要か」を見る。global tablesは各レプリカが既に書き込み可能で、Aurora Global DatabaseやRDSリードレプリカのような単一ライター昇格型とは異なる。MRECでは同じ項目への同時書き込み競合をアプリケーション設計に含める。

8. 関連サービスとの比較

MREC global tablesは非同期でmulti-active、短い不一致を許容する。MRSC global tablesは対応条件の下でmulti-Region強整合性を提供するが、作成後に整合性モードを変更できず、リージョン構成などの制約確認が必要である。Aurora Global Databaseは通常1つのプライマリリージョンで書き込み、ElastiCache Global Datastoreもプライマリからセカンダリへの非同期複製が基本である。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3

問題 068 | Domain 3 / 展開・自動化 | 本番相当 | 四択（1つ選択）

問題 68 一度直すのではなく、望ましい状態へ戻し続ける

ある製造会社は、複数のVPCにある約600台のLinux EC2インスタンスをSystems Managerのマネージドノードとして運用している。監視標準では、CloudWatchエージェントの指定バージョン、承認済み設定ファイル、およびサービスの自動起動が必要である。しかし、障害調査中の一時変更や手作業によって、数日後には設定がばらつく。セキュリティチームは、インストール済みアプリケーションとバージョンの一覧も毎日取得し、環境タグ単位で構成準拠状況を確認したい。

SSHポートや踏み台は追加できない。設定のずれは30分以内に再評価し、承認済み状態へ自動的に戻したい。一方、AMIを毎回置き換えるほどの変更ではなく、既存インスタンスを継続利用する。最も適切な構成はどれか。

選択肢

A Run Commandで全ノードへ設定スクリプトを1回送信し、CloudTrailで SendCommand を記録する。以後のドリフトは月次作業で再送信する

B Patch Managerのカスタムパッチベースラインへ CloudWatchエージェントのパッケージ名と設定ファイルを登録し、30分ごとに ScanAndInstall を実行する

C State Manager associationをタグ対象で作成し、承認済みSSMドキュメントを30分ごとに実行してパッケージ、設定ファイル、サービス状態を検査・修正する。別のassociationで AWS-GatherSoftwareInventory を毎日実行し、associationの準拠状況をComplianceで、収集したソフトウェア情報をInventoryで確認する

D AWS Configの記録対象にEC2インスタンスを追加し、インスタンスが非準拠になったら必ず終了して、同じAMIから新規起動する

ここでいったん止める | 解答と解説は次ページ

問題 068 正解・解説 本番相当

問題 68の正解・解説

1. 正解

C

2. 問題文の重要な条件

- 既存ノードの設定が時間とともにずれるため、定期的な再評価と自動修復が必要である。
- パッチではなく、エージェント、ファイル、サービス状態というゲストOS内の望ましい構成を維持する。
- ソフトウェア一覧の収集と、構成適用の準拠状況の両方が必要である。
- SSHを使わず、タグ単位で多数ノードを管理する。

3. 正解へ至る判断過程

一度だけ命令を送るのか、宣言した状態を繰り返し維持するのかを見分ける。本問は30分以内にドリフトを戻すため、一回限りのRun Commandではなく State Manager associationが中心になる。構成維持とソフトウェア台帳は別目的なので、後者にはInventoryの収集associationを組み合わせる。

4. 正解が要件を満たす理由

State ManagerはSSMドキュメントと対象をassociationとして結び、スケジュールに従って再実行できる。タグを対象にすれば、Auto Scalingなどで増えたノードも個別IDの更新なしに含められる。ドキュメントを冪等に作り、現状態を検査して差があるときだけパッケージ、ファイル、サービスを修正すれば、不要な再起動を避けながら望ましい状態を維持できる。

Systems Manager Inventoryは AWS-GatherSoftwareInventory のassociationで有効化でき、アプリケーション、AWSコンポーネント、ネットワーク構成などのメタデータを収集する。State Manager associationの実行状態とInventoryのデータを分けて持つことで、「設定が準拠しているか」と「何がインストールされているか」を混同せず監査できる。

5. 各不正解選択肢が不適切な理由

- A：最初の適用とAPI監査はできるが、その後に発生したずれを30分以内に検出・修復しない。月次再送では要件を満たさない。
- B：Patch Managerのパッチベースラインは OSパッチの承認と適用を制御するもので、任意の設定ファイルやサービス起動状態を維持する構成管理機能ではない。
- D：AWS ConfigはAWSリソース構成の履歴と評価に向くが、標準の記録だけでゲストOS内ファイルを修復しない。同じ未修正AMIから再起動すれば同じ差異が再現し、状態保持中のノード終了も過剰である。

6. 各不正解選択肢が正解になり得る条件

- A：緊急時の一回限りのコマンドや、再発しないことが分かっている変更を監査付きで大量実行する場合。
- B：目的がOSセキュリティ更新の承認、スキャン、インストールであり、ファイルやサービス構成は別手段で管理する場合。
- D：完全にイミュータブルなステートレスフリートで、修正版AMIからAuto Scalingインスタンス更新を行い、既存ノードを修正しない方針の場合。

7. 今後使える判断基準

Run Commandは「今これを実行」、State Managerは「この状態を保つ」、Inventoryは「中に何があるか記録」、Patch Managerは「承認済みOSパッチを適用」と覚える。定期associationで使うドキュメントは、何度実行しても同じ安全な結果になる冪等性が重要である。

8. 関連サービスとの比較

State Managerは定常状態の維持、Maintenance Windowsは中断を伴う作業の時間枠、Automationは複数のAWS APIやノード操作を順序・分岐付きで実行するワークフローである。Inventoryは収集のみで自動修復しない。AWS ConfigとInventoryを組み合わせればOS情報の経時監査を補強できるが、修復主体はState ManagerやAutomationになる。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4

問題 069 | Domain 5 / ネットワーク | 本番より難しい | 四択（1つ選択）

問題 69 VPNトンネル障害を先に知る

オンプレミスデータセンターとTransit GatewayをSite-to-Site VPNで接続し、BGPによる動的ルーティングを使用している。VPN接続には2本のトンネルがあり、現在は片方が主に利用されている。過去に待機側トンネルが数日前からダウンしていたことに気づかず、利用中トンネルの保守時に完全断が起きた。経路を手動で固定せず、トンネルの冗長性を維持したまま、片方だけの障害でも直ちに通知したい。

最適な対応はどれか。

選択肢

A	VPC Flow LogsのACCEPTレコード数が0になったときだけ通知する。
B	BGPを無効にし、単一の静的ルートを利用中トンネルへ向ける。
C	各VPNトンネルのCloudWatch TunnelStateを監視するアラームを作成し、SNSへ通知する。BGPと2トンネルは維持する。
D	Route 53ヘルスチェックでオンプレミスルーターのプライベートを監視する。

ここでいったん止める | 解答と解説は次ページ

問題 069 正解・解説 本番より難しい

問題 69の正解・解説

1. 正解

C

2. 問題文の重要な条件

1本のトンネルが稼働している間にも、もう1本のダウンを知る必要がある。BGPと冗長構成は維持し、即時通知したい。

3. 正解へ至る判断過程

Site-to-Site VPNはトンネルごとのCloudWatchメトリクスを発行する。TunnelStateを各トンネルについて監視すれば、アプリケーショントラフィックが継続していても冗長性の低下を検出できる。

4. 正解が要件を満たす理由

片方だけのダウンを直接検出し、CloudWatch AlarmからSNSへ通知できる。BGPによる動的な経路選択と2トンネル構成を変えないため、復旧力を損なわない。

5. 各不正解選択肢が不適切な理由

A: もう一方のトンネルに通信が流れていれば0にならず、冗長性低下を検出できない。Flow LogsはVPNトンネル状態の直接メトリクスでもない。
B: 待機経路を失い、今回防ぎたい完全断の可能性を高める。
C: 正解肢のため対象外。
D: Route 53ヘルスチェッカーは通常、インターネットから到達不能なプライベートIPを直接監視できず、VPNトンネル単位の状態も示さない。

6. 各不正解選択肢が正解になり得る条件

AはVPC内の実トラフィック傾向を補助的に調査する場合に使える。Bの静的ルートはBGP非対応装置で小規模な固定経路しかない場合に必要となる。Dは公開エンドポイントの可用性を外部視点で監視し、DNSフェイルオーバーへ利用する場合に適する。

7. 今後使える判断基準

HA構成では「サービスがまだ動くか」だけでなく「冗長系が失われていないか」を個別メトリクスで監視する。VPNならトンネル単位のTunnelStateを確認する。

8. 関連サービスとの比較

TunnelStateは制御面の状態、TunnelDataIn/Outは転送量である。Network Synthetic Monitorを併用すれば、トンネルがUPでも生じるオンプレミスまでのパケット損失や往復遅延を継続評価できる。

公式確認先 AWS公式 1 / AWS公式 2

問題 070 | Domain 4 / セキュリティ | 複合難問 | 複数選択（5つから2つ選択）

問題 70 人の異動を80アカウントへ安全に反映する

企業はAWS Organizations配下の80アカウントを、開発・本番・監査OUに分けている。従業員の認証は既存のSAML 2.0対応IdPで統一され、このIdPはIAM Identity Center対応のSCIM v2.0によるユーザー・グループの自動プロビジョニングにも対応している。入社・異動・退職の情報はIdP側のグループで管理している。各アカウントへIAMユーザーや長期アクセスキーを作らず、同じ職務の利用者には同じ権限セットを複数アカウントへ割り当てたい。本番運用者のセッション時間は1時間、監査者は読み取り専用にし、異動時の反映を自動化する必要がある。

要件を満たす対策を2つ選べ。

選択肢

A	IAM Identity Centerを既存の外部IdPと連携し、SCIMによるユーザー・グループの自動プロビジョニングを構成する。
B	各アカウントに同名IAMユーザーを作り、アクセスキーをIdPの属性へ保存する。
C	SCPでAllowした操作を各利用者の実権限として付与し、IAMロールは作成しない。
D	職務ごとのpermission setに最小権限ポリシーとsession durationを定義し、IdP同期グループを対象アカウントへ割り当てる。
E	管理アカウントrootの認証情報をSecrets Managerへ保存し、各OU管理者へ共有する。

ここでいったん止める | 解答と解説は次ページ

問題 070 正解・解説 複合難問

問題 70の正解・解説

1. 正解

A、D

2. 問題文の重要な条件

既存IdPが人のライフサイクルを管理し、80アカウントへ職務単位の一貫した短期アクセスを配布する。IAMユーザーと長期キーは禁止で、職務ごとにセッション時間も変える。

3. 正解へ至る判断過程

IAM Identity Centerは外部IdPの認証とSCIM同期を利用できる。Permission setはアカウントへプロビジョニングされるIAMロールの権限・セッション設定を一元定義し、ユーザーまたはグループとアカウントの組み合わせへ割り当てる。したがって、アイデンティティ同期と権限配布の二つを組み合わせる。

4. 正解が要件を満たす理由

Aで入社・異動・退職をIdPグループから同期し、Dで開発者・本番運用者・監査者のpermission setを各アカウントへ再利用できる。利用者はフェデレーション後に短期認証情報を取得するため、長期アクセスキーを配らずに済む。

5. 各不正解選択肢が不適切な理由

A: 正解肢のため対象外。
B: 80アカウントで重複する長期認証情報と退職処理が生まれ、要件に反する。
C: SCPはアカウント内主体の最大権限を制限するだけで、利用者へ権限を付与しない。
D: 正解肢のため対象外。
E: root共有は職務分離、監査、最小権限のすべてに反し、通常操作へrootを使うべきではない。

6. 各不正解選択肢が正解になり得る条件

Bはフェデレーション非対応の古い仕組みで例外的にIAMユーザーが必要な場合でも、アクセスキーを避け、厳格なライフサイクル管理を行う。CはOU単位で禁止操作の上限を追加する補助統制として有効である。Eが正解になる通常条件はなく、rootは保護して限定的なアカウント作業にだけ使う。

7. 今後使える判断基準

人のマルチアカウントアクセスはIdentity Center、職務権限の再利用はpermission set、人の所属同期はSCIM、組織の最大権限はSCPと分ける。Permission setはSCPを越えられない。

8. 関連サービスとの比較

IAM role federationをアカウントごとに直接構成することもできるが、Identity Centerは割り当て・ポータル・短期認証情報を組織規模で統合する。Permissions boundaryは個別IAM主体の上限で、permission setによる人の割り当て管理とは目的が異なる。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3

問題 071 | Domain 1 / 監視・性能 | 本番より難しい | 複数選択（5つから2つ選択）

問題 71 短い障害と少数標本

動画配信APIは、リクエスト数、5xx数、応答時間をカスタムメトリクスとして発行している。大規模配信中には20〜30秒の5xx率上昇でも自動フェイルオーバーを開始したい。一方、深夜は1分あたり数件しかリクエストがなく、1件の遅い応答だけでp99アラームが頻繁に状態遷移している。リクエスト量には曜日と時刻による強い周期性がある。運用チームは、短い実障害を検出しつつ、統計的に標本が少ない時間帯のp99誤通知を抑えたい。

要件を満たすために行うべき変更を2つ選べ。

選択肢

A	リクエスト数と5xx数を StorageResolution=1 の高解像度メトリクスとして発行し、メトリクス数式で5xx率を算出する。10秒または30秒周期の高解像度アラームを作成し、必要な評価期間とdatapoints-to-alarmを設定する
B	既存の60秒標準解像度メトリクスに対し、アラームのPeriodだけを1秒へ変更する
C	リクエスト数の異常検出バンドを作り、バンドを上回る場合も下回る場合も、5xx率を確認せず直ちにフェイルオーバーする
D	応答時間のp99アラームで、低サンプル時のパーセンタイル評価を無視して現在状態を維持する設定を選ぶ
E	p99の代わりに1分間のMaximumだけを使用し、欠損データを常にbreachingとして扱う

ここでいったん止める | 解答と解説は次ページ

問題 071 正解・解説 本番より難しい

問題 71の正解・解説

1. 正解

A、D

2. 問題文の重要な条件

- 20〜30秒の障害を検知するには、60秒未満のデータと評価周期が必要である。
- 判断対象は絶対5xx数ではなく、トラフィック量で正規化した5xx率である。
- 深夜のp99は標本数不足によって不安定であり、欠損とは別問題である。
- 周期性はあるが、リクエスト量の変動自体を障害と断定してはいけない。

3. 正解へ至る判断過程

短時間検知については、最初から高解像度でデータを発行し、率をメトリクス数式で計算して高解像度アラームにする。標準解像度のままPeriodだけ短くしても、必要な粒度の観測値は得られない。p99については、少数標本時に統計的評価を続けるか、状態を維持して十分なデータを待つかを設定できるため、後者を選ぶ。

4. 正解が要件を満たす理由

Aは1秒ストレージ解像度のカスタムメトリクスと10秒・30秒の高解像度アラームを組み合わせ、20〜30秒級の上昇を評価できる。分子と分母を同周期で収集して5xx率を計算するため、リクエスト量の大小にも対応する。Dは低サンプル時にp99を無理に評価せず、アラームの現在状態を維持するため、深夜の1件による不要な状態遷移を減らす。

5. 各不正解選択肢が不適切な理由

A: 正解肢のため対象外。
B: 60秒の標準解像度で発行されたデータから、1秒ごとの新しい事実は生成できない。また高解像度アラームで指定できる代表的な短周期は10秒または30秒である。
C: 異常検出は周期性を学習できるが、リクエスト数が予想範囲外というだけで5xx障害とは限らない。低トラフィックも正常な営業変化もフェイルオーバーさせ得る。
D: 正解肢のため対象外。
E: Maximumは外れ値1件にさらに敏感であり、p99誤通知の問題を悪化させる。低サンプルと欠損データを同一視している。

6. 各不正解選択肢が正解になり得る条件

B: 1分以上続く事象だけが対象で、元メトリクスもアラームPeriodも60秒以上でよいなら標準解像度で十分である。
C: 需要急増そのものが容量枯渇の先行指標であり、別の安全条件と複合してスケールアウトする用途なら異常検出が役立つ。
E: 1件でもしきい値超過が重大事故を意味し、無通信も故障として扱うハートビート型メトリクスならMaximumとbreachingが妥当になり得る。

7. 今後使える判断基準

検知したい最短事象より粗い解像度では検知できない。率は分子・分母から同じ時間窓で計算する。さらに「データがない」と「データはあるがパーセンタイルを信頼できる標本数がない」を区別し、前者はmissing data、後者はlow sample countの設定で扱う。

8. 関連サービスとの比較

静的しきい値は明確なSLO境界に、異常検出は曜日・時間帯によって正常範囲が変わるメトリクスに向く。メトリクス数式はエラー率などの派生値を作り、複合アラームは複数の既存アラーム状態を論理結合する。高解像度メトリクスと高解像度アラームには追加料金があるため、短時間検知が必要な指標へ限定する。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4

問題 072 | Domain 2 / 信頼性・BC | 本番相当 | 四択（1つ選択）

問題 72 公開カタログとログイン状態を同じキャッシュにしない

小売企業のWebアプリケーションには2種類の負荷がある。

- /catalog：世界中から参照され、同じ言語・検索条件なら全利用者で同一の応答を返す。60秒の古さを許容し、現在はALB背後のAPIとRDSに毎回到達している。
- /session：ログイン中ユーザーごとの一時状態を保持する。複数AZのEC2間で共有する必要があり、リージョン内で数ミリ秒のアクセスを求める。DBにも最終状態が保存されるため、キャッシュフェイルオーバー時のごく短い差分は許容する。

世界規模のレイテンシーとオリジン負荷を下げながら、セッションを誤って利用者間で共有せず、単一キャッシュノード障害も避ける構成はどれか。

選択肢

A	CloudFrontで /catalog と /session の両方を同じキャッシュビヘイビアにし、CookieとAuthorizationヘッダーをキャッシュキーから除外する
B	リージョン内の単一ElastiCacheノードへカタログとセッションをすべて保存し、CloudFrontは使わない
C	/catalog には言語・必要なクエリ文字列だけをキャッシュキーに含めるCloudFrontビヘイビアを設定する。/session はキャッシュ対象外とし、アプリケーションからMulti-AZと自動フェイルオーバーを有効にしたElastiCache for Valkey/Redis OSSレプリケーショングループへ保存する
D	/catalog はDAXへ、/session はCloudFrontへ保存し、どちらもTTLを60秒に統一する

ここでいったん止める | 解答と解説は次ページ

問題 072 正解・解説 本番相当

問題 72の正解・解説

1. 正解

C

2. 問題文の重要な条件

- カタログは利用者間で共有可能かつ世界配信、60秒の古さを許容。
- セッションは利用者固有で、EC2間共有とリージョン内低遅延が必要。
- セッションキャッシュはノード/AZ障害時に自動復旧したい。

3. 正解へ至る判断過程

キャッシュするデータの共有範囲が異なる。公開カタログはCloudFrontのエッジキャッシュでオリジン到達を減らす。ユーザー固有セッションを同じキーでエッジ共有すると情報漏えいになるため、CloudFrontではキャッシュせず、アプリケーションがリージョン内の共有インメモリストアへ保存する。ElastiCacheではレプリカを別AZに置き自動フェイルオーバーを有効にする。

4. 正解が要件を満たす理由

CloudFrontはキャッシュキーに必要なヘッダー、Cookie、クエリ文字列だけを含められ、世界のエッジから同一カタログを返してAPI/RDS負荷を減らす。ElastiCacheのValkey/Redis OSSレプリケーショングループは、プライマリ障害時に別AZのレプリカを自動昇格でき、EC2ローカルメモリより可用で共有可能なセッションキャッシュとなる。

5. 各不正解選択肢が不適切な理由

- A：ユーザー固有情報を区別する要素をキーから外してキャッシュすると、他利用者のセッション応答を返す重大な危険がある。
- B：世界のエッジ配信を得られず、単一ノードが障害点になる。カタログ要求もすべてリージョンへ到達する。
- D：DAXはDynamoDB用キャッシュで、RDS背後の任意API応答を直接キャッシュするものではない。CloudFrontでセッションを一律キャッシュする設計も不適切。

6. 各不正解選択肢が正解になり得る条件

- A：両パスが完全に公開情報で、利用者固有要素が応答に一切影響しない場合。
- B：利用者が単一リージョン内だけで、短時間停止を許容する開発環境。
- D：カタログのソースがDynamoDBで、低レイテンシーの読み取りキャッシュとしてDAXを必要とし、セッションは別途正しく非キャッシュ化する場合。

7. 今後使える判断基準

キャッシュ選定では「どこで共有するデータか」を見る。全世界で共有できるHTTP応答はCloudFront、アプリケーション内部で共有するホットデータはElastiCache、DynamoDBの読み取りAPIを高速化するならDAXである。ユーザー固有応答はキャッシュキーを正しく分離するか、エッジキャッシュしない。

8. 関連サービスとの比較

CloudFrontはHTTPレイヤーのグローバルCDN、ElastiCacheはリージョン内のマネージドインメモリデータストアである。ElastiCache Multi-AZのレプリカ更新は非同期のため、絶対に失えないセッションの唯一の永続先にはせず、必要ならDBを正とする。CloudFrontの stale-if-error を使えば、許容された範囲でオリジン障害中も古い公開カタログを返せる。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4

問題 073 | Domain 3 / 展開・自動化 | 複合難問 | 四択（1つ選択）

問題 73 変更可能な時間、手順、失敗停止を一つにする

ある医療システムは、タグ Application=claims が付いた24台のEC2インスタンスで稼働している。各アベイラビリティーゾーンに8台ずつあり、ALBがトラフィックを分散する。四半期ごとのミドルウェア更新では、各対象について次の処理を順番に行う必要がある。

1. ALBターゲットの正常台数と空きディスクを事前確認する。
2. EBSスナップショットを作成する。
3. 対象をALBからドレインし、サービス停止、更新、再起動、ヘルス確認を行う。
4. 失敗した対象はスナップショット情報を残してロールバック手順へ分岐する。
5. 正常性を確認した対象だけをALBへ戻す。

変更は、承認済みの土曜01:00〜04:00にだけ開始できる。大規模イベントの日は同じ土曜日でも変更禁止にしたい。一度に更新できるのは全体で1台までで、2台を超えて失敗したら未着手ノードへの配布を止める。実行担当者へEC2、ELB、EBSの広い直接権限を与えず、実行履歴を残したい。

最も適切な設計はどれか。

選択肢

A EventBridge Schedulerから毎週土曜01:00にRun Commandを全24台へ同時送信する。シェルスクリプト内でAWS CLIを呼び出し、各インスタンスプロファイルにELBとEBSの管理権限を付与する

B State Manager associationを30分ごとに実行し、ミドルウェアのバージョンが異なるノードを見つけるたびに即時更新する。イベント日はassociationを担当者が削除する

C ALBのターゲットグループを2つ作り、Route 53の加重ルーティングだけで1台ずつ更新する。スナップショット、事前条件、失敗数の判定は手順書に従って担当者が実行する

D 事前確認、スナップショット、ドレイン、Run Command、検証、分岐・ロールバックを記述したSystems Manager Automation runbookを作成し、最小権限のAutomation Assume Roleを指定する。最小権限のMaintenance Windowサービスロールでタグ対象のAutomationタスクとして登録し、同時実行数1、エラーしきい値2を設定する。AutomationをDEFAULT_CLOSEDのChange Calendarと統合し、承認済み期間だけOPENにする

ここでいったん止める | 解答と解説は次ページ

問題 073 正解・解説 複合難問

問題 73の正解・解説

1. 正解

D

2. 問題文の重要な条件

- EC2内部のコマンドだけでなく、ALB、EBS、事前条件、分岐、ロールバックを含む複数手順である。
- 定例時間枠に加え、個別の変更禁止日を強制したい。
- 可用性のため同時実行を制限し、一定数の失敗で未着手対象への実行を止める。
- 人には広い直接権限を与えず、ワークフロー用ロールへ権限を集約する。

3. 正解へ至る判断過程

まず、単一コマンドか複数サービスをまたぐワークフローかを見る。本問はAWS API操作、ノード内処理、条件分岐、ロールバックがあるためAutomation runbookが適する。次に「いつ実行するか」はMaintenance Window、「例外日を含めて実行を許可するか」はChange Calendar、「何台ずつ進め、いつ止めるか」はレート制御に分離する。

4. 正解が要件を満たす理由

Automation runbookは、AWS APIの呼び出し、別のrunbookやRun Commandの実行、出力の受け渡し、条件分岐、失敗処理を順序立てて定義できる。AutomationをMaintenance Windowの登録タスクにすれば、タグ対象へ予定時間内に実行し、maxConcurrency=1 で一度に1台へ制限できる。maxErrors=2 なら、3件目のエラーを受けた時点で未着手対象への実行を止める。既に処理中の対象まで即時中断されるわけではない点には注意する。

Automation Assume Roleにスナップショット作成やターゲット登録解除などの必要最小限を許可し、Maintenance Windowサービスロールにはタスク開始に必要な権限だけを与える。実行者には承認されたrunbookや保守設定を扱う限定権限だけを与えれば、日常の広い直接権限を減らせる。Change Calendarとの統合を有効にし、DEFAULT_CLOSEDのカレンダーを承認済み時間だけOPENにすれば、通常の定例スケジュールに加えてイベント日の禁止も強制できる。

5. 各不正解選択肢が不適切な理由

- A：全台同時実行は可用性要件に反する。各インスタンスプロファイルへELB・EBSの広い権限を付けると、侵害時の権限範囲も拡大する。Schedulerだけでは例外日、分岐、失敗停止を一体管理しにくい。
- B：State Managerは継続的な望ましい状態には向くが、明示的な承認時間だけに行う破壊的な多段変更を30分ごとに試行する設計は不適切である。手動削除は監査性と確実性が低い。
- C：トラフィック分離の一部には使えるが、スナップショット、事前条件、分岐、失敗数の制御を自動化しない。Route 53のDNS切り替えはALB配下の1台単位更新を直接制御する手段でもない。

6. 各不正解選択肢が正解になり得る条件

- A：停止を許容できる小規模な単発処理で、全対象へ同時に同じコマンドを送るだけの場合。権限は別途最小化する必要がある。
- B：非破壊的で冪等な設定を常時維持し、ずれを見つけたら時間帯に関係なく戻してよい場合。
- C：アプリケーション全体を独立したblue/green環境として用意し、DNSレベルの段階切り替えだけが必要な場合。更新内部の制御は別のデプロイ基盤が担う。

7. 今後使える判断基準

Systems Managerの設計では、Automationを「何をどの順に」、Maintenance Windowsを「いつ・どの対象へ」、Change Calendarを「今は実行を許すか」、レート制御を「何台ずつ・何件失敗で止めるか」と分解する。権限は人やノードへ広く配るのではなく、runbookの役割に合わせたAssume Roleへ絞る。

8. 関連サービスとの比較

Run Commandはノード上の一回限りのコマンド、AutomationはAWSリソース操作を含む多段ワークフロー、State Managerは望ましい状態の継続維持である。Maintenance Windowsは時間枠と対象・タスクを管理するが、手順そのものはrunbookやCommandドキュメントが定義する。EventBridge Schedulerも時刻起動はできるが、Maintenance Windowのターゲット、優先順位、レート制御と一体になった保守作業管理とは役割が異なる。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4 / AWS公式 5

問題 074 | Domain 5 / ネットワーク | 複合難問 | 複数選択（5つから2つ選択）

問題 74 ALBの502を層ごとに判別する

ALB配下のECSサービスで、デプロイ後からHTTP 502が増えた。クライアント側ログだけでは、ALB自身が接続を確立できず生成した502なのか、コンテナが502を返したのか判別できない。再現頻度が低いため、個別タスクへ手動ログインせず、発生時刻・リクエスト単位とメトリクス単位の両方で原因層を絞りたい。

有効な調査を2つ選べ。

選択肢

A	ALBアクセスログのelb_status_code、target_status_code、エラー関連フィールドと処理時間を確認する。
B	Route 53 query loggingだけを有効にし、502を返したDNSサーバーを特定する。
C	CloudTrailでInvokeデータイベントを有効にし、各HTTPレスポンス本文を収集する。
D	CloudWatchのHTTPCode_ELB_5XX_CountとHTTPCode_Target_5XX_Count、ターゲット正常性関連メトリクスを比較する。
E	S3サーバーアクセスログでECSタスクへのTCPリセットを確認する。

ここでいったん止める | 解答と解説は次ページ

問題 074 正解・解説 複合難問

問題 74の正解・解説

1. 正解

A、D

2. 問題文の重要な条件

ALB生成かターゲット生成かを区別し、低頻度の事象をリクエスト単位と集計メトリクス単位の双方で調査したい。

3. 正解へ至る判断過程

ALBアクセスログは個々の要求についてロードバランサーとターゲットのステータスを記録する。CloudWatchではELB側5xxとターゲット側5xxが別メトリクスなので、傾向と発生層を比較できる。両者を時刻で突き合わせるのが最短である。

4. 正解が要件を満たす理由

Aは個別リクエストの証拠、Dはサービス全体の時系列傾向を提供する。タスクへの対話ログインなしに、接続失敗、ターゲット応答、unhealthy増加など次の調査先を決められる。

5. 各不正解選択肢が不適切な理由

A: 正解肢のため対象外。
B: DNSログは名前解決を記録し、HTTPステータスコードを返した層を示さない。
C: CloudTrailは通常のALB HTTP要求本文を収集するアクセスログではない。
D: 正解肢のため対象外。
E: S3アクセスログはS3への要求を記録し、ECSタスクのTCP接続を監視しない。

6. 各不正解選択肢が正解になり得る条件

Bは誤ったDNS応答やResolver経路を調べる場合、CはAWS APIを誰が呼んだか監査する場合、EはS3オブジェクトアクセスとレスポンスを調べる場合に適する。

7. 今後使える判断基準

ロードバランサー障害は「ELBが生成したコード」と「targetが返したコード」を分離する。個別要求はaccess log、集計・アラームはCloudWatch、設定変更者はCloudTrailで見る。

8. 関連サービスとの比較

ALB access logsはS3へ配送される詳細記録、CloudWatch metricsは近リアルタイムの集計値、ECS/アプリケーションログは処理内部を示す。三層を同じ時刻・trace ID等で関連付けると原因範囲を狭めやすい。

公式確認先 AWS公式 1 / AWS公式 2

問題 075 | Domain 4 / セキュリティ | 複合難問 | 複数選択（5つから2つ選択）

問題 75 全アカウントの操作証跡を改ざんから守る

Organizations配下で新規アカウントが毎月増える。監査部門は、全アカウント・全リージョンのmanagement eventsを中央ログアーカイブへ自動収集し、メンバーアカウント管理者にtrailの停止やログ削除をさせたくない。ログファイルが後から変更・削除されていないことを検証でき、7年間の保持期間中はWORM要件を満たす必要がある。監査アカウント以外からの読み取りも禁止する。

中核となる対策を2つ選べ。

選択肢

A	各アカウントで単一リージョンtrailを手作業作成し、ローカルS3へ保存する。
B	Organizationsのorganization trailを全リージョンで作成し、ログアーカイブアカウントの専用S3バケットへ配信してlog file validationを有効にする。
C	CloudWatch MetricsのCallCountだけを7年間保持する。
D	メンバーアカウントrootへ中央バケットのs3:DeleteObjectVersionを許可する。
E	中央S3バケットでVersioningとS3 Object Lock Compliance modeを適切なretentionで構成し、bucket policy/SCPで書込み経路と監査読み取りを限定する。

ここでいったん止める | 解答と解説は次ページ

問題 075 正解・解説 複合難問

問題 75の正解・解説

1. 正解

B、E

2. 問題文の重要な条件

新規アカウント自動包含、全リージョンmanagement events、中央化、停止・削除耐性、完全性検証、7年WORM、読み取り分離が必要である。

3. 正解へ至る判断過程

Organization trailは組織内アカウントを一元的に対象化し、multi-Region trailで全リージョンを収集できる。Log file validationはdigestで変更・欠落の検証を支援する。保存先S3のObject Lock Compliance modeが期限前削除・上書きを防ぐ。

4. 正解が要件を満たす理由

Bが収集範囲と完全性検証、Eが保存後のWORMとアクセス分離を担う。メンバーアカウントごとの手作業なしに、新規加入もorganization trailへ含められる。

5. 各不正解選択肢が不適切な理由

A: 手作業・単一リージョン・ローカル管理で抜けと改ざん余地が大きい。
B: 正解肢のため対象外。
C: 集計値は個々のAPI主体・時刻・パラメーターを保持せず監査証跡にならない。
D: 削除権限を広げ、WORMと職務分離を破る。
E: 正解肢のため対象外。

6. 各不正解選択肢が正解になり得る条件

AはOrganizationsを使わない単一アカウント・単一リージョンの小規模監査なら最低限の案になる。CはAPI量の異常検知やダッシュボードには有効。Dは非保持データの正式な削除ワークフローで限定ロールへ許可する場合に限る。

7. 今後使える判断基準

CloudTrail保護は「収集漏れ防止」「ファイル完全性検証」「保存先の不変性」「管理境界分離」の四層で考える。Log file validationだけでは削除を防止しない。

8. 関連サービスとの比較

CloudTrail Lakeはイベント分析・保持をマネージド化する選択肢だが、S3 Object Lockを指定したWORMアーカイブ要件ではtrail + locked bucketが明確である。AWS Configはリソース構成履歴で、API監査の代替ではない。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3

問題 076 | Domain 1 / 監視・性能 | 本番より難しい | 四択（1つ選択）

問題 76 カスタムメトリクスの次元爆発

Auto Scalingグループで数百台のEC2インスタンスを起動する分析基盤がある。CloudWatch agentは各インスタンスから mem_used_percent、disk_used_percent、アプリケーションのキュー長を送信している。設定変更後、InstanceId、ImageId、InstanceType、AutoScalingGroupName の組み合わせごとに元メトリクスが発行され、さらにグループ集約メトリクスも発行されるようになり、カスタムメトリクス費用が急増した。運用チームがアラームに必要なのはAuto Scalingグループ単位のメモリとキュー長である。ただし、ルートボリュームの使用率だけは障害調査のためインスタンス単位で残したい。

要件を満たしながらメトリクス数を最も適切に削減する設定はどれか。

選択肢

A aggregation_dimensions に AutoScalingGroupName の集約を定義し、メモリとキュー長について drop_original_metrics を指定する。disk_used_percent は元メトリクスを残し、必要なデバイス・マウントポイントに限定する

B すべてのメトリクスから全ディメンションを削除し、アカウント・リージョン全体で一系列へ集約する。元メトリクスは保持する

C append_dimensions に InstanceId、ImageId、InstanceType を追加し、収集間隔を10秒へ短縮することで集約精度を上げる

D CloudWatch agentを停止し、EC2標準メトリクスの MemoryUtilization と DiskSpaceUtilization に置き換える

ここでいったん止める | 解答と解説は次ページ

問題 076 正解・解説 本番より難しい

問題 76の正解・解説

1. 正解

A

2. 問題文の重要な条件

- 費用増の主因は値の頻度だけでなく、ディメンション組み合わせごとの別メトリクス系列である。
- メモリとキュー長はASG単位だけが必要で、インスタンス別系列は不要である。
- ディスク使用率だけはインスタンス別の診断能力を残す。
- すべてを一系列に潰すのではなく、指標ごとに保持粒度を変える必要がある。

3. 正解へ至る判断過程

aggregation_dimensions でASG単位のロールアップを作っても、既定では元のディメンション別メトリクスも送られるため、それだけでは系列数を十分に減らせない。不要なメモリとキュー長の元系列を drop_original_metrics で止める。一方、ディスクは元系列を残し、収集対象ファイルシステムやマウントポイントを限定して診断性と費用を両立させる。

4. 正解が要件を満たす理由

Aは、アラームに使うASG集約系列を維持しながら、同じ値のInstanceId等による多数の元系列を送信しない。
drop_original_metrics は集約を有効にした場合に、特定の元メトリクスをCloudWatchへ発行しないための設定である。ディスクのみ個体識別を残すので、容量逼迫したインスタンスを特定できる。

5. 各不正解選択肢が不適切な理由

A: 正解肢のため対象外。
B: アカウント全体への集約では問題のASGを識別できず、元系列を保持するため費用削減も限定的である。
C: ディメンションを増やすと系列数が増え、10秒収集は高解像度メトリクスの発行量と費用も増やす。集約精度の改善にはならない。
D: EC2標準メトリクスにはゲストOSのメモリ使用率やファイルシステム使用率は含まれないため、要件を満たせない。

6. 各不正解選択肢が正解になり得る条件

B: 単一ワークロードしかなく、アカウント全体の合計だけで容量制御でき、個別診断が不要なら全体集約を選べる。
C: 短時間の個体別スパイクを追跡する明確な要件があり、追加費用を受け入れる場合は詳細ディメンションと短周期が有効である。
D: CPU、ネットワーク、EBS I/OなどEC2が標準で発行するホスト側メトリクスだけで要件を満たす場合、agentを使わない選択が最も低運用である。

7. 今後使える判断基準

CloudWatchカスタムメトリクスの設計では、メトリクス名だけでなくディメンションの一意な組み合わせを数える。集約を追加しただけでは元系列が自動的に消えない。運用判断に必要な最小粒度を指標ごとに決め、不要な元系列だけを落とす。

8. 関連サービスとの比較

append_dimensions は識別軸を追加し、aggregation_dimensions は指定軸で集約系列を作る。drop_original_metrics は集約後に不要な元系列の発行を抑える。Metrics Insightsは既に保存された多数系列をクエリで集約するため、保存系列そのものの費用削減とは異なる。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3

問題 077 | Domain 2 / 信頼性・BC | 複合難問 | 複数選択（5つから2つ選択）

問題 77 バックアップ管理者まで想定した7年保管

AWS Organizations配下に80のメンバーアカウントがあり、各アカウントのEBS、RDS、Amazon FSxを毎日バックアップする。RPOは24時間、保管期間は7年である。ランサムウェア対策として、ワークロードアカウントの管理者認証情報が侵害されてもバックアップを削除できないようにしたい。さらに、プライマリリージョンの広域障害にも備え、別リージョンかつ専用バックアップアカウントに復旧ポイントを保持する。

バックアップポリシーは組織全体で一元配布し、導入後72時間は保管値の誤設定を修正できるが、それ以降はバックアップ管理者やルートユーザーを含めて保持設定の短縮・Vault削除をできないようにする。要件を満たす対策を2つ選べ。

選択肢

A	AWS Backupのクロスアカウント管理とOrganizationsのバックアップポリシーを用い、各対象を毎日バックアップして、専用バックアップアカウントの別リージョンのVaultへコピーする
B	各ワークロードアカウントでAWS Backupの連続バックアップだけを有効にし、35日のPITR復旧ポイントを7年間保持する
C	各ワークロードアカウントのルートユーザーだけにVault削除を許可し、ルート認証情報を運用チームの共有金庫へ保存する
D	コピー先Vaultに、72時間の変更可能猶予期間を設定したAWS Backup Vault LockのCompliance modeと、7年の最小/最大保持要件に整合する設定を適用する
E	EBS、RDS、FSxのデータをすべてS3へ定期エクスポートし、S3 Cross-Region Replicationだけで一元保護する

ここでいったん止める

解答と解説は次ページ

問題 077 正解・解説 複合難問

問題 77の正解・解説

1. 正解

A、D

2. 問題文の重要な条件

- 80アカウントへ一元的なバックアップルールを配布する。
- 日次RPO、7年保持。
- 別アカウント・別リージョンへ隔離する。
- 72時間後はルートを含めて改変不能なWORM保護が必要。

3. 正解へ至る判断過程

まず障害ドメインと権限境界を分けるため、AWS Backupで組織的にバックアップを配布し、別アカウント・別リージョンへコピーする。次に、そのコピー先をCompliance modeのVault Lockで保護する。Compliance modeは猶予期間中だけ設定を修正でき、猶予終了後は保持を短縮したりVault Lockを解除したりできない。

4. 正解が要件を満たす理由

- A：AWS BackupのOrganizations連携により、タグやリソース種別に基づくバックアップポリシーを複数アカウントへ配布できる。クロスアカウント・クロスリージョンコピーは、資格情報侵害とリージョン障害の双方から復旧ポイントを分離する。
- D：Vault Lock Compliance modeは猶予期間終了後、アカウント所有者やルートを含めてロック設定を変更・削除できない。保持期間の強制により、ランサムウェアによる早期削除を防ぐ。

5. 各不正解選択肢が不適切な理由

- B：AWS Backupの連続バックアップの最大保持は35日であり、7年保持を連続PITRだけで満たせない。コピー時に連続復旧ポイントが定期スナップショットになる場合もあり、コピー先でPITRが維持されるとは限らない。
- C：ルートユーザーも侵害対象になり得るうえ、Compliance modeのような技術的な削除不能性を提供しない。共有認証情報は統制も悪化させる。
- E：サービスごとの整合性ある復旧、RDS/PITR、FSxファイルシステム復元をS3 CRRだけで一律に置き換えられない。

6. 各不正解選択肢が正解になり得る条件

- B：35日以内の細かな時点復旧を主目的とし、長期保存は別の定期バックアップで補う場合。
- C：正解になる条件はほぼない。緊急用ルート認証情報を厳格保管することは必要だが、不変バックアップの代替にはならない。
- E：元データがS3オブジェクトで、オブジェクト単位の別リージョン複製だけが要件の場合。

7. 今後使える判断基準

バックアップの耐攻撃性は、(1)本番とは別アカウント、(2)別リージョン、(3)保持を短縮できないWORM、(4)組織ポリシーによる自動適用、の層で考える。PITRの短期復旧と、年単位の定期スナップショット保持を同一機能だと思わない。

8. 関連サービスとの比較

Vaultアクセスポリシーは誰がVaultへ操作できるかを制御するが、許可主体やルートを含む絶対的な保持強制とは異なる。Vault Lock Governance modeは適切な権限で回避できるが、Compliance modeは猶予終了後に解除できない。論理エアギャップVaultはCompliance modeのVault Lockを備え、AWS RAMで復旧利用を共有できる別の隔離選択肢である。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4 / AWS公式 5

問題 078 | Domain 3 / 展開・自動化 | 複合難問 | 複数選択（5つから2つ選択）

問題 78 対話調査と一括操作を同じ道具に押し込まない

金融会社は、インターネット経路もパブリックIPも持たないプライベートサブネット内で、400台のEC2インスタンスを運用している。SSM Agentと必要なインスタンスプロファイルは導入済みである。セキュリティ部門は、管理用のインバウンドポート、踏み台、共有SSHキーを禁止している。

運用要件は二つある。

- オンコール担当者は、障害時に許可されたタグのインスタンスだけへ対話的に接続したい。誰がいつ接続したかに加え、通常のシェルセッションでは入力コマンドと出力も暗号化して保存したい。
- 定型修復は Environment=production の対象へ一括実行する。ただし同時実行は10%とし、3件目のエラーを受けた時点で未着手対象への配布を止め、標準出力・標準エラーを後から検索できるようにする。パスワードをAPIパラメータへ平文で含めてはならない。

要件を満たすために選ぶべき対策はどれか。**2つ選択せよ。**

選択肢

A Session Managerを使用し、Systems Managerの必要なインターフェイスVPCエンドポイントへのHTTPS経路を構成する。IAM条件で許可タグとSessionドキュメントを制限し、Session Managerの設定でKMS暗号化とS3またはCloudWatch Logsへの通常シェルセッションログを有効にし、CloudTrailでセッションAPIを監査する

B 各サブネットにSSH踏み台を置き、Session Managerのポートフォワーディングで踏み台の22番ポートへ接続する。ポートフォワーディング内のSSHコマンドと出力はSession Managerがすべて記録するため、OS側の監査設定は不要とする

C 定型修復もSession Managerの対話シェルで担当者が1台ずつ実行し、400台の完了状況と失敗件数をスプレッドシートで記録する

D Run Commandで承認済みSSMドキュメントをタグ対象へ送信し、max-concurrency=10% と max-errors=2 を設定する。出力をCloudWatch LogsまたはS3へ保存し、秘密値は平文のコマンド引数にせず、ノードロールで許可したParameter Storeの SecureString などから実行時に取得する

E EC2 Instance Connect Endpointを作成して全担当者にOS管理者権限を与え、同じSSHコマンドを並列実行する。CloudTrailに接続APIが残るため、シェル内の全コマンドと出力も自動的に保存されるとみなす

ここでいったん止める | 解答と解説は次ページ

問題 078 正解・解説 複合難問

問題 78の正解・解説

1. 正解

A、D

2. 問題文の重要な条件

- インバウンド管理ポート、踏み台、共有鍵を使えず、ノードからAWSサービスへのプライベート接続が必要である。
- 人による対話調査と、400台への非対話一括処理は別の操作特性を持つ。
- 接続APIだけでなく、通常シェルのコマンド・出力と、一括処理の標準出力・標準エラーを保存したい。
- 一括処理ではタグ対象、同時実行率、失敗停止、秘密値保護が必要である。

3. 正解へ至る判断過程

対話が必要な作業にはSession Manager、一回の定型コマンドを多数ノードへ配る作業にはRun Commandを選ぶ。次に、それぞれの監査範囲を確認する。CloudTrailはStartSessionやSendCommandなどのAPIを記録するが、シェル内の全入出力の代わりではないため、Session Managerのログ設定とRun Commandの出力先を別途構成する。最後に、プライベートノードの到達性と、秘密値をコマンド履歴へ露出させない方法を確認する。

4. 正解が要件を満たす理由

Aは、ノードからSystems Managerの必要なリージョンエンドポイントへHTTPSで到達させ、ユーザー側からインバウンド接続せずに対話セッションを確立する。IAMのリソースタグ条件と許可するSessionドキュメントで接続範囲を絞れる。CloudTrailは開始・終了などのAPI監査に、S3またはCloudWatch Logsは通常シェルの入出力保存に使い、KMSでセッションデータや保存先を保護できる。

Dは、タグで対象を動的に選び、Run Commandのレート制御で同時実行とエラーしきい値を設定できる。CloudWatch Logsなら出力をほぼリアルタイムに検索でき、S3ならコンソールの表示上限を超える出力も保管できる。秘密を平文のSendCommand パラメータに入れるとCloudTrailなどから見える可能性があるため、SecureString 等を最小権限で実行時取得する設計が必要である。

5. 各不正解選択肢が不適切な理由

- B：踏み台とSSHは明示的な禁止条件に反する。さらに、Session Managerのポートフォワーディングおよびセッションでは、Session Managerによるコマンド・出力ログは利用できない。
- C：対話シェルは障害調査には適するが、400台の同時実行率、エラーしきい値、機械的な完了追跡を提供しない。手作業の転記も監査品質を下げる。
- E：Instance Connect EndpointはSSH到達性の選択肢にはなるが、OS管理者権限を全員へ付与するのは最小権限に反する。CloudTrailの接続API記録だけでSSH内のコマンドと出力が自動保存されるわけではない。

6. 各不正解選択肢が正解になり得る条件

- B：既存SSHクライアントやSSH固有機能が必須で、踏み台またはトンネルが許可され、OS側の監査ログでセッション内容を別途取得する場合。
- C：対象が1台で、探索的な診断のため次のコマンドを前の結果に応じて人が決める場合。
- E：組織標準がSSHで、EC2 Instance Connect Endpointのアクセス制御とOS監査を適切に実装し、Session Managerを利用できない場合。

7. 今後使える判断基準

「人が結果を見ながら次を決める」ならSession Manager、「同じ承認済み操作を多数へ配る」ならRun Commandを優先する。監査では、API監査、セッション内容、コマンド出力を別物として確認する。また、Session Manager経由でもSSH・ポートフォワーディングの中身は標準のセッションログ対象外である。

8. 関連サービスとの比較

Session Managerは対話アクセス、Run Commandは非対話の一括コマンド、State Managerは定期的な状態維持、Automationは複数手順とAWS APIを含むワークフローである。EC2 Instance Connect EndpointはプライベートIPへのSSH/RDP到達性を提供できるが、Session Managerと同じログ・ドキュメント・Run Command機能を持つわけではない。Secrets Managerも秘密値取得に使えるが、ローテーションやデータベース資格情報管理が不要な単純設定値ならParameter StoreのSecureStringが軽量である。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4 / AWS公式 5

問題 079 | Domain 5 / ネットワーク | 複合難問 | 複数選択（5つから3つ選択）

問題 79 NATなしでECRイメージを取得する

Fargateタスクをインターネット経路のないプライベートサブネットで起動する。コンテナイメージは同じリージョンのプライベートECRにあり、タスク実行ロールの権限は正しい。会社はNATゲートウェイを追加せず、イメージ取得に必要な通信をAWSネットワーク内に限定したい。ECR APIへの問い合わせ、Docker Registry操作、イメージレイヤーの取得をすべて成立させる必要がある。

作成すべきVPCエンドポイントを3つ選べ。

選択肢

A	com.amazonaws.<region>.ecr.apiのインターフェイスVPCエンドポイント
B	com.amazonaws.<region>.ecr.dkrのインターフェイスVPCエンドポイント
C	Amazon S3のゲートウェイVPCエンドポイント
D	Amazon ECSのゲートウェイVPCエンドポイント
E	Amazon CloudFrontのインターフェイスVPCエンドポイント

ここでいったん止める | 解答と解説は次ページ

問題 079 正解・解説 複合難問

問題 79の正解・解説

1. 正解

A、B、C

2. 問題文の重要な条件

Fargate、プライベートECR、NATなし、ECR API・Registry・レイヤー取得のすべてが必要である。同一リージョンを前提としている。

3. 正解へ至る判断過程

ECRのコントロール/API操作にはecr.api、イメージのDocker Registry操作にはecr.dkrのinterface endpointを使う。ECRのイメージレイヤーはS3に保存されるため、S3 gateway endpointも必要になる。

4. 正解が要件を満たす理由

3つを組み合わせることで、イメージmanifestの取得からレイヤーダウンロードまでNATなしで完結する。Private DNS、endpoint SG、S3 endpointのroute table関連付けも正しく構成する。

5. 各不正解選択肢が不適切な理由

A: 正解肢のため対象外。
B: 正解肢のため対象外。
C: 正解肢のため対象外。
D: ECSにゲートウェイ型endpointはなく、FargateタスクがECRからpullする要件の3経路を代替しない。
E: CloudFront endpointはECRレイヤー取得経路ではない。

6. 各不正解選択肢が正解になり得る条件

Dに近いECS interface endpointsは、EC2起動タイプのECS agent通信など別のプライベート接続要件で検討する。Eはこの用途で正解にならない。さらにログをCloudWatch Logsへ送る、Secrets Managerから秘密を読む場合は、それぞれ追加のinterface endpointが必要になる。

7. 今後使える判断基準

プライベートECR pullは「API」「DKR」「レイヤーのS3」の三経路に分解する。IAMが正しくても、ネットワーク経路のどれか一つが欠ければ起動に失敗する。

8. 関連サービスとの比較

Interface endpointはENIとSGを使い時間・処理料金が発生する。S3 gateway endpointはroute tableへ関連付け、VPC内からのS3アクセスに追加料金がない。NATは外部も含む汎用送信経路だが、固定料金とデータ処理料金がある。

公式確認先 AWS公式 1 / AWS公式 2

問題 080 | Domain 4 / セキュリティ | 複合難問 | 四択（1つ選択）

問題 80 開発工程のレビューとペネトレーションテスト

アプリケーションセキュリティ部門は、組織独自のセキュリティ要件に照らして設計文書とGitHub pull requestをレビューし、公開前のWeb APIへオンデマンドのペネトレーションテストを行いたい。検証済みFindingには再現可能な攻撃経路と修正案が必要で、承認後はプライベートリポジトリへ修正pull requestを生成したい。稼働中EC2のCVE一覧やAWS APIの異常検出だけでは要件を満たさない。

現行のSOA-C03 v1.1でこの用途に最も合うサービスはどれか。

選択肢

A	Amazon Inspectorだけを有効にし、設計文書をEC2のタグとして保存する。
B	Amazon GuardDutyのFinding suppression ruleでpull requestを生成する。
C	AWS Config custom ruleでWeb APIへ侵入テストを実行する。
D	AWS Security AgentでAgent Space、組織要件、GitHub連携、code/design reviewおよびpenetration testを構成し、生成修正はレビュー後に取り込む。

ここでいったん止める | 解答と解説は次ページ

問題 080 正解・解説 複合難問

問題 80の正解・解説

1. 正解

D

2. 問題文の重要な条件

設計・コード・実アプリの三段階、組織固有要件、オンデマンド侵入テスト、検証済みFinding、GitHub修正PRという開発ライフサイクル要件である。

3. 正解へ至る判断過程

AWS Security Agentはdesign security review、code security review、on-demand penetration testingを提供し、Findingの修正コードを接続リポジトリへ提案できる。SOA-C03ガイドv1.1でin-scopeへ追加されたサービスでもある。

4. 正解が要件を満たす理由

中央のsecurity requirementsを各レビューへ適用し、アプリケーション文脈を使った検証と修正提案を一連で扱える。生成修正は自動的に本番へ反映せず、人のコードレビューとテストを挟める。

5. 各不正解選択肢が不適切な理由

A: Inspectorは主にworkloadの脆弱性管理で、設計文書レビューや文脈付き侵入テスト・修正PRを一括提供しない。
B: GuardDuty suppressionはFinding表示の制御で、コード修正生成ではない。
C: Config ruleは構成準拠評価であり、Webアプリへの多段侵入テスト用サービスではない。
D: 正解肢のため対象外。

6. 各不正解選択肢が正解になり得る条件

AIはEC2/ECR/LambdaのCVE継続評価、Bは既知の受容リスクや誤検出Findingを条件付きで抑制する場合、CはAWSリソース構成が独自要件へ適合するかを評価する場合に適する。

7. 今後使える判断基準

インフラ/パッケージCVEはInspector、クラウド内の脅威挙動はGuardDuty、構成準拠はConfig、設計・コード・アプリ侵入テストを開発工程へ組み込むならSecurity Agentと分ける。

8. 関連サービスとの比較

生成された修正はAI出力なので、Findingの検証スクリプト、非本番テスト、通常のレビュー/承認を省略しない。Security Agentはセキュリティ統制の責任を置き換えるのではなく、レビューと検証を拡張する。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3

問題 081 | Domain 1 / 監視・性能 | 本番相当 | 四択（1つ選択）

問題 81 増え続けるロググループの集中配送

AWS Organizations配下の80アカウントで、ECS、Lambda、EC2上のアプリケーションがCloudWatch Logsへログを出力している。デプロイごとに新しいロググループが作成されるため、個別設定では監査ログの配送漏れが発生している。セキュリティアカウントでは、エラーと認証イベントを数分以内にストリーム処理し、変換後の全ログをS3へ長期保存したい。送信元アカウントへ分析基盤を置かず、中央アカウントへのクロスアカウント配送を行う。配送基盤自身のログを再び同じ配送経路へ入れて再帰ループを起こしてはならず、新規ロググループへの追随作業も最小化する必要がある。

最も適切な構成はどれか。

選択肢

A 各ロググループの作成イベントをEventBridgeで検出し、Lambdaでロググループレベルのサブスクリプションフィルターを1件ずつ作成する。中央アカウントのLambdaを直接宛先に指定する

B 各送信元アカウントとリージョンにCloudWatch Logsのアカウントレベルサブスクリプションフィルターポリシーを設定し、配送基盤のロググループをselection criteriaで除外する。中央アカウントに論理的なCloudWatch Logs destinationと宛先ポリシーを作成し、Kinesis Data StreamsまたはData Firehoseを介して処理・S3保存する

C CloudWatch cross-account observabilityのOAMリンクで全ロググループを中央監視アカウントへ共有し、中央アカウントのLogs Insightsクエリを1分ごとに実行して、結果だけをS3へ書き出す

D Organizationsの全アカウントに対するCloudTrail organization trailを作成し、S3データイベントを含めて中央S3バケットへ配信する。これをアプリケーションログの代替とする

ここでいったん止める | 解答と解説は次ページ

問題 081 正解・解説 本番相当

問題 81の正解・解説

1. 正解

B

2. 問題文の重要な条件

- 新しいロググループが継続的に作られ、個別フィルターでは配送漏れがある。
- 数分以内のストリーム処理と、変換後ログのS3長期保存が必要である。
- 80アカウントから中央アカウントへ安全に配送する。
- 配送処理自身のログを再配送して再帰させてはならない。
- 送信元での継続的な設定作業を減らす。

3. 正解へ至る判断過程

要件は中央からログを閲覧することではなく、各ログイベントを中央ストリームへ継続配送することである。そのためCloudWatch Logs subscriptionsを選ぶ。新規ロググループへ自動的に適用するにはロググループ単位ではなくアカウントレベルのポリシーを使う。クロスアカウントでは受信側のdestinationとそのアクセスポリシーを用意し、KinesisまたはFirehoseへ接続する。selection criteriaで配送パイプライン自身などを除外し、ログ再帰を防ぐ。

4. 正解が要件を満たす理由

アカウントレベルサブスクリプションは、ポリシーに合うアカウント内のロググループへ一括適用されるため、デプロイ後の個別追随が不要になる。サブスクリプションはログ取り込み後まもなく宛先へ配信する。中央のKinesis Data Streamsなら複数コンシューマーによるリアルタイム処理、Data Firehoseなら変換・S3配送を管理サービスで構築できる。destination policyをOrganizationsの組織IDなどで制限し、送信ロールと混乱した代理対策も設定できる。

5. 各不正解選択肢が不適切な理由

A: 自動化しても、イベント処理失敗や競合による設定漏れ、Lambdaの保守が残る。クロスアカウントサブスクリプションでは、対応する論理destinationと権限設計を用いる構成の方が目的に合う。
B: 正解肢のため対象外。
C: OAMは中央での観測・クエリに有用だが、Logs Insightsの定期クエリ結果は全ログイベントの耐久性あるストリーム配送の代替にならない。1分ポーリングの重複・欠落管理も必要になる。
D: CloudTrailはAWS APIアクティビティの監査証跡であり、任意のアプリケーションログを収集しない。S3データイベントを増やしても用途は変わらない。

6. 各不正解選択肢が正解になり得る条件

A: 対象ロググループが少数で、ロググループごとに異なる宛先や最大2件の個別フィルターを使い分ける必要がある場合は有効である。
C: ログを複製せず、中央運用者が複数アカウントのログを対話的に検索・相関することだけが目的ならOAMが適する。
D: 収集対象がアプリケーションログではなく、Organizations全体のAWS API監査だけならorganization trailが適切である。

7. 今後使える判断基準

「中央で見えるようにする」と「中央へイベントを配送・保存する」を区別する。継続ストリームはsubscription、共有観測はOAM、AWS API監査はCloudTrailを選ぶ。動的に増えるロググループにはアカウントレベル適用を検討し、配送先自身のログ除外と宛先容量も必ず設計する。

8. 関連サービスとの比較

Kinesis Data Streamsは保持期間内の再読込や複数独立コンシューマーに向き、Data Firehoseはバッファリング、変換、S3やOpenSearch等への管理された配送に向く。Lambda宛先は軽量なイベント処理に向くが、急増時の同時実行・再試行を設計する。subscription filterはmetric filterと違い、一致したログを別サービスへ配送する。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4

問題 082 | Domain 2 / 信頼性・BC | 本番相当 | 四択（1つ選択）

問題 82 誤更新の1分前へ戻すが、現在も残す

Amazon RDS for MySQLで自動バックアップを7日間保持している。14:06に誤ったSQL更新が実行され、注文テーブルの一部が上書きされた。14:25に発見した時点でも、他の正常な注文は継続して書き込まれている。監査部門は、障害発生後の現在のDBを証跡として保持するよう求めている。運用チームは、誤更新直前の14:05の状態を得て影響行を検証し、必要なデータだけを戻した後に切り替えたい。

データ損失と監査上のリスクを最小化する手順はどれか。

選択肢

A 自動バックアップから14:05を指定して別のDBインスタンスへポイントインタイムリストアし、差分を検証・修復する。現在のDBは保持し、検証後に接続先を計画的に切り替える

B 当日00:00の手動スナップショットを現在のDBへ上書き復元し、14時間分の注文をアプリケーションログから再投入する

C 既存のリードレプリカを直ちに昇格すれば誤更新は複製されていないと仮定し、そのまま本番へ切り替える

D 現在のDBインスタンスを停止し、同じ識別子のまま14:05へ巻き戻す

ここでいったん止める | 解答と解説は次ページ

問題 082 正解・解説 本番相当

問題 82の正解・解説

1. 正解

A

2. 問題文の重要な条件

- 自動バックアップ保持期間内の特定時刻へ戻したい。
- 誤更新後も正常な書き込みが続いている。
- 現在のDBを監査証跡として残す。
- 直ちに全体を古い状態へ置換せず、影響行を検証したい。

3. 正解へ至る判断過程

RDSのPITRは既存DBをその場で巻き戻すのではなく、指定時点から新しいDBインスタンスを作成する。この特性を利用すれば、14:05の整合したコピーと現在のDBを並べ、誤更新後に入った正常データを失わずに差分修復方針を決められる。

4. 正解が要件を満たす理由

自動バックアップはトランザクションログとスナップショットを使い、保持期間内の復元可能時刻を指定して新規DBへ復元できる。現在のDBを変更しないため証跡を維持でき、復元DBで影響範囲を確認してから、行単位の戻しまたは本番接続の切替を選べる。

5. 各不正解選択肢が不適切な理由

- B：14時間分の正常データを失い、ログ再投入の漏れ・順序・重複リスクが大きい。
- C：リードレプリカは通常、誤ったSQL更新も非同期で複製する。未複製を確認せず昇格するのは危険で、昇格後は独立DBになる。
- D：RDS PITRは既存インスタンスのin-place巻き戻しではない。現在状態も失うため監査要件に反する。

6. 各不正解選択肢が正解になり得る条件

- B：PITRが無効で、古いスナップショットと完全な再実行可能ログしかなく、長いRTO/RPOを受容する場合。
- C：レプリケーションを誤更新前に意図的に停止しており、遅延と整合性を確認したDR用レプリカがある場合。
- D：利用サービスがin-placeリストアを明示的に提供し、現在状態の保持が不要な場合。RDS DBインスタンスのPITRには当てはまらない。

7. 今後使える判断基準

DB復旧では「元へ上書き」か「新規リソースへ復元」かを確認する。RDS/Aurora/DynamoDBのPITRは一般に新しいDB/テーブルを作るため、検証・差分移行・接続切替までが復旧手順である。RPOだけでなく、復元後のデータ統合時間もRTOへ含める。

8. 関連サービスとの比較

手動スナップショットは取得時点だけへ戻す。自動バックアップ/PITRは保持期間内の細かな時点を選べる。Multi-AZはインフラ障害時の可用性を高めるが、論理的な誤更新はスタンバイにも反映されるためPITRの代替ではない。リードレプリカも通常は誤更新を複製する。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3

問題 083 | Domain 3 / 展開・自動化 | 本番より難しい | 四択（1つ選択）

問題 83 イベントを再送できても、処理が一度だけになるとは限らない

あるメディア会社では、外部企業がバージョニング有効のS3バケットへ動画メタデータをアップロードする。同じオブジェクトキーは修正版で上書きされることがある。オブジェクト作成を契機に、検証Lambdaと検索インデックス更新Lambdaを独立して実行したい。1時間に数回、同じ通知が重複して届いたり、同じキーの古い更新イベントが新しい更新イベントより後に処理されたりして、検索インデックスが古い状態へ戻る障害が起きている。

新しい構成には次の要件がある。

- incoming/ プレフィックスのJSONだけを対象にし、検証とインデックス更新を疎結合に追加・変更できる。
- 一時的なターゲット障害は再試行し、配信不能イベントは調査用キューへ残す。
- Lambdaのバグを修正した後、指定時間帯の過去イベントを再処理できる。
- 重複配信と同一キー内の順序逆転が起きても、最終状態を古い版へ戻さない。
- 「S3通知またはEventBridgeが完全に一度だけ、発生順に配る」という前提を置かない。

最も適切な構成はどれか。

選択肢

A S3からEventBridgeへのイベント送信を有効にし、イベントパターンでバケット、Object Created、プレフィックス、拡張子を絞ったルールから各ターゲットへ配信する。ターゲットごとに再試行ポリシーとSQS DLQを設定し、イベントバスに対象イベントのアーカイブを作る。Lambdaはバケット・キー・version-id などを冪等キーにし、同一キーの sequencer を条件付き更新で比較して古いイベントの反映を拒否する

B S3 Event Notificationから2つのLambdaを直接指定し、Lambdaの予約済み同時実行数を1にする。これによりバケット全体のイベントが発生順に完全に一度だけ処理されるため、状態管理は不要とする

C CloudTrailデータイベントをCloudWatch Logsへ送り、メトリクスフィルターがPutObjectを検出したらSNSからLambdaを呼び出す。Lambdaが失敗した場合はCloudWatch Logsを手動で読み直して再実行する

D S3の同一通知設定で同じイベントタイプ・重複プレフィックスを持つ複数のLambda宛先を登録し、失敗時は各LambdaがS3オブジェクトを一覧走査する。上書きイベントの順序はイベント時刻だけで判定する

ここでいったん止める | 解答と解説は次ページ

問題 083 正解・解説 本番より難しい

問題 83の正解・解説

1. 正解

A

2. 問題文の重要な条件

- S3イベントは重複や順序逆転を前提に処理する必要がある。
- 同じキーが更新されるため、イベント全体の時刻ではなく、そのキーに対する新旧を判定する必要がある。
- 複数の処理先、再試行、DLQ、過去イベントの再処理が求められる。
- 対象のプレフィックス・拡張子をイベント側で絞り、処理追加時の結合を弱めたい。

3. 正解へ至る判断過程

まず、配信基盤の機能とコンシューマーの正しさを分ける。EventBridgeはルールで複数ターゲットへルーティングし、再試行、DLQ、アーカイブ、リプレイを提供できる。しかし、リプレイを含むイベント処理は重複し得るため、最終状態の一貫性はLambda側の冪等処理で担保する。version-id などで同じオブジェクト版の二重処理を識別し、同じS3キーについては sequencer の大小を用いて、古いイベントによる上書きを条件付き更新で拒否する。

4. 正解が要件を満たす理由

S3のEventBridge統合を有効にすると、S3イベントをEventBridgeルールのイベントパターンで選別し、検証とインデックス更新を別ルールまたは別ターゲットへ配信できる。各ターゲットには独立した再試行とDLQを設定でき、アーカイブから指定期間をソースイベントバスへリプレイできる。

ただし、アーカイブのリプレイも厳密な全順序を保証しない。Lambdaは、処理済みのイベント識別子に加え、同一バケット・キーについて最後に反映した sequencer をDynamoDBなどへ保存し、条件式で大きいものだけを反映する。version-id 自体を時系列の大小比較には使わない。sequencer も異なるキー間の順序比較には使えず、長さが異なる場合の比較方法に注意する。この責任分界が本問の中心である。

5. 各不正解選択肢が不適切な理由

- B：同時実行数を1にしても、配信の重複や到着順序を完全に一度だけ・発生順へ変えられない。全キーを直列化して性能も不必要に落とす。
- C：CloudTrailデータイベントは監査には有用だが、アプリケーション向けS3イベントルーティング、ターゲット別DLQ、アーカイブ・リプレイを直接満たさず、手動復旧の運用負荷が高い。
- D：重複するS3通知フィルター設定には制約があり、処理先の追加もバケット設定へ結合する。イベント時刻だけでは同一キーへの更新順序を安全に確定できず、全件一覧走査は遅延と費用を増やす。

6. 各不正解選択肢が正解になり得る条件

- B：低頻度で、順序や重複が結果に影響せず、単一Lambdaだけを最小構成で起動したい場合。ただし冪等性はなお推奨される。
- C：目的がオブジェクトデータ操作の監査・追跡であり、リアルタイム業務処理や自動リプレイを求めない場合。
- D：単一の直接宛先だけで十分で、単純なプレフィックス・サフィックスフィルターを使い、障害時の再走査を受容できる小規模処理の場合。

7. 今後使える判断基準

イベント駆動では、「届け直せること」と「二重に反映しないこと」を分ける。再試行、DLQ、アーカイブは配信・復旧機能であり、冪等キー、条件付き書き込み、同一エンティティの版比較はコンシューマーの責任である。順序用の値がある場合も、どの範囲で比較可能かを確認する。

8. 関連サービスとの比較

S3 Event NotificationsはSQS、SNS、Lambdaなどへ直接通知する単純な構成に向く。EventBridgeは内容ベースルーティング、複数ターゲット、SaaS連携、アーカイブ・リプレイを加えたい場合に向く。SQS FIFOはメッセージグループ内の順序と重複排除を強化できるが、S3イベントからグループIDをどう付与するか、処理側の外部副作用まで一度だけになるかは別途設計が必要である。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4 / AWS公式 5

問題 084 | Domain 5 / ネットワーク | 複合難問 | 複数選択（5つから2つ選択）

問題 84 DNSによる持ち出しを止めて記録する

セキュリティチームは、複数のVPCから既知のマルウェア・コマンド&コントロールドメインへのDNS問い合わせを遮断し、どのワークロードが何を問い合わせたかを後から調査したい。ワークロードはAmazonProvidedDNSを使用している。HTTPだけでなくDNS段階で制御し、独自DNSアプライアンスをEC2で運用したくない。ルール更新とログ分析は集中化する予定である。

必要な機能を2つ選べ。

選択肢

A	Route 53 Resolver DNS Firewallのドメインリストとルールグループを作成し、対象VPCへ関連付ける。
B	AWS WAFのWeb ACLを各VPCのRoute 53 Resolverへ関連付ける。
C	Route 53 Resolver query loggingを構成し、CloudWatch Logs、S3、またはData Firehoseへ配送する。
D	Network ACLでUDP/TCP 53をすべて拒否し、DNSキャッシュだけで運用する。
E	CloudFrontの標準ログを有効にし、全DNS問い合わせを記録する。

ここでいったん止める | 解答と解説は次ページ

問題 084 正解・解説 複合難問

問題 84の正解・解説

1. 正解

A、C

2. 問題文の重要な条件

AmazonProvidedDNSを使う複数VPCで、ドメイン名に基づくDNS遮断と問い合わせ主体を含むログが必要。EC2アプライアンス運用は避ける。

3. 正解へ至る判断過程

DNS FirewallはResolverを通る問い合わせをドメインリストに基づいてALLOW/BLOCK/ALERTできる。Resolver query loggingはVPC DNS問い合わせを記録し、集中保存先へ送れる。制御と証跡を別機能で組み合わせる。

4. 正解が要件を満たす理由

Aで悪性ドメインの名前解決をDNS段階で阻止し、Cで送信元VPC・リソースや問い合わせ名などの調査材料を残せる。マネージド機能なのでDNSサーバーのパッチやHA設計が不要である。

5. 各不正解選択肢が不適切な理由

A: 正解肢のため対象外。
B: AWS WAFは対応するHTTP(S)リソースへのWeb要求を検査し、VPC ResolverへWeb ACLを付ける機能ではない。
C: 正解肢のため対象外。
D: DNSを全面拒否すると正当な名前解決も停止し、ドメイン単位の制御やログ要件を満たさない。
E: CloudFront logsはディストリビューションへの視聴者リクエストであり、VPCのDNS問い合わせ記録ではない。

6. 各不正解選択肢が正解になり得る条件

BはALB、API Gateway、CloudFrontなど対応リソースへのHTTP攻撃をL7で制御する場合に適する。Dは外部DNSを強制的に遮断し、許可済みResolverだけへ限定するACL設計の一部にはなり得る。EはCDNアクセス分析に使う。

7. 今後使える判断基準

DNSの内容を制御するならDNS Firewall、DNSの利用記録はResolver query logging、HTTP内容はWAF、IP/ポートはSG/NACL/Network Firewallと層を分ける。

8. 関連サービスとの比較

GuardDutyはDNSログ等を分析して脅威検出を行うが、任意の社内許可・拒否リストをDNS問い合わせ時に強制する機能ではない。DNS Firewallは予防的制御、GuardDutyは検出的統制として補完関係にある。

公式確認先 AWS公式 1 / AWS公式 2

問題 085 | Domain 1 / 監視・性能 | 複合難問 | 複数選択（5つから2つ選択）

問題 85 時刻で起こす処理と変更で起こす処理

プラットフォームチームには、性質の異なる二つの自動化要件がある。

1. 顧客ごとに指定された日時に一度だけ、最大数百万件のリソース終了APIを呼び出す。数分の範囲で実行時刻を分散でき、失敗時の再試行回数・イベント保持時間とSQSデッドレターキューを個別に設定したい。ターゲット側は冪等に実装する。
2. 本番アカウントで PutBucketPolicy が呼び出され、ポリシーに禁止された外部プリンシパルが追加された場合、数分以内に運用チケットを作成し、承認後にSystems Manager Automation runbookで直前の承認済みポリシーへ戻したい。API監査証跡も保持する。

これらを最小の独自スケジューラとポーリングで実現する構成要素を2つ選べ。

選択肢

A	EventBridgeのlegacy scheduled ruleを顧客ごとに作り、cron式とLambda内の再試行だけで一回限りの実行、保持時間、DLQを管理する
B	EventBridge Schedulerでone-time scheduleを作成し、flexible time window、retry policy、イベント保持時間、SQS DLQ、実行ロールと ActionAfterCompletion=DELETE を設定する
C	CloudTrailログをS3へ配信し、Athenaのスケジュールクエリを15分ごとに実行して PutBucketPolicy を検索する。結果があればEC2上のスクリプトで修復する
D	AWS Configの定期評価だけを24時間ごとに実行し、CloudTrailを無効化してS3保管費を削減する
E	CloudTrailで管理イベントの証跡を保持し、EventBridgeルールでCloudTrail経由の該当API呼び出しイベントを照合する。ターゲットでOpsItemまたはチケットを作成し、承認を含むSystems Manager Automationを開始する

ここでいったん止める | 解答と解説は次ページ

問題 085 正解・解説 複合難問

問題 85の正解・解説

1. 正解

B、E

2. 問題文の重要な条件

- 一つ目は大量の一回限りスケジュールで、柔軟な時間窓、再試行、保持期間、DLQが必要である。
- 二つ目は時刻ではなくAPI変更イベントが起点で、数分以内に検知したい。
- PutBucketPolicy の主体・時刻・要求内容を監査証跡として残す。
- 自動修復の前に承認が必要である。
- ポーリング用サーバーや独自スケジューラを減らしたい。
- 数百万件の完了済み一回限りスケジュールを残さず、クォータ消費と清掃運用を抑える。

3. 正解へ至る判断過程

時間起点とイベント起点を分ける。一回限りの大規模なスケジュールには、legacy scheduled ruleよりEventBridge Schedulerの機能が直接合う。完了後は ActionAfterCompletion=DELETE でスケジュール自体を自動削除する。API変更の検知では、CloudTrailが管理イベントを監査として記録し、EventBridgeがCloudTrail経由で届く該当APIイベントをルーティングする。修復はSSM Automationへ渡し、runbook内の承認を挟む。

4. 正解が要件を満たす理由

Bはone-time scheduleをネイティブに扱い、柔軟な時間窓で呼び出しを分散できる。再試行回数、失敗イベントの最大保持時間、DLQ、ターゲット実行ロールも管理でき、完了後の自動削除でスケジュール数クォータを不要に消費しない。EはS3バケットポリシー変更というAPIイベントへポーリングなしで反応し、OpsItem作成やAutomation起動へ接続できる。CloudTrailのtrailを別途保持することで、EventBridgeでの即応とS3等での長期監査を両立する。

5. 各不正解選択肢が不適切な理由

A: scheduled ruleはlegacy機能で、一回限りの大量スケジュール、柔軟な時間窓、個別の保持・再試行をSchedulerほど直接扱えない。再試行をLambdaへ自作すると運用負荷が増える。
B: 正解肢のため対象外。
C: 15分ポーリングは数分以内という要件を満たさず、Athena結果の重複処理やEC2スクリプトの可用性も自前管理になる。
D: 24時間周期では遅すぎ、CloudTrailを無効化すると誰がどのAPIを呼んだかという監査証跡を失う。Config評価はAPI監査そのものではない。
E: 正解肢のため対象外。

6. 各不正解選択肢が正解になり得る条件

A: 少数の単純な定期実行が既にscheduled ruleで安定運用され、one-time、柔軟な窓、詳細な再試行設定が不要なら継続利用できる。
C: 即応不要の過去監査や複数年分のAPI傾向分析なら、S3上のCloudTrailログをAthenaで検索する方法が適する。
D: APIの主体追跡ではなく、ある時点のリソース構成がポリシー準拠かを定期的に評価する用途ならConfig ruleが適する。

7. 今後使える判断基準

「何時に実行するか」はScheduler、「何が起きたら実行するか」はEventBridge ruleで考える。大量のone-time scheduleでは実行設定だけでなく、完了後削除も設計に含める。監査記録はCloudTrail、望ましい構成からの逸脱評価はConfig、複数手順の修復はAutomationへ分担する。少なくとも1回の呼び出しや再試行を前提に、終了APIは冪等にする。

8. 関連サービスとの比較

EventBridge Schedulerはone-time/cron/rate、柔軟な時間窓、再試行とDLQを持つ。EventBridge rulesはイベントパターンに一致したAWSサービスイベントやCloudTrail経由APIイベントをターゲットへ渡す。CloudTrail LakeやAthenaは履歴の調査に、Configは構成準拠の継続評価に向く。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4 / AWS公式 5 / AWS公式 6

問題 086 | Domain 2 / 信頼性・BC | 本番より難しい | 複数選択（5つから3つ選択）

問題 86 既存オブジェクトも、削除命令からも守る

監査証跡を保管するS3バケットには、過去3年分のオブジェクトが既に存在し、最も新しい既存バージョンも作成から30日を経過している。今後の新規オブジェクトは、別アカウント・別リージョンのバケットへ15分以内というSLAを伴って複製したい。過去分も移行完了後には同じ宛先へ揃える必要がある。

ソースで通常の DeleteObject が誤実行されても、宛先ではそのオブジェクトを現行バージョンとして参照可能なままにしたい。また、ソースと宛先の各オブジェクトバージョンは作成後30日間、管理者やルートユーザーでも完全削除・上書きできないようにする。要件を満たす構成要素を3つ選べ。

選択肢

A	ソースと宛先の両バケットでS3 VersioningとS3 Object Lockを有効にし、Compliance modeのデフォルト保持期間を30日にする
B	新規オブジェクトに対してS3 Cross-Region ReplicationとS3 Replication Time Control（S3 RTC）を設定し、Delete Marker Replicationは有効にしない
C	過去3年分の既存オブジェクトにはS3 Batch Replicationを実行する
D	ソースでの削除を正確に再現するため、Delete Marker Replicationを有効にする
E	非現行バージョンを1日後に期限切れにするS3 Lifecycleを両バケットへ設定し、MFA Deleteだけで30日保護を代替する

ここでいったん止める | 解答と解説は次ページ

問題 086 正解・解説 本番より難しい

問題 86の正解・解説

1. 正解

A、B、C

2. 問題文の重要な条件

- 新規オブジェクトは15分SLAでクロスリージョン複製。
- 既存オブジェクトも後から複製。
- 既存バージョンはすべて、要求される作成後30日の保護期間を経過済み。
- ソースの通常削除を宛先へ伝播させない。
- 30日間はルートを含めて削除不能。

3. 正解へ至る判断過程

ライブレプリケーションは設定後の新規オブジェクトが対象なので、既存分にはBatch Replicationが必要である。15分のSLAはS3 RTCで満たす。削除命令を宛先へ反映しないためDelete Marker Replicationは無効のままにする。不変性は両バケットのVersioningとObject Lock Compliance modeで担保する。

4. 正解が要件を満たす理由

- A：Versioningは上書き・削除時にも以前のバージョンを残す。Object Lock Compliance modeでは保持期間中、ルートを含む誰も保護バージョンを削除・上書きできない。ロック済みオブジェクトと保持メタデータを複製するには宛先にもObject Lockが必要である。
- B：S3 RTCは新規オブジェクトの99.9%を15分以内に複製するSLAを提供する。Delete Marker Replicationを有効にしなければ、ソースの通常削除で作られた削除マーカーを宛先の現行状態へ伝播させない。
- C：S3 Batch Replicationは、ライブレプリケーション設定前に存在したオブジェクトを複製できる。

5. 各不正解選択肢が不適切な理由

- D：ソースの削除マーカーが宛先にも複製され、宛先でオブジェクトを通常参照できるままにする要件と反対である。
- E：1日後の非現行バージョン削除は30日保持に反する。MFA DeleteはObject Lock Compliance modeと同じWORM強制ではなく、管理方法や対応操作も異なる。

6. 各不正解選択肢が正解になり得る条件

- D：災害対策先をソースの論理状態と同一に保ち、削除も意図どおり複製したい場合。
- E：保持要件が1日で、ルート＋MFAによるバージョン完全削除の統制で十分な場合。ただし規制上のWORM要件にはObject Lockを選ぶ。

7. 今後使える判断基準

S3レプリケーション問題では、(1)設定後の新規か既存か、(2)複製時間にSLAが要るか、(3)削除マーカーを伝播するか、(4)上書き/完全削除を誰まで防ぐか、を分けて判断する。バケットのデフォルト保持は既存バージョンへ遡及しないため、保持期間内の既存版があるならS3 Batch Operationsで保持期限を追加する。CRRだけでは既存オブジェクトも不変性も自動的には満たさない。

8. 関連サービスとの比較

S3 Versioningは復元可能な旧バージョンを残すが、権限のある主体による完全削除は防がない。Object Lockはバージョン単位のWORM保護を加える。CRR/SRRは新規変更の非同期ライブ複製、Batch Replicationは既存または再複製、S3 RTCはライブ複製時間の予測可能性とSLAを提供する。AWS Backup for S3の連続バックアップは最大35日のPITRという別の復旧モデルである。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4 / AWS公式 5

問題 087 | Domain 3 / 展開・自動化 | 本番より難しい | 四択（1つ選択）

問題 87 コンテナを段階公開し、旧版を戻せる時間を残す

ある決済APIは、Application Load Balancerの背後にあるAmazon ECS on Fargateサービスとして稼働している。これまでのローリング更新では、同じ latest タグが別イメージへ上書きされ、障害時にどのイメージへ戻すべきか判別できないことがあった。また、タスクのヘルスチェックは通るが、実トラフィックの一部でのみ発生する互換性不具合がリリース後に見つかった。

次のリリースからは、OSおよび言語パッケージの重大な脆弱性があるイメージを昇格させず、承認された同一成果物を各段階で使う。新タスクへのテストトラフィックでスモークテストを実行した後、本番トラフィックの10%を15分間だけ流し、5xx率またはp95レイテンシーのアラームが発報しなければ100%へ切り替える。全量切り替え後も旧タスクを一定時間残し、問題時には自動的に旧版へ戻したい。一時的に新旧両方のタスク費用が発生することは許容する。

最も適切な構成はどれか。

選択肢

A ECRのタグを可変のまま latest に統一し、ECSのローリング更新で minimumHealthyPercent=0、maximumPercent=100 とする。デプロイ後にCloudWatchダッシュボードを人が確認して、必要なら同じタグを再プッシュする

B ECRでリリースタグをイミュータブルにし、イメージダイジェストを昇格単位としてEnhanced Scanningの結果をパイプラインのゲートにする。ALBを使用するECSサービスでcanaryデプロイを構成し、テストトラフィックとライフサイクルフック、10%と評価時間、CloudWatchアラームによる自動ロールバック、全量移行後のbake timeを設定する

C 新しいECSサービスを別リージョンに作成し、Route 53のフェイルオーバールーティングでヘルスチェックが成功した瞬間に100%を新リージョンへ切り替える。ECRイメージスキャンはタスク起動後にだけ実行する

D ECR Lifecycle Policyで直前のイメージを即時削除し、ECSのデプロイサーキットブレーカーだけを有効にする。ALBヘルスチェックが成功したタスクへは直ちに全トラフィックを送る

ここでいったん止める | 解答と解説は次ページ

問題 087 正解・解説 本番より難しい

問題 87の正解・解説

1. 正解

B

2. 問題文の重要な条件

- 同じ成果物を識別可能に保ち、タグ上書きによる再現不能を防ぐ。
- 脆弱性スキャンを本番起動後ではなく昇格前のゲートにする。
- テストトラフィック、10%の本番canary、15分評価、全量切り替えという段階が明示されている。
- アプリケーションメトリクスで自動ロールバックし、旧版をbake time中に保持する。

3. 正解へ至る判断過程

問題を「成果物の完全性」と「公開方法」に分ける。ECR側ではタグの再利用を止め、実体を一意に示すダイジェストで昇格する。スキャン合格は公開前に判定する。ECS側では、単なる起動成功では捉えられない実トラフィック不具合を小さい割合で観測するため、canaryトラフィックシフト、ライフサイクルフック、CloudWatchアラーム、自動ロールバック、bake timeを組み合わせる。

4. 正解が要件を満たす理由

ECRのタグイミュータビリティは、同じリリースタグを別イメージで上書きする操作を拒否する。Enhanced ScanningはAmazon Inspectorと連携し、OSとプログラミング言語パッケージの脆弱性を継続的に検出できる。パイプラインではスキャン結果を評価し、合格したダイジェストをタスク定義へ固定する。

ECSのcanaryデプロイは、新しいサービスリビジョンへ最初に小割合、その後に残りを送る二段階方式である。ALBのテストトラフィックで本番切り替え前の検証を行い、ライフサイクルフックでスモークテストを自動化できる。canary評価中と全量移行後にCloudWatchアラームを監視し、異常時は旧サービスリビジョンへロールバックする。bake time中は新旧が併存するので、速い復旧と引き換えに一時的な二重費用が発生するという条件にも合う。

5. 各不正解選択肢が不適切な理由

- A：latest の上書きで同一性を失い、旧版の再現可能なロールバックができない。minimumHealthyPercent=0 は更新中に利用可能タスクがゼロになり得て、段階トラフィックも実装しない。
- C：別リージョンは災害対策にはなるが、本問の10%・15分という同一サービスの段階公開を満たさず、コストとデータ整合性の問題を増やす。スキャンを起動後に行うと脆弱な成果物を先に公開する。
- D：直前イメージを削除すると迅速なロールバックを妨げる。サーキットブレーカーはタスク起動・ヘルス失敗のロールバックには有用だが、それだけでテストトラフィック、10% canary、アプリメトリクス評価、bake timeを満たさない。

6. 各不正解選択肢が正解になり得る条件

- A：非本番の使い捨て環境で、停止時間と成果物の追跡性を許容し、素早い上書きを優先する場合。
- C：リージョン全体の障害や地理的移行を検証し、データレプリケーションを含むマルチリージョン切り替えが主目的の場合。
- D：小規模で後方互換性が高く、タスク起動失敗だけを検出すればよく、ローリング更新の低い追加費用を優先する場合。旧イメージは保持する必要がある。

7. 今後使える判断基準

安全なコンテナ展開は、(1)識別可能で不変な成果物、(2)公開前の検査、(3)小さい影響範囲からのトラフィック移行、(4)技術・業務メトリクスによる停止、(5)旧版を戻せる保持時間に分けて考える。ヘルスチェック成功は、業務的な正しさやレイテンシーSLOの保証ではない。

8. 関連サービスとの比較

ローリング更新は追加容量を抑えやすく、デプロイサーキットブレーカーで起動失敗を戻せる。blue/greenは新旧環境を並べてテストし、一括切り替えと速い復旧に向く。canaryは小割合の実トラフィックで評価後に全量へ移す。linearは一定割合ずつ複数段階で増やす。ECRのスキャンとタグ不変性は成果物側の統制であり、ECSのデプロイ方式を代替しない。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4 / AWS公式 5

問題 088 | Domain 5 / ネットワーク | 複合難問 | 四択（1つ選択）

問題 88 ハイブリッド経路の遅延と損失を継続監視する

AWS上の業務システムは、Direct ConnectとSite-to-Site VPNを介してオンプレミスのデータベースへ接続する。トンネルやBGPセッションはUPのままなのに、利用者から時折遅いと報告される。運用チームは、指定したVPCサブネットからオンプレミスIPまでの往復遅延とパケット損失を一定間隔で測定し、しきい値を超えたらCloudWatch Alarmを発報したい。各EC2へ監視エージェントを導入せず、インターネット利用者からAWSアプリへの品質ではなく、ハイブリッド経路を観測したい。

最適な機能はどれか。

選択肢

A	CloudWatch Internet Monitorで、世界のISP別トラフィックだけを監視する。
B	VPC Flow Logsのバイト数から、各パケットの往復遅延と損失率を算出する。
C	Route 53 health checkをオンプレミスのプライベートIPへ直接設定する。
D	CloudWatch Network Synthetic Monitorで、VPCサブネットを送信元、オンプレミスIPを宛先とするprobeを作成する。

ここでいったん止める | 解答と解説は次ページ

問題 088 正解・解説 複合難問

問題 88の正解・解説

1. 正解

D

2. 問題文の重要な条件

制御面はUPでもデータ面の遅延・損失がある。VPCサブネットからオンプレミスIPへのハイブリッド経路、定期測定、Alarm、エージェント不要が条件である。

3. 正解へ至る判断過程

Network Synthetic MonitorはAWS側サブネットとオンプレミス宛先間にマネージドprobeを作り、round-trip timeとpacket lossをCloudWatchへ発行する。トンネル状態とは別に、実際の経路品質を継続監視できる。

4. 正解が要件を満たす理由

EC2へのソフトウェア導入なしに、ICMPまたはTCPを使うprobeとしきい値Alarmを構成できる。Direct Connect/VPNを含むハイブリッド経路の劣化に焦点を当てられる。

5. 各不正解選択肢が不適切な理由

A: Internet Monitorはインターネット利用者とAWSワークロード間の可用性・性能把握に向き、指定オンプレミスIPへの私設経路probeとは異なる。
B: Flow Logsはフローのメタデータを記録するが、各パケットのRTTや損失率を直接提供しない。
C: Route 53の標準ヘルスチェッカーはインターネットからプライベートIPへ到達できず、経路品質の継続メトリクス用途でもない。
D: 正解肢のため対象外。

6. 各不正解選択肢が正解になり得る条件

Aは世界のエンドユーザーから公開アプリへのインターネット品質を地域・ASN別に評価する場合、Bは実際の通信のACCEPT/REJECTや量を調べる場合、Cは公開エンドポイントの外形監視とDNSフェイルオーバーに適する。

7. 今後使える判断基準

VPNのTunnelStateは経路が論理的にUPか、Network Synthetic Monitorはハイブリッド経路のRTT/損失、Internet Monitorはインターネット利用者視点、と観測対象を区別する。

8. 関連サービスとの比較

CloudWatch Network Flow Monitorはエージェントを使ってVPC内などの実TCPフローを詳細観測する。一方、Network Synthetic Monitorはマネージドなsynthetic probeでAWSからオンプレミス宛先までを測るため、本問のエージェント不要・指定経路監視に合う。

公式確認先 AWS公式 1 / AWS公式 2

問題 089 | Domain 1 / 監視・性能 | 複合難問 | 四択（1つ選択）

問題 89 承認と配布速度を別に制御する

金融会社は、Environment=Prod タグを持つ500台のSystems Manager managed nodeへOS設定変更を展開する。この会社は2025年11月7日より前からSystems Manager Change Managerを利用している既存顧客である。変更は、指定されたChange Calendarの開放期間内に限り、運用担当者とは別の承認者2名の承認を得て開始しなければならない。一度に変更するノードは対象の10%以下とし、失敗率が3%を超えた時点で未開始ノードへの新規配布を停止したい。さらに、変更中にサービスSLOのCloudWatch alarmがALARMになった場合も実行を停止し、誰が承認し、どのrunbook版を実行したか追跡できる必要がある。既に実行中のノードは停止判定時点で完了する可能性があることは、リスク部門が受け入れている。

最も適切な構成はどれか。

選択肢

A Maintenance WindowsにRun Commandを登録し、500台を同時実行する。承認はウィンドウ名にチケット番号を記載することで代替する

B 各ノードを対象とするAutomationを500件別々に開始し、各実行に aws:approve を置く。Lambdaで同時実行数と失敗率を1秒ごとに数えて停止する

C Systems Manager Change Managerのchange templateとchange requestで承認者、Change Calendar、実行runbookを統制する。Automationをタグターゲットでrate control実行し、MaxConcurrency=10%、MaxErrors=3% と監視用CloudWatch alarmを設定し、実行履歴を保持する

D State Manager associationを即時作成し、ComplianceがNon-compliantのノードに同時適用する。CloudTrailの CreateAssociation イベントだけを承認記録とみなす

ここでいったん止める | 解答と解説は次ページ

問題 089 正解・解説 複合難問

問題 89の正解・解説

1. 正解

C

2. 問題文の重要な条件

- 別担当者2名による事前承認とChange Calendarによる時間統制が必要である。
- Change Managerを利用できる既存顧客である。
- タグで500台を対象化し、最大同時実行10%、エラーしきい値3%を指定する。
- CloudWatch alarm発報でも新たな実行を止めたい。
- 承認者、runbook、実行履歴の監査性が必要である。
- しきい値到達時に既に動いている実行が完了し、最終失敗数が3%をわずかに超え得ることは許容されている。

3. 正解へ至る判断過程

承認・変更期間・監査はChange Manager、対象への実行速度と停止条件はAutomationのrate controlとして分ける。Change templateで承認やrunbookを標準化し、change requestをCalendarと結び付ける。Automationではタグをターゲットにして最大同時実行数とエラーしきい値を指定する。CloudWatch alarm監視を付けるとSLO悪化時にも停止できる。

4. 正解が要件を満たす理由

Change Managerは変更要求、承認者、スケジュール、実行ワークフローを一貫して記録する。AutomationのMaxConcurrencyは同時に処理する対象を割合または絶対数で制限する。MaxErrors=3%は3%までのエラーを許容し、3%を超えるエラーを受信すると未開始対象への配布を止める。既に走行中の処理は完了し得るという仕様も問題の許容条件に一致する。監視アラームがALARMになればAutomationを停止させられる。

5. 各不正解選択肢が不適切な理由

A: Maintenance Windowsは時間帯とタスク実行には使えるが、名前への番号記載は2名承認の強制や承認証跡にならない。全台同時実行も10%制約に反する。
B: aws:approve 自体は承認に使えるが、500件の個別実行と独自Lambdaによるレート制御は不要に複雑で、承認が実行ごとに重複する。
C: 正解肢のため対象外。
D: State Managerは望ましい状態の継続適用に向くが、即時associationは事前承認とCalendar統制を満たさない。API作成者のCloudTrail記録は変更承認記録の代替ではない。

6. 各不正解選択肢が正解になり得る条件

A: 定例の低リスク保守で、外部チケットシステムに承認があり、Maintenance Windowのrate controlを適切に設定するなら利用できる。
B: 単一または少数の高リスク操作で、runbook内の特定ステップ直前にその場の承認を挟みたい場合、aws:approve が適する。
D: 承認付き一回変更ではなく、全ノードが常に一定設定を保つよう継続的に収束させたい場合はState Managerが適切である。

7. 今後使える判断基準

Change Managerはガバナンス、Automationは複数手順、Run Commandはノード上コマンド、State Managerは望ましい状態の維持、Maintenance Windowsは実行時間帯の編成、と役割を分ける。MaxErrors は指定数・割合までを許容し、それを超えた後に新規配布を止めるため、厳密な最大失敗数保証ではない。厳密性が必要なら値を一つ手前に置き、同時実行も1に近づける。

8. 関連サービスとの比較

runbook内の aws:approve は単一ワークフローを一時停止する。Change Managerはテンプレート、複数承認、Calendar、変更要求履歴を組織的に統制する。ただしChange Managerは2025年11月7日以降、新規顧客には提供されていないため、新規導入なら外部ITSMの承認とAutomation/Change Calendarを組み合わせる。CloudTrailは各API呼び出しの監査を補完するが、業務上の承認ワークフローそのものではない。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4 / AWS公式 5

問題 090 | Domain 2 / 信頼性・BC | 本番より難しい | 四択（1つ選択）

問題 90 ファイル1個の復元に新しいファイルサーバーを作らない

設計部門はAmazon FSx for Windows File ServerをSMB共有として使用している。利用者がCADファイルを誤って上書き・削除する問い合わせが1日に数回あり、ヘルプデスクが昨夜のファイルシステムバックアップから新しいFSxファイルシステムを作成し、対象ファイルをコピーしている。この手順には1時間以上かかり、その間の当日変更も戻せない。

要件は、直近48時間について1時間間隔の版を保持し、通常のWindows権限を持つ利用者がエクスプローラーから数分で個々のファイルまたはフォルダを元に戻せるようにすることである。ファイルシステム全体の災害復旧用に、毎日のAWS Backupとクロスリージョンコピーは継続する。最も適切な追加構成はどれか。

選択肢

A	AWS Backupの取得間隔を1時間にし、利用者へAWS Backupコンソールの復元権限を付与する
B	FSx for Windows File Serverでシャドウコピーのストレージ上限と1時間間隔のスケジュールを構成し、Windowsの「以前のバージョン」から利用者が復元できるよう権限を整える
C	FSxファイルシステムでS3 Versioningを有効にし、SMBクライアントへS3のversion IDを表示する
D	AWS DataSyncで15分ごとに別のFSxファイルシステムへ同期し、誤削除も同じ状態になる前に毎回ジョブを手動停止する

ここでいったん止める | 解答と解説は次ページ

問題 090 正解・解説 本番より難しい

問題 90の正解・解説

1. 正解

B

2. 問題文の重要な条件

- 個別ファイル/フォルダの頻繁な論理復旧。
- 1時間間隔、48時間の細かい版。
- 利用者がWindowsエクスプローラーから自己復旧する。
- ファイルシステム全体のDRバックアップは別に継続する。

3. 正解へ至る判断過程

FSxバックアップはファイルシステム全体を新規ファイルシステムへ復元するための手段であり、頻繁な1ファイル復旧には重い。FSx for Windowsのシャドウコピーは、同じファイルシステム内で過去版を保持し、Windowsの「以前のバージョン」操作を提供するため、本問の粒度とRTOに合う。

4. 正解が要件を満たす理由

管理者はシャドウコピーのスケジュールと最大使用ストレージを設定できる。利用者は使い慣れたWindows File Explorerから、ファイルまたはフォルダの以前のバージョンを表示・復元できる。日次バックアップを廃止しないため、ファイルシステム損失やリージョン障害には従来のDR経路も残る。

5. 各不正解選択肢が不適切な理由

- A：1時間ごとのファイルシステムバックアップは費用・ジョブ数・復元時間が大きく、利用者に広いAWS復元権限を与える。復元先も新しいファイルシステムになる。
- C：FSx for WindowsのSMBファイルにS3 Versioningを直接有効化する機能はない。
- D：同期はバックアップ版管理ではなく、誤削除・上書きも宛先へ反映し得る。人がジョブを止める設計はRPOと運用負荷を保証できない。

6. 各不正解選択肢が正解になり得る条件

- A：ファイルシステム全体を1時間単位で復旧する規制要件があり、対応サービス・費用・ジョブ制限を検証済みの場合。
- C：対象がFSxではなくS3オブジェクトで、アプリケーションがオブジェクトバージョンを扱える場合。
- D：別ファイルシステムへの移行・配布が目的で、削除伝播を含む同期動作を受け入れる場合。

7. 今後使える判断基準

ファイル保護では、復元単位と利用者を確認する。「利用者が1ファイルを即時に戻す」ならシャドウコピー、「管理者がファイルシステム全体を別リソースとして復元」ならFSx/AWS Backupである。両者は代替ではなく、日常復旧と災害復旧の多層防御として併用する。

8. 関連サービスとの比較

FSxシャドウコピーは同一ファイルシステム上の短期版管理であり、ファイルシステム自体を失う障害には弱い。FSxバックアップはファイルシステム整合性を持つ増分バックアップから新しいFSxを作成する。AWS Backupを使うとスケジュール、保持、クロスリージョン/クロスアカウントコピーを集中管理できる。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3

問題 091 | Domain 3 / 展開・自動化 | 本番より難しい | 四択（1つ選択）

問題 91 EKS更新失敗をforceで押し切る前に直すもの

あるSaaS企業は、3つのAZにまたがるAmazon EKSクラスターで、カスタムAMIを使うマネージドノードグループを運用している。ノードグループは作成時からカスタムEC2起動テンプレートを使用している。緊急度の高いOS修正を含む新AMIを作成し、同じ起動テンプレートの新バージョンへAMI IDを設定した。

検証環境のローリング更新は途中で PodEvictionFailure になった。調査すると、単一レプリカの決済ワーカーに minAvailable: 1 のPodDisruptionBudget（PDB）があり、退避先にできる余剰Podがない。ワーカー停止は許容されない。本番ノードグループは6台で、更新中も容量を維持できる一時的な追加ノード枠はある。更新は1台ずつ行い、ノード参加やPod退避に失敗した場合はforceで押し切らず、未更新ノードを残したまま原因を直したい。クラスターのコントロールプレーンとVPC CNIアドオンは今回の対象外である。

最も適切な対応はどれか。

選択肢

A force を指定して同じ更新を再実行する。force更新はPDBを無視してPodを削除するが、マネージドノードグループが同じPodを即時再作成するため、単一レプリカでも停止は発生しない

B EKSコントロールプレーンを先に次のKubernetesマイナーバージョンへ更新する。コントロールプレーン更新が成功すれば、カスタムAMI、全ノード、VPC CNIも自動的に最新版へ更新される

C 先にワーカーを複数レプリカ化し、AZ分散と十分な余剰容量を確保して、PDBが1Podの退避を許可できる状態を検証する。ノードグループの maxUnavailable=1 とdefault更新戦略を使用し、同じ起動テンプレートの新バージョンを指定してローリング更新する。更新状態とPodのreadinessを監視し、更新失敗時は原因を修正してから再開または以前の構成へロールバックする

D 現在のノードグループを、新しい名前の起動テンプレートへ直接変更する。desiredSize を0へ下げて全旧ノードを終了した後、新AMIのノードを6台起動すればPDBが自動的に満たされる

ここでいったん止める | 解答と解説は次ページ

問題 091 正解・解説 本番より難しい

問題 91の正解・解説

1. 正解

C

2. 問題文の重要な条件

- 更新失敗の原因は、単一レプリカとPDBによりPodを安全に退避できないことである。
- ワーカー停止は許容されず、forceによる強制削除は使えない。
- 一時的な追加容量を許容し、1台ずつ更新したい。
- 既存ノードグループはカスタム起動テンプレートで作成済みで、新AMIは同じテンプレートの新バージョンにある。

3. 正解へ至る判断過程

マネージドノードグループ更新はノードを作るだけでなく、旧ノードのPodをdrainする。PDBが退避を一切許さないなら、更新機能を変える前にアプリケーションの可用性条件を成立させる必要がある。単一レプリカを増やし、トポロジー分散と容量を確認した上で、PDBを尊重するdefault戦略と maxUnavailable=1 で更新する。forceは「更新を成功させる」選択肢ではなく、「PDBを破ってでもPodを削除する」選択肢である。

4. 正解が要件を満たす理由

EKSのdefault更新戦略は、旧ノードを終了する前に新ノードを起動し、容量を維持しながら対象ノードをcordon・drainする。maxUnavailable=1 は並列で更新されるノード数を1台に制限する。複数レプリカと適切なPDB・トポロジー分散があれば、1Podを別ノードへ移してもサービスを継続できる。

カスタムAMIを使う既存ノードグループでは、同じカスタム起動テンプレートの新バージョンを作成し、そのバージョンへ更新する。更新すると全ノードが新しいテンプレート構成へ順次リサイクルされる。更新状態、Podのreadiness、アプリケーションSLOを監視し、失敗時はforceで隠さず、PDB、容量、ブートストラップなどの原因を修正する。必要なら以前のKubernetes/テンプレート構成を使う更新としてロールバックする。

5. 各不正解選択肢が不適切な理由

- A：force更新はPDBを尊重せずPodを削除する。単一レプリカの停止時間をゼロにする保証はなく、問題文の可用性要件に反する。
- B：コントロールプレーンの更新はカスタムAMIのノードグループやEKSアドオンを自動更新しない。今回の原因はKubernetes版ではなくPod退避条件であり、不要な変更範囲を広げる。
- D：既存のカスタム起動テンプレート利用ノードグループは、同じテンプレートの別バージョンへ更新する。別テンプレート名へ直接切り替える設計ではない。desiredSize=0 のスケールダウンはPDBを尊重せず、全停止を招く。

6. 各不正解選択肢が正解になり得る条件

- A：停止可能なバッチPodなどで、PDBが誤設定であることを確認し、強制削除の影響を明示的に受容する緊急更新の場合。
- B：目的がサポート対象のKubernetes版へコントロールプレーンを上げることで、互換性確認後にノードとアドオンを別工程で更新する場合。
- D：既存グループを直接変更するのではなく、新しい起動テンプレートを使う別ノードグループをblue/green方式で作成し、Podを安全に移して旧グループを縮小する場合。

7. 今後使える判断基準

EKSノード更新の失敗では、(1)新ノードが起動・参加できるか、(2)旧Podを退避できるか、(3)PDBとレプリカ数が矛盾していないか、(4)更新用の一時容量があるかを分けて調べる。PodEvictionFailure に対するforceは最後の影響受容であり、無停止要件の解決策ではない。

8. 関連サービスとの比較

マネージドノードグループはノードのローリング更新とdrainを管理する。セルフマネージドノードでは同じ手順をAuto ScalingやKubernetes操作で自分で組む必要がある。EKS Auto Modeはノード基盤のパッチと更新をさらに自動化できるが、ブロッキングPDBやアプリケーションのレプリカ不足まで自動的に正しく解消するものではない。EKSアドオンの更新とコントロールプレーン更新も、ノードAMI更新とは別のライフサイクルで計画する。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4

問題 092 | Domain 1 / 監視・性能 | 本番相当 | 四択（1つ選択）

問題 92 利用者の遅さとサービスの遅さ

あるECサイトはCloudFront、ALB、ECS、Lambda、RDSで構成され、ブラウザ向けSPAを提供している。運用チームには、(a)実際の利用者について国・ブラウザ・ページ別のCore Web VitalsとJavaScriptエラーを把握する、(b)利用者がいない時間もログインと購入APIを定期実行して外形可用性を測る、(c)ECSからLambda、RDSなどの依存関係とリクエストごとの遅延箇所を追う、(d)サービスレベル目標（SLO）に対する状態をサービス単位で監視する、という要件がある。単一のメトリクス画面へすべてを無理に押し込むのではなく、AWSの管理機能を組み合わせて相互にドリルダウンできることを優先する。

最も適切な構成はどれか。

選択肢

A CloudWatch Logs Insightsだけを使い、ALBアクセスログから実利用者のCore Web Vitals、ブラウザ内JavaScriptエラー、未アクセス時間の外形監視をすべて推定する

B AWS X-Rayだけを全サービスで有効にし、ブラウザの全セッションを100%サンプリングしてSLO、外形監視、Core Web VitalsもX-Rayトレースから生成する

C CloudWatch Synthetics canaryだけを作成し、canaryの成功率を実利用者全体の体験およびすべての内部依存関係の代替指標にする

D CloudWatch RUMをSPAへ導入し、Synthetics canaryで重要経路を定期実行する。Application Signalsを対応ワークロードへ有効化してSLO、サービスマップ、標準アプリケーションメトリクスを監視し、X-Rayトレースおよび関連ログへドリルダウンできるようにする

ここでいったん止める | 解答と解説は次ページ

問題 092 正解・解説 本番相当

問題 92の正解・解説

1. 正解

D

2. 問題文の重要な条件

- 実利用者のブラウザ側体験とJavaScriptエラーが必要である。
- 利用者がいなくても重要経路を能動的に検査する。
- サービス間依存関係と個別リクエストの遅延箇所を追跡する。
- SLOをサービス単位で監視する。
- 各観測方式を相関させ、詳細へ進めることを重視する。

3. 正解へ至る判断過程

観測主体で分ける。実ブラウザからの受動観測はRUM、合成クライアントからの能動試験はSynthetics、バックエンドサービスの健康・依存関係・SLOはApplication Signals、リクエスト単位の詳細はX-Rayトレースで扱う。Application SignalsとRUM/SyntheticsはX-Ray tracingを有効にすることでサービスビューから相関できる。

4. 正解が要件を満たす理由

RUMは実ユーザーのページロード、Web Vitals、クライアントエラーを端末属性とともに収集する。Synthetics canaryはスケジュールに従い、ログインやAPI呼び出しを利用者不在時にも検証できる。Application Signalsは対応アプリケーションを計装し、サービス、操作、依存先のメトリクスとSLOをアプリケーション中心に表示する。X-Rayトレースを関連付ければ、遅い操作から下流セグメントへ進める。

5. 各不正解選択肢が不適切な理由

A: ALBログはサーバー側リクエストを記録するが、ブラウザ描画、Core Web Vitals、クライアント内JavaScript例外、利用者不在時の検査を直接観測しない。
B: X-Rayは分散トレースに適するが、それ単独でRUMのブラウザ体験やSyntheticsの能動実行、Application SignalsのSLOビューをすべて置き換えない。全件トレースは費用と負荷も増やす。
C: canaryは決められた経路の外形監視であり、多様な実ユーザー環境や全内部呼び出しを代表しない。
D: 正解肢のため対象外。

6. 各不正解選択肢が正解になり得る条件

A: サーバー側の特定エラーを過去ログから集計するだけならLogs Insightsが適する。
B: 要件が個々のバックエンドリクエストのサービス間経路と遅延分析だけなら、X-Rayを中心にできる。
C: 公開エンドポイントの到達性と固定ユーザージャーニーだけを低運用で継続検査したい場合、Syntheticsが正解になる。

7. 今後使える判断基準

RUMはreal user、Syntheticsはrobot user、X-Rayはrequest trace、Application Signalsはservice health/SLOと覚える。ただし別々の島にせず、トレースID、サービスマップ、関連ログを通じて症状から原因へ移れる構成にする。

8. 関連サービスとの比較

Container Insightsはクラスター、タスク、コンテナ資源の可視化に強く、Application Signalsはアプリケーション操作と依存関係に強い。Logs Insightsはログの対話検索、CloudWatch dashboardsは選んだメトリクスの共有表示を担う。いずれもRUMやSyntheticsの観測主体とは異なる。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4

問題 093 | Domain 2 / 信頼性・BC | 複合難問 | 複数選択（5つから2つ選択）

問題 93 パイロットライトに残すもの、残さないもの

企業は、プライマリリージョンでALB、EC2 Auto Scaling、Aurora PostgreSQLを使う業務システムのDRを設計している。事業部が合意した目標はRTO 45分、RPO 5分である。予算上、復旧リージョンでアプリケーションスタックを常時リクエスト処理可能な状態にすることはできないが、日次バックアップから全データを戻す時間ではRTO/RPOを満たさない。運用チームはパイロットライト戦略を採用し、四半期ごとに復旧訓練を行う。

この戦略を正しく実装する構成・手順を2つ選べ。

選択肢

A	復旧リージョンには、Aurora Global Databaseのセカンダリなど、RPOを満たす継続レプリケーション済みの中核データ層を小規模で維持する
B	復旧リージョンでALB、全アプリケーション層、DBを縮小構成ながら常時稼働させ、ヘルスチェック要求を継続処理する
C	VPC、IAM、暗号鍵、AMI/コンテナ、Auto Scaling定義をIaCで事前に準備し、障害時にデータ層を昇格または書き込み可能にした後、アプリケーション容量を起動・拡張してトラフィックを切り替える手順を自動化・訓練する
D	復旧リージョンには何も作らず、日次スナップショットだけをコピーし、障害後にネットワークから全データまで手動で構築する
E	両リージョンを常に本番容量で稼働させ、通常時から50%ずつユーザートラフィックを処理する

ここでいったん止める | 解答と解説は次ページ

問題 093 正解・解説 複合難問

問題 93の正解・解説

1. 正解

A、C

2. 問題文の重要な条件

- RTO 45分、RPO 5分で、日次復元では不足。
- 復旧側のフルアプリケーションは常時稼働できない。
- パイロットライトを選択済み。
- 実際の昇格・起動・経路切替まで訓練する。

3. 正解へ至る判断過程

パイロットライトでは、データ複製など復旧の中核だけを常時動かし、アプリケーション計算容量は障害時に立ち上げる。したがって、短いRPOを継続レプリケーションで満たし、残りの環境をIaCと自動手順で45分以内に展開・拡張できるようにする必要がある。

4. 正解が要件を満たす理由

- A：データ層を継続複製することで、日次バックアップでは不可能な5分RPOを狙える。小規模の中核だけを維持するため、完全な待機系より費用を抑えられる。
- C：ネットワーク、権限、成果物、容量定義を事前にコード化し、データ昇格->アプリ起動->トラフィック切替の依存順序を訓練することで、パイロットライトの復旧時間を現実に45分以内へ収める。

5. 各不正解選択肢が不適切な理由

- B：縮小されていても完全なアプリケーションが常時機能するのはwarm standbyであり、予算条件に反する。
- D：backup and restore戦略であり、日次RPOと全環境構築時間が本問の目標を満たさない。
- E：multi-site active/activeであり、最も高い平常時費用と運用複雑性を持つ。

6. 各不正解選択肢が正解になり得る条件

- B：RTOを数分まで短くし、縮小版アプリケーションを常時動かす費用を受容する場合。
- D：RTOが数時間〜日、RPOが日次でよく、費用最小化を最優先する場合。
- E：RTOをほぼ0にし、両リージョンから通常時にサービスする事業・レイテンシー要件がある場合。

7. 今後使える判断基準

DR方式は「復旧側で何が平常時から動くか」で見分ける。データ/中核のみがパイロットライト、縮小版の完全スタックがwarm standby、全復元がbackup and restore、複数拠点が通常トラフィックを処理するのがactive/activeである。

8. 関連サービスとの比較

Aurora Global Database、RDSクロスリージョンリードレプリカ、DynamoDB global tables、S3 CRRなどは短いRPOを支えるが、サービスごとに書き込み昇格の要否が異なる。AWS Elastic Disaster Recoveryは、ブロックレベルの継続レプリケーションを使い、パイロットライトに近い低い待機費用で短いRTO/RPOを狙う別の選択肢である。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3

問題 094 | Domain 3 / 展開・自動化 | 複合難問 | 四択（1つ選択）

問題 94 Terraformのコードだけでなく、stateと実行経路を本番化する

ある企業は、GitHubで管理するTerraformを使って、12個のAWSアカウントに開発、検証、本番環境を構築している。現在は各担当者がローカルPCで terraform apply を実行し、terraform.tfstate もローカルに保存している。先月、2人が同時に本番へ適用してstateが不整合になり、その後PC故障で最新stateを失った。GitHub ActionsにはIAMユーザーの長期アクセスキーがSecretとして登録されている。

監査部門は次を要求している。

- 変更はPull Requestでplanを確認し、承認後に保護された経路からだけ本番へ適用する。
- 同時applyを防ぎ、stateを暗号化・世代管理し、誤変更から復旧できる。
- 開発、検証、本番、およびアカウント間でstateと権限の影響範囲を分離する。
- 長期アクセスキーを廃止し、どのリポジトリ・ブランチのワークフローがどのAWSロールを引き受けられるか制限する。
- stateに含まれ得る機密情報へ開発者が直接アクセスしない。
- 既に本番で手作業作成された一部リソースは、削除・再作成せずTerraform管理へ移したい。

最も適切な移行設計はどれか。

選択肢

A terraform.tfstate とロックファイルをGitリポジトリへコミットし、Gitのブランチ保護で同時更新を防ぐ。state内の文字列はbase64へ変換し、レビュー担当者がPR上で差分確認する

B 全アカウント・全環境で1つのS3バックエンドと1つのstateキーを共有し、DynamoDBロックを追加する。GitHub Actions専用IAMユーザーのアクセスキーを90日ごとにローテーションし、AdministratorAccessを付与する

C stateは担当者のPCに残し、applyが成功した後だけS3へバックアップコピーする。GitHub Actionsはplanだけを実行し、本番applyは承認者が各自のIAMユーザーでローカル実行する

D 環境・アカウントごとに分離したS3リモートバックエンドを用意し、暗号化、バージョニング、厳格なIAM、CloudTrail監査、Terraform 1.10以降のS3ネイティブstate lockingを有効にする。GitHub ActionsはOIDCでリポジトリ・ブランチ条件付きの環境別最小権限ロールを引き受け、PR検証・plan・承認済みapplyをパイプライン化する。既存リソースはimportしてplanを収束させ、秘密値はSecrets Manager等で管理してstateへの格納を最小化する

ここでいったん止める | 解答と解説は次ページ

問題 094 正解・解説 複合難問

問題 94の正解・解説

1. 正解

D

2. 問題文の重要な条件

- state消失と同時applyという、コード以外のTerraform運用問題が既に発生している。
- 環境・アカウントごとの影響範囲分離と、本番stateへの直接アクセス制限が必要である。
- GitHub Actionsから長期キーなしでAWSへ認証し、リポジトリやブランチを信頼条件に含めたい。
- 手作業リソースを破壊せず、Terraform stateへ安全に取り込む必要がある。

3. 正解へ至る判断過程

Terraform運用を、(1)コードレビュー、(2)state、(3)ロック、(4)実行ID、(5)環境分離、(6)既存資産の取り込みに分ける。Gitだけを整えてもstateの整合性は守れず、S3へ置くだけでも同時applyは止まらない。S3リモートstate、ネイティブロック、バージョニング、環境別バックエンド、OIDCでの短期資格情報、PRからapplyまでの保護経路を一体として設計する。既存リソースはコードを用意してimportし、差分を精査してから通常管理へ移る。

4. 正解が要件を満たす理由

S3バックエンドはstateをローカルPCから切り離し、耐久性、暗号化、アクセス制御、バージョニングを提供する。Terraform 1.10以降ではS3ネイティブstate lockingを使用でき、同じstateへの同時書き込みを防げる。S3 Versioningは誤ったstate更新や削除から過去版を回復する手掛かりになり、CloudTrailでstateバケットへのAPI操作を追跡できる。

環境・アカウントごとにバックエンドと実行ロールを分ければ、開発の誤操作が本番stateへ波及する範囲を狭められる。GitHub ActionsのOIDCトークンをIAMロールの信頼ポリシーで検証し、対象Organization、Repository、BranchまたはEnvironmentを条件にすれば、保存済みアクセスキーを廃止できる。本番変更はPRの静的検査とplan、承認、保護ブランチまたはEnvironmentからのapplyに限定する。planファイル自体にも機密値が含まれ得るため、保存する場合は成果物のアクセスと保持期間も制限する。

既存リソースは対応するTerraform構成を作成してimportし、plan が意図しない変更や再作成を示さなくなるまで属性とライフサイクルを調整する。importはコードを自動的に正しく設計する魔法ではないため、適用前のplan確認が不可欠である。

5. 各不正解選択肢が不適切な理由

- A：stateには機密属性が含まれ得るため、ソース管理へコミットすべきではない。Gitのマージロックは Terraformの実行中ロックではなく、base64は暗号化でもない。
- B：リモートstateとロックの方向はよいが、全環境を同じstateへ入れると影響範囲と権限制御を分離できない。DynamoDBロックは既存環境では使えるものの、S3ネイティブロックが推奨される現在、長期IAMキーとAdministratorAccessを残す理由はない。
- C：apply中は中央ロックがなく、別担当者は古いstateで同時実行できる。成功後バックアップでは、実行途中の障害やPC故障に弱い。人の長期資格情報とローカル本番applyも監査経路を分散させる。

6. 各不正解選択肢が正解になり得る条件

- A：Terraformコードとプロバイダロックファイルは Git管理するが、terraform.tfstate は除外する、という形なら一部は正しい。stateをGitへ置く選択はしない。

- B：既にDynamoDBロックを使う古いTerraform環境を段階移行し、stateキーとIAMロールを環境別に分け、OIDCへ変更する途中なら暫定構成になり得る。
- C：個人の一時的な学習環境で、共同作業も機密情報もなく、失っても再作成できる場合。それでも本番には適さない。

7. 今後使える判断基準

Terraformの本番問題では「HCLが正しいか」だけでなく、「誰がapplyするか」「どのstateへ書くか」「同時実行をどう止めるか」「stateを誰が読めるか」「過去版をどう戻すか」を確認する。stateはバックアップファイルではなく、現実のリソースと宣言を対応付ける重要データベースとして扱う。

8. 関連サービスとの比較

S3リモートバックエンドはAWS上で自己管理する軽量な方式で、HCP Terraformはリモート実行、ポリシー、承認などを含むマネージドな選択肢である。CloudFormationはAWSサービス側がスタック状態を管理するため、利用者が tfstate を設計する必要がない。AWS CDKも最終的にはCloudFormationスタックへ合成する。GitHub OIDCは認証を短期化する仕組みであり、TerraformのstateロックやPR承認を代替しない。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4

問題 095 | Domain 1 / 監視・性能 | 本番より難しい | 四択（1つ選択）

問題 95 REJECTの証拠と遮断箇所

プライベートサブネットのEC2アプリケーションから、別サブネットのRDSへTCP接続している。セキュリティ強化でネットワークACLとセキュリティグループを変更した後、特定のアプリケーションサブネットから開始した新規接続の一部だけがタイムアウトするようになった。既存接続は継続する場合があり、アプリケーションCPU、RDS CPU、DB接続上限には余裕がある。運用チームは、実際の通信がACCEPT/REJECTのどちらだったかを送信元・宛先・ポートと時間帯で確認し、さらに現在のVPC構成上、どのコンポーネントが経路を遮断するかをパケット送信なしで特定したい。ペイロードの取得は許可されない。

最も適切な診断方法はどれか。

選択肢

A 対象VPC、サブネットまたはENIでVPC Flow Logsを有効にし、必要なフィールドをCloudWatch LogsまたはS3で分析する。併せてVPC Reachability AnalyzerでEC2 ENIからRDSへのプロトコル・ポートを指定した経路解析を実行する

B Traffic Mirroringですべてのパケットを検査用EC2へ複製し、ペイロードを完全保存する。セキュリティグループとNACLは分析対象から外す

C CloudWatch agentの netstat 情報だけを両ホストで収集し、RDSホストへSession Managerでログインしてiptablesを変更する

D AWS Network Managerのグローバルネットワークだけを作成し、Cloud WANの地理マップからRDSのセキュリティグループ規則違反を自動修復する

ここでいったん止める | 解答と解説は次ページ

問題 095 正解・解説 本番より難しい

問題 95の正解・解説

1. 正解

A

2. 問題文の重要な条件

- 変更対象はSGとNACLであり、CPUやDB上限ではない。
- 実際に起きた通信のACCEPT/REJECTと5-tuple相当の情報が必要である。
- 現在の設定を静的に解析し、遮断コンポーネントを特定したい。
- ペイロード取得は禁止されている。
- RDS基盤ホストへログインできない。

3. 正解へ至る判断過程

過去または実際のフローの事実と、構成上の到達可能性を別々に調べる。VPC Flow LogsはENIを通るIPトラフィックのメタデータを記録し、ACCEPT/REJECT、アドレス、ポート、時刻を分析できる。Reachability Analyzerはパケットを送らずにVPC構成をモデル化し、到達可能ならホップ、不可なら遮断コンポーネントを示す。この二つでNACLの戻り用エフェメラルポート不足やSG参照ミスを絞り込む。

4. 正解が要件を満たす理由

Flow Logsはペイロードを含まず、監査要件を守りながら実トラフィックの許可・拒否を検証できる。集約間隔や配信遅延を踏まえて該当時刻を検索する。Reachability AnalyzerはSG、NACL、ルートなどの構成を経路として検査し、ブロック位置を示す。状態を持つSGと状態を持たないNACLの違いも、双方向の経路分析で確認できる。

5. 各不正解選択肢が不適切な理由

A: 正解肢のため対象外。
B: Traffic Mirroringは詳細パケット分析に使えるが、ペイロード保存禁止に反し、静的構成の遮断箇所を直接説明しない。全トラフィック複製の費用と運用も大きい。
C: agentのホスト情報だけではVPC側REJECTを十分に示せない。利用者はRDSホストへログインもiptables変更もできない。
D: Network Managerはグローバル・ハイブリッドネットワークの可視化に有用だが、単一VPC内のSG/NACL遮断をこの要件どおり解析・自動修復する手段ではない。

6. 各不正解選択肢が正解になり得る条件

B: IDS、プロトコル異常、アプリケーションペイロードなどL7に近いパケット内容を許可された検査基盤で解析する必要がある場合はTraffic Mirroringが適する。
C: 自己管理EC2同士で、OSのソケット枯渇やローカルファイアウォールが疑わしい場合はホストメトリクスとnetstatが役立つ。
D: Transit Gateway、Cloud WAN、Direct Connect、Site-to-Site VPNを含む広域トポロジーとリンク状態の運用ならNetwork Managerが適する。

7. 今後使える判断基準

Flow Logsは「実際のIPフローの記録」、Reachability Analyzerは「現在の構成上の経路」、Traffic Mirroringは「パケット内容」、Network Managerは「広域ネットワークの運用ビュー」で選ぶ。タイムアウトではアプリ、OS、VPC構成、経路、宛先サービスを一層ずつ確認する。

8. 関連サービスとの比較

CloudWatchのNAT Gateway、Transit Gateway、VPNなどのメトリクスは帯域・パケットドロップ・トンネル状態の傾向監視に向く。Flow Logsはフロー単位のメタデータ、Reachability Analyzerは構成の論理検証であり、継続的な帯域測定ツールではない。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4

問題 096 | Domain 2 / 信頼性・BC | 複合難問 | 複数選択（5つから3つ選択）

問題 96 active/activeを「DNSだけ」で作らない

イベント受付APIを東京とシドニーの2リージョンでmulti-site active/active化する。通常時から両リージョンがユーザートラフィックを処理し、一方のリージョンを退避しても受付を継続する。APIはステートレスで、イベントは冪等キー付きでDynamoDBへ書き込む。リージョン間の短い非同期複製遅延を許容し、同じイベントの重複はアプリケーションが排除できる。

目標はRTOほぼ0、低いRPOである。片側退避時には残りのリージョンが100%負荷を処理しなければならず、平常時に成功するDNS応答だけでなく、実際に退避可能であることを継続確認したい。設計に必要な対策を3つ選べ。

選択肢

A	Route 53のレイテンシー/重み付けルーティングとヘルス評価、または要件に合うGlobal Acceleratorを使い、両リージョンの正常なALBへ通常時からトラフィックを分散し、異常リージョンを除外する
B	DynamoDB global tablesを使用し、各リージョンのAPIはローカルレプリカへ読み書きする。冪等性・同時更新競合・複製遅延をアプリケーションと監視に含める
C	両リージョンで必要なサービスクォータ、外部依存、Auto Scaling最大容量、データアクセス権を事前確保し、片側100%負荷のゲームデー/リージョン退避を定期実施する
D	Aurora Global Databaseの各セカンダリクラスターへ通常時から同時に直接書き込み、DynamoDBは使用しない
E	復旧側のAuto Scaling希望容量を0にし、障害後に初めてネットワークとデータベースを作る

ここでいったん止める | 解答と解説は次ページ

問題 096 正解・解説 複合難問

問題 96の正解・解説

1. 正解

A、B、C

2. 問題文の重要な条件

- 両リージョンが通常時から処理するactive/active。
- ローカルで読み書きでき、短い非同期不一致と重複を扱える。
- 片側だけで全負荷を処理できることが必要。
- RTOほぼ0を机上ではなく訓練で確認する。

3. 正解へ至る判断過程

active/activeには、入口、アプリケーション容量、データの3層がすべてmulti-Region対応している必要がある。Aがトラフィック、Bがmulti-activeデータ、Cが実運用容量と復旧可能性を担う。DNSレコードだけを二重化しても、データが書けない、クォータが足りない、残り側がスケールできないならRTOは達成できない。

4. 正解が要件を満たす理由

- A：通常時から両リージョンへ配信し、ヘルス状態に基づいて障害リージョンを新規トラフィックから外せる。
- B：global tablesは各レプリカが読み書き可能なmulti-activeデータストアで、DB昇格待ちを避けられる。アプリケーションの冪等性は非同期複製中の再試行・競合リスクを吸収する。
- C：退避先が100%負荷を受けるためのクォータ、最大容量、依存先、権限を事前に確保し、定期試験で実効RTOを測る。これは構成図だけでは保証できない部分である。

5. 各不正解選択肢が不適切な理由

- D：Aurora Global Databaseは通常、1つのプライマリリージョンが書き込みを担当し、セカンダリは読み取り用である。各セカンダリを独立したmulti-writerとして直接更新する構成ではない。
- E：障害後に環境とデータ層を作るのはbackup and restoreまたはpilot light寄りで、通常時active/activeでもRTOほぼ0でもない。

6. 各不正解選択肢が正解になり得る条件

- D：各リージョンが読み取り中心で、書き込みを単一プライマリへ送るactive/passive/グローバル読み取り構成ならAurora Global Databaseが候補になる。
- E：RTOが長く、待機費用を最小化するbackup and restoreまたは限定的なpilot light戦略を採る場合。

7. 今後使える判断基準

active/activeは「両方にデプロイ済み」だけではない。通常時のトラフィック、ローカル書き込み可能なデータモデル、片側全負荷の容量、依存サービス、クォータ、シークレット/鍵、退避訓練まで成立して初めてRTOほぼ0を主張できる。

8. 関連サービスとの比較

Route 53はDNS TTLとリゾルバーキャッシュの影響を受け、Global Acceleratorは固定Anycast IPとエンドポイントヘルスに基づくネットワークレベルの切替を提供する。DynamoDB global tablesはmulti-active、Aurora Global DatabaseとElastiCache Global Datastoreは基本的に単一プライマリからセカンダリへの複製であり、フェイルオーバー時の昇格を考慮する。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4

問題 097 | Domain 3 / 展開・自動化 | 本番相当 | 複数選択（5つから2つ選択）

問題 97 AI調査員に広い変更権限を渡さず、観測文脈を渡す

ある企業の注文システムは、4つのAWSアカウントにあるECS、Lambda、DynamoDBと、オンプレミスの決済ゲートウェイで構成される。メトリクスとログはCloudWatchとSplunk、コードはGitHub、デプロイ履歴はCI/CD、インシデントはServiceNowで管理している。障害時には、別々の監視ツールから同じ原因に対するアラートが大量に発生し、担当者がコード変更、デプロイ、メトリクス、ログを手作業で時系列に並べるため、根本原因特定に時間がかかる。

運用部門はAWS DevOps Agentを使い、ServiceNowチケットを契機に関連イベントをまとめ、環境トポロジーと観測データを横断して調査し、根本原因と、検証・切り戻しを含む緩和案を得たい。ただし、本番リソースの変更は既存の承認付きSystems Manager AutomationまたはCI/CDからのみ実行し、AIサービスへ本番管理権限を与えない。調査過程も監査できなければならない。

この要件を満たす対策はどれか。**2つ選択せよ。**

選択肢

A 全ログを一つのCloudWatch Logsロググループへ複製し、固定キーワードのメトリクスフィルターだけで原因を決定する。DevOps AgentにはServiceNowとコードリポジトリを接続せず、誤った相関を避ける

B 対象アプリケーション用のDevOps Agent Spaceを作成し、必要なAWSアカウント・リソースをprimary/secondary account roleで範囲指定する。調査に必要な読み取り専用の最小権限を与え、CloudWatch、Splunk、GitHub、CI/CD、ServiceNowをそのSpaceへ接続して、チケットから調査を開始する

C DevOps Agentの役割にAdministratorAccessを付与し、提案された緩和策を本番へ自動適用させる。Agent Spaceの内部制御があるため、IAMの最小権限や既存承認は不要とする

D ServiceNowチケットをKiro IDEのファイル保存イベントへ変換し、各開発者PCのhookから本番AWS CLIコマンドを自動実行する。PCがオフラインの間は次回保存時にまとめて実行する

E 組織固有の調査手順、既知のノイズ除外、相関基準をDevOps Agent Skillsやagent instructionsとして管理し、調査journalとCloudTrailを監査する。Agentが提示した緩和計画は人が確認し、承認済みAutomationまたはCI/CDへ引き渡して実行する

ここでいったん止める | 解答と解説は次ページ

問題 097 正解・解説 本番相当

問題 97の正解・解説

1. 正解

B、E

2. 問題文の重要な条件

- AWS、オンプレミス、複数の観測・コード・チケットシステムをまたいだ相関が必要である。
- ServiceNowチケットから自動的に調査を開始し、重複イベントをまとめたい。
- DevOps Agentは調査と緩和計画に使うが、本番変更の承認・実行経路は既存の仕組みに残す。
- 複数アカウントのアクセス範囲、読み取り最小権限、調査過程の監査が必要である。

3. 正解へ至る判断過程

DevOps Agentへ大量の生データを無差別に渡すのではなく、Agent Spaceというセキュリティ境界に、対象アプリケーションのAWSアカウント、観測ツール、コード、デプロイ、チケットを接続する。調査に必要な読み取り範囲だけをロールで許可する。次に、会社固有のrunbookや相関ルールをSkill・instructionとして与え、journalとCloudTrailで判断とAPI利用を追跡する。緩和案の生成と、本番変更の実行権限は分離する。

4. 正解が要件を満たす理由

BのAgent Spaceは、どのAWSアカウント・リソースと外部統合へアクセスできるかを定義する主要な境界である。primary account roleと各secondary account roleを調査に必要な読み取りへ絞り、CloudWatch、Splunk、GitHub、CI/CD、ServiceNowを接続すると、アラートやチケットを起点にテレメトリ、コード変更、デプロイ履歴を相関できる。DevOps Agentは新しい外部イベントを既存調査へlink、skip、または新規調査としてtriageできる。

EのSkillsとinstructionsは、組織の調査方法、既知の誤検知、相関ロジックなどを再利用可能にする。Incident Investigationのjournalは推論ステップと行動を記録し、DevOps Agent APIはCloudTrailに記録される。標準のDevOps Agentツールは、チケットやサポートケース作成を除きリソースを変更できない制限があるため、緩和計画を人が確認し、既存のAutomationやCI/CDへ渡す責任分界は要件に合う。カスタムMCPツールを追加する場合も読み取り専用を基本にし、別の変更経路を安易に作らない。

5. 各不正解選択肢が不適切な理由

- A：ログ集約とメトリクスフィルターは個別検知には有用だが、Splunk、コード、デプロイ、チケット、リソース関係の相関を捨てている。固定キーワードだけで根本原因を決定するのも脆い。
- C：AWS公式のセキュリティ指針はAgent Spaceのロールを調査に必要な読み取り専用・最小権限にすることを推奨している。内部制御はIAM最小権限を不要にしない。標準ツールが本番リソースを自由に変更するという前提も誤りである。
- D：Kiroのhookは開発ワークスペースのイベントに応じた開発作業自動化であり、常時稼働するインシデント受付・相関基盤ではない。開発者PCから本番変更を行うと、可用性、資格情報、承認、監査の要件を破る。

6. 各不正解選択肢が正解になり得る条件

- A：単一システムの既知エラー文字列を安価に検出し、通知するだけで十分な場合。根本原因調査は別工程になる。
- C：AdministratorAccessが必要になるのは、DevOps Agentとは別の厳格に制御された自動化ロールで、対象・操作・承認を限定できない例外時だけである。通常運用の選択にはしない。
- D：Kiro hookをローカルのlint、テスト、ドキュメント更新など、失敗しても本番を変更しない開発作業に使う場合。

7. 今後使える判断基準

運用AIの問題では、(1)観測できる範囲、(2)推論・提案、(3)変更の実行、(4)監査を分離する。調査の質を上げるには関連データ源を接続するが、権限は読み取り最小限にする。提案が具体的でも、既存の変更承認とロールバック経路を迂回させない。

8. 関連サービスとの比較

AWS DevOps Agentは、環境トポロジー、テレメトリ、コード、デプロイ、チケットを相関したインシデント調査と予防提案に向く。CloudWatchアラームとEventBridgeは決定論的な条件検知・ルーティング、Systems Manager Automationは承認済みの実行可能runbook、Kiroは仕様からコード・テストを作る開発支援を担う。これらは競合ではなく、DevOps Agentの調査結果を人が承認し、AutomationやCI/CDで実行し、必要なコード変更をKiroで準備するという連携ができる。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4 / AWS公式 5

問題 098 | Domain 1 / 監視・性能 | 複合難問 | 四択（1つ選択）

問題 98 正常に起動する不良リリース

ECS on FargateのサービスがALBの背後で稼働し、RDSへアクセスしている。現在はECSのrolling deploymentを使用している。新しいタスク定義へ更新すると、すべてのタスクは起動しALBヘルスチェックにも合格するが、特定APIの5xx率とp95応答時間が段階的に上昇する。ECSのCPU・メモリには余裕があり、RDSのDB Loadと待機イベントは平常である。直前の安定版へ数分以内に自動で戻し、低トラフィック時の1件の5xxでは戻さず、十分なリクエスト数のもとでエラー率または遅延が継続した場合だけ失敗と判断したい。既存のdeployment方式を大きく変更せず、デプロイ後の原因調査ではサービス操作から関連トレースとログへ移りたい。

最も適切な構成はどれか。

選択肢

A ECS target trackingでCPU目標値を下げてタスク数を増やし、RDS Multi-AZの手動フェイルオーバーを同時に実施する。デプロイは成功扱いのままにする

B ALBの RequestCount と HTTPCode_Target_5XX_Count から求めた5xx率、および TargetResponseTime のp95を、メトリクス数式と必要に応じた複合条件でCloudWatch alarm化する。ECS rolling deploymentのCloudWatch alarmによる失敗検出とrollbackを有効化し、Application Signals/X-Rayと関連ログを用いてサービス操作を追跡する

C ECS deployment circuit breakerだけを有効にする。タスクが定常状態へ到達した後のアプリケーションエラーも、CPU値に関係なくcircuit breakerが自動検出すると仮定する

D EventBridgeで5xxログを1件検出するたびにSystems Manager Automationから UpdateService を呼び、直前と思われるタスク定義番号を推測して設定する。CloudWatch alarmは使用しない

ここでいったん止める | 解答と解説は次ページ

問題 098 正解・解説 複合難問

問題 98の正解・解説

1. 正解

B

2. 問題文の重要な条件

- 新タスクは起動・ヘルスチェックに成功するため、起動失敗だけを見る仕組みでは検知できない。
- 症状はアプリケーション5xxとp95遅延で、CPU、メモリ、DB Loadは平常である。
- 十分なリクエスト母数と継続時間を条件にし、低トラフィックの1件を除外する。
- rolling deploymentを維持し、直前の完了済み版へ自動rollbackしたい。
- 事後にサービス操作からトレース・ログへ相関したい。

3. 正解へ至る判断過程

まず、性能悪化をCPU不足やDB障害と決めつけず、デプロイに相関したアプリケーション指標で判断する。5xx率は分子とリクエスト数から算出し、最小トラフィック条件と複数評価期間を使う。p95遅延も別アラームにし、求める論理条件で通知・デプロイ失敗を構成する。ECSのrolling deploymentはCloudWatch alarmsを使ってアプリケーションメトリクスに基づく失敗とrollbackを行える。原因分析はApplication Signalsからサービス操作、X-Rayトレース、ログへ進む。

4. 正解が要件を満たす理由

Bは、タスク起動の成否では見えない論理的な不良リリースを実トラフィック指標で検知する。datapoints-to-alarmにより継続条件を表現し、メトリクス数式で率と母数を分離できる。ECSのデプロイ設定でCloudWatch alarm監視とrollbackを有効にすれば、失敗時に最後に正常完了したサービスリビジョンへ戻せる。Application Signalsは操作メトリクス、依存関係、関連トレース・ログをまとめ、DBが平常という仮説も検証しやすい。

5. 各不正解選択肢が不適切な理由

A: CPUに余裕があるためタスク追加はコード起因の5xxを直さない。DB Loadが平常なのにMulti-AZフェイルオーバーすると不要な可用性影響を与え、悪いリリースも残る。
B: 正解肢のため対象外。
C: deployment circuit breakerは主にタスクが起動・定常状態へ到達できないデプロイを検出する。ヘルスチェック通過後の業務エラーを任意のアプリケーション指標から自動推定するものではない。
D: 1件でのロールバックは誤検知に弱く、推測したリビジョンは安全でない。重複イベント、権限、失敗時再試行、競合を独自実装するよりECSのデプロイ失敗・rollback統合が適切である。

6. 各不正解選択肢が正解になり得る条件

A: 原因がCPU飽和による容量不足で、バージョンに依存せずtarget trackingで安定化できる場合はスケールアウトが正しい。RDSフェイルオーバーはプライマリ障害時に検討する。
C: 新タスクが起動できない、コンテナが終了する、またはヘルスチェックに合格せず定常状態へ到達できないことだけが失敗条件ならcircuit breakerが適する。
D: ECS以外も含む特殊な復旧手順で、組み込みrollbackでは表現できず、承認・冪等性・正確な版管理をrunbookへ実装済みならAutomationを使う余地がある。

7. 今後使える判断基準

デプロイ障害を「起動できない」と「起動するが振る舞いが悪い」に分ける。前者はcircuit breakerやヘルスチェック、後者はエラー率・遅延・業務KPIのCloudWatch alarmで検出する。率のアラームには母数、継続時間、欠損・少数標本の扱いを必ず含める。

8. 関連サービスとの比較

ECS deployment circuit breakerとCloudWatch alarm監視はいずれもrolling deploymentの失敗検出とrollbackに使えるが、見ている信号が異なる。blue/greenやcanary/linear deploymentは本番トラフィックを段階移行してリスクをさらに下げられる一方、一時的な二重容量やdeployment方式の変更が伴う。Application Signalsは診断、CloudWatch alarmsは判定、ECSはrollback実行を担当する。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4

問題 099 | Domain 2 / 信頼性・BC | 複合難問 | 四択（1つ選択）

問題 99 DB昇格、容量拡張、DNS切替を一つの復旧計画へ

ある業務システムは2リージョンのwarm standby構成である。プライマリではEC2 Auto Scalingグループが30台、Aurora Global Databaseのライターが本番サイズで稼働する。スタンバイではAuto Scalingグループ3台と小さいAuroraインスタンスを維持し、Route 53のactive/passiveレコードを用意している。

現在の復旧手順は、担当者が複数のCLIスクリプトを順番に実行している。過去の訓練では、DNSを先に切り替えてからスタンバイ容量を増やしてしまい、過負荷になった。新要件では、次の処理を観測可能な一つの計画として順序制御し、定期的に設定・権限の不備を評価したい。正常な両リージョン間で行う計画保守のDB switchover直前には別担当者の承認を必須とし、実障害では権限を持つインシデント責任者がデータ損失可能性のあるungraceful実行を明示的に選ぶ。

1. スタンバイのAuroraとEC2容量を本番相当へ拡張
2. 計画保守ならAurora switchover、実障害ならデータ損失可能性を明示したfailover
3. Route 53でトラフィック切替

最も適切な改善はどれか。

選択肢

A	3つのCLIスクリプトを1つの大きなシェルスクリプトに連結し、運用端末のcronから四半期ごとに実行する
B	ARCルーティングコントロールだけを導入してDNS切替を行い、Aurora昇格とAuto Scaling拡張は従来どおり別の手動作業にする
C	CloudFormationスタック更新で両リージョンの希望容量、DBロール、DNSレコードを毎回書き換え、変更セットの完了順には依存しない
D	Amazon Application Recovery Controller（ARC）Region switchプランを作成し、Aurora Provisioned Scaling、EC2 Auto Scaling、計画切替用の手動承認、Aurora Global Database、Route 53ヘルスチェック（または重要度に応じARC routing control）の実行ブロックを依存順に配置する。graceful/ungracefulの動作とプラン評価結果を訓練で検証する

ここでいったん止める | 解答と解説は次ページ

問題 099 正解・解説 複合難問

問題 99の正解・解説

1. 正解

D

2. 問題文の重要な条件

- 複数サービスの復旧手順を順序制御する。
- 容量確保前のDNS切替を防ぐ。
- 計画切替と障害切替でAuroraの動作を分ける。
- 計画切替の手動承認、観測可能性、定期的な設定/権限評価が必要。

3. 正解へ至る判断過程

ARC Region switchは、multi-Regionアプリケーションの復旧をワークフローと実行ブロックでオーケストレーションする。Auto Scaling、Auroraの容量変更とswitchover/failover、Route 53、手動承認を同じ計画へ組み込み、直列または並列の依存関係を表現できる。定期的なプラン評価も、単なるスクリプトとの決定的な差である。

4. 正解が要件を満たす理由

Region switchのEC2 Auto Scaling実行ブロックはソース容量に対する割合で宛先を拡張し、Aurora Provisioned Scalingは宛先インスタンスを本番相当にする。Aurora Global Databaseブロックはgracefulなswitchoverまたはungracefulなfailoverを実行できる。計画切替のワークフローでは手動承認ブロックで処理を停止できる。実障害用のungraceful構成は、手動承認ブロックがungracefulをサポートしない点を踏まえて権限と起動手順を分ける。Route 53ブロックで最後にトラフィックを切り替え、プラン評価はリソース、構成、実行ロール権限などの問題を事前に示す。

5. 各不正解選択肢が不適切な理由

- A：順序を記述できても、分散した権限・リソースの継続評価、組み込み承認、graceful/ungracefulの意味付け、実行状況の統合表示を自作する必要がある。
- B：DNSの安全な切替には有効だが、容量拡張とDB昇格の順序事故を解消しない。ルーティングコントロールは単独では復旧全体のオーケストレーターではない。
- C：DBロール切替は単なる宣言的プロパティ変更ではなく、データ同期/損失判断を伴う運用操作である。依存順を無視すれば同じ過負荷を再発させる。

6. 各不正解選択肢が正解になり得る条件

- A：対象が少数で、専用実行ブロックが対応しない独自処理を、十分にテストされた補助手順として実行する場合。
- B：アプリケーションとデータが両リージョンで既に本番容量・書き込み可能で、必要な操作がトラフィック切替だけの場合。
- C：通常の構成変更や、フェイルオーバー以外の再現可能なインフラ展開を行う場合。

7. 今後使える判断基準

DR手順が複数サービスと依存順序を持つなら、単一操作の機能と復旧オーケストレーションを区別する。Route 53/ARC routing controlは主に入口、Aurora failoverはDB、Auto Scalingは容量であり、それらを「容量->データ->トラフィック」のように安全な順序へ束ねるのがRegion switchである。

8. 関連サービスとの比較

ARC routing controlは100% SLAの高信頼なトラフィックスイッチと安全ルールを提供する。Region switchのRoute 53ヘルスチェック実行ブロックは、多くの用途でより低コストにDNS切替を計画へ統合できる。AWS Step Functionsでも独自オーケストレーションは作れるが、Region switchは復旧向けの実行ブロック、計画評価、graceful/ungracefulモード、承認を組み込みで提供する。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4 / AWS公式 5

問題 100 | Domain 3 / 展開・自動化 | 本番相当 | 四択（1つ選択）

問題 100 運用変更の仕様化と、本番実行を分離する

ある運用チームは、Terraformモジュール、Lambdaの運用ツール、Systems Manager Automation runbookを一つのGitリポジトリで管理している。インシデントの再発防止として「ECSデプロイ失敗時のアラームと自動ロールバックを標準化する」という変更依頼を受けたが、過去には担当者が要件をすぐコード化したため、受け入れ条件、設計判断、テスト、ロールバック手順がレビュー時に欠けていた。

今回は、依頼をユーザーストーリーと受け入れ条件へ分解し、設計と実装タスクを追跡したい。既存のタグ規約、Terraform構成、セキュリティ制約を生成内容へ常に反映し、ファイル保存時には該当するlintと単体テストを自動実行したい。ただし、生成されたコードは必ずPull Requestでレビューし、既存CI/CDの承認後にだけAWSへ適用する。IDE上の自動化に本番資格情報は持たせない。

最も適切な構成はどれか。

選択肢

A EventBridgeでGitのファイル保存イベントを受信し、Lambdaから各開発者のローカルリポジトリへ設計書とテストを直接書き込む。本番用IAMロールもLambdaへ付与して、保存のたびにapplyする

B AWS DevOps Agentだけに本番の読み書き権限を与え、過去インシデントからコードを生成して直接デプロイさせる。要件、設計、タスクの文書化とPull Requestは省略する

C Kiroでspecを作成して requirements.md、design.md、tasks.md に要件・設計・作業を分け、workspace steeringへタグ規約、技術スタック、セキュリティ制約を記述する。対象ファイルのイベントに対するagent hookでlintやテストを実行し、成果物はGitのPull Requestと既存CI/CDを通して承認・適用する

D Systems Manager State Manager associationを開発者PCへ配布し、30分ごとにリポジトリ内のTerraformコードを書き換える。associationがCompliantならコードレビューとCIテストは不要とする

ここでいったん止める | 解答と解説は次ページ

問題 100 正解・解説 本番相当

問題 100の正解・解説

1. 正解

C

2. 問題文の重要な条件

- 高水準の依頼を、追跡可能な要件、設計、実装タスクへ分解したい。
- リポジトリ固有の標準や制約を、生成・修正時の継続的な文脈として与えたい。
- ファイルイベントでlintとテストを自動化したい。
- 生成支援と本番適用は分離し、Pull Request、CI/CD、承認を残す。

3. 正解へ至る判断過程

求められているのは常時稼働するAWSリソースの自動修復ではなく、変更を仕様化して実装・テストする開発ワークフローである。Kiroのspecは要件・設計・タスクの構造化、steeringはプロジェクト文脈、agent hookはIDEイベントに応じた反復作業に対応する。一方、Kiroが生成した内容の正しさと本番承認は別問題なので、Gitと既存CI/CDを境界として残す。

4. 正解が要件を満たす理由

Kiroのspecは、高水準の機能や修正依頼を、ユーザーストーリー・受け入れ条件を持つ requirements.md、技術設計の design.md、追跡可能な tasks.md へ分ける。workspace steeringは .kiro/steering/ 配下で、そのリポジトリに固有の製品文脈、技術スタック、規約、セキュリティ要件をエージェントへ継続的に伝えられる。

agent hookは、ファイルの作成・保存・削除、プロンプト、ツール実行、specタスクなどのイベントでエージェントプロンプトまたはシェルコマンドを起動できる。Terraformファイルだけにformat・validate・lint、Lambdaコードには単体テストというように対象を絞れば、反復確認を自動化できる。hookの成功は本番安全性の保証ではないため、差分、spec、テスト結果をPull Requestで人が確認し、AWS資格情報を持つ既存CI/CDが承認後に適用する。

5. 各不正解選択肢が不適切な理由

- A：EventBridgeはAWSやSaaSイベントのルーティングに向くが、各IDEのローカルファイル保存を標準で検出し、ローカルファイルへ書き戻す開発機能ではない。保存ごとの本番applyは承認要件にも反する。
- B：DevOps Agentはインシデント調査、緩和計画、予防提案に使えるが、仕様・設計・タスクを省略して本番へ直接変更する構成は要件に反する。標準ツールが本番リソースを自由に変更するという前提も誤りである。
- D：State ManagerはSystems Managerマネージドノードの望ましい実行時状態を維持するもので、開発者のソースコード設計やPRレビューを置き換えない。Compliantはコードの業務要件充足を意味しない。

6. 各不正解選択肢が正解になり得る条件

- A：S3オブジェクト作成やCodePipeline状態変更など、AWS上のイベントを複数ターゲットへルーティングする場合。ローカルIDE操作とは分ける。
- B：DevOps Agentで過去インシデントを分析し、再発防止の緩和案やKiroへ渡すagent-ready instructionsを作る場合。コード変更と適用にはレビュー経路を残す。
- D：対象がEC2などのマネージドノードで、エージェント設定やサービス状態を定期的に維持したい場合。

7. 今後使える判断基準

生成AIを選ぶ問題でも、対象ライフサイクルを確認する。IDE内で要件からコード・テストを作るならKiro、稼働環境のインシデント相関ならDevOps Agent、AWSイベントの決定論的な配送ならEventBridge、ノード状態の維持ならState Managerである。生成できることと、本番へ無承認で適用してよいことは同義ではない。

8. 関連サービスとの比較

Kiroのspec・steering・hookは、構造化された開発とIDE内自動化を支援する。AWS DevOps Agentは稼働環境の調査から緩和計画やagent-ready instructionsを生成でき、Kiroへ実装作業をつなげられる。GitHub Actions、CodeBuild、CodePipelineなどのCI/CDは、再現可能な検査、資格情報、承認、本番適用の実行境界を担う。Systems Manager Automationは、既に承認された運用runbookをAWS環境で実行するもので、仕様策定の代替ではない。

公式確認先 AWS公式 1 / AWS公式 2 / AWS公式 3 / AWS公式 4 / AWS公式 5

基準資料

本書は次のAWS公式公開資料を基準にしています。各問末尾の「AWS公式」リンクは、その設問で特に重要な仕様を確認できるページです。サービス仕様は変更される可能性があるため、受験直前には試験ガイドのrevisionとin-scope servicesを再確認してください。

AWS Certified CloudOps Engineer - Associate Exam Guide (SOA-C03)

SOA-C03 Revisions - Version 1.1 (2026-06-01)

SOA-C03 In-Scope AWS Services

100問 完了
一問ずつ、設計条件の差を見抜くための問題集