AWS Certified DevOps Engineer - Professional (DOP-C02) Exam Guide

はじめに

AWS Certified DevOps Engineer - Professional (DOP-C02) 試験は、DevOps エンジニアロールを担う個人を対象としています。この試験では、AWS での分散システムおよびサービスのプロビジョン、運用、および管理についての受験者の技術的な専門知識を検証します。

また、次のタスクについての受験者の能力も検証します。

- AWS での継続的デリバリーシステムとその配信方法を実装および管理する。
- セキュリティコントロール、ガバナンスプロセス、コンプライアンス検証を実装および自動化する。
- AWS でのモニタリング、メトリクス、ロギングシステムを定義およびデプロイする。
- AWS での可用性、スケーラビリティ、自己修復性の高いシステムを実装する。
- 運用プロセスを自動化するためのツールを設計、管理、および保守する。

受験対象者について

受験者には、AWS 環境でのプロビジョン、運用、管理に関する 2 年以上の経験が必要です。受験対象者は、ソフトウェア開発ライフサイクルとプログラミングおよび/またはスクリプティングの経験が必要です。

推奨される IT 全般に関する知識と経験

受験対象者には、以下の経験が求められます。

- 高度に自動化されたインフラストラクチャの構築に関する経験
- オペレーティングシステムの管理に関する経験
- 最新の開発プロセス、運用プロセス、開発手法、運用手法に関する経験

推奨される AWS の知識と経験

受験対象者には、AWS インフラストラクチャのセキュリティ保護の経験が求められます。

受験対象者として範囲外の職務

受験対象者が実施できることが想定されていない職務は、以下のリストのとおりです。このリストはすべてを網羅しているわけではありません。以下のタスクは、本試験の範囲外です。

- 高度なネットワークに関する知識 (高度なルーティングアルゴリズム、フェイルオーバーの手法など) を身に付けている。
- デベロッパーに対して高度なセキュリティに関する推奨事項を提供する。
- データベースの設計、クエリ、パフォーマンスの最適化を行う。
- フルスタックアプリケーションのコード開発を行う。

試験に出題される可能性のあるテクノロジーと概念のリストと、範囲内の AWS サービスと機能のリストについては、付録を参照してください。

試験内容

解答タイプ

試験には次の 2 種類の設問があります。

- **択一選択問題:** 正しい選択肢が 1 つ、誤った選択肢 (不正解) が 3 つ提示される。
- **複数選択問題:** 5 つ以上の選択肢のうち、正解が 2 つ以上ある。

設問の記述に最もよく当てはまるもの、または正解となるものを 1 つ以上選択します。不正解の選択肢は、知識や技術が不十分な受験者が選択してしまいそうな、設問内容と一致するもっともらしい解答になっています。

設問に対して未回答の場合は不正解とみなされます。推測による回答についてのペナルティはありません。試験には、スコアに影響する設問が 65 問含まれています。

採点対象外の設問

試験には、スコアに影響しない採点対象外の設問が 10 問含まれています。AWS では、このような採点対象外の設問での成績情報を収集し、今後採点対象の設問として使用できるかどうかを評価します。試験では、どの設問が採点対象外かは受験者にわからないようになっています。

試験の結果

AWS Certified DevOps Engineer - Professional (DOP-C02) 試験は、合否判定方式です。試験の採点は、認定業界のベストプラクティスおよびガイドラインに基づいた、AWS の専門家によって定められる最低基準に照らして行われます。

試験の結果は、100～1,000 のスケールスコアとして報告されます。合格スコアは 750 です。このスコアにより、試験全体の成績と合否がわかります。複数の試験間で難易度がわずかに異なる可能性があるため、スコアを均等化するためにスケールスコアが使用されます。

スコアレポートには、各セクションの成績を示す分類表が含まれる場合があります。試験には補整スコアリングモデルが使用されるため、セクションごとに合否ラインは設定されておらず、試験全体のスコアで合否が判定されます。

試験の各セクションには特定の重みが設定されているため、各セクションに割り当てられる設問数が異なる場合があります。分類表には、受験者の得意な部分と弱点を示す全般的な情報が含まれます。セクションごとのフィードバックを解釈する際は注意してください。

試験内容の概要

この試験ガイドには、セクションに設定された重み、コンテンツ分野、タスクステートメントについての説明が含まれています。本ガイドは、試験内容の包括的なリストを提供するものではありません。ただし、各タスクステートメントの追加情報を使って、試験の準備に役立てることができます。

本試験のコンテンツ分野と重み設定は以下のとおりです。

- 第 1 分野: SDLC のオートメーション (採点対象コンテンツの 22%)
- 第 2 分野: 設定管理と IaC (採点対象コンテンツの 17%)
- 第 3 分野: 耐障害性の高いクラウドソリューション (採点対象コンテンツの 15%)
- 第 4 分野: モニタリングとロギング (採点対象コンテンツの 15%)
- 第 5 分野: インシデントとイベントへの対応 (採点対象コンテンツの 14%)
- 第 6 分野: セキュリティとコンプライアンス (採点対象コンテンツの 17%)

第 1 分野: SDLC のオートメーション

タスクステートメント 1.1: CI/CD パイプラインを実装する。

対象知識:

- ソフトウェア開発ライフサイクル (SDLC) の概念、フェーズ、モデル
- シングルアカウントとマルチアカウント環境のパイプラインデプロイパターン

対象スキル:

- コード、イメージ、アーティファクトリポジトリの設定
- バージョン管理を使用してパイプラインをアプリケーション環境に統合
- 構築プロセスのセットアップ (AWS CodeBuild など)
- 構築とデプロイのシークレットの管理 (AWS Secrets Manager、AWS Systems Manager Parameter Store など)
- 適切なデプロイ戦略の決定 (AWS CodeDeploy など)

タスクステートメント 1.2: 自動テストを CI/CD パイプラインに統合する。

対象知識:

- 各種テスト (単体テスト、統合テスト、受け入れテスト、ユーザーインターフェイステスト、セキュリティスキャンなど)
- CI/CD パイプラインの各段階でさまざまなタイプのテストを合理的に使用

対象スキル:

- プルリクエストまたはコードマージを生成するときに構築またはテストを実行 (AWS CodeCommit、CodeBuild など)
- 負荷/ストレステスト、パフォーマンスベンチマーキング、アプリケーションテストを大規模環境で実行
- アプリケーション終了コードに基づいてアプリケーションのヘルスを測定
- 単位テストとコードカバレッジの自動化
- テストのためパイプラインでの AWS サービスの呼び出し

タスクステートメント 1.3: アーティファクトを構築して管理する。

対象知識:

- アーティファクトのユースケースとセキュアな管理
- アーティファクトを作成および生成するメソッド
- アーティファクトのライフサイクルに関する注意事項

対象スキル:

- アーティファクトリポジトリの作成と設定 (AWS CodeArtifact、Amazon S3、Amazon Elastic Container Registry [Amazon ECR] など)
- アーティファクトを生成する構築ツールの設定 (CodeBuild、AWS Lambda など)
- Amazon EC2 インスタンスとコンテナイメージの構築プロセスの自動化 (EC2 Image Builder など)

タスクステートメント 1.4: インスタンス、コンテナ、サーバーレス環境のデプロイ戦略を実装する。

対象知識:

- さまざまなプラットフォームのデプロイ方法 (Amazon EC2、Amazon Elastic Container Service [Amazon ECS]、Amazon Elastic Kubernetes Service [Amazon EKS]、Lambda など)
- アプリケーションストレージパターン (Amazon Elastic File System [Amazon EFS]、Amazon S3、Amazon Elastic Block Store [Amazon EBS] など)
- ミュータブルなデプロイパターンとイミュータブルなデプロイパターンの比較
- コードの配布に使用できるツールとサービス (CodeDeploy、EC2 Image Builder など)

対象スキル:

- アーティファクトリポジトリへのアクセスを許可するセキュリティ権限の設定 (AWS Identity and Access Management [IAM]、CodeArtifact など)
- デプロイメントエージェントの設定 (CodeDeploy エージェントなど)
- デプロイに関する問題のトラブルシューティング
- さまざまなデプロイ方法の使用 (blue/green、Canary など)

第 2 分野: 設定管理と IaC

タスクステートメント 2.1: クラウドインフラストラクチャと再利用可能なコンポーネントを定義して、ライフサイクル全体でシステムをプロビジョンおよび管理する。

対象知識:

- AWS の Infrastructure as Code (IaC) のオプションとツール
- IaC ベースのプラットフォームの変更管理プロセス
- 設定管理サービスと戦略

対象スキル:

- IaC テンプレートの作成とデプロイ (AWS Serverless Application Model [AWS SAM]、AWS CloudFormation、AWS Cloud Development Kit [AWS CDK] など)
- CloudFormation StackSets を複数のアカウントと複数の AWS リージョンに適用
- 最適な設定管理サービスを決定 (AWS OpsWorks、AWS Systems Manager、AWS Config、AWS AppConfig など)
- インフラストラクチャのパターン、ガバナンスコントロール、セキュリティ標準を再利用可能な IaC テンプレート (AWS Service Catalog、CloudFormation モジュール、AWS CDK など) に実装

タスクステートメント 2.2: オートメーションをデプロイして、マルチアカウント環境またはマルチリージョン環境で AWS アカウントを作成、オンボーディング、保護する。

対象知識:

- AWS アカウント構造、ベストプラクティス、および関連する AWS サービス

対象スキル:

- アカウントのプロビジョンと設定の標準化と自動化
- アカウントの作成、統合、および一元管理 (AWS Organizations、AWS Control Tower など)
- 複数アカウントや複雑な組織構造 (SCP、ロールを引き受けるなど) に IAM ソリューションを適用
- 大規模環境でのガバナンスとセキュリティコントロールの実装と開発 (AWS Config、AWS Control Tower、AWS Security Hub、Amazon Detective、Amazon GuardDuty、AWS Service Catalog、SCP)

タスクステートメント 2.3: 複雑なタスクや大規模環境向けの自動化ソリューションを設計および構築する。

対象知識:

- タスクとプロセスを自動化する AWS のサービスとソリューション
- AWS ソフトウェア定義インフラストラクチャとのインタラクション方法と戦略

対象スキル:

- システムインベントリ、設定、およびパッチ管理の自動化 (Systems Manager、AWS Config など)
- 複雑なシナリオ (AWS SDK、Lambda、AWS Step Functions など) 向けに Lambda 関数オートメーションを開発
- ソフトウェアアプリケーションを希望の状態に自動設定 (OpsWorks、Systems Manager ステートマネージャーなど)
- ソフトウェアコンプライアンスの維持 (Systems Manager など)

第 3 分野: 耐障害性の高いクラウドソリューション

タスクステートメント 3.1: 耐障害性とビジネス要件を満たす高可用性ソリューションを実装する。

対象知識:

- マルチ AZ およびマルチリージョンデプロイ (コンピューティングレイヤー、データレイヤーなど)
- SLA
- ステートフルサービスのためのレプリケーションとフェイルオーバーの方法
- 高可用性を実現する手法 (マルチ AZ、マルチリージョンなど)

対象スキル:

- ビジネス要件を技術的耐障害性のニーズに変換
- 既存のワークロードで単一障害点を特定して修正
- 利用可能な場合はクロスリージョンソリューションを有効化 (Amazon DynamoDB、Amazon RDS、Amazon Route 53、Amazon S3、Amazon CloudFront など)
- クロス AZ サービスをサポートするためにロードバランシングを設定
- ダウンタイムを最小限に抑えながら、複数のアベイラビリティーゾーンとリージョンをサポートするようにアプリケーションと関連サービスを設定

タスクステートメント 3.2: ビジネス要件を満たすスケーラブルなソリューションを実装する。

対象知識:

- サービスをスケーリングするための適切なメトリクス
- 疎結合および分散アーキテクチャ
- サーバーレスアーキテクチャ
- コンテナプラットフォーム

対象スキル:

- スケーリングに関する問題を特定して修正
- 適切なオートスケーリング、ロードバランシング、およびキャッシュソリューションを特定して実装
- コンテナベースのアプリケーション (Amazon ECS、Amazon EKS など) のデプロイ
- 複数のリージョンにワークロードをデプロイしてグローバルなスケーラビリティを実現
- サーバーレスアプリケーションの設定 (Amazon API Gateway、Lambda、AWS Fargate など)

タスクステートメント 3.3: RTO 要件と RPO 要件を満たす自動復旧プロセスを実装する。

対象知識:

- 災害対策の概念 (RTO、RPO など)
- バックアップと復旧戦略 (パイロットライト、ウォームスタンバイなど)
- 復旧手順

対象スキル:

- マルチ AZ とマルチリージョンのワークロード (Amazon RDS、Amazon Aurora、Route 53、CloudFront など) のフェイルオーバーのテスト
- 適切なリージョン間バックアップとリカバリ戦略 (AWS Backup、Amazon S3、Systems Manager など) の特定と実装
- バックエンドの障害から復旧するためのロードバランサーの設定

第 4 分野: モニタリングとロギング

タスクステートメント 4.1: ログとメトリクスの収集、集計、および保存を設定する。

対象知識:

- アプリケーションとインフラストラクチャをモニタリングする方法
- Amazon CloudWatch メトリクス (名前空間、メトリクス、ディメンション、解像度など)
- リアルタイムのログ取り込み
- 保存中および転送中のログとメトリクスの暗号化オプション (クライアント側とサーバー側、AWS Key Management Service [AWS KMS] など)
- セキュリティ設定 (ログ収集を許可する IAM ロールや権限など)

対象スキル:

- ログをセキュアに保存して管理
- メトリクスフィルターを使用してログイベントから CloudWatch メトリクスを作成
- CloudWatch メトリクスストリームの作成 (Amazon S3 または Amazon Kinesis Data Firehose オプションなど)
- カスタムメトリクスの収集 (CloudWatch エージェントの使用など)
- ログストレージライフサイクルの管理 (S3 ライフサイクル、CloudWatch Log グループの保持など)
- CloudWatch Log サブスクリプションを使用してログデータを処理 (Kinesis、Lambda、Amazon OpenSearch Service など)
- フィルターとパターン構文または CloudWatch Logs Insights を使用してログデータを検索
- ログデータの暗号化の設定 (AWS KMS など)

タスクステートメント 4.2: ログとメトリクスを監査、モニタリング、分析して問題を検出する。

対象知識:

- 異常検出アラーム (CloudWatch 異常検知など)
- 一般的な CloudWatch メトリクスとログ (Amazon EC2 の CPU 使用率、Amazon RDS でのキュー長、Application Load Balancer (ALB) の 5xx エラーなど)
- Amazon Inspector と一般的な評価テンプレート

- AWS Config ルール
- AWS CloudTrail ログイベント

対象スキル:

- CloudWatch ダッシュボードと Amazon QuickSight ビジュアライゼーションの構築
- CloudWatch アラームと CloudWatch メトリクス (標準およびカスタム) との関連付け
- さまざまなサービス (コンテナ、API Gateway、Lambda など) 用に AWS X-Ray を設定
- リアルタイムログストリームの分析 (Kinesis Data Streams の使用など)
- AWS のサービスでのログの分析 (Amazon Athena、CloudWatch Logs Insights など)

タスクステートメント 4.3: 複雑な環境のモニタリングとイベント管理を自動化する。

対象知識:

- イベント駆動型の非同期設計パターン (S3 イベント通知または Amazon Simple Notification Service [Amazon SNS] または Lambda に対する Amazon EventBridge イベントなど)
- さまざまな AWS サービスのオートスケーリング機能 (EC2 Auto Scaling グループ、RDS ストレージオートスケーリング、DynamoDB、ECS キャパシティープロバイダー、EKS オートスケーラーなど)
- アラート通知とアクション機能 (Amazon SNS、Lambda、EC2 の自動復旧に対する CloudWatch アラームなど)
- AWS サービスのヘルスチェック機能 (ALB ターゲットグループ、Route 53 など)

対象スキル:

- オートスケーリングのソリューションの設定 (DynamoDB、EC2 Auto Scaling グループ、RDS ストレージのオートスケーリング、ECS キャパシティープロバイダーなど)
- CloudWatch カスタムメトリクスとメトリクスフィルター、アラーム、通知 (Amazon SNS、Lambda など) の作成
- ログファイルを処理し (例えば Lambda を使用)、ログファイルを (OpenSearch Service、CloudWatch Logs などの) 別の送信先に配信するように S3 イベントを設定

- 特定のイベントパターンに基づいて通知を送信するように EventBridge を設定
- EC2 インスタンスにエージェントをインストールして設定 (AWS Systems Manager Agent [SSM Agent]、CloudWatch エージェントなど)
- 問題を修復するために AWS Config ルールを設定
- ヘルスチェックを設定 (Route 53、ALB など)

第 5 分野: インシデントとイベントへの対応

タスクステートメント 5.1: イベントソースを管理して、イベントを処理、通知し、イベントに応じてアクションを実行する。

対象知識:

- イベントを生成、キャプチャ、処理する AWS のサービス (AWS Health、EventBridge、CloudTrail など)
- イベント駆動型アーキテクチャ (ファンアウト、イベントストリーミング、キューイングなど)

対象スキル:

- AWS イベントソースの統合 (AWS Health、EventBridge、CloudTrail など)
- イベント処理ワークフローの構築 (Amazon Simple Queue Service [Amazon SQS]、Kinesis, Amazon SNS, Lambda, Step Functions など)

タスクステートメント 5.2: イベントに応じて設定の変更を実装する。

対象知識:

- フリート管理サービス (Systems Manager、AWS Auto Scaling など)
- 設定管理サービス (AWS Config など)

対象スキル:

- 設定の変更をシステムに適用
- イベントに応じたインフラストラクチャ設定の変更
- 望ましくないシステム状態の修復

タスクステートメント 5.3: システムとアプリケーションの障害をトラブルシューティングする。

対象知識:

- AWS メトリクスとロギングサービス (CloudWatch、X-Ray など)

- AWS サービスのヘルスサービス (AWS Health, CloudWatch, Systems Manager OpsCenter など)
- 根本原因分析

対象スキル:

- 失敗したデプロイの分析 (AWS CodePipeline、CodeBuild、CodeDeploy、CloudFormation、CloudWatch 模擬モニタリングなど)
- 失敗したプロセスに関するインシデントの分析 (オートスケーリング、Amazon ECS、Amazon EKS など)

第 6 分野: セキュリティとコンプライアンス

タスクステートメント 6.1: Identity and Access Management の手法を大規模環境に実装する。

対象知識:

- 人間とマシンのアクセスに対するさまざまな IAM エンティティ (ユーザー、グループ、ロール、ID プロバイダー、ID ベースのポリシー、リソースベースのポリシー、セッションポリシーなど) の適切な使用
- ID フェデレーション手法 (IAM ID プロバイダーと AWS IAM アイデンティティセンター [AWS Single Sign-On] の使用など)
- IAM アクセス許可の境界を使用したアクセス許可管理の委任
- 組織 SCP

対象スキル:

- 最小権限アクセスを強制するポリシーの設計
- ロールベースおよび属性ベースのアクセス制御パターンの実装
- マシン ID (Secrets Manager など) の認証情報ローテーションの自動化
- 人間とマシン ID へのアクセスを制御するアクセス許可の管理 (多要素認証 [MFA]、AWS Security Token Service [AWS STS]、IAM プロファイルの有効化など)

タスクステートメント 6.2: セキュリティコントロールとデータ保護のオートメーションを適用する。

対象知識:

- ネットワークセキュリティコンポーネント (セキュリティグループ、ネットワーク ACL、ルーティング、AWS Network Firewall、AWS WAF、AWS Shield など)
- 証明書とパブリックキーインフラストラクチャ (PKI)
- データ管理 (データ分類、暗号化、キー管理、アクセスコントロールなど)

対象スキル:

- マルチアカウント環境とマルチリージョン環境におけるセキュリティコントロール適用の
  自動化 (Security Hub、Organizations、AWS Control Tower、Systems Manager など)
- セキュリティコントロールを組み合わせた多層防御の適用 (AWS Certificate Manager [ACM]、AWS WAF、AWS Config、AWS Config ルール、Security Hub、GuardDuty、セキュリティグループ、ネットワーク ACL、Amazon Detective、Network Firewall など)
- 大規模環境における機密データの検出の自動化 (Amazon Macie など)
- 転送中のデータと保存中のデータの暗号化 (AWS KMS、AWS CloudHSM、ACM など)

タスクステートメント 6.3: セキュリティモニタリングおよび監査ソリューションを実装する。

対象知識:

- セキュリティモニタリングサービスと機能 (CloudTrail、AWS Config、VPC フローログ、CloudFormation ドリフト検出など)
- セキュリティの脆弱性とイベントを特定するための AWS のサービス (GuardDuty、Amazon Inspector、IAM Access Analyzer、AWS Config など)
- 一般的なクラウドセキュリティの脅威 (セキュアでないウェブトラフィック、公開された AWS アクセスキー、パブリックアクセスが有効か、または暗号化が無効な S3 バケットなど)

対象スキル:

- 堅牢なセキュリティ監査の実装

- 予期しない、または異常なセキュリティイベントに基づくアラートの設定
- サービスとアプリケーションのロギングの設定 (CloudTrail、CloudWatch Logs など)
- ログ、メトリクス、セキュリティ結果の分析

付録

試験に出題される可能性のあるテクノロジーと概念

以下は、試験に出題される可能性のあるテクノロジーと概念のリストです。このリストはすべてを網羅しているわけではなく、また、変更される場合があります。このリストにおける項目の掲載順序や配置は、その項目の相対的な重みや試験における重要性を示すものではありません。

- アプリケーションのデプロイ
- アプリケーション統合
- アプリケーションパイプライン
- オートメーション
- コードリポジトリのベストプラクティス
- コスト最適化
- デプロイの要件
- ハイブリッドデプロイ
- IAM Policy
- メトリクス、モニタリング、アラーム、ロギング
- ネットワーク ACL およびセキュリティグループの設計と実装
- 運用上のベストプラクティス
- ロールバック手順

範囲内の AWS のサービスと機能

以下に、試験範囲の AWS のサービスと機能のリストを示します。このリストはすべてを網羅しているわけではなく、また、変更される場合があります。各 AWS のサービスは、サービスの主な機能に応じたカテゴリに分けられています。

分析:

- Amazon Athena
- Amazon EMR
- Amazon Kinesis Data Firehose
- Amazon Kinesis Data Streams
- Amazon OpenSearch Service
- Amazon QuickSight

アプリケーション統合:

- Amazon AppFlow
- Amazon EventBridge

コンピューティング:

- AWS App Runner
- Amazon EC2
- Amazon EC2 Auto Scaling
- EC2 Image Builder
- AWS Elastic Beanstalk
- AWS Serverless Application Repository

コンテナ:

- AWS App2Container
- AWS Copilot
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon Elastic Container Service (Amazon ECS)
- Amazon Elastic Kubernetes Service (Amazon EKS)
- Amazon EKS Distro
- AWS Fargate
- Red Hat OpenShift Service on AWS (ROSA)

データベース:

- Amazon Aurora
- Amazon Aurora Serverless v2
- AWS Database Migration Service (AWS DMS)
- Amazon DocumentDB (MongoDB 互換)
- Amazon DynamoDB
- Amazon ElastiCache
- Amazon MemoryDB for Redis
- Amazon RDS
- Amazon Redshift

デベロッパーツール:

- AWS CLI
- AWS Cloud Development Kit (AWS CDK)
- AWS CloudShell
- AWS CodeArtifact
- AWS CodeBuild
- AWS CodeCommit
- AWS CodeDeploy
- Amazon CodeGuru
- AWS CodePipeline
- AWS CodeStar
- AWS Fault Injection Simulator (AWS FIS)
- AWS SDK とツール
- AWS X-Ray

マネジメントとガバナンス:

- AWS Auto Scaling
- AWS CloudFormation
- AWS CloudTrail
- Amazon CloudWatch
- Amazon CloudWatch Logs
- AWS Compute Optimizer
- AWS Config
- AWS Control Tower
- AWS Health
- AWS License Manager
- Amazon Managed Grafana
- Amazon Managed Service for Prometheus
- AWS OpsWorks
- AWS Organizations
- AWS Proton
- AWS Resilience Hub
- AWS Service Catalog
- AWS Systems Manager
- AWS Trusted Advisor

ネットワークとコンテンツ配信:

- Amazon API Gateway
- AWS Client VPN
- Amazon CloudFront
- Elastic Load Balancing (ELB)
- AWS PrivateLink
- Amazon Route 53
- AWS Site-to-Site VPN
- AWS Transit Gateway
- Amazon VPC

セキュリティ、アイデンティティ、コンプライアンス:

- AWS Certificate Manager (ACM)
- AWS CloudHSM
- Amazon Cognito
- Amazon Detective
- AWS Directory Service
- Amazon GuardDuty
- AWS IAM アイデンティティセンター (AWS Single Sign-On)
- AWS Identity and Access Management (IAM)
- Amazon Inspector
- AWS Key Management Service (AWS KMS)
- Amazon Macie
- AWS Network Firewall
- AWS Resource Access Manager (AWS RAM)
- AWS Secrets Manager
- AWS Security Hub
- AWS Security Token Service (AWS STS)
- AWS Shield
- AWS WAF

サーバーレス:

- AWS Lambda
- AWS Serverless Application Model (AWS SAM)
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Queue Service (Amazon SQS)
- AWS Step Functions

ストレージ:

- AWS Backup
- Amazon Elastic Block Store (Amazon EBS)
- AWS Elastic Disaster Recovery
- Amazon Elastic File System (Amazon EFS)
- Amazon FSx for Lustre
- Amazon FSx for NetApp ONTAP
- Amazon FSx for OpenZFS
- Amazon FSx for Windows File Server
- Amazon S3
- Amazon S3 Glacier
- AWS Storage Gateway

アンケート

この試験ガイドはどの程度役に立ちましたか？ アンケートに答えてお知らせください。