



AMS の高度な概念と手順

# AMS Advanced ユーザーガイド



Version March 31, 2026

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

# AMS Advanced ユーザーガイド: AMS の高度な概念と手順

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標およびトレードドレスは Amazon 以外の製品およびサービスに使用することはできません。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使用することもできません。Amazon が所有していない他のすべての商標は、それぞれの所有者の所有物であり、Amazon と提携、接続、または後援されている場合とされていない場合があります。

# Table of Contents

|                                                             |    |
|-------------------------------------------------------------|----|
| AWS Managed Services とは .....                               | 1  |
| 本ガイドについて .....                                              | 2  |
| 運用計画 .....                                                  | 2  |
| 運用計画の迅速化 .....                                              | 3  |
| 高度な運用計画 .....                                               | 3  |
| はじめに .....                                                  | 3  |
| 重要な用語 .....                                                 | 4  |
| サービスの説明 .....                                               | 10 |
| AWS Managed Services (AMS) AMS Advanced オペレーションプランの機能 ..... | 11 |
| 何をするか、何をしないか .....                                          | 16 |
| AMS 責任マトリックス (RACI) .....                                   | 17 |
| AMS 環境の基本コンポーネント .....                                      | 39 |
| AMS アカウントの制限 .....                                          | 42 |
| AMS サービスレベル目標 (SLOs) .....                                  | 44 |
| サポートされている AWS サービス .....                                    | 45 |
| サポートされている設定 .....                                           | 48 |
| サポートされていないオペレーティングシステム .....                                | 51 |
| AMS Advanced インターフェイス .....                                 | 52 |
| VPC エンドポイント .....                                           | 53 |
| AMS で保護された名前空間 .....                                        | 54 |
| AMS 予約プレフィックス .....                                         | 55 |
| AMS メンテナンスウィンドウ .....                                       | 56 |
| AMS 情報リソース .....                                            | 57 |
| AMS コンプライアンス .....                                          | 58 |
| AMS でサポートされているコンプライアンス標準 .....                              | 58 |
| 共有責任 .....                                                  | 61 |
| AMS Amazon マシンイメージ (AMIs) .....                             | 61 |
| セキュリティ強化 AMIs .....                                         | 65 |
| AD FS と AMS の統合の仕組み .....                                   | 65 |
| AMS Managed Active Directory .....                          | 66 |
| アプリケーションのデプロイ .....                                         | 69 |
| サービス管理 .....                                                | 71 |
| アカウントガバナンス .....                                            | 71 |
| サービス開始 .....                                                | 71 |

|                                           |     |
|-------------------------------------------|-----|
| 顧客関係管理 (CRM) .....                        | 72  |
| CRM プロセス .....                            | 73  |
| CRM 会議 .....                              | 73  |
| CRM ミーティングの手配 .....                       | 75  |
| CRM 月次レポート .....                          | 75  |
| コスト最適化 .....                              | 76  |
| コスト最適化フレームワーク .....                       | 77  |
| コスト最適化責任マトリックス .....                      | 79  |
| サービス時間 .....                              | 81  |
| ヘルプの利用 .....                              | 81  |
| 計画されたイベント管理 .....                         | 82  |
| AMS PEM 基準 .....                          | 82  |
| PEM のタイプ .....                            | 82  |
| AMS PEM プロセス .....                        | 83  |
| PEM FAQs .....                            | 83  |
| ネットワークアーキテクチャ .....                       | 85  |
| MALZ ネットワークアーキテクチャ .....                  | 85  |
| マルチアカウントランディングゾーンのネットワークアーキテクチャについて ..... | 85  |
| 単一の MALZ または複数の MALZs の選択 .....           | 88  |
| マルチアカウントランディングゾーンアカウント .....              | 93  |
| SALZ ネットワークアーキテクチャ .....                  | 116 |
| AMS シングルアカウントランディングゾーン共有サービス .....        | 117 |
| AMS のセットアップ .....                         | 119 |
| AMS のデフォルト設定 .....                        | 120 |
| DNS 解決のデフォルト (MALZ) .....                 | 120 |
| EC2 IAM インスタンスプロファイル .....                | 121 |
| AMS でのベースラインモニタリングからのアラート .....           | 128 |
| ログの保持とローテーションのデフォルト .....                 | 149 |
| AMS コンソールの使用 .....                        | 149 |
| AMS API と CLI の使用 .....                   | 151 |
| REST コール用の AMS API HTTP エンドポイント .....     | 151 |
| AMS CLI のインストールまたはアップグレード .....           | 152 |
| CLI、Ruby、Python、Java での AMS API の使用 ..... | 153 |
| AMS が独自の EPS を導入する .....                  | 163 |
| アカウントの BYOEPS を有効にする .....                | 165 |
| AMS 通知の受信 .....                           | 167 |

|                                                   |     |
|---------------------------------------------------|-----|
| SNS を使用した AMS AMI 通知 .....                        | 169 |
| サービス通知 .....                                      | 173 |
| RFC 状態変更通知 .....                                  | 173 |
| プライベート DNS とパブリック DNS のセットアップ .....               | 177 |
| AMS 出カトラフィック管理 .....                              | 179 |
| IAM リソースのデプロイ .....                               | 180 |
| 自動 IAM プロビジョニング .....                             | 181 |
| IAM ロールとプロファイルを使用したアクセス許可の設定 .....                | 203 |
| 新しい IAM ユーザーロールまたはインスタンスプロファイルのリクエスト .....        | 203 |
| IAM ロールポリシーステートメントを使用してアクセス許可を制限する .....          | 204 |
| Amazon EC2 IAM インスタンスプロファイルを使用してアクセス許可を制限する ..... | 206 |
| AD FS クレームルールと SAML 設定 .....                      | 206 |
| ADFS クレームルールの設定 .....                             | 207 |
| ウェブコンソール .....                                    | 208 |
| SAML による API および CLI アクセス .....                   | 208 |
| ネットワーク ACL で制限する .....                            | 211 |
| Outposts での AMS .....                             | 212 |
| AWS Outposts インストールと運用管理 .....                    | 212 |
| での AMS マネージドリソースのプロビジョニング AWS Outposts .....      | 215 |
| での AMS の制限 AWS Outposts .....                     | 215 |
| AWS Outposts コンプライアンスに関する AMS .....               | 216 |
| AMS on AWS Outposts FAQs .....                    | 217 |
| タグの使用 .....                                       | 219 |
| AMS インフラストラクチャの自動タグ付け .....                       | 221 |
| AMS 推奨タグ .....                                    | 222 |
| タグ一括更新ノート .....                                   | 226 |
| Resource Scheduler .....                          | 228 |
| Resource Scheduler のデプロイ .....                    | 229 |
| Resource Scheduler のカスタマイズ .....                  | 229 |
| Resource Scheduler の使用 .....                      | 230 |
| AMS Resource Scheduler のコスト見積りツール .....           | 231 |
| AMS Resource Scheduler のベストプラクティス .....           | 232 |
| AWS Systems Manager AMS Advanced の .....          | 234 |
| 利用可能な AMS Advanced SSM ドキュメント .....               | 234 |
| AMS Advanced SSM ドキュメントバージョン .....                | 235 |
| Systems Manager の料金 .....                         | 235 |

|                                       |     |
|---------------------------------------|-----|
| AMS アカウントのオフボード .....                 | 235 |
| シングルアカウントランディングゾーンアカウントからのオフボード ..... | 236 |
| マルチアカウントランディングゾーンアカウントからのオフボード .....  | 240 |
| 変更管理モード .....                         | 261 |
| モードの概要 .....                          | 262 |
| AMS のモードとアカウントのタイプ .....              | 262 |
| AMS モードとアプリケーションまたはワークロード .....       | 266 |
| AMS モードの実際のユースケース .....               | 273 |
| RFC モード .....                         | 276 |
| RFCs の詳細 .....                        | 277 |
| 変更タイプとは? .....                        | 315 |
| RFC エラーのトラブルシューティング .....             | 328 |
| 直接変更モード .....                         | 338 |
| 直接変更モードの開始方法 .....                    | 339 |
| セキュリティとコンプライアンス .....                 | 341 |
| Direct Change モードでの変更管理 .....         | 346 |
| Direct Change モードを使用したスタックの作成 .....   | 348 |
| 直接変更モードのユースケース .....                  | 352 |
| デベロッパーモード .....                       | 352 |
| デベロッパーモードの開始方法 .....                  | 353 |
| セキュリティとコンプライアンス .....                 | 356 |
| 変更管理 .....                            | 357 |
| インフラストラクチャーのプロビジョニングをします。 .....       | 363 |
| 「発見的コントロール」 .....                     | 364 |
| ログ記録、モニタリング、イベント管理 .....              | 364 |
| インシデント管理 .....                        | 364 |
| パッチ管理 .....                           | 365 |
| 継続性管理 .....                           | 365 |
| セキュリティとアクセスの管理 .....                  | 365 |
| AMS でのセルフサービスプロビジョニングモード .....        | 365 |
| AMS での SSP モードの開始方法 .....             | 366 |
| Amazon API Gateway .....              | 367 |
| Alexa for Business .....              | 368 |
| Amazon WorkSpaces Applications .....  | 370 |
| Amazon Athena .....                   | 373 |
| Amazon Bedrock .....                  | 374 |

|                                                 |     |
|-------------------------------------------------|-----|
| Amazon CloudSearch .....                        | 375 |
| Amazon CloudWatch Synthetics .....              | 376 |
| Amazon Cognito .....                            | 377 |
| Amazon Comprehend .....                         | 379 |
| Amazon Connect .....                            | 380 |
| Amazon Data Firehose .....                      | 382 |
| Amazon DevOps Guru .....                        | 383 |
| Amazon DocumentDB (MongoDB 互換性) .....           | 384 |
| Amazon DynamoDB .....                           | 385 |
| Amazon Elastic Container Registry .....         | 387 |
| EC2 イメージビルダー .....                              | 388 |
| での Amazon ECS AWS Fargate .....                 | 390 |
| での Amazon EKS AWS Fargate .....                 | 392 |
| Amazon EMR .....                                | 395 |
| Amazon EventBridge .....                        | 398 |
| Amazon Forecast .....                           | 400 |
| Amazon FSx .....                                | 403 |
| Amazon FSx for OpenZFS .....                    | 405 |
| Amazon FSx for NetApp ONTAP .....               | 406 |
| Amazon Inspector Classic .....                  | 408 |
| Amazon Kendra .....                             | 409 |
| Amazon Kinesis Data Streams .....               | 410 |
| Amazon Kinesis Video Streams .....              | 411 |
| Amazon Lex .....                                | 412 |
| Amazon MQ .....                                 | 413 |
| Amazon Managed Service for Apache Flink .....   | 414 |
| Amazon Managed Streaming for Apache Kafka ..... | 415 |
| Amazon Managed Service for Prometheus .....     | 416 |
| Amazon Personalize .....                        | 417 |
| Amazon Quick .....                              | 420 |
| Amazon Rekognition .....                        | 422 |
| Amazon SageMaker AI .....                       | 423 |
| Amazon Simple Email Service .....               | 426 |
| Amazon Simple Workflow Service .....            | 428 |
| Amazon Textract .....                           | 429 |
| Amazon Transcribe .....                         | 429 |

|                                         |     |
|-----------------------------------------|-----|
| Amazon WorkSpaces .....                 | 431 |
| AMS コードサービス .....                       | 433 |
| AWS Amplify .....                       | 436 |
| AWS AppSync .....                       | 437 |
| AWS App Mesh .....                      | 438 |
| AWS Audit Manager .....                 | 439 |
| AWS Batch .....                         | 440 |
| AWS Certificate Manager .....           | 441 |
| AWS Private Certificate Authority ..... | 443 |
| AWS CloudEndure .....                   | 445 |
| AWS CloudHSM .....                      | 447 |
| AWS CodeBuild .....                     | 448 |
| AWS CodeCommit .....                    | 450 |
| AWS CodeDeploy .....                    | 451 |
| AWS CodePipeline .....                  | 453 |
| AWS Compute Optimizer .....             | 454 |
| AWS DataSync .....                      | 456 |
| AWS Device Farm .....                   | 457 |
| AWS Elastic Disaster Recovery .....     | 458 |
| AWS Elemental MediaConvert .....        | 460 |
| AWS Elemental MediaLive .....           | 461 |
| AWS Elemental MediaPackage .....        | 462 |
| AWS Elemental MediaStore .....          | 463 |
| AWS Elemental MediaTailor .....         | 464 |
| AWS Global Accelerator .....            | 465 |
| AWS Glue .....                          | 465 |
| AWS Lake Formation .....                | 467 |
| AWS Lambda .....                        | 468 |
| AWS License Manager .....               | 470 |
| AWS Migration Hub .....                 | 471 |
| AWS Outposts .....                      | 472 |
| AWS Resilience Hub .....                | 472 |
| AWS Secrets Manager .....               | 474 |
| AWS Security Hub CSPM .....             | 477 |
| AWS Service Catalog AppRegistry .....   | 478 |
| AWS Shield .....                        | 479 |



|                                           |     |
|-------------------------------------------|-----|
| AWS Snowball Edge .....                   | 480 |
| AWS Step Functions .....                  | 482 |
| AWS Systems Manager パラメータストア .....        | 483 |
| AWS Systems Manager Automation .....      | 484 |
| AWS Transfer Family .....                 | 487 |
| AWS Transit Gateway .....                 | 489 |
| AWS WAF .....                             | 490 |
| AWS Well-Architected Tool .....           | 491 |
| AWS X-Ray .....                           | 492 |
| VM Import/Export .....                    | 493 |
| カスタマーマネージドモード .....                       | 495 |
| カスタマーマネージドモードの開始方法 .....                  | 495 |
| AMS と AWS Service Catalog .....           | 495 |
| Service Catalog の開始方法 .....               | 496 |
| 開始する前に AMS の Service Catalog .....        | 496 |
| 必要なデータの検索 (SKMS) .....                    | 500 |
| サービスナレッジ管理とは .....                        | 500 |
| VPC IDs の検索 .....                         | 501 |
| サブネット IDs .....                           | 503 |
| AMI IDs .....                             | 506 |
| セキュリティグループ (SG) IDs .....                 | 507 |
| IAM エンティティの検索 .....                       | 507 |
| スタック IDs .....                            | 508 |
| インスタンス IDs または IP アドレスを検索する .....         | 510 |
| ARNs の検索 .....                            | 513 |
| ARN でリソースを検索する .....                      | 515 |
| アカウント設定の検索 .....                          | 516 |
| FQDNs の検索 .....                           | 517 |
| アベイラビリティゾーン (AZs) .....                   | 518 |
| SNS トピックの検索 .....                         | 519 |
| バックアップ設定の検索 .....                         | 519 |
| アクセス管理 .....                              | 521 |
| アクセス管理とは .....                            | 521 |
| アカウントにアクセスする理由とタイミング .....                | 522 |
| root を使用する方法とタイミング .....                  | 527 |
| AMS Advanced コンソールと Amazon EC2 アクセス ..... | 528 |

|                                                                  |     |
|------------------------------------------------------------------|-----|
| AWS マネジメントコンソールと AMS コンソールへのアクセス .....                           | 529 |
| AMS コンソールへの一時的なアクセス .....                                        | 529 |
| 踏み台を使用したインスタンスへのアクセス .....                                       | 530 |
| DNS フレンドリ踏み台名 .....                                              | 532 |
| 単一アカウントランディングゾーン (SALZ) 踏み台でのコスト削減 .....                         | 533 |
| 踏み台 IP アドレスの使用 .....                                             | 534 |
| インスタンスアクセスの例 .....                                               | 534 |
| AMS アカウントのチームまたはロールベースのアクセスコントロール .....                          | 545 |
| EC2 インスタンスの自動設定 .....                                            | 546 |
| 自動インスタンス設定の前提条件 .....                                            | 546 |
| SSM エージェントの自動インストール .....                                        | 547 |
| 前提条件 .....                                                       | 547 |
| SSM エージェントの自動インストールをリクエストする .....                                | 548 |
| SSM Agent 自動インストールの仕組み .....                                     | 549 |
| 自動変更 .....                                                       | 549 |
| Linux インスタンスでコードを自動的に更新する .....                                  | 549 |
| Linux インスタンスで PBIS を自動的に更新する .....                               | 550 |
| SSM エージェントの最小バージョンと CloudWatch エージェントを自動的に更新する .....             | 551 |
| CloudWatch 設定ファイル、更新の詳細 .....                                    | 552 |
| 自動的に設定されたログ .....                                                | 553 |
| モニタリングとイベント管理 .....                                              | 555 |
| モニタリングとは .....                                                   | 556 |
| AMS モニタリングシステムは何をモニタリングしますか？ .....                               | 557 |
| Active Directory Trust の単一アカウントランディングゾーンのプロアクティブモニタリン<br>グ ..... | 558 |
| モニタリングの仕組み .....                                                 | 558 |
| EC2 インスタンスグループ化通知 .....                                          | 560 |
| タグベースのアラート通知 .....                                               | 561 |
| アカウントのモニタリング設定の表示 .....                                          | 562 |
| アカウントのモニタリング設定の変更 .....                                          | 562 |
| AMS でのアプリケーション対応インシデント通知 .....                                   | 563 |
| AMS アカウントに AppRegistry をプロビジョニングし、アプリケーションを作成する .....            | 563 |
| タグを作成してケースエンリッチメントを有効にする .....                                   | 564 |
| アプリケーションの AMS サポートケースの重要度をカスタマイズする .....                         | 564 |
| 必要なアクセス許可を確認する .....                                             | 565 |
| OpsCenter の使用 .....                                              | 566 |

|                                                                  |     |
|------------------------------------------------------------------|-----|
| アラート通知 .....                                                     | 566 |
| アラートの受信 .....                                                    | 566 |
| タグベースのアラート通知 .....                                               | 567 |
| アラートの AMS 自動修復 .....                                             | 568 |
| 追加の CloudWatch アラームの作成 .....                                     | 578 |
| カスタム CloudWatch メトリクスとアラームの作成 .....                              | 579 |
| .Net および SQL Server での CloudWatch Application Insights の使用 ..... | 581 |
| AMS イベントルーター .....                                               | 581 |
| AMS によってデプロイされた Amazon EventBridge マネージドルール .....                | 582 |
| AMS のマネージドルールの作成 .....                                           | 582 |
| AMS のマネージドルールの編集 .....                                           | 582 |
| AMS のマネージドルールの削除 .....                                           | 583 |
| Trusted Remediator .....                                         | 583 |
| 主な利点 .....                                                       | 583 |
| Trusted Remediator の仕組み .....                                    | 584 |
| 重要な用語 .....                                                      | 584 |
| 信頼できる修復の開始方法 .....                                               | 586 |
| サポートされている Compute Optimizer の推奨事項 .....                          | 588 |
| サポートされている Trusted Advisor チェック .....                             | 592 |
| サポートされている Security Hub CSPM の推奨事項 .....                          | 646 |
| チェック修復を設定する .....                                                | 648 |
| 実行モード決定ワークフロー .....                                              | 652 |
| 修復チュートリアルを設定する .....                                             | 652 |
| 修復の操作 .....                                                      | 655 |
| 修復ログ .....                                                       | 659 |
| ベストプラクティス .....                                                  | 663 |
| よくある質問 .....                                                     | 663 |
| ログ管理 .....                                                       | 666 |
| ログ管理とは .....                                                     | 666 |
| AMS ログ記録の仕組み .....                                               | 666 |
| ログのアクセス .....                                                    | 667 |
| AMS 集計サービスログ .....                                               | 667 |
| AMS 共有サービスログ .....                                               | 680 |
| Amazon Elastic Compute Cloud (Amazon EC2) - システムレベルのログ .....     | 683 |
| Splunk との統合 .....                                                | 684 |
| ログ設定のカスタマイズ .....                                                | 685 |

|                                              |     |
|----------------------------------------------|-----|
| CloudWatch のログ保持期間の変更 .....                  | 685 |
| サポートされているサービスのログ記録の有効化 .....                 | 685 |
| セキュリティ管理 .....                               | 687 |
| AMS でのデータ保護 .....                            | 687 |
| Amazon Macie .....                           | 688 |
| GuardDuty .....                              | 689 |
| Amazon Route 53 Resolver DNS ファイアウォール .....  | 692 |
| AWS Certificate Manager (ACM) 証明書 .....      | 694 |
| AMS でのデータの暗号化 .....                          | 694 |
| ID とアクセス管理 .....                             | 696 |
| マルチアカウントランディングゾーン (MALZ) IAM 保護 .....        | 696 |
| アイデンティティを使用した認証 .....                        | 697 |
| セキュリティイベントのロギングとモニタリング .....                 | 719 |
| エンドポイントセキュリティ (EPS) .....                    | 719 |
| マルウェアの軽減プロセス .....                           | 724 |
| Amazon Inspector のセキュリティ .....               | 725 |
| AMS インシデント対応 .....                           | 727 |
| コンプライアンス検証 .....                             | 728 |
| のコンプライアンスステータスを表示するマルチアカウントランディングゾーン AWS     |     |
| Config ルール .....                             | 729 |
| AMS マルチアカウントランディングゾーンサービスコントロールポリシーの制限 ..... | 730 |
| 耐障害性 .....                                   | 730 |
| インフラストラクチャセキュリティ .....                       | 730 |
| セキュリティのベストプラクティス .....                       | 763 |
| AMS マルチアカウントランディングゾーン EPS のデフォルト以外の設定 .....  | 763 |
| AMS ガードレール .....                             | 763 |
| MALZ サービスコントロールポリシー .....                    | 763 |
| Security Incident Response .....             | 763 |
| 仕組み .....                                    | 764 |
| 準備 .....                                     | 765 |
| 検出 .....                                     | 766 |
| 分析 .....                                     | 766 |
| 封じ込め .....                                   | 767 |
| 根絶 .....                                     | 769 |
| 復旧 .....                                     | 770 |
| インシデント後レポート .....                            | 770 |

|                                         |     |
|-----------------------------------------|-----|
| セキュリティインシデント対応ランブック .....               | 771 |
| AMS Advanced での変更リクエストのセキュリティレビュー ..... | 777 |
| カスタマーセキュリティリスク管理プロセス .....              | 777 |
| AMS Advanced 技術標準 .....                 | 778 |
| AMS Advanced の標準コントロール .....            | 779 |
| 環境に高い、または非常に高いセキュリティリスクをもたらす変更 .....    | 804 |
| 継続性管理 .....                             | 807 |
| 継続性管理とは .....                           | 807 |
| 継続性管理の仕組み .....                         | 807 |
| バックアッププラン .....                         | 808 |
| バックアップポールト .....                        | 811 |
| バックアップ変更タイプ .....                       | 812 |
| バックアップのモニタリングとレポート .....                | 813 |
| ディザスタリカバリレスポンス .....                    | 814 |
| ディザスタリカバリ計画 .....                       | 814 |
| マルチサイトまたは高可用性 (HA) .....                | 815 |
| ウォームスタンバイ .....                         | 816 |
| パイロットライト .....                          | 817 |
| バックアップと復元 .....                         | 818 |
| パッチ管理 .....                             | 823 |
| AMS パッチオーケストレーター: タグベースのパッチ適用モデル .....  | 824 |
| パッチオーケストレーターの使用 .....                   | 826 |
| パッチオーケストレーターの前提条件 .....                 | 829 |
| パッチウィンドウ .....                          | 831 |
| パッチ通知 .....                             | 832 |
| パッチベースライン .....                         | 835 |
| パッチオーケストレーターの予約済みタグ .....               | 835 |
| オンデマンドパッチ適用 .....                       | 835 |
| AMS 標準パッチ適用 .....                       | 836 |
| サポートされるオペレーティングシステム .....               | 837 |
| サポートされているパッチ .....                      | 837 |
| パッチ適用とインフラストラクチャ設計 .....                | 840 |
| AMS 標準パッチの仕組み .....                     | 841 |
| AMS 標準パッチ適用の失敗 .....                    | 846 |
| AMS 標準パッチ適用で実行できるアクション .....            | 846 |
| AMS 標準パッチ適用FAQs .....                   | 849 |

|                                                           |     |
|-----------------------------------------------------------|-----|
| サービスコミットメントのパッチ適用 .....                                   | 852 |
| 標準パッチ適用 .....                                             | 852 |
| 重要なパッチ適用 .....                                            | 853 |
| レポートとオプション .....                                          | 857 |
| リクエスト時レポート .....                                          | 857 |
| AMS パッチレポート .....                                         | 858 |
| AMS Backup レポート .....                                     | 866 |
| Incidents Prevented and Monitoring Top Talkers レポート ..... | 869 |
| 請求料金の詳細レポート .....                                         | 871 |
| 信頼できる修復レポート .....                                         | 872 |
| セルフサービスレポート .....                                         | 875 |
| 内部 API オペレーション .....                                      | 876 |
| パッチレポート (毎日) .....                                        | 879 |
| バックアップレポート (毎日) .....                                     | 889 |
| インシデントレポート (毎週) .....                                     | 893 |
| 請求レポート (毎月) .....                                         | 896 |
| 集計レポート .....                                              | 899 |
| AMS セルフサービスレポートダッシュボード .....                              | 901 |
| データ保持ポリシー .....                                           | 908 |
| SSR からのオフボード .....                                        | 909 |
| サポートを受ける .....                                            | 910 |
| インシデント管理 .....                                            | 910 |
| インシデント管理とは? .....                                         | 912 |
| インシデント管理サービスのコミットメント .....                                | 913 |
| インシデント管理の例 .....                                          | 916 |
| サービスリクエスト管理 .....                                         | 922 |
| サービスリクエストを使用するタイミング .....                                 | 923 |
| サービスリクエスト管理の仕組み .....                                     | 923 |
| サービスリクエストのテスト .....                                       | 924 |
| サービスリクエストの作成 .....                                        | 924 |
| サービスリクエストのモニタリングと更新 .....                                 | 927 |
| AMS で生成されたサービスリクエストへの応答 .....                             | 928 |
| 請求に関する質問 .....                                            | 929 |
| オペレーションオンデマンド .....                                       | 930 |
| オンデマンドでの AMS オペレーションのリクエスト .....                          | 936 |
| Operations on Demand サービスに変更を加える .....                    | 937 |

ドキュメント履歴 ..... 938

以前の更新 ..... 959

..... cmlxxxix

# AWS Managed Services とは

Amazon Web Services (AWS) のインフラストラクチャオペレーション管理である AWS Managed Services (AMS) へようこそAWS。AMS は、AWS インフラストラクチャを継続的に管理するエンタープライズサービスです。

このユーザーガイドは、IT およびアプリケーション開発者向けです。IT 機能、ネットワーク、アプリケーションのデプロイに関する用語とプラクティスの基本的な理解が前提です。

AMS はベストプラクティスを実装し、運用上のオーバーヘッドとリスクを軽減するためにインフラストラクチャを維持します。AMS は、インフラストラクチャをプロビジョニング、実行、サポートするためのフルライフサイクルサービスを提供し、変更リクエスト、モニタリング、パッチ管理、セキュリティ、バックアップサービスなどの一般的なアクティビティを自動化します。AMS は、企業およびセキュリティインフラストラクチャポリシーを適用し、任意の開発アプローチを使用してソリューションとアプリケーションを開発できるようにします。

AMS アーキテクチャをよりよく理解するには、[以下の図](#)を参照してください。

## トピック

- [この AMS ユーザーガイドについて](#)
- [AMS オペレーションプラン](#)
- [AWS Managed Services の開始方法](#)
- [AMS の主要な用語](#)
- [サービスの説明](#)
- [AMS 情報リソース](#)
- [AMS コンプライアンス](#)
- [AMS Amazon マシンイメージ \(AMIs\)](#)
- [AD FS と AMS の統合の仕組み](#)
- [AMS Managed Active Directory](#)
- [AMS アプリケーションのデプロイ](#)



**Note**

新しい AWS リージョン は頻繁に追加されます。最新の AMS 対応オペレーティングシステムと最新の AMS 対応オペレーティングシステムについては AWS リージョン、「」を参照してください[サポートされている設定](#)。

詳細については AWS リージョン、「[の管理 AWS リージョン](#)」を参照してください。

AMS は、お客様からのフィードバックに基づいてサービスを継続的に改善することを目指しています。いくつかのメカニズムを使用して、セルフサービスを有効にし、反復タスクを自動化し、リリース時に新しい AWS のサービス および 機能を実装します。AMS サービスリクエストはいつでも送信して、新機能や機能の改善を提案できます。

AMS の営業時間は、1 日 24 時間、1 週間 7 日、1 年 365 日です。

AMS は、IT サービスをビジネスニーズに合わせることに焦点を当てた IT サービス管理 (ITSM) の一連のプラクティスに従います。

## この AMS ユーザーガイドについて

このユーザーガイドは、マルチアカウントまたはシングルアカウントのランディングゾーンを持つ AMS Advanced のお客様を対象としています。AMS ランディングゾーンのサービスの詳細については、「[AMS の主要な用語](#)」を参照してください。また、「[マルチアカウントランディングゾーンアーキテクチャ](#)」と「[シングルアカウントランディングゾーンアーキテクチャ](#)」も参照してください。

## AMS オペレーションプラン

AWS Managed Services (AMS) は、AMS Accelerate と AMS Advanced の 2 つのオペレーションプランで利用できます。運用計画には、特定の一連の機能が用意されており、サービス、技術機能、要件、料金、制限のレベルが異なります。当社の運用計画では、AWS ワークロードごとに適切なサイズの運用機能を柔軟に選択できます。このセクションでは、機能や相違点、および各プランに関連する責任、機能、利点について概説し、どのオペレーションプランがアカウントに最適かを理解できるようにします。

2 つのオペレーションプランの詳細な機能比較については、[AWS Managed Services機能](#)」を参照してください。

## AMS Accelerate オペレーションプラン

AMS Accelerate は、新規または既存の AWS 環境の day-to-day インフラストラクチャ管理を運用するのに役立つ AMS オペレーションプランです。AMS Accelerate は、モニタリング、インシデント管理、セキュリティなどの運用サービスを提供します。AMS Accelerate は、定期的なパッチ適用を必要とする Amazon EC2 ベースのワークロード用のオプションのパッチアドオンも提供します。

AMS Accelerate では、AMS Accelerate AWS アカウント を運用する対象、AMS Accelerate を運用する AWS リージョン、必要なアドオン、必要なサービスレベルアグリーメント (SLAs) を決定します。詳細については、[「AMS Accelerate オペレーションプランの使用」](#)と [「サービスの説明」](#)を参照してください。

## AMS Advanced オペレーションプラン

AMS Advanced は、インフラストラクチャをプロビジョニング、実行、サポートするためのフルライフサイクルサービスを提供します。AMS Accelerate が提供する運用サービスに加えて、AMS Advanced には、ランディングゾーン管理、インフラストラクチャの変更とプロビジョニング、アクセス管理、エンドポイントセキュリティなどの追加サービスも含まれています。

AMS Advanced は、AWS ワークロードを移行して AMS 運用サービスを受けるランディングゾーンをデプロイします。マネージドマルチアカウントランディングゾーンは、認証、セキュリティ、ネットワーク、ログ記録を容易にするために、インフラストラクチャで事前設定されています。

AMS Advanced には、AWS インフラストラクチャへの不正アクセスやリスクのある変更の実装を防止することでワークロードを保護する変更およびアクセス管理システムも含まれています。お客様は、AMS Advanced アカウントにほとんどの変更を実装するために、変更管理システムを使用して変更リクエスト (RFC) を作成する必要があります。セキュリティチームと運用チームによって事前に審査された自動変更のライブラリから RFCs を作成するか、AMS Advanced によって安全でサポートされていると判断された場合は、運用チームによってレビューおよび実装された手動変更をリクエストします。

AMS Advanced にはさまざまな SLAs。詳細については、[AWS Managed Services AMS Advanced サービスの説明](#)を参照してください。

## AWS Managed Services の開始方法

マルチアカウントランディングゾーン AMS サービスの開始方法の詳細については、[AWS Managed Services オンボーディングの概要](#)を参照してください。2 つのオンボーディングガイドには、サー

ビスの説明と、開始する際に考慮すべき質問が記載されています。[AWS Managed Services](#) の機能セットと、[AWS Managed Services](#) リソースの現在のリソースを確認します。

## AMS の主要な用語

- AMS Advanced: AMS Advanced ドキュメントの「サービスの説明」セクションで説明されているサービス。[「サービスの説明」](#)を参照してください。
- AMS アドバンスドアカウント: AMS アドバンスドオンボーディング要件のすべての要件を満たしている AWS アカウント。AMS Advanced の利点、導入事例、販売担当者へのお問い合わせについては、[AWS Managed Services](#)」を参照してください。
- AMS Accelerate Accounts: AMS Accelerate オンボーディング要件のすべての要件を満たしている AWS アカウント。[「AMS Accelerate の開始方法」](#)を参照してください。
- AWS Managed Services: AMS および/または AMS Accelerate。
- AWS Managed Services アカウント: AMS アカウントまたは AMS Accelerate アカウント。
- 重要な推奨事項: リソースまたは に対する潜在的なリスクや中断から保護するためにアクションが必要であることを知らせるサービスリクエスト AWS を通じて によって発行された推奨事項 AWS のサービス。指定された日付までにクリティカルレコメンデーションに従わないことを決定した場合、その決定に起因する損害については、お客様が単独で責任を負います。
- お客様がリクエストした設定: 以下で特定されていないソフトウェア、サービス、またはその他の設定。
  - Accelerate: [サポートされている設定](#)または [AMS Accelerate、サービスの説明](#)。
  - AMS Advanced: [サポートされている設定](#)または [AMS Advanced、サービスの説明](#)。
- インシデントコミュニケーション: AMS は、AMS Accelerate 用サポートセンターおよび AMS 用 AMS コンソールで作成されたインシデントを介して、インシデントをユーザーに伝達するか、AMS でインシデントをリクエストします。AMS Accelerate コンソールには、ダッシュボードのインシデントとサービスリクエストの概要と、サポートセンターへのリンクが表示されます。
- マネージド環境: AMS Advanced アカウントまたは AMS Accelerate アカウント。

AMS Advanced の場合、マルチアカウントランディングゾーン (MALZ) アカウントとシングルアカウントランディングゾーン (SALZ) アカウントが含まれます。

- 請求開始日: が AWS Managed Services オンボーディング E メールでリクエストされた情報 AWS を受信する翌営業日。AWS マネージドサービスのオンボーディング E メールは、アカウントで AWS Managed Services アクティブ化するために必要な情報を収集するために から AWS に送信される E メールを指します。

後で登録されたアカウントの場合、請求開始日は、AWS Managed Services が登録済みアカウントの AWS Managed Services アクティベーション通知を送信した翌日です。AWS Managed Services アクティベーション通知は、次の場合に発生します。

1. 互換性のある AWS アカウントへのアクセスを許可し、AWS Managed Services に引き渡します。
  2. AWS Managed Services は、AWS Managed Services アカウントを設計および構築します。
- サービスの終了: すべての AWS Managed Services アカウント、または指定された AWS Managed Services サービスアカウントの AWS Managed Services サービスは、サービスリクエストを通じて AWS 少なくとも 30 日前に通知することで、何らかの理由で終了できます。サービス終了日に、次のいずれかを実行します。
    1. AWS 必要に応じて、すべての AWS Managed Services アカウントまたは指定された AWS Managed Services アカウントのコントロールをユーザーに引き渡します。
    2. 関係者は、必要に応じて、すべての AWS Managed Services アカウントまたは指定された AWS Managed Services アカウントから AWS アクセスを許可する AWS Identity and Access Management ロールを削除します。
  - サービス終了日: サービス終了日は、30 日間の必要な終了通知期間の終了後の暦月の最終日です。必要な終了通知期間の終了日が暦月の 20 日以降である場合、サービス終了日は翌月の最終日になります。終了日のシナリオの例を次に示します。
    - 終了通知が 4 月 12 日に提供された場合、30 日間の通知は 5 月 12 日に終了します。サービス終了日は 5 月 31 日です。
    - 終了通知が 4 月 29 日に提供された場合、30 日間の通知は 5 月 29 日に終了します。サービス終了日は 6 月 30 日です。
  - AWS Managed Services: makes のプロビジョニングを利用でき、サービス開始日から AWS Managed Services アカウントごとに AWS Managed Services にアクセスして使用できます。AWS
  - 指定された AWS Managed Services アカウントの終了: サービスリクエスト (AWS Managed Services 「AMS アカウント終了リクエスト」) を通じて AWS 通知を提供することで、何らかの理由で指定された AWS AWS Managed Services マネージドサービスを終了できます。

インシデント管理の条件:

- イベント: AMS 環境の変更。

- アラート: サポートされている からのイベントがしきい値 AWS のサービス を超え、アラームをトリガーするたびに、アラートが作成され、連絡先リストに通知が送信されます。さらに、インシデントリストにインシデントが作成されます。
- インシデント: AMS 環境または AWS Managed Services 予期しない中断またはパフォーマンスの低下。AWS Managed Services または ユーザーによって報告された影響をもたらします。
- 問題: 1 つ以上のインシデントの根本的な根本原因の共有。
- インシデントの解決またはインシデントの解決 :
  - AMS が、そのインシデントに関連するすべての利用できない AMS サービスまたはリソースを利用可能な状態に復元した場合、または
  - AMS が、使用できないスタックまたはリソースを使用可能な状態に復元できないと判断した場合、または
  - AMS は、ユーザーによって承認されたインフラストラクチャの復元を開始しました。
- インシデント対応時間: インシデントを作成するときと、AMS がコンソール、E メール、データセンター、または電話を使用して初期応答を提供するときの時間の差。
- インシデント解決時間: AMS またはユーザーがインシデントを作成してからインシデントが解決されるまでの時間の差。
- Incident Priority: 低、中、高のいずれかで、AMS またはユーザーによってインシデントが優先される方法。
  - 低: AMS サービスの重大でない問題。
  - 中: マネージド環境内の AWS サービスを利用できますが、(該当するサービスの説明に従って) 意図したとおりに動作しません。
  - 高: (1) AMS コンソール、またはマネージド環境内の 1 つ以上の AMS APIs が使用できない、または (2) マネージド環境内の 1 つ以上の AMS スタックまたはリソースが使用できないため、アプリケーションが関数を実行できない。

AMS は、上記のガイドラインに従ってインシデントを再分類することがあります。

- インフラストラクチャの復元: 影響を受けたスタックのテンプレートに基づいて既存のスタックを再デプロイし、インシデント解決が不可能な場合に、ユーザーが特に指定しない限り、最後の既知の復元ポイントに基づいてデータ復元を開始します。

インフラストラクチャ用語 :

- マネージド型本番稼働環境: 顧客の本番稼働用アプリケーションが存在するユーザーアカウント。

- マネージド非本番環境: 開発およびテスト用のアプリケーションなど、非本番アプリケーションのみを含むユーザーアカウント。
- AMS スタック: AMS によって単一のユニットとして管理される 1 つ以上の AWS リソースのグループ。
- イミュータブルインフラストラクチャ: Amazon EC2 Auto Scaling グループ (ASGs) に一般的なインフラストラクチャメンテナンスモデル。更新されたインフラストラクチャコンポーネント (AMI 内) は AWS、インプレースで更新されるのではなく、デプロイごとに置き換えられます。イミュータブルインフラストラクチャの利点は、すべてのコンポーネントが常に同じベースから生成されるため、同期状態のままであることです。イミュータビリティは、AMI を構築するためのツールやワークフローとは無関係です。
- ミュータブルインフラストラクチャ: Amazon EC2 Auto Scaling グループではなく、単一のインスタンスまたは少数のインスタンスのみを含むスタックに一般的なインフラストラクチャメンテナンスモデル。このモデルは、ライフサイクルの開始時にシステムがデプロイされ、時間の経過とともに更新がシステムにレイヤー化される、従来のハードウェアベースのシステムデプロイに最も近いものです。システムの更新はインスタンスに個別に適用され、アプリケーションまたはシステムの再起動により (スタック設定に応じて) システムのダウンタイムが発生する可能性があります。
- セキュリティグループ: インバウンドトラフィックとアウトバウンドトラフィックを制御するためのインスタンスの仮想ファイアウォール。セキュリティグループは、サブネットレベルでなくインスタンスレベルで動作します。したがって、VPC 内のサブネット内の各インスタンスには、異なるセキュリティグループのセットを割り当てることができます。
- サービスレベルアグリーメント (SLAs): 期待されるサービスのレベルを定義する AMS 契約の一部。
- SLA が使用不可および使用不可:
  - ユーザーが送信した API リクエストがエラーになります。
  - 5xx HTTP レスポンスになるコンソールリクエスト (サーバーはリクエストを実行できません)。
  - AMS マネージドインフラストラクチャのスタックまたはリソースを構成する AWS のサービスサービスはすべて、[Service Health Dashboard](#) に示すように「サービス中断」の状態です。
  - AMS 除外から直接または間接的に生じる利用不可は、サービスクレジットの適格性を判断する際に考慮されません。サービスは、利用不可の基準を満たしていない限り、利用可能と見なされます。
- サービスレベル目標 (SLOs): AMS サービスの特定のサービス目標を定義する AMS 契約の一部。

パッチ適用用語:



- 必須パッチ: 環境またはアカウントのセキュリティ状態を損なう可能性のある問題に対処するための重要なセキュリティ更新プログラム。「Critical Security update」は、AMS がサポートするオペレーティングシステムのベンダーによって「Critical」と評価されたセキュリティ更新プログラムです。
- 発表されたパッチとリリースされたパッチ: パッチは通常、スケジュールに従って発表およびリリースされます。エマージェントパッチは、パッチの必要性が検出された時点で発表され、通常はその直後にパッチがリリースされます。
- パッチアドオン: AWS Systems Manager (SSM) 機能を利用する AMS インスタンスのタグベースのパッチ適用。これにより、ベースラインと設定したウィンドウを使用してインスタンスにタグを付け、それらのインスタンスにパッチを適用できます。
- パッチメソッド:
  - インプレースパッチ適用: 既存のインスタンスを変更することで実行されるパッチ適用。
  - AMI 置換パッチ適用: 既存の EC2 Auto Scaling グループ起動設定の AMI リファレンスパラメータを変更することで実行されるパッチ適用。
- パッチプロバイダー (OS ベンダー、サードパーティー): パッチは、アプリケーションのベンダーまたは管理機関によって提供されます。
- パッチタイプ:
  - 重要なセキュリティ更新プログラム (CSU): サポートされているオペレーティングシステムのベンダーによって「重要な」と評価されたセキュリティ更新プログラム。
  - 重要な更新 (IU): サポートされているオペレーティングシステムのベンダーによって「重要」と評価されたセキュリティ更新プログラム、または「重要」と評価されたセキュリティ以外の更新プログラム。
  - その他の更新 (OU): CSU または IU ではないサポートされているオペレーティングシステムのベンダーによる更新。
- サポートされているパッチ: AMS はオペレーティングシステムレベルのパッチをサポートしています。アップグレードは、セキュリティの脆弱性やその他のバグを修正するため、またはパフォーマンスを向上させるために、ベンダーによってリリースされます。現在サポートされている OSs [「サポート設定」](#) を参照してください。

#### セキュリティ条件:

- Detective Controls: AMS が作成または有効化したモニターのライブラリ。セキュリティ、運用、またはカスタマーコントロールと一致しない設定について、カスタマーマネージド環境とワーク

ロードを継続的に監視し、所有者に通知し、リソースをプロアクティブに変更または終了することでアクションを実行します。

サービスリクエストの条件：

- サービスリクエスト: AMS がユーザーに代わって実行するアクションに対するユーザーによるリクエスト。
- アラート通知: AMS アラートがトリガーされたときに、AMS によってサービスリクエストリストページに投稿された通知。アカウントに設定された連絡先は、設定された方法 (E メールなど) から通知されます。インスタンス/リソースに問い合わせタグがあり、タグベースの通知について Cloud Service Delivery Manager (CSDM) に同意している場合、タグの連絡先情報 (キー値) にも自動 AMS アラートが通知されます。
- サービス通知: サービスリクエストリストページに投稿される AMS からの通知。

その他の用語：

- AWS Managed Servicesインターフェイス: AMS の場合: AWS Managed Servicesアドバンスドコンソール、AMS CM API、サポート および API。AMS Accelerate の場合: サポート コンソールとサポート API。
- 顧客満足度 (CSAT): AMS CSAT には、提供されたすべてのケースまたはコレスポнденスに関するケースコレスポнденス評価、四半期ごとのアンケートなど、詳細な分析情報が提供されます。
- DevOps: DevOps は、すべてのステップで自動化とモニタリングを強く推奨する開発手法です。DevOps は、自動化の基盤の上に開発と運用の従来の分離機能を組み合わせることで、開発サイクルの短縮、デプロイ頻度の向上、より信頼性の高いリリースを目指しています。デベロッパーがオペレーションを管理でき、オペレーションが開発を通知すると、問題や問題をより迅速に発見して解決し、ビジネス目標をより簡単に達成できます。
- ITIL: Information Technology Infrastructure Library (ITIL) は、IT サービスのライフサイクルを標準化するために設計された ITSM フレームワークです。ITIL は、IT サービスのライフサイクルをカバーする 5 つの段階で構成されています。サービス戦略、サービス設計、サービス移行、サービス運用、サービス改善です。
- IT サービス管理 (ITSM): IT サービスをビジネスニーズに合わせる一連のプラクティス。
- Managed Monitoring Services (MMS): AMS は、独自のモニタリングシステムである Managed Monitoring Service (MMS) を運用します。これは、AWS ヘルスイベントを消費し、Amazon CloudWatch データ、および他の からのデータを集約し AWS のサービス、Amazon Simple



Notification Service (Amazon SNS) トピックを通じて作成されたアラームを AMS オペレーター (オンライン 24 時間 365 日) に通知します。

- 名前空間: IAM ポリシーを作成するとき、または Amazon リソースネーム (ARNs) を操作するとき、名前空間 AWS のサービスを使用してを識別します。アクションとリソースを識別するときに名前空間を使用します。

## サービスの説明

AMS Advanced (AMS) は、AWS インフラストラクチャのオペレーションを管理するための AWS Managed Services サービスのオペレーションプランです。AMS Advanced は、パッチ、継続性管理、セキュリティ管理、インシデント、変更、サービスリクエスト管理などの IT 管理プロセスなどの日常的なインフラストラクチャオペレーションを提供します。サポートされているサービスのリストについては、「[サポートされている AWS サービス](#)」を参照してください。

YouTube 動画: [AMS はクラウドで運用上の優秀性を達成するのにどのように役立ちますか？](#)

### トピック

- [AWS Managed Services \(AMS\) AMS Advanced オペレーションプランの機能](#)
- [何をするか、何をしないか](#)
- [AMS 責任マトリックス \(RACI\)](#)
- [AMS 環境の基本コンポーネント](#)
- [AMS アカウントの制限](#)
- [AMS サービスレベル目標 \(SLOs\)](#)
- [サポートされている AWS サービス](#)
- [サポートされている設定](#)
- [AMS でサポートされていないオペレーティングシステムの機能](#)
- [AMS Advanced インターフェイス](#)
- [AMS VPC エンドポイント](#)
- [AMS で保護された名前空間](#)
- [AMS 予約プレフィックス](#)
- [AMS メンテナンスウィンドウ](#)

# AWS Managed Services (AMS) AMS Advanced オペレーションプランの機能

AMS Advanced は、サポートされている AWS サービスに次の機能を提供します。

- ログ記録、モニタリング、ガードレール、イベント管理：

AMS は、マネージド環境のログ記録アクティビティを設定およびモニタリングし、さまざまなヘルスチェックに基づいてアラートを定義します。アラートは、該当する AWS のサービスについて AMS によって調査され、それらのサービスの使用に悪影響を及ぼすとインシデントが作成されます。AMS は、すべてのオペレーションの結果として生成されたすべてのログを CloudWatch、CloudTrail、および Amazon S3 のシステムログに集約して保存します。追加のアラートをリクエストできます。AMS の予防的コントロールに加えて、AMS は設定ガードレールと検出コントロールをデプロイして、マネージドアカウントの運用とセキュリティの整合性を低下させる可能性のある設定ミスから継続的に保護し、タグ付けやコンプライアンスなどのコントロールを適用します。モニタリング対象のコントロールが検出されると、ユーザーが変更できる事前定義された AMS のデフォルトに基づいて、リソースの通知、変更、または終了が発生するアラームが生成されます。

- 継続性管理 (バックアップと復元):

AMS は、お客様が決定したスケジュールされた間隔で、標準の既存の AWS Backup 機能を使用してリソースのバックアップを提供します。特定のスナップショットからの復元アクションは、RFC を使用して AMS で実行できます。スナップショット間隔の間に発生するデータ変更は、ユーザーがバックアップする責任があります。スケジュールされた間隔外にバックアップまたはスナップショットリクエストの RFC を送信できます。AWS リージョンでアベイラビリティゾーン (AZ) が利用できない場合、AMS は、影響を受ける スタックのテンプレートと使用可能な EBS スナップショットに基づいて新しいスタック (複数可) を再作成することで、マネージド環境を復元します。

- セキュリティとアクセスの管理：

AMS は、ウイルス対策やマルウェア対策などのエンドポイントセキュリティ (EPS) を提供します。独自の EPS ツールとプロセスを使用でき、独自の EPS の持ち込み (BYOEPS) と呼ばれる機能を使用して EPS に AMS を使用することはできません。また、AMS は AWS Identity and Access Management、(IAM) ロールや Amazon EC2 AWS セキュリティグループなど、オンボーディング中に承認されたデフォルトのセキュリティ機能を設定し、標準 AWS ツール (Amazon Macie AWS Security Hub CSPM、Amazon GuardDuty など) を使用してセキュリティの問題を監視して対応します。ユーザーを管理するには、ユーザーが提供する承認済みのディレクトリサー

ビスを使用します。承認されたディレクトリサービスのリストについては、「」を参照してください [サポートされている設定](#)。

AMS には、エンドポイントセキュリティ (EPS) が含まれます。これには、ウイルス対策 (AV)、マルウェア対策保護、マルウェア、侵入検出 (Trend Micro) が含まれます。セキュリティグループはスタックテンプレートごとに定義され、アプリケーション (パブリック/プライベート) セキュリティグループの可視性に応じて起動時に変更されます。

システムへのアクセスは、変更管理の変更リクエスト (RFCs)。アクセス管理は、Amazon EC2 インスタンス、AWS マネジメントコンソール APIs などの個別のリソースへのアクセスを提供します。AWS へのオンボーディングとフェデレーション中に AMS Microsoft Active Directory デプロイで一方向の信頼を確立したら、既存の企業認証情報をすべてのやり取りに使用できます。

- パッチ管理 :

AMS は、サポートされているオペレーティングシステム (OSs) と、サポートされているオペレーティングシステムがプリインストールされたソフトウェアの EC2 インスタンスに更新を適用してインストールします。サポートされているオペレーティングシステムのリストについては、「」を参照してください [サポートされている設定](#)。

AMS には、パッチ適用用の 2 つのモデルがあります。

- 従来のアカウントベースのパッチ適用用の AMS 標準パッチ
- タグベースのパッチ適用用の AMS パッチオーケストレーター。

AMS 標準パッチでは、AMS がほとんどのパッチ適用アクティビティを実行するために、毎月のメンテナンスウィンドウが選択されます。AMS は、選択したメンテナンスウィンドウ外で重要なセキュリティ更新プログラム (適切な通知を使用) を適用し、選択したメンテナンスウィンドウ中に重要な更新プログラムを適用します。AMS は、選択したメンテナンスウィンドウ中にインフラストラクチャ管理ツールに更新をさらに適用します。必要に応じて、スタックをパッチ管理から除外したり、更新を拒否したりできます。

アカウントごとのデフォルトのメンテナンスウィンドウである AMS Patch Orchestrator は、AMS がパッチ適用アクティビティを実行するために定義されます。AMS の追加のカスタムメンテナンスウィンドウをスケジュールして、ユーザーが定義した特定のインスタンスセットにタグでパッチを適用できます。AMS は利用可能なすべての更新を適用しますが、カスタムパッチベースラインを作成することで更新をフィルタリングまたは拒否できます。どちらのモデルでも、パッチ管理で提供される更新を承認または拒否しても後で気が変わった場合は、RFC を介して更新を開始する責任があります。AMS はリソースのパッチステータスを追跡し、毎月のビジネスレビューで最新ではないシステムを強調します。パッチ管理は、すべての AMS マネージドアプリケーション

や、パッチ機能を持つサポートされている AWS サービス (RDS など) を含む、マネージド環境のスタックに限定されます。更新がリリースされたときにすべてのタイプのインフラストラクチャ設定をサポートするために、AMS a) は EC2 インスタンスを更新し、b) は更新された AMS AMI を提供します。上記で特に説明されていない追加のアプリケーションをインストール、設定、パッチ適用、モニタリングするのはお客様の責任です。

- 変更管理：

AMS 変更管理は、マネージド環境の変更を制御するメカニズムです。AMS は、予防的コントロールと検出的コントロールを組み合わせることでこのプロセスを容易にし、選択した AMS モードに応じて異なるレベルのコントロールと関連するリスクを提供します。

AMS 環境内のすべてのアクションがログインされます AWS CloudTrail。

AMS 変更管理とさまざまなモードの詳細については、[「AMS 変更管理ガイド」](#)と[「AMS モード」](#)を参照してください。

- 自動およびセルフサービスのプロビジョニング管理：

AMS Advanced で AWS リソースをプロビジョニングするには、いくつかの方法があります。

- プロビジョニングと設定の変更リクエスト (RFCs) を送信する
- AWS Service Catalog を使用してデプロイする
- [直接変更モード](#)でデプロイする
- [デベロッパーモード](#)でデプロイします。デベロッパーモードで作成されたリソースは AMS によって管理されないことに注意してください。
- Select AWS のサービスのセルフサービスプロビジョニングを使用して AWS サービスを直接設定します (「」を参照[サポートされている AWS サービス](#))。

- インシデント管理：

AMS は、AMS によって検出されたインシデントをプロアクティブに通知します。AMS は、お客様が送信したインシデントと AMS が生成したインシデントの両方に対応し、インシデントの優先度に基づいてインシデントを解決します。お客様から特に指示がない限り、AMS によってマネージド環境のセキュリティ上のリスクであると判断されるインシデント、および AMS およびその他の AWS サービスの可用性に関連するインシデントは、事前に対処されます。AMS は、認可を受け取ると、他のすべてのインシデントに対してアクションを実行します。繰り返し発生するインシデントは、問題管理プロセスによって対処されます。

- 問題管理：

AMS は傾向分析を実行して、問題を特定して調査し、根本原因を特定します。問題は、回避策または同様の将来のサービスへの影響の再発を防ぐ永続的なソリューションで修正されます。インシデント後レポート (PIR) は、解決時に「高」インシデントに対してリクエストされる場合があります。PIR は、根本原因と、予防策の実装など、実行された予防策をキャプチャします。

- レポート :

AMS は、エグゼクティブサマリーとインサイト、運用メトリクス、マネージドリソース、AMS サービスレベルアグリーメント (SLA) の遵守、支出、削減、コスト最適化に関する財務メトリクスなど、AMS の主要なパフォーマンスメトリクスをまとめた月次サービスレポートを提供します。レポートは、割り当てられた AMS Cloud Service Delivery Manager (CSDM) によって配信されます。

- サービスリクエスト管理:

マネージド環境、AMS、または AWS サービス提供に関する情報をリクエストするには、AMS コンソールを使用してサービスリクエストを送信します。サービス AWS や機能に関する「方法」の質問や、追加の AMS サービスをリクエストするサービスリクエストを送信できます。

- サービスデスク:

AMS は、インシデント管理、サービスリクエスト管理、変更管理など、自動化されていないリクエストに対応するために、フルタイムの Amazon 従業員によるエンジニアリングオペレーションをスタッフとして配置します。サービスデスクは、24 時間 365 日営業しています。

- 指定されたリソース :

各顧客には、Cloud Service Delivery Manager (CSDM) と Cloud Architect (CA) が割り当てられます。

- CSDMsに直接連絡できます。実装、移行、運用ライフサイクルのすべてのフェーズを通じて、サービスレビュー、配信レポート、インサイトを実行します。CSDMs毎月ビジネスレビューを行い、財務支出、コスト削減の推奨事項、サービス使用率、リスクレポートなどの項目について詳しく説明します。運用パフォーマンス統計を深く掘り下げ、改善点に関する推奨事項を提供します。

- CAsに直接連絡し、技術的な専門知識を提供して、AWS クラウドの使用を最適化できます。CA アクティビティの例には、移行するワークロードの選択、追加のアカウントとワークロードのオンボーディングの支援、ゲームデー、ディザスタリカバリテスト、問題管理、AMS とを最大限に活用するための技術アドバイスなどの運用アクティビティの技術リーダーとしての役割を果たします AWS。CAs、組織のあらゆるレベルで技術的な議論を推進し、インシデント管理、トレードオフ、ベストプラクティスの確立、技術的リスクの軽減を支援します。

- デベロッパーモード:

この機能を使用すると、AMS 変更管理プロセスへのアクセスに加えて、AWS サービス APIs と AWS コンソールへの直接アクセスを許可することで、インフラストラクチャの設計とデプロイを AMS 設定アカウント内ですばやく反復できます[1]。変更管理プロセス外でデベロッパーモードのアクセス許可を使用してプロビジョニングまたは設定されたリソースは、お客様が管理する必要があります (「自動およびセルフサービスプロビジョニング管理」を参照してください)。AMS 変更管理プロセスを通じてプロビジョニングされたリソースは、AMS 上の他の変更管理でプロビジョニングされたワークロードと同様にサポートされます。

- AWS サポート:

AMS のお客様は、AMS オペレーションプランを補完するために必要な AWS サポートのレベルを選択できます。AMS に登録されているアカウントは、ビジネスサポートまたはエンタープライズサポートのいずれかにサブスクライブできます。サポートプランの違いについては、[「AWS サポートプラン」](#)を参照してください。

- カスタマー管理アカウント:

この機能を使用すると、同じマネージド環境内の AWS アカウントをリクエストできますが、それらのアカウント内のワークロードと AWS リソースの継続的なオペレーションはお客様の責任となります。AMS はカスタマーマネージドアカウントをプロビジョニングしますが、アカウントが作成されると、それらのアカウントに他の AMS 機能やサービスは提供されません。AWS は、カスタマーマネージドアカウントをエンタープライズレベルのプレミアムサポートに登録しません。カスタマー管理アカウントは、選択したサポートレートで AWS サポートに登録する責任があります。

- ファイアウォール管理:

AMS は、サポートされているファイアウォールサービス用のオプションのマネージドファイアウォールソリューションを提供します。これにより、マネージド環境内のネットワークのインターネットバウンド送信トラフィックフィルタリングが可能になります。これには、AWS ネットワークインフラストラクチャを使用せず、トラフィックがインターネットに直接送信されるパブリックサービスは含まれません。このソリューションは、業界をリードするファイアウォールテクノロジーと AMS インフラストラクチャ管理機能を組み合わせて、ファイアウォールインフラストラクチャをデプロイ、モニタリング、管理、スケーリング、復元します。

AMS をオンボードすると、AMS ネットワークインフラストラクチャの完全なリストが表示されます。AMS インフラストラクチャのサポートで実行されているサービスの最新のリストをいつでも取得するには、必要な情報の詳細を含むサービスリクエストをファイルします。ネットワーク設計の変



更をリクエストするには、VPC の追加やセキュリティグループルールの変更のリクエストなど、変更内容を説明するサービスリクエストを作成します。

## 何をするか、何をしないか

AMS は、AWS インフラストラクチャをデプロイするための標準化されたアプローチを提供し、必要な継続的な運用管理を提供します。ロール、責任、サポートされているサービスの詳細については、「[サービスの説明](#)」を参照してください。

### Note

AMS が追加の AWS サービスを提供するようにリクエストするには、サービスリクエストをファイルします。詳細については、「[サービスリクエストの作成](#)」を参照してください。

#### • 当社の業務 :

オンボーディングが完了すると、AMS 環境は変更リクエスト (RFCs)、インシデント、サービスリクエストを受け取ることができます。AMS サービスとのやり取りは、アプリケーションスタックのライフサイクルを中心に展開されます。新しいスタックは、テンプレートの事前設定されたリストから順序付けられ、特定の Virtual Private Cloud (VPC) サブネットに起動され、変更リクエスト (RFCs) を通じて運用期間中に変更され、イベントとインシデントが 24 時間 365 日モニタリングされます。

アクティブなアプリケーションスタックは、パッチ適用など、AMS によってモニタリングおよび維持され、変更が必要な場合やスタックが廃止されない限り、スタックの存続期間中はそれ以上のアクションは必要ありません。スタックのヘルスと機能に影響する AMS によって検出されたインシデントは、通知を生成し、解決または検証するためのアクションが必要になる場合と必要でない場合があります。ハウツーに関する質問やその他の問い合わせは、サービスリクエストを送信することで行うことができます。

さらに、AMS では、AMS によって管理されていない互換性のある AWS サービスを有効にすることができます。AWS-AMS 互換サービスの詳細については、「[セルフサービスプロビジョニングモード](#)」を参照してください。

#### • 行わないこと :

AMS は、手動および自動のオプションを多数提供することでアプリケーションのデプロイを簡素化しますが、アプリケーションの開発、テスト、更新、管理はお客様の責任となります。AMS は、アプリケーションに影響を与えるインフラストラクチャの問題のトラブルシューティングを支援しますが、AMS はアプリケーション設定にアクセスして検証することはできません。

## AMS 責任マトリックス (RACI)

### Note

AWS Managed Services (AMS) は、適時に義務を果たすために、適切な一連のアクションを決定するためにお客様からの入力を要求する場合があります。AMS は、そのようなすべての明確化と入力について、指定された顧客連絡先に連絡します。AMS は、このようなクエリに対する応答を 24 営業日以内に想定します。24 時間以内に返信がない場合、AMS はユーザーに代わってアクションを選択できます。

AMS 責任、説明責任、相談、情報、または RACI マトリックスは、さまざまなアクティビティについて顧客または AMS に主な責任を割り当てます。

AMS は AWS インフラストラクチャを管理します。次の表は、AMS マネージド環境内で実行されているアプリケーションのライフサイクルにおけるアクティビティに関する顧客と AMS の責任の概要を示しています。

AMS は、カスターマネージドアカウントまたはそのアカウント内で実行されているインフラストラクチャに関する以下のアクティビティについて責任を負いません。したがって、この RACI は適用されません。

- R は、タスクを達成するために作業を行う責任者を表します。
- C は、相談された当事者、通常は対象分野の専門家として意見を求める当事者、二国間通信を行う当事者を指します。
- 「情報」の略です。多くの場合、タスクまたは成果物の完了時にのみ、進捗状況が通知される当事者です。
- セルフサービスプロビジョニングとは、デベロッパーモードやセルフサービスプロビジョニングサービスなど、AWS API またはコンソールを通じてセルフサービスを使用してお客様がプロビジョニングするリソースを指します。



 Note

一部のセクションには、AMS とお客様の両方に「R」が含まれています。これは、責任 AWS 共有モデルでは、AMS と顧客の両方がインフラストラクチャとアプリケーションの問題に対処するために共同所有権を持っているためです。

セルフサービスプロビジョニング機能を提供するために、AMS は、サービスへの直接 AWS アクセスから意図しない変更を制限するためのアクセス許可の境界を持つ昇格された IAM ロールを作成しました。ロールによってすべての変更が妨げられるわけではなく、ユーザーは、内部コントロール、コンプライアンスに従い、使用されているすべての AWS サービスが必要な認定を満たしていることを確認する責任があります。これはセルフサービスプロビジョニングモードと呼ばれます。AWS コンプライアンス要件の詳細については、[AWS「コンプライアンス」](#)を参照してください。

セルフサービスでプロビジョニングするリソースの場合、AMS は、インシデント管理、検出コントロールとガードレール、レポート、指定されたリソース (Cloud Service Delivery Manager と Cloud Architect)、セキュリティとアクセス、サービスリクエストによるテクニカルサポートを提供します。さらに、該当する場合、AMS 変更管理システムの外部でプロビジョニングまたは設定されたリソースの継続管理、パッチ管理、インフラストラクチャモニタリング、変更管理に責任を負います。

| アクティビティ                    | お客様 | AWS Managed Services (AMS) |
|----------------------------|-----|----------------------------|
| アプリケーションのライフサイクル           |     |                            |
| アプリケーション開発                 | R   | I                          |
| アプリケーションインフラストラクチャ要件の分析と設計 | R   | C                          |
| 非標準 AMS スタックの設計と最適化        | R   | C                          |
| AMS 標準スタックの設計と最適化          | I   | R                          |
| アプリケーションのデプロイ              | R   | C                          |

| アクティビティ                                      | お客様 | AWS Managed Services (AMS) |
|----------------------------------------------|-----|----------------------------|
| AWS インフラストラクチャのデプロイ                          | C   | R                          |
| アプリケーションのモニタリング                              | R   | I                          |
| アプリケーションのテスト/最適化                             | R   | I                          |
| AWS インフラストラクチャ最適化ガイダンス                       | I   | R                          |
| AWS インフラストラクチャのモニタリング                        | I   | R                          |
| アプリケーションの問題のトラブルシューティングと解決                   | R   | C                          |
| AWS ネットワーク問題のトラブルシューティングと解決                  | C   | R                          |
| オペレーティングシステムとインフラストラクチャの問題をトラブルシューティングして解決する | C   | R                          |
|                                              | R   | C                          |
| セルフサービスプロビジョニング                              |     |                            |
| アプリケーションと ITSM の統合                           |     |                            |
| AWS サービスサービスとのアプリケーション統合                     | R   | C                          |
| AWS Managed Services Interface との ITSM 統合    | R   | C                          |
| ネットワーク                                       |     |                            |
| マネージド環境 VPC と VPC のセットアップと設定                 | C   | R                          |
| VPCs のプライベートアドレススペースを割り当てる (/16 など )         | R   | C                          |

| アクティビティ                                                               | お客様 | AWS Managed Services (AMS) |
|-----------------------------------------------------------------------|-----|----------------------------|
| AWS Managed Services、カスタマーマネージド Firewalls/Proxy/Bastions/HOSTs の設定と運用 | R   | C                          |
| マネージド環境内で AWS セキュリティ Groups/NAT/Customer 拠点/NACL を設定および運用する           | I   | R                          |
| お客様のネットワーク内でのネットワーク (DirectConnect など) の設定と実装                         | R   | C                          |
| マネージド環境内のネットワーク設定と実装                                                  | C   | R                          |
| マネージド環境設定                                                             |     |                            |
| ベースラインスタックテンプレートのデフォルトの Auto Scaling 設定を定義する                          | I   | R                          |
| RI 最適化の推奨                                                             | C   | R                          |
| RI と PIOP の容量を購入する                                                    | R   | C                          |
| 容量が過剰にプロビジョニングされたときの容量の削除 (お客様のアプリケーションでサポートされている場合)                  | C   | R                          |
| AWS Managed Services の AWS 顧客固有の情報を作成/更新する                            | C   | R                          |
| S3 設定                                                                 | C   | R                          |
| セルフサービスプロビジョニング                                                       | R   | C                          |
| Glacier 設定                                                            | C   | R                          |
| アーカイブポリシーを定義する                                                        | R   | C                          |

| アクティビティ                                | お客様 | AWS Managed Services (AMS) |
|----------------------------------------|-----|----------------------------|
| アーカイブポリシーの設定                           | C   | R                          |
| カスタマーメンテナンスウィンドウの選択                    | R   | I                          |
| AWS RDS 管理                             |     |                            |
| source/replica/RO レプリケーションの状態をモニタリングする | I   | R                          |
| ソースフェイルオーバーの RCA を特定する                 | I   | R                          |
| 自動スナップショット (バックアップ) 設定                 | C   | R                          |
| セルフサービスプロビジョニング                        | R   | C                          |
| DB エンジンパッチ管理の調整とスケジュール                 | C   | R                          |
| セルフサービスプロビジョニング                        | R   | C                          |
| DB ストレージと PIOP 容量の推奨                   | C   | R                          |
| セルフサービスプロビジョニング                        | R   | C                          |
| データベースを実行するためにインスタンスのサイズ設定を推奨          | C   | R                          |
| セルフサービスプロビジョニング                        | R   | C                          |
| マネージド環境の RI 最適化を推奨                     | C   | R                          |
| セルフサービスプロビジョニング                        | R   | C                          |
| RDS パフォーマンスモニタリング (CloudWatch)         | C   | R                          |
| セルフサービスプロビジョニング                        | R   | C                          |

| アクティビティ                                                                                            | お客様 | AWS Managed Services (AMS) |
|----------------------------------------------------------------------------------------------------|-----|----------------------------|
| RDS イベントサブスクリプション設定 (SNS)                                                                          | C   | R                          |
| セルフサービスプロビジョニング                                                                                    | R   | C                          |
| RDS セキュリティグループ設定                                                                                   | C   | R                          |
| セルフサービスプロビジョニング                                                                                    | R   | C                          |
| RDS エンジンパラメータ/オプション設定                                                                              | R   | C                          |
| DB テーブル設計                                                                                          | R   | I                          |
| DB インデックス作成                                                                                        | R   | I                          |
| DB ログ分析                                                                                            | R   | I                          |
| AMS 変更管理                                                                                           |     |                            |
| 顧客 RFCs の作成 (マネージドスタック creating/updating/deleting リソースへのアクセス、アプリケーションのデプロイ/更新、AWS サービス内容の設定の変更など ) | R   | I                          |
| 顧客 RFCs の承認                                                                                        | I   | R                          |
| AWS Managed Services RFCs の作成 (リソースへのアクセス、お客様に代わってリソースを作成する、パッチ管理の一部として OS に更新を適用するなど )            | I   | R                          |
| 自動ではない RFCs の承認                                                                                    | R   | I                          |
| 新しい変更タイプのリクエストの送信                                                                                  | R   | C                          |
| 新しい変更タイプの作成                                                                                        | I   | R                          |
| アプリケーション変更カレンダーのメンテナンス                                                                             | R   | C                          |

| アクティビティ                                                                       | お客様 | AWS Managed Services (AMS) |
|-------------------------------------------------------------------------------|-----|----------------------------|
| 今後のメンテナンスウィンドウの通知                                                             | I   | R                          |
| AWS Service Catalog                                                           |     |                            |
| ポートフォリオと製品を作成する                                                               | R   | I                          |
| エンドユーザーに製品を配布する                                                               | R   | I                          |
| タグとタグオプションライブラリを作成する                                                          | R   | C                          |
| ポートフォリオと製品をエンドユーザーと共有する                                                       | R   | I                          |
| ポートフォリオと製品を修正/更新する                                                            | R   | I                          |
| ポートフォリオと製品に制約を作成して割り当てる                                                       | R   | C                          |
| サービスアクションを製品に関連付ける                                                            | R   | C                          |
| プロビジョニングされたリソースを新しいバージョンの製品で更新する                                              | R   | I                          |
| プロビジョニング                                                                      |     |                            |
| AWS Managed Services ベースライン AMI へのお客様固有の追加                                    | R   | C                          |
| スタックテンプレートのプロビジョニングに使用される追加の承認済み変更タイプを設定する                                    | C   | R                          |
| AMS 変更管理プロセスまたは AWS Service Catalog を通じて送信されたマネージドスタックおよび関連する AWS リソースを起動します。 | I   | R                          |
|                                                                               | R   | I                          |
| セルフサービスプロビジョニング                                                               |     |                            |

| アクティビティ                                                                                          | お客様 | AWS Managed Services (AMS) |
|--------------------------------------------------------------------------------------------------|-----|----------------------------|
| AMS 変更管理プロセスまたは AWS Service Catalog を通じてプロビジョニングされたインスタンスに、カスタムおよびサードパーティーアプリケーションをインストール/更新します。 | R   | I                          |
| プロビジョニング - スタックアーキテクチャ                                                                           |     |                            |
| OS ライセンスの提供 (EC2 や RDS など、該当する AWS のサービスの使用料を含む )<br><br>セルフサービスプロビジョニング                         | I   | R                          |
|                                                                                                  | R   | I                          |
| AMS 変更管理システムを介したアプリケーションデプロイ用のベースラインインフラストラクチャテンプレート (スタック) を定義します。                              | I   | R                          |
|                                                                                                  | R   | I                          |
| セルフサービスプロビジョニング                                                                                  |     |                            |
| ベースライン承認済み AMIs の作成 <sup>8</sup>                                                                 | I   | R                          |
| 顧客のアプリケーションインベントリを評価し、利用可能なインフラストラクチャテンプレート (スタック) との適合性を判断する                                    | R   | C                          |
| ベースラインテンプレートサービスに加えて一意のスタックを定義する                                                                 | R   | C                          |
| ログ記録、モニタリング、イベント管理                                                                               |     |                            |
| AWS インフラストラクチャ変更ログの記録                                                                            | I   | R                          |
| すべてのアプリケーション変更ログの記録                                                                              | R   | C                          |

| アクティビティ                                                                                  | お客様 | AWS Managed Services (AMS) |
|------------------------------------------------------------------------------------------|-----|----------------------------|
| AMS 変更管理プロセスを通じてプロビジョニングされた AWS インフラストラクチャのパッチ適用、セキュリティ、モニタリングなどのエージェントとスクリプトのインストールと設定。 | I   | R                          |
|                                                                                          | R   | C                          |
| セルフサービスプロビジョニング                                                                          |     |                            |
| 顧客固有のモニタリング要件とインシデント要件を定義する                                                              | R   | C                          |
| マネージド環境のアラートの設定                                                                          | I   | R                          |
| すべての AMS 設定済みアラートのモニタリング                                                                 | I   | R                          |
|                                                                                          | R   | C                          |
| セルフサービスプロビジョニング                                                                          |     |                            |
| インシデント通知のインフラストラクチャアラートの調査                                                               | I   | R                          |
|                                                                                          | R   | C                          |
| セルフサービスプロビジョニング                                                                          |     |                            |
| アプリケーションアラームの調査                                                                          | R   | C                          |
| インシデント管理                                                                                 |     |                            |
| モニタリングに基づいて AWS インフラストラクチャ上のインシデントにプロアクティブに通知する                                          | I   | R                          |
|                                                                                          | R   | C                          |
| セルフサービスプロビジョニング                                                                          |     |                            |
| アプリケーションのパフォーマンスの問題と停止に対処する                                                              | R   | I                          |
| インシデントの優先度を分類する                                                                          | I   | R                          |



| アクティビティ                                                                                                                                                                                                                                 | お客様 | AWS Managed Services (AMS) |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|----------------------------|
| インシデント対応を提供する                                                                                                                                                                                                                           | I   | R                          |
| インシデント解決/インフラストラクチャの復元を提供する                                                                                                                                                                                                             | C   | R                          |
| <div>  <b>Note</b><br/>           SLAs、セルフサービスプロビジョニングとデベロッパーモードを使用してプロビジョニングされたリソースを含め、AMS 変更管理の外部でプロビジョニングされたインスタンスベースのリソースには適用されません。         </div> |     |                            |
| <b>問題管理</b>                                                                                                                                                                                                                             |     |                            |
| マネージド環境の問題を特定する                                                                                                                                                                                                                         | C   | R                          |
| マネージド環境での問題に対して RCA を実行する                                                                                                                                                                                                               | C   | R                          |
| マネージド環境の問題の修復                                                                                                                                                                                                                           | C   | R                          |
| アプリケーションの問題を特定して修正する                                                                                                                                                                                                                    | R   | I                          |
| <b>セキュリティ管理</b>                                                                                                                                                                                                                         |     |                            |
| 顧客インフラストラクチャのセキュリティ、および/または顧客のオンボーディング中に決定され合意されたセキュリティコンプライアンスプロセスのベースラインの確立。                                                                                                                                                          | C   | R                          |
|                                                                                                                                                                                                                                         | R   | C                          |
| セルフサービスプロビジョニング                                                                                                                                                                                                                         |     |                            |
| Managed EPS の有効なライセンスの維持                                                                                                                                                                                                                | R   | C                          |

| アクティビティ                                                                         | お客様 | AWS Managed Services (AMS) |
|---------------------------------------------------------------------------------|-----|----------------------------|
| マネージド EPS の設定                                                                   | I   | R                          |
| セルフサービスプロビジョニング                                                                 | R   | C                          |
| マネージド EPS の更新                                                                   | I   | R                          |
| セルフサービスプロビジョニング                                                                 | R   | C                          |
| AMS CM プロセスを通じてプロビジョニングされたインスタンスのマルウェアのモニタリング。                                  | I   | R                          |
|                                                                                 | R   | C                          |
| セルフサービスプロビジョニング                                                                 |     |                            |
| ウイルス署名の維持と更新。                                                                   | I   | R                          |
| セルフサービスプロビジョニング                                                                 | R   | C                          |
| マルウェアに感染したインスタンスの修復。                                                            | C   | R                          |
| セルフサービスプロビジョニング                                                                 | R   | C                          |
| セキュリティイベント管理                                                                    | C   | R                          |
| セキュリティ - アクセス管理                                                                 |     |                            |
| ユーザーのライフサイクルと、AWS Managed Services へのアクセスに使用されるローカルディレクトリサービスのアクセス許可を管理する       | R   | I                          |
| AWS コンソール/APIs                                                                  | R   | C                          |
| AWS Managed Services AD からカスタマー マネージド AD への Active Directory (AD) の信頼を受け入れ、維持する | R   | C                          |

| アクティビティ                                                         | お客様 | AWS Managed Services (AMS) |
|-----------------------------------------------------------------|-----|----------------------------|
| オンボーディング中に、各マネージドアカウント内にクロスアカウント IAM 管理者ロールを作成します。              | R   | C                          |
| 各アカウントの AWS ルート認証情報を保護する                                        | I   | R                          |
| マネージド環境の IAM リソースを定義する                                          | C   | R                          |
| AMS エンジニアの OS アクセスの特権認証情報を管理する                                  | I   | R                          |
| AMS によってお客様に提供される OS アクセスの特権認証情報を管理する                           | R   | I                          |
| セキュリティインシデント対応 - 準備                                             |     |                            |
| 通信                                                              |     |                            |
| AMS がセキュリティイベント通知とセキュリティエスカレーション中に使用する顧客のセキュリティ連絡先の詳細を提供する      | R   | I                          |
| セキュリティイベントやセキュリティエスカレーション中に使用する、提供された顧客セキュリティ連絡先の詳細を保存および管理します。 | CI  | R                          |
| トレーニング                                                          |     |                            |
| インシデント対応プロセス中に AMS をサポートするドキュメントを顧客に提供する                        | I   | R                          |
| セキュリティのゲームデーを通じて、インシデント対応プロセス中に責任共有を実践する                        | RI  | RC                         |
| リソース管理                                                          |     |                            |

| アクティビティ                                                                | お客様 | AWS Managed Services (AMS) |
|------------------------------------------------------------------------|-----|----------------------------|
| アラート、アラート関連、ノイズ削減、その他のルール AWS のサービス に対してサポートされているセキュリティ管理を設定する         | I   | R                          |
| アセット (AWS リソース) インベントリを維持し、アセットの価値と重要性を把握します。この情報は、インシデント封じ込め戦略に役立ちます。 | R   | CI                         |
| AWS タグを使用してリソースとワークロードを識別する                                            | R   | CI                         |
| ログの保持とアーカイブを定義および設定する                                                  | CI  | R                          |
| 設定 AWS アカウント、ポリシー、アクセス管理の安全なベースライン                                     | CI  | RC                         |
| セキュリティインシデント対応 - 検出                                                    |     |                            |
| ログ記録、インジケータ、モニタリング                                                     |     |                            |
| インスタンスとアカウントのイベント管理を有効にするようにログ記録とモニタリングを設定する                           | CI  | R                          |
| セキュリティアラート AWS のサービス でサポートされているモニタリング                                  | I   | R                          |
| エンドポイントセキュリティツールのデプロイと管理                                               | CI  | R                          |
| AMS がサポートするエンドポイントセキュリティツールを使用して、インスタンスのマルウェアをモニタリングする                 | I   | R                          |

| アクティビティ                                                                     | お客様 | AWS Managed Services (AMS) |
|-----------------------------------------------------------------------------|-----|----------------------------|
| アウトバウンドメッセージングを通じて検出されたイベントを顧客に通知する                                         | I   | R                          |
| 特定のアカウントとワークロードの意思決定者に通知とその後の更新をルーティングして、インシデント対応時間を短縮する                    | R   | CI                         |
| AMS 標準検出サービス (Amazon GuardDuty やなど AWS Config) の定義、デプロイ、保守                  | CI  | R                          |
| AWS インフラストラクチャ変更ログを記録する                                                     | I   | RC                         |
| ログ記録とモニタリングを有効にして設定し、アプリケーションのイベント管理を有効にする                                  | R   | C                          |
| サポートされている AWS セキュリティサービス (Amazon GuardDuty など) で許可リスト、拒否リスト、カスタム検出を実装して維持する | RCI | R                          |
| セキュリティイベントレポート                                                              |     |                            |
| 疑わしいアクティビティまたはアクティブなセキュリティ調査を AMS に通知する                                     | R   | CI                         |
| 検出されたセキュリティイベントとインシデントを顧客に通知する                                              | I   | R                          |
| セキュリティインシデント対応プロセスをトリガーする可能性のある計画されたイベントを通知する                               | R   | CI                         |
| セキュリティインシデント対応 - 分析                                                         |     |                            |
| 調査と分析                                                                       |     |                            |

| アクティビティ                                                                | お客様 | AWS Managed Services (AMS) |
|------------------------------------------------------------------------|-----|----------------------------|
| サポートされている検出ソースによって生成されたサポートされているセキュリティアラートの初期レスポンスを実行する                | I   | RC                         |
| 利用可能なデータを使用して誤検出/真陽性を評価する                                              | RI  | RC                         |
| 必要に応じて、影響を受けるインスタンスのスナップショットを生成して顧客と共有します。                             | I   | R                          |
| 保管チェーン、ファイルシステム分析、メモリフォレンジック、バイナリ分析などのフォレンジックタスクを実行する                  | R   | CI                         |
| 調査に役立つアプリケーションログの収集                                                    | R   | I                          |
| セキュリティアラートの調査に役立つデータとログの収集                                             | RCI | RC                         |
| セキュリティ調査 AWS のサービス に 内の SMEs を関与させる                                    | CI  | R                          |
| 調査中にサードパーティーベンダーを関与させる (たとえば、EPS マルウェア対策調査や TrendMicro サポートチームとの連携など ) | RCI | I                          |
| 調査中にサポートされている から AWS のサービス 顧客に調査ログを共有する                                | I   | R                          |
| 通信                                                                     |     |                            |
| マネージドリソースの AMS 検出ソースからアラートと通知を送信する                                     | I   | R                          |
| アプリケーションセキュリティイベントのアラートと通知を管理する                                        | R   | I                          |

| アクティビティ                                                       | お客様 | AWS Managed Services (AMS) |
|---------------------------------------------------------------|-----|----------------------------|
| セキュリティインシデントの調査中に顧客のセキュリティ担当者を関与させる                           | R   | I                          |
| セキュリティインシデント対応 - 含む                                           |     |                            |
| 封じ込め戦略と実行                                                     |     |                            |
| 合意された封じ込め戦略の実行を決定し、封じ込め期間中にサービスの可用性に影響を与える可能性のある結果に同意する       | R   | CI                         |
| 影響を受けるシステムのバックアップを作成してさらに分析する                                 | CI  | R                          |
| アプリケーションとワークロードを含める (アプリケーション固有の設定またはレスポンスアクティビティ経由)          | R   | CI                         |
| セキュリティインシデントと影響を受けるリソースに基づいて封じ込め戦略を定義する                       | CI  | R                          |
| 影響を受けるシステムのポイントインタイムバックアップの暗号化と安全なストレージを有効にする                 | CI  | R                          |
| EC2 インスタンス、ネットワーク、IAM などの AWS リソースに対してサポートされている封じ込めアクションを実行する | CI  | R                          |
| セキュリティインシデント対応 - 根絶                                           |     |                            |
| 根絶戦略と実行                                                       |     |                            |
| セキュリティインシデントとお客様のアプリケーションワークロードで影響を受けるリソースに基づいて根絶オプションを定義する   | R   | CI                         |

| アクティビティ                                                                              | お客様 | AWS Managed Services (AMS) |
|--------------------------------------------------------------------------------------|-----|----------------------------|
| 合意された根絶戦略、根絶実行のタイミング、結果を決定する                                                         | R   | CI                         |
| AMS マネージドワークロードのセキュリティインシデントと影響を受けるリソースに基づいて根絶ステップを定義する                              | CI  | R                          |
| EC2 インスタンス、ネットワーク、IAM 根絶などの AWS リソースを根絶して強化する                                        | CI  | R                          |
| ( アプリケーション固有の設定またはレスポンスアクティビティを通じて) アプリケーションとワークロードを根絶して強化する                         | R   | I                          |
| セキュリティインシデント対応 - 復旧                                                                  |     |                            |
| 復旧の準備と実行                                                                             |     |                            |
| お客様からのリクエストに応じてバックアッププランとターゲットを設定する                                                  | R   | I                          |
| AMS マネージドワークロードを復元するためのバックアッププランを確認する                                                | CI  | R                          |
| サポートされている のリソースのバックアップ復元アクティビティを実行する AWS のサービス                                       | I   | R                          |
| お客様のアプリケーション、APP 設定、デプロイ設定をバックアップし、インシデント後にお客様のアプリケーションとワークロードを復元するためのバックアッププランを確認する | R   | I                          |
| アプリケーションとお客様のワークロードを復元する (アプリケーション固有の復元ステップによる )                                     | R   | I                          |



| アクティビティ                                                                                                          | お客様 | AWS Managed Services (AMS) |
|------------------------------------------------------------------------------------------------------------------|-----|----------------------------|
| セキュリティインシデント対応 – インシデント後レポート                                                                                     |     |                            |
| インシデント後レポート                                                                                                      |     |                            |
| 必要に応じて、学んだ適切な教訓とアクション項目を顧客のインシデント後に共有する                                                                          | I   | R                          |
| パッチ管理 <sup>9</sup>                                                                                               |     |                            |
| EC2 インスタンスでサポートされている OS と、サポートされている OS がプリインストールされたソフトウェアに対する適切な更新をモニタリングします。                                    | I   | R                          |
|                                                                                                                  | R   | C                          |
| セルフサービスプロビジョニング                                                                                                  |     |                            |
| 今後の更新を顧客に通知する (AMS Standard Patch のみに適用 )                                                                        | I   | R                          |
| 特定の更新や特定のスタックをパッチ適用アクティビティから除外する                                                                                 | R   | I                          |
| デフォルトおよびカスタムのメンテナンスウィンドウスケジュールとその他のパラメータ (メンテナンスウィンドウの期間など) を定義して、パッチ (AMS Patch に適用) を適用する<br><br>オーケストレーターのみ ) | R   | I                          |
| 特定のパッチをフィルタリングおよび除外する<br>カスタムパッチベースラインを定義する (AMS パッチオーケストレーターのみに適用 )                                             | R   | I                          |

| アクティビティ                                                                                              | お客様    | AWS Managed Services (AMS) |
|------------------------------------------------------------------------------------------------------|--------|----------------------------|
| インスタンスにタグ付けしてカスタムメンテナンスウィンドウとパッチベースラインに関連付ける (AMS パッチオーケストレーターのみに適用)                                 | R      | I                          |
| リソースのパッチステータスを追跡し、毎月のビジネスレビューで最新ではないシステムを強調表示します。                                                    | C      | R                          |
| Windows オペレーティングシステム、および Windows Update によって管理されるオペレーティングシステムにインストールされている Microsoft パッケージにパッチを適用する   | I<br>R | R<br>-                     |
| セルフサービスプロビジョニング                                                                                      |        |                            |
| Windows Update で管理されていないインストール済みアプリケーション、ソフトウェア、またはアプリケーションの依存関係にパッチを適用する                            | R<br>R | I<br>-                     |
| セルフサービスプロビジョニング                                                                                      |        |                            |
| Linux オペレーティングシステムと、オペレーティングシステムのネイティブパッケージマネージャー (Yum、Apt、Zypper など) による管理が有効になっているパッケージにパッチを適用します。 | I<br>R | R<br>-                     |
| セルフサービスプロビジョニング                                                                                      |        |                            |

| アクティビティ                                                                                              | お客様 | AWS Managed Services (AMS) |
|------------------------------------------------------------------------------------------------------|-----|----------------------------|
| Linux オペレーティングシステムのネイティブパッケージマネージャーによって管理されていない、インストールされているアプリケーション、ソフトウェア、またはアプリケーションの依存関係にパッチを適用する | R   | I                          |
| セルフサービスプロビジョニング                                                                                      | R   | -                          |
| 継続性管理                                                                                                |     |                            |
| バックアップスケジュールを指定する                                                                                    | R   | I                          |
| スケジュールに従ってバックアップを実行します。                                                                              | I   | R                          |
| セルフサービスプロビジョニング                                                                                      | R   | C                          |
| バックアップの検証                                                                                            | R   | I                          |
| バックアップ復元アクティビティをリクエストする                                                                              | R   | I                          |
| バックアップ復元アクティビティを実行します。                                                                               | I   | R                          |
| セルフサービスプロビジョニング                                                                                      | R   | C                          |
| 影響を受ける スタックと VPCs。                                                                                   | I   | R                          |
| セルフサービスプロビジョニング                                                                                      | R   | C                          |
| 影響を受けるカスタム/サードパーティーアプリケーションを復元する                                                                     | R   | C                          |
| レポート作成                                                                                               |     |                            |

| アクティビティ                                                 | お客様  | AWS Managed Services (AMS) |
|---------------------------------------------------------|------|----------------------------|
| 毎月のサービスレポートの準備と配信                                       | I    | R                          |
| での AMS AWS Outposts                                     | R    | I                          |
| API 監査履歴をオンデマンド (CloudTrail) で設定して取得します。                | I    | R                          |
| セルフサービスプロビジョニング                                         | R    | I                          |
| AWS Managed Services Interface を使用してインシデント履歴へのアクセスを提供する | I    | R                          |
| AWS Managed Services Interface を通じて変更履歴へのアクセスを提供します。    | I    | R                          |
| セルフサービスプロビジョニング                                         | 該当なし | 該当なし                       |
| サービスリクエスト管理                                             |      |                            |
| サービスリクエストを使用した情報のリクエスト                                  | R    | I                          |
| サービスリクエストへの返信                                           | I    | R                          |
| マネージドファイアウォール                                           |      |                            |
| AMS マネージドファイアウォールのデプロイをリクエストする                          | R    | I                          |
| AMS が管理するファイアウォールアーキテクチャの設計と最適化                         | I    | R                          |
| AWS インフラストラクチャと AMS マネージドファイアウォールアプライアンスのデプロイ           | I    | R                          |
| Firewall ライセンスの提供 (該当する AWS サービスの使用料を含む – EC2 など )      | R    | I                          |

| アクティビティ                                 | お客様 | AWS Managed Services (AMS) |
|-----------------------------------------|-----|----------------------------|
| デフォルトのドメイン許可リストを定義する                    | I   | R                          |
| カスタム許可リストとセキュリティポリシーを追加、変更、削除するリクエスト    | R   | I                          |
| AMS が管理するファイアウォールのアラートの設定               | I   | R                          |
| すべての AMS マネージドファイアウォール設定済みアラートのモニタリング   | I   | R                          |
| ファイアウォール設定のバックアップを実行する                  | I   | R                          |
| バックアップ復元アクティビティをリクエストする                 | R   | I                          |
| プロビジョニングされたリソースを新しいバージョンの製品で更新する        | I   | R                          |
| AMS が管理するファイアウォールログの記録                  | I   | R                          |
| AMS が管理するファイアウォールから CloudWatch にログを転送する | I   | R                          |
| AMS が管理するファイアウォールで設定変更をリクエストする          | R   | I                          |
| AMS が管理するファイアウォールで設定変更を承認する             | I   | R                          |
| AMS が管理するファイアウォールで設定変更を実行する             | I   | R                          |

<sup>8</sup>AMS は Amazon EC2 の AMIs のみを提供します

<sup>9</sup>AMS はOSes ベンダーと延長サポート契約に署名した場合にのみ、サポート終了 OS に責任を負います。

## AMS 環境の基本コンポーネント

### Multi-Account Landing Zone

これは、コアアカウントのインフラストラクチャのコンポーネントと潜在的なコストの見積もりです。これには、帯域幅、CloudWatch 詳細モニタリング、ログ記録、アラーム、Route53、Amazon S3、Simple Notification Service (Amazon SNS)、スナップショット、リザーブド Amazon EC2 インスタンスなどのその他のコストは含まれません。

AMS が管理する AWS ランディングゾーンインフラストラクチャに必要なコンポーネントに対して料金が発生します。見積もりでは、プレーン AMS マルチアカウントランディングゾーン環境のコストは 1 か月あたり 2,450 USD、プレーンアプリケーションアカウントの場合は 50 USD になります。

料金の詳細については、[「AWS の料金」](#)を参照してください。

### 基本的な環境コンポーネント

| コンポーネント     | コスト       | 説明                                                                                                                                                                                                                                                                                                                              |
|-------------|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 管理アカウント     | 60 USD    | <p>AWS Organizations Management アカウント。メンバーアカウントを作成して財務管理します。これには、AWS Landing Zone (ALZ) フレームワーク、アカウント設定スタックセット、AWS Organization サービスコントロールポリシー (SCPs)が含まれます。</p> <ul style="list-style-type: none"> <li>• Directory Service: 35 USD</li> <li>• CloudTrail: 7 USD</li> <li>• CloudWatch: 6 USD</li> <li>• その他: 12 USD</li> </ul> |
| 共有サービスアカウント | 2,000 USD | <p>アクセス管理 (Active Directory など)、エンドポイントセキュリティ管理 (Trend Micro)、踏み台 (SSH/RDP) に必要なインフラストラクチャとリソースが含まれています。見積もりは 1 か月あたり 2,400 USD です。この見積もりには、Trend Micro ライセンスのコストは含まれません。</p>                                                                                                                                                   |

| コンポーネント      | エスト。コスト | 説明                                                                                                                                                                                                                                                                                                                                         |
|--------------|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              |         | <ul style="list-style-type: none"><li>• EC2: 800 USD (最小踏み台数 )</li><li>• RDS: 300 USD (EPS)</li><li>• VPC (エンドポイント): 400 USD</li><li>• Directory Service: 300 USD</li><li>• CloudWatch: 100 USD</li><li>• GuardDuty: 15 USD</li><li>• Secrets Manager: 10 USD</li><li>• データ転送: 10 USD</li><li>• 設定: 10 USD</li><li>• その他: 45 USD</li></ul> |
| ネットワークアカウント  | 350 USD | <p>AMS アカウント、オンプレミスネットワーク、インターネットへの送信トラフィック間のネットワークルーティングのための中央ハブ。さらに、にはパブリック DMZ 踏み台 (AMS エンジニアが AMS 環境のホストにアクセスするためのエントリポイント) が含まれています。Transit Gateway と Direct Connect を通過するトラフィックによっては、料金が高くなる場合があります。</p> <ul style="list-style-type: none"><li>• EC2: 250 USD (踏み台 )</li><li>• VPC: 80 USD</li><li>• その他: 20 USD</li></ul>           |
| ログアーカイブアカウント | 20 USD  | <p>各 AMS 環境アカウントからの AWS CloudTrail および AWS Config ログファイルのコピーを含む S3 バケット。ログが収集されるにつれてコストが増加します。</p> <ul style="list-style-type: none"><li>• S3: 10 USD</li><li>• CloudWatch: 5 USD</li><li>• その他: 5 USD</li></ul>                                                                                                                           |

| コンポーネント     | エスト。コスト | 説明                                                                                                                                                                                                                                                                  |
|-------------|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| セキュリティアカウント | 20 USD  | <p>セキュリティ関連のオペレーションの中心的なハブであり、AMS コントロールプレーンサービスに通知とアラートをファネルするための主要なポイントです。さらに、には Amazon Guard Duty 管理アカウントが格納されています。Amazon GuardDuty を使用してより多くのイベントを分析すると、コストが増加します。</p> <ul style="list-style-type: none"> <li>CloudWatch: 15 USD</li> <li>その他: 5 USD</li> </ul> |

## Single-Account Landing Zone

次の表に、AMS マネージドインフラストラクチャの例のコンポーネントを示します。

基本的な環境コンポーネント、最終更新日 2020/07/09

| 名前                      | インスタンスタイプ | OS      | コンポーネントの数 |  |
|-------------------------|-----------|---------|-----------|--|
| mc-eps-dsm              | m5.large  | リナックス   | 2         |  |
| mc-management           | m5.large  | Windows | 2         |  |
| mc-bastion-dmz-ssh      | m5.large  | リナックス   | 2         |  |
| mc-bastion-customer-rdp | m5.large  | Windows | 2         |  |
| mc-eps-relay            | m5.large  | リナックス   | 2         |  |
| ディレクトリサービス              | 該当なし      | 該当なし    |           |  |
| 追加のコンポーネント              | 該当なし      | 該当なし    |           |  |

料金の詳細については、[「AWS 料金表」](#)を参照してください。



## AMS アカウントの制限

AMS マルチアカウントランディングゾーン内で考慮すべき制限には、AMS API の制限、AMS リソースの制限、AWS の制限の 3 種類があります。

AMS シングルアカウントランディングゾーン内で考慮すべき制限には、AMS API の制限と AWS の制限の 2 種類があります。

### AMS アカウント API の制限

このセクションでは、AWS Managed Services (AMS) が AMS SKMS API サービスをスロットリングした後のアカウントレベルの制限について説明します。つまり、リストされている APIs「スロットリング」されます (を受け取ります `ThrottleException`)。まれに、外部またはダウンストリームの依存関係によって AMS API がスロットリングされ、AMS によって API コールがより低いレートでスロットリングされる場合があります。

#### Note

AMS SKMS API の詳細については、AWS Artifact コンソールのレポートタブからリファレンスをダウンロードしてください。

リストされている AMS SKMS API ごとに、オペレーションは 10 TPS (トランザクション/秒) 後にスロットリングされます。

- `GetStack`
- `GetSubnet`
- `GetVpc`
- `ListAmis`
- `ListStackSummaries`
- `ListSubnetSummaries`
- `ListVpcSummaries`

### AMS マルチアカウントランディングゾーンアカウントのリソース制限

アカウントリソースの制限は、AMS マルチアカウントランディングゾーンアプリケーションアカウントと VPCs およびサブネットに関連しています。

## アプリケーションアカウントのリソース制限

組織ごとに 50 個のアプリケーションアカウントというソフト制限があります。50 を超えるアプリケーションアカウントのユースケースがある場合は、クラウドサービスデリバリーマネージャー (CSDM) に連絡して要件を伝達してください。

## VPCsとサブネットのリソース制限

組織の事前定義された AWS リージョン内のアプリケーションアカウントあたり 10 VPCs というソフト制限があります。

各 VPC には、2~3 つのアベイラビリティゾーンにまたがる 1~10 のプライベートサブネット層があります。さらに、各 VPC には、2~3 つのアベイラビリティゾーンにまたがる 0~5 つのパブリックサブネット層があります。これらの制限を超える要件がある場合は、CSDM または Cloud Architect に連絡してユースケースを確認してください。

## AMS マルチアカウントランディングゾーンアプリケーションとアカウントの比率

AMS マルチアカウントランディングゾーンでは、アプリケーションごとに 1 つのアカウントがサポートされています。ただし、各アプリケーションアカウントは低コストで、1 時間あたりの Transit Gateway への接続数と、Transit Gateway AWS を通過するトラフィック量に対して課金されます。したがって、アプリケーションがアカウントまたは VPCs に分離されるほど、コストは高くなります。

コストを削減し、適切な職務分離を確保するために、AMS では、1) 緊密に結合されたビジネスプロセスを持つチームによってアプリケーションをグループ化し、2) 異なる段階 (製品と非製品) にあるか、異なるチームによって管理されているアプリケーションを混在させないことをお勧めします。これにより、アカウントが少なくなり、アクセス管理と職務の分離が容易になり、トラフィックコストが軽減される可能性があります。

例: 企業では、本番環境に取引アプリケーションとポートフォリオ管理アプリケーションがあり、どちらのアプリケーションも投資 IT チームによって管理され、相互に大量のトラフィックを交換します。このシナリオでは、投資 IT チームが複数のアプリケーションアカウントへのアクセスをリクエストする必要はなく、トラフィックコストを節約できるため、会社は同じアカウントと同じ VPC の両方のアプリケーションをグループ化することでメリットを得ることができます。この場合、会社は開発段階で同じアプリケーション用に別のアカウントを作成し、開発チームにアクセスを提供する必要があります。

別のシナリオでは、企業は本番稼働中に給与アプリケーションと経理アプリケーションがあり、それぞれ人事 IT チームおよび経理 IT チームによって管理されています。ペイロールアプリケーションは

アカウントティングアプリケーションと情報を交換する必要がありますが、両方のアプリケーションをチームごとに異なるアカウントに分離し、ネットワーキングアカウントを使用して両方のアプリケーションの VPCs 間の接続を確立することをお勧めします。このようにして、同社は人事 IT チームが会計アプリケーションインフラストラクチャに影響を与える変更をリクエストすることを禁止しますが、その変更には知識がありません。

アカウントを組織単位 (OUs にグループ化する方法に関するヒント。OU は、アカウントを分類 (グループ化) し、それらのグループに基づいてポリシーと設定を に適用できる論理的なグループ化メカニズムです。OUs を作成するための推奨アプローチは、レポート構造内のチームの内部階層ではなく、特定のアカウントグループに適用する必要があるポリシーに基づいて作成することです。OU は Active Directory の OU と同等ではなく、で AD OU 構造をレプリケートしようとすることは推奨 AWS Organizations されず、構造の維持や運用が困難になります。

## AWS アカウントの制限

AWS アカウント制限は、AWS Managed Services (AMS) アカウントに適用されます。AWS サービスのデフォルトと現在の制限を決定する最も簡単な方法は、[AWS Service Quotas](#) を活用することです。AMS では、アカウントでサービスを実行するために、個々のサービス制限を適切なサイズにサイズ変更することをお勧めします (複数可)。制限はガードレールのように動作し、セキュリティとコストの暴走のためにアカウントを保護します。特定の制限を引き上げる場合は、AMS でサービスリクエストを送信すると、AMS Operations がユーザーに代わって制限を引き上げます。例えば、RDS インスタンスのデフォルトの制限 (またはクォータ) は 40 です。ワークロードに 50 個の RDS インスタンスが必要な場合は、AMS オペレーションのサービスリクエストを発行して、必要な値に制限を引き上げます。

## AMS サービスレベル目標 (SLOs)

次の表に、AWS Managed Services (AMS) サービスの目標を示します。インシデント管理を含む AMS サービスの他の側面のサービスレベルアグリーメント (SLAs) は、AMS にサブスクライブしたときに共有される SLA ドキュメントに記載されています。詳細については、CSDM にお問い合わせください。

## AMS サービスレベルの目標

| 機能          | パフォーマンスインジケータ (PI)                     | + (足し算)<br><br>(Business Days, M-F 8AM to 6PM local time) | プレミアム<br><br>(Calendar Days, 24 x 7) |
|-------------|----------------------------------------|-----------------------------------------------------------|--------------------------------------|
| 変更管理        | 自動 RFCs スケジュールまたは拒否するのにかかった時間          | <=30 分                                                    | <=30 分                               |
|             | スケジュールされた実行時間と比較したスケジュールされた RFCs の開始時間 | <=1 分                                                     | <=1 分                                |
|             | 自動ではない RFCs の承認/拒否にかかる時間。CT カタログで使用可能  | <=48 時間                                                   | <=24 時間                              |
|             | CT カタログで使用できない非自動 RFCs の承認/拒否にかかる時間    | <=5 日                                                     | <=5 日                                |
| 問題管理        | 根本原因分析 (RCA) の完了にかかる時間                 | <=10 日                                                    | <=10 日                               |
| サービスリクエスト管理 | 最初とその後のすべての応答の応答時間                     | <=8 時間                                                    | <=4 時間                               |

## サポートされている AWS サービス

AWS Managed Services (AMS) は、以下のサービスの運用管理サポート AWS サービスを提供します。各 AWS サービスは異なるため、AMS の運用管理レベルにより、サポートは基盤となる AWS サービスの性質と特性によって異なります。特定の AWS サービスは、AMS が提供する運用管理サポートサービスの複雑さと範囲に基づいてグループ化されます。

**Note**

A、B、C の 3 つのグループは、2021 年 3 月 16 日以前の AMS のお客様について、サポートプラン (Plus または Premium) に基づいて、AMS サービスのアカウントあたりの合計月額支出の割合として料金を示します。2021 年 3 月 16 日以降にオンボーディングされた AMS のお客様は、追加の料金情報についてサービスリクエストを送信する必要があります。グループ A は追加料金なしを示します。グループ B は、12% (Plus) または 18% (Premium) の追加料金を示します。グループ C は、25% (Plus) または 42% (Premium) の追加料金を示します。

1 つの星 (\*) は、AWS コンソールと APIs を使用してお客様が AMS マネージド環境にデプロイするサービスを示します。この方法でサービスをプロビジョニングおよび設定する際のお客様の責任の詳細については[AWS Managed Services \(AMS\) AMS Advanced オペレーションプランの機能](#)、「」の「自動およびセルフサービスのプロビジョニング管理」を参照してください。

2 つの星 (\*\*) は、の Amazon EC2 AWS Outposts がグループ B サービスとして請求されることを示します。でホストされている他のすべてのリソース AWS Outposts は、標準料金で請求されます。

## サポートされている AWS サービス

| グループ A                                                                                                                                                                                                                                                                                                                     | グループ B                                                                                                                                                                                                                                                                                                                                     | グループ C                                                                                                                                                                                                                                                                                               |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Amazon Alexa for Business*<br>Amazon Managed Streaming for Apache Kafka*<br>Amazon CloudFront<br>Amazon Elastic File System<br>Amazon Glacier<br>Amazon Simple Storage Service<br>AWS Amplify*<br>AWS AppMesh*<br>AWS Auto Scaling<br>AWS Backup<br>AWS CloudFormation<br>AWS Compute Optimizer<br>AWS Global Accelerator* | Amazon API Gateway*<br>Amazon AppStream*<br>Amazon Athena*<br>Amazon Bedrock*<br>Amazon CloudSearch*<br>Amazon Cognito*<br>Amazon Comprehend*<br>Amazon Connect*<br>Amazon Document DB (with MongoDB compatibility)*<br>Amazon DynamoDB*<br>Amazon EC2 Container Registry (ECR)*<br>Amazon Elastic Container Service (ECS) on AWS Fargate* | Amazon Aurora<br>Amazon CloudWatch<br>Amazon Elastic Block Store (EBS)<br>Amazon Elastic Compute Cloud**<br>Amazon Elastic Load Balancing (classic, application, and network; not gateway)<br>Amazon ElastiCache<br>Amazon OpenSearch Service<br>Amazon GuardDuty<br>Amazon Macie<br>Amazon Redshift |

| グループ A                                                                                                                                                                             | グループ B                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | グループ C                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AWS Identity and Access Management<br>AWS License Manager*<br>AWS Management Console<br>AWS Marketplace<br>AWS Lake Formation*<br>AWS Well-Architected Tool*<br>VM Import/ Export* | Amazon Elastic Kubernetes Service (EKS) on Fargate*<br>Amazon Elemental MediaConvert*<br>Amazon Elemental MediaPackage*<br>Amazon Elemental MediaStore*<br>Amazon Elemental MediaTailor*<br>Amazon Elastic MapReduce*<br>AmazonEventBridge*<br>Amazon Forecast*<br>Amazon FSx*<br>Amazon Inspector*<br>Amazon Kendra*<br>Amazon Kinesis Analytics*<br>Amazon Kinesis Data Stream*<br>Amazon Kinesis Firehose*<br>Amazon Kinesis Video Streams*<br>Amazon Lex*<br>Amazon Managed Service for Prometheus*<br>Amazon MQ*<br>Amazon Personalize**<br>Amazon Quantum Ledger Database (QLDB)*<br>Amazon QuickSight*<br>Amazon Rekognition*<br>Amazon SageMaker*<br>Amazon SimpleDB*<br>Amazon Simple Workflow*<br>Amazon Textract*<br>Amazon Transcribe*<br>Amazon Translate*<br>Amazon WorkSpaces* | Amazon Relational Database Service<br>Amazon Route 53<br>Amazon Route 53 Resolver DNS Firewall<br>Amazon Simple Email Service<br>Amazon Simple Notification Service<br>Amazon Simple Queue Service<br>Amazon Virtual Private Cloud (VPC)<br>AWS CloudTrail<br>AWS Config<br>AWS Database Migration Service<br>AWS Data Transfer<br>AWS Direct Connect<br>AWS Directory Service<br>AWS Key Management Service<br>AWS Systems Manager (SSM) |

| グループ A | グループ B                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | グループ C |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|
|        | <div><div>AWS AppSync*</div><div>AWS Audit Manager*</div><div>AWS Batch*</div><div>AWS Certificate Manager*</div><div>AWS CloudEndure*</div><div>AWS CloudHSM*</div><div>AWS CodeBuild*</div><div>AWS CodeCommit*</div><div>AWS CodeDeploy*</div><div>AWS CodePipeline*</div><div>AWS DataSync*</div><div>AWS Elemental MediaLive*</div><div>AWS Glue*</div><div>AWS Lambda*</div><div>AWS MigrationHub*</div><div>AWS Outposts**</div><div>AWS Resilience Hub*</div><div>AWS Secrets Manager*</div><div>AWS Security Hub*</div><div>AWS Service Catalog</div><div>AWS Service Catalog AppRegistry*</div><div>AWS Transfer for SFTP*</div><div>AWS Shield*</div><div>AWS Snowball*</div><div>AWS Step Functions*</div><div>AWS Transit Gateway*</div><div>AWS WAF*</div><div>AWS X-Ray*</div></div> |        |

以下でサポートされるものとして明示的に特定されていないソフトウェアまたはサービスに対するサービスの提供を AWS Managed Servicesにリクエストした場合、お客様がリクエストした設定に対して提供される AWS Managed Services、サービス条件の下で「ベータサービス」として扱われます。

## サポートされている設定

AWS Managed Services (AMS) がサポートする設定は次のとおりです。

- 言語: AMS は英語で利用できます。
- ファイアウォールサービス:
  - Amazon Route 53 Resolver DNS ファイアウォール
  - Palo Alto VM シリーズ次世代ファイアウォール
- セキュリティソフトウェア: Trend Micro からの Deep Security (必須)。AWS Marketplace: [Trend Micro Deep Security](#)
- 承認されたディレクトリサービス: Microsoft Active Directory (AD)
- [サポートされている AWS サービス](#).
- サポートされている AWS リージョン:

AMS はすべての AWS リージョンのサブセットで動作しますが、AMS API/CLI は「米国東部 (バージニア北部)」リージョンでのみ動作します。AMS 変更管理 API (amscm) または AMS サービスナレッジ管理 API (amsskms)、米国以外の東部リージョンで を実行する場合は、コマンド `--region us-east-1` に を追加する必要があります。

- 米国東部 (バージニア)
- 米国西部 (北カリフォルニア)
- 米国西部 (オレゴン)
- 米国東部 (オハイオ)
- カナダ (中部)
- 南米 (サンパウロ)
- 欧州 (アイルランド)
- 欧州 (フランクフルト)
- 欧州 (ロンドン)
- 欧州西部 (パリ)
- アジアパシフィック (ムンバイ)
- アジアパシフィック (ソウル)
- アジアパシフィック (シンガポール)
- アジアパシフィック (シドニー)
- アジアパシフィック (東京)
- Amazon マシンイメージ (AMIs): AMS は AMIsAMS でサポートされているオペレーティングシステムのサブセットの CIS Level 1 ベンチマークに基づいて、セキュリティ拡張イメージ (AMI) を提供します。セキュリティ拡張イメージが利用可能なオペレーティングシステムを見つけるに



は、「AMS セキュリティユーザーガイド」を参照してください。このガイドにアクセスするには、で AWS Artifact AWS Managed Services レポートタブをフィルタリングします。アクセスするには AWS Artifact、CSDM に問い合わせるか、[「AWS Artifact の開始方法」](#)を参照してください。

- サポートされるオペレーティングシステム

サポートされているオペレーティングシステム (x86-64)

- Amazon Linux 2023
- Amazon Linux 2 (AMS サポート終了日は 2026 年 6 月 30 日と想定)
- Oracle Linux 9.x、8.x
- Red Hat Enterprise Linux (RHEL) 9.x、8.x
- SUSE Linux Enterprise Server 15 SP6
- SUSE Linux Enterprise Server for SAP 15 SP3 以降
- Microsoft Windows Server 2025、2022、2019、2016
- Ubuntu 20.04、22.04、24.04

サポートされているオペレーティングシステム (ARM64)

- Amazon Linux 2023
- Amazon Linux 2 (AMS サポート終了日は 2026 年 6 月 30 日と想定)

- サポート終了 (EOS) オペレーティングシステム:

 Note

サポート終了 (EOS) オペレーティングシステムは、オペレーティングシステム製造元の一般的なサポート期間外であり、セキュリティリスクが増加しています。EOS オペレーティングシステムは、AMS が必要とするエージェントがオペレーティングシステムをサポートし、以下が当てはまる場合にのみ、サポートされている設定と見なされます。

1. 更新を受信できるオペレーティングシステムベンダーのサポートが延長されている、または
2. EOS オペレーティングシステムを使用するインスタンスは、アドバンスドユーザーガイドの AMS で指定されている[セキュリティコントロール](#)に従います。
3. AMS に必要なその他の補償セキュリティコントロールに準拠していること。

AMS が EOS オペレーティングシステムをサポートできなくなった場合、AMS はオペレーティングシステムをアップグレードするための[重要な推奨事項](#)を発行します。

AMS に必要なエージェントには、Amazon CloudWatch AWS Systems Manager、Endpoint Security (EPS) エージェント、Active Directory (AD) Bridge (Linux のみ) が含まれますが、これらに限定されません。

- Ubuntu Linux 18.04
- SUSE Linux Enterprise Server 15 SP3, SP4、および SP5
- SAP 15 SP2 用 SUSE Linux Enterprise Server
- SUSE Linux Enterprise Server 12 SP5
- SUSE Linux Enterprise Service for SAP 12 SP5
- Microsoft Windows Server 2012/2012 R2

## AMS でサポートされていないオペレーティングシステムの機能

サポートされていないオペレーティングシステムは、に記載されていないオペレーティングシステムです[サポートされている設定](#)。AMS は、サポートされていないオペレーティングシステムのインスタンスを[AWS、ベータ版およびプレビュー版のサービス条件の対象となる「お客様がリクエストした設定」](#)と見なします。

サポートされていないオペレーティングシステムのインスタンスでは、以下の AMS 機能の限定セットを使用できます。

| 機能              | 注                                                                                                                                     |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------|
| インシデント管理        | AMS はインシデント対応を提供します。                                                                                                                  |
| サービスリクエスト管理     | AMS はサービスリクエストに応答します。                                                                                                                 |
| 変更のリクエスト (RFCs) | AMS は RFCs の実行を評価します。サポートされていないオペレーティングシステムは、RFCsを実行する機能に影響を与える可能性があります。                                                              |
| モニタリング          | AMS は、Amazon EC2 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をモニタリングして応答します。システムステータスチェックには、ネットワーク接続の喪失、システム電源の喪失、物理ホストのソフトウェアの問題、およびネットワークの到達可能性に影響 |

| 機能        | 注                                                                                                               |
|-----------|-----------------------------------------------------------------------------------------------------------------|
|           | 響を与える物理ホストのハードウェアの問題が含まれます。<br><br>インスタンスのステータスチェックには、ネットワーク設定または起動設定の誤り、メモリの枯渇、ファイルシステムの破損、カーネルの互換性の欠如などがあります。 |
| セキュリティ管理  | AMS は Amazon EC2 <a href="#">GuardDuty の検出結果</a> をモニタリングして応答します。                                                |
| バックアップの管理 | AMS は、 <a href="#">AMS がカスタマイズしたプランとボルトを使用して、AMS Advanced for EC2 で継続性管理</a> を提供します。EC2 AWS Backup              |

## AMS Advanced インターフェイス

- AMS Advanced コンソール: AMS Advanced コンソールを使用して、RFCs の作成、インシデントの報告と対応、サービスリクエストの作成、既存の VPCs とスタックに関する情報の検索を行います。何をすべきかわからない場合、または AMS またはマネージドリソースに関するヘルプが必要な場合は、このインターフェイスを使用してサービスリクエストを作成します。
- AWS マネジメントコンソール: 多くの AWS コンソールは、AMS 情報の表示に役立ちます。次に例を示します。
  - Amazon EC2 コンソール: 踏み台 IP アドレス、Amazon EC2 Auto Scaling グループ、ロードバランサーなどのインスタンス情報を表示します。
  - マルチアカウントランディングゾーン AWS Config ルールのコンプライアンス: アカウント全体のコンプライアンスステータスを表示し、非準拠リソースを特定できます。
  - AWS CloudFormation コンソール: を使用して、スタック IDsを含むスタック情報を表示します (Amazon RDS スタックと Amazon RDS インスタンス IDs、イベント情報はこちら)。
  - Amazon RDS コンソール: を使用して、アカウントのサイトの WordPress アプリに対する投稿などのイベント情報を表示します。Amazon RDS インスタンス ID が必要です。

ログインロールのモードに応じて、AWS マネジメントコンソールへのアクセスレベルが異なります。モードの詳細については、「[AMS モード](#)」を参照してください。

- AMS Advanced 変更管理 API – 読み取り/書き込み: 変更管理 API (CM API) を使用して、リソースのモニタリング、ログ、バックアップ、パッチ設定など、マネージドインフラストラクチャへの追加と特定の変更をリクエストします。また、この API を使用して、リソースへのアクセスのリクエスト、リソースの削除、AMIs の作成、IAM インスタンスプロファイルの作成を行います。AMS CLI と SDKs を使用して CM API にアクセスできます。
- AMS SKMS API – 読み取り専用: この API を使用してマネージドリソースを一覧表示し、変更リクエストをレポートまたは準備するために必要な情報を取得します。
- サポート API: 標準 サポート API を使用して、インシデントとサービスリクエストをプログラムで作成して応答します。詳細については、[「の開始方法 サポート」](#)を参照してください。
- AWS APIs 読み取り専用: メイン IT 管理者は、AWS APIs を使用して、管理対象のすべてのリソースの表示、CloudTrail ログの表示、請求情報、その他の多くの読み取り機能を表示できます。

## AMS VPC エンドポイント

VPC エンドポイントを使用すると、インターネットゲートウェイを必要と AWS のサービス せずに VPC を にプライベートに接続できます。VPC のインスタンスは、サービスのリソースと通信するためにパブリック IP アドレスを必要としません。

エンドポイントは仮想デバイスです。エンドポイントは、VPC のインスタンスとサービスの間で通信を可能にする VPC コンポーネントであり、冗長性と高可用性を備え、水平にスケールされます。ネットワークトラフィックに対する可用性のリスクや帯域幅の制約はありません。詳細については、[「VPC エンドポイント」](#)を参照してください。

VPC エンドポイントには 2 種類あります。インターフェイスエンドポイントとゲートウェイエンドポイントです。

- ゲートウェイエンドポイント: アカウントの VPC では、Amazon S3 Gateway エンドポイントがデフォルトで有効になっています。
- インターフェイスエンドポイント: AMS 環境のインスタンスは、Amazon ネットワークを離れることなく、サポートされているサービスと通信できます。これはシングルアカウントのランディングゾーンではオプションであり、デフォルトではアカウントで有効になっていません。これを有効にするには、サービスリクエストを AMS オペレーションに送信します。ただし、マルチアカウントランディングゾーンの場合、インターフェイスエンドポイントは共有サービスアカウントでデフォルトで有効になっています。

AMS でサポートされているインターフェイスエンドポイントのリスト：

- AWS CloudFormation

- AWS CloudTrail
- AWS Config
- Amazon EC2 API
- AWS Key Management Service
- Amazon CloudWatch
- Amazon CloudWatch Events
- Amazon CloudWatch Logs
- AWS Secrets Manager
- Amazon SNS
- AWS Systems Manager
- AWS Security Token Service

## AMS で保護された名前空間

AWS Managed Services (AMS) の保護された名前空間のリスト。AWS リソースを使用する場合は、これらの名前空間を使用しないことで AMS との競合を防止します。他の AWS サービス名前空間の詳細については、[「Amazon リソースネーム \(ARNs AWS 「サービス名前空間」を参照してください。](#)

- ams-\* (これは新しいリソースに推奨される命名基準です )
- /ams/\* (これはパスベースのリソースに推奨される命名基準です )
- AWSManagedServices\* (これは、CamelCase が適切なリソースに推奨される命名基準です )
- ams\*、AMS\*、および Ams\*
- AWS\_\* および aws\*
- \*/aws\_reserved/\*
- CloudTrail\* および Cloudtrail\*
- codedeploy\_service\_role
- customer-mc-\*
- eps および EPS
- EPSMarketplaceSubscriptionRole
- EPSDB\*
- IAMPolicy\*

- INGEST\*
- LandingZone\*
- Managed\_Services\*
- managementhost
- mc\*、MC\*、および Mc\*
- MMS\*
- ms-
- NewAMS\*
- Root\*
- sentinel\* および Sentinel\*
- sentinel.int.
- StateMachine\*
- StackSet-ams\*
- StackSet-AWS-Landing-Zone
- TemplateId\*
- UnhealthyInServiceBastion
- VPC\_\*

## AMS 予約プレフィックス

AMS リソース属性は、特定のパターンに準拠する必要があります。例えば、IAM インスタンスプロファイル名、BackupVault 名、タグ名などは、AMS 予約プレフィックスで始めることはできません。リザーブドプレフィックスは次のとおりです。

```
*/aws_reserved/*  
ams- *  
/ams/*  
ams*  
AMS*  
Ams*  
aws*  
AWS*  
AWS_*  
AWSManagedServices*  
codedeploy_service_role
```

```
CloudTrail*
Cloudtrail*
customer-mc-*
eps
EPSDB*
IAMPolicy*
INGEST*
LandingZone*
Managed_Services*
managementhost
mc*
MC*
Mc*
MMS*
ms-
NewAMS*
Root*
sentinel*
Sentinel*
sentinel.int.
StackSet-ams*
StackSet-AWS-Landing-Zone
StateMachine*
TemplateId*
VPC_*
UnhealthyInServiceBastion
```

## AMS メンテナンスウィンドウ

AWS Managed Servicesメンテナンスウィンドウ (またはメンテナンスウィンドウ) は、AWS Managed Services (AMS) のメンテナンスアクティビティを実行し、毎月第 2 木曜日の太平洋標準時の午後 3 時から午後 4 時まで繰り返します。AMS は、48 時間前に通知することでメンテナンスウィンドウを変更する場合があります。これは AWS Managed Services (AMS) 用です。新しい AMS AMIs のデプロイなど、マネージドインフラストラクチャのメンテナンスアクティビティを実行します。

メンテナンスウィンドウは、AMS がパッチを適用し、オンボーディング時にメンテナンスウィンドウを決定するときです。パッチ適用サービス通知に記載されている提案されたパッチ適用ウィンドウに同意するか、別のウィンドウを提案することもできます。

メンテナンスウィンドウの作成に関するガイダンスについては、[「メンテナンスウィンドウ」](#)を参照してください。

# AMS 情報リソース

AMS には、成功に役立つ情報リソースがいくつか用意されています。

- AMS Accelerate ユーザーガイド: AMS Accelerate が提供するコンポーネントと機能、およびその使用方法を理解するのに役立ちます。AMS Accelerate の背景情報とデフォルト設定、検出結果リソース、ハウツーの例については、こちらを参照してください。[HTML インデックス](#)、[PDF](#)
- AMS Advanced ユーザーガイド: AMS Advanced が提供するコンポーネントと機能、およびその使用方法を理解するのに役立ちます。AMS Advanced の背景情報とデフォルト設定、検出結果リソース、ハウツーの例については、こちらを参照してください。[HTML インデックス](#)、[PDF](#)
- AMS Advanced Application Guide: AWS Managed Services インフラストラクチャにアプリケーションをデプロイする手順について説明します。アプリケーションのデプロイとメンテナンスの方法と考慮事項については、こちらを参照してください。[HTML インデックス](#)、[PDF](#)。
- AMS Advanced Onboarding Guide: AMS アカウントに基本的な AWS Managed Services マルチアカウントまたはシングルアカウントのランディングゾーンインフラストラクチャを作成するための最初のステップについて説明します。AMS アカウントの基本、検証、および AMS へのオンボーディングを準備するための質問については、こちらを参照してください。[HTML インデックス](#)、[PDF](#)。
- AMS Advanced Change Type Reference: AWS Managed Services が提供する現在の変更タイプに関する参考資料を提供します。これには、変更タイプスキーマや、各変更タイプとヒントのウォークスルーの例が含まれます。変更タイプに関する一般的な情報が含まれています。変更リクエスト (RFCs) と AMS 変更タイプ (CTs) のすべての側面を理解できます。関連情報へのリンクなど、変更タイプの詳細については、こちらを参照してください。[HTML インデックス](#)、[PDF](#)。
- AMS CM (変更管理) API リファレンス: AWS Managed Services CM API について説明します。この API は、変更リクエストを作成およびモニタリングするためのオペレーションと、マネージドサービスによって管理されるリソースに関する情報を提供します。[HTML インデックス](#)。
- AMS セキュリティガイド: 独自の AMS セキュリティ情報について説明します。

Private。AWS Artifact コンソールの AMS レポートタブで使用できます。

- AMS Developer's Resources: amscm と amsskms の両方の AMS CLI と SDK へのアクセス。<https://console.aws.amazon.com/managedservices/> を参照してください。
- AMS YouTube Videos: 動画で説明されている主要な顧客オペレーション。[AWS Managed Services YouTube Instructional Videos](#)」を参照してください。
- AMS ブログ記事: AWS Managed Services の専門分野に関する情報。[AWS ブログを参照してください](#)。



# AMS コンプライアンス

AMS は、以下の規格の監査を受けており、コンプライアンス認定を取得する必要があるソリューションの一部として使用できます。

## AMS でサポートされているコンプライアンス標準

AMS は AWS コンプライアンス標準をサポートしています。AWS コンプライアンスプログラムの詳細については、[AWS「コンプライアンス」](#)を参照してください。

これらは、AMS でサポートされている現在のコンプライアンス標準です。

FedRAMP: 米国連邦政府は、最も革新的な、安全でコスト効率の高い方法で米国国民にサービスを提供することに専念しています。クラウドコンピューティングは、連邦政府が運用効率を達成し、オンデマンドで革新して国家全体でミッションを前進させる方法において重要な役割を果たします。そのため、現在、多くの連邦政府機関が AWS クラウドサービスを使用して連邦政府データを処理、保存、送信しています。

[および FedRAMP の詳細については、「」](#)を参照してください。

HIPAA: AWS は、医療保険の相互運用性と説明責任に関する法律 (HIPAA) コンプライアンスプログラムを拡張し、AMS を [HIPAA 対応サービス](#)として含めました。AWS と事業提携契約 (BAA) を結んでいる場合は、AMS を使用して HIPAA 準拠のアプリケーションを構築できます。

医療情報の処理と保存に AMS を活用する方法については、[HIPAA に焦点を当てたホワイトペーパー](#)を参照してください。詳細については、「[HIPAA コンプライアンス](#)」を参照してください。

HITRUST: Health Information Trust Alliance Common Security Framework (HITRUST CSF) は、GDPR、ISO、NIST、PCI、HIPAA などの国内外で受け入れられている標準と規制を活用して、包括的なベースラインセキュリティとプライバシーコントロールのセットを作成します。

詳細については、[「HITRUST CSF」](#)を参照してください。

ISO 27001: ISO/IEC 27001:2013 は、ISO/IEC 27002 ベストプラクティスガイダンスに従って、セキュリティ管理のベストプラクティスと包括的なセキュリティコントロールを指定するセキュリティ管理標準です。この認定の基礎は、厳格なセキュリティプログラムの開発と実装です。これには、AWS がセキュリティを包括的かつ包括的な方法で永続的に管理する方法を定義する情報セキュリティ管理システム (ISMS) の開発と実装が含まれます。

詳細については、[「ISO/IEC 27001:2013」](#)を参照してください。

ISO 27017: ISO/IEC 27017:2015 は、クラウドコンピューティングの情報セキュリティの側面に関するガイダンスを提供し、ISO/IEC 27002 および ISO/IEC 27001 標準のガイダンスを補足するクラウド固有の情報セキュリティコントロールの実装を推奨します。このプラクティスコードは、クラウドサービスプロバイダーに固有の追加の情報セキュリティコントロール実装ガイダンスを提供します。

詳細については、[「ISO/IEC 27017:2015 コンプライアンス」](#)を参照してください。

ISO 27018: ISO/IEC 27018:2019 は、クラウド内の個人データの保護に焦点を当てた実践コードです。ISO/IEC 情報セキュリティ標準 27002 に基づいており、パブリッククラウドの個人を特定できる情報 (PII) に適用される ISO/IEC 27002 コントロールに関する実装ガイダンスを提供します。また、既存の ISO/IEC 27002 コントロールセットで対処されていないパブリッククラウド PII 保護要件に対処することを目的とした、一連の追加のコントロールおよび関連するガイダンスも提供します。

詳細については、[「ISO/IEC 27018:2019 Compliance」](#)を参照してください。

ISO 9001: ISO 9001:2015 は、組織内で効果的な品質管理を達成するために必要な構造、責任、手順を文書化し、レビューするためのプロセス指向のアプローチの概要を示しています。標準の特定のセクションには、次のようなトピックに関する情報が含まれています。

- 品質マニュアルのドキュメント、ドキュメントコントロール、プロセスインタラクションの決定など、品質管理システムの要件
- 管理の責任
- 人事や組織の作業環境を含む リソースの管理
- 設計からデリバリーまでのステップを含むサービス開発
- 顧客満足度
- 内部監査や是正措置、予防措置などの活動による QMS の測定、分析、改善

詳細については、[「ISO 9001:2015 コンプライアンス」](#)を参照してください。

PCI: AMS には、サービスプロバイダーレベル 1 の「PCI (Payment Card Industry) データセキュリティ標準 (DSS) バージョン 3.2 の準拠証明書」があります。AWS 製品およびサービスを使用してカード所有者データを保存、処理、または送信するお客様は、独自の PCI DSS コンプライアンス認定を管理する際に AMS を使用できます。

PCI DSS の詳細 (AWS PCI Compliance Package をリクエストする方法など) については、[「PCI DSS レベル 1」](#)を参照してください。重要なのは、PCI DSS バージョン 3.2 標準に準拠するように、AMS できめ細かなパスワードポリシーを設定する必要があります。適用する必要があるポリシーの詳細については、[「AWS Microsoft AD Directory の PCI コンプライアンスを有効にする」](#)を参照してください。

SOC: AMS System & Organization Control (SOC) レポートは、AMS が主要なコンプライアンスコントロールと目標を達成する方法を示す、独立したサードパーティーの検査レポートです。これらのレポートの目的は、運用とコンプライアンスをサポートするために確立された AMS コントロールをユーザーと監査人が理解できるようにすることです。AMS SOC レポートには 3 つのタイプがあります。

- AWS SOC 1 レポート - [AWS Artifact でダウンロード](#)
- AWS SOC 2: セキュリティ、可用性、機密性レポート - [AWS Artifact でのダウンロード](#)
- [AWS SOC 3: セキュリティ、可用性、機密性レポート](#)

詳細については、[「SOC Compliance」](#)を参照してください。

## 共有責任

PCI コンプライアンスを含むセキュリティは、[共有責任](#)です。AMS コンプライアンスステータスは、AWS クラウドで実行するアプリケーションに自動的に適用されないことを理解することが重要です。AWS サービスの使用が標準に準拠していることを確認する必要があります。AMS が特定のアクティビティで顧客と連携する方法の詳細については、AMS を参照してください[AMS 責任マトリックス \(RACI\)](#)。

## AMS Amazon マシンイメージ (AMIs)

AMS は、AMS がサポートするオペレーティングシステム用に毎月更新された Amazon マシンイメージ (AMIs) を生成します。さらに、AMS は、AMS でサポートされているオペレーティングシステムのサブセットの CIS レベル 1 ベンチマークに基づいてセキュリティ拡張イメージ (AMIs) も生成します。<https://docs.aws.amazon.com/managedservices/latest/userguide/supported-configs.html> セキュリティ拡張イメージが利用可能なオペレーティングシステムを確認するには、AMS セキュリティユーザーガイドを参照してください。このユーザーガイドは、AWS AWS Managed Services 用にフィルタリングされた AWS Artifact -> レポートページ (左側のナビゲーションペインのレポートオプションを参照) から入手できます。AWS Artifact にアクセスするには、 から CSDM に連絡して手順を確認するか、[「AWS Artifact の開始方法」](#)を参照してください。

新しい AMS AMIs 「AMS AMI」という Amazon Simple Notification Service (Amazon SNS) 通知トピックをサブスクライブできます。詳細については、[「SNS を使用した AMS AMI 通知」](#)を参照してください。

AMS AMI の命名規則は `customer-ams-rhel6-2018.11-3customer-ams-<operating system>-<release date> - <version>`。

で始まる AMS AMIs のみを使用してくださいcustomer。

AMS では、常に最新の AMI を使用することをお勧めします。最新の AMIs は、次のいずれかで確認できます。

- AMS コンソールの AMIs ページを参照してください。
- CSDM またはこの ZIP ファイルを介して利用可能な最新の AMS AMI CSV ファイルを表示する:  
[AMS 11.2024 AMI コンテンツと CSV ファイルを ZIP で表示します](#)。

過去の AMI ZIP ファイルについては、[「Doc History」](#)を参照してください。

- この AMS SKMS コマンドの実行 (AMS SKMS SDK が必要):

```
aws amsskms list-amis --vpc-id VPC_ID --query "Amis.sort_by(@,&Name)[?starts_with(Name,'customer')].[Name,AmiId,CreationTime]" --output table
```

オペレーティングシステム (OS) によって AWS AMIsに追加された AMS AMI コンテンツ

- Linux AMIs:
  - [AWS CLI ツール](#)
  - [NTP](#)
  - [Trend Micro Endpoint Protection Service エージェント](#)
  - [コードデプロイ](#)
  - [PBIS Enterprise / Beyond Trust AD Bridge](#)

#### Note

2022 年 6 月現在、BeyondTrust は PBIS Open をサポートしていません。2022 年 6 月以降、AMS がサポートする AMIs で PBIS Open を使用することはできません。AMS が 2022 年 6 月より前に AMI をサポートしている場合は、独自の判断で PBIS Open を引き続き使用できます。

- [SSM Agent](#)
- 重要なパッチの Yum アップグレード
- AMS カスタムスクリプト/管理ソフトウェア (起動、AD 結合、モニタリング、セキュリティ、ログ記録の制御)
- Windows Server AMIs:
  - [Microsoft .NET Framework 4.5](#)
  - [PowerShell 5.1](#)
  - [AWS Tools for Windows PowerShell](#)
  - 起動、AD 結合、モニタリング、セキュリティ、ログ記録を制御する AMS PowerShell モジュール
  - [Trend Micro Endpoint Protection Service エージェント](#)
  - [SSM Agent](#)
  - [CloudWatch エージェント](#)
  - EC2Config サービス (Windows Server 2012 R2 経由)
  - EC2Launch (Windows Server 2016 および Windows Server 2019)
  - EC2LaunchV2 (Windows Server 2022 以降)

#### Linux ベースの AMIs:

- Amazon Linux 2023 (最新のマイナーリリース) (最小 AMI はサポートされていません)
- Amazon Linux 2 (最新のマイナーリリース)
- Amazon Linux 2 (ARM64)
- Red Hat Enterprise 8 (最新のマイナーリリース)
- Red Hat Enterprise 9 (最新のマイナーリリース)
- SUSE Linux Enterprise Server 15 SP6
- Ubuntu Linux 20.04
- Ubuntu Linux 22.04
- Ubuntu Linux 24.04
- Amazon Linux: 製品の概要、料金情報、使用状況情報、サポート情報については、[「Amazon Linux 2」](#) を参照してください。

詳細については、「[Amazon Linux 2 に関するよくある質問](#)」を参照してください。

- SUSE Linux Enterprise Server for SAP アプリケーション 15 SP6:
  - アカウントごとに次の手順を 1 回実行します。
    1. AWS Marketplace に移動します。
    2. SUSE 15 SAP 製品を検索します。
    3. [サブスクリプションを続行する] を選択します。
    4. 次に [規約の受諾] を選択します。
  - SAP Applications 15 SP6 インスタンス用の新しい SUSE Linux Enterprise Server を起動する必要があるたびに、次の手順を実行します。
    1. サブスクライブしている SUSE Linux Enterprise Server for SAP Applications 15 AMI の AMI ID を書き留めます。
    2. デプロイの作成 | 高度なスタックコンポーネント | EC2 スタック | 変更タイプの作成 ct-14027q0sjyt1h RFC。 *InstanceAmiId* をサブスクライブした AWS Marketplace AMI ID に置き換えます。

Windows ベースの AMIs:

最新の Windows AMIs に基づく Microsoft Windows Server (2016、2019、2022、2025)。

AMIs [「AMI の作成」](#) を参照してください。

AMS AMIs オフボーディング:

AMS は、依存関係への影響を避けるため、オフボーディング中に AMIs の共有を解除しません。アカウントから AMS AMIs を削除する場合は、cancel-image-launch-permission API を使用して特定の AMIs を非表示にできます。たとえば、以下のスクリプトを使用して、以前にアカウントと共有されたすべての AMS AMIs を非表示にできます。

```
for ami in $(aws ec2 describe-images --executable-users self --owners 027415890775 --
query 'Images[].ImageId' --output text) ;
do
    aws ec2 cancel-image-launch-permission --image-id $ami ;
done
```

スクリプトをエラーなしで実行するには、AWS CLI v2 がインストールされている必要があります。AWS CLI のインストール手順については、[「AWS CLI の最新バージョンのインストールまたは更新」](#) を参照してください。cancel-image-launch-permission コマンドの詳細については、「」を参照してください[cancel-image-launch-permission](#)。



## セキュリティ強化 AMIs

AMS は、AMS でサポートされているオペレーティングシステムのサブセットの CIS レベル 1 ベンチマークに基づくセキュリティ拡張イメージ (AMIs) を提供します。セキュリティ拡張イメージが利用可能なオペレーティングシステムを確認するには、AWS Managed Services (AMS) カスタマーセキュリティガイドを参照してください。このガイドにアクセスするには、を開き AWS Artifact、左側のナビゲーションペインでレポートを選択し、AWS Managed Services をフィルタリングします。アクセス方法については AWS Artifact、CSDM に問い合わせるか、[「の開始方法 AWS Artifact」](#)を参照してください。

## AD FS と AMS の統合の仕組み

スタックと VPCs。VPC とスタックが作成されると、事前設定された Active Directory セキュリティグループを介してアクセスが許可されます。さらに、へのアクセス AWS マネジメントコンソールは、Active Directory フェデレーションサービス (AD FS)、または SAML をサポートするフェデレーションソフトウェアを使用して、AWS マネジメントコンソールへのシングルサインオン (SSO) 用に設定できます。

### Note

AMS は、Ping、Okta などの多くのフェデレーションサービスにフェデレーションできます。AD FS に限定されません。ここでは、利用可能な 1 つのフェデレーションテクノロジーの例を示します。

ここでの情報は、このブログ記事 [「Windows Active Directory、AD FS、および SAML 2.0 AWS の使用へのフェデレーションの有効化」](#) から複製されています。

1. フローは、ユーザー (ボブを呼び出します) がドメイン内の AD FS サンプルサイト (<https://Fully.Qualified.Domain.Name.Here/adfs/ls/IdpInitiatedSignOn.aspx>) を参照したときに開始されます。AD FS をインストールすると、このページを含むデフォルトのウェブサイトの adfs という名前の新しい仮想ディレクトリが表示されます。
2. サインオンページは、AD に対して Bob を認証します。Bob が使用しているブラウザによっては、AD のユーザー名とパスワードの入力を求められる場合があります。
3. Bob のブラウザは、AD FS からの認証レスポンスの形式で SAML アサーションを受け取ります。



4. Bob のブラウザは、SAML アサーションを AWS SAML のサインインエンドポイント (<https://signin.aws.amazon.com/saml>) に投稿します。バックグラウンドでは、サインインは [AssumeRoleWithSAML](#) API を使用して一時的なセキュリティ認証情報をリクエストし、のサインイン URL を構築します AWS マネジメントコンソール。
5. Bob のブラウザはサインイン URL を受け取り、コンソールにリダイレクトされます。

Bob の視点では、プロセスは透過的に行われます。彼は内部ウェブサイトから始めて、AWS 認証情報を指定しなくても AWS マネジメントコンソールにたどり着きます。

#### Note

AMS コンソールへのフェデレーションの設定の詳細については、以下を参照してください。

- マルチアカウントランディングゾーン: [AMS コンソールへのフェデレーションの設定](#)
- 単一アカウントランディングゾーン: [AMS コンソールへのフェデレーションの設定](#)

さらに、[付録: AD FS クレームルールと SAML 設定](#)を参照してください。AWS Microsoft AD を使用して、コンプライアンス要件の対象となる Active Directory 対応アプリケーションを AWS クラウドでサポートする方法については、「[Microsoft AD コンプライアンスの管理](#)」を参照してください。

## AMS Managed Active Directory

AMS は、AMS が Active Directory (AD) インフラストラクチャオペレーションを処理できるようにする Managed Active Directory (別名 Managed AD) と呼ばれる新しいサービスを提供し、Active Directory 管理を制御できるようになりました。

Managed AD の AMS サポートは、Amazon Relational Database Service (Amazon RDS) の AMS サポートと似ています。いずれの場合も、AWS (AMS を含む) はサービスを実行しているインフラストラクチャの作成と管理をサポートし、アクセスコントロールとすべての管理機能を実行します。このモデルには次の利点があります。

- セキュリティリスクを制限します。AWS AMS にはドメインに対する管理者権限は必要ありません。
- 直接統合: 現在の認可モデルを使用し、AMS とインターフェイスすることなく AD と統合できます。

**注意:**

- AMS もユーザーも Managed AD ドメインコントローラーにアクセスできないため、ドメインコントローラーにソフトウェアをインストールすることはできません。ドメインコントローラーにソフトウェアをインストールする必要があるサードパーティソリューションは許可されていないため、これは重要です。

アクセスは次のようになります。

- AWS Directory Service チーム: ドメインコントローラーにアクセスできます。
- AMS: Directory Service APIs にアクセスして、ドメインで特定のアクションを実行できます。これらのアクションには、AD スナップショットの作成、AD スキーマの変更、その他のアクションが含まれます。
- ユーザー: ユーザー、グループなどを作成するためのドメイン (AD) にアクセスできます。
- 従来の AD 環境のすべての機能が Managed AD 環境で利用できるわけではないため、企業 AD を移行する前に Managed AD で概念実証を実行することをお勧めします。
- AMS は AD 管理を管理またはガイダンスしません。例えば、AMS は組織単位構造、グループポリシー構造、AD ユーザーの命名規則などに関するガイダンスを提供しません。

次のようになります。

1. AMS は AWS アカウント、AMS アカウントとは別の新しい をオンボードし、AWS Directory Service を通じて Active Directory (AD) 環境をプロビジョニングします ([AWS Directory Service とはも参照してください](#))。

以下は、AMS が Managed AD にオンボードするために、システムインテグレーターがお客様から収集する必要がある情報です。

- アカウント情報
  - AMS 管理 AD: AWS アカウント number 用に AWS アカウント 作成された のアカウント ID
  - Managed AD をオンボードするリージョン : AWS リージョン
- マネージド Active Directory 情報 :
  - Microsoft AD Edition: Standard/Enterprise. AWS Microsoft AD (Standard Edition) には、1 GB のディレクトリオブジェクトストレージが含まれています。この容量は、ユーザー、グループ、コンピュータなど、最大 5,000 ユーザーまたは 30,000 ディレクトリオブジェクトをサポートできます。AWS Microsoft AD (Enterprise Edition) には 17 GB のディレクトリオブジェ

クトストレージが含まれており、最大 100,000 ユーザーまたは 500,000 オブジェクトをサポートできます。

詳細については、[AWS Directory Service のFAQs](#)」を参照してください。

- ドメイン FQDN: AMS Managed AD ドメインの FQDN。
- ドメイン NetBIOS 名: AMS Managed AD ドメインの NetBIOS 名。
- Managed AD 統合先の AMS 標準アカウントのアカウント番号 (AMS は AMS 標準アカウントの AD から Managed AD への一方向の信頼を設定します )
- Active Directory スキーマの変更が必要で、必要な場合はどのような変更が必要ですか？
- デフォルトでは、2 つのドメインコントローラーがプロビジョニングされます。さらに が必要ですか？ その場合は、必要な数と理由を教えてください。
- Managed Active Directory 情報のネットワーク :
  - ドメインコントローラーの Managed AD VPC CIDR ( Managed AD ドメインコントローラーのプライベートサブネット範囲内の CIDR)。
  - ドメインコントローラーのサブネット CIDR 1: [CIDR、AMS Managed AD VPC CIDR の一部である必要があります]
  - ドメインコントローラーのサブネット CIDR 2: [CIDR、AMS Managed AD VPC CIDR の一部である必要があります]

例:

- マネージド AD VPC CIDR: 192.168.0.0/16
- ドメインコントローラーの CIDR 1: 192.168.1.0/24
- ドメインコントローラーの CIDR 2: 192.168.2.0/24

IP アドレスの競合を回避するには、指定する Managed AD VPC CIDR が、企業ネットワークで使用している他のプライベートサブネット CIDR と競合しないことを確認してください。

- VPN テクノロジー (オプション): [Direct Connect/Direct Connect と VPN]
  - ゲートウェイの BGP 自律システム番号 (ASN): [お客様が用意した ASN]
  - ゲートウェイの外部インターフェイスのインターネットルーティング可能な IP アドレス。アドレスは静的である必要があります: [お客様提供の IP アドレス]
- VPN 接続に静的ルートが必要かどうか: [はい/いいえ]

2. AMS は AD 環境の管理者アカウントのパスワードを提供し、AMS エンジニアが AD 環境にアクセスできなくなるようにパスワードをリセットするよう要求します。

3. 管理者アカウントのパスワードをリセットするには、Active Directory ユーザーとコンピュータ (ADUC) を使用して Active Directory 環境に接続します。ADUC およびその他のリモートサーバー管理ツール (RSAT) は、AMS 以外のインフラストラクチャでプロビジョニングされた管理ホストにインストールして実行する必要があります。Microsoft には、このような管理ホストを保護するためのベストプラクティスがあります。詳細については、[「安全な管理ホストの実装」](#)を参照してください。これらの管理ホストを使用して Active Directory 環境を管理します。
4. 日常業務では、AMS は、VPC 設定、AD バックアップ、AD 信頼の作成と削除など、AWS Directory Service 側 AWS アカウント までの を管理します。AD 環境を使用および管理します。例えば、ユーザーの作成、グループの作成、グループポリシーの作成などです。

最新の RACI テーブルについては、[「サービスの説明」](#)の「役割と責任」セクションを参照してください。

## AMS アプリケーションのデプロイ

AMS Application Developer ガイドには、以下のデプロイの詳細な説明とチュートリアルが記載されています。

- AMS ワークロード取り込み CT を使用すると、ユーザーと AMS クラウド移行パートナーは、既存のワークロードを AMS マネージド VPC に簡単に移動できます。AMS ワークロード取り込みを使用して、デプロイ | 取り込み | 移行パートナー移行インスタンスからのスタック | CT の作成 (ct-257p9zjk14ija) で RFC を送信することで、AMS AMI を作成できます。インスタンスをオンプレミスから移行パートナー、およびインスタンスを取り込むターゲット AMS VPC とサブネット AWS によって に移行する必要があります。

詳細については、「ワークロード取り込み」の「AMS アプリケーション開発者[ガイド](#)」を参照してください。

- CloudFormation 取り込み変更タイプ (ct-36cn2avfrj9v) 機能を使用すると、既存の CloudFormation テンプレートを使用して、AMS マネージド VPC にカスタムスタックを簡単にデプロイできます。

詳細については、「CloudFormation テンプレート取り込み」の「AMS アプリケーション開発者[ガイド](#)」を参照してください。 [CloudFormation](#)

- オンプレミスデータベースを新しいデータベースに AMS 管理の Amazon S3 バケットまたは Amazon RDS インスタンスにインポートできます。これを行うには、デプロイ | 高度なスタック

クコンポーネント | Database Migration Service (DMS) の変更タイプを使用します。これには、レプリケーションインスタンスの作成 (ct-27apldkhqr0ol)、レプリケーションサブネットグループの作成 (ct-2q5azjd8p1ag5)、レプリケーションタスクの作成 (ct-1d2fml15b9eth)、ソースエンドポイントの作成 (ct-0attesnjqy2cx)、ソースエンドポイントの作成 (S3) (ct-2oxl37nphsrjz)、ターゲットエンドポイントの作成 (ct-3gf8dolbo8x9p)、またはターゲットエンドポイントの作成 (ct-05muqzievnxk5) が含まれます。

詳細については、[「Database Migration Service」](#)の「AMS アプリケーション開発者ガイド」を参照してください。

- オンプレミスの MS SQL データベースを AMS マネージド RDS SQL インスタンスの新しいデータベースにインポートできます。これを行うには、さまざまな AMS 変更タイプ、Amazon RDS API、および AWS コンソールを使用します。

詳細については、[「Database \(DB\) Import to MS SQL RDS」](#)の「AMS Application Guide」を参照してください。

# AWS Managed Services でのサービス管理

## トピック

- [AWS Managed Services でのアカウントガバナンス](#)
- [AWS Managed Services でのサービス開始](#)
- [顧客関係管理 \(CRM\)](#)
- [AWS Managed Services コスト最適化](#)
- [AWS Managed Services のサービス時間](#)
- [AWS Managed Services でのヘルプの取得](#)

AMS サービスの仕組み。

## AWS Managed Services でのアカウントガバナンス

このセクションでは、AMS アカウントガバナンスについて説明します。

お客様は、AMS 全体でアドバイザリ支援を提供するクラウドサービスデリバリーマネージャー (CSDM) として指定され、マネージド環境のユースケースとテクノロジーアーキテクチャを詳細に理解しています。CSDMs、必要に応じてアカウントマネージャー、テクニカルアカウントマネージャー、AWS Managed Services クラウドアーキテクト (CAs)、および AWS ソリューションアーキテクト (SAs) と連携して、新しいプロジェクトの起動を支援し、ソフトウェア開発および運用プロセス全体でベストプラクティスのレコメンデーションを提供します。CSDM は AMS の主な連絡先です。CSDM の主な責任は次のとおりです。

- 顧客との毎月のサービスレビューミーティングを主催し、主導します。
- セキュリティ、環境のソフトウェア更新、最適化の機会に関する詳細を提供します。
- AMS の機能リクエストを含む要件を支持します。
- 請求およびサービスレポートリクエストに回答して解決します。
- 財務およびキャパシティ最適化のレコメンデーションに関するインサイトを提供します。

## AWS Managed Services でのサービス開始

サービス開始日: AWS Managed Services アカウントのサービス開始日は、その AWS Managed Services アカウントのオンボーディング要件に設定されたアクティビティが完了したことを AWS が

通知した最初の暦月の最初の日です。ただし、AWS が暦月の 20 日以降にそのような通知を行う場合、サービス開始日は、そのような通知の日付の翌日の 2 番目の暦月の最初の日です。

## サービスの開始

- R は、タスクを達成するために作業を行う責任者を表します。
- 「情報」の略です。多くの場合、タスクまたは成果物の完了時にのみ、進捗状況が通知される当事者です。

## サービス開始

| ステップ # | ステップタイトル                         | 説明                                                | お客様 | AMS |
|--------|----------------------------------|---------------------------------------------------|-----|-----|
| 1.     | お客様の AWS アカウントの引き渡し              | 顧客が新しい AWS アカウントを作成し、AWS Managed Services に引き渡す   | R   | I   |
| 2.     | AWS Managed Services アカウント - 設計  | AWS Managed Services アカウントの設計を確定する                | I   | R   |
| 3.     | AWS Managed Services アカウント - ビルド | AWS Managed Services アカウントは、ステップ 2 の設計に従って構築されます。 | I   | R   |

## 顧客関係管理 (CRM)

AWS Managed Services (AMS) は、明確に定義された関係が確立され、維持されるように、顧客関係管理 (CRM) プロセスを提供します。この関係の基盤は、ビジネス要件に関する AMS のインサイトに基づいています。CRM プロセスは、以下を正確かつ包括的に理解するのに役立ちます。

- ビジネスニーズとそのニーズを満たす方法
- 機能と制約
- AMS とさまざまな責任と義務



CRM プロセスにより、AMS は一貫した方法を使用してサービスを提供し、AMS との関係のガバナンスを提供できます。CRM プロセスには以下が含まれます。

- 主要な利害関係者の特定
- ガバナンスチームの設立
- サービスレビューミーティングの実施と文書化
- エスカレーション手順を含む正式なサービス苦情手順の提供
- 満足度とフィードバックプロセスの実装とモニタリング
- 契約の管理

## CRM プロセス

CRM プロセスには、次のアクティビティが含まれます。

- ビジネスプロセスとニーズを特定して理解します。AMS との契約により、ステークホルダーが特定されます。
- ニーズと要件を満たすために提供されるサービスを定義します。
- サービスレビュー会議で会議を開き、AMS サービスの範囲、SLA、契約、ビジネスニーズの変更について話し合います。暫定会議を開催して、パフォーマンス、成果、問題、アクションプランについて話し合うことができます。
- 顧客満足度調査と会議で提供されたフィードバックを使用して、満足度をモニタリングします。
- 内部で測定された毎月のパフォーマンスレポートのパフォーマンスを報告します。
- サービスを確認して、改善の機会を決定します。これには、提供される AMS サービスのレベルと品質に関する頻繁なコミュニケーションが含まれます。

## CRM 会議

AMS クラウドサービスデリバリーマネージャー (CSDMs) は、サービストラック (運用、セキュリティ、製品イノベーション) とエグゼクティブトラック (SLA レポート、満足度評価、ビジネスニーズの変化) について、定期的に会議を開催します。



| 会議                  | 目的                                                                                                                 | モード                              | 参加者                                                                                                                                    |
|---------------------|--------------------------------------------------------------------------------------------------------------------|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| 週次ステータスレビュー (オプション) | <p>未解決の問題またはインシデント、パッチ適用、セキュリティイベント、問題レコード</p> <p>12 週間の運用傾向 (+/- 6)</p> <p>アプリケーションオペレーターの懸念</p> <p>週末のスケジュール</p> | オンサイトのお客様のlocation/Telecom/Chime | <p>AMS: CSDM とクラウドアーキテクト (CA)</p> <p>顧客に割り当てられたチームメンバー (クラウド/インフラストラクチャ、アプリケーションサポート、アーキテクチャチームなど)</p>                                 |
| 毎月のビジネスレビュー         | <p>サービスレベルのパフォーマンス (レポート、分析、傾向) を確認する</p> <p>財務分析</p> <p>製品ロードマップ</p> <p>CSAT</p>                                  | オンサイトのお客様のlocation/Telecom/Chime | <p>AMS: CSDM、クラウドアーキテクト (CA)、AMS アカウントチーム、AMS テクニカルプロダクトマネージャー (TPM) (オプション)、AMS OPS マネージャー (オプション)</p> <p>お客様: アプリケーションオペレーターの担当者</p> |
| 四半期ごとのビジネスレビュー      | <p>スコアカードとサービスレベルアグリーメント (SLA) のパフォーマンスと傾向 (6 か月)</p> <p>今後の 3/6/9/12 か月の計画/移行</p>                                 | オンサイトのカスタマーロケーション                | AMS: CSDM、クラウドアーキテクト、AMS アカウントチー                                                                                                       |

| 会議 | 目的           | モード | 参加者                                       |
|----|--------------|-----|-------------------------------------------|
|    | リスクとリスクの軽減   |     | ム、AMS サービスディレクター、AMS オペレーションマネージャー        |
|    | 主要な改善イニシアチブ  |     |                                           |
|    | 製品ロードマップ項目   |     |                                           |
|    | 将来の方向性に沿った機会 |     | お客様: アプリケーションオペレーター担当者、サービス担当者、サービスディレクター |
|    | 財務           |     |                                           |
|    | コスト削減の取り組み   |     |                                           |
|    | ビジネスの最適化     |     |                                           |

## CRM ミーティングの手配

AMS CSDM は、以下を含む会議を文書化する責任があります。

- アクション項目、問題、参加者リストを含むアジェンダの作成。
- 各会議でレビューされたアクション項目のリストを作成して、項目がスケジュールどおりに完了および解決されていることを確認します。
- 会議の後 1 営業日以内に、会議の参加者に会議議事録とアクション項目リストを E メールで配布します。
- 会議の議事録を適切なドキュメントリポジトリに保存します。

CSDM がない場合、会議を主導する AMS 担当者が議事録を作成して配布します。

### Note

CSDM はお客様と協力してアカウントガバナンスを確立します。

## CRM 月次レポート

AMS CSDM は、毎月のサービスパフォーマンスプレゼンテーションを準備して送信します。プレゼンテーションには、以下に関する情報が含まれています。

- レポート日
- 概要とインサイト :
  - 主なコールアウト: 合計スタック数とアクティブなスタック数、スタックパッチ適用ステータス、アカウントのオンボーディングステータス (オンボーディング中のみ)、お客様固有の問題の概要
  - パフォーマンス: インシデント解決、アラート、パッチ適用、変更リクエスト (RFCs)、サービスリクエスト、コンソールと API の可用性に関する統計
  - 問題、課題、懸念、リスク: お客様固有の問題のステータス
  - 今後のアイテム: 顧客固有のオンボーディングプランまたはインシデント解決プラン
- マネージドリソース: スタックのグラフと円グラフ
- AMS メトリクス: モニタリングとイベントメトリクス、インシデントメトリクス、AMS SLA 準拠メトリクス、サービスリクエストメトリクス、変更管理メトリクス、ストレージメトリクス、継続性メトリクス、Trusted Advisor メトリクス、コスト概要 (いくつかの方法を提示)。機能リクエスト。連絡先情報。

#### Note

説明されている情報に加えて、CSDM は、AMS による運用活動のための下請業者の使用など、範囲または条件の重要な変更についても通知します。

AMS は、CSDM が月次レポートに含めるパッチ適用とバックアップに関するレポートを生成します。レポート生成システムの一部として、AMS はアクセスできないインフラストラクチャをアカウントに追加します。

- 未加工データが報告された S3 バケット
- データをクエリするためのクエリ定義を含む Athena インスタンス
- S3 バケットから raw データを読み取る Glue クローラ

## AWS Managed Servicesコスト最適化

AWS Managed Services は、毎月のビジネスレビュー (MBRs) 中に、毎月詳細なコスト使用率と削減額レポートを提供します。

AMS は、標準のプロセスとメカニズムのセットに従って、マネージドアカウントのコスト削減手段を特定し、AWS 支出を最適化するための変更の計画とロールアウトを支援します。

**Note**

AMS は、コスト最適化に役立つ動画を開発しています。最初のステップでは、コスト最適化のベストプラクティスの PDF と Excel スプレッドシートを提供します。これらのリソースにアクセスするには、[クイックガイドを開いてコスト最適化](#) ZIP ファイルにアクセスします。

## コスト最適化フレームワーク

AMS は、AWS コストを最適化するために 3 段階のアプローチに従います。

1. マネージド環境のコスト最適化方法を特定する
2. コスト最適化プランを提示する
3. 測定可能な方法でコスト最適化の達成を支援する

### マネージド環境のコスト最適化手段を特定する

AMS は Cost Explorer や Trusted Advisor などの AWS ネイティブツールを活用し、アーキテクチャの最適化、EC2 インスタンス、AWS アカウントに焦点を当てた最適化全体で 20 を超えるコスト削減パターンを活用して、カスタマイズされたコスト削減のレコメンデーションを構築します。

最適化に関する推奨事項には、次のようなものがあります。

アーキテクチャ最適化の推奨事項：

- 最適な S3 ストレージクラスの使用: Amazon S3 は、データアクセス、耐障害性、コストに基づいて、さまざまなワークロード要件を満たすストレージクラスを提供します。ワークロードのニーズに基づく S3 Intelligent-Tiering と S3 ストレージクラス分析により、S3 のコストを効率的に管理できます。
- キャッシュアーキテクチャの使用: 必要に応じてキャッシュインスタンスを活用すると、IOPS 要件を満たすと同時に、一部のデータベースインスタンスを置き換えるのに役立ちます。
- EBS アップグレードの削減: EBS ボリュームを gp2 から gp3 に移行すると、最大 20% のコスト削減を実現し、ボリュームサイズに関係なく、予測可能な 3,000 IOPS ベースラインパフォーマンスと 125 MiB/秒を活用できます。

- 伸縮性の使用: AWS が提供する自動スケーリング機能により、効果的なリソース使用率とコスト最適化の手段が可能になります。必要に応じてインスタンススケーリングポリシーを定期的に確認および更新することで、さらにコスト削減につながります。

## EC2 インスタンスに焦点を当てた推奨事項

- インスタンスの適正化: インスタンスのサイズ設定と使用状況に基づく最適な設定に焦点を当てた推奨事項。推奨事項には、Amazon EC2 Auto Scaling 機能の使用や、該当する場合は EC2 インスタンスを Amazon S3 AWS Lambda の静的ウェブコンテンツに置き換えることなどが含まれます。
- インスタンススケジューリング: AMS リソーススケジューラを使用して、スケジュールに基づいてインスタンスを自動的に開始および停止すると、特に営業時間外に使用されない非本番稼働用インスタンスのコストを抑えるのに役立ちます。
- Savings Plans にサブスクライブする: Savings Plans は AWS、使用量を節約する最も簡単な方法です。EC2 Instance Savings Plans は、Amazon EC2 インスタンスの使用量に対するオンデマンド料金と比較して、最大 72% の割引を提供します。Amazon SageMaker AI Savings Plans は、Amazon SageMaker AI サービスの使用量を最大 64% 削減します。AMS は、AWS リソースの使用状況に基づいて Savings プランに関する適切な推奨事項を提供します。
- リザーブドインスタンス (RI) の使用および消費ガイダンス: Amazon EC2 リザーブドインスタンス (RI) は、オンデマンド料金と比較して大幅な割引 (最大 75%) を提供し、特定の Availability ティアゾーンで使用する容量予約を提供します。
- スポットインスタンスの使用: フォールトトレラントワークロードはスポットインスタンスを活用し、最大 90% の料金を削減できます。
- アイドルインスタンスの終了: アイドル状態のインスタンス、または終了可能な使用率が低いインスタンスを特定してレポートします。

## アカウントに焦点を当てたレコメンデーション

- アカウントのクリーンアップ: アカウントレベルでは、AMS は未使用の EBS ボリューム、重複する CloudTrail 証跡、未使用のリソースを持つ空のアカウントなども識別し、クリーンアップの推奨事項を提供します。
- SLA 推奨事項: さらに、AMS は Plus アカウントと Premium アカウントを定期的に確認し、アカウントに適した SLA レベルを選択することをお勧めします。
- AMS オートメーションの最適化: AMS は、AMS サービスを提供するために使用される AMS オートメーションとインフラストラクチャを継続的に最適化します。

## 顧客に提示し、計画を支援する

AMS は、主要な顧客のステークホルダーと毎月のビジネスレビュー (MBRs) を実施し、特定されたコスト削減の方法、メカニズム、推奨事項と、潜在的なコスト削減を提示します。さらに、お客様と協力して必要な変更を計画します。

## レコメンデーションの実装を支援し、コストへの影響を測定する

AMS は、コストへの影響と最適化の変更の達成と測定を支援します。

推奨される変更のアプリケーションへの影響、リスク、成功基準を評価し、AMS コンソールを使用して適切な変更リクエスト (RFCs) を作成します。AMS はお客様と協力して、マネージドアカウントのコスト最適化に関連する変更を実装します。AMS は、コストへの影響を測定し、月次ビジネスレビュー (MBRs)。

## コスト最適化責任マトリックス

AMS コスト最適化の責任。

コスト最適化 RACI

| アクティビティ                      | お客様 | AMS |
|------------------------------|-----|-----|
| コスト削減レコメンデーションのコンパイルとレポートの準備 | I   | R   |
| コスト削減レポートの表示                 | C   | R   |
| コスト削減に関連                     | R   | C   |

|                         |     |     |
|-------------------------|-----|-----|
| アクティビティ                 | お客様 | AMS |
| する変更の計画                 |     |     |
| 変更の影響とリスクの評価            | R   | C   |
| 変更を実装するための RFCs の引き上げ   | R   | C   |
| RFCs の確認と変更の実装          | C   | R   |
| アプリケーションのテストと変更実装の検証    | R   | C   |
| 変更後のコストへの影響を測定し、顧客に提示する | I   | R   |

## AWS Managed Services のサービス時間

| 機能                         | AMS アドバンスト                  |
|----------------------------|-----------------------------|
|                            | プレミアム階層                     |
| サービスリクエスト                  | 24 時間 365 日                 |
| インシデント管理 (P2-P3)           | 24 時間 365 日                 |
| バックアップとリカバリ                | 24 時間 365 日                 |
| パッチ管理                      | 24 時間 365 日                 |
| モニタリングとアラート                | 24 時間 365 日                 |
| 変更の自動リクエスト (RFC)           | 24 時間 365 日                 |
| 自動変更リクエスト (RFC)            | 24 時間 365 日                 |
| クラウドサービスデリバリーマネージャー (CSDM) | 月曜日～金曜日: 08:00～17:00、現地営業時間 |

## AWS Managed Services でのヘルプの取得

AMS は、インシデント管理、サービスリクエスト管理、変更管理を 1 日 24 時間、週 7 日、1 年 365 日サポートします (アカウントに適用される AMS サービスレベルアグリーメントに準拠)。

マネージド環境に影響する AWS または AMS サービスのパフォーマンスの問題を報告するには、AMS コンソールを使用してインシデントレポートを送信します。詳細については、[「インシデントの報告」](#)を参照してください。AMS インシデント管理の一般的な情報については、[「インシデント対応」](#)を参照してください。

情報やアドバイスを求めたり、AMS から追加のサービスをリクエストしたりするには、AMS コンソールを使用してサービスリクエストを送信します。詳細については、[「サービスリクエストの作成」](#)を参照してください。AMS サービスリクエストの一般的な情報については、[「サービスリクエスト管理」](#)を参照してください。



# AWS Managed Services での計画されたイベント管理

AWS Managed Services (AMS) の計画イベント管理 (PEM) は AMS サービスです。PEM は、AMS サービスを使用して、顧客のイベントやプロジェクト中にエンゲージメント、調整、支援を行います。PEM は、PEM イベントまたはプロジェクトの合意された範囲とタイムラインに沿った一連の関連 RFCs の調整を支援します。

## AMS PEM 基準

計画されたイベントは、スコープバウンドプロジェクトと時間バウンドプロジェクトです。AMS は、お客様が提供した詳細 (計画と範囲、期待される成果、AMS オペレーションで期待される変更を含む) を使用して、PEM アクティビティ中にお客様を効果的にサポートします。その後、クラウドアーキテクト (CAs) は、PEM アクティビティの完全性、技術実装、AMS オペレーションのエンゲージメントを確認して評価します。CA のレビュー後、AMS オペレーションは計画を確認し、運用チームのエンゲージメントについてクラウドサービスデリバリーマネージャー (CSDM) と調整します。

## PEM のタイプ

使用可能な PEM タイプは次のとおりです。

- ゲームデー
  - 運用ゲームデー：プロセス、人材、システムの統合を検証することを目的とした、運用対応に対するシナリオベースのゲームアプローチ。
  - Security Gameday: システム、プロセス、人員の統合を評価するシナリオベースのゲームアプローチを採用するセキュリティインシデント対応戦略。
- BYOEPS: AMS 「Bring Your Own Endpoint Security」 (BYOEPS) 機能を使用して、デフォルトの Trend Micro Deep Security エージェントを任意のエンドポイントセキュリティソリューションまたはカスタム Trend Micro ライセンスに置き換えます。詳細については、「[AMS が独自の EPS を導入する](#)」を参照してください。
- ディザスタリカバリ：ディザスタリカバリイベントには、計画された DR アクティビティ中に AMS が支援します。詳細については、「[ディザスタリカバリ計画](#)」を参照してください。
- カスタマーセキュリティイベント：計画されたセキュリティイベント。例えば、ルートユーザーのアクティビティや侵入テストなどです。
- 移行サポート：計画されたオンボーディングと移行アクティビティのサポート。

このワークフローは、AMS サポートに関する計画されたイベントと移行アクティビティを調整するために、AMS とのコラボレーションを容易にします。RFCs on Demand (OOD) エンゲージメントを使用することをお勧めします。詳細については、「[オペレーションオンデマンド](#)」を参照してください。

## AMS PEM プロセス

PEM プロセスは、次のフェーズで構成されます。

- **PEM 開始**：CSDM と協力して、計画されたイベントの目標を定義し、AMS オペレーションに必要なものを決定します。AMS CAs PEM 計画の技術的側面を確認します。CAs、コンプライアンス、実行の最適化と自動化に関する AMS セキュリティとオペレーションと連携して、PEM 前実行タスクと成果物を定義します。次に、CSDM は PEM チケットを作成し、プロジェクト情報と技術詳細を AMS に提供します。AMS では、AMS Operations チームによる計画、技術レビュー、リソースの割り当てに 14 暦日のリードタイムが必要です。
- **PEM レビュー**：AMS オペレーションチームは PEM リクエストを確認し、CSDM と連携して PEM プランの情報が正しく、完了していることを確認します。
- **PEM の承諾**：AMS は提供された情報を確認し、PEM アクティビティ中のサポートレベルを CSDM に伝えます。PEM に完全な情報が含まれており、CSDM が作業範囲に同意する場合、PEM は承認されます。
- **準備と実行**：AMS は、PEM の開始前に必要なタスクが完了し、内部および顧客とのコミュニケーションが円滑に行われるようにします。AMS は、PEM プランが正しく実行され、ステータスと進行状況のレポートを提供することを確認します。

## PEM FAQs

PEM イベント中に AMS を RFC/サービスリクエスト (SR) とエンゲージするにはどうすればよいですか？

- CSDM によって共有される PEM ID を、RFC/SR の件名の形式 で使用します **PEM-ID**。
- また、サービスリクエスト (SR) を作成して、ユースケースについて話し合ったり、計画されたイベントについて質問したりすることもできます。SR を使用する場合、PEM が有効である必要はありません。

PEM 関連の RFC が送信されると、どのような検証が実行されますか？

- アカウント ID が PEM にリストされていることを確認します。
- 指定された開始日と終了日の間に PEM ステータスが承認され、アクティブになっていることを確認します。

PEM リクエストの SLAs または SLOs はありますか？

- PEMsは SLAs または SLOs に関連付けられていません。
- PEM 関連の作業項目 (RFC/サービスリクエスト) SLOs SLAs と SLO は、AMS SLOs によって定義されます。

詳細については、[「AMS サービスレベル目標 \(SLOs\)」](#)を参照してください。

サービスリクエスト (SR) を使用して PEM を作成できますか？

- いいえ。PEM の作成は Cloud Service Delivery Manager (CSDM) によって管理する必要があります。

# ネットワークアーキテクチャ

AWS Managed Services (AMS) には 2 つのネットワークアーキテクチャがあります。

- マルチアカウントランディングゾーン (MALZ): は、個別のメンバーアカウントにデプロイされたワークロードの共有アカウントから、アクセス、エンドポイントセキュリティ、ネットワークなどの一般的なサービスを提供します。
- シングルアカウントランディングゾーン (SALZ): は、アクセス、エンドポイントセキュリティ、ネットワークなどの一般的なサービスがワークロードと同じアカウントにデプロイされる自己完結型アカウントを提供します。AWS のコストが高くなるため、高レベルの分離を必要とするワークロードにお勧めします。

## MALZ ネットワークアーキテクチャ

### マルチアカウントランディングゾーンのネットワークアーキテクチャについて

AWS Managed Services (AMS) マルチアカウントランディングゾーン (MALZ) へのオンボーディングプロセスを開始する前に、AMS がユーザーに代わって作成するベースラインアーキテクチャまたはランディングゾーン、そのコンポーネント、および関数を理解することが重要です。

AMS マルチアカウントランディングゾーンは、認証、セキュリティ、ネットワーク、ログ記録を容易にするために、インフラストラクチャで事前設定されたマルチアカウントアーキテクチャです。

#### Note

コストの見積もりについては、[「AMS マルチアカウントランディングゾーン環境の基本コンポーネント」](#)を参照してください。

#### トピック

- [サービスリージョン](#)
- [組織単位](#)
- [サービスコントロールポリシーと AWS Organization](#)

次の図は、アカウント構造の概要と、インフラストラクチャを各アカウントに分離する方法を示しています。

## サービスリージョン

AMS マルチアカウントランディングゾーン内のすべてのリソースは、Active Directory と Transit Gateway の現在のクロスリージョン制限により、選択した 1 つの AWS リージョン内にデプロイされます。

## 組織単位

一般的な AMS マルチアカウントランディングゾーンは、4 つの最上位組織単位 (OUs で構成されます。

- コア組織単位 (OU) (アカウントをグループ化して 1 つの単位として管理するために使用します)
- アプリケーション OU
- カスタマー管理の OU
- 高速化 OU

AMS マネージドマルチアカウントランディングゾーンでは、AWS アカウントをグループ化および整理するためのカスタム OUs を作成し、カスタム SCPs <https://docs.aws.amazon.com/managedservices/latest/ctref/deployment-managed-management-account-create-custom-scp-review-required.html#OUs>」をそれぞれ参照してください。AMS は、新しい OUs とアカウントをリクエストできる 4 つの既存の OUs を提供します。高速化、アプリケーション > マネージド、アプリケーション > 開発、カスタマーマネージドです。

- OU の高速化:

これは、AMS マルチアカウントランディングゾーン (MALZ) の最上位 OU です。この OU の下にあるアカウントは、RFC を使用して AMS によってプロビジョニングされます (デプロイ | マネージドランディングゾーン | 管理アカウント | Create Accelerate アカウント、変更タイプ ID: ct-2p93tyd5angmi)。アプリケーションアカウントを高速化することで、モニタリングとアラート、インシデント管理、セキュリティ管理、バックアップ管理などの運用サービスを加速できます。詳細については、「[AMS Accelerate アカウント](#)」を参照してください。

- アプリケーション > マネージド OU:

アプリケーション OU のこのサブ組織単位では、アカウントはすべての運用タスクを含む AMS によって完全に管理されます。運用タスクには、サービスリクエスト管理、インシデント管理、セキュリティ管理、継続管理、パッチ管理、コスト最適化、モニタリング、イベント管理が含まれます。これらのタスクは、インフラストラクチャの管理のために実行されます。AWS 組織でネストされた OUs の最大数に達するまで、必要に応じて複数の子 OUs を作成できます。詳細については、[AWS Organizations](#)」を参照してください。

- アプリケーション > 開発 OU:

AMS マネージドランディングゾーンのアプリケーション OU のこのサブ OU では、アカウントは、AMS 変更管理プロセス外で AWS リソースをプロビジョニングおよび更新するための昇格されたアクセス許可を提供する[デベロッパーモード](#)アカウントです。この OU は、必要に応じて新しい子 OU の作成もサポートしています。

- カスタマーマネージド OU:

これは、AMS マルチアカウントランディングゾーンの最上位 OU です。この OU に基づくアカウントは、RFC を使用して AMS によってプロビジョニングされます。これらのアカウントでは、ワークロードと AWS リソースの運用はお客様の責任となります。この OU は、必要に応じて新しい子 OU の作成もサポートしています。

ベストプラクティスとして、これらの OUs およびカスタムリクエストされたサブ OUs の下にあるアカウントは、その機能とポリシーに基づいてグループ化することをお勧めします。

## サービスコントロールポリシーと AWS Organization

AWS は、AWS Organization のアクセス許可管理のためのサービスコントロールポリシー (SCPs) を提供します。SCPs は、ユーザーがどの OUs で実行できるアクションに追加のガードレールを定義するために使用されます。デフォルトでは、AMS はさまざまなデフォルト OU レベルで保護を提供する一連の SCPs を管理アカウントにデプロイします。SCP の制限については、CSDM にお問い合わせください。

カスタム SCPs を作成して特定の OUs にアタッチすることもできます。これらは、変更タイプ `ct-33ste5yc7hprs` を使用して管理アカウントからリクエストできます。AMS は、リクエスト SCPs を確認してから、ターゲット OUs。例については、「[管理アカウント | カスタム OUs](#)」を参照してください。 <https://docs.aws.amazon.com/managedservices/latest/ctref/deployment-managed-management-account-create-custom-scp-review-required.html>

## 単一の MALZ または複数の MALZs の選択

次の表は、1 つのマルチアカウントランディングゾーン (MALZ) と複数のマルチアカウントランディングゾーン (例: 2 つのマルチアカウントランディングゾーン - Prod と非 Prod) のどちらかを決定する際の考慮事項の概要を示しています。一般的に、選択は個々のニーズ、法的要件、運用慣行によって異なります。

### 単一マルチアカウントランディングゾーンと複数マルチアカウントランディングゾーン

| エンティティ                              | 単一 AMS ランディングゾーン                                                     | 複数の (2 つ以上の) ランディングゾーン                                                                    |
|-------------------------------------|----------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| 基本費用                                | 低く、1 か月あたり約 3,000 USD で最適化されています。                                    | より高い場合は、環境ごとに約 3,000 USD の追加コストが発生します。                                                    |
| 請求                                  | 単一の請求/管理アカウントによる単一の請求。                                               | マルチアカウントランディングゾーンごとに個別の請求書。現在、AWS Org は 1 回の請求でマルチ管理アカウントをサポートしていません。                     |
| 既存のリザーブドインスタンス (RIs) の移植性           | 低。AWS RIs は現在、複数の請求アカウント間で変換できません。マルチアカウントランディングゾーンの既存の RIs を再利用します。 | 下。RIs を再利用し、すべてのマルチアカウントランディングゾーンに分散します。                                                  |
| 製品階層化の割引                            | 高 <a href="#">「ボリューム割引」を参照してください。</a>                                | 低。 <a href="#">「ボリューム割引」を参照してください。</a>                                                    |
| 初期セットアップのオーバーヘッド (プロジェクト/移行タイムライン上) | 低。Active Directory、ネットワーク、およびシングルサインオン (SSO) 統合は 1 回のみです。            | 高 ランディングゾーンごとに Active Directory、ネットワーク統合、および SSO 統合を実行します。これにより、移行プロジェクトに遅延が発生する可能性があります。 |
| 一般的なサービスの設定可能性                      | 労力が少ない。DNS、バックアップ、モニタリング、ログ記録などの共通/共有サービスを設定します。                     | 高い労力。一般的なインフラストラクチャやサービスが置かれている場所に対処するには、追加の計画が必要です。各ランディングゾーンの複数のト                       |



| エンティティ        | 単一 AMS ランディングゾーン                                                                                                                                                                                                                                                                                                     | 複数の (2 つ以上の) ランディングゾーン                                                                                              |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
|               |                                                                                                                                                                                                                                                                                                                      | ランジットゲートウェイ (TGWs) を通過するトラフィックは、追加料金が発生する可能性があります。                                                                  |
| スケーラビリティ      | Medium。AMS には、マルチアカウントランディングゾーンあたり 150 個のアカウントという現在の実用的な制限があります。同じアカウントでアプリケーションを実行している複数のチームまたはベンダーは、異なるチームが所有するスタックにアクセスできる可能性があります。この制限は、Service Now レイヤーでアプリケーション固有のスタックへのアクセスを制御することで (AMS ServiceNow Connector アプリケーションを統合してタグを使用することで) 軽減できます。AMS テクニカルデリバリーマネージャー (TDMs) またはクラウドアーキテクト (CAs) に、この実装方法を依頼します。 | 高 アカウントまたはアプリケーションレベルの分離を達成しながら、複数のマルチアカウントランディングゾーンを活用してアカウントを分散する機能。多数のアカウントを管理すると、運用またはコストのオーバーヘッドにつながる可能性があります。 |
| 運用上のリスク       | (依存) 低。運用上の統合と準備は 1 回のみ。プロセスドリフトの可能性が低くなります。                                                                                                                                                                                                                                                                         | (依存) 低。複数の統合および運用アクティビティ。期間中の複数のランディングゾーンのドリフトは、運用上のリスクにつながる可能性があります。                                               |
| マルチ AWS リージョン | 単一の AWS リージョン。AMS マルチアカウントランディングゾーンは、単一の AWS リージョンに制限されています。複数の AWS リージョンにまたがるには、複数のマルチアカウントランディングゾーンを使用します。                                                                                                                                                                                                         | マルチ AWS リージョン。複数のマルチアカウントランディングゾーンを使用すると、各 MALZ を 1 つのリージョンにデプロイし、トランジットゲートウェイ (TGW) ピアリングを使用して相互接続できます。            |



| エンティティ           | 単一 AMS ランディングゾーン                                                                                                                                                               | 複数の (2 つ以上の) ランディングゾーン                                                                                                           |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| アカウントの移行または移植性   | はい。ある OU から同じ AWS Organization 内の別の OU にアカウントを移動できます。                                                                                                                          | いいえ。AMS はランディングゾーン間、つまり AWS Organizations 間でのアカウントの移行をサポートしていません。ワークロードは、トランジットゲートウェイ (TGW) または VPC ピアリングを使用してランディングゾーン間で到達できます。 |
| 変更管理             | Medium。TGW、Active Directory (AD)、アウトバウンド (Egress) などの一般的なコンポーネントに破壊的な変更を加えると、マルチアカウントランディングゾーン内のすべてのワークロードに影響を与える可能性があります。ただし、AMS マネージドコンポーネントへの変更は内部的にテストされ、ローリング更新でプッシュされます。 | 低。TGW、AD、アウトバウンド (エグレス) などの一般的なコンポーネントに破壊的な変更を加えると、その特定のマルチアカウントランディングゾーンのワークロードにのみ影響します。                                        |
| データおよびアクセスコントロール | (依存) Prod ワークロードと Non-Prod ワークロードの異なるオンプレミス ADs とネットワークに接続する場合は、コントロールが低くなります。SAML フェデレーション、TGW ドメイン、セキュリティグループ (SGs も、必要なコントロールを実装するのに役立ちます。                                  | (依存) Prod ワークロードと Non-Prod ワークロードの異なるオンプレミス ADs とネットワークに接続する場合は、高い制御が可能です。厳格なコンプライアンス要件には、個別のランディングゾーンを使用します。                    |

| エンティティ          | 単一 AMS ランディングゾーン                                                                                   | 複数の (2 つ以上の) ランディングゾーン                                                                                                           |
|-----------------|----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| コンプライアンスとセキュリティ | ( 依存) マテリアルワークロードと非マテリアルワークロードを完全に分離するために厳格なコンプライアンスが必要な場合は、低。AMS 標準の予防的コントロールと検出的コントロールが導入されています。 | ( 依存) マルチアカウントランディングゾーンが複数ある場合、マテリアルワークロードと非マテリアルワークロードを完全に分離することで、厳格なコンプライアンス要件を満たすことができます。AMS 標準の予防的コントロールと検出的コントロールが導入されています。 |

推奨事項: 厳密なコンプライアンスやマルチリージョンの必要性がなければ、単一の AMS マルチアカウントランディングゾーンから始めると、コスト、セキュリティ、運用上の優秀性、移行の複雑さのバランスが取れます。アカウントまたはビジネスの制約が発生した場合は、いつでも追加のランディングゾーンを設定できます。

## 単一マルチアカウントランディングゾーンと複数マルチアカウントランディングゾーンFAQs

1 つのマルチアカウントランディングゾーンまたは複数のマルチアカウントランディングゾーンを設定する場合によくある質問:

Q1: アカウントの制限やビジネス上の制約が発生した場合、単一のマルチアカウントランディングゾーンから始めて、複数のマルチアカウントランディングゾーンに移動できますか？

A: はい。いつでも別のマルチアカウントランディングゾーンを設定できます。

- 新しい請求支払者アカウントを設定する必要があります (現在、AWS は単一の AWS 組織内の複数支払者アカウントをサポートしていません)。
- マルチアカウントランディングゾーンのベースビルドには、マルチアカウントランディングゾーンのアンケートに入力されてから最大 2 週間かかります。
- すべてのマルチアカウントランディングゾーンでは、1 か月あたり最大 3,000 USD のランニングコストが追加されます。
- 新しい MALZ の を確立するには、N/W、AD、DNS、および SSO の統合が必要です。
- リザーブドインスタンス (RIs)、コスト削減プランは、新しいマルチアカウントランディングゾーン用に設定する必要があります (RIsは移管できません)。

- AMS マルチアカウントランディングゾーンは、AWS 組織間など、マルチアカウントランディングゾーンアカウント間のアカウントの移行をサポートしていません。ただし、標準の移行方法を使用して、あるアカウントから別のアカウントにアプリケーションを移動することは可能です。

Q2: MALZ の基盤/共有インフラストラクチャの更新/変更に対する AMS アプローチとは何ですか？プロセスにラップされる保証の詳細を入力します。顧客は、MALZ の更新/変更が顧客に影響を与えないという安心感をどのように得られますか？中断を防ぐためにお客様が取るべき対策はありますか？

A: AMS は、お客様の環境の変更を定義、レビュー、スケジュール、実行できる内部ツールを使用して、厳格な変更方法に従います。

更新をリリースするプロセスでは、お客様の環境にリリースする前に、コードレビュー、統合テスト、ガンマおよびベータ環境でのデプロイ、ベータおよびガンマ環境での追加ベーキング時間とテストが適用されます。すべてのリリースにはロールバック手順が含まれており、リリースチームと変更を作成およびリクエストしたチームによって詳細にモニタリングされます。リリースの範囲は、AMS が所有およびプロビジョニングするスタックに限定されます。平均して、1 週間に少なくとも 1 つのリリースを実行します。

さらに:

- AMS SLA が適用されます。AMS サービスの説明に従って、共有インフラストラクチャメンテナンスアクティビティ後に発生したインシデントは、解決またはクレジットの資格のある SLA に準拠します。
- 一般的なインフラストラクチャの中断を防ぐために、お客様は特別な予防措置を講じる必要はありません。お客様は AWS Org または Core OU アカウントで読み取り専用アクセス許可を持っているため、MALZ Core env に破壊的な変更を加えることはできません。Core インフラストラクチャに対するお客様のすべてのリクエストには、AMS のレビューと承認が必要です。
- お客様は、アプリケーション OU レベルで変更を伝達する前に SCPs/ロールなどの特定の組織レベルの変更を個々の非製品アカウントレベルでテストできます。AMS ロードマップでは、複数の APP OUs (2020 年第 2 四半期) を許可しています。これにより、ORG レベルの変更に伴うリスクがさらに軽減されます。MALZ チームは、顧客の所有権と個別のコントロールを明確に分離するために、「ビルドモード」アカウント用に個別の OU を既にリリースしています。
- これらの大部分は、AMS が効果的かつ効率的な方法でワークロードを運用できるようにする変更であり、必ずしもお客様のワークロードに影響を与えるわけではありません。AMS が共有インフラストラクチャの変更が顧客のワークロードに影響を与える可能性があると考える場合、AMS は顧客の変更ウィンドウと連携します。

次の場合は、高レベルのレコメンデーションとして、複数のマルチアカウントランディングゾーンから始めます。

- 特定のコンプライアンスを達成するのに役立つ場合。
- マルチリージョンを使用する必要がある場合。
- Prod/Material ワークロードと Non-Prod/Non-Material ワークロードのオンプレミス ADs とネットワークが異なる場合は、ワークロードを b/w 明確に分離します。

## マルチアカウントランディングゾーンアカウント

### トピック

- [管理アカウント](#)
- [ネットワークアカウント](#)
- [共有サービスアカウント](#)
- [ログアーカイブアカウント](#)
- [セキュリティアカウント](#)
- [アプリケーションアカウントタイプ](#)
- [AMS Tools アカウント \(ワークロードの移行\)](#)

### 管理アカウント

管理アカウントは、AMS でのオンボーディングを開始する最初の AWS アカウントです。管理アカウント (すべてのメンバーアカウントの料金を支払う支払者アカウントとも呼ばれます) として AWS Organizations を利用します。これにより、アカウントはメンバーアカウントを作成および財務管理できるようになります。これには、AWS ランディングゾーン (ALZ) フレームワーク、アカウント設定スタックセット、AWS Organization サービスコントロールポリシー (SCPsなどが含まれます。

管理アカウントの使用の詳細については、[「管理アカウントのベストプラクティス」](#)を参照してください。

次の図は、管理アカウントに含まれるリソースの概要を示しています。

### 管理アカウントのリソース

上記の標準サービスを除き、オンボーディング中に管理アカウントに追加の AWS リソースは作成されません。AMS へのオンボーディングには、次の入力が必要です。

- 管理アカウント ID: ユーザーが最初に作成した AWS アカウント ID。
- コアアカウントの E メール: ネットワーク、共有サービス、ログ記録、セキュリティの各コアアカウントに関連付ける E メールを指定します。
- サービスリージョン: AMS ランディングゾーンのすべてのリソースがデプロイされる AWS リージョンを指定します。

## ネットワークアカウント

ネットワークアカウントは、AMS マルチアカウントランディングゾーンアカウント、オンプレミスネットワーク、インターネットへの送信トラフィック間のネットワークルーティングの中央ハブとして機能します。さらに、このアカウントには、AMS エンジニアが AMS 環境のホストにアクセスするためのエントリポイントであるパブリック DMZ 踏み台が含まれています。詳細については、以下のネットワークアカウントの大まかな図を参照してください。

### ネットワークアカウントアーキテクチャ

次の図は、AMS マルチアカウントランディングゾーン環境を示し、アカウント間のネットワークトラフィックフローを示し、可用性の高いセットアップの例です。

AMS は、標準テンプレートとオンボーディング中に提供された選択したオプションに基づいて、ネットワーキングのあらゆる側面を設定します。標準の AWS ネットワーク設計が AWS アカウントに適用され、VPC が自動的に作成され、VPN または Direct Connect によって AMS に接続されます。Direct Connect の詳細については、「[AWS Direct Connect](#)」を参照してください。標準 VPCs には、DMZ、共有サービス、アプリケーションサブネットが含まれます。オンボーディングプロセス中に、ニーズ (顧客部門、パートナーなど) に合わせて追加の VPCs がリクエストおよび作成される場合があります。オンボーディング後、ネットワーク図が提供されます。これは、ネットワークの設定方法を説明する環境ドキュメントです。

#### Note

すべてのアクティブなサービスのデフォルトのサービス制限と制約については、[AWS Service Limits](#) ドキュメントを参照してください。

当社のネットワーク設計は、Amazon の「[最小特権の原則](#)」を中心に構築されています。これを実現するために、信頼できるネットワークからのトラフィックを除くすべてのトラフィックを DMZ 経由でルーティングします。唯一の信頼されたネットワークは、VPN や AWS Direct Connect (DX) を使用してオンプレミス環境と VPC 間で設定されるネットワークです。アクセスは踏み台インスタンスを使用して付与されるため、本番稼働用リソースに直接アクセスできなくなります。すべてのアプリケーションとリソースは、パブリックロードバランサーを介して到達可能なプライベートサブネット内に存在します。パブリックエグレストラフィックは、エグレス VPC (ネットワークアカウント) の NAT ゲートウェイを介してインターネットゲートウェイに、次にインターネットに流れます。または、トラフィックが VPN または Direct Connect 経由でオンプレミス環境に流れることもあります。

## AMS マルチアカウントランディングゾーン環境へのプライベートネットワーク接続

AWS は、仮想プライベートネットワーク (VPN) 接続、または AWS Direct Connect との専用ラインを介したプライベート接続を提供します。マルチアカウント環境のプライベート接続は、次に説明する方法のいずれかを使用して設定されます。

- Transit Gateway を使用した一元化された Edge 接続
- Direct Connect (DX) や VPN をアカウント仮想プライベートクラウド (VPCs) に接続する

### Transit Gateway を使用した一元化されたエッジ接続

AWS Transit Gateway は、VPCs とオンプレミスネットワークを単一のゲートウェイに接続できるサービスです。トランジットゲートウェイ (TGW) を使用して、既存のエッジ接続を統合し、単一の進入/退出ポイントにルーティングできます。トランジットゲートウェイは、AMS マルチアカウント環境のネットワークアカウントに作成されます。Transit Gateway の詳細については、[AWS Transit Gateway](#)」を参照してください。

AWS Direct Connect (DX) ゲートウェイは、トランジット仮想インターフェイスを介して、トランジットゲートウェイにアタッチされている VPCs VPNs に DX 接続を接続するために使用されます。Direct Connect ゲートウェイを Transit Gateway に関連付けます。次に、Direct Connect ゲートウェイへの AWS Direct Connect 接続のトランジット仮想インターフェイスを作成します。DX 仮想インターフェイスの詳細については、「[AWS Direct Connect 仮想インターフェイス](#)」を参照してください。

この設定には次のような利点があります。以下を実行できます。

- 同じ AWS リージョンにある複数の VPCs VPNs に対して 1 つの接続を管理します。
- プレフィックスをオンプレミスから AWS、AWS からオンプレミスにアドバタイズします。

**Note**

AWS のサービスで DX を使用する方法については、「Resiliency Toolkit」セクション「[Classic](#)」を参照してください。詳細については、「[Transit Gateway の関連付け](#)」を参照してください。

接続の耐障害性を高めるには、異なる AWS Direct Connect ロケーションから Direct Connect ゲートウェイに少なくとも 2 つのトランジット仮想インターフェイスをアタッチすることをお勧めします。詳細については、[AWS Direct Connect の障害耐性に関する推奨事項](#)を参照してください。

DX または VPN をアカウント VPCs に接続する

このオプションを使用すると、AMS マルチアカウントランディングゾーン環境 VPCs は Direct Connect または VPN に直接接続されます。トラフィックは、トランジットゲートウェイを経由することなく VPCs から Direct Connect または VPN に直接流れます。

ネットワークアカウントのリソース

ネットワークアカウント図に示すように、以下のコンポーネントがアカウントに作成され、入力が必要です。

ネットワークアカウントには、Egress VPCs と Perimeter VPC と呼ばれる DMZ VPC の 2 つの VPC が含まれています。

AWS Network Manager

AWS Network Manager は、トランジットゲートウェイ (TGW) ネットワークを AMS に追加コストなしで視覚化できるサービスです。AWS リソースとオンプレミスネットワークの両方での一元化されたネットワークモニタリング、トポロジ図と地理的マップでのプライベートネットワークの単一のグローバルビュー、およびバイトイン/アウト、パケットイン/アウト、ドロップされたパケット、トポロジ、ルーティング、およびアップ/ダウン接続ステータスの変更に関するアラートなどの使用率メトリクスを提供します。詳細については、「[AWS Network Manager](#)」を参照してください。

このリソースにアクセスするには、次のいずれかのロールを使用します。

- AWSManagedServicesCaseRole
- AWSManagedServicesReadOnlyRole



- AWSManagedServicesChangeManagementRole

## エグレス VPC

Egress VPC は主にインターネットへの Egress トラフィックに使用され、最大 3 つのアベイラビリティゾーン (AZs) のパブリック/プライベートサブネットで構成されます。ネットワークアドレス変換 (NAT) ゲートウェイはパブリックサブネットにプロビジョニングされ、トランジットゲートウェイ (TGW) VPC アタッチメントはプライベートサブネットに作成されます。すべてのネットワークからの送信またはアウトバウンドのインターネットトラフィックは TGW を介してプライベートサブネットを経由して入り、VPC ルートテーブルを介して NAT にルーティングされます。

パブリックサブネットにパブリック向けアプリケーションを含む VPCs の場合、インターネットから発信されるトラフィックはその VPC 内に含まれます。リターントラフィックは TGW または Egress VPC にルーティングされませんが、VPC のインターネットゲートウェイ (IGW) 経由でルーティングされます。

### Note

ネットワーク VPC CIDR 範囲: VPC を作成するときは、VPC の IPv4 アドレスの範囲を Classless Inter-Domain Routing (CIDR) ブロックの形式で指定する必要があります。たとえば、10.0.16.0/24 です。これは VPC のプライマリ CIDR ブロックです。  
AMS マルチアカウントランディングゾーンチームは、今後他のリソース/アプライアンスがデプロイされる場合に備えて、バッファを提供するために 24 の範囲 (より多くの IP アドレスを使用) を推奨します。

## 境界 (DMZ) VPC

Perimeter、または DMZ、VPC には、AMS オペレーションエンジニアが AMS ネットワークにアクセスするために必要なリソースが含まれています。これには、2~3 AZs のパブリックサブネットが含まれており、AMS Operations エンジニアがログインまたはトンネルスルーするための Auto Scaling グループ (ASG) の SSH Bastions ホストがあります。DMZ 踏み台にアタッチされたセキュリティグループには、Amazon Corp Networks からのポート 22 インバウンドルールが含まれています。

DMZ VPC CIDR 範囲: VPC を作成するときは、10.0.16.0/24 など、Classless Inter-Domain Routing (CIDR) ブロックの形式で VPC の IPv4 アドレスの範囲を指定する必要があります。これは VPC のプライマリ CIDR ブロックです。



**Note**

AMS チームは、ファイアウォールなどの他のリソースが将来デプロイされる場合に備えて、バッファを提供するために 24 の範囲 (より多くの IP アドレスを使用) を推奨します。

## AWS Transit Gateway

AWS Transit Gateway (TGW) は、Amazon Virtual Private Cloud (VPCs) とオンプレミスネットワークを単一のゲートウェイに接続できるサービスです。トランジットゲートウェイは、AMS アカウントネットワークと外部ネットワーク間のルーティングを処理するネットワークバックボーンです。トランジットゲートウェイの詳細については、[AWS Transit Gateway](#)」を参照してください。

このリソースを作成するには、次の入力を指定します。

- トランジットゲートウェイ ASN 番号\*: トランジットゲートウェイのプライベート自律システム番号 (ASN) を指定します。これは、ボーダーゲートウェイプロトコル (BGP) セッションの AWS 側の ASN になります。16 ビット ASN の場合、その範囲は 64512 ~ 65534 です。

## 共有サービスアカウント

共有サービスアカウントは、ほとんどの AMS データプレーンサービスの中央ハブとして機能します。アカウントには、アクセス管理 (AD)、エンドポイントセキュリティ管理 (Trend Micro)、カスタマー踏み台 (SSH/RDP) に必要なインフラストラクチャとリソースが含まれています。共有サービスアカウントに含まれるリソースの概要を次の図に示します。

共有サービス VPC は、3 つのアベイラビリティーゾーン (AZs) の AD サブネット、EPS サブネット、カスタマー踏み台サブネットで構成されます。共有サービス VPC で作成されたリソースを以下に示します。入力が必要です。

- 共有サービス VPC CIDR 範囲: VPC を作成するときは、10.0. 1.0/24 など、Classless Inter-Domain Routing (CIDR) ブロックの形式で VPC の IPv4 アドレスの範囲を指定する必要があります。これは VPC のプライマリ CIDR ブロックです。

**Note**

AMS チームは /23 の範囲を推奨します。

- **Active Directory の詳細:** Microsoft Active Directory (AD) は、すべての AMS マルチアカウントランディングゾーンアカウントで、ユーザー/リソース管理、認証/認可、DNS に使用されます。AMS AD には、信頼ベースの認証のために Active Directory への一方向の信頼も設定されています。AD を作成するには、次の入力が必要です。
- **ドメイン完全修飾ドメイン名 (FQDN):** AWS Managed Microsoft AD ディレクトリの完全修飾ドメイン名。ドメインは、ネットワーク内の既存のドメインの既存のドメインまたは子ドメインにすることはできません。
- **ドメイン NetBIOS 名:** NetBIOS 名を指定しない場合、AMS はデフォルトでディレクトリ DNS の最初の部分に名前を付けます。たとえば、ディレクトリ DNS corp.example.com の corp です。

- **Trend Micro – エンドポイント保護セキュリティ (EPS):** Trend Micro エンドポイント保護 (EPS) は、オペレーティングシステムのセキュリティのための AMS 内の主要なコンポーネントです。システムは、Deep Security Manager (DSM)、EC2 インスタンス、リレー EC2 インスタンス、およびすべてのデータプレーンとカスタマー EC2 インスタンス内に存在するエージェントで構成されます。

共有サービスアカウントEPSTMarketplaceSubscriptionRoleで を引き受け、Trend Micro Deep Security (BYOL) AMI または Trend Micro Deep Security (Marketplace) のいずれかにサブスクリプションする必要があります。

EPS を作成するには、次のデフォルト入力が必要です (デフォルトから変更する場合 )。

- **リレーインスタンスタイプ:** デフォルト値 - m5.large
  - **DSM インスタンスタイプ:** デフォルト値 - m5.xlarge
  - **DB インスタンスサイズ:** デフォルト値 - 200 GB
  - **RDS インスタンスタイプ:** デフォルト値 - db.m5.large
- 
- **カスタマー踏み台:** AMS 環境内の他のホストにアクセスするために、共有サービスアカウントで SSH または RDP 踏み台 (またはその両方) が提供されます。ユーザー (SSH/RDP) として AMS ネットワークにアクセスするには、「customer」踏み台をエントリポイントとして使用する必要があります。ネットワークパスはオンプレミスネットワークから発信され、DX/VPN を介してトランジットゲートウェイ (TGW) にルーティングされ、共有サービス VPC にルーティングされます。踏み台にアクセスできるようになったら、アクセスリクエストが付与されていれば、AMS 環境内の他のホストにジャンプできます。
  - **SSH 踏み台:** には次の入力が必要です。

- SSH 踏み台に必要なインスタンス容量: デフォルト値 - 2。
- SSH 踏み台最大インスタンス: デフォルト値 - 4。
- SSH 踏み台最小インスタンス: デフォルト値 - 2。
- SSH 踏み台インスタンスタイプ: デフォルト値 - m5.large (t3.medium など、コストを節約するために変更できます)。
- SSH 踏み台入力 CIDRs: ネットワーク内のユーザーが SSH 踏み台にアクセスする IP アドレス範囲。
- Windows RDP 踏み台には、次の入力が必要です。
  - RDP 踏み台インスタンスタイプ: デフォルト値 - t3.medium。
  - RDP 踏み台で必要な最小セッション数: デフォルト値 - 2。
  - RDP 最大セッション数: デフォルト値 - 10。
  - RDP 踏み台設定タイプ: 次のいずれかの設定を選択できます。
    - SecureStandard = ユーザーは 1 つの踏み台を受け取り、1 人のユーザーだけが踏み台に接続できます。
    - SecureHA = ユーザーは 2 つの異なる AZ で 2 つの踏み台を受け取り、1 人のユーザーだけが踏み台に接続できます。
    - SharedStandard = ユーザーは に接続するための踏み台を 1 つ受け取り、2 人のユーザーは一度に同じ踏み台に接続できます。
    - SharedHA = ユーザーは 2 つの異なる AZ で 2 つの踏み台を受け取り、2 人のユーザーは一度に同じ踏み台に接続できます。
- お客様の RDP Ingress CIDRs: ネットワーク内のユーザーが RDP 踏み台にアクセスする IP アドレス範囲。

## 共有サービスの更新: マルチアカウントランディングゾーン

AMS は、データプレーンリリースを毎月、事前の通知なしにマネージドアカウントに適用します。

AMS はコア OU を使用して、アクセス、ネットワーク、EPS、ログストレージ、アラート集約などの共有サービスをマルチアカウントランディングゾーンで提供します。AMS は、これらの共有サービスの脆弱性、パッチ適用、デプロイに対応する責任があります。AMS は、これらの共有サービスの提供に使用されるリソースを定期的に更新し、ユーザーが最新の機能やセキュリティ更新プログラムにアクセスできるようにします。更新は通常、毎月行われます。これらの更新に含まれるリソースは次のとおりです。

- コア OU の一部であるアカウント。

管理アカウント、共有サービスアカウント、ネットワークアカウント、セキュリティアカウント、ログアーカイブアカウントには、通常毎月更新される RDP および SSH 踏み台、プロキシ、管理ホスト、エンドポイントセキュリティ (EPS) 用のリソースがあります。AMS は、共有サービスインフラストラクチャの一部としてイミュータブルな EC2 デプロイを使用します。

- 最新の更新を組み込んだ新しい AMS AMIs。

#### Note

AMS 演算子は、データプレーンの変更を実行するときに内部アラーム抑制変更タイプ (CT) を使用し、その CT の RFC が RFC リストに表示されます。これは、データプレーンのリリースがデプロイされると、さまざまなインフラストラクチャがシャットダウン、再起動、オフラインになるか、データプレーンのデプロイ中に無関係なアラームをトリガーする CPU スパイクやその他のデプロイの影響が発生する可能性があるためです。デプロイが完了すると、すべてのインフラストラクチャが正常に実行されていることが確認され、アラームが再び有効になります。

## ログアーカイブアカウント

Log Archive アカウントは、AMS マルチアカウントランディングゾーン環境全体でログをアーカイブするための中央ハブとして機能します。アカウントには、各 AMS マルチアカウントランディングゾーン環境アカウントからの AWS CloudTrail ログファイルと AWS Config ログファイルのコピーを含む S3 バケットがあります。このアカウントは、AWS Firehose や Splunk などの集中ロギングソリューションに使用できます。このアカウントへの AMS アクセスは少数のユーザーに制限され、アカウントアクティビティに関連するコンプライアンスとフォレンジック調査のために監査人とセキュリティチームに限定されます。

## セキュリティアカウント

セキュリティアカウントは、セキュリティ関連のオペレーションを格納するための中心的なハブであり、AMS コントロールプレーンサービスに通知とアラートをファネルするための主要なポイントです。さらに、セキュリティアカウントには Amazon Guard Duty 管理アカウントと AWS Config アグリゲータが格納されます。

## アプリケーションアカウントタイプ

アプリケーションアカウントは、ワークロードのホストに使用する AMS マネージドランディングゾーンアーキテクチャ内の AWS アカウントです。AMS には 3 種類のアプリケーションアカウントがあります。

- [AMS マネージドアプリケーションアカウント](#)
- [AMS Accelerate アカウント](#)
- [カスターマネージドアプリケーションアカウント](#)

アプリケーションアカウントは、アプリケーションアカウントタイプに応じて AWS Organizations の異なる OUs にグループ化されます。

- ルート OU:
  1. アプリケーション OU
    - マネージド OU: AMS マネージドアカウント
    - 開発 OU: デベロッパーモードが有効になっている AMS マネージドアカウント
  2. OU の高速化: AMS Accelerate Application アカウント
  3. カスターマネージド OU: カスターマネージドアプリケーションアカウント

アプリケーションアカウントは、管理アカウントから送信された RFC を通じてプロビジョニングされます。

- VPC [ct-1zdasmc2ewzrs](#) を使用してアプリケーションアカウントを作成する
- Accelerate アカウントの作成 [ct-2p93tyd5angmi](#)
- カスターマネージドアプリケーションアカウント [ct-3pwbixz27n3tn](#) を作成する

### AMS マネージドアプリケーションアカウント

AMS によって完全に管理されているアプリケーションアカウントは AMS 管理のアプリケーションアカウントと呼ばれ、サービスリクエスト管理、インシデント管理、セキュリティ管理、継続管理 (バックアップ)、パッチ管理、コスト最適化、インフラストラクチャのモニタリングとイベント管理などの運用タスクの一部またはすべてが AMS によって実行されます。

AMS によって実行されるタスクの量は、選択した変更管理モードによって異なります。AMS マネージドアカウントは、変更管理のさまざまなモードをサポートしています。

- [RFC モード](#)
- [AMS の直接変更モード](#)
- [AMS と AWS Service Catalog](#)
- [AMS Advanced Developer モード](#)
- [AMS でのセルフサービスプロビジョニングモード](#)

変更管理とさまざまなモードの詳細については、「」を参照してください[変更管理モード](#)。

AMS 管理なしで AMS 管理アカウントで利用できる AWS のサービスがいくつかあります。これらの AWS サービスのリストと、それらを AMS アカウントに追加する方法については、「[セルフサービスプロビジョニング](#)」セクションを参照してください。

## AMS Accelerate アカウント

AMS Accelerate は、ワークロードをサポートする AWS インフラストラクチャを運用できる AMS 運用プランです。モニタリングとアラート、インシデント管理、セキュリティ管理、バックアップ管理などの AMS Accelerate 運用サービスのメリットを享受できます。新しい移行、ダウンタイムの発生、AWS の使用方法の変更は不要です。AMS Accelerate は、定期的なパッチ適用を必要とする EC2 ベースのワークロード用のオプションのパッチアドオンも提供します。

AMS Accelerate を使用すると、すべての AWS サービスをネイティブに、または任意のツールで自由に使用、設定、デプロイできます。AMS は、チームのスケーリング、コストの最適化、セキュリティと効率の向上、回復力の向上に役立つ実証済みのプラクティスを一貫して適用しながら、希望するアクセスと変更のメカニズムを使用します。

### Note

AMS Advanced の AMS Accelerate アカウントには、AMS 変更管理 (RFCs) や AMS Advanced コンソールはありません。代わりに、AMS Accelerate コンソールと機能があります。

Accelerate アカウントは、AMS マルチアカウントランディングゾーン管理アカウントからのみプロビジョニングできます。Accelerate にはさまざまな運用機能があります。詳細については、[Accelerate サービスの説明](#)を参照してください。

- 集中ログ記録、単一請求、セキュリティアカウントと SCPs の Config Aggregator など、マルチアカウントランディングゾーン (MALZ) コアアカウントの一部の機能は引き続き利用できます。

- AMS Accelerate は、EPS、アクセス管理、変更管理、プロビジョニングなどの一部の AMS Advanced サービスを提供していません。トランジットゲートウェイ (TGW) にアクセスして設定するには、次のステップに従うことをお勧めします。

Accelerate の詳細については、「What [is Accelerate](#)」を参照してください。

## Accelerate アカウントの作成

Accelerate アカウントを作成するには、「[Accelerate アカウントを作成する](#)」で説明されているステップに従います。

## Accelerate アカウントへのアクセス

マルチアカウントランディングゾーン (MALZ) アカウントに Accelerate アカウントをプロビジョニングすると、[管理者アクセス](#)許可を持つロール AccelerateDefaultAdminRole が、引き受けるアカウントにあります。

新しい Accelerate アカウントにアクセスするには：

- CustomerDefaultAssumeRole ロールを使用して管理アカウントの IAM コンソールにログインします。
- IAM コンソールのナビゲーションバーで、ユーザー名を選択します。
- [Switch Role] (ロールの切り替え) を選択します。このオプションを選択するのが初めての場合、詳細な情報がページに表示されます。情報を読んだ後、[ロールの切り替え] を選択します。ブラウザの Cookie をオフにすると、このページが再び表示されることがあります。
- ロールの切り替えページで、Accelerate アカウント ID と引き受けるロールの名前を入力します。AccelerateDefaultAdminRole

アクセス権限が付与されたので、新しい IAM ロールを作成して、引き続き環境にアクセスできます。Accelerate アカウントに SAML フェデレーションを活用する場合は、「[SAML 2.0 フェデレーションユーザーが AWS マネジメントコンソールにアクセスできるようにする](#)」を参照してください。

## Accelerate アカウントを Transit Gateway に接続する

AMS は Accelerate アカウントのネットワーク設定を管理しません。AWS APIs「[ネットワークソリューション](#)」を参照)、AMS MALZ にデプロイされた既存の Transit Gateway (TGW) を使用して AMS によって管理される MALZ ネットワークに接続するかを選択できます。



**Note**

Accelerate アカウントが同じ AWS リージョンにある場合にのみ、VPC を TGW にアタッチできます。詳細については、[「トランジットゲートウェイ」](#)を参照してください。

Accelerate アカウントを Transit Gateway に追加するには、[デプロイ | マネージドランディングゾーン | ネットワークアカウント | 静的ルート \(ct-3r2ckznm0a59\) 変更タイプ](#)を使用して新しいルートをリクエストし、次の情報を含めます。

- **ブラックホール:** ルートのターゲットが使用できないことを示すために true。これを行うのは、静的ルートのトラフィックが Transit Gateway によってドロップされる場合です。指定した TGW アタッチメント ID にトラフィックをルーティングする場合は False。デフォルト値は false です。
- **DestinationCidrBlock:** 送信先の一致に使用される IPV4 CIDR 範囲。ルーティングの決定は、最も具体的な一致に基づきます。例: 10.0.2.0/24。
- **TransitGatewayAttachmentId:** ルートテーブルターゲットとして機能する TGW アタッチメント ID。ブラックホールが false の場合、このパラメータは必須です。それ以外の場合は、このパラメータを空白のままにします。例: tgw-attach-04eb40d1e14ec7272。
- **TransitGatewayRouteTableId:** TGW ルートテーブルの ID。例: tgw-rtb-06ddc751c0c0c881c。

TGW ルートテーブルにルートを作成して、この VPC に接続します。

1. デフォルトでは、この VPC は MALZ ネットワーク内の他の VPCs と通信できません。
2. この Accelerate VPCs と通信する VPC をソリューションアーキテクトで決定します。
3. [デプロイの送信 | マネージドランディングゾーン | ネットワークアカウント | 静的ルート \(ct-3r2ckznm0a59\) 変更タイプ](#)を追加し、この情報を含めます。

- **ブラックホール:** ルートのターゲットが使用できないことを示すために true。これを行うのは、静的ルートのトラフィックが Transit Gateway によってドロップされる場合です。指定した TGW アタッチメント ID にトラフィックをルーティングする場合は False。デフォルト値は false です。
- **DestinationCidrBlock:** 送信先の一致に使用される IPV4 CIDR 範囲。ルーティングの決定は、最も具体的な一致に基づきます。例: 10.0.2.0/24。
- **TransitGatewayAttachmentId:** ルートテーブルターゲットとして機能する TGW アタッチメント ID。ブラックホールが false の場合、このパラメータは必須です。それ以外の場合は、このパラメータを空白のままにします。例: tgw-attach-04eb40d1e14ec7272。



- TransitGatewayRouteTableId: TGW ルートテーブルの ID。例: tgw-rtb-06ddc751c0c0c881c。

新しい Accelerate アカウント VPC を AMS マルチアカウントランディングゾーンネットワークに接続する (TGW VPC アタッチメントを作成する)。

1. マルチアカウントランディングゾーンのネットワークアカウントで、[Amazon VPC コンソール](#)を開きます。
2. ナビゲーションペインで [Transit Gateways] を選択します。表示されるトランジットゲートウェイの TGW ID を記録します。
3. Accelerate アカウントで、[Amazon VPC コンソール](#)を開きます。
4. ナビゲーションペインで、トランジットゲートウェイアタッチメント > トランジットゲートウェイアタッチメントの作成を選択します。以下の選択を行います。
  - トランジットゲートウェイ ID で、ステップ 2 で記録したトランジットゲートウェイ ID を選択します。
  - [添付タイプ] で、[VPC] を選択します。
  - オプションで、[VPC Attachment (VPC アタッチメント)] に [アタッチメントタグの名前] を入力します。
  - [DNS サポート] と [IPv6 サポート] を有効にするかどうかを選択します。
  - [VPC ID] で、Transit Gateway にアタッチする VPC を選択します。この VPC には少なくとも 1 つのサブネットが関連付けられている必要があります。
  - [サブネット ID] で、トラフィックをルーティングするためにトランジットゲートウェイが使用するアベイラビリティゾーンごとに 1 つのサブネットを選択します。少なくとも 1 つのサブネットを選択する必要があります。アベイラビリティゾーンごとに 1 つだけサブネットを選択できます。
5. [アタッチメント作成] を選択します。新しく作成した TGW アタッチメントの ID を記録します。

TGW アタッチメントをルートテーブルに関連付ける：

1. VPC を関連付ける TGW ルートテーブルを決定します。デプロイ | マネージドランディングゾーン | ネットワークアカウント | トランジットゲートウェイルートテーブルの作成 (ct-3dscwaeyi6cup) 変更タイプを使用して、Accelerate アカウント VPCs 用の新しいアプリケーションルートテーブルを作成することをお勧めします。

2. [管理 | マネージドランディングゾーン | ネットワークアカウント | ネットワークアカウントの TGW アタッチメント](#) (ct-3nmh0qr338q6) RFC を関連付けて、VPC または TGW アタッチメントを選択したルートテーブルに関連付けます。

TGW ルートテーブルにルートを作成して、この VPC に接続します。

1. デフォルトでは、この VPC はマルチアカウントランディングゾーンネットワーク内の他の VPCs と通信できません。
2. この Accelerate アカウント VPCs と通信する VPC をソリューションアーキテクトで決定します。
3. [デプロイを送信する | マネージドランディングゾーン | ネットワークアカウント | ネットワークアカウントに対して静的ルート](#) (ct-3r2ckznmt0a59) RFC を追加して、必要な TGW ルートを作成します。

AMS マルチアカウントランディングゾーントランジットゲートウェイを指すように VPC Route テーブルを設定します。

1. ソリューションを使用して、AMS マルチアカウントランディングゾーントランジットゲートウェイに送信するトラフィックを設計します。
2. [デプロイを送信する | マネージドランディングゾーン | ネットワークアカウント | ネットワークアカウントに対して静的ルート](#) (ct-3r2ckznmt0a59) RFC を追加して、必要な TGW ルートを作成します。

## カスターマネージドアプリケーションアカウント

AMS が標準の方法で管理しないアカウントを作成できます。これらのアカウントはカスターマネージドアカウントと呼ばれ、AMS によって管理される一元化されたアーキテクチャの利点を享受しながら、アカウント内のインフラストラクチャを自己運用するための完全な制御を提供します。

カスターマネージドアカウントは、AMS コンソールまたは提供するサービス (パッチ、バックアップなど) にアクセスできません。

カスターマネージドアカウントは、AMS マルチアカウントランディングゾーン管理アカウントからのみプロビジョニングできます。

アプリケーションアカウントと連携する AMS モードは異なります。モードの詳細については、[AWS Managed Servicesモード](#)」を参照してください。

カスタマーマネージドアプリケーションアカウントを作成するには、[「管理アカウント | カスタマーマネージドアプリケーションアカウントの作成」](#)を参照してください。

カスタマーマネージドアプリケーションアカウントを削除するには、[管理アカウント | オフボードアプリケーションアカウント](#)を使用します。( [オフボーディングの確認](#) CT はカスタマーマネージドアプリケーションアカウントには適用されません )。

## カスタマーマネージドアカウントへのアクセス

マルチアカウントランディングゾーンでカスタマーマネージドアカウント (CMA) をプロビジョニングすると、(MALZ) 管理者ロール CustomerDefaultAdminRoleがアカウントに入り、SAML フェデレーションを通じてアカウントを設定できるようになります。

CMA にアクセスするには :

1. CustomerDefaultAssumeRole ロールを使用して、管理アカウントの IAM コンソールにログインします。
2. IAM コンソールのナビゲーションバーで、ユーザー名を選択します。
3. [Switch Role] (ロールの切り替え) を選択します。このオプションを選択するのが初めての場合、詳細な情報がページに表示されます。情報を読んだ後、[ロールの切り替え] を選択します。ブラウザの Cookie をオフにすると、このページが再び表示されることがあります。
4. ロールの切り替えページで、カスタマーマネージドアカウント ID と引き受けるロールの名前を入力します: CustomerDefaultAdminRole。

アクセス権が付与されたので、新しい IAM ロールを作成して、引き続き環境にアクセスできます。CMA アカウントに SAML フェデレーションを活用する場合は、[「SAML 2.0 フェデレーティッドユーザーが AWS マネジメントコンソールにアクセスできるようにする」](#)を参照してください。

## CMA と Transit Gateway の接続

AMS は、カスタマーマネージドアカウント (CMAs) のネットワーク設定を管理しません。AWS APIs [「ネットワークソリューション」](#)を参照)、AMS MALZ にデプロイされた既存の Transit Gateway (TGW) を使用して AMS によって管理されるマルチアカウントランディングゾーンネットワークに接続するかを選択できます。

**Note**

CMA が同じ AWS リージョンにある場合にのみ、VPC を TGW にアタッチできます。詳細については、[「トランジットゲートウェイ」](#)を参照してください。

CMA を Transit Gateway に追加するには、[ネットワークアカウントで新しいルートをリクエストする | 静的ルート \(ct-3r2ckznmt0a59\) の変更タイプを追加](#)し、この情報を含めます。

- **ブラックホール:** ルートのターゲットが使用できないことを示すために true。これは、静的ルートのトラフィックが Transit Gateway によってドロップされる場合に行います。指定した TGW アタッチメント ID にトラフィックをルーティングする場合は False。デフォルト値は false です。
- **DestinationCidrBlock:** 送信先の一致に使用される IPV4 CIDR 範囲。ルーティングの決定は、最も具体的な一致に基づきます。例えば、10.0.2.0/24 などです。
- **TransitGatewayAttachmentId:** ルートテーブルターゲットとして機能する TGW アタッチメント ID。ブラックホールが false の場合、このパラメータは必須です。それ以外の場合は、このパラメータを空白のままにします。例えば、tgw-attach-04eb40d1e14ec7272 などです。
- **TransitGatewayRouteTableId:** TGW ルートテーブルの ID。例えば、tgw-rtb-06ddc751c0c0c881c などです。

新しいカスターマネージド VPC を AMS マルチアカウントランディングゾーンネットワークに接続する (TGW VPC アタッチメントを作成する)。

1. マルチアカウントランディングゾーンのネットワークアカウントで、[Amazon VPC コンソール](#)を開きます。
2. ナビゲーションペインで、トランジットゲートウェイを選択します。表示されるトランジットゲートウェイの TGW ID を記録します。
3. カスターマネージドアカウントで、[Amazon VPC コンソール](#)を開きます。
4. ナビゲーションペインで、トランジットゲートウェイアタッチメント > トランジットゲートウェイアタッチメントの作成を選択します。以下の選択を行います。
  - a. トランジットゲートウェイ ID で、ステップ 2 で記録したトランジットゲートウェイ ID を選択します。
  - b. [添付タイプ] で、[VPC] を選択します。
  - c. オプションで、[VPC Attachment (VPC アタッチメント)] に [アタッチメントタグの名前] を入力します。

- d. [DNS サポート] と [IPv6 サポート] を有効にするかどうかを選択します。
  - e. [VPC ID] で、Transit Gateway にアタッチする VPC を選択します。この VPC には少なくとも 1 つのサブネットが関連付けられている必要があります。
  - f. [サブネット ID] で、トラフィックをルーティングするためにトランジットゲートウェイが使用するアベイラビリティゾーンごとに 1 つのサブネットを選択します。少なくとも 1 つのサブネットを選択する必要があります。アベイラビリティゾーンごとに 1 つだけサブネットを選択できます。
5. [アタッチメント作成] を選択します。新しく作成した TGW アタッチメントの ID を記録します。

TGW アタッチメントをルートテーブルに関連付ける：

VPC を関連付ける TGW ルートテーブルを決定します。デプロイ | マネージドランディングゾーン | ネットワークアカウント | トランジットゲートウェイルートテーブル (ct-3dscwaeyi6cup) RFC を送信して、カスターマネージド VPCs の新しいアプリケーションルートテーブルを作成することをお勧めします。VPC または TGW アタッチメントを選択したルートテーブルに関連付けるには、デプロイ | マネージドランディングゾーン | ネットワークアカウント | TGW アタッチメントの関連付け (ct-3nmh0qr338q6) RFC をネットワークアカウントに送信します。

TGW ルートテーブルにルートを作成して、この VPC に接続します。

1. デフォルトでは、この VPC はマルチアカウントランディングゾーンネットワーク内の他の VPCs と通信できません。
2. ソリューションを使用して、このカスターマネージド VPCs と通信する VPC を設計します。デプロイを送信する | マネージドランディングゾーン | ネットワークアカウント | ネットワークアカウントに対して静的ルート (ct-3r2ckznmt0a59) RFC を追加して、必要な TGW ルートを作成します。

**Note**

この CT (ct-3r2ckznmt0a59) では、コアルートテーブル EgressRouteDomain に静的ルートを追加することはできません。CMA で出力トラフィックを許可する必要がある場合は、ct-0xdawir96cy7k を使用して管理 | その他 | その他 (MOO) RFC を送信します。

AMS マルチアカウントランディングゾーントランジットゲートウェイを指すように VPC ルートテーブルを設定します。

ソリューションを使用して、AMS マルチアカウントランディングゾーントランジットゲートウェイに送信するトラフィックを設計します。VPC ルートテーブルを更新して、前に作成した TGW アタッチメントにトラフィックを送信する

カスタマーマネージドアカウントに関する運用上のヘルプの取得

AMS は、アカウントを AMS Accelerate にオンボーディングすることで、カスタマーマネージドアカウントにデプロイしたワークロードを運用するのに役立ちます。AMS Accelerate を使用すると、新しい移行を経験したり、ダウンタイムが発生したり、使用方法を変更したりすることなく、モニタリングとアラート、インシデント管理、セキュリティ管理、バックアップ管理などの運用サービスからメリットを得ることができます AWS。AMS Accelerate は、定期的なパッチ適用を必要とする EC2-based ワークロード用のオプションのパッチアドオンも提供します。AMS Accelerate では、AMS Advanced カスタマーマネージドアカウントと同様に、すべての AWS サービスをネイティブに、または任意のツールで引き続き使用、設定、デプロイします。AMS は、チームのスケーリング、コストの最適化、セキュリティと効率の向上、回復性の向上に役立つ実証済みのプラクティスを適用しながら、任意のアクセスと変更のメカニズムを使用します。詳細については、[Accelerate サービスの説明](#)を参照してください。

カスタマーマネージドアカウントを Accelerate にオンボードするには、CSDM に連絡し、[「AMS Accelerate の開始方法」](#)のステップに従います。

**Note**

AMS Advanced の AMS Accelerate アカウントには、AMS 変更管理 (変更または RFCs のリクエスト) や AMS Advanced コンソールはありません。代わりに、AMS Accelerate コンソールと機能があります。

## AMS Tools アカウント (ワークロードの移行)

マルチアカウントランディングゾーンツールアカウント (VPC を使用) は、移行作業の迅速化、セキュリティポジションの向上、コストと複雑さの軽減、使用パターンの標準化に役立ちます。

ツールアカウントには以下が用意されています。

- 本番ワークロード外のシステムインテグレーターのレプリケーションインスタンスにアクセスするための明確に定義された境界。
- 分離されたチェンバーを作成して、他のワークロードのアカウントに配置する前に、ワークロードにマルウェアや不明なネットワークルートがないか確認します。
- 定義されたアカウント設定として、ワークロードの移行のためのオンボーディングとセットアップにかかる時間を短縮します。
- 隔離されたネットワークルートは、オンプレミス -> CloudEndure -> Tools account -> AMS 取り込みイメージからのトラフィックを保護します。イメージが取り込まれたら、AMS Management | Advanced stack components | AMI | Share (ct-1eiczxw8ihc18) RFC を介してイメージを送信先アカウントと共有できます。

高レベルのアーキテクチャ図:

Deployment | Managed Landing Zone | Management Account | Create tools account (with VPC) change type (ct-2j7q1hgf26x5c) を使用して、ツールアカウントをすばやくデプロイし、マルチアカウント Landing Zone 環境内でワークロード取り込みプロセスをインスタンス化します。 [「管理アカウント」](#)、[「ツールアカウント: 作成 \(VPC を使用\)」](#) を参照してください。

### Note

これは移行ハブであるため、2 つのアベイラビリティーゾーン (AZs) を使用することをお勧めします。

デフォルトでは、AMS はすべてのアカウントに次の 2 つのセキュリティグループ (SGs) を作成します。これら 2 つの SGs が存在することを確認します。存在しない場合は、AMS チームで新しいサービスリクエストを開いてリクエストしてください。

- SentinelDefaultSecurityGroupPrivateOnlyEgressAll
- InitialGarden-SentinelDefaultSecurityGroupPrivateOnly



CloudEndure レプリケーションインスタンスが、オンプレミスに戻るルートがあるプライベートサブネットに作成されていることを確認します。プライベートサブネットのルートテーブルに TGW へのデフォルトルートがあることを確認することができます。ただし、CloudEndure マシンのカットオーバーを実行すると、オンプレミスに戻るルートがなく、インターネットアウトバウンドトラフィックのみが許可される「分離された」プライベートサブネットに移動する必要があります。オンプレミスリソースへの潜在的な問題を回避するために、分離されたサブネットでカットオーバーが発生するようにすることが重要です。

#### 前提条件:

1. Plus または Premium のサポートレベル。
2. AMIs がデプロイされる KMS キーのアプリケーションアカウント IDs。
3. 前述のように作成されたツールアカウント。

#### AWS アプリケーション移行サービス (AWS MGN)

[AWS Application Migration Service](#) (AWS MGN) は、ツールアカウントのプロビジョニング中に自動的に作成される IAM `AWSManagedServicesMigrationRole` ロールを介して MALZ Tools アカウントで使用できます。AWS MGN を使用して、サポートされているバージョンの Windows および Linux [オペレーティングシステム](#)で実行されるアプリケーションとデータベースを移行できます。

AWS リージョン サポートに関するup-to-dateについては、[AWS 「リージョンサービスリスト」](#)を参照してください。

希望する AWS リージョン が現在 MGN AWS でサポートされていない場合、またはアプリケーションが実行されているオペレーティングシステムが現在 MGN AWS でサポートされていない場合は、代わりにツールアカウントで [CloudEndure Migration](#) を使用することを検討してください。

#### MGN AWS 初期化のリクエスト

AWS MGN は、最初に使用する前に AMS によって[初期化](#)する必要があります。新しい Tools アカウントに対してこれをリクエストするには、管理 | その他 | その他の RFC を Tools アカウントから以下の詳細とともに送信します。

RFC Subject=Please initialize AWS MGN in this account

RFC Comment=Please click 'Get started' on the MGN welcome page here:



[https://console.aws.amazon.com/mgn/home?region=MALZ\\_PRIMARY\\_REGION#/welcome](https://console.aws.amazon.com/mgn/home?region=MALZ_PRIMARY_REGION#/welcome) using all default values to 'Create template' and complete the initialization process.

AMS が RFC を正常に完了し、ツールアカウントで AWS MGN を初期化したら、AWSManagedServicesMigrationRoleを使用して要件のデフォルトテンプレートを編集できます。

## 新しい AMS Tools アカウントへのアクセスを有効にする

ツールアカウントが作成されると、AMS はアカウント ID を提供します。次のステップは、新しいアカウントへのアクセスを設定することです。以下の手順に従ってください。

### 1. 適切な Active Directory グループを適切なアカウント IDs。

新しい AMS 作成アカウントは、ReadOnly ロールポリシーと、ユーザーが RFCs。

Tools アカウントには、追加の IAM ロールとユーザーも用意されています。

- IAM ロール: AWSManagedServicesMigrationRole
- IAM ユーザー: customer\_cloud\_endure\_user

### 2. サービス統合チームのメンバーが次のレベルのツールを設定できるように、ポリシーとロールをリクエストします。

AMS コンソールに移動し、次の RFCs。

- a. KMS キーを作成します。 [KMS キーの作成 \(自動\)](#) または [KMS キーの作成 \(マネージドオートメーション\)](#) を使用します。

KMS を使用して取り込まれたリソースを暗号化する場合、他のマルチアカウントランディングゾーンアプリケーションアカウントと共有されている単一の KMS キーを使用すると、は取り込まれたイメージを宛先アカウントで復号化できる場所にセキュリティを提供します。

- b. KMS キーを共有します。

管理 | 高度なスタックコンポーネント | KMS キー | 共有 (マネージドオートメーション) 変更タイプ (ct-05yb337abq3x5) を使用して、新しい KMS キーが取り込まれた AMIs が存在するアプリケーションアカウントと共有されるようにリクエストします。

最終的なアカウント設定の例:

## AMS の事前承認された IAM CloudEndure ポリシーの例

AMS の事前承認された IAM CloudEndure ポリシーを表示するには: [WIGS Cloud Endure ランディングゾーン](#)の例ファイルを解凍し、を開きますcustomer\_cloud\_endure\_policy.json。

## AMS Tools アカウント接続とend-to-endテスト

1. まず、CloudEndure を設定し、AMS にレプリケートするサーバーに CloudEndure エージェントをインストールします。
2. CloudEndure でプロジェクトを作成します。
3. シークレットマネージャーを使用して、前提条件を実行したときに共有された AWS 認証情報を入力します。
4. レプリケーション設定:
  - a. レプリケーションサーバーに適用するセキュリティグループを選択するオプションで、両方の AMS "Sentinel" セキュリティグループ (プライベートのみと EgressAll) を選択します。
  - b. マシン (インスタンス) のカットオーバーオプションを定義します。詳細については、[「ステップ 5」を参照してください。カットオーバー](#)
  - c. サブネット: プライベートサブネット。
5. セキュリティグループ:
  - a. AMS "Sentinel" セキュリティグループ (プライベートのみと EgressAll) の両方を選択します。
  - b. カットオーバーインスタンスは、AMS 管理の Active Directory (MAD) と AWS パブリックエンドポイントと通信する必要があります。
    - i. Elastic IP: なし
    - ii. パブリック IP: なし
    - iii. IAM ロール: customer-mc-ec2-instance-profile
  - c. 内部タグ付け規則に従ってタグを設定します。
6. CloudEndure エージェントをマシンにインストールし、EC2 コンソールの AMS アカウントに表示されるレプリケーションインスタンスを探します。

## AMS 取り込みプロセス:

## AMS Tools アカウントのハイジーン

アカウントで AMI を共有し、レプリケートされたインスタンスが不要になったら、クリーンアップする必要があります。

- インスタンス後の WIGs 取り込み：
  - カットオーバーインスタンス: 少なくとも、作業が完了したら、AWS コンソールを介してこのインスタンスを停止または終了します。
  - 取り込み前 AMI バックアップ: インスタンスが取り込まれ、オンプレミスインスタンスが終了したら削除する
  - AMS で取り込まれたインスタンス: スタックをオフにするか、AMI を共有したら終了します。
  - AMS で取り込まれた AMIs: 送信先アカウントとの共有が完了したら削除する
- 移行のクリーンアップの終了: デベロッパーモードでデプロイされたリソースを文書化して、クリーンアップが定期的に行われるようにします。次に例を示します。
  - セキュリティグループ
  - クラウド形式を使用して作成されたリソース
  - ネットワーク ACK
  - サブネット
  - VPC
  - ルートテーブル
  - ロール
  - ユーザーとアカウント

### 大規模な移行 - Migration Factory

[「AWS CloudEndure Migration Factory ソリューションの紹介」](#)を参照してください。

## SALZ ネットワークアーキテクチャ

次の図は、AWS Managed Services (AMS) シングルアカウントランディングゾーン (SALZ) VPC ネットワークレイアウトを示しており、可用性の高いセットアップの例です。

AMS は、標準テンプレートとオンボーディング中に提供された選択したオプションに基づいて、ネットワーキングのあらゆる側面を設定します。標準の AWS ネットワーク設計が AWS アカウントに適用され、仮想プライベートクラウド (VPC) が作成され、VPN または Direct Connect によって AMS に接続されます。Direct Connect の詳細については、[AWS Direct Connect](#) を参照してください。標準 VPCs には、DMZ、共有サービス、アプリケーションサブネットが含まれます。オンボーディングプロセス中に、ニーズ (顧客部門、パートナーなど) に合わせて追加の VPCs がリクエストおよび作成される場合があります。オンボーディング後、ネットワーク図が提供されます。ネットワークの設定方法を説明する環境ドキュメントです。

#### Note

すべてのアクティブなサービスのデフォルトのサービス制限と制約については、[AWS Service Limits](#) ドキュメントを参照してください。

当社のネットワーク設計は、Amazon の「[最小特権の原則](#)」を中心に構築されています。これを実現するために、信頼されたネットワークからのトラフィックを除き、インバウンドとアウトバウンドのすべてのトラフィックをゲートウェイ経由でルーティングします。唯一の信頼されたネットワークは、VPN や AWS Direct Connect (DX) を使用してオンプレミス環境と VPC 間で設定されるネットワークです。アクセスは踏み台インスタンスを使用して付与されるため、本番稼働用リソースに直接アクセスできなくなります。すべてのアプリケーションとリソースは、パブリックロードバランサーを介して到達可能なプライベートサブネット内に存在します。パブリックエグレストラフィックは、転送プロキシを介してインターネットゲートウェイに、次にインターネットに流れます。または、トラフィックが VPN または Direct Connect 経由でオンプレミス環境に流れることもあります。

## AMS シングルアカウントランディングゾーン共有サービス

共有サービスサブネットには、AMS Directory Services、プロビジョニングと一般的なタスクを自動化する管理ホスト、ウイルス対策 (TrendMicro) 管理サーバー、内部踏み台ホストが含まれます。

- AMS Directory Services = AD ドメインコントローラー

AMS アカウントに Active Directory を作成し、AMS ドメインを作成し、起動時にマネージドスタックをドメインに結合します。

- 管理ホスト = AMS 管理ホスト (プロビジョニングと一般的なタスクを自動化)

Directory Service ドメインコントローラーを変更、操作する API Directory Service エンドポイントとして機能します。

- セキュリティサービス: ウイルス対策 (TrendMicro) 管理サーバー = EPS DSM + EPS Relay

Trend Micro" Deep Security ソフトウェア (DSM) を活用し、クライアント/サーバーモデルで動作し、Deep Security マネージャー、エージェント、リレーを含むバックエンドデータベースを備えています。

- 内部踏み台ホスト = 顧客踏み台

インターネットからのプライマリアクセスポイントであり、他の Amazon EC2 インスタンスのプロキシとして機能するように設計された専用サーバー。

# AMS のセットアップ

## トピック

- [AMS のデフォルト設定を理解する](#)
- [AMS コンソールの使用](#)
- [AMS API と CLI の使用](#)
- [AMS が独自の EPS を導入する](#)
- [AMS 通知の受信](#)
- [プライベート DNS とパブリック DNS のセットアップ](#)
- [AMS 出カトラフィック管理](#)
- [AMS Advanced での IAM リソースのデプロイ](#)
- [IAM ロールとプロファイルを使用した AMS でのアクセス許可の設定](#)
- [AD FS クレームルールと SAML 設定](#)
- [ネットワーク ACL で制限する](#)
- [Outposts での AMS](#)
- [AMS でのタグの使用](#)
- [AWS Managed Services リソーススケジューラ](#)
- [AWS Systems Manager AMS Advanced の](#)
- [AMS アカウントのオフボード](#)

一部の AMS セットアップタスクは、オンボーディング時に完了する場合があります。

AMS を含む役割と責任の詳細については、[サポートされている AWS サービス](#)「」を参照してください。[AMS 責任マトリックス \(RACI\)](#)。

### Note

AMS に追加の AWS サービスを提供するようにリクエストするには、サービスリクエストをファイルします。このリクエストを行う方法については、「」を参照してください。[サービスリクエスト管理](#)。

# AMS のデフォルト設定を理解する

AWS Managed Services (AMS) ネットワークには、ほとんどのサービスのデフォルトを含む標準化された設定があります。

このセクションでは、AMS がアクセス、モニタリング、ログ記録、管理に使用するデフォルト設定について説明します。

マルチアカウントランディングゾーンまたはシングルアカウントランディングゾーンのインフラストラクチャコストの例については、「」を参照してください[AMS 環境の基本コンポーネント](#)。

## トピック

- [DNS 解決のデフォルト \(MALZ\)](#)
- [EC2 IAM インスタンスプロファイル](#)
- [AMS でのベースラインモニタリングからのアラート](#)
- [ログの保持とローテーションのデフォルト](#)

## DNS 解決のデフォルト (MALZ)

AWS Managed Services (AMS) マルチアカウントランディングゾーン: AWS 環境では、Resolver 転送ルールを設定することで、VPC 内の Route 53 Resolver と DNS リゾルバー間のドメイン名システム (DNS) 解決を統合できます。これらのルールを使用して DNS クエリを転送する前に、これらのクエリを転送できるインバウンドリゾルバーエンドポイントとアウトバウンドリゾルバーエンドポイントを設定する必要があります。

デフォルトでは、AMS のマルチアカウント設定のアプリケーションアカウント VPCs 内の DNS クエリは、共有サービスアカウントに存在する AWS Directory Service for Microsoft Active Directory (マネージド AD と呼ばれます) ドメインの条件付きフォワーダーに転送されます。AMS では、オプションで AmazonProvidedDNS を使用できます。たとえば、AmazonProvidedDNS を使用して DNS クエリを転送できます。これにより、現在 Amazon Route 53 を介して Amazon が提供する DNS のみをサポートする VPC エンドポイントを利用できます。それに応じて、リゾルバールールは、共有サービスアカウントにデフォルトでデプロイされる一般的な VPC エンドポイントにも自動的に設定されます。これらの一般的な VPC エンドポイントの詳細については、「」を参照してください[AMS VPC エンドポイント](#)。

VPCs で Dynamic Host Configuration Protocol (DHCP) オプションセットを設定するには、およびには、共有サービスアカウントの共通 VPC エンドポイントを指す Route53 Resolver ルールがあります (オンプレミスドメイン用のオプションの Resolver ルールを使用)。管理の作成 | その他 | そ

の他 | 共有サービスアカウントを指定する変更リクエスト (RFC) の作成 および は、VPC エンドポイントのアプリケーションアカウント VPC ローカル DNS および Route 53 Resolver ルールの有効化をリクエストします。

## EC2 IAM インスタンスプロファイル

インスタンスプロファイルは IAM ロールのコンテナであり、インスタンスの起動時に EC2 インスタンスにロール情報を渡すために使用できます。

### MALZ

と の 2 つの AMS customer-mc-ec2-instance-profile デフォルトインスタンスプロファイルがありますcustomer-mc-ec2-instance-profile-s3。これらのインスタンスプロファイルは、次の表で説明するアクセス許可を提供します。

#### ポリシーの説明

| プロファイル                              | ポリシー                                                                                              |
|-------------------------------------|---------------------------------------------------------------------------------------------------|
| customer-mc-ec2-instance-profile    | AmazonSSMManagedInstanceCore : Ec2 インスタンスに SSM エージェントの使用を許可します。                                   |
|                                     | AMSInstanceProfileLoggingPolicy : Ec2 インスタンスが S3 と CloudWatch にログをプッシュできるようにします。                  |
|                                     | AMSInstanceProfileManagementPolicy : Ec2 インスタンスが Active Directory の結合などの起動アクションを実行できるようにします。      |
|                                     | AMSInstanceProfileMonitoringPolicy : Ec2 インスタンスが AMS モニタリングサービスに結果をレポートできるようにします。                 |
|                                     | AMSInstanceProfilePatchPolicy : Ec2 インスタンスがパッチを受信できるようにします。                                       |
| customer-mc-ec2-instance-profile-s3 | AMSInstanceProfileBYOEPSPolicy : Ec2 インスタンスが <a href="#">AMS Bring Your Own EPS</a> を使用できるようにします。 |



| プロファイル | ポリシー                                                                                                             |
|--------|------------------------------------------------------------------------------------------------------------------|
|        | <p><code>AMSInstanceProfileLoggingPolicy</code> : Ec2 インスタンスが S3 と CloudWatch にログをプッシュできるようにします。</p>             |
|        | <p><code>AMSInstanceProfileManagementPolicy</code> : Ec2 インスタンスが Active Directory の結合などの起動アクションを実行できるようにします。</p> |
|        | <p><code>AMSInstanceProfileMonitoringPolicy</code> : Ec2 インスタンスが AMS モニタリングサービスに結果をレポートできるようにします。</p>            |
|        | <p><code>AMSInstanceProfilePatchPolicy</code> : Ec2 インスタンスがパッチを受信できるようにします。</p>                                  |
|        | <p><code>AMSInstanceProfileS3WritePolicy</code> : Ec2 インスタンスがお客様の S3 バケットを読み書きできるようにします。</p>                     |

## SALZ

IAM インスタンスポリシー からのアクセス許可を付与 `customer-mc-ec2-instance-profile` する AMS デフォルトインスタンスプロファイル が 1 つあります `customer_ec2_instance_profile_policy`。このインスタンスプロファイルは、次の表で説明するアクセス許可を提供します。プロファイルは、インスタンスにログインするユーザーではなく、インスタンスで実行されているアプリケーションにアクセス許可を付与します。

ポリシーには、多くの場合、複数のステートメントが含まれます。各ステートメントは、異なるリソースセットにアクセス許可を付与するか、特定の条件下でアクセス許可を付与します。

CW = CloudWatch。ARN = Amazon リソースネーム。\* = ワイルドカード (任意)。

## EC2 のデフォルトの IAM インスタンスプロファイルのアクセス許可

CW = CloudWatch。ARN = Amazon リソースネーム。\* = ワイルドカード (任意)。

| ポリシーステートメント                               | 効果 | アクション                                                                          | 説明とリソース (ARN)                                                                                                      |
|-------------------------------------------|----|--------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Amazon Elastic Compute Cloud (Amazon EC2) |    |                                                                                |                                                                                                                    |
| EC2 メッセージアクション                            | 許可 | AcknowledgeMessage、DeleteMessage、FailMessage、GetEndpoint、GetMessages、SendReply | アカウントで EC2 Systems Manager メッセージングアクションを許可します。                                                                     |
| Ec2 の説明                                   | 許可 | *(すべて)                                                                         | コンソールがアカウント内の EC2 の設定の詳細を表示できるようにします。                                                                              |
| IAM ロール ID を取得する                          | 許可 | GetRole                                                                        | EC2 が <code>aws:iam::*:role/customer-*</code> および から IAM ID を取得できるようにします <code>aws:iam::*:role/customer_*</code> 。 |
| ログイベントをアップロードするインスタンス                     | 許可 | ロググループの作成                                                                      | ログの作成を に許可します。<br><code>aws:logs::*:log-group:i-*</code>                                                           |
|                                           |    | ログストリームの作成                                                                     | ログのストリーミング先を許可します。 <code>aws:logs::*:log-group:i-*</code>                                                          |
| MMS の CW                                  | 許可 | DescribeAlarms、                                                                | CloudWatch がアカウントのアラームを取得できるようにします。                                                                                |

CW = CloudWatch。ARN = Amazon リソースネーム。\* = ワイルドカード (任意)。

| ポリシーステートメント                             | 効果 | アクション                                                                                                              | 説明とリソース (ARN)                                                                          |
|-----------------------------------------|----|--------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
|                                         |    | PutMetricAlarm、<br>PutMetricData                                                                                   | CW がアラームを作成または更新し、指定されたメトリクスに関連付けることを許可します。<br><br>CW がメトリクスデータポイントをアカウントに発行できるようにします。 |
| Ec2 タグ                                  | 許可 | CreateTags、<br>DescribeTags、                                                                                       | アカウントの指定されたインスタンスでタグを追加、上書き、および記述できるようにします。                                            |
| CW ログを明示的に拒否する                          | 拒否 | DescribeLogStreams、<br>FilterLogEvents、<br>GetLogEvents                                                            | 次のログストリームの一覧表示、フィルタリング、取得を禁止します。aws:logs:*:*:log-group:/mc/*                           |
| Amazon EC2 Simple Systems Manager (SSM) |    |                                                                                                                    |                                                                                        |
| SSM アクション                               | 許可 | DescribeAssociation、<br>GetDocument、<br>ListAssociations、<br>UpdateAssociationStatus、<br>UpdateInstanceInformation | アカウントでさまざまな SSM 関数を許可します。                                                              |

CW = CloudWatch。ARN = Amazon リソースネーム。\* = ワイルドカード (任意)。

| ポリシーステートメント    | 効果 | アクション                                                                                                        | 説明とリソース (ARN)                                                                                                                    |
|----------------|----|--------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| S3 での SSM アクセス | 許可 | GetObject、<br>PutObject、<br>AbortMultipartUpload、<br>ListMultipartUploadParts、<br>ListBucketMultipartUploads | EC2 の SSM が、オブジェクトを取得および更新し、マルチパートオブジェクトのアップロードを中止して、でマルチパートアップロードに使用できるポートとバケットを一覧表示できるようにしますaws:s3:::mc-*-internal-*/aws/ssm*。 |

#### Amazon EC2 Simple Storage Service (S3)

|                       |    |            |                                                                              |
|-----------------------|----|------------|------------------------------------------------------------------------------|
| S3 でオブジェクトを取得する       | 許可 | Get<br>リスト | EC2 アプリケーションがアカウントの S3 バケット内のオブジェクトを取得して一覧表示できるようにします。                       |
| お客様が暗号化したログ S3 アクセス   | 許可 | PutObject  | EC2 アプリケーションがでオブジェクトを更新することを許可する aws:s3:::mc-*logs-*/encrypted/app/*         |
| パッチデータアップロードオブジェクト S3 | 許可 | PutObject  | EC2 アプリケーションがの S3 バケットにパッチデータをアップロードすることを許可する aws:s3:::awsms-a*-patch-data-* |

CW = CloudWatch。ARN = Amazon リソースネーム。\* = ワイルドカード (任意)。

| ポリシーステートメント            | 効果 | アクション              | 説明とリソース (ARN)                                                                                                                                                    |
|------------------------|----|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| S3 への独自のログのアップロード      | 許可 | PutObject          | EC2 アプリケーションがカスタムログを以下にアップロードできるようにします。<br>aws:s3:::mc-a*-logs-*/aws/instances/*/\${aws:userid}/*                                                                |
| MC 名前空間 S3 ログを明示的に拒否する | 拒否 | GetObject*<br>Put* | EC2 アプリケーションが以下との間でオブジェクトを取得または配置することを禁止します。<br><br>aws:s3:::mc-*-logs-*/encrypted/mc* ,<br><br>aws:s3:::mc-*-logs-*/mc/* ,<br><br>aws:s3:::mc-a*-logs-*-audit/* |
| S3 削除を明示的に拒否する         | 拒否 | *(すべて)             | 以下のオブジェクトに対して EC2 アプリケーションがアクションを実行することを禁止します。<br><br>aws:s3:::mc-a*-logs-*/* ,<br><br>aws:s3:::mc-a*-internal-*/* ,                                             |
| S3 CFN バケットを明示的に拒否する   | 拒否 | 削除*                | 以下からのオブジェクトの削除を EC2 アプリケーションに禁止します。aws:s3:::cf-templates-*                                                                                                       |

CW = CloudWatch。ARN = Amazon リソースネーム。\* = ワイルドカード (任意)。

| ポリシーステートメント      | 効果 | アクション      | 説明とリソース (ARN)                                                 |
|------------------|----|------------|---------------------------------------------------------------|
| 明示的に拒否リストバケット S3 | 拒否 | ListBucket | 暗号化、監査ログ、またはリザーブド (mc) オブジェクトの一覧表示を禁止します。aws:s3::mc-* -logs-* |

#### AWS Secrets Manager Amazon EC2 の

|                              |    |                |                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------|----|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Trend Cloud One Secrets アクセス | 許可 | GetSecretValue | <p>Amazon EC2 が Trend Cloud One 移行のシークレットにアクセスできるようにします。</p> <p>aws:secretsmanager::*:secret:/ams/eps/cloud-one-agent-tenant-id* ,</p> <p>arn:aws:secretsmanager::*:secret:/ams/eps/cloud-one-agent-activation-token* ,</p> <p>aws:secretsmanager::*:secret:/ams/eps/cloud-one-agent-tenant-id* ,</p> <p>aws:secretsmanager::*:secret:/ams/eps/cloud-one-agent-tenant-guid*</p> |
|------------------------------|----|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### AWS Key Management Service Amazon EC2 の

CW = CloudWatch。ARN = Amazon リソースネーム。\* = ワイルドカード (任意)。

| ポリシーステートメント             | 効果 | アクション   | 説明とリソース (ARN)                                                                                                                                     |
|-------------------------|----|---------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| Trend Cloud One<br>復号キー | 許可 | Decrypt | Amazon EC2 がエイリアス名 /<br>ams/eps/cloudone-migration で<br>AWS KMS キーを復号できるよう<br>にする<br><br>arn:aws:kms:*:*:alias/<br>ams/eps/cloudone-migrat<br>ion |

Amazon IAM ポリシーに慣れていない場合は、[「IAM ポリシーの概要」](#)で重要な情報を参照してください。

#### Note

ポリシーには、多くの場合、複数のステートメントが含まれます。各ステートメントは、異なるリソースセットにアクセス許可を付与するか、特定の条件下でアクセス許可を付与します。

## AMS でのベースラインモニタリングからのアラート

AMS モニタリングのデフォルトについて説明します。詳細については、[「AMS でのモニタリングとイベント管理」](#)を参照してください。

次の表は、モニタリング対象とデフォルトのアラートしきい値を示しています。アラートしきい値は、必要な変更を決定し、関連する CloudWatch Amazon SNS トピックにサブスクライブした後、管理 | その他 | その他 | 更新 (ct-0xdawir96cy7k) RFC で変更できます。トピックの作成とサブスクライブの詳細については、[「トピックのサブスクライブ」](#)を参照してください。一般的な情報については、[Amazon SNS のFAQs](#)」を参照してください。アラームがしきい値を超えたときに直接通知を受けるには、AMS の標準アラートプロセスに加えて、アラーム設定を上書きする方法に関する以下の手順に従ってください[AMS によって生成されたアラートの受信](#)。

Amazon CloudWatch は、メトリクスの保持期間を延長します。詳細については、[CloudWatch の制限](#)」を参照してください。

#### Note

AMS はベースラインモニタリングを定期的にキャリブレーションします。新しいアカウントは常に最新のベースラインモニタリングでオンボーディングされ、表は新しくオンボーディングされたアカウントのベースラインモニタリングを示しています。AMS は、既存のアカウントのベースラインモニタリングを定期的に更新し、更新が行われるまでに遅延が発生する場合があります。詳細については、「[AMS アカウントのモニタリング設定の表示](#)」を参照してください。

#### Note

EC2 インスタンスアラートNon-root volume usageはデフォルトで DISABLED です。このアラームに基づいてアラート生成が必要な場合は、RFC 変更タイプ [ct-0erkoad6uyvg](#) を使用して有効にする必要があります。

### ベースラインモニタリングからのアラート

| サービス | セキュリティアラート | アラート名とトリガー条件 | 注意事項 |
|------|------------|--------------|------|
|------|------------|--------------|------|

スター付き (\*) アラートの場合、AMS は影響を事前に評価し、可能な場合は修復します。修復が不可能な場合は、AMS がインシデントを作成します。自動化によって問題が修正されない場合、AMS はインシデントケースを通知し、AMS エンジニアが対応します。さらに、これらのアラートは E メールに直接送信できます (Direct-Customer-Alerts SNS トピックにオプトインしている場合)。

|                  |     |                         |                                    |
|------------------|-----|-------------------------|------------------------------------|
| Application Load | いいえ | RejectedConnectionCount | CloudWatch アラームは、ロードバランサーが最大数に達したた |
|------------------|-----|-------------------------|------------------------------------|



| サービス                                  | セキュリティアラート | アラート名とトリガー条件                                                                                           | 注意事項                                                      |
|---------------------------------------|------------|--------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|
| Balancer (ALB) インスタンス                 |            | sum > 0 for 1 min, 5 consecutive times。                                                                | めに拒否された接続の数を示します。                                         |
| Application Load Balancer (ALB) ターゲット | いいえ        | TargetConnectionErrorCount<br>sum > 0 for 1 min, 5 consecutive times。                                  | ロードバランサーと登録されたインスタンス間の接続数が正常に確立されなかった場合の CloudWatch アラーム。 |
| Amazon EC2 インスタンス – Windows           | いいえ        | SecureChannelFailure<br>過去 15 個のデータポイントのうち 10 個が > 0.0。                                                | Windows インスタンスの CloudWatch アラームは、チャネル接続の保護が失敗したときに警告します。  |
| Aurora インスタンス                         | いいえ        | CPUUtilization<br>> 5 分間 85%、2 回連続。                                                                    | CloudWatch アラーム。                                          |
| AWS Backup                            | はい         | DeleteRecoveryPoint<br>予期しない IAM ロールプリンシパルまたは IAM ユーザープリンシパルが AWS Backup 復旧ポイントを削除しました。                | CloudWatch イベント。バックアップ復旧ポイントが削除されたときに出力されます。              |
| AWS Outposts                          | はい         | AMSOupostsInstanceFamilyCapacityAvailability InstanceFamilyCapacityAvailability<br>= 5 分間 80%、連続 12 回。 | リソースのインスタンスファミリー容量の可用性に関する CloudWatch AWS Outposts アラーム。  |

| サービス             | セキュリティアラート | アラート名とトリガー条件                                                                                   | 注意事項                                                                               |
|------------------|------------|------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| EC2 インスタンス - OSs |            | AMSOupostsInstanceTypeCapacityAvailability TypeCapacityAvailability<br><br>= 5 分間 80%、連続 12 回。 | リソースのインスタンスタイプのキャパシティの可用性に関する CloudWatch AWS Outposts アラーム。                        |
|                  |            | AMSOupostsConnectedStatusC<br>onnectedStatus<br><br>< 1 を 5 分間、1 回連続。                          | AWS Outposts サービスリンク接続の CloudWatch アラーム。1 カウント未満で障害が発生します。                         |
|                  |            | AMSOupostsCapacityException<br>nCapacityExceptions<br><br>0 は 5 分間、1 回連続。                      | AWS Outposts リソースのインスタンス起動の容量不足エラーに関する CloudWatch アラーム<br>.                        |
|                  | いいえ        | CPUUtilization*<br><br>>= インスタンスがポーリング Systems Manager コマンドに 응답しない場合、5 分間 6 回連続して 95%。         | CloudWatch アラーム。CPU 使用率が高いことは、デッドロック、無限ループ、悪意のある攻撃、その他の異常など、アプリケーションの状態の変化を示す指標です。 |
|                  |            | StatusCheckFailed<br><br>> 0 を 5 分間、連続 3 回。                                                    | CloudWatch アラーム。                                                                   |
|                  |            | ルートボリュームの使用<br><br>>= 5 分間 95%、連続 6 回。                                                         |                                                                                    |

| サービス                      | セキュリティアラート | アラート名とトリガー条件                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 注意事項                                   |
|---------------------------|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|
|                           |            | <p>非ルートボリュームの使用</p> <p>&gt; 5 分間 85%、2 回連続。</p> <p>デフォルトでは無効になっています。詳細については、「」を参照してください<a href="https://docs.aws.amazon.com/managedservices/latest/ctref/management-monitoring-cloudwatch-enable-non-root-volumes-monitoring.html#management-monitoring-cloudwatch-enable-non-root-volumes-monitoring-info">https://docs.aws.amazon.com/managedservices/latest/ctref/management-monitoring-cloudwatch-enable-non-root-volumes-monitoring.html#management-monitoring-cloudwatch-enable-non-root-volumes-monitoring-info</a>。</p> |                                        |
|                           |            | <p>メモリ無料*</p> <p>MemoryFree &lt; 5%、5 分間、6 回連続。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                        |
|                           | はい         | <p>EPS マルウェア</p> <p>インスタンスでマルウェアが見つかりました。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | CloudWatch イベント。                       |
| Amazon EC2 インスタンス - Linux | いいえ        | <p>ルートボリューム Inode の使用</p> <p>平均 &gt;= 5 分間 95%、連続 6 回。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | CloudWatch アラーム。Linux インスタンスにのみ適用されます。 |

| サービス              | セキュリティアラート | アラート名とトリガー条件                | 注意事項                                                                                                          |
|-------------------|------------|-----------------------------|---------------------------------------------------------------------------------------------------------------|
|                   |            | スワップ無料*                     |                                                                                                               |
|                   |            | メモリスワップ < 5% を 5 分間、連続 6 回。 |                                                                                                               |
| ElastiCache クラスター | いいえ        | CurrConnections = 65000     | <p>このアラームは、ElastiCache ホストの最大接続制限を AMS に通知します。</p> <p>CloudWatch アラーム。このしきい値を更新する場合は、AMS サポートにお問い合わせください。</p> |

| サービス            | セキュリティアラート | アラート名とトリガー条件                                          | 注意事項                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------|------------|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ElastiCache ノード | いいえ        | CPUUtilization<br><br>Average > 15 分間の事前定義された値、2 回連続。 | CloudWatch アラーム。デフォルトは 90 です。Redis の場合は、インスタンスタイプに基づいて次のいずれかの値を使用します。 <ul style="list-style-type: none"><li>• cache.t1.micro: 90%</li><li>• cache.m1.small: 90%</li><li>• cache.m1.medium: 90%</li><li>• cache.m1.large: 45%</li><li>• cache.m1.xlarge: 22.5%</li><li>• cache.m2.xlarge: 45%</li><li>• cache.m2.4xlarge: 11.25%</li><li>• cache.c1.xlarge: 11.25%</li><li>• cache.t2.micro: 90%</li><li>• cache.t2.small: 90%</li><li>• cache.t2.medium: 45%</li><li>• cache.m3.medium: 90%</li><li>• cache.m3.large: 45%</li><li>• cache.m3.xlarge: 22.5%</li><li>• cache.m3.2xlarge: 11.25%</li><li>• cache.r3.large: 45%</li><li>• cache.r3.xlarge: 22.5%</li><li>• cache.r3.2xlarge: 11.25%</li><li>• cache.r3.4xlarge: 5.625%</li></ul> |

| サービス                         | セキュリティアラート | アラート名とトリガー条件                                                                                                               | 注意事項                                                                                                                                                                  |
|------------------------------|------------|----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                              |            |                                                                                                                            | <ul style="list-style-type: none"> <li>• cache.r3.8xlarge: 2.8125%</li> </ul>                                                                                         |
| ElasticCache ノード - memcached | いいえ        | SwapUsage<br><br>最大 > 50,000,000 バイト、5 分間、5 回連続。                                                                           | CloudWatch アラーム。memcached にのみ適用されます。                                                                                                                                  |
| OpenSearch クラスター             | いいえ        | ClusterStatus.red<br><br>maximum は $\geq 1$ で 1 分間、連続 1 回です。<br><br>AMS は、このアラートがトリガーされたときに、運用への影響を軽減するために積極的なアクションを実行します。 | CloudWatch アラーム。少なくとも 1 つのプライマリシャードとそのレプリカがノードに割り当てられていません。詳細については、 <a href="#">「Red Cluster Status」</a> を参照してください。                                                   |
| OpenSearch ドメイン              | いいえ        | KMSKeyError<br><br>$\geq 1$ を 1 分間、連続 1 回。                                                                                 | CloudWatch アラーム。ドメインに保存されているデータを暗号化する KMS 暗号化キーが無効になっています。通常のオペレーションを復元するために、再度有効にしてください。詳細については、 <a href="#">OpenSearch Service Service の保管中のデータの暗号化</a> 」を参照してください。 |

| サービス | セキュリティアラート | アラート名とトリガー条件                                                                                                                           | 注意事項                                                                                              |
|------|------------|----------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
|      |            | <p>ClusterStatus.yellow</p> <p>最大は <math>\geq 1</math> で 1 分間、連続 1 回</p> <p>AMS は、このアラートがトリガーされたときに、運用への影響を軽減するために積極的なアクションを実行します。</p> | <p>少なくとも 1 つのレプリカシャードがノードに割り当てられていません。詳細については、<a href="#">「黄色のクラスターステータス」</a>を参照してください。</p>       |
|      |            | <p>FreeStorageSpace</p> <p>最小は <math>\leq 20480</math> で 1 分間、連続 1 回</p> <p>AMS は、このアラートがトリガーされたときに、運用への影響を軽減するために積極的なアクションを実行します。</p> | <p>クラスターのノードの空きストレージ容量が 20 GiB に下がっています。詳細については、<a href="#">「使用可能なストレージスペースがない」</a>を参照してください。</p> |
|      |            | <p>ClusterIndexWritesBlocked</p> <p><math>\geq 1</math> を 5 分間、1 回連続</p> <p>AMS は、このアラートがトリガーされたときに、運用への影響を軽減するために積極的なアクションを実行します。</p> | <p>クラスターが書き込みリクエストをブロックしています。詳細については、<a href="#">「ClusterB lockException」</a>を参照してください。</p>       |

| サービス | セキュリティ<br>アラート | アラート名とトリガー条件                                                                                                                        | 注意事項                                                                                                                                          |
|------|----------------|-------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
|      |                | <p>ノード</p> <p>最小は <math>&lt; x</math> で 1 日、連続 1 回</p> <p>AMS は、このアラートがトリガーされたときに、運用への影響を軽減するために積極的なアクションを実行します。</p>                | <p><math>x</math> はクラスター内のノード数です。このアラームは、クラスター内の少なくとも 1 つのノードが 1 日間にわたってアクセスできない状態を意味します。詳細については、<a href="#">「失敗したクラスターノード」</a>を参照してください。</p> |
|      |                | <p>CPUUtilization</p> <p>平均は 15 分間で <math>\geq 80\%</math>、連続 3 回</p> <p>AMS は、このアラートがトリガーされたときに、運用への影響を軽減するために積極的なアクションを実行します。</p> | <p>100% の CPU 使用率が一般的ですが、持続的な高い平均は問題です。より大規模なインスタンスタイプを使用するか、インスタンスを追加することを検討してください。</p>                                                      |



| サービス | セキュリティアラート | アラート名とトリガー条件                                                                                                                              | 注意事項                                                                                                                                                                                                 |
|------|------------|-------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |            | <p>JVMMemoryPressure</p> <p>最大は <math>\geq 80\%</math> で 5 分間、3 回連続</p> <p>AMS は、このアラートがトリガーされたときに、運用への影響を軽減するために積極的なアクションを実行します。</p>     | <p>使用量が増加した場合にクラスターでメモリ不足エラーが発生する可能性があります。垂直スケーリングを検討してください。Amazon ES は、Java ヒープにインスタンスの RAM の半分を使用し、ヒープサイズは 32 GiB までです。インスタンスは最大 64 GiB の RAM まで垂直スケーリングでき、それ以上はインスタンスを追加することで水平方向にスケーリングできます。</p> |
|      |            | <p>MasterCPUUtilization</p> <p>平均は 15 分間で <math>\geq 50\%</math>、連続 3 回</p> <p>AMS は、このアラートがトリガーされたときに、運用への影響を軽減するために積極的なアクションを実行します。</p> | <p><a href="#">専用マスターノード</a>には、より大きなインスタンスタイプを使用することを検討してください。クラスターの安定性と<a href="#">ブルー/グリーンデプロイ</a>における役割により、専用マスターノードの平均 CPU 使用率はデータノードよりも低くなります。</p>                                              |

| サービス                          | セキュリティアラート | アラート名とトリガー条件                                                                                                                                   | 注意事項                                                                                                                                                    |
|-------------------------------|------------|------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
|                               |            | <p>MasterJVMMemoryPressure</p> <p>最大は <math>\geq 80\%</math> で 15 分間、1 回連続</p> <p>AMS は、このアラートがトリガーされたときに、運用への影響を軽減するために積極的なアクションを実行します。</p>   | <p><a href="#">専用マスターノード</a>には、より大きなインスタンスタイプを使用することを検討してください。クラスターの安定性と<a href="#">ブルー/グリーンデプロイ</a>における役割により、専用マスターノードの平均 CPU 使用率はデータノードよりも低くなります。</p> |
| OpenSearch インスタンス             | いいえ        | <p>AutomatedSnapshotFailure</p> <p>maximum は <math>\geq 1</math> で 1 分間、連続 1 回です。</p>                                                          | <p>CloudWatch アラーム。自動スナップショットが失敗しました。多くの場合、この失敗によってクラスター状態が赤になります。<a href="#">「赤クラスターのステータス」</a>を参照してください。</p>                                          |
| Elastic Load Balancing インスタンス | いいえ        | <p>SurgeQueueLength</p> <p><math>&gt; 100</math> を 1 分間、15 回連続。</p> <p>HTTPCode_ELB_5XX_Count</p> <p>合計 <math>&gt; 0</math> を 5 分間、連続 3 回。</p> | <p>過剰な数のリクエストがルーティングを保留している場合、CloudWatch アラームが発生します。</p> <p>ロードバランサーから送信される HTTP 5XX レスポンスコードの過剰数に関する CloudWatch アラーム。</p>                              |

| サービス           | セキュリティアラート | アラート名とトリガー条件                                                                                                                    | 注意事項                                                                                                                                                                             |
|----------------|------------|---------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                |            | <p>SpilloverCount</p> <p>&gt; 1 を 1 分間、連続 15 回。</p>                                                                             | <p>サージキューがいっぱいであるために拒否されたリクエストの数が過剰である場合、CloudWatch アラームが発生します。</p>                                                                                                              |
| GuardDuty サービス | はい         | <p>該当なし。すべての検出結果 (脅威の目的) がモニタリングされます。各検出結果はアラートに対応します。</p> <p>GuardDuty の検出結果の変更。このような変更には新しく生成された結果や、既存の結果の後続のすべての発生を含みます。</p> | <p>サポートされている GuardDuty 検出結果タイプのリストは、<a href="#">GuardDuty アクティブ検出結果タイプ</a>にあります。</p>                                                                                             |
| 健康             | 可変         | AWS Health Dashboard                                                                                                            | <p>通知は、AMS オペレーションからのアクションを必要とする AMS でサポートされているベースラインサービスに関連して AWS Health Dashboard、(AWS Health) イベントのステータスに変更されたときに送信されます。詳細については、「<a href="#">サポートされているサービス</a>」を参照してください。</p> |

| サービス                     | セキュリティアラート | アラート名とトリガー条件                                                                          | 注意事項                                                                                               |
|--------------------------|------------|---------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| AWS Managed Microsoft AD | いいえ        | Active Directory のステータス<br><br>AWS Managed Microsoft AD インスタンスはアクティブなステータスイベントを送信します。 | サービスイベント。イベント後にディレクトリが正常に動作している場合に出力されます。                                                          |
|                          |            | ディレクトリステータスの障害<br><br>AWS Managed Microsoft AD インスタンスは障害のあるディレクトリステータスイベントを送信します。     | サービスイベント。ディレクトリがパフォーマンス低下状態で実行されている場合に出力されます。1 つまたは複数の問題が検出され、すべてのディレクトリのオペレーションが最適に動作しているとは限りません。 |
|                          |            | 操作できないディレクトリのステータス<br><br>AWS Managed Microsoft AD インスタンスは、動作不能なステータスイベントを送信します。      | サービスイベント。ディレクトリが機能していない場合に発行されます。すべてのディレクトリエンドポイントが問題を報告しています。                                     |
|                          |            | ディレクトリステータスの削除<br><br>AWS Managed Microsoft AD インスタンスは、ディレクトリステータスの削除イベントを送信します。      | サービスイベント。ディレクトリが現在削除されているときに発行されます。                                                                |

| サービス              | セキュリティアラート | アラート名とトリガー条件                                                                                      | 注意事項                                                                       |
|-------------------|------------|---------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
|                   |            | 失敗したディレクトリのステータス<br><br>AWS Managed Microsoft AD インスタンスは失敗したステータスイベントを送信します。                      | サービスイベント。ディレクトリを作成できなかったときに出力されます。                                         |
|                   |            | RestoreFailed ディレクトリのステータス<br><br>AWS Managed Microsoft AD インスタンスは、復元に失敗したディレクトリステータスイベントを送信します。  | サービスイベント。スナップショットからディレクトリを復元できませんでした。                                      |
| Amazon RDS インスタンス | いいえ        | DB インスタンスに割り当てられたストレージが使い果たされると、低ストレージアラートがトリガーされます。                                              | RDS-EVENT-0007 の詳細については、 <a href="#">「Amazon RDS イベント通知の使用」</a> を参照してください。 |
|                   |            | DB インスタンスが失敗する<br><br>DB インスタンスは、互換性のない設定または基本的なストレージの問題により失敗しました。DB インスタンスのポイントインタイムの復元をスタートします。 | サービスイベント。RDS-EVENT-0031、 <a href="#">Amazon RDS イベントカテゴリとイベントメッセージ</a> 。   |

| サービス | セキュリティアラート | アラート名とトリガー条件                                                                                                                 | 注意事項                                                                          |
|------|------------|------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
|      |            | フェイルオーバーが試行されない<br><br>Amazon RDS はリクエストされたフェイルオーバーを実行できません。これは、DB インスタンスでフェイルオーバーが最近発生したためです。                               | サービスイベント。RDS-EVENT-0034、 <a href="#">Amazon RDS イベントカテゴリとイベントメッセージ</a> 。<br>。 |
|      |            | DB インスタンスの無効なパラメータ<br><br>たとえば、このインスタンスクラスでメモリ関連のパラメータが高すぎるため、MySQL を起動できなかったため、お客様のアクションはメモリパラメータを変更して DB インスタンスを再起動することです。 | サービスイベント。RDS-EVENT-0035、 <a href="#">Amazon RDS イベントカテゴリとイベントメッセージ</a> 。<br>。 |
|      |            | 無効なサブネット IDs インスタンス<br><br>DB インスタンスが互換性のないネットワーク上にあります。指定したサブネット ID の一部は無効であるか、存在しません。                                      | サービスイベント。RDS-EVENT-0036、 <a href="#">Amazon RDS イベントカテゴリとイベントメッセージ</a> 。<br>。 |

| サービス | セキュリティアラート | アラート名とトリガー条件                                                                                                                                                                 | 注意事項                                                                          |
|------|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
|      |            | <p>DB インスタンスのリードレプリカエラー</p> <p>リードレプリケーションプロセスでエラーが発生しました。詳細については、イベントメッセージを参照してください。リードレプリカエラーのトラブルシューティングについては、<a href="#">MySQL リードレプリカの問題のトラブルシューティング</a>」を参照してください。</p> | <p>サービスイベント。RDS-EVENT-0045、<a href="#">Amazon RDS イベントカテゴリとイベントメッセージ</a>。</p> |
|      |            | <p>DB インスタンスの読み取りレプリケーションが終了しました</p> <p>リードレプリカのレプリケーションが終了しました。</p>                                                                                                         | <p>サービスイベント。RDS-EVENT-0057、<a href="#">Amazon RDS イベントカテゴリとイベントメッセージ</a>。</p> |
|      |            | <p>statspack ユーザーアカウントの作成中にエラーが発生しました</p> <p>Statspack ユーザーアカウント PERFSTAT の作成中にエラーが発生しました。Statspack オプションを追加する前に、アカウントを削除します。</p>                                            | <p>サービスイベント。RDS-EVENT-0058、<a href="#">Amazon RDS イベントカテゴリとイベントメッセージ</a>。</p> |

| サービス | セキュリティアラート | アラート名とトリガー条件                                                                                                                                                                                  | 注意事項                                                                                |
|------|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
|      |            | DB インスタンス復旧の開始<br><br>SQL Server DB インスタンスは、ミラーを再構築しています。ミラーが再構築されるまで、パフォーマンスが低下します。FULL ではない復旧モデルのデータベースが見つかりました。復旧モデルが FULL に戻され、ミラーリング復旧が開始されました (<dbname>: <recovery model found>[,...])。 | サービスイベント。RDS-EVENT-0066、 <a href="#">Amazon RDS イベントカテゴリとイベントメッセージ</a> 。<br>。       |
|      |            | DB クラスターのフェイルオーバーが失敗しました。                                                                                                                                                                     | RDS-EVENT-0069 の詳細については、「 <a href="#">Amazon RDS イベントカテゴリとイベントメッセージ</a> 」を参照してください。 |
|      |            | 無効なアクセス許可復旧 S3 バケット<br><br>Amazon S3 バケットにアクセスして SQL Server のネイティブバックアップと復元を行うための IAM ロールが正しく設定されていません。詳細については、「 <a href="#">ネイティブバックアップと復元のセットアップ</a> 」を参照してください。                            | サービスイベント。RDS-EVENT-0081、 <a href="#">Amazon RDS イベントカテゴリとイベントメッセージ</a> 。<br>。       |



| サービス | セキュリティアラート | アラート名とトリガー条件                                                                        | 注意事項                                                                                |
|------|------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
|      |            | Aurora は、Amazon S3 バケットからバックアップデータをコピーできませんでした。                                     | RDS-EVENT-0082 の詳細については、 <a href="#">「Amazon RDS イベントカテゴリとイベントメッセージ」</a> を参照してください。 |
|      |            | DB インスタンスが割り当てられたストレージの 90% 以上を消費した場合の低ストレージアラート                                    | RDS-EVENT-0089 の詳細については、 <a href="#">「Amazon RDS イベントカテゴリとイベントメッセージ」</a> を参照してください。 |
|      |            | Aurora Serverless DB クラスターのスケールリングが失敗したときの通知サービス。                                   | RDS-EVENT-0143 の詳細については、 <a href="#">「Amazon RDS イベントカテゴリとイベントメッセージ」</a> を参照してください。 |
|      |            | DB インスタンスは無効な状態です。操作は必要ありません。オートスケールリングは後で再試行されます。                                  | RDS-EVENT-0219 の詳細については、 <a href="#">「Amazon RDS イベントカテゴリとイベントメッセージ」</a> を参照してください。 |
|      |            | DB インスタンスがストレージフルのしきい値に達し、データベースがシャットダウンされました。                                      | RDS-EVENT-0221 の詳細については、 <a href="#">「Amazon RDS イベントカテゴリとイベントメッセージ」</a> を参照してください。 |
|      |            | このイベントは、RDS インスタンスストレージの自動スケールリングがスケールリングできないことを示します。自動スケールリングが失敗した理由は複数ある可能性があります。 | RDS-EVENT-0223 の詳細については、 <a href="#">「Amazon RDS イベントカテゴリとイベントメッセージ」</a> を参照してください。 |

| サービス | セキュリティアラート | アラート名とトリガー条件                                                       | 注意事項                                                                                |
|------|------------|--------------------------------------------------------------------|-------------------------------------------------------------------------------------|
|      |            | ストレージのオートスケーリングにより、保留中のスケールストレージタスクの最大ストレージしきい値到達がトリガーされました。       | RDS-EVENT-0224 の詳細については、 <a href="#">「Amazon RDS イベントカテゴリとイベントメッセージ」</a> を参照してください。 |
|      |            | DB インスタンスのストレージタイプが、アベイラビリティゾーンで現在使用できないタイプです。オートスケーリングは後で再試行されます。 | RDS-EVENT-0237 の詳細については、 <a href="#">「Amazon RDS イベントカテゴリとイベントメッセージ」</a> を参照してください。 |
|      |            | サブネットに十分な IP アドレスがないため、RDS はプロキシの容量をプロビジョニングできませんでした。              | RDS-EVENT-0243 の詳細については、 <a href="#">「Amazon RDS イベントカテゴリとイベントメッセージ」</a> を参照してください。 |
|      |            | AWS アカウントのストレージが、許可されたストレージクォータを超えています。                            | RDS-EVENT-0254 の詳細については、 <a href="#">「Amazon RDS イベントカテゴリとイベントメッセージ」</a> を参照してください。 |
|      |            | CPUUtilization<br><br>平均 CPU 使用率 > 90%、15 分間、2 回連続。                | CloudWatch アラーム。                                                                    |
|      |            | DiskQueueDepth<br><br>合計は 1 分間 > 75 で、連続して 15 回です。                 |                                                                                     |

| サービス                  | セキュリティアラート | アラート名とトリガー条件                                                                                                                       | 注意事項                                                                                                                                       |
|-----------------------|------------|------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
|                       |            | <p>FreeStorageSpace</p> <p>平均 &lt; 1,073,741,824 バイト、5 分間、2 回連続。</p> <p>SwapUsage</p> <p>平均 &gt;= 5 分間 104,857,600 バイト、連続 2 回。</p> |                                                                                                                                            |
| Amazon Redshift クラスター | いいえ        | <p>RedshiftClusterStatus</p> <p>メンテナンスモードでない場合のクラスターの状態 &lt; 1 を 5 分間。</p>                                                         | 1 は正常なクラスターを表します。                                                                                                                          |
| Amazon Macie          | はい         | <p>新しく生成されたアラートと既存のアラートの更新。</p> <p>Macie は検出結果の変更を検出します。このような変更には新しく生成された結果や、既存の結果の後続のすべての発生を含みます。</p>                             | Amazon Macie アラート。サポートされている Macie アラートタイプのリストについては、 <a href="#">Amazon Macie の検出結果の分析</a> を参照してください。Macie はすべてのアカウントで有効になっていないことに注意してください。 |

AMS は、このアラートがトリガーされたときにプロアクティブアクションを実行 (クラスターのスケーリング) します。

修復作業の詳細については、「」を参照してください[アラートの AMS 自動修復](#)。

[詳細については、Andrew の動画をご覧ください \(7:03\)](#)

## ログの保持とローテーションのデフォルト

このセクションでは、AMS ログ管理のデフォルトについて説明します。詳細については、[「ログ管理」](#)を参照してください。

- ローテーション = インスタンス内のログターンオーバー
- 保持期間 = Amazon CloudWatch Logs と Amazon Simple Storage Service (S3) にログを保持する期間

ログは、必要に応じて CloudWatch Logs および S3 に保持されます (これを設定できます)。有効期限が切れたり削除されたりすることなく、サービスの耐久性の対象となります。S3 の耐久性の詳細については、[Amazon S3でのデータ保護](#)を参照してください。

監査およびセキュリティ上の理由から 10 年間保持されるログを除き、すべての AWS CloudTrail ログのログ保持の変更をリクエストできます。

ログローテーションはインスタンス内で設定されます。デフォルトでは、オペレーティングシステムとセキュリティログが 100MB を超える場合、1 時間ごとにローテーションされます。これは、インスタンスのディスクでショートが発生しないようにするためです。

インスタンス内のログエージェントは、ログをオンラインで CloudWatch Logs にアップロードし、そこからログが S3 にアーカイブされます。

ログは、生成された raw 形式で CloudWatch Logs と S3 に保存されます。前処理はありません。

## AMS コンソールの使用

AWS マネジメントコンソールの AMS コンソールを使用して、AMS を操作し、AMS Advanced マネージドリソースと AMS Accelerate リソースを運用できます。AMS コンソールは通常、どの AWS コンソールと同じように動作しますが、AMS はプライベート組織であるため、AMS が有効になっているアカウントのみがコンソールにアクセスできます。アカウントで AMS を有効にすると、統合検索バーで「マネージドサービス」を検索してコンソールにアクセスできます。

### Note

アカウントロールに応じて、AMS Advanced コンソールまたは AMS Accelerate コンソールにアクセスします。

AMS コンソールを使用する場合は、次の点に注意してください。

- AMS コンソールはアカウント固有です。したがって、組織の「テスト」アカウントを使用している場合、その組織の「Prod」アカウントでリソースを表示することはできません。同様に、AMS Advanced コンソールにアクセスするには、AMS Advanced ロールが必要です。
- AMS コンソールは、認証時に IAM ポリシーを適用し、アクセスできるコンソールとそこで実行できる操作を決定します。管理者は、デフォルトの AMS ポリシーに追加のポリシーを適用して、コンソールで表示および実行できる操作を制限できます。

AMS Advanced コンソールには以下の機能があります。

- 開始ページ: 開始ページには、既存の RFCs インシデント、サービスリクエスト、レポートへのアクセスを容易にするための情報ボックスとリンクがあります。
- 機能ページ、左側のナビゲーションペインのリンク:
  - ダッシュボード: アカウントの現在のステータスの概要を示します。
    - 変更のリクエスト: レスポンスを待っている RFCs の数を確認し、そのフィルターがアクティブな RFC リストページにジャンプします。承認を待っている RFCs の数を確認し、そのフィルターがアクティブな RFC リストページにジャンプします。開いている RFCs の数を確認し、そのフィルターがアクティブな RFC リストページにジャンプします。すべての表示リンクをクリックして、RFCs のリストページを開きます。
  - インシデント: 対応を待っているインシデントケースの数を確認し、そのフィルターがアクティブなインシデントリストページにジャンプします。「」と「開いている」の数を確認し、そのフィルターがアクティブなインシデントリストページにジャンプします。すべての表示リンクをクリックして、インシデントリストページを開きます。
  - サービスリクエスト: レスポンスを待っているサービスリクエストの数を確認し、そのフィルターがアクティブなサービスリクエストリストページにジャンプします。「」と「開いているの数」を参照し、そのフィルターがアクティブなサービスリクエストリストページにジャンプします。すべての表示リンクをクリックして、サービスリクエストリストページを開きます。
- 最近更新された RFCs: 日付、RFC の詳細へのリンク、ステータス
- 最近作成されたインシデントとサービスリクエスト: 日付、ケースの詳細へのリンク、タイプ (インシデントまたはサービスリクエスト)
- RFCs: アカウントの既存の RFCs のリストを開きます
- Incidents: アカウントのオープンインシデントのリストを開きます。
- サービスリクエスト: アカウントのオープンサービスリクエストのリストを開きます。

- レポート: レポートページとデフォルトレポート、日次バックアップと日次パッチ、毎月の請求を開きます
- リソース:
  - VPCs: アカウントの既存の VPCs のリストを開きます
  - スタック: アカウントの既存のスタックのリストを開きます
  - AMIs: 使用可能な AMS AMIs
- 機能のスポットライト: コンソールの最新の更新に関する情報
- 開発者のリソース: AMS Advanced 変更管理 SDK などを含むダウンロード可能なファイルのページ
- ドキュメント: AWS Managed Services ドキュメントのランディングページ

## AMS API と CLI の使用

AWS Managed Services (AMS) API は、他の AWS サービスの APIs と似ています。AMS API については、「[AMS API リファレンス](#)」を参照してください。

### REST コール用の AMS API HTTP エンドポイント

さまざまな SDKs に加えて、AMS は CLI を提供します。AMS エンドポイントに対して REST API コールを呼び出すこともできます。

2 つの AMS APIs があります (両方のエンドポイントは us-east-1 にあります)。

- 変更管理: この API を使用して、RFCs の作成と更新、新しいインスタンスのデプロイ、インスタンスの更新と削除、CTs に関する情報の取得、AMIs の作成など、インフラストラクチャへのアクセスまたは変更をリクエストします。HTTP エンドポイントは次のとおりです。

`https://amscm.us-east-1.amazonaws.com`

- SKMS: この API を使用して、VPCs、スタック、サブネット、AMIs などのインフラストラクチャに関する情報を取得します。HTTP エンドポイントは次のとおりです。

`https://amsskms.us-east-1.amazonaws.com`

## AMS CLI のインストールまたはアップグレード

AMS CLI は AMS API を操作する簡単な方法であり、このセクションの例で使います。CLI および AMS AWS CLI の使用規則については、[AWS 「コマンドラインインターフェイスの使用」](#)を参照してください。

SAML のインストールについては、「」を参照してください[AD FS クレームルールと SAML 設定](#)。

AMS CLI をインストールまたはアップグレードするには、次の手順に従います。

### Note

この手順には管理者認証情報が必要です。

AWS CLI は、AWS Managed Services (AMS) CLIs (変更管理と SKMS) を使用するための前提条件です。

1. AWS CLI をインストールするには、[「AWS コマンドラインインターフェイスのインストール」](#)を参照して、適切な手順に従ってください。このページの下部には、さまざまなインストーラー、[Linux](#)、[MS Windows](#)、[macOS](#)、[仮想環境](#)、[バンドルインストーラー \(Linux、macOS、または Unix\)](#) を使用する手順があることに注意してください。

インストール後、`aws help`を実行してインストールを確認します。

2. AWS CLI がインストールされたら、AMS CLI をインストールまたはアップグレードするには、AMS AMS CLI または AMS SDK 配布用 zip ファイルをダウンロードして解凍します。AMS CLI ディストリビューションには、AMS コンソールの左ナビゲーションにある[デベロッパーのリソース](#)リンクからアクセスできます。
3. README ファイルには、インストールの手順が記載されています。

次のいずれかを開きます。

- CLI zip: AMS CLI のみを提供します。
- SDK zip: すべての AMS APIs と AMS CLI を提供します。

Windows の場合は、適切なインストーラ (32 ビットまたは 64 ビットシステムのみ) を実行します。

- 32 ビット: ManagedCloudAPI\_x86.msi

- 64 ビット: ManagedCloudAPI\_x64.msi

Mac/Linux の場合は、次のコマンドを実行して AWSManagedServices\_InstallCLI.sh という名前のファイルを実行します。sh AWSManagedServices\_InstallCLI.shamscm および amsskms ディレクトリとそのコンテンツは、AWSManagedServices\_InstallCLI.sh ファイルと同じディレクトリにある必要があります。

4. 企業の認証情報を AWS とのフェデレーション (AMS デフォルト設定) で使用する場合は、フェデレーションサービスにアクセスできる認証情報管理ツールをインストールする必要があります。例えば、この AWS セキュリティブログ [How to Implement Federated API and CLI Access Using SAML 2.0 and AD FS](#) を使用して、認証情報管理ツールの設定に役立てることができます。
5. インストール後、aws amscm help と aws amsskms help を実行してコマンドとオプションを表示します。

#### Note

これらのコマンドを機能させるには、AMS CLI をインストールする必要があります。AMS API または CLI をインストールするには、AMS コンソールのデベロッパーリソースページに移動します。AMS CM API または AMS SKMS API のリファレンスマテリアルについては、「ユーザーガイド」の「AMS 情報リソース」セクションを参照してください。認証--profileのオプションを追加する必要がある場合があります。例: aws amsskms *ams-cli-command* --profile SAML。また、など、すべての AMS コマンドが us-east-1 を使い果たすため、--regionオプションを追加する必要がある場合がありますaws amscm *ams-cli-command* --region=us-east-1。

## CLI、Ruby、Python、Java での AMS API の使用

以下は、利用可能なすべての言語での AMS API ListChangeTypeClassificationSummariesオペレーションのコードスニペットのリストです。

Python、Ruby、Java SDKs [「Amazon Web Services のツール」SDKs](#) セクションまでスクロールします。各 SDK インストーラには、追加のコードスニペットを含む README が含まれています。



## AMS API から CLI への例

AMS CLI をインストールしたら (CLI AWS が必要。「」を参照[AMS CLI のインストールまたはアップグレード](#))、まずどの AMS API `aws amscm` または `aws amsskms` を指定して呼び出しを変更し、キャメルケースを置き換えるハイフンでアクションを指定することで `aws amsskms`、任意の AMS API オペレーションを実行できます。最後に、SAML などの認証情報を指定します。

詳細については、[AWS 「コマンドラインインターフェイスの使用」](#) を参照してください。

例:

- API: `'ChangeTypeClassificationSummaries[]`.  
`[Category,Subcategory,Item,Operation,ChangeTypeId]'`
- CLI: `amscm list-change-type-classification-summaries`  
`--query "ChangeTypeClassificationSummaries[*]`.  
`[Category,Subcategory,Item,Operation,ChangeTypeId]" --output table`

### Note

SAML で認証する場合は、コマンドの先頭 `aws --profile saml` にを追加します。例えば、などです

```
aws --profile saml amscm list-change-type-classification-  
summaries --query "ChangeTypeClassificationSummaries[*].  
[Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
```

## AMS API から Python へのサンプル

Python で AMS API を使用するには、AMS CLI をインストールし、`boto3` をインストールします。以下の手順に従ってください。

- AMS CLI をインストールします。「[AMS CLI のインストールまたはアップグレード](#)」を参照してください。
- AWS SDK for Python である `boto3` をインストールします。詳細については、このブログ記事「[Now Available – AWS SDK for Python \(Boto3\)](#)」を参照してください。

```
import boto3
```

### 3. AMS 変更管理クライアントを取得します。

```
cm = boto3.client('amscm')
```

### 4. AMS CTsを取得します。

```
cts = cm.list_change_type_classification_summaries()

print(cts)
```

## Python の例

以下は、AMS での Python の使用、EC2 インスタンスの作成、Lambda の使用の例です。

### EC2 を作成する Python の例

この例では、Python コード内から amscm RESTful API を使用して、RFC プロセスをファイルして実行する方法を示します。

1. アクセスできる場所に AMS CLI をインストールします。用意されているファイルが必要です。
2. Python ライブラリを呼び出し、EC2 インスタンスを作成します。

```
import boto3
import json
import time

# Create the amscm client
cm = boto3.client('amscm')

# Define the execution parameters for EC2 Create
AMSExecParams = {
    "Description": "EC2-Create",
    "VpcId": "VPC_ID",
    "Name": "My-EC2",
    "TimeoutInMinutes": 60,
    "Parameters": {
        "InstanceAmiId": "INSTANCE_ID",
        "InstanceSubnetId": "SUBNET_ID"
    }
}

# Create the AMS RFC
```

```
cts = cm.create_rfc(
    ChangeTypeId="ct-14027q0sjyt1h",
    ChangeTypeVersion="3.0",
    Title="Python Code RFC Create",
    ExecutionParameters=json.dumps(AMSExecParams)
)

# Extract the RFC ID from the response
NewRfcID = cts['RfcId']

# Submit the RFC
RFC_Submit_Return=cm.submit_rfc(RfcId=NewRfcID)

# Check the RFC status every 30 seconds
RFC_Status = cm.get_rfc(RfcId=NewRfcID)
RFC_Status_Code = RFC_Status['Rfc']['Status']['Name']

while RFC_Status_Code != "Success":
    if RFC_Status_Code == "PendingApproval":
        print(RFC_Status_Code)
        time.sleep(30)
    elif RFC_Status_Code == "InProgress":
        print(RFC_Status_Code)
        time.sleep(30)
    elif RFC_Status_Code == "Failure":
        print(RFC_Status_Code)
        break
    else:
        print(RFC_Status_Code)

RFC_Status = cm.get_rfc(RfcId=NewRfcID)
RFC_Status_Code = RFC_Status['Rfc']['Status']['Name']
```

## Lambda を使用した Python の例

この例では、AMS モデルをコードにバンドルして、Lambda または EC2 で使用する方法を示します。インストールできない、またはインストールできない場所です `amsccli`。

 Note

AMS は、インポート可能な AMS 固有の Python SDK を提供しません。amsccli インストールスクリプトは、CLI の通常のパスに AMS サービスデータモデルをインストールします。CLI の使用とシステム Python の使用については、amsccli との両方が同じデフォルトの場所 ( ) からサービスモデル boto3 を読み取るため、問題ありません。~/.aws/models。ただし、Lambda (または他のローカル以外のランタイム) で boto3 経由で AMS サービスを使用する場合、データモデルがなくなったため、中断します。データモデルを関数でパッケージ化して、これを修正する方法を次に示します。

Lambda または EC2、Fargate などの別のランタイムで AMS 統合 Python コードを実行するための簡単な手順があります。次のワークフローは、AMS 統合 Lambda 関数に必要なステップを示しています。

データモデルをコードのデプロイパッケージに追加し、SDK 検索パスを更新することで、SDK エクスperiエンスをシミュレートできます。

 Important

この例と表示されているすべての非 Python コマンドは、Mac コンピュータでテストされています。

ワークフローの例：

1. amsccli をインストールします。これにより、コンピュータ (Mac) の ~/.aws/models にフォルダが作成されます。
2. モデルをローカルディレクトリにコピーします `cp ~/.aws/models ./models`。
3. モデルをコードのデプロイパッケージに含めます。
4. 関数コードを更新して、SDK パスに新しいモデルを追加します。このコードは、boto3 または botocore をインポートする前に実行する必要があることに注意してください。

```
# Force Python to search local directory for boto3 data models
import os
os.environ['AWS_DATA_PATH'] = './models'
```

```
import boto3
import botocore
```

#### Note

サンプルモデルは という名前のディレクトリにあるためmodels、AWS\_DATA\_PATH ./modelsに を追加します。ディレクトリの名前が の場合/ams/boto3models、次のコードを追加します。

```
import os.environ['AWS_DATA_PATH'] = './ams/boto3models'

import boto3
import botocore
```

コードは AMS モデルを正常に見つける必要があります。パッケージングに関するより具体的な例として、Lambda 固有のワークフローを次に示します。

AMS Lambda ワークフローの例：

これらのステップは、前述の一般的な例を AWS Lambda 関数の作成に適用します。

1. amscli をインストールします。これにより、コンピュータ (Mac) の ~/.aws/models にフォルダが作成されます。
2. モデルをローカルディレクトリにコピーします。

```
cp ~/.aws/models ./models
```

3. モデルを関数のデプロイ zip ファイルに追加します。

```
zip -r9 function.zip ./models
```

#### Important

関数コードを更新して、SDK パスに新しいモデルを追加します。このコードは、boto3 または botocore をインポートする前に実行する必要があることに注意してください。

```
# Force Python to search local directory for boto3 data models
import os
os.environ['AWS_DATA_PATH'] = './models'

import boto3
import botocore
```

#### Note

サンプルモデルは という名前のディレクトリにあるためmodels、AWS\_DATA\_PATH ./modelsに を追加します。ディレクトリの名前が の場合/ams/boto3models、次のコードを追加します。

```
import os
os.environ['AWS_DATA_PATH'] = './ams/boto3models'

import boto3
import botocore
```

次に、関数をデプロイします。

1. 関数コードをデプロイ zip ファイルに追加します (まだ追加していない場合 )。

```
zip -g function.zip lambda-amscm-test.py
```

2. 作成した zip ファイル (コンソールまたは CLI) を使用して関数を作成または更新します。

```
aws lambda update-function-code --function-name lambda-amscm-test --zip-file fileb://function.zip --region us-east-1
```

AMS 統合 Python Lambda が機能するようになりました。

#### Note

関数に の IAM アクセス許可が必要です。amscmそうしないと、アクセス許可エラーが発生します。

amscm (lambda-amscm-test.py の内容) をテストするための Lambda 関数コードの例 :

```
import json

# Force lambda to search local directory for boto3 data models
import os
os.environ['AWS_DATA_PATH'] = './models'

import boto3
import botocore

def lambda_handler(event, context):
    use_session = boto3.session.Session(region_name="us-east-1")
    try:
        cm = use_session.client("amscm")
        cts = cm.list_change_type_categories()
        print(cts)
    except botocore.exceptions.UnknownServiceError:
        print("amscm not found")

    return {
        'statusCode': 200,
        'body': json.dumps('Hello from Lambda!')
    }
```

テスト出力 (成功) :

関数レスポンス :

```
{
  "statusCode": 200,
  "body": "\"Hello from Lambda!\""
}
```

Request ID:  
"1cea13c0-ed46-43b1-b102-a8ea28529c27"

関数ログ :

```
START RequestId: 1cea13c0-ed46-43b1-b102-a8ea28529c27 Version: $LATEST
{'ChangeTypeCategories': ['Deployment', 'Internal Infrastructure Management',
  'Management'], 'ResponseMetadata': {'RequestId': 'e27276a0-e081-408d-
```

```
bcc2-10cf0aa19ece', 'HTTPStatusCode': 200, 'HTTPHeaders': {'x-amzn-requestid':  
  'e27276a0-e081-408d-bcc2-10cf0aa19ece', 'content-type': 'application/x-amz-json-1.1',  
  'content-length': '89', 'date': 'Sun, 10 May 2020 23:21:19 GMT'}, 'RetryAttempts': 0}}  
END RequestId: 1cea13c0-ed46-43b1-b102-a8ea28529c27
```

## AMS API から Ruby への例

Ruby で AMS API を使用するには、AWS Ruby SDK と AMS CLI をインストールします。以下の手順に従ってください。

1. AMS CLI をインストールします。「[AMS CLI のインストールまたはアップグレード](#)」を参照してください。
2. AWS Ruby SDK をインストールします。「[Amazon Web Services のツール](#)」を参照してください。
3. 次のコマンドを使用して Ruby を設定します。

```
require 'aws-sdk'  
  
config = {  
  region: 'us-east-1',  
  credentials: Aws::Credentials.new('ACCESS_KEY', 'SECRET_KEY')}
```

4. AMS CTsを取得します。

```
ams_cm = Aws::amscm::Client.new(config)  
  
cts = ams_cm.list_change_type_classification_summaries  
  
print(cts)
```

## AMS API から Java への例

Java で AMS API を使用するには、Java SDK AWS と AMS CLI をインストールします。以下の手順に従ってください。

1. AMS CLI をインストールします。「[AMS CLI のインストールまたはアップグレード](#)」を参照してください。
2. Java SDK AWS をインストールします。「[アマゾン ウェブ サービスのツール](#)」を参照してください。



### 3. 次のコマンドを使用して Java を設定します。

```
import com.amazonaws.auth.BasicAWSCredentials;

import com.amazonaws.services.amscm.model.AWSManagedServicesCMClient;

import
com.amazonaws.services.amscm.model.ListChangeTypeClassificationSummariesReque

import
com.amazonaws.services.amscm.model.ListChangeTypeClassificationSummariesResul

public static void getChangeTypeClassificationSummaries() {
```

### 4. 認証情報を設定します。これをハードコードしないことをお勧めします。

```
final BasicAWSCredentials awsCredsCm =

    new BasicAWSCredentials("ACCESS_KEY", "SECRET_KEY");
```

### 5. AMS 変更管理クライアントを作成します。

```
final AWSManagedServicesCMClient cmClient =

    new AWSManagedServicesCMClient(awsCredsCm);
```

### 6. AMS CTsを取得します。

```
final ListChangeTypeClassificationSummariesRequest listCtsRequest = new
ListChangeTypeClassification SummariesRequest();

final ListChangeTypeClassificationSummariesResult listCtsResult =

cmClient.listChangeTypeClassificationSummaries(listCtsRequest);

System.out.println("List of CTs");

listCtsResult.getChangeTypeClassificationSummaries().stream()

.map(x -> x.getCategory() + "/" + x.getSubcategory() + "/" +
x.getItem() + "/" + x.getOperation())

.forEach(System.out::println);
```

```
}
```

## AMS が独自の EPS を導入する

AMS の「独自のエンドポイントセキュリティの提供」(BYOEPS) 機能を使用して、デフォルトの Trend Micro Deep Security エージェントを独自のエンドポイントセキュリティソリューションまたは Trend Micro ライセンスに置き換えます。Trend Micro Deep Security または EPS を提供するチーム以外の製品の費用対効果の高いライセンスがすでにある場合、または特定の EPS ツールを使用する場合は、インスタンスで BYOEPS を使用します。

BYOEPS はアカウントレベルで機能します。アカウントのインスタンスは、BYOEPS またはデフォルトの AMS 管理 EPS を使用します。

- マルチアカウントランディングゾーン (MALZ): BYOEPS またはマネージド EPS を使用するアプリケーションアカウントを指定します。
- シングルアカウントランディングゾーン (SALZ): AMS アカウントは BYOEPS またはマネージド EPS を使用します。

BYOEPS を使用すると、Trend Micro Deep Security のコストが AWS 請求額を削減できます。AMS 管理の EPS は、アクセス管理 (踏み台、管理ホスト) に必要な AMS が作成および管理する EC2 インスタンスを保護するために引き続き必要であるため、引き続き EPS のコストが発生します。総コストへの影響を計算するには、新しいツールのライセンスコストと、必要なサービスレベルで EPS を管理するコストを考慮する必要があります。

BYOEPS を使用すると、セキュリティ管理の AMS の役割と責任が変わります。

- R は、タスクを達成するために作業を行う責任者を表します。
- C は、相談された当事者、通常は対象分野の専門家として意見を求める当事者、二国間通信を行う当事者を指します。
- 「情報」の略です。多くの場合、タスクまたは成果物の完了時にのみ、進捗状況が通知される当事者です。

| セキュリティ管理                                         | お客様 | AWS Managed Services |
|--------------------------------------------------|-----|----------------------|
| AMS 共有サービスの EC2 インスタンスの Managed EPS の有効なライセンスの維持 | R   | C                    |
| AMS 共有サービスの EC2 インスタンスのマネージド EPS を設定する           | I   | R                    |
| AMS 共有サービスの EC2 インスタンスのマネージド EPS を更新する           | I   | R                    |
| AMS 共有サービスの EC2 インスタンスでのマルウェアのモニタリング             | I   | R                    |
| AMS 共有サービスの EC2 インスタンスのウイルス署名の維持と更新              | I   | R                    |
| AMS 共有サービスの EC2 インスタンスのマルウェアに感染したインスタンスの修正       | C   | R                    |

BYOEPS を使用すると、AMS が提供するセキュリティコントロールの 1 つが失われます。Amazon GuardDuty、Amazon Macie などのツール、および IAM 設定のレビューなどのプロセスコントロールを通じて、引き続きセキュリティ管理が提供されます。BYOEPS を使用しても、AMS コンプライアンスの認定や認証には影響しません。ただし、多くのセキュリティフレームワークと証明書には、マルウェアや悪意のあるコードから保護するための要件があります。アカウントの安全性とコンプライアンスを維持するために、計画されたコントロールを評価して、ワークロードのコンプライアンス証明書のセキュリティ要件を満たしていることを確認します。

## アカウントの BYOEPS を有効にする

BYOEPS を有効にするプロセスには 3 つのステージが含まれており、複数の RFCs を使用します。BYOEPS を有効にするために必要な 3 つのステージについては、以下の情報を参照してください。次に、CSDM と連携して、アカウントの BYOEPS を有効にします。

### トピック

- [ステージ 1: 前提条件](#)
- [ステージ 2: アカウントで BYOEPS を有効にする](#)
- [ステージ 3: インスタンスの移行](#)

### ステージ 1: 前提条件

- デフォルトの Amazon EC2 インスタンスプロファイルは `customer-mc-ec2-instance-profile` です。デフォルトプロファイルに加えて別の Amazon EC2 インスタンスプロファイルを使用する場合は、`/ams/end-point-security` リソースの `ssm:GetParameter` アクションを EC2 インスタンスプロファイルに許可します。

EC2 インスタンスプロファイルを更新できない場合は、更新する必要があるインスタンスプロファイルを指定する RFC を送信します。

- この変更の範囲を理解します。

AMS 自動変更タイプ (CT) によるデプロイでは、作成時に使用する AMI を指定できます。

AMS マネージド EPS を使用するアカウントで BYOEPS を使用するには、AMS を使用してそれらの EC2 インスタンスから Trend Micro エージェントをアンインストールし、それらのインスタンスの AMS コード (ブートスクリプトなど) を更新する必要があります。これらのアクションには再起動が必要になる可能性があるため、メンテナンスウィンドウの一部としてこれらのアクションを実行するのがベストプラクティスです。CSDM に連絡して、このアクティビティを実行するメンテナンスウィンドウを特定し、移行計画を作成します。移行計画では、次の質問を検討してください。

1. 移行する必要があるインスタンスの数 インスタンスの合計数を小さい増分バッチに分割します。
2. インスタンスをバッチで分割する方法 たとえば、リソースグループで分割し、AMS オペレーションチームと共有するためのリストを作成できます。

3. 各バッチにはどのくらいの時間がかかりますか？ 必要な合計時間はどれくらいですか？ 同じメンテナンスウィンドウに任意の EPS ツールをインストールすることを検討してください。これにはどのくらいの時間がかかりますか？
- CSDM は、移行計画を AMS 運用チームと共有します。インスタンスフリートが 50 を超える場合は、CSDM と協力して、計画されたイベント管理 (PEM) プロセスを使用して計画されたイベントを作成します。詳細については、[AWS Managed Services での計画されたイベント管理](#)を参照してください。

AMS オペレーションは CSDM と連携して、アカウントのインスタンス数に基づいて、メンテナンスウィンドウに従って RFCs を送信する方法をアドバイスします。

- カスタム AMI または AMS AMIs を使用して EC2 インスタンス起動のオートメーションまたはプロセスを更新し、2020 年 12 月以降にリリースされた AMS AMIs を使用します。

## ステージ 2: アカウントで BYOEPS を有効にする

アカウントで BYOEPS を使用すると、AMS のセキュリティ管理に関する責任が変わります。BYOEPS を有効にする前に、セキュリティおよびクラウドプラットフォームチームに相談してください。

アカウントの BYOEPS をリクエストするには、ct-0xdawir96cy7k を使用して「MOO」更新 RFC (管理 | その他 | その他 | 更新) を以下の詳細とともに送信します。

Please enable BYOEPS for this account/these accounts  
Account IDs: *IDs for the accounts for BYOEPS.*

AMS は、パラメータストアの更新をアカウントにデプロイし、[Amazon EC2 IAM インスタンスプロファイル](#)を更新します。

### Note

- 最新の AMS AMIs を使用する新しいインスタンス起動のアカウントは、Trend Micro エージェントのインストールをスキップできます。2020 年 12 月より前の AMIs は BYOEPS 機能をサポートしていません。古い AMIs を使用するオートメーションを更新して、BYOEPS 機能をサポートする最新の AMS AMIs を使用します。
- 既存の EC2 インスタンスの処理については、「ステージ 3: インスタンスの移行」を参照してください。

## ステージ 3: インスタンスの移行

ユースケースに応じて、次のいずれかのオプションを使用してインスタンスを移行します。どのオプションを選択するかわからない場合は、CA または CSDM にお問い合わせください。

### AMS マネージド EPS を使用する EC2 インスタンスを持つアカウント

メンテナンス期間中、ステージ 1 の計画に従って、BYOEPS にオンボードする必要がある各インスタンスで次のアクションを実行します。

- AMS によって実行される: AMS コード (ブートスクリプト、モジュールなど) を最新バージョンに更新します。これは、古い AMS ブートスクリプトに BYOEPS 機能のサポートがなく、起動のたびに Trend Micro エージェントを再インストールするため必要です。また、Trend Micro エージェントをアンインストールします。
- ユーザーが実行: 任意の EPS ツールをインストールして設定します。

#### Important

Trend Micro Agent はマルウェア保護を提供します。インスタンスを保護するために、適切な代替 をインストールしてください。

これらの変更を送信するために、変更タイプ ct-2iz9nvw8zlhst の RFCs を送信するには、[Trend Micro DSM | Trend Micro EPS Agent \(マネージドオートメーション\)](#) をバッチで削除します。

### AMS マネージド EPS を使用する EC2 インスタンスのないアカウント

最新の AMS AMIs を使用する新しいインスタンス起動のアカウントは、Trend Micro エージェントのインストールをスキップできます。2020 年 12 月より前の AMIs は BYOEPS 機能をサポートしていません。古い AMIs を使用するオートメーションを更新して、BYOEPS 機能をサポートする最新の AMS AMIs を使用します。

### EC2 インスタンスにエージェントを追加する

AMS パターンを使用して、CrowdStrike や Qualys などのツールのエージェントをデプロイし、サービスリクエストを送信してサポートを受けることができます。

## AMS 通知の受信

ユーザーと AMS 間の通信は、さまざまな理由で発生します。

- 承認が必要な AMS によって作成された RFC
- 失敗した RFC を調査するために作成された AMS ケース
- アラートをモニタリングして作成されたイベント
- 今後のパッチ適用を通知するパッチサービス通知
- サービスリクエストとインシデントレポート
- 毎月の CRM レポート
- ときどき重要な AWS の発表 (お客様側のアクションが必要な場合は CSDM から連絡があります )

これらの通知はすべて、オンボーディング時に AMS に提供したデフォルトの連絡先情報 (ルートアカウントの E メール) に送信されます。個々の Eメールの更新は難しいため、後で更新できるグループ Eメールを使用することをお勧めします。送信されたすべての通知も AMS オペレーションによって受信され、応答する前に分析されます。

AMS 通知サービスには、通知の連絡先を設定する 2 つの方法があります。

- リソースに問い合わせタグ (連絡先情報であるタグの Key Value) をタグ付けし、CSDM にタグの Key Name を指定します。これらのリソースに対するアラームは、オンボーディング時に作成されたアカウントの連絡先に加えて、キーバリューで指定された連絡先に送信されます。これは、アプリケーション所有者にとって特に便利です。詳細については、「[タグベースのアラート通知](#)」を参照してください。
- ( オンボーディング時に必須) リソースベースの通知以外の連絡先のリストを CSDM に送信します。たとえば、「SecurityContacts」という名前のリストと「OperationsContacts」という名前のリストがあるとします。AMS は通知サービスにリストを追加し、そのリストのコンテキストに適用されるアラームがそれらの連絡先に送信されます。これは、組織の問題に特に役立ちます。

この高度なアラートルーティング機能は、Amazon EC2 インスタンスの障害、Amazon Elastic Block Store (Amazon EBS) ボリューム容量使用率 - ルート使用率、Amazon EBS NonRoot 使用率、高メモリ使用率、高スワップ使用率、Amazon EC2 の高 CPU 使用率など、重要な CloudWatch アラームのほとんどでアクティブです。

さらに、サービスリクエストまたはインシデントレポートを提出する際に、「CC E メール」(強く推奨) を追加するオプションがあり、それらの E メールアドレスはサービスリクエストまたはインシデントに関する通知を受け取ります。



### ⚠ Important

サービスリクエストやインシデントレポートで提供される CC E メールアドレスは通信に関する E メール通知を受信しますが、パッチ適用通知などの他の通知は、注意を待っている通信があることを明示的に通知することなく、サービスリクエストリストに表示されます (E メールもデフォルトの連絡先に送信されます)。そのため、可能な場所に CC E メールを追加し、AMS を使用するすべてのユーザーがメンバーになるグループとしてデフォルトの連絡先 E メールを設定することを強くお勧めします。

さらに、新しい AMIs、RFC 状態変更、および AMS アカウントの設定変更に関する特別な通知をリクエストできます。次に、これらのオプションの通知サービスについて説明します。

## SNS を使用した AMS AMI 通知

AMS は AMI 通知サービスを提供します。これを使用して、AMS AMI の更新がリリースされたときに通知する Amazon Simple Notification Service (SNS) トピックをサブスクライブできます。使用する AMS AMIs のみの通知を受信するか、サインアップしてすべての AMS AMIs の更新通知を受信するかを選択できます。SNS トピックの詳細については、[「Amazon Simple Notification Service とは」を参照してください。](#)

AMIs がリリースされるたびに、対応するトピックのサブスクライバーに通知が送信されます。このセクションでは、AMS AMI 通知をサブスクライブする方法について説明します。

### サンプルメッセージ

```
{
  "Type" : "Notification",
  "MessageId" : "example messageId",
  "TopicArn" : "arn:aws:sns:us-east-1:591688410472:customer-ams-windows2019",
  "Subject" : "New AMS AMIs are Now Available",
  "Message" : "{\"v1\": {\"Message\": \"A new version of the AMS Amazon Machine Images has been released. You are now able to launch new EC2 stacks from these AMIs. Please use this time to update any dependencies such as CloudFormation or Autoscaling groups. Release Notes Windows - Contains latest Windows Patches: Microsoft Windows Server 2008 R2 Datacenter - (KB2819745, KB3018238, KB4507004, KB4507437) Microsoft Windows Server 2016 Datacenter Security Enhancedn - (KB4509091, KB4507459) Microsoft Windows Server 2016 Datacenter - (KB4509091, KB4507459) Microsoft Windows Server 2012 R2 Security Enhancedn - (KB3191564, KB3003057, KB3013172, KB3185319, KB4504418,
```



```
KB4506996, KB4507463) Microsoft Windows Server 2012 R2 Standardn - (KB3003057,
KB3013172, KB3185319, KB4504418, KB4506996, KB4507463) Linux - Contains latest Linux
patches -
All AMIs now force domainjoin-cli leave before domainjoin-cli join for better
stability in the domain join process.", "images":
{"images": {"image_name": "customer-ams-windows2019-2021.08-1", "image_id":
"ami-05dfa45396fddaa5e"}}, "region": "us-east-1"}},
"Timestamp" : "2021-09-03T19:05:57.882Z",
"SignatureVersion" : "1",
"Signature" : "example sig",
"SigningCertURL" : "example url",
"UnsubscribeURL" : "example url"
}
```

### サブスクライブ可能な AMS AMI トピック :

- ALL: を使用しますcustomer-ams-all-amis。このトピックサブスクリプションは、いずれかの AMS AMIs が更新されたときに通知します。
- AMS AWS Linux AMIs: Amazon Linux の場合は、 customer-ams-amazon1と を使用しますcustomer-ams-amazon1-security-enhanced。Amazon Linux 2 の場合は、 customer-ams-amazon2と を使用しますcustomer-ams-amazon2-security-enhanced。
- AMS SUSE Linux AMIs: customer-ams-sles12または を使用しますcustomer-ams-sles15。
- AMS AWS RedHat AMIs: customer-ams-rhel8、customer-ams-rhel8-security-enhanced、customer-ams-rhel7、 を使用しますcustomer-ams-rhel7-security-enhanced。
- AMS AWS CentOS AMIs: customer-ams-centos7、 を使用しますcustomer-ams-centos7-security-enhanced。
- AMS Ubuntu AMIs: を使用しますcustomer-ams-ubuntu18。
- AMS AWS Windows AMIs: customer-ams-windows2019、customer-ams-windows2019-security-enhanced、customer-ams-windows2016、customer-ams-windows2016-security-enhanced、customer-ams-windows2012r2-security-enhanced、customer-ams-windows2012customer-ams-windows2012r2、 を使用しますcustomer-ams-windows2022。

Amazon SNS コンソールを使用して AMS の新しい AMI 通知をサブスクライブするには :

1. Amazon SNS コンソールの [\[ダッシュボード\]](#) を開きます。

2. 右上隅で、サブスクライブする AMIs の AWS リージョンに変更します。
3. 左ナビゲーションペインで、サブスクリプションを選択し、サブスクリプションの作成を選択します。
4. 以下の情報を指定します。
  - a. トピック ARN: `arn:aws:sns:{REGION}:287847593866:{AMS_AMI_NAME}` REGION は選択した AWS リージョン (SNS 通知が作成された場所) で、AMS\_AMI\_NAME は通知の対象となる AMI です。例:
    - AWS リージョン us-east-1 の新しい AMS Amazon Linux AMIs の通知をサブスクライブするには、このトピック ARN = `arn:aws:sns:us-east-1:287847593866:customer-ams-amazon1`。
    - AWS リージョン us-west-2 の新しい AMS Window Server 2016 AMIs の通知をサブスクライブするには、このトピック ARN = `arn:aws:sns:us-west-2:287847593866:customer-ams-windows2016`
  - b. [プロトコル] で [E メール] を選択します。
  - c. [エンドポイント] に、通知を受信するために使用できる E メールアドレスを入力します。個人の E メールではなく、ディストリビューションリストを使用することをお勧めします。
5. [Create subscription] を選択してください。
6. 件名が「AWS 通知 - サブスクリプションの確認」である確認 E メールを受信したら、E メールを開き、サブスクリプションの確認を選択してサブスクリプションを完了します。

 Note

プロトコルの E メールに限定されません。その他の許容可能なプロトコルとその使用方法については、[「サブスクライブ」](#)を参照してください。

AWS SNS コンソールを使用して AMS の新しい AMI 通知のサブスクリプションを解除するには：

1. Amazon SNS コンソールの [\[ダッシュボード\]](#) を開きます。
2. ナビゲーションバーで、を任意の AWS リージョンに変更します。対応する AMIs の通知を受信する AWS リージョンを使用する必要があります。

3. ナビゲーションペインで、サブスクリプションを選択し、サブスクリプションを選択し、アクション -> サブスクリプションの削除を選択します。
4. 確認を求めるメッセージが表示されたら、[削除] を選択してください。

デプロイ | 取り込み | CloudFormation テンプレートからのスタック | 作成 (ct-36cn2avfrrj9v) を使用して AMS の新しい AMI 通知をサブスクライブするには：

1. AmazonLinuxSubscription をサブスクライブするには、実行パラメータ JSON ファイルを作成して保存します。この例では、CreateSubscribeAmiParams.json:

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Resources": {
    "AmazonLinuxSubscription": {
      "Type": "AWS::SNS::Subscription",
      "Properties": {
        "TopicArn": "arn:aws:sns:{REGION}:287847593866:{AMS_AMI_NAME}",
        "Protocol": "email",
        "Endpoint": "username@yourdomain.com"
      }
    }
  }
}
```

2. 次の内容の RFC パラメータ JSON ファイルを作成して保存します。この例では、CreateSubscribeAmiRfc.json ファイルという名前を付けます。

```
{
  "ChangeTypeId": "ct-36cn2avfrrj9v",
  "ChangeTypeVersion": "1.0",
  "Title": "cfn-ingest-subscribe-ami"
}
```

3. CreateSubscribeAmiRfc ファイルと CreateSubscribeAmiParams ファイルを指定して、RFC を作成します。

```
aws amscm create-rfc --cli-input-json file://CreateSubscribeAmiRfc.json --
execution-parameters file://CreateSubscribeAmiParams.json
```

レスポンスで新しい RFC の ID を受け取り、それを使用して RFC を送信およびモニタリングできます。送信するまで、RFC は編集状態のままであり、開始されません。

AMIs [「AMI の作成」](#) を参照してください。

プログラムによる AMIs」を参照してください。 [EC2](#)

## サービス通知

AMS は、アカウントまたはリソースに影響を与える可能性のある対応が必要な場合、または認識する必要がある場合、アウトバウンドサービスリクエストまたはサービス通知を送信します。これには、以下が含まれます。

- インフラストラクチャへの影響: AMS は、基盤となる AWS サービスがインフラストラクチャに影響を与え、特定の日付より前にアクションを実行する必要がある場合、または停止する可能性がある場合に、サービス通知を送信します。
- EC2 ハードウェアの問題: AMS は、特定の日付より前に EC2 インスタンスを再起動する必要がある EC2 ハードウェアの問題に対してサービス通知を送信します。または、AMS がインスタンスを再起動することを知らせます。これは重要な通知です。再起動によって停止が発生する可能性があるため、インスタンスを自分で再起動するには、許容できる日付で応答するか、ct-09qbhy7kvtxqw で RFC を作成する必要があります。このようなサービス通知は、応答しない場合、5 日後に自動的に終了します。

## RFC 状態変更通知

AMS は、E メールと CloudWatch Events による RFC 状態変更の通知を提供します。

- AMS コンソールによる E メール: RFC 作成ウィザードの 2 ページ目にオプションがあり、RFC 状態が変更されたときに通知される E メールアドレスを最大 5 つまで追加できます。
- CloudWatch Events: CloudWatch Events のさまざまなルールとターゲットを設定して、RFC の状態が変化するたびに通知を受け取ることができます。

## E メール通知

E メールアドレスを追加して、AMS コンソールで、または AMS API/CLI を使用して作成した RFC に RFC 状態の変更を受け取ることができます。

AMS コンソールで、RFC 作成ウィザードの 2 ページ目の E メール通知オプションを使用します。

AMS API/CLI で、RFC の RFC パラメータセクションに次のような行を追加します (実行パラメータセクションに行を追加しないでください)。

```
--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}\"
```

通知の動作は、RFC スケジューリングタイプによって異なります。

- スケジュールされた RFCs、で E メール通知を受け取ります。送信済み、スケジュール済み、InProgress、完了済み、拒否済み、キャンセル済み、自動拒否済み、または自動キャンセル済み。
- ASAP RFCs、送信済み、InProgress、完了済み、拒否済み、キャンセル済み、AutoRejected、または自動キャンセル済みの E メール通知を受け取ります。

#### Note

- E メール通知は、次のアドレスから送信されます: `no-reply@managedservices.amazonaws.com`。
- RFC タイトルの特殊文字と URLs は、送信する E メールで編集されます。これはセキュリティ対策です。

## CloudWatch Events 通知

AMS は、CloudWatch Events を通じて RFC 状態の変更に関するプッシュ通知を提供します。これらの通知を取得するには：

1. 通知が送信されるトピックとサブスクリプションを作成します。トピックに名前を付けることができます。これを行う方法については、[「SNS Topic and Subscription: Creating」](#)を参照してください。
2. 管理 | その他 | その他 | 変更タイプを作成し、RFC 状態変更通知のリクエストに SNS トピックとサブスクリプションを含め、RFC を送信します。

この機能の管理 | その他 | その他の RFC リクエストを送信するときに、通知を受ける RFC 状態の変更と変更タイプを指定し、他のフィルターを設定できます。たとえば、管理者アクセスの変更タイプ

が EventType = RfcSubmitted および EventType = RfcUpdated の場合にのみ、通知をリクエストできます。

これは、受信できる CloudWatch イベント通知のテンプレートです (可能なすべての値を含む)。

```
{
  "source ": "aws.managedservices",
  "detail-type": "AMS RFC State Change",
  "detail": {
    "ActionState": "null | AwsActionPending | AwsOperatorAssigned | CustomerActionPending | NotApplicable | NoActionPending",
    "ActualExecutionTimeRange": {
      "StartTime": "null | Actual Start Time",
      "EndTime": "null | Actual End Time"
    },
    "AutomationStatus": "Automated | Manual",
    "AwsAccountId": "AWS Account ID",
    "AwsApprovalStatus": "null | SubmissionPending | NotRequired | ApprovalPending | Rejected | Approved",
    "ChangeTypeId": "Change_Type_ID",
    "ChangeTypeVersion": "Change_Type_Version",
    "CreatedTime": "Created_Time",
    "CustomerApprovalStatus": "null | SubmissionPending | NotRequired | ApprovalPending | Rejected | Approved",
    "EventType": "RfcActionStateUpdated | RfcApproved | RfcAutoRejected | RfcCanceled | RfcCompleted | RfcCreated | RfcInProgress | RfcRejected | RfcSubmitted | RfcUpdated",
    "LastModifiedTime": "Last_Updated_Time",
    "LastSubmittedTime": "null | Last_Submitted_Time",
    "RequestedExecutionTimeRange": {
      "StartTime": "null | Expected_Start_Time",
      "EndTime": "null | Expected_End_Time"
    },
    "RfcId": "RFC_ID",
    "Status": "Editing | PendingApproval | Scheduled | Rejected | Canceled | ExecutionLock | InProgress | Success | Failure",
    "Title": "Title"
  }
}
```

実際の CloudWatch Events 通知に表示されるように、サポートされている RFC 状態 (EventType) が変更されます。

- RfcActionStateUpdated (AMS コンソールオプションなし): 後述するいずれかの状態の RFC が変更されました。
- RfcApproved (AMS コンソールオプションなし): RFC がシステムおよび/または AMS オペレータの検証に合格し、完了が承認されました。
- RfcAutoRejected (自動拒否): RFC がシステム検証または AMS 演算子に失敗し、拒否されました。
- RfcCanceled (キャンセル済みまたは自動キャンセル済み): RFC は送信者または AMS 演算子によってキャンセルされました。
- RfcCompleted (Completed): UserData を含む RFC 実行パラメータが完了しました。
- RfcCreated (AMS コンソールオプションなし): RFC が正常に作成されました (JSON および送信されたパラメータは有効でした)。
- RfcInProgress (InProgress): RFC 実行はまだ進行中です。
- RfcRejected (拒否): RFC が失敗したシステムまたは AMS オペレータの検証が拒否されました。
- RfcSubmitted (送信済み): RFC が送信され、システム検証中です。
- RfcUpdated (AMS コンソールオプションなし): RFC は AMS オペレータによって手動で更新されました。

さらに、CloudWatch Events (CWE) 通知をサポートされている任意の送信先に送信し、これらの自動通知に加えて独自のシステムを構築できます。

- Amazon EC2 インスタンス
- AWS Lambda 関数
- Amazon Kinesis Data Streams のストリーム
- Amazon Data Firehose の配信ストリーム
- Amazon CloudWatch Logs のロググループ
- Amazon ECS タスク
- Systems Manager Run Command
- Systems Manager Automation
- AWS Batch ジョブ
- Step Functions ステートマシン
- CodePipeline のパイプライン
- CodeBuild プロジェクト

- Amazon Inspector の評価テンプレート
- Amazon SNS トピック
- Amazon SQS キュー
- 組み込みターゲット: EC2 CreateSnapshot API コール、EC2 RebootInstances API コール、EC2 StopInstances API コール、および EC2 TerminateInstances API コール。
- 別の AWS アカウントのデフォルトのイベントバス

#### Note

RFC 状態の変更に関する CloudWatch Events 通知をベストエフォートベースで送信します。

## プライベート DNS とパブリック DNS のセットアップ

オンボーディング中、AMS はマネージドリソースと AMS 間の通信用にプライベート DNS サービスを設定します。

AMS Route 53 を使用して、この情報をパブリックインターネットに公開することなく、アプリケーションリソース (ウェブサーバー、アプリケーションサーバー、データベースなど) の内部 DNS 名を管理できます。これにより、セキュリティレイヤーが追加され、DNS 名を別の IP アドレスにマッピングすることで、プライマリリソースからセカンダリリソース (多くの場合、「フリップ」と呼ばれます) にフェイルオーバーすることもできます。

デプロイ | アドバンスドスタックコンポーネント | DNS (プライベート) | 作成 (ct-0c38gftq56zj6) または デプロイ | アドバンスドスタックコンポーネント | DNS (パブリック) | 作成 (ct-0vzsr2nyraedl) を使用してプライベート DNS リソースを作成した後、管理 | アドバンスドスタックコンポーネント | DNS (プライベート) | 更新 (ct-1d5pi44ff21u) および 管理 | アドバンスドスタックコンポーネント | DNS (パブリック) | 更新 (ct-1hzofpphabs3i) CTs を使用して、追加または既存のレコードセットを更新できます。マルチアカウントランディングゾーン (MALZ) アカウントの場合、アプリケーションアカウント VPCs で作成された DNS リソースを共有サービスアカウント VPC と共有して、AMS AD を使用して一元化された DNS を維持できます。

### MALZ

次の図は、マルチアカウントランディングゾーン AMS で可能な DNS 設定を示しています。AMS と一般的なカスタマーネットワーク間のハイブリッド DNS セットアップを示してい



ます。カスタマーネットワーク DNS サーバーの正規名レコード (CNAME) は、AMS FQDN の CNAME が A レコードに転送された条件付き転送で、共有サービスアカウントの AMS AD DNS に転送します。

## SALZ

次の図は、単一アカウントランディングゾーン (SALZ) で可能な DNS 設定を示しています。AMS と一般的なカスタマーネットワーク間のハイブリッド DNS 設定を示します。カスタマーネットワーク DNS サーバーの CNAME は、AMS FQDN の CNAME が A レコードに転送された条件付き転送で AMS AD DNS に転送されます。

## SALZ Route53 DNS

次の図は、単一アカウントランディングゾーン (SALZ) で可能な DNS 設定を示しています。AMS と一般的なカスタマーネットワーク間のハイブリッド DNS 設定を示します。カスタマーネットワーク DNS サーバーの CNAME は、AMS FQDN の CNAME が A レコードに転送された条件付き転送で AMS AD DNS に転送されます。これにより、アウトバウンドネットワークトラフィックに Route53 も活用されるため、アカウント内のすべてのアプリケーションで可用性が最も高いアカウントで DNS 解決を行うことができます。

Route53 が有効な解決パス:

- AMS MAD 名を解決しようとしているインスタンス --> VPC +2 (Route53/AmazonProvidedDNS) --> 条件付きフォワーダーが評価 --> Route53 MAD 条件付きフォワーダールールが一致 --> Route53 アウトバウンドリゾルバー --> マネージド AD DNS
- お客様のオンプレミス名を解決しようとするインスタンス --> VPC +2 (Route53/AmazonProvidedDNS) --> 条件付きフォワーダーが評価 --> Route53 オンプレミス条件付きフォワーダールールが一致 --> Route53 アウトバウンドリゾルバー --> お客様のオンプレミス DNS
- インターネット名を解決しようとしているインスタンス --> VPC +2 (Route53/AmazonProvidedDNS) --> 条件付きフォワーダーが評価されました --> 一致するフォワーダーがありません --> インターネット DNS サービス

詳細については、[「VPC での DNS の使用」](#) および [「プライベートホストゾーンの使用」](#) を参照してください。

# AMS 出力トラフィック管理

デフォルトでは、AMS プライベートサブネットとカスタマーアプリケーションサブネットの送信先 CIDR が 0.0.0.0/0 のルートには、ターゲットとしてネットワークアドレス変換 (NAT) ゲートウェイがあります。AMS サービスである TrendMicro とパッチ適用は、AMS がそのサービスを提供し、TrendMicro とオペレーティングシステムが更新を取得できるように、インターネットへの出力アクセス権を持つ必要があるコンポーネントです。

AMS は、次の条件を満たす限り、カスタマー管理の Egress デバイスを介して Egress トラフィックをインターネットに転送することをサポートしています。

- 暗黙的な (透過的な) プロキシとして機能します。

and

- AMS マネージドインフラストラクチャの継続的なパッチ適用とメンテナンスを可能にするために、AMS HTTP と HTTPS の依存関係 (このセクションに記載) を許可します。

いくつか例を挙げます。

- Transit Gateway (TGW) には、マルチアカウントランディングゾーンネットワークアカウントの AWS Direct Connect 接続を介したカスタマー管理のオンプレミスファイアウォールを指すデフォルトルートがあります。
- TGW には、AWS PrivateLink を利用するマルチアカウントランディングゾーン出力 VPC の AWS エンドポイントを指すデフォルトルートがあり、別の AWS アカウントのカスタマーマネージドプロキシを指します。
- TGW には、別の AWS アカウントのカスタマーマネージドファイアウォールを指すデフォルトルートがあり、site-to-site接続をマルチアカウントランディングゾーン TGW へのアタッチメントとして使用します。

AMS は、対応する AMS HTTP と HTTPS の依存関係を特定し、これらの依存関係を継続的に開発および改良しています。「[egressMgmt.zip](#)」を参照してください。JSON ファイルに加えて、ZIP には README が含まれています。

## Note

- この情報は包括的ではありません。必須の外部サイトの一部はここには記載されていません。

- このリストを拒否リストまたはブロック戦略で使用しないでください。
- このリストは、出力フィルタリングルールセットの開始点として意図されており、実際のトラフィックがリストのどこから逸脱するかを正確に判断するためにレポートツールが使用されることを期待しています。

送信トラフィックのフィルタリングに関する情報を尋ねるには、CSDM に E メールを送信します：  
ams-csdm@amazon.com。

## AMS Advanced での IAM リソースのデプロイ

AMS は、次の 2 つの方法でマルチアカウントランディングゾーン (MALZ) アプリケーションとシングルアカウントランディングゾーン (SALZ) アカウントに IAM リソースをデプロイします。

- 自動 IAM プロビジョニング: AMS のこの機能を使用すると、オペレータによるレビューなしで、IAM ロールまたはポリシープロビジョニングの変更タイプを作成、更新、または削除し、IAM と AMS の検証チェックを自動的に実行できます。

この機能は、管理 | マネージドアカウント | 読み取り/書き込みアクセス許可を持つ AMS 自動 IAM プロビジョニング | [\(マネージドオートメーション\)](#) 変更タイプを有効にする (ct-1706xvvk6j9hf) で明示的に有効にする必要があります。詳細については[自動 IAM プロビジョニング AMS](#)を参照してください。AMS 自動 IAM プロビジョニングを有効にすると、IAM リソースを管理するための変更タイプの作成、更新、削除にアクセスできます。

- マネージドオートメーション IAM 変更タイプ: この変更タイプ、デプロイ | アドバンスドスタックコンポーネント | Identity and Access Management (IAM) | [Create entity or policy \(マネージドオートメーション\)](#) (ct-3dpd8mdd9jn1r) では、AMS オペレータによるレビューが必要です。明確化が必要な場合、完了までに数日かかることがあります。

### Note

どちらの方法を使用する場合でも、IAM ロールは関連するアカウントまたはアカウントにプロビジョニングされ、ロールがプロビジョニングされた後、フェデレーションソリューションでロールをオンボードする必要があります。

## 自動 IAM プロビジョニング AMS

AWS Managed Services (AMS) は、AMS Advanced requests for change (RFCs) と新しい変更タイプ (CTs) を使用したロールとポリシーを含む IAM リソースの自動検証とプロビジョニングをサポートしています。以前は、これらのリクエストは半自動プロセスを経ており、待機時間が長くなる場合があります。これで、AMS 自動 IAM プロビジョニングを使用して IAM リソースをプロビジョニングし、結果をより迅速に取得できるようになりました。

### AMS での IAM 自動プロビジョニングの仕組み

自動 IAM プロビジョニングは、IAM リソースの変更を検証するために IAM の自動ランタイムチェックに依存します。これらの自動チェックは、変更タイプの作成、更新、削除が実行されたときに実行され、過度に許可されている、または安全でないパターンを持つ IAM リソースがアカウントにデプロイされるのを防ぎます。これにより、IAM レビューの厳密さのレベルをチームの専門知識と一致させることができます。クラウドサービスを初めて使用し、すべての IAM リソースの変更に手動チェックが必要なチームは、既存のレビューで必要な変更タイプ デプロイ | 高度なスタックコンポーネント | Identity and Access Management (IAM) | [エンティティまたはポリシーの作成 \(マネージドオートメーション\)](#)、(ct-3dpd8mdd9jn1r) を使用することをお勧めします。環境の AWS 専門知識と制御を持つチームは、自動 IAM プロビジョニングを使用してデプロイを高速化できます。この機能を使用して、自動ランタイムチェックによる検証を実行したり、検証が成功した後に IAM リソースの検証とプロビジョニングを実行したりできます。

#### Important

AWS Managed Services は、特定のアクセス許可と条件を持つ IAM リソースまたはポリシーの作成を妨げる検証 [ランタイムチェック](#) のリストを事前に実装しています。これらの権限と条件の詳細については、[「AMS Advanced での IAM リソースのデプロイ」](#) を参照してください。自動変更タイプ [ct-1n9gfnog5x7fl](#)、[ct-1e0xmuy1diafq](#)、[ct-17cj84y7632o6](#) では、IAM リソースの管理に精通しているユーザーが、読み取り専用権限を超えるアクションを許可する IAM ロールとポリシーをプロビジョニングできます。

さらに、自動変更タイプ [ct-1n9gfnog5x7fl](#)、[ct-1e0xmuy1diafq](#)、[ct-17cj84y7632o6](#) で作成されたロールを使用して、新しいリソースを作成できます。ただし、リソースは AMS 命名基準に従うことができず、標準 AMS スタックの一部ではありません。AMS は、ベストエフォートベースでこれらの特定のリソースの運用およびセキュリティサポートを提供します。

手動プロセスと自動プロセスの両方がセキュリティ標準を維持することを目指していますが、この 2 つのチェックには違いがあることに注意してください。自動プロビジョニングにより、ロールとポリシーの作成と更新の柔軟性が向上します。したがって、これらは同じで

はありません。組織が AMS ユーザーガイドに記載されている検証[ランタイムチェック](#)を注意深く確認し、組織の期待と要件に沿っていることを確認することをお勧めします。

## 検証フロー

### 検証とプロビジョニングのフロー

#### Note

この機能は、AWS および IAM リソースの経験があるチームに適しています。また、初めてのチームにはお勧めしません AWS。自動検証プロセスは、ほとんどのエラーをキャッチするように設計されており、チームが必要なアクセス許可を理解したときに、IAM の変更をすばやくレビューするのに役立ちます。新しい変更タイプを安全かつ効果的に使用するには、IAM AWS と、変更タイプによって提供される[ランタイムチェック](#)をよく理解し、それがチームに適しているかどうかを判断することをお勧めします。

## AMS での AMS 自動 IAM プロビジョニングへのオンボーディング

新しい変更タイプを使用するには、まず、次の変更タイプを使用して RFC を送信して AMS 自動 IAM プロビジョニングを有効にします。管理 | マネージドアカウント | 読み取り/書き込みアクセス許可を持つ AMS 自動 IAM プロビジョニング | [有効化 \(マネージドオートメーション\)](#) (ct-1706xvvk6j9hf)。AWS では、これらの変更タイプの使用が組織ポリシーと一致していることを確認するために、組織がカスタマーセキュリティリスク管理 (CSRM) プロセスを経る必要があります。AWS 運用チームはお客様と協力して、必要なレビューの一環として、リスク承諾の形式でセキュリティチームの連絡先から明示的な承認を取得します。詳細については、[RFC カスタマーリスク管理 \(CSRM\) プロセス](#)を参照してください。

読み取り/書き込みアクセス許可機能を使用して AMS 自動 IAM プロビジョニングを有効にするための RFC が成功すると、AMS は、有効化 RFC の送信に使用したアカウントで AMS 自動 IAM プロビジョニングの変更タイプを有効にします。アカウントで AMS 自動 IAM プロビジョニングが有効になっていることを確認するには、IAM コンソールで `AWSManagedServicesIAMProvisionAdminRole` ロールを確認します。

オンボーディングの一環として、AMS はアカウントの同じ AWS リージョンに IAM Access Analyzer をプロビジョニングして、アクセスプレビュー機能を活用します。IAM Access Analyzer は、組織

内のリソースと外部エンティティと共有されているアカウントを識別し、ポリシーの文法とベストプラクティスに照らして IAM ポリシーを検証し、AWS CloudTrail ログ内のアクセスアクティビティに基づいて IAM ポリシーを生成します。詳細については、「[「の使用 AWS Identity and Access Management Access Analyzer」](#)」を参照してください。

オンボーディングされると、AWSManagedServicesIAMProvisionAdminRoleは有効なアカウントにデプロイされます。SAML フェデレーションでこのロールを使用する場合は、フェデレーションソリューションにロールをオンボードする必要があります。

オンボーディングの一環として、AWSManagedServicesIAMProvisionAdminRole の信頼ポリシーを更新して、このロールを引き受ける別の IAM ロール ARN を付与するようにリクエストできます AWS Security Token Service。

## AMS での AMS 自動 IAM プロビジョニングの使用

次の AMS 自動 IAM プロビジョニング変更タイプを使用して RFCs を作成できます。

### Note

- ロールとポリシーのプロビジョニングのみがサポートされています。

ロールの更新中、Update CT は、マネージドポリシー Amazon リソースネーム (ARNs) ポリシードキュメントを、提供されたマネージドポリシー ARNs と「ロールを引き受ける」ポリシードキュメントに置き換えます。部分的な更新では、例えば、マネージドポリシー ARN の既存のリストで ARNs」ポリシードキュメントに追加または削除することはできません。同様に、ポリシーの更新中、Update CT は既存のポリシードキュメントを置き換え、既存のポリシードキュメントで個々のポリシーステートメントを追加または削除することはできません。

- 「検証のみ」オプションを選択すると、IAM エンティティまたはポリシーをプロビジョニングせずにランタイムチェックが実行されます。検出結果に関係なく、RFC ステータスは「成功」です。「成功」ステータスは、指定された IAM エンティティまたはポリシーに対する検証が成功したことを示します。

- デプロイ | アドバンスドスタックコンポーネント | Identity and Access Management (IAM) | [エンティティまたはポリシーの作成 \(読み取り/書き込みアクセス許可\)](#)(ct-1n9gfnog5x7fl): 新しい IAM エンティティまたはポリシーが自動的に検証およびプロビジョニングされます。



- 管理 | アドバンスドスタックコンポーネント | Identity and Access Management (IAM) | [更新エンティティまたはポリシー \(読み取り/書き込みアクセス許可\)](#)(ct-1e0xmuy1diafq): 既存の IAM エンティティまたはポリシーは自動的に更新および検証されます。
- 管理 | アドバンスドスタックコンポーネント | Identity and Access Management (IAM) | [Delete entity or policy \(読み取り/書き込みアクセス許可\)](#)(ct-17cj84y7632o6): 自動作成エンティティまたはポリシー変更タイプを使用してプロビジョニングされた既存の IAM エンティティまたはポリシーが削除されます。

専用 IAM ロール を使用してのみ、前述の 3 つの CTs を呼び出すことができます。AWSManagedServicesIAMProvisionAdminRole。このロールは、管理 | マネージドアカウント | AMS 自動 IAM プロビジョニングの読み取り/書き込みアクセス許可 | [有効 \(マネージドオートメーション\)](#) (ct-1706xvvk6j9hf) を使用して 機能にオンボードされたアカウントでのみ使用できます。

#### Important

変更タイプの作成、更新、削除は常にアカウントに表示されますが、デフォルトでは有効になっていません。最初に AMS 自動 IAM プロビジョニング機能を有効にせずに、これらの変更タイプのいずれかを使用して RFC を送信しようとする、と、「未承認」エラーが表示されます。

#### 機能制限:

- Create CT では、AWS リソースを作成するアクセス許可を持つ IAM ロールまたはポリシーを作成できる場合があります。ただし、これらのロールとポリシーによって作成された AWS リソースは AMS によって管理されません。このようなロールやポリシーの作成を制限するために、組織の管理に従うのがベストプラクティスです。
- Update CT は、CFN Ingest、Direct Change Mode、Developer Mode、または場合によっては既存の AMS Advanced 手動または自動 CTs を使用して作成された IAM ロールとポリシーを変更できません。
- Delete CT は、AMS 自動 IAM プロビジョニング Create CT で作成されていない既存のロールやポリシーを削除することはできません。
- 読み取り/書き込みアクセス許可を持つ AMS 自動 IAM プロビジョニング機能は、Direct Change Mode ロールではサポートされていません。つまり、これらのロールを使用して読み取り/書き込

みアクセス許可を持つ IAM ロールとポリシーをプロビジョニングまたは更新することはできません。

- 読み取り/書き込みアクセス許可を持つ AMS 自動 IAM プロビジョニング 変更タイプの作成、更新、削除は、ServiceNow Connector と互換性がありません。

## AMS での AMS 自動 IAM プロビジョニングのランタイムチェック

自動 IAM プロビジョニングは、からのチェックを活用し AWS Identity and Access Management Access Analyzer、AMS 境界ポリシーに対して追加のチェックと検証を実行します。AMS は、IAM のベストプラクティス、クラウドでのお客様のワークロードの運用経験、および集合的な AMS IAM 手動評価経験に基づいて、追加のチェックと検証を定義しました。

ポリシーランタイムチェックの結果は、変更リクエスト (RFC) 出力で表示できます。検出結果には、リソース識別子、検出結果を生成したロールやポリシー内の場所、IAM エンティティまたはリソースが合格できなかったことのチェックの概要を示すメッセージが含まれます。これらの検出結果は、機能し、セキュリティのベストプラクティスに準拠するポリシーを作成するのに役立ちます。

### Note

自動 IAM プロビジョニングは、チェックに合格しなかったエンティティまたはポリシー定義内の場所について特定しようとします。タイプに応じて、場所にはリソース名または ARN、または配列内のインデックスが含まれる場合があります。例えば、エンティティまたはポリシーを正常な結果に調整するのに役立つステートメントです。

スムーズな AMS 自動 IAM プロビジョニングエクスペリエンスを得るには、「検証のみ」オプションを使用して、RFC 出力で報告された検証チェックの結果がなくなるまで検証チェックを実行することをお勧めします。検証チェックで検出結果が報告されない場合は、AMS コンソールからコピーの作成を選択して、既存の RFC のコピーをすばやく作成します。プロビジョニングの準備ができたら、「パラメータ」セクションで、検証のみの値を「はい」から「いいえ」に切り替え、続行します。

IAM リソースが安全であることを確認するために AMS 自動 IAM プロビジョニングが実行するランタイムチェックは次のとおりです。



**Note**

これらの自動変更タイプによって拒否されたアクションを含む IAM ポリシーをプロビジョニングするには、RFC カスタマーセキュリティリスク管理 (CSRM) プロセスに従う必要があります。次の変更タイプを使用します: デプロイ | 高度なスタックコンポーネント | Identity and Access Management (IAM) | エンティティまたはポリシーの作成 (マネージドオートメーション) (ct-3dpd8mdd9jn1r)。

- IAM Access Analyzer ポリシーのチェックと検証: [「Access Analyzer ポリシーのチェックリファレンス」](#)と [「IAM Access Analyzer ポリシーの検証」](#) も参照してください。
- AMS アクセス許可の境界ポリシーチェック: デフォルトで拒否される一連のサービスに対するアクション。詳細については、[「自動 IAM プロビジョニングアクセス許可の境界チェック」](#)を参照してください。
- カスタマー定義のアクセス許可の境界ポリシーチェック: 拒否された一連のサービスに対する追加の制限付きアクション。詳細については、[「自動 IAM プロビジョニングアクセス許可の境界チェック」](#)を参照してください。
- AMS 定義のカスタムチェック: リクエストされた IAM エンティティまたはポリシー内のさまざまな安全でないポリシーや過度に寛容なポリシー、またはアクセスパターンを識別し、見つかった場合はリクエストを拒否するチェック。詳細については、[AWS「JSON ポリシー要素: プリンシパル」](#)を参照してください。

| 結果                              | 説明                                                                                                                                                                                                                  |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ロールには、信頼ゾーン外の外部アカウントからアクセスできます。 | この検出結果は、信頼ゾーン外のロール信頼ポリシーにリストされているプリンシパルを指します。信頼ゾーンは、ロールが作成されるアカウントまたはアカウントが属する AWS 組織として定義されます。アカウントまたは同じ AWS Organization に属していないエンティティは外部エンティティです。検出結果を解決するには、プリンシパル ARNs、それらが自分に属していて、AMS オンボードアカウントであることを確認します。 |

| 結果                                                                                                               | 説明                                                                                                                                                                    |
|------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ロールには、AMS 顧客所有アカウント<br><code>Account_ID #####</code><br><code>External_Account_ID</code> が所有する外部エンティティがアクセスできます。 | この検出結果は、ロールの信頼ポリシーに、自分と AMS オンボーディングアカウントが所有していないアカウント ID を持つプリンシパル ARN が含まれている場合に生成されます。この結果を解決するには、ロールの信頼ポリシーからそのようなプリンシパルを削除します。                                   |
| 正規ユーザー ID は、IAM 信頼ポリシーでサポートされているプリンシパルではありません。                                                                   | 正規プリンシパル IDs は IAM 信頼ポリシーではサポートされていません。検出結果を解決するには、ロールの信頼ポリシーからそのようなプリンシパルを削除します。                                                                                     |
| ロールには、信頼ゾーン外の外部ウェブ ID からアクセスできます。                                                                                | この検出結果は、ロール信頼ポリシーが SAML IdP 以外の外部ウェブ ID プロバイダー (IdP) を許可する場合に生成されます。この結果を解決するには、ロールの信頼ポリシーを確認し、 <code>sts:AssumeRoleWithWebIdentity</code> オペレーションを許可するステートメントを削除します。 |
| ロールには SAML フェデレーションを介してアクセスできますが、提供された SAML ID プロバイダー (IdP) は存在しません。                                             | この検出結果は、ロールの信頼ポリシーに、アカウントに存在しない SAML IdP が含まれている場合に生成されます。解決するには、リストされているすべての SAML IdP がアカウントに存在することを確認します。                                                           |

| 結果                                                                                                                                                                                                                                    | 説明                                                                                                                                                                                                                                                                                          |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>ポリシーには、管理者またはパワーユーザーアクセスに相当する特権アクションが含まれています。アクセス許可の範囲を特定のサービス、アクション、またはリソースに減らすことを検討してください。NotAction や NotResource などの高度なポリシー要素を使用する場合は、特に Allow ステートメントで、意図した以上のアクセスを許可していないことを確認してください。</p>                                     | <p>IAM ポリシーでアクセス許可を設定するときに、タスクの実行に必要なアクセス許可のみを付与 AWS Identity and Access Management するのが、のベストプラクティスです。これを行うには、最小特権のアクセス許可とも呼ばれる特定の条件下で特定のリソースに対して実行できるアクションを定義します。この検出結果は、自動化がポリシーが広範なアクセス許可を付与していることを検出し、最小特権の原則に準拠していない場合に生成されます。検出結果を解決するには、アクセス許可を確認して減らします。</p>                        |
| <p>ステートメントには、<i>Service_Name</i> の特権アクションが含まれています。拒否ステートメントを使用してこれらのアクションを除外することを検討してください。特権アクションのリストについては、AMS ドキュメントの境界ポリシーリファレンスを参照してください。</p>                                                                                      | <p>AMS は、特定のサービスの特定のアクションをリスクのあるものとして特定し、顧客セキュリティチームによるさらなるリスクレビューと承認を必要とします。この検出結果は、オートメーションがそのようなアクセス許可を付与する特定のポリシーを検出したときに生成されます。この結果を解決するには、ポリシーでこれらのアクションを拒否します。アクションのリストについては、AMS 境界ポリシーを参照してください。AMS 境界ポリシーの詳細については、「」を参照してください<a href="#">AMS 自動 IAM プロビジョニングアクセス許可の境界チェック</a>。</p> |
| <p>ステートメントは、<i>service_Name</i> の特権 RFC 変更タイプ <a href="#">ct-1n9gfnog5x7fl</a>、<a href="#">ct-1e0xmu y1diafq</a>、<a href="#">ct-17cj84y7632o6</a> へのアクセスを許可します。特定の変更タイプへのアクセス許可の範囲を指定するか、拒否ステートメントを使用してこれらの変更タイプを除外することを検討してください。</p> | <p>この検出結果は、ポリシーが自動 IAM プロビジョニング変更タイプ (CTs。CTs はリスク承諾の対象であり、オンボーディングされたロールを通じてのみ使用する必要があります。したがって、これらの CTs にアクセス許可を付与することはできません。この結果を解決するには、これらの CTs。</p>                                                                                                                                    |

| 結果                                                                                                                                                                          | 説明                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>ステートメントには、service <i>Service_Name</i> のリソースに限定されていない特権アクションが含まれています。アクションを特定のリソースにスコープするか、AMS 名前空間プレフィックスを持つリソースを除外することを検討してください。ワイルドカードを使用する場合は、スコープをリソースに制限してください。</p> | <p>この検出結果は、ポリシーが特定のサービスのリソースにスコープされていない特権アクションを付与した場合に生成されます。ワイルドカードは、多くの場合、アクセス許可の範囲にさまざまなリソースやアクションを取り込む過度に寛容なポリシーを作成します。検出結果を解決するには、所有するリソースへのアクセス許可の範囲を減らすか、AMS 名前空間にあるリソースを除外します。AMS 名前空間プレフィックスのリストについては、AMS ドキュメントの境界ポリシーを参照してください。すべてのプレフィックスがすべてのサービスに適用されるわけではありません。AMS 境界ポリシーの詳細については、「」を参照してください<a href="#">AMS 自動 IAM プロビジョニングアクセス許可の境界チェック</a>。</p> |
| <p>無効なアカウント ID または Amazon リソースネーム (ARN)。</p>                                                                                                                                | <p>この検出結果は、ポリシーまたはロールの信頼ポリシーで指定された ARN またはアカウント ID が無効である場合に生成されます。サービスの有効なリソース ARN のリソースを確認するには、「<a href="#">サービス認可リファレンス</a>」を参照してください。アカウント ID が 12 桁の数字であり、アカウントがアクティブであることを確認します AWS。</p>                                                                                                                                                                    |
| <p>ARN のアカウント ID にワイルドカード (*) を使用することは制限されています。</p>                                                                                                                         | <p>この検出結果は、ARN のアカウント ID フィールドにワイルドカード (*) が指定されている場合に生成されます。アカウント ID フィールドのワイルドカードは任意のアカウントと一致し、リソースに意図しないアクセス許可を付与する可能性があります。これを解決するには、ワイルドカードを特定のアカウント ID に置き換えます。</p>                                                                                                                                                                                         |

| 結果                                                           | 説明                                                                                                                                                                                        |
|--------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Account_ <b>ID</b> を所有する同じ AMS 顧客によって所有されていない指定されたリソースアカウント。 | この検出結果は、リソース ARN で指定されたアカウント ID がユーザーに属しておらず、AMS によって管理されていない場合に生成されます。これを解決するには、すべてのリソース (ポリシーの ARN で指定) が AMS によって管理されているアカウントに属していることを確認します。                                           |
| ロール名は AMS の制限付き名前空間にあります。                                    | この検出結果は、AMS 予約プレフィックスで始まる名前のロールを作成しようとするときに生成されます。これを解決するには、ユースケースに固有のロールの名前を使用します。AMS 予約プレフィックスのリストについては、 <a href="#">「AMS 予約プレフィックス」</a> を参照してください。                                     |
| ポリシー名は AMS の制限付き名前空間にあります。                                   | この結果は、AMS 予約プレフィックスで始まる名前のポリシーを作成しようとするときに生成されます。これを解決するには、ユースケースに固有のポリシーの名前を使用します。AMS 予約プレフィックスのリストについては、 <a href="#">「AMS 予約プレフィックス」</a> を参照してください。                                     |
| ARN のリソース ID は AMS の制限付き名前空間にあります。                           | この検出結果は、AMS 名前空間にある名前付きリソースにアクセス許可を付与するポリシーを作成しようとするときに生成されます。これを解決するには、アクセス許可をリソースにスコープするか、AMS 名前空間にあるリソースへのアクセス許可を拒否してください。AMS 名前空間の詳細については、 <a href="#">「AMS の制限付き名前空間」</a> を参照してください。 |

| 結果                                                                                                                   | 説明                                                                                                                                                                                                                                         |
|----------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>ポリシー変数の大文字と小文字が無効です。変数を <i>Variable_Names</i> に更新します。</p>                                                         | <p>この検出結果は、正しくないケースで IAM グローバルポリシー変数を含むポリシーを作成しようすると生成されます。これを解決するには、ポリシーのグローバル変数に正しい大文字と小文字を使用します。グローバル変数のリストについては、<a href="#">AWS 「グローバル条件コンテキストキー」</a> を参照してください。ポリシー変数の詳細については、<a href="#">「IAM ポリシー要素: 変数とタグ」</a> を参照してください。</p>      |
| <p>ステートメントには、KMS キーの範囲に含まれていない特権アクションが含まれています。これらのアクセス許可を特定のキーにスコープするか、AMS 所有のキーを除外することを検討してください。</p>                | <p>この検出結果は、ポリシーに、所有する特定の KMS キーに限定されていないアクセス許可が含まれている場合に生成されます。これを解決するには、アクセス許可を特定のキーにスコープするか、AMS が所有するキーを除外します。AMS 所有のキーには、特定のエイリアスセットがあります。AMS 所有のキーエイリアスのリストについては、「」を参照してください<a href="#">AMS 自動 IAM プロビジョニングアクセス許可の境界チェック</a>。</p>      |
| <p>ステートメントには、KMS キーエイリアスの範囲に含まれていない特権アクションが含まれています。これらのアクセス許可をキーまたはエイリアスにスコープするか、AMS 所有のキーエイリアスを除外することを検討してください。</p> | <p>この検出結果は、ポリシーに、所有する特定の KMS キーエイリアスに限定されていないアクセス許可が含まれている場合に生成されます。これを解決するには、アクセス許可を特定のキーにスコープするか、AMS が所有するキーを除外します。AMS 所有のキーには、特定のエイリアスセットがあります。AMS 所有のキーエイリアスのリストについては、「」を参照してください<a href="#">AMS 自動 IAM プロビジョニングアクセス許可の境界チェック</a>。</p> |

| 結果                                                                                                                                                                                                        | 説明                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>ステートメントには、 を使用して KMS キーに適切にスコープされていない特権アクションが含まれています <code>kms:ResourceAliases condition</code> 。条件キーに適切なセット演算子とともに、特定のエイリアス名を使用することを検討してください。エイリアス名にワイルドカードを使用する場合は、範囲を KMS キーの限定されたセットに制限してください。</p> | <p>この検出結果は、条件を使用して KMS キーへのアクセス許可をスコープし、 を使用して KMS キーのエイリアスにスコープダウンしない場合 <code>kms:ResourceAliases</code> に生成されます。または、 <code>kms:ResourceAliases</code> 条件キーに AMS 所有の KMS キーエイリアスも含まれる値がある場合。これを解決するには、条件を更新して、KMS キーのエイリアスにのみアクセス許可をスコープダウンするか、AMS 所有の KMS キーのエイリアスを除外します。AMS 所有のキーエイリアスのリストについては、「」を参照してください <a href="#">AMS 自動 IAM プロビジョニングアクセス許可の境界チェック</a>。</p> |
| <p>ロールには <code>customer_deny_policy</code> がアタッチされている必要があります。マネージドポリシー ARN のリストにポリシー ARNs。</p>                                                                                                            | <p>この検出結果は、作成するロールに <code>customer_deny_policy</code> アタッチされていない場合に生成されます。これを解決するには、マネージドポリシー ARN リスト <code>customer_deny_policy</code> に を含めません。 ARNs</p>                                                                                                                                                                                                           |
| <p>AWS 管理ポリシーは過度に許可されているか、AMS 境界ポリシーによって制限されたアクセス許可を付与します。</p>                                                                                                                                            | <p>この検出結果は、ロールの <code>ManagedPolicyArns</code> 値に、関連するサービスへのフルレベルまたは管理者レベルのアクセスを提供する AMS 管理ポリシーが含まれている場合に生成されます。これを解決するには、AWS 管理ポリシーの使用を確認し、スコープダウン許可を提供するポリシーを使用するか、最小特権の原則に従う独自のポリシーを定義します。</p>                                                                                                                                                                    |



| 結果                                                                      | 説明                                                                                                                                                                                                                                     |
|-------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| カスタマー管理ポリシーは、制限された AMS 名前空間にあります。                                       | この検出結果は、名前 AWS 空間に名前のプレフィックスが付いたカスタマー管理ポリシーがロールにアタッチされている場合に生成されます。これを解決するには、ロールの ManagedPolicyArn リストからポリシーを削除します。                                                                                                                    |
| customer_deny_policy をロールからデタッチすることはできません。マネージドポリシー ARN のリストにポリシー ARNs。 | この検出結果は、更新中に customer_deny_policy がロールからデタッチされた場合に生成されます。これを解決するには、ロールの customer_deny_policy ManagedPolicyArns フィールドに を追加して、もう一度試してください。                                                                                               |
| カスタマー管理ポリシーは、AMS 変更管理サービス外または事前検証なしでプロビジョニングされました。                      | この検出結果は、1 つ以上の既存のカスタマー管理ポリシー ARNs がロールにアタッチされていて、ポリシーが AMS 変更管理サービス (RFC) を通じてプロビジョニングされていない場合に生成されます。たとえば、デベロッパーモードまたは直接変更モードを使用すると、お客様は RFC なしで IAM ポリシーをプロビジョニングできます。これを解決するには、ロールの ManagedPolicyArns リストからカスタマー管理ポリシー ARNs を削除します。 |
| 提供された管理ポリシー ARNs の数が、ロールごとのアタッチされたポリシーのクォータを超えています。                     | この検出結果は、ロールにアタッチされた管理ポリシーの総数が、ロールあたりのポリシーのクォータを超えた場合に生成されます。IAM クォータの詳細については、 <a href="#">「IAM および AWS STS クォータ、名前の要件、および文字制限」</a> を参照してください。この情報を使用して、ロールにアタッチするポリシーの数を減らします。                                                         |



| 結果                                                                                                                                                    | 説明                                                                                                                                                                              |
|-------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>信頼ポリシーサイズ ({trust_policy}) が {size} の引き受けロールポリシーサイズのクォータを超えています。</p>                                                                               | <p>この検出結果は、ロールを引き受けるポリシードキュメントのサイズがポリシーサイズのクォータを超えた場合に生成されます。IAM クォータの詳細については、<a href="#">「IAM および AWS STS クォータ、名前の要件、および文字制限」</a>を参照してください。</p>                                |
| <p>ステートメントには、Amazon S3 のすべての変更アクションが含まれます。これらのアクセス許可を必要なアクションのみにスコープすることを検討してください。ワイルドカードを使用する場合は、制限された一連のミュータティブアクションの範囲を指定してください。</p>               | <p>この検出結果は、特定のポリシーが 1 つ以上のリソースに関係なく、すべての Amazon Simple Storage Service ミューテーションアクセス許可を付与した場合に生成されます。これを解決するには、バケットに対して必要な Amazon S3 ミュータティブアクションのみを含めます。</p>                    |
| <p>ステートメントには、Amazon S3 のバケットに対して許可されていない特権アクションが含まれています。これらのアクションを拒否するステートメントを追加することを検討してください。</p>                                                    | <p>この検出結果は、ポリシーが任意のバケットに特権アクションを付与した場合に生成されます。特権アクションのリストについては、「この検出結果を解決<a href="#">AMS 自動 IAM プロビジョニングアクセス許可の境界チェック</a>するには、ポリシーでこれらのアクションを削除または拒否する」を参照してください。</p>           |
| <p>ステートメントには、Amazon S3 のバケットに限定されていない特権アクションが含まれています。バケットを含めるか、AMS 名前空間プレフィックスを持つバケットを除外することを検討してください。ワイルドカードを使用する場合は、名前空間内のバケットと一致することを確認してください。</p> | <p>この検出結果は、ポリシーがバケットに限定されていない Amazon S3 アクションのみを許可する場合に生成されます。これは、バケットリソースを指定するときにワイルドカードを使用する場合によく発生します。これを解決するには、所有しているバケット名または ARNs を指定するか、AMS 名前空間プレフィックスを持つバケットを除外します。</p> |

| 結果                                                                                                                                                                       | 説明                                                                                                                                                                                                                                                                                           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>ステートメントには、Amazon S3 のバケットに限定されていない特権アクションが含まれています。アカウント内のすべてのバケットをスコープするワイルドカード (*) の使用は避けることを検討してください。</p>                                                           | <p>この検出結果は、ポリシーがバケットにスコープされていない Amazon S3 アクションを付与した場合に生成されます。これは、バケットリソースを指定するときにワイルドカードを使用する場合によく発生します。これを解決するには、所有しているバケット名または ARNs を指定するか、AMS 名前空間プレフィックスを持つバケットを除外します。</p>                                                                                                              |
| <p>ステートメントには、存在しないバケットやを所有していないバケットなど、すべての Amazon S3 バケットを対象とするリソースワイルドカードが含まれています。条件と <code>s3:ResourceAccount</code> 条件キーを使用してアクセス許可の範囲を設定することを検討してください。</p>           | <p>この検出結果は、ポリシーがワイルドカードを使用して指定されたバケットにアクセス許可を付与した場合に生成されます。ワイルドカードを使用すると、多くの場合、存在しないバケットや所有者以外のバケットが対象範囲に含まれます。これを解決するには、条件と <code>aws:ResourceAccount</code> 条件キーを使用して、現在のアカウント内のバケットにのみアクセス許可をスコープします。詳細については、<a href="#">「特定の AWS アカウントが所有する Amazon S3 バケットへのアクセスを制限する」</a>を参照してください。</p> |
| <p>ステートメントには <code>NotResource</code> ポリシー要素が含まれており、存在しないバケットや所有していないバケットなど、多数のバケットにスコープできます。条件と <code>s3:ResourceAccount</code> 条件キーを使用してアクセス許可の範囲を設定することを検討してください。</p> | <p>この検出結果は、ポリシーが <code>NotResources</code> ポリシー要素を使用してバケットリソースを指定した場合に生成されます。 <code>NotResource</code> 要素を使用すると、存在しないバケットや所有者ではないバケットなど、多数のバケットがスコープされる可能性があります。これを解決するには、条件と <code>aws:ResourceAccount</code> 条件キーを使用して、現在のアカウント内のバケットにのみアクセス許可をスコープします。</p>                                |

| 結果                                                                                                                                                                                                                                                    | 説明                                                                                                                                                                                                                                                                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>ステートメントには、存在しないバケット、アカウント <code>Account_ID #####</code> <code># Bucket_Name</code> への Amazon S3 アクション、または所有していないバケットや存在しないバケットなど、多数のバケットを対象とする可能性のあるワイルドカードの名前が含まれています。条件と条件キーを使用してアクセス許可の範囲を設定することを検討してください <code>s3:ResourceAccount</code> 。</p> | <p>この検出結果は、ポリシーが、存在しないバケット、ユーザーが所有していないバケット、または多数のバケットをカバーするバケット名にワイルドカードがあり、アクセスが現在のアカウントのみにスコープされていない場合に生成されます。これを解決するには、条件と <code>aws:ResourceAccount</code> 条件キーを使用して、現在のアカウント内のバケットにのみアクセス許可をスコープします。</p>                                                                                 |
| <p>ステートメントには、存在しないバケット、アカウント <code>Account_ID #####</code> <code>Bucket_Name</code> への Amazon S3 アクション、または所有していないバケットや存在しないバケットなど、多数のバケットにスコープされる可能性のあるワイルドカードの名前が含まれています。条件の <code>s3:ResourceAccount</code> または指定されたリソースアカウントを使用してアクセスは制限されません。</p> | <p>この検出結果は、ポリシーが、存在しないバケット、ユーザーが所有していないバケット、または多数のバケットをカバーするバケット名にワイルドカードがあり、アクセスが特定のアカウントのみにスコープされている場合に生成されます。ただし、<code>aws:ResourceAccount</code> 条件キーで指定されたアカウントはユーザーに属さず、AMS によって管理されます。これを解決するには、<code>aws:ResourceAccount</code> 条件キーを更新し、所有していて AMS によって管理されている適切なアカウント ID を設定します。</p> |
| <p>ステートメントには、Amazon EC2 のインスタンスに限定されていない特権アクションが含まれています。アクションを特定のインスタンス ARNs、AMS 名前空間プレフィックスの値を持つ名前タグキーを持つインスタンスを除外することを検討してください。ワイルドカードを使用する場合は、所有している名前空間と一致することを確認してください。</p>                                                                      | <p>この検出結果は、ポリシーが AMS が所有する Amazon EC2 インスタンスに対して特権アクションを付与した場合に生成されます。AMS インスタンスには、AMS 名前空間の値を持つ名前タグキーがタグ付けされます。これを解決するには、<code>StringNotLike</code> 演算子を使用して AMS 名前空間の値を除外する <code>aws:ResourceTag/Name</code> キーを持つ条件を使用して、リソースを指定するか、AMS インスタンスを除外します。</p>                                  |

| 結果                                                                                                                                                                                      | 説明                                                                                                                                                                                                  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>ステートメントには、AWS Systems Manager パラメータストアのリソースに限定されていない特権アクションが含まれています。パラメータの ARNs を指定するか、AMS 名前空間プレフィックスを使用してパラメータを除外することを検討してください。ワイルドカードを使用する場合は、パラメータのみを対象とするようにしてください。</p>         | <p>この検出結果は、ポリシーが所有していないパラメータにアクセス許可を付与した場合に生成されます。これは通常、ワイルドカードが使用されている場合、または AMS 名前空間プレフィックスを持つパラメータがポリシーステートメントのリソースにリストされている場合です。これを解決するには、名前空間内のパラメータを指定するか、拒否ステートメントを使用して AMS パラメータを除外します。</p> |
| <p>ステートメントには、 のリソースに対する特権アクションが含まれています AWS Systems Manager。リソースに対するアクションまたはアクションのみを読み取るためのアクセス許可の範囲を設定することを検討してください。</p>                                                                | <p>この検出結果は、ポリシーが Systems Manager リソースに対してパラメータストアまたは読み取り専用アクション以外のアクセス許可を付与した場合に生成されます。この結果を解決するには、読み取り専用アクションまたはパラメータストアのみのアクセス許可を減らします。</p>                                                       |
| <p>ステートメントには、所有する <i>Service_Name</i> の {message} に限定されていない特権アクションが含まれています。必要に応じて、これらのアクセス許可を特定のリソースタイプにスコープするか、AMS が所有するリソースを除外することを検討してください。ワイルドカードを使用する場合は、####と一致することを確認してください。</p> | <p>この検出結果は、ポリシーがリソース、特に名前付きリソースに対して付与されない特権アクションを許可する場合に生成されます。この結果を解決するには、リソースリストを確認し、それらが名前空間にあるリソースのみをスコープするかどうかを確認します。または、AMS 名前空間にあるリソースを除外します。</p>                                            |

| 結果                                                                                                                                                                                                                                                                                  | 説明                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>ステートメントには、名前タグキーの特定の値にスコープされていない <code>{Service_Name}</code> のタグ付けアクションが含まれています。名前空間の値で <code>aws:RequestTag/Name</code> 条件キーを設定してこれらのアクションの範囲を設定するか、AMS 名前空間プレフィックスの値で <code>StringNotLike</code> 演算子で <code>aws:RequestTag/Name</code> 条件キーを設定してこれらのアクションを制限することを検討してください。</p> | <p>この検出結果は、ポリシーが特定のサービスのタグ付けアクセス許可を付与し、そのアクセス許可が特定のタグキー/値の範囲に含まれていない場合に生成されます。タグアクションで使用するキーまたは値を絞り込むには、たとえば、アクションを実行するようにリクエストするときは、<code>aws:RequestTag/tag key</code> 条件を使用します。したがって、これを解決するには、この条件キーを使用して名前空間のキーまたは値を制限します。または、AMS 名前空間の値を持つ Name タグキー (<code>aws:RequestTag/Name</code>) を拒否します。</p> |
| <p>IAM ロールの信頼ポリシーの検証中に内部エラーが発生しました。</p>                                                                                                                                                                                                                                             | <p>この検出結果は、CT オートメーションが IAM Access Analyzer サービスを介して IAM ロールの信頼ポリシーの検証を実行する際にエラーが発生した場合に生成されます。これを解決するには、RFC を再送信します。エラーが解決しない場合は、AMS オペレーションに連絡してエラーのトラブルシューティングを行います。</p>                                                                                                                               |
| <p>カスタマー管理ポリシーの検証中に内部エラーが発生しました。</p>                                                                                                                                                                                                                                                | <p>この検出結果は、IAM Access Analyzer サービスを介してカスタマー管理ポリシーで楕円化を実行する際に、CT オートメーションでエラーが発生した場合に生成されます。これを解決するには、RFC を再送信します。エラーが解決しない場合は、AMS オペレーションに連絡してエラーのトラブルシューティングを行います。</p>                                                                                                                                  |

| 結果                                                                           | 説明                                                                                                                                                     |
|------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| アクセスアナライザーが に見つかりません <b>AWS #####</b> 。ロール信頼ポリシーのアクセスプレビューチェックを実行できません。      | この検出結果は、IAM Access Analyzer リソースが に見つからない場合に生成されます AWS リージョン。AMS オペレーションに連絡して、AWS リージョンで IAM Access Analyzer リソースのトラブルシューティングと作成を行います。                 |
| Role_ <b>Name</b> ロールの信頼ポリシーが無効です                                            | この検出結果は、指定された IAM ロールに無効な信頼ポリシーが含まれている場合に生成されます。解決するには、信頼ポリシーを確認して、そのポリシーが有効であることを確認します。                                                               |
| IAM Access Analyzer で内部エラーが発生しました。Role_ <b>Name</b> ロールのアクセスプレビューを作成できませんでした | この検出結果は、IAM Access Analyzer を使用してロールのアクセスプレビューを作成中にオートメーションでエラーが発生した場合に生成されます。これを解決するには、RFC を再送信します。エラーが解決しない場合は、AMS オペレーションに連絡してエラーのトラブルシューティングを行います。 |
| Role_ <b>Name</b> ロールの信頼ポリシーのアクセスプレビューを作成できませんでした                            | この検出結果は、IAM Access Analyzer を使用してロールのアクセスプレビューを作成中にオートメーションでエラーが発生した場合に生成されます。これを解決するには、RFC を再送信します。エラーが解決しない場合は、AMS オペレーションに連絡してエラーのトラブルシューティングを行います。 |

| 結果                                                   | 説明                                                                                                                                                    |
|------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| リストされた SAML IdP の検証中に内部エラーが発生しました。                   | この検出結果は、ロール信頼ポリシーにリストされている指定された SAML IdPs の検証中にオートメーションでエラーが発生した場合に生成されます。これを解決するには、RFC を再送信します。エラーが解決しない場合は、AMS オペレーションに連絡してエラーのトラブルシューティングを行います。    |
| アクセス許可の検証に関する内部エラー AWS Key Management Service。       | この検出結果は、提供されたポリシーで AWS KMS キーアクセス許可の検証中にオートメーションでエラーが発生した場合に生成されます。これを解決するには、RFC を再送信します。エラーが解決しない場合は、AMS オペレーションに連絡してエラーのトラブルシューティングを行います。           |
| リストされた管理ポリシー ARNs を検証する内部エラー。                        | この検出結果は、リストされた管理ポリシー ARNs。これを解決するには、RFC を再送信します。エラーが解決しない場合は、AMS オペレーションに連絡してエラーのトラブルシューティングを行います。                                                    |
| デフォルトのcustomer_deny_policy アタッチメントの検証中に内部エラーが発生しました。 | この検出結果は、customer_deny_policy がロールにアタッチされていることの検証中にオートメーションでエラーが発生した場合に生成されます。これを解決するには、RFC を再送信します。エラーが解決しない場合は、AMS オペレーションに連絡してエラーのトラブルシューティングを行います。 |
| Role_ <i>Name</i> ロールのマネージドポリシー ARN の検証の内部エラー        | この検出結果は、ロールのマネージドポリシー ARNsに生成されます。これを解決するには、RFC を再送信します。エラーが解決しない場合は、AMS オペレーションに連絡してエラーのトラブルシューティングを行います。                                            |



| 結果                                                                                                                                                   | 説明                                                                                                                                                                                                            |
|------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ユーザー定義の境界ポリシーに対する <b>Policy_name</b> の検証の内部エラー<br>AWSManagedServicesIAMProvisionCustomerBoundaryPolicy                                               | この検出結果は、カスタム拒否リストを含むポリシーの検証中にオートメーションでエラーが発生した場合に生成されます。これを解決するには、RFC を再送信します。エラーが解決しない場合は、AMS オペレーションに連絡してエラーのトラブルシューティングを行います。                                                                              |
| カスタマー定義の境界ポリシーAWSManagedServicesIAMProvisionCustomerBoundaryPolicy がアカウントに存在する。ただし、ポリシーには、アクセス許可を付与する許可ステートメントが含まれています。ポリシーには拒否ステートメントのみを含める必要があります。 | この検出結果は、カスタム拒否リストを含むポリシーに、アクセス許可を付与するステートメントが含まれている場合に生成されます。カスタム拒否リストは IAM 管理ポリシーとしてアカウント内に存在しますが、アクセス許可管理には使用できません。ポリシーには、AMS 自動 IAM プロビジョニングが作成する IAM ポリシーでそれらのアクションを検証および拒否することを示す拒否ステートメントのみを含める必要があります。 |
| ステートメントには、 <b>Service_Name</b> の組織によって定義された特権アクションが含まれています。拒否ステートメントを使用してこれらのアクションを除外することを検討してください。制限付きアクションのリストを参照するには、アカウントで という名前のポリシーを参照してください。  | この検出結果は、カスタム拒否リストで定義したポリシー内のアクションをオートメーションが検出したときに生成されます。検出結果を解決するには、ポリシーステートメントを確認し、カスタム拒否リストで定義されているアクションを削除するか、それらのアクションを拒否する拒否ステートメントを追加します。                                                              |
| ロールには <b>POLICY_ARN</b> がアタッチされている必要があります。マネージドポリシー ARN のリストにポリシー ARNs。                                                                              | この検出結果は、作成するロールに <b>POLICY_ARN</b> がアタッチされていない場合に生成されます。これを解決するには、ロールの ManagedPolicyArns フィールドに <b>POLICY_ARN</b> を含めて、もう一度試してください。                                                                           |



| 結果                                                                          | 説明                                                                                                                                               |
|-----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| <b><i>POLICY_ARN</i></b> をロールからデタッチすることはできません。マネージドポリシー ARN のリストにポリシー ARNs。 | この検出結果は、更新中に <b><i>POLICY_ARN</i></b> がロールからデタッチされた場合に生成されます。これを解決するには、ロールの ManagedPolicyArns フィールドに <b><i>POLICY_ARN</i></b> を追加して、もう一度試してください。 |

## AMS 自動 IAM プロビジョニングアクセス許可の境界チェック

AMS アクセス許可の境界チェックは、AMS が提供するデフォルトのアクセス許可の境界ポリシーに準拠するのに役立ちます。このポリシーは、AMS 自動 IAM プロビジョニングによって拒否されたアクションのリストです。これらの制限されたアクションを含むプロビジョニングポリシーには、追加の明示的なリスク承諾が必要です。ポリシーをここでダウンロードします: [boundary-policy.zip](#)。

カスタマー定義のアクセス許可境界ポリシーチェックを使用して、AMS アクセス許可境界ポリシーのデフォルトを超える拒否アクションをカスタマイズします。次の変更タイプを使用して AMS 自動 IAM プロビジョニングにオンボードする場合: 管理 | マネージドアカウント | 読み取り/書き込みアクセス許可を持つ AMS 自動 IAM プロビジョニング | [有効化 \(マネージドオートメーション\)](#) (ct-1706xvvk6j9hf)、追加の制限付きアクションを指定するカスタム拒否アクションのリストを含めることができます。

拒否アクションのリストは、次の変更タイプを使用して更新できます。管理 | マネージドアカウント | 読み取り/書き込みアクセス許可による自動 IAM プロビジョニング | [カスタム拒否リストの更新](#) (ct-2r9xvd3sdsic0)。この変更タイプ AWSManagedServicesIAMProvisionAdminRole を実行するには、専用の IAM ロールを使用する必要があります。

### Note

- 更新ごとに拒否アクションの包括的なリストを提供する必要があります。前のリストは新しいリストに置き換えられます。
- 拒否アクションのリストには、拒否するアクションのみを含める必要があります。許可アクションはサポートされていません。
- 拒否アクションのリストは、という名前の IAM 管理ポリシーとしてアカウント内にあります AWSManagedServicesIAMProvisionCustomerBoundaryPolicy。ポリシーをロールにアタッチすることはできません。

- AMS 自動 IAM プロビジョニングで拒否されたアクションを示すために使用されるアクセス許可の境界という用語は、IAM アクセス許可の境界とは異なるコンテキスト上の意味を持ちます。IAM アクセス許可の境界は、ポリシーが実行時に IAM エンティティに付与できるアクセス許可の上限を設定します。IAM アクセス許可の境界の詳細については、AWS Identity and Access Management 「ユーザーガイド」の「[ポリシータイプ](#)」を参照してください。AMS 自動 IAM プロビジョニングのアクセス許可の境界により、アクションの拒否リストなど、特定のアクセス許可のセットを含む IAM ポリシーをプロビジョニングできなくなります。

## AMS 自動 IAM プロビジョニングのフェンディングとエラーのトラブルシューティング

AMS 自動 IAM プロビジョニングを使用する際に問題が発生する方法は 3 つあります。

- RFC エラー: これらは、誤った入力など、さまざまな理由で発生する可能性があります。詳細については、「[AMS での RFC エラーのトラブルシューティング](#)」を参照してください。
- SSM エラー: フォーマットが悪いなど、さまざまな理由で発生する可能性があります。詳細については、「[Systems Manager Automation のトラブルシューティング](#)」を参照してください。
- 検証チェックの検出結果: 自動 IAM プロビジョニングが実行する多数の検証チェックのいずれかで問題が見つかった場合に発生します。検証チェックのリストと修正すべき推奨アクションについては、「」を参照してください[AMS での AMS 自動 IAM プロビジョニングのランタイムチェック](#)。

## IAM ロールとプロファイルを使用した AMS でのアクセス許可の設定

AMS は AWS Identity and Access Management (IAM) を使用して、ユーザー、アクセスキーなどのセキュリティ認証情報、およびユーザーとアプリケーションがアクセスできるリソースを制御する AWS アクセス許可を管理します。AMS は、デフォルトの IAM ユーザーロールとデフォルトの Amazon EC2 インスタンスプロファイル (デフォルトの IAM ユーザーロールへのリソースアクセスを許可するステートメントを含む) を提供します。

### 新しい IAM ユーザーロールまたはインスタンスプロファイルのリクエスト

AMS は IAM ロールを使用して、フェデレーションサービスと IAM インスタンスプロファイルを通じてその IAM ロールのコンテナとしてユーザーアクセス許可を設定します。

デプロイ | 高度なスタックコンポーネント | Identity and Access Management (IAM) | Create entity or policy (マネージドオートメーション) change type (ct-3dpd8mdd9jn1r)、または Management | Applications | IAM インスタンスプロファイル | Create Management | Applications | IAM インスタンスプロファイル | Create (マネージドオートメーション) change type (ct-0ixp4ch2tiu04) を使用して IAM インスタンスプロファイルをリクエストできます。このセクションの各 の説明を参照してください。

#### Note

AMS には、危険な名前空間とアクションをブロック customer\_deny\_policy する IAM ポリシーがあります。このポリシーはデフォルトですべての AMS カスタマーロールにアタッチされ、ユーザーにとって問題になることはほとんどありません。IAM ユーザーとロールのリクエストにはこのポリシーは含まれませんが、IAM ロールのリクエスト customer\_deny\_policy に を自動的に含めることで、AMS は新しい IAM インスタンスプロファイルをより迅速にデプロイできます。customer\_deny\_policy ポリシーの除外をリクエストできます。ただし、このリクエストは重いセキュリティレビューを受け、セキュリティ上の理由から拒否される可能性があります。

## IAM ロールポリシーステートメントを使用してアクセス許可を制限する

AMS は IAM ロールを使用して、フェデレーションサービスを通じてユーザーアクセス許可を設定します。

単一アカウントランディングゾーン AMS: [「SALZ: デフォルトの IAM ユーザーロール」](#) を参照してください。

マルチアカウントランディングゾーン AMS: [「MALZ: デフォルトの IAM ユーザーロール」](#) を参照してください。

IAM ロールは、AWS サービスリクエストを行うための一連のアクセス許可を定義する IAM エンティティです。IAM ロールは、特定のユーザーまたはグループに関連付けられていません。代わりに、信頼されたエンティティは、IAM ユーザー、アプリケーション、Amazon EC2 などの AWS サービスなどのロールを引き受けます。詳細については、[「IAM ロール」](#) を参照してください。

Policy リクエストフィールドでより制限の厳しい IAM ポリシーを渡すことで、AWS Security Token Service (STS) API オペレーション [AssumeRole](#) を使用して、AMS IAM ユーザーロールを引き受けるユーザーに必要なポリシーの範囲を絞り込むことができます。

次に、CT アクセスを制限するために使用できるポリシーステートメントの例を示します。

設定した Active Directory (AD) グループと AWS Security Token Service (STS) API オペレーション [AssumeRole](#) を使用して、特定の変更タイプ (CTs) へのアクセスの制限など、特定のユーザーまたはグループのアクセス許可を設定できます。以下に示すポリシーステートメントを使用して、さまざまな方法で CT アクセスを制限できます。

すべての AMS API コール (amscm および amsskms) およびすべての変更タイプへのアクセスを許可するデフォルトの IAM インスタンスプロファイルの AMS 変更タイプステートメント:

```
{
  "Sid": "AWSManagedServicesFullAccess",
  "Effect": "Allow",
  "Action": [
    "amscm:*",
    "amsskms:*"
  ],
  "Resource": [
    "*"
  ]
}
```

1. 指定された 2 つの CTs 「アクション」は AMS API オペレーション ( amscmまたは amsskms) で、「リソースIDs とバージョン番号を表します。

## JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "amscm:*",
      "Resource": [
        "arn:aws:amscm:*:*:changetype/ct-ID1:1.0",
        "arn:aws:amscm:*:*:changetype/ct-ID2:1.0"
      ]
    }
  ]
}
```

2. 指定された 2 つの CTs でのみ CreateRfc、UpdateRfc、および SubmitRfc へのアクセスを許可するステートメント:

3. 使用可能なすべての CTs で CreateRfc、UpdateRfc、および SubmitRfc へのアクセスを許可するステートメント:
4. 制限付き CT に対するすべてのアクションのアクセスを拒否し、他の CTs で許可するステートメント:

## Amazon EC2 IAM インスタンスプロファイルを使用してアクセス許可を制限する

IAM インスタンスプロファイルは、インスタンスの起動時にロール情報を Amazon EC2 インスタンスに渡すために使用できる IAM ロールのコンテナです。

現在、インスタンスにログインするユーザーではなく `customer-mc-ec2-instance-profile`、インスタンスで実行されているアプリケーションにアクセス許可を付与する AWS Managed Services (AMS) のデフォルトインスタンスプロファイル が 1 つあります。インスタンスに何かへのアクセス権を付与する場合は、他のインスタンスにもアクセス権を付与せずに、デフォルトのインスタンスプロファイルを変更したり、新しいインスタンスプロファイルを作成したりできます。Management | Applications | IAM インスタンスプロファイル | Create change type (ct-0ixp4ch2tiu04) を使用して、新しい IAM インスタンスプロファイルをリクエストできます。RFC を送信するときは、独自のインスタンスプロファイルを構成して InstanceProfileDescription として含めるか、AMS に (同じフィールドを使用して) 必要な変更を通知するだけで済みます。これは手動 CT であるため、AMS は変更を承認する必要があるため、それについて連絡します。

Amazon IAM ポリシーに慣れていない場合は、[「IAM ポリシーの概要」](#)で重要な情報を参照してください。良いブログ記事[Amazon EC2 リソースレベルのアクセス許可をわかりやすくする](#)もあります。AMS は現在リソースベースのアクセスコントロールをサポートしていませんが、IAM ロールポリシーを使用したリソースレベルのコントロールをサポートしていることに注意してください (違いについては、[AWS 「IAM と連携するサービス」](#)を参照してください)。

単一アカウントランディングゾーン AMS :

デフォルトの AMS IAM インスタンスプロファイルが付与するアクセス許可の表を確認するには、[EC2 IAM インスタンスプロファイル](#)」を参照してください。

## AD FS クレームルールと SAML 設定

AWS マネージドサービス (AMS) の ActiveDirectory フェデレーションサービス (AD FS) クレームルールと SAML 設定 AWS Managed Services

AD FS をインストールして設定する方法のstep-by-stepについては、[「Windows Active Directory、ADFS、および SAML 2.0 を使用した AWS へのフェデレーションの有効化」](#)を参照してください。

## ADFS クレームルールの設定

ADFS 実装が既にある場合は、以下を設定します。

- 信頼する相手の信頼
- クレームルール

証明書利用者の信頼とクレームのルールステップは、[Windows Active Directory、AD FS、および SAML 2.0 ブログ](#)を使用して AWS へのフェデレーションを有効にするから実行します。

- クレームルール:
  - Nameid: ブログ投稿ごとの設定
  - RoleSessionName: 次のように設定します
    - クレームルール名: **RoleSessionName**
    - 属性ストア: **Active Directory**
    - LDAP 属性: **SAM-Account-Name**
    - 送信クレームタイプ: **https://aws.amazon.com/SAML/Attributes/RoleSessionName**
    - AD グループの取得: [ブログ投稿](#)ごとの設定
    - ロールクレーム: 次のように を設定します。

```
c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-([\d]{12})-"]
```

```
=> issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value =  
  RegExReplace(c.Value, "AWS-([\d]{12})-", "arn:aws:iam:$1:saml-provider/  
customer-readonly-saml,arn:aws:iam:$1:role/"));
```

## ウェブコンソール

[*ADFS-FQDN*] を ADFS 実装の FQDN に置き換えることで、AWS ウェブコンソールにアクセスできます。

`https://[ADFS-FQDN]/adfs/ls/IdpInitiatedSignOn.aspx`

IT 部門は、グループポリシーを介して上記のリンクをユーザー母集団にデプロイできます。

## SAML による API および CLI アクセス

SAML を使用して API および CLI アクセスを設定する方法。

Python パッケージは、以下のブログ記事から入手できます。

- NTLM: [SAML 2.0 と AD FS を使用してフェデレーティッド API と CLI アクセスを実装する方法](#)
- フォーム: [SAML 2.0 を使用してフェデレーティッド API/CLI アクセスの一般的なソリューションを実装する方法](#)
- PowerShell: [Windows PowerShell を使用して AWS へのフェデレーティッド API アクセスをセットアップする方法](#)

## スクリプト設定

1. Notepad++ を使用して、デフォルトのリージョンを正しいリージョンに変更する
2. Notepad++ を使用して、テスト環境と開発環境の SSL 検証を無効にする
3. Notepad++ を使用して idpentryurl を設定する

```
https://[ADFS-FQDN]/adfs/ls/IdpInitiatedSignOn.aspx?  
loginToRp=urn:amazon:webservices
```

## Windows 設定

以下に、Python パッケージの手順を示します。生成された認証情報は 1 時間有効です。

1. [Python をダウンロードしてインストールする \(2.7.11\)](#)
2. [AWS CLI ツールをダウンロードしてインストールする](#)
3. AMS CLI をインストールします。



- a. Cloud Service Delivery Manager (CSDM) が提供する AMS 頒布可能ファイルをダウンロードして解凍します。

いくつかのディレクトリとファイルが利用可能になりました。

- b. オペレーティングシステムに応じて、Managed Cloud Distributables -> CLI -> Windows または Managed Cloud Distributables -> CLI -> Linux / MacOS ディレクトリを開きます。

Windows の場合は、適切なインストーラを実行します (この方法は Windows 32 または 64 ビットシステムでのみ機能します)。

- 32 ビット: ManagedCloudAPI\_x86.msi
- 64 ビット: ManagedCloudAPI\_x64.msi

Mac/Linux の場合は、MC\_CLI.sh という名前のファイルを実行します。これを行うには、次のコマンドを実行します: sh MC\_CLI.sh。amscm および amsskms ディレクトリとその内容は、MC\_CLI.sh ファイルと同じディレクトリにある必要があります。

- c. 企業の認証情報を AWS とのフェデレーション (AMS デフォルト設定) 経由で使用する場合は、フェデレーションサービスにアクセスできる認証情報管理ツールをインストールする必要があります。例えば、この AWS セキュリティブログ [How to Implement Federated API and CLI Access Using SAML 2.0 and AD FS](#) を使用して、認証情報管理ツールの設定に役立てることができます。
- d. インストール後、aws amscm help と aws amsskms help を実行してコマンドとオプションを表示します。

#### 4. 必要な SAML スクリプトをダウンロードする

c:\aws\scripts にダウンロードする

#### 5. [PIP のダウンロード](#)

c:\aws\downloads にダウンロードする

#### 6. PowerShell を使用して PIP をインストールする

```
<pythondir>.\python.exe c:\aws\downloads\get-pip.py
```

#### 7. PowerShell を使用して boto モジュールをインストールする

```
<pythondir\scripts>pip install boto
```

#### 8. PowerShell を使用してリクエストモジュールをインストールする



```
<pythondir\scripts>pip インストールリクエスト
```

9. PowerShell を使用してリクエストセキュリティモジュールをインストールする

```
<pythondir\scripts>pip インストールリクエスト [セキュリティ]
```

10. PowerShell を使用して beautifulsoup モジュールをインストールする

```
<pythondir\scripts>pip install beautifulsoup4
```

11. PowerShell を使用して、ユーザープロファイルに .aws という名前のフォルダを作成します (%userprofile%\.aws)。

```
mkdir .aws
```

12. PowerShell を使用して、.aws フォルダに認証情報ファイルを作成します。

```
New-Item 認証情報 - タイプのファイル -force
```

認証情報ファイルにはファイル拡張子を付けることはできません

ファイル名はすべて小文字で、名前認証情報が必要です

13. メモ帳を使用して認証情報ファイルを開き、正しいリージョンを指定して次のデータに貼り付けます。

```
[default]
output = json
region = us-east-1
aws_access_key_id =
aws_secret_access_key =
```

14. PowerShell を使用した SAML スクリプトとログイン

```
<pythondir>.\python.exe c:\aws\scripts\samlapi.py
```

ユーザー名: [USERNAME]@upn

引き受けるロールを選択する

## Linux 設定

生成された認証情報は 1 時間有効です。

1. WinSCP を使用して SAML スクリプトを転送する
2. WinSCP を使用してルート CA 証明書を転送する (テストと開発には無視)
3. 信頼できるルート証明書に ROOT CA を追加する (テストと開発には無視)

```
$ openssl x509 -inform der -in [certname].cer -out certificate.pem (テストと開発では無視)
```

certificate.pem の内容を /etc/ssl/certs/ca-bundle.crt ファイルの末尾に追加する ((テスト開発では無視)

4. home/ec2-user 5 に .aws フォルダを作成する

```
[default]
output = json
region = us-east-1
aws_access_key_id =
aws_secret_access_key =
```

5. WinSCP を使用して認証情報ファイルを .aws フォルダに転送する
6. boto モジュールをインストールする

```
$ sudo pip install boto
```

7. リクエストモジュールをインストールする

```
$ sudo pip インストールリクエスト
```

8. beautifulsoup モジュールをインストールする

```
$ sudo pip install beautifulsoup4
```

9. スクリプトを home/ec2-user にコピーする

必要なアクセス許可を設定する

スクリプトを実行します: samlapi.py

## ネットワーク ACL で制限する

ネットワークアクセスコントロールリスト (NACL) は、1 つ以上のサブネットに出入りするトラフィックを制御するファイアウォールとして機能する VPC 用のオプションのセキュリティレイヤーです。セキュリティの追加レイヤーを VPC に追加するには、セキュリティグループと同様のルー

ルを指定したネットワーク ACL をセットアップできます。セキュリティグループとネットワーク ACLs [「セキュリティグループとネットワーク ACLs」](#) を参照してください。

ただし、AMS マネージドマルチアカウントランディングゾーンでは、AMS がインフラストラクチャを効果的に管理およびモニタリングするために、NACLs されます。

- NACLs は、管理アカウント、ネットワーク、共有サービス、ログ記録、セキュリティなどのマルチアカウントランディングゾーンコアアカウントではサポートされていません。
- NACLs は、「拒否」リストとしてのみ使用され、AMS のモニタリングおよび管理オペレーションを許可する「すべてを許可」がある限り、マルチアカウントランディングゾーンアプリケーションアカウントでサポートされます。

大規模なマルチアカウント環境では、一元化されたエグレスファイアウォールなどの機能を活用して AMS マルチアカウントランディングゾーンのアウトバウンドトラフィックや AWS Transit Gateway ルーティングテーブルを制御し、VPCs 間でネットワークトラフィックを分離することもできます。

## Outposts での AMS

[AWS Outposts](#) は、AMS マネージドランディングゾーンをカスタマーデータセンターに拡張するマネージドハードウェアソリューションです。AMS のサポートにより AWS Outposts、AMS が提供するクラウドの専門知識、コスト削減、標準化されたプラットフォームを求めるお客様は、内部でのリソースのホスティングに制限されなくなりました AWS リージョン。AMS をオンにすると AWS Outposts、オンプレミスの要件を持つお客様は、AMS が提供するパッチ適用、バックアップ AWS、プロビジョニング、インシデント管理、ビジネス継続性、コスト最適化サービスを活用しながら、をモダナイズできるようになりました。

AMS マルチアカウントランディングゾーンまたはシングルアカウントランディングゾーンアカウントで AWS Outposts がアクティブ化されたら、既存の AMS 変更管理プロセスに従って AWS リソースをプロビジョニングおよび管理できます。AMS がホストするインフラストラクチャは、AWS Outposts 特定の subnet を指定することで管理できます。AWS Outposts ライフサイクルは、AWS Outposts セルフプロビジョニングサービスロールを使用して AWS Outposts コンソールで直接管理できます。

ロールの詳細については、「」を参照してください [AWS Outposts](#)。

## AWS Outposts インストールと運用管理

AWS Outposts プロセスでの AMS へのオンボーディングは、以下で構成されます。

1. Outposts の計画
2. 注文の検証
3. Outposts の AMS へのオンボーディング
4. ライフサイクル管理

## AWS Outposts 計画

AWS Outposts 計画中に、AWS Outposts ユースケースに関する AMS を特定し、AMS アカウントチームや AWS Outposts 担当者などの主要な利害関係者を関与させて、キャパシティ戦略に合わせます。

1. で AMS を必要とするユースケース AWS Outposts を特定したら、AMS アカウントチームと協力してキャパシティプランニングについて話し合います。
2. AWS Outposts キャパシティ要件が決定されると、AMS アカウントチームは AWS Outposts サービスチームと協力して AWS Outposts オンボーディング計画、役割と責任について話し合います。この間、AWS Outposts 単一連絡先 (SPOC) が割り当てられます。AWS Outposts SPOC は AWS Outposts 、サイズ要件の確定に役立ちます。

## AWS Outposts 注文の検証

注文の検証中に、AWS Outposts サイトを作成し、必要な容量を AWS Outposts コンソールまたは AWS Outposts アカウント担当者から直接注文します。

AMS アカウントチームの調整 AWS Outposts が完了したら、変更タイプ ID ct-3qe6io8t6jtny を使用してセルフプロビジョニングサービスロールをリクエスト AWS Outposts し、AWS Outposts コンソールでサイト AWS Outposts を作成して直接注文できます。

または、AWS Outposts SPOC を使用して Outpost サイトと注文を作成することもできます。AWS Outposts SPOC は、サイトと注文の検証と AWS Outposts インストール中に、ユーザーと AMS アカウントチームにステータスの更新を提供し続けます。

## AWS Outposts AMS へのオンボーディング

AMS マネージド VPC で AWS Outposts ユニットがアクティブ化されると、Outposts ハードウェアの可用性、容量、例外、ネットワーク接続を追跡するためにモニターの作成をリクエストできます。次に説明するモニタリングデプロイのステップに従うことで、AWS Outposts ハードウェアは AMS によってアクティブにモニタリングされます。

1. AWS Outposts をインストールしてアクティブ化したら、管理 | その他 | その他 | 作成 (ct-1e1xtak34nx76) 変更タイプを使用して RFC で次のテンプレートを送信することで、AWS Outposts固有のモニタリングをリクエストできます。AMS オペレーションにより、AWS Outposts サブネットが AMS 内部ツールで追跡されます。
  - AWS Outposts ID
  - Subnet CIDR
  - 推奨される AWS Outposts アラーム :
    - InstanceFamilyCapacityAvailabilityAlert
    - InstanceTypeCapacityAvailabilityAlert
    - EBSVolumeTypeCapacityAvailabilityAlert
    - CapacityExceptionsAlert
    - Direct Connect ConnectionAlert
  - 上記のアラートごとに、次のパラメータを指定します。
    - 統計 (「平均」が推奨されます。その他のオプションには、合計、最大、最小、サンプル数、p90 などがあります )
    - 期間 (「5 分」を推奨します。その他のオプションには、10 秒と 30 秒、1、5、15 分、1 時間と 6 時間、1 日があります )
    - しきい値タイプ (「Static」が推奨されます。「異常」もオプションです。)
    - 条件 (「呼び出し回数がより大きい場合」、「等しい」、「未満」もオプションです )。
    - 条件値 ("25%" はデフォルトで設定されています。もう 1 つの正の整数を使用できます。)
    - 通知トピック (AMS オペレーショントピックは自動的に割り当てられます。ただし、他のトピックやカスタムトピックを追加することもできます )。
2. モニタリングとオペレーションのサポート
  - AMS オペレーションは、ネットワークの切断やコンポーネントの障害に関する AWS Outposts メトリクスをモニタリングします。AMS オペレーションは、AWS Outposts 問題に対する最初の対応サービスを提供し、必要に応じて Premium サポートまたは EC2 サポートにエスカレーションします。
  - AMS オペレーションは、AWS Outposts ユニットに関連する問題に対処するために使用できません。
3. EC2 インスタンスのステータスまたはシステムステータスチェックが失敗すると、AMS オペレーションは既存のプロセスに従ってインスタンスをオンラインに戻します。再起動が失敗した場合、または AWS Outposts 容量が不十分な場合、AMS オペレーションチームのメンバーが次のステップを決定するために直接通知します。

## AWS Outposts ライフサイクル管理

AWS Outposts が AMS アカウントにオンボーディングされると、可用性、容量、またはネットワーク例外が発生した場合に通知されます。コンソールまたは AWS Outposts SPOC AWS Outposts から直接 AWS Outposts 廃止できます。

AWS Outposts セルフサービスプロビジョニングサービスロールまたは開発者モードを使用して、AWS Outposts コンソールで AWS Outposts 直接 を管理できます。CSDM または AWS Outposts 単一連絡先 (SPOC) AWS Outposts を通じてリクエストすることもできます。

の高可用性は、2 つ以上の をデプロイすることで実現 AWS Outposts できます AWS Outposts。2 つ以上の を設定すると、Amazon Relational Database Service インスタンスのマルチアベイラビリティゾーンオプション AWS Outposts が有効になります。

## での AMS マネージドリソースのプロビジョニング AWS Outposts

AMS アカウント AWS Outposts ( 単一アカウントランディングゾーン、マルチアカウントランディングゾーン、高速化アカウント) でホストされている AWS リソース (Amazon EC2、Amazon EMR、Amazon EKS、Amazon ECS、Amazon EBS、Amazon S3 など) のプロビジョニングには、のリソースと同じ AMS サポートレベルが適用されます AWS リージョン。AMS 変更管理、セルフサービスプロビジョニングサービス、または開発者モードを使用して、 で作成されたリソースを作成および変更できます AWS Outposts。

現在、すべてのインスタンスタイプ (M5/M5d、C5/C5d、R5/R5d、I3en、G4dn)、Amazon Elastic Block Store、Amazon Elastic Container Service、Amazon Elastic Kubernetes Service、Amazon EMR、Amazon Relational Database Service DBsApplication Load Balancer、App Mesh Envoy プロキシが で直接利用できます AWS Outposts。これらのリソースは、既存のリージョンのリソースと同じ AMS オペレーションサポートの対象となります。

## での AMS の制限 AWS Outposts

- AWS Outpostsホストされたリソースの運用サポートは、一貫したネットワーク接続に依存します。AWS Outposts ネットワークの切断により、AMS オペレーションは切断された AWS Outposts ユニットで発生したインシデントや問題をトラブルシューティングできなくなります。サービスレベルの緊急事態に関する AWS Outposts AMS については、更新された[AWS サービスレベルアグリーメント \(SLAs\)](#)を参照してください。
- Amazon Relational Database Service:
  - RDS 変更タイプの作成 (ct-2z60dyvto9g6c) は、デフォルトでマルチ AZ を有効にし、DB サブネットグループを必要とします。DB サブネットグループには、2 つの別々のアベイラビリティゾーンが必要です。



ティーゾーン (AZ) に 2 つのサブネットが必要です。が 1 つの AZ にのみ AWS Outposts 割り当てられているため AWS Outposts、DB サブネットグループの作成は問題です。この制限を回避するには、次の手順に従います。

1. 管理 | その他 | その他の CT を使用して RFC を介して DB サブネットグループをリクエストし、 でサブネットを指定します AWS Outposts。
  2. RDS をデプロイするカスタム CFN テンプレートを作成し AWS Outposts、前のステップで作成したサブネットグループを指定します。これを行う方法の詳細については、[「カスタムリソース」](#)を参照してください。
  3. AMS がターゲット RDS インスタンスを含む CFN テンプレートを AMS CFN 取り込み CT (ct-36cn2avfrj9v) を介してデプロイするようにリクエストします。
  4. 現在、RDS for AWS Outposts は RDS Service の制限によりメトリクスとログを提供しないことに注意してください。
- ワークロード取り込み (WIGs: Linux WIGsは、WIGs EC2 インスタンスがAWS Outposts サブネット以外にある場合にのみ機能します。これは、Linux WIGsデフォルトで m4.large を使用して最初の EC2 インスタンスのサブネットに WIGs ノードを作成するためです。AWS Outposts にはそのインスタンスタイプがないため、WIGs はワーカーノードを起動できません。この問題の回避策は、AWS Outposts 非サブネットに最初の EC2 インスタンスを作成してから、ターゲットインスタンスを作成できます AWS Outposts。さらに、現在、CC5, C5d, M5, M5d, R5, R5d, G4, I3en などの Nitro ベースの EC2 インスタンスタイプのみがサポートされています AWS Outposts。
  - Amazon Elastic Block Store (EBS): EBS ボリューム CT (ct-16xg8qguovg2w) の作成は機能しません。これは、AWS Outposts Amazon リソース番号 (ARN) を CT の入力パラメータとして提供しないため AWS 、ボリュームが で作成される AWS Outposts ためです。
  - ネットワーク接続: ネットワーク接続は AWS Outposts チームごとにお客様の責任となります。
  - ブラウンフィールドとアカウント乗っ取り: 非 AMS アカウントで AWS Outposts アクティブ化された は、AWS Outposts 請求およびエンタープライズサポート要件の性質上、AMS に移行できません。

## AWS Outposts コンプライアンスに関する AMS

### AWS Outposts コンプライアンス認証に関する AMS

AWS Outposts コントロールプレーンは、HIPAA 対応、PCI、および ISO に準拠していることが証明されています。ただし、AWS Outposts コントロールプレーンの AMS は認証されていませ

ん AWS Outposts。このため、お客様は 環境でコンプライアンス認証 AMS AWS Outposts を追求することをお勧めします。

Outpost ユニットでのリソース作成を制御するには、標準の AMS マネージドアカウントでの過剰な開発者アクセスを防ぐために、Outpost への開発者アクセスを分離することをお勧めします。

## FedRAMP コンプライアンスを必要とする AMS マネージドワークロード

何よりも、コントロールプレーンデータは から AMS 管理アカウントに流出するため、AMS AWS Outposts 管理アカウントはまず規制コンプライアンスについて評価する必要があります。

FedRAMP 証明書が必要で、AMS アカウント構造が準拠している場合は、必要な証明書が既にあり、すべてのサービスリンクアップライアンスを所有している (または既に出力データを暗号化している) データセンターベンダーを使用することをお勧めします。

最後に、アカウントチームと協力して、データを に制限 AWS Outposts し、Outpost をホストするアカウント内のリージョン内リソースの作成を防止する SCP をデプロイすることで、追加のデータ保護を実施できます。

## AMS アカウントの既存のコンプライアンスへの影響

を使用するアカウントは、規制されたデータが消費されておらず、アカウントが論理的に分離されている限り、コンプライアンスを再テスト AWS Outposts する必要はありません。AMS 管理アカウントは、クロスアカウント認証/認可と入出力データフローが VPCs 間で分離されている限り、非規制アカウントと規制アカウントを管理できます。したがって、非準拠の Outpost アカウントと既存の準拠アプリケーションアカウントの両方が同じ組織 (共有サービス、ネットワーク、ログ記録、マスター、セキュリティ AMS サービスを含む) にある場合でも、データが論理的に分離されるため、コンプライアンスアプリケーションアカウントはコンプライアンスを保持します。

## AMS on AWS Outposts FAQs

どのユースケースが AMS サポートの対象となります AWS Outpostsか？

の AMS は、実証済みのクラウド運用モデルを必要とする企業が、低レイテンシー (ファクトリロボット管理やメインフレーム移行など)、エッジコンピューティング (リモートワークステーションやエッジデータの合理化など)、大規模なデータ転送負荷を必要とするワークロードを活用 AWS Outposts できます。



## この機能を使用する理由は何ですか？

AMS は、AWS Outposts ハードウェアのモニタリングと、ハードウェアの問題に対する AWS Outposts 最初の対応を提供します。さらに、でホストされているすべてのマネージドリソースについて、次のサポート機能があります AWS Outposts。

- ログ記録、モニタリング、ガードレール、イベント管理
- 継続性管理
- セキュリティとアクセスの管理
- パッチ管理
- 変更管理
- 自動およびセルフサービスプロビジョニング管理
- インシデントと問題の管理
- レポート (AWS Outposts ハードウェアのレポートは、最初は の AMS ではサポートされていません AWS Outposts )
- サービスリクエスト管理
- デベロッパーモード
- エンタープライズサポート

この機能の使用方法を教えてください。

**AWS Outposts 計画:** AWS Outposts 計画中に、AWS Outposts ユースケースに関する AMS を特定し、AMS アカウントチームや AWS Outposts 担当者などの主要な利害関係者を関与させて、キャパシティ戦略に合わせます。

**注文検証:** 注文検証中に AWS Outposts サイトを作成し、必要な容量を AWS Outposts コンソールまたは AWS Outposts アカウント担当者から直接注文します。

**AWS Outposts AMS へのオンボーディング:** AWS Outposts ユニットが AMS マネージド VPC でアクティブ化されたら、AMS ユーザーガイド () のテンプレートを使用して変更リクエスト (RFC) を送信することで、を AMS アカウントに AWS Outposts オンボーディングするようにリクエストできます [AWS Outposts](#)。次に、AMS オペレーションはサブネットを作成し、RFC で提供された入力を使用して Outpost をモニタリングします。

**ライフサイクル管理:** AWS Outposts が AMS アカウントにオンボーディングされると、可用性、容量、またはネットワーク例外が通知されます。AWS Outposts コンソールまたは AWS Outposts 単一連絡先 (SPOC) から直接廃止 AWS Outposts できます。

## での AMS の制限は何ですか AWS Outposts ?

データレジデンシー (国固有のデータローカリゼーション法など) のユースケースは、AMS ではまだ検証されていません AWS Outposts。

AWS Outposts AWS Outposts 請求とエンタープライズサポートの要件の性質上、非 AMS アカウントでアクティブ化された を AMS に移行することはできません。

AWS Outposts コントロールプレーンは、HIPAA 対応、PCI、および ISO に準拠していることが証明されています。ただし、AWS Outposts コントロールプレーンの AMS は認証されていません AWS Outposts。このため、お客様は 環境でコンプライアンス認証 AMS AWS Outposts を追求することをお勧めします。

## この機能からオプトアウトできますか？

AMS 環境 AWS Outposts へのプロビジョニングはオプションです。AMS アカウントにデプロイされると、不要になった は AWS Outposts コンソールからいつでもプロビジョニング解除 AWS Outposts できます。

## での AMS AWS Outposts の請求方法

AWS Outposts 料金に対する AMS の引き上げは、グループ B 階層に適用されます。

## AMS サービスレベルアグリーメントはどのように変更されますか AWS Outposts ?

インシデント管理は AWS Outposts 可用性に左右されます。AWS Outposts の可用性は、お客様の責任であるお客様のネットワークの可用性に左右されます。 の AWS Outposts 可用性は、AWS Outposts サービスレベルアグリーメントに依存する AWS Outposts ハードウェアの稼働時間にも左右されます。

よくある質問も [参照AWS Outposts FAQs](#)。

# AMS でのタグの使用

## トピック

- [AMS インフラストラクチャの自動タグ付け](#)
- [AMS 推奨タグ](#)
- [タグ一括更新ノート](#)

タグを提供することは大きな価値があります。詳細については、[Amazon EC2 リソースのタグ付け](#)を参照してください。

Amazon S3 バケットや Elastic Load Balancer (ELB) AWS などのインスタンスを作成する RFCs は、通常、最大 7 つのタグ (キーと値のペア) を追加できるスキーマを提供します。管理 | 高度なスタックコンポーネント | Amazon S3 ストレージ | CT を更新することで、S3 バケットにタグを追加できます。Amazon EC2、Amazon EFS、Amazon RDS、および多層 (HA 2 階層および HA 1 階層) スキーマでは、最大 50 個のタグを使用できます。タグは、スキーマの ExecutionParameters 部分で指定されます。

AMS コンソールを使用する場合は、タグを追加するには追加設定ビューを有効にする必要があります。

 Tip

多くの CT スキーマには、スキーマの上部近くに Description および Name フィールドがあります。これらのフィールドは、スタックまたはスタックコンポーネントに名前を付けるために使用されます。作成するリソースには名前を付けません。一部のスキーマには、作成するリソースに名前を付けるパラメータがあり、そうでないスキーマもあります。例えば、Create Amazon EC2 スタックの CT スキーマは、Amazon EC2 インスタンスに名前を付けるパラメータを提供しません。そのためには、キー「Name」と名前の値を持つタグを作成する必要があります。このようなタグを作成しない場合、Amazon EC2 インスタンスは名前属性なしで Amazon EC2 コンソールに表示されます。

タグの制限はありますか？ はい：

- タグでは、大文字と小文字が区別されます。
- キーの最大長は Unicode 文字で 128 文字です。
- 値の最大長は Unicode 文字で 256 文字です。
- リソースあたりのタグの最大数は 50 です。
- 予約済みのプレフィックスは aws: です。
- AWS 生成のタグの名前と値には aws: プレフィックスが自動的に割り当てられますが、これをユーザーが割り当てることはできません。ユーザー定義タグの名前は、user: というプレフィックスを付けてコスト配分レポートに表示されます。
- 各キーは、各リソースに対して 1 回だけ使用してください。同じリソースで同じキーを 2 回使用しようとすると、リクエストは拒否されます。

- 使用できる文字は、Unicode 文字、空白、数字、および次の特殊文字です: + - = . \_ : /

タグをサポートする AWS リソースタイプはどれですか？ [AWS 「リソースごとに最大 50 個のタグを使用してリソースを整理する」](#) を参照してください。

## AMS インフラストラクチャの自動タグ付け

AMS は、Deployment | Advanced stack components | Tag | Create (managed automation) change type (ct-0176f0n99vcps) を使用して、変更リクエスト (RFC) を通じて、マルチアカウントランディングゾーン (MALZ) およびシングルアカウントランディングゾーン (SALZ) アカウントの管理目的で AMS によって作成されたすべてのリソースにタグを付けることができます。これは、管理目的で AMS によって作成されたリソースを識別するのに役立ちます。

AMS は、命名基準に基づいて AMS が作成したリソースを自動的に識別し、リソースに「AppName」、AppId」、AMSResource」、EnvironmentType」のタグキーと値があるかどうかを確認できます。タグキーが存在しない場合、または値が空の場合、それらのタグキーは AMS によってタグ値AMSInfrastructure」で自動的に作成できます。

組織のタグ付け標準に基づいて、AMS が作成したリソースに必要なタグをカスタマイズできます。AMS にリクエストを送信するときに、独自のタグキーとタグ値を含めることができます。AWS タグの命名基準： [タグ付けのベストプラクティス](#) に従う

### Note

MALZ アカウントの場合、AMS インフラストラクチャのカスタムタグ付けはアプリケーションアカウントでのみサポートされています。コアアカウントのカスタムタグ付けは現在サポートされていません。

RFC で指定したタグキー名がすでにリソースに存在する場合、タグ値は RFC で指定した新しいタグ値に置き換えられます。

タグのキーと値のペアの合計長は 256 文字以下にする必要があります。

デプロイ | 高度なスタックコンポーネント | タグ | AMS が作成したリソースにタグ付けするための (マネージドオートメーション) 変更タイプ (ct-0176f0n99vcps) を使用して、RFC に次の情報を含めます。

1. 管理目的で AMS 作成リソースにタグを付けるマルチアカウントランディングゾーンまたはシングルアカウントランディングゾーンアカウントのリスト。

2. 必須の tag-key 名と tag-value (必要な場合)。デフォルトでは、AMS は tag-key 名を「EnvironmentType」、tag-value を「AMSInfrastructure」としてタグ付けできます。カスタムタグキー名とタグ値が必要な場合は、AWS タグ命名基準「[タグ付けのベストプラクティス](#)」に従ってください。

これらのリソースは現在、AMS インフラストラクチャのタグ付けでサポートされています。

```
API Gateway
Amazon CloudFront
Amazon DynamoDB
Amazon EBS
Amazon EC2
Amazon OpenSearch Service
Amazon Quantum Ledger Database (QLDB)
Amazon Redshift
Amazon RDS
Amazon S3 (specific buckets only*)
Amazon Simple Queue Service (SQS)
Amazon Simple Notification Service (SNS)
Amazon VPC
AWS Certificate Manager
AWS CloudFormation
AWS CloudTrail
AWS CodeBuild
AWS CodePipeline
AWS Elastic Beanstalk
AWS Lambda
AWS Secrets Manager
AWS Service Catalog
AWS Systems Manager
AWS WAF Regional
Elastic Load Balancing
```

\* "arn:aws::awsms-a\*-patch-data-\*", "arn:aws:s3::ams-a\*-log-management-\*", "arn:aws:s3::cf-templates-\*", "arn:aws:s3::mcc-a\*", "arn:aws::aws::ams-a\*-backup-reports-\*", "arn:aws:s3::ams-patch-data-customer-reports-\*", "arn:aws-a\*-patch-data-raw-\*", "arn:aws:s3::patch-data-reporting-ams-cfn-drift-remediation-ams-reporting-data-a

## AMS 推奨タグ

AMS では、サポートされているリソースに次のタグを推奨しています。スター付き (\*) タグは強くお勧めします。

### Note

タグを使用してパッチ適用をスケジュールできます。詳細については、[「AMS Advanced Patch Orchestrator: タグベースのパッチ適用モデル」](#)を参照してください。

## AMS 予約プレフィックス

AMS リソース属性は、特定のパターンに準拠する必要があります。例えば、IAM インスタンスプロファイル名、BackupVault 名、タグ名などは、AMS 予約プレフィックスで始めることはできません。リザーブドプレフィックスは次のとおりです。

```
*/aws_reserved/*
ams-*
/ams/*
ams*
AMS*
Ams*
aws*
AWS*
AWS_*
AWSManagedServices*
codedeploy_service_role
CloudTrail*
Cloudtrail*
customer-mc-*
eps
EPSDB*
IAMPolicy*
INGEST*
LandingZone*
Managed_Services*
managementhost
mc*
MC*
Mc*
MMS*
ms-
NewAMS*
Root*
sentinel*
Sentinel*
sentinel.int.
StackSet-ams*
StackSet-AWS-Landing-Zone
StateMachine*
TemplateId*
VPC_*
UnhealthyInServiceBastion
```

## AMS 推奨タグ

| タグキー                | サポートされる値                  | 注意                                                                                                               |
|---------------------|---------------------------|------------------------------------------------------------------------------------------------------------------|
| AppName*            | 制約なし。                     | リソースに存在するか、リソースへのアクセスを必要とするアプリケーションを特定します。これにより、AMS とユーザー間の追跡と通信が容易になります。                                        |
| AppId*              |                           |                                                                                                                  |
| EnvironmentType *   |                           |                                                                                                                  |
| OwnerTeamEmail *    | ディストリビューションリストの E メールアドレス | リソースを担当するチームのディストリビューションリストの E メールアドレスを特定します。E メールは個人の E メールではなく、ディストリビューションリストなどの匿名 E メールである必要があります。            |
| ComplianceFramework | 拘束されない                    | リソースに適用するコントロールとポリシーを特定します。                                                                                      |
| CostCenter          |                           | リソースに関連付けられているコストセンターまたはビジネスユニットを特定します (通常はコスト配分と追跡用)。                                                           |
| Customer            |                           | 複数の顧客 (AMS サブ顧客) からのリソースを持つ AMS 顧客が使用します。マネージド環境のリソースを、提供している特定の顧客にグループ化します。特定のリソースまたはサービスのグループで特定のクライアントを特定します。 |

| タグキー               | サポートされる値                                                                                                                                                                                                                                                                                        | 注意                                                        |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|
| DataClassification |                                                                                                                                                                                                                                                                                                 | リソースがサポートする特定のデータ機密性レベルを特定します。リソースに適用するコントロールとポリシーを特定します。 |
| HoursOfOperation   |                                                                                                                                                                                                                                                                                                 | リソースを開始、停止、削除、またはローテーションする日時を特定します。                       |
| OwnerTeam          |                                                                                                                                                                                                                                                                                                 | リソースを担当するチームを特定します。リソースを担当するチームとのコミュニケーションを促進します。         |
| Patch Group        | <p>これには 2 つのオプションがあります。</p> <ul style="list-style-type: none"><li>• <a href="#">AMS Advanced Patch Orchestrator で説明されている情報を使用してサービスリクエストを送信できます。タグベースのパッチ適用モデル</a>と AMS は指定されたリソースに を作成し、提供された情報を使用してPatch Groupタグを作成します。</li><li>• リソースに既にPatch Groupタグを作成している場合、サポートされている値は制約されません。</li></ul> | 自動パッチ適用メンテナンスウィンドウに含めるリソース。                               |



| タグキー            | サポートされる値                                                                                                                            | 注意                                    |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|
| ProjectId       | 拘束されない                                                                                                                              | リソースがサポートするプロジェクトを特定します。              |
| SupportPriority | 機密性、完全性、可用性の 6 つの頭字語のいずれか。頭字語の順序が優先されます。たとえば、I.C.A. は、順序が整合性、機密性、可用性であることを意味します。その他の許容値は、C.I.A.、C.A.I.、I.A.C.、A.C.I.、および A.I.C. です。 | どのタイプのサポートを優先すべきかを特定します: 機密性、整合性、可用性。 |

## タグ一括更新ノート

これらの注意事項は、「[Tag | Bulk Update](#)」および「[Tag | Bulk Update \(Managed Automation\) change type example walkthroughs](#)」で使用するためのものです。

一括更新タグに関する注意事項:

- サポートされているサービス:
  - [タグ | 一括更新 \(マネージドオートメーション\)](#) の場合: すべて。
  - [タグ | 一括更新](#) の場合:
    - Auto Scaling
    - Amazon EC2
    - Elastic Load Balancing
    - Amazon RDS
    - Amazon S3 バケット
- カンマ区切り値 (CSV) ファイルを生成するには、AWS コンソールで Resource Groups > Tag Editor にログインし、タグ付けするリソースを見つけて、CSV ファイルにエクスポートします。詳細については、「結果を [CSV にエクスポート](#) する」を参照してください。

注: CSV オブジェクトの場所を指定するには、S3 の署名付き URL を使用することをお勧めします。

- サービス、タイプ、識別子のヘッダーを持つ列が必要です。これらの列は必須です。
- 列識別子の名前を ID に変更します。
- Service、Type、および Identifier (ID に変更) 列の値は、Resource Groups のタグエディタによって提供される値です。
- タグを付けるリソースがタグエディタで利用できない場合は、列識別子 (ID に変更) のリソースの Amazon リソースネーム (ARN) を使用し、サービスとタイプを空白のままにします。
- 追加または変更するタグの列ヘッダーの形式は Tag: **TagKey** である必要があります。
- 削除するタグの列ヘッダーは、Untag: **TagKey** の形式である必要があります。
- 各行は、リソースにタグ付けまたはタグ付け解除するためのものです。
- タグをリソースに追加する場合は、適切な Tag: **TagKey** 列でタグの値を指定します。
- タグをリソースから削除する場合は、適切な Untag: **TagKey** 列で True を指定します。
- Tag: **TagKey** または Untag: **TagKey** がリソースに適用できない場合は、ダッシュ (-) をそれぞれの列に追加するか、空白のままにします。

注: Untag はタグを上書きします。これは、Tag とは異なり、Untag を手動で CSV ファイルに追加する必要があるため、タグは変更するのではなく削除することを意図していると想定しているためです。

- 条件に合わない追加の列は無視されます。

#### Important

タグエディタのエクスポートでは、すべてのリソースに対するすべてのタグの行列が入力され、欠落しているタグには「タグ付けされていない」の値が入力されます。このエクスポート CSV を RFC への入力として再利用すると、以前に欠落していたすべてのタグが作成され、リテラル値は「タグ付けされていません」になります。

**Note**

CSV ファイルにタグをエクスポートする方法については、[「タグ付けするリソースの検索 -> 結果を CSV にエクスポートする」](#)を参照してください。

## AWS Managed Services リソーススケジューラ

AWS Managed Services (AMS) リソーススケジューラを使用して、アカウント内の AutoScaling グループ、Amazon EC2 インスタンス、および RDS インスタンスの自動起動と停止をスケジュールします。これにより、リソースが 24 時間 365 日稼働することを意図していないインフラストラクチャコストを削減できます。このソリューションは、上の [Instance Scheduler AWS](#) 上に構築されていますが、AMS のニーズに固有の追加機能とカスタマイズが含まれています。

**Note**

デフォルトでは、AMS Resource Scheduler は AWS CloudFormation スタックに含まれていないリソースとやり取りしません。リソースは、「スタック」、「sc-」、または「SC-」で始まるスタックの一部である必要があります。CloudFormation スタックに含まれていないリソースをスケジュールするには、Resource Scheduler スタックパラメータを `ScheduleNonStackResources` に更新します Yes。

AMS Resource Scheduler は、期間とスケジュールを使用します。

- 期間は、開始時刻、終了時刻、月の日数など、Resource Scheduler が実行される時間を定義します。
- スケジュールには、定義された期間と、SSM メンテナンスウィンドウ、タイムゾーン、休止設定などの追加の設定が含まれており、設定された期間ルールに基づいてリソースを実行するタイミングを指定します。

これらの期間とスケジュールは、AMS Resource Scheduler の自動変更タイプ (CTs) を使用して設定できます。

AMS Resource Scheduler で使用できる設定の詳細については、[「ソリューションコンポーネント」](#)の対応する AWS Instance Scheduler ドキュメントを参照してください。ソリューションのアーキテ

クチャビューについては、[「アーキテクチャの概要.html」](#) の対応する AWS Instance Scheduler ドキュメントを参照してください。

## AMS リソーススケジューラのデプロイ

AMS リソーススケジューラをデプロイするには、自動変更タイプ (CT) : デプロイ | AMS リソーススケジューラ | ソリューション | デプロイ (ct-0ywnhc8e5k9z5) を使用して、ソリューションをアカウントにデプロイする RFC を生成します。RFC が実行されると、デフォルト設定の AMS Resource Scheduler リソースを含む CloudFormation スタックがアカウントに自動的にプロビジョニングされます。Resource Scheduler の変更タイプの詳細については、[「AMS Resource Scheduler」](#) を参照してください。

### Note

AMS Resource Scheduler がアカウントに既にデプロイされているかどうかを確認するには、そのアカウントの AWS Lambda コンソールをチェックし、AMSResourceScheduler 関数を探します。

AMS リソーススケジューラがアカウントでプロビジョニングされたら、デフォルト設定を確認し、必要に応じてタグキー、タイムゾーン、スケジュールされたサービスなどの設定をユーザー設定に基づいてカスタマイズすることをお勧めします。推奨されるカスタマイズの詳細については、次の[AMS リソーススケジューラのカスタマイズ](#)「」を参照してください。

カスタム設定を行うか、Resource Scheduler の設定を確認するだけです。

## AMS リソーススケジューラのカスタマイズ

AMS Resource Scheduler の更新変更タイプを使用して、AMS Resource Scheduler の次のプロパティをカスタマイズすることをお勧めします。[「AMS Resource Scheduler」](#) を参照してください。

- タグ名: Resource Scheduler がインスタンススケジュールをリソースに関連付けるために使用されるタグの名前。デフォルト値は Schedule です。
- スケジュールされたサービス: Resource Scheduler が管理できるサービスのカンマ区切りリスト。デフォルト値は「ec2,rds,autoscaling」です。有効な値は「ec2」、「rds」、「autoscaling」です。
- デフォルトのタイムゾーン: Resource Scheduler で使用するデフォルトのタイムゾーンを指定します。デフォルト値は UTC です。

- CMK を使用する: Resource Scheduler にアクセス許可を付与できる Amazon KMS カスタマーマネージドキー (CMK) ARNs のカンマ区切りリスト。
- LicenseManager を使用する: その Resource Scheduler AWS に対する Licence Manager ARNs のカンマ区切りリストには、アクセス許可を付与できます。

#### Note

AMS は、AMS Resource Scheduler をアカウントの最新の状態に保つために、機能や修正をリリースすることがあります。この場合、AMS Resource Scheduler に対して行ったカスタマイズは保持されます。

## AMS リソーススケジューラの使用

ソリューションのデプロイ後に AMS Resource Scheduler を設定するには、自動化された Resource Scheduler CTs を使用して、AMS Resource Scheduler の期間 (Resource Scheduler が実行される時間) とスケジュール (設定された期間およびその他のオプション) を作成、削除、更新、記述 (詳細を取得) します。AMS Resource Scheduler の変更タイプを使用する例については、[「AMS Resource Scheduler」](#) を参照してください。

AMS Resource Scheduler によって管理されるリソースを選択するには、デプロイとスケジュールの作成後に、AMS Tag Create CTs を使用して、デプロイ時に指定したタグキーと定義されたスケジュールをタグ値として Auto Scaling グループ、Amazon RDS スタック、Amazon EC2 リソースにタグ付けします。リソースにタグを付けると、リソースは定義された Resource Scheduler スケジュールに従って開始または停止するようにスケジュールされます。

AMS Resource Scheduler の使用には追加料金はかかりません。ただし、このソリューションでは複数の が使用され AWS のサービスでおり、これらのリソースの使用時に課金されます。詳細については、[「アーキテクチャの概要」](#) を参照してください。

AMS Resource Scheduler をオプトアウトするには：

- 一時的なオプトアウトまたは無効化の場合: 自動管理 | AMS リソーススケジューラ | 状態 | 変更タイプを無効にする (ct-14v49adibs4db) を使用して RFC を送信する
- 永続的な削除の場合: 管理を送信する | その他 | その他 | 更新 (レビューが必要) (ct-0xdawir96cy7k) RFC が Resource Scheduler リリースオートメーションシステムからの削除をリクエストする

## AMS Resource Scheduler のコスト見積りツール

コスト削減を追跡するために、AMS リソーススケジューラには、スケジューラによって管理される Amazon EC2 および RDS リソースの推定コスト削減を時間単位で計算するコンポーネントがあります。このコスト削減データは、追跡に役立つ CloudWatch メトリクス (AMS/ResourceScheduler) として公開されます。コスト削減推定器は、インスタンスの実行時間の節約のみを推定します。リソースに関連するデータ転送コストなど、他のコストは考慮されません。

Resource Scheduler では、コスト削減推定器が有効になっています。1 時間ごとに実行され、からコストと使用状況データを取得します AWS Cost Explorer。そのデータから、各インスタンスタイプの 1 時間あたりの平均コストを計算し、スケジュールなしで実行されていた場合は 1 日のコストを予測します。コスト削減は、特定の日における Cost Explorer からの予測コストと実際に報告されたコストの差です。

たとえば、インスタンス A が Resource Scheduler で午前 9 時から午後 5 時まで実行されるように設定されている場合、特定の日に 8 時間になります。Cost Explorer はコストを 1 USD、使用量を 8 と報告します。したがって、1 時間あたりの平均コストは 0.125 USD です。インスタンスが Resource Scheduler でスケジュールされていない場合、インスタンスはその日に 24 時間実行されます。この場合、コストは  $24 \times 0.125 = 3$  USD になります。Resource Scheduler は、2 USD のコスト削減を実現しました。

Cost Explorer から Resource Scheduler によって管理されるリソースのコストと使用状況のみを取得するために、Resource Scheduler がリソースをターゲットにするために使用するタグキーを Billing Dashboard のコスト配分タグとしてアクティブ化する必要があります。アカウントが組織に属している場合、タグキーは組織の管理アカウントでアクティブ化する必要があります。これを行う方法については、[「ユーザー定義のコスト配分タグとユーザー定義のコスト配分タグのアクティブ化」](https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/custom-tags.html)を参照してください。 <https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/custom-tags.html>

タグキーがコスト配分タグとしてアクティブ化されると、AWS 請求は Resource Scheduler によって管理されるリソースのコストと使用状況の追跡を開始し、そのデータが利用可能になると、コスト削減推定器はコスト削減の計算を開始し、CloudWatch の AMS/ResourceScheduler メトリクス名前空間にデータを発行します。

### コスト見積りツールのヒント

Cost Savings Estimator は、リザーブドインスタンスや Savings Plans などの割引を計算で考慮に入れません。推定器は Cost Explorer から使用コストを受け取り、リソースの 1 時間あたりの平均コストを計算します。詳細については、[AWS 「コストデータセットを理解する: チートシート」](#)を参照してください。



Cost Explorer から Resource Scheduler によって管理されるリソースのコストと使用状況のみを取得するために、Resource Scheduler がリソースをターゲットにするために使用するタグキーを Billing Dashboard の Cost Allocation タグとしてアクティブ化する必要があります。アカウントが組織に属している場合、タグキーは組織の管理アカウントでアクティブ化する必要があります。これを行う方法については、「[ユーザー定義のコスト配分タグ](#)」を参照してください。コスト配分タグが有効になっていない場合、推定器は、有効になっていても削減額を計算してメトリクスを発行することはできません。

## AMS Resource Scheduler のベストプラクティス

### Amazon EC2 インスタンスのスケジューリング

- インスタンスのシャットダウン動作は `stop` に設定し、`terminate` に設定しないでください。これは、AMS Amazon EC2 自動変更タイプの作成 (ct-14027q0sjyt1h) で作成されたインスタンス `stop` の場合は `stop` に事前設定されており、AWS CloudFormation `InstanceInitiatedShutdownBehavior` プロパティを `stop` に設定することで、取り込みで作成された Amazon EC2 インスタンスに設定できます。インスタンスのシャットダウン動作が `terminate` に設定されている場合、Resource Scheduler が停止し、スケジューラが起動できなくなるとインスタンスは終了します。
- Auto Scaling グループの一部である Amazon EC2 インスタンスは、タグ付けされていても、AMS Resource Scheduler によって個別に処理されません。
- ターゲットインスタンスのルートボリュームが KMS カスタマーマスターキー (CMK) で暗号化されている場合は、スケジューラがそのようなインスタンスを開始できるように、Resource Scheduler IAM ロールに追加の `kms:CreateGrant` アクセス許可を追加する必要があります。このアクセス許可は、セキュリティを向上させるためにデフォルトではロールに追加されません。このアクセス許可が必要な場合は、Management | AMS Resource Scheduler | Solution | Update change type を使用して RFC を送信し、KMS CMKs の ARNs のカンマ区切りリストを指定します。

### Auto Scaling グループのスケジューリング

- AMS Resource Scheduler は、グループ内の個々のインスタンスではなく、Auto Scaling グループの自動スケーリングを開始または停止します。つまり、スケジューラは Auto Scaling グループのサイズを復元 (開始) するか、サイズを 0 (停止) に設定します。
- AutoScaling グループに、グループ内のインスタンスではなく、指定されたタグをタグ付けします。

- 停止中、AMS Resource Scheduler は Auto Scaling グループの最小容量、希望容量、最大容量の値を保存し、最小容量と希望容量を 0 に設定します。起動時に、スケジューラは Auto Scaling グループサイズを停止時と同じように復元します。したがって、Auto Scaling グループインスタンスは、インスタンスの終了と再起動が Auto Scaling グループで実行されているアプリケーションに影響を与えないように、適切な容量設定を使用する必要があります。
- 実行中に Auto Scaling グループが変更された場合 (最小容量または最大容量)、スケジューラは新しい Auto Scaling グループサイズを保存し、停止スケジュールの最後にグループを復元するときに使用します。

## Amazon RDS インスタンスのスケジュール

- スケジューラは、RDS インスタンスを停止する前にスナップショットを作成できます (Aurora DB クラスターには適用されません)。この機能はデフォルトで有効になっており、RDS インスタンススナップショットの作成 CloudFormation テンプレートパラメータは true に設定されています。スナップショットは、次回 Amazon RDS インスタンスが停止し、新しいスナップショットが作成されるまで保持されます。

スケジューラは、クラスターまたは Amazon RDS Aurora データベースの一部である Amazon RDS インスタンス、またはマルチアベイラビリティゾーン (マルチ AZ) 設定で起動/停止できます。ただし、スケジューラが Amazon RDS インスタンス、特にマルチ AZ インスタンスを停止できない場合は、Amazon RDS の制限を確認してください。Aurora クラスターの開始または停止をスケジュールするには、Schedule Aurora Clusters テンプレートパラメータを使用します (デフォルトは true)。Aurora クラスター (クラスター内の個々のインスタンスではなく) には、初期設定時に定義されたタグキーと、そのクラスターをスケジュールするためのタグ値としてスケジュール名をタグ付けする必要があります。

すべての Amazon RDS インスタンスには、システムの変更が適用される毎週のメンテナンスウィンドウがあります。メンテナンスウィンドウ中、Amazon RDS は 7 日以上停止したインスタンスを自動的に起動し、メンテナンスを適用します。メンテナンスイベントが完了すると、Amazon RDS はインスタンスを停止しないことに注意してください。

スケジューラを使用すると、Amazon RDS インスタンスの優先メンテナンスウィンドウをスケジュールの実行期間として追加するかどうかを指定できます。ソリューションでは、メンテナンスウィンドウの最初にインスタンスを起動しますが、他の実行期間でインスタンスを実行するように指定されておらず、メンテナンスイベントが完了した場合はメンテナンスウィンドウの終了時にインスタンスを停止します。



メンテナンスウィンドウの終了までにメンテナンスイベントが完了しなかった場合、インスタンスはメンテナンスイベントが完了した後のスケジュール間隔まで実行されます。

#### Note

スケジューラは、リソースの開始または停止を検証しません。API コールを行い、次に進みます。API コールが失敗すると、調査のためにエラーがログに記録されます。

## AWS Systems Manager AMS Advanced の

AWS Systems Manager ドキュメント (SSM ドキュメント) は、Systems Manager が AWS リソースに対して実行するアクションを定義します。Systems Manager には、実行時にパラメータを指定することで使用できる事前設定されたドキュメントが 12 個以上含まれています。ドキュメントは JavaScript Object Notation (JSON) や YAML を使用し、これにはユーザーが指定するパラメータおよびステップが含まれます。

AWS Managed Services (AMS) は、SSM ドキュメントの信頼できるパブリッシャーです。AMS が所有する SSM ドキュメントは、オンボードされた AMS アカウントとのみ共有され、常に予約済みプレフィックス (AWSManagedServices-\*) で始まり、が所有する Systems Manager コンソールに表示されます AWS。SSM ドキュメントの開発と公開の AMS プロセスは AWS ベストプラクティスに従い、ドキュメントのライフサイクル全体で複数のピアレビューが必要です。SSM ドキュメントを共有するための AWS ベストプラクティスの詳細については、[「共有 SSM ドキュメントのベストプラクティス」](#)を参照してください。

## 利用可能な AMS Advanced SSM ドキュメント

AMS Advanced SSM ドキュメントは AMS Advanced のお客様のみが利用でき、アカウントを運用するための運用ワークフローを自動化するために使用されます。

から利用可能な AMS Advanced SSM ドキュメントを表示するには AWS マネジメントコンソール：

1. [AWS Systems Manager コンソール](#)で Systems Managerconsole を開きます。
2. 自分と共有を選択します。
3. 検索バーで、ドキュメント名のプレフィックスでフィルタリングし、次に Equals でフィルタリングして、値を AWSManagedServices- に設定します。

AWS CLI の手順については、[「共有 SSM ドキュメントの使用」](#)を参照してください。

## AMS Advanced SSM ドキュメントバージョン

SSM ドキュメントはバージョニングをサポートしています。AMS Advanced SSM ドキュメントをお客様のアカウントから変更したり、再共有したりすることはできません。アカウントを運用するために、AMS Advanced によって一元管理および保守されます。

バージョン番号は、特定のドキュメントの更新ごとに増分されます AWS リージョン。新しいリージョンが利用可能になると、2 つのリージョンで同じドキュメントコンテンツに異なるバージョン番号を付けることができます。これは一般的であり、動作が異なるわけではありません。2 つの AMS Advanced SSM ドキュメントを比較する場合は、ハッシュを AWS CLI と比較することをお勧めします。

```
aws ssm describe-document \  
--name AWSManagedServices-DOCUMENTNAME \  
--output text --query "Document.Hash"
```

ハッシュが一致した場合、2 つの SSM ドキュメントは同じです。

## AMS での Systems Manager の料金

AMS Advanced SSM ドキュメントアクセスに関連するコストはありません。ランタイムコストは、SSM ドキュメントのタイプ、ステップ、ランタイム期間によって異なります。詳細については、「[の AWS Systems Manager 料金](#)」を参照してください。

## AMS アカウントのオフボード

AMS は、シングルアカウントランディングゾーンとマルチアカウントランディングゾーンアカウントにオフボーディング支援を提供します。

AMS は、非依存関係への影響を避けるため、オフボーディング中に AMIs の共有を解除しません。アカウントから AMS AMIs を削除する場合は、cancel-image-launch-permission API を使用して特定の AMIs を非表示にできます。たとえば、以下のスクリプトを使用して、以前にアカウントと共有されたすべての AMS AMIs を非表示にできます。

```
for ami in $(aws ec2 describe-images --executable-users self --owners 027415890775 --
query 'Images[].ImageId' --output text) ;
do
aws ec2 cancel-image-launch-permission --image-id $ami ;
done
```

スクリプトをエラーなしで実行するには、AWS CLI v2 がインストールされている必要があります。AWS CLI のインストール手順については、[「AWS CLI の最新バージョンのインストールまたは更新」](#)を参照してください。cancel-image-launch-permission コマンドの詳細については、「」を参照してください[cancel-image-launch-permission](#)。

#### Note

サービス終了日は、30 日間の必要な終了通知期間の終了後の暦月の最終日です。必要な終了通知期間の終了日が暦月の 20 日以降である場合、サービス終了日は翌月の最終日になります。終了日のシナリオの例を次に示します。

- 終了通知が 4 月 12 日に提供された場合、30 日間の通知は 5 月 12 日に終了します。サービス終了日は 5 月 31 日です。
- 終了通知が 4 月 29 日に提供された場合、30 日間の通知は 5 月 29 日に終了します。サービス終了日は 6 月 30 日です。

## トピック

- [AMS シングルアカウントランディングゾーンアカウントからのオフボード](#)
- [AMS マルチアカウントランディングゾーンアカウントからのオフボード](#)

## AMS シングルアカウントランディングゾーンアカウントからのオフボード

AMS は、AMS の終了前 30 日以内にオフボーディング支援を提供します。

このような支援を提供するには、少なくとも 7 日前にオフボーディング支援をリクエストする必要があります。オフボーディング支援は、次の 2 つの形式で提供できます。

- コントロールの引き渡し: AMS は、すべての AMS マネージドアプリケーションのアクセス認証情報とともに、アカウントコントロールをユーザーに移管します。または

- アカウント閉鎖のためのリソース終了: AMS は AMS マネージド環境内のすべてのデータを削除し、アカウント内のアクティブなリソースのプロビジョニングを解除します。オフボーディングリクエストを送信すると、お客様は AMS に以下をリクエストできます。
- Amazon S3 バケットに保存されているデータオブジェクト (ログを含む) を削除または保持する
- Amazon S3 バケットを削除または保持する
- AWS Backup 復元ポイントを削除または保持する

#### Important

その他の特定のリクエスト (妥当性による) は、オフボーディングの初期化前に AMS に通知する必要があります。

オプションの前提条件 (必要な場合):

#### Note

オフボーディングリクエストの前に、お客様は、AWS Snowball Edge または と AWS インターフェイスする他のメディアを使用して、既存の形式でデータを転送するための AMS サポートをリクエストできます。

データバックアップに加えて、オフボーディング支援の一環として以下の顧客データを提供できます。

- ログを含むストレージサービスに保存されているデータ
- お客様固有の変更タイプスキーマ
- 変更タイプスキーマの CloudFormation テンプレート

AMS の終了時にオフボーディングアクティビティが完了しない場合、保留中のアクティビティを完了できるように、アカウントのコントロール (複数可) が引き渡されます。

| 関数               | 削除されたもの            | 影響                  | 必要なアクション                    |
|------------------|--------------------|---------------------|-----------------------------|
| モニタリング、ログ記録、アラート | AMS モニタリングが削除されました | AMS は、リソースと環境へのアクセス | 削除およびサブスクリプション解除されたサービスの不測の |

| 関数        | 削除されたもの                                                                                                                                                                   | 影響                                                                                                                                    | 必要なアクション                                                       |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
|           | <p>MMS (マネージドモニタリングシステム) のサブスクリプション解除</p> <p>Resource Tagger と Alarm Manager が削除されました</p> <p>ベースライン CloudWatch アラートは既存のリソースに残ります</p> <p>GuardDuty と Macie: 所有権が元に戻ります</p> | <p>や可視性を失いました。</p>                                                                                                                    | <p>事態は、お客様が所有します。</p>                                          |
| バックアップの管理 | <p>AMS Backup オートメーションは削除されますが、AWS Backup サービスは引き続き使用できます。削除がリクエストされない限り、バックアップポリシーとデータは保持されます。</p>                                                                       | <p>AMS は、バックアップジョブをモニタリングしたり、インシデント中に復元アクションを実行したりしなくなりました。アラームとアラートは無効になっています。IAM バックアップポリシーと KMS キーを削除すると、AMS バックアップが動作しなくなります。</p> | <p>AMS Backup Plans は再設定する必要があります。すべてのモニタリングと修復の所有権が返されます。</p> |

| 関数                      | 削除されたもの                                                                                                 | 影響                                                                            | 必要なアクション                                              |
|-------------------------|---------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|-------------------------------------------------------|
| サービス管理のための AMS オートメーション | AMS が厳選した AWS SSM オートメーションランブック、Amazon Simple Notification Service (SNS)、および AWS Lambda 関数は使用できなくなりました。 | アカウントへの AMS アクセスがありません。すべてのオートメーションが無効になっています。                                | 必要に応じて、SSM、SNS、Lambda 関数を含むすべてのオートメーションを再作成する必要があります。 |
| コンプライアンス                | すべての GuardDuty および削除された AWS Config ルールに対する AMS の可視性とモニタリング。ただし、これらのルールはアカウントに残ります。                      | Amazon GuardDuty および ルールからのすべてのモニタリング、レポート、修復は、AMS によって管理されなくなりました。AWS Config | お客様が引き受けるすべてのセキュリティおよびコンプライアンスツールのモニタリングと修復。          |
| インスタンスエージェント            | EC2 インスタンスに必要なエージェントをインストールするための Resource Scheduler、Resource Tagger、または自動インスタンス設定へのアクセスは削除されます。         | インスタンスの CloudWatch エージェントと SSM エージェントは既存の設定のままになりますが、AMS はこれらの設定をサポートしません。    | タグ付けとインスタンス上の CloudWatch および SSM エージェント設定を管理します。      |

| 関数                 | 削除されたもの                                                           | 影響                                                                                                                                                   | 必要なアクション                                                                                                                                |
|--------------------|-------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| パッチとレポートインフラストラクチャ | AMS はパッチ適用後のアクティビティを管理しなくなり、これらのサービスへのアクセスと可視性は削除されます。            | AMS は、パッチ適用前にインスタンスのスナップショットを作成しなくなり、パッチのインストールをインストールしてモニタリングしなくなり、結果を通知しなくなりました。レポートと「監査S3バケットは、リクエストに応じてアカウントに残ります。AMS はサービスメトリクスレポートを生成しなくなりました。 | 過去に作成したパッチベースラインとスナップショットは保持します。さらに、パッチメンテナンスウィンドウの設定は残りますが、パッチは AMS によってインストールまたは修正されなくなります。インフラストラクチャの運用メトリクスに関するレポートはすべてお客様の責任となります。 |
| プロセス管理             | すべてのアカウントは、サービスリクエスト、問題、変更、管理など、インシデントに対して提供されるサービス管理からオフボードされます。 | インシデントやサービスリクエストによって AMS によって以前修復されたサービスの中断、環境の変更、根本原因の調査はすべて、AMS によってより長く管理されます。                                                                    | すべてのプロセス管理の完全な所有権を回復します。                                                                                                                |

## AMS マルチアカウントランディングゾーンアカウントからのオフボード

AMS Advanced マルチアカウントランディングゾーンからオフボード AWS できるアカウントには、次の 2 つのタイプがあります。

- アプリケーションアカウント
- コアアカウント

AMS マルチアカウントランディングゾーンからすべてのアカウントをオフボードするには、コアアカウントをオフボードする前に、すべてのアプリケーションアカウントをオフボードする必要があります。

オフボードのアプリケーションアカウントまたは Core アカウントでワークロードを引き継ぎ、引き続き運用するには、AMS アカウントチームでこのドキュメントを確認してください。このドキュメントでは、オフボードプロセス中に AMS が実行する変更の概要を説明します。

## オフボーディングされたアカウントの継続的な運用のために完了するタスク

AMS マルチアカウントランディングゾーンからオフボードしたアカウントの継続的なオペレーションには、次のタスクが必要です。

- **デベロッパーモードを有効にする:** アカウントに対するアクセス許可をさらに取得するには、アプリケーションアカウントを AMS からオフボードする前に、デベロッパーモードをオンにします。デベロッパーモードを有効にすると、オフボーディングの準備に必要な変更をより簡単に行うことができます。AMS インフラストラクチャリソースを削除または変更しようとししないでください。AMS インフラストラクチャリソースを削除すると、AMS はアカウントを正常にオフボードできない可能性があります。デベロッパーモードを有効にする方法については、「」を参照してください [AMS Advanced Developer モードの開始方法](#)。

デベロッパーモードを有効にした後、オフボーディングの準備に必要な変更を完了できない場合は、AMS アカウントチームに連絡して要件について話し合ってください。

- **EC2 スタックアクセスの代替方法を選択:** AMS からアプリケーションアカウントをオフボードした後、RFCs を使用してスタックリソースにアクセスすることはできません。を確認してから [オフボーディングの変更](#)、スタックへのアクセスを保持する代替アクセス方法を選択します。詳細については、「[代替手段にアクセスする](#)」を参照してください。

## AMS アプリケーションアカウントのオフボード

マルチアカウントランディングゾーン環境からアプリケーションアカウントをオフボードするには、アカウントごとに次の手順を実行します。

1. アカウントに開いている RFCs がないことを確認します。詳細については、「[RFCs の作成、クローン作成、更新、検索、キャンセル](#)」を参照してください。
2. アカウントのプライマリまたはルートユーザーの E メールアドレスにアクセスできることを確認します。



3. アプリケーションアカウントから、[アプリケーションアカウント | オフボーディングの確認](#) (ct-2wlfo2jxj2rkj) 変更タイプを使用して RFC を送信します。RFC で、オフボードするアプリケーションアカウントを指定します。
4. 管理アカウントから、[管理アカウント | オフボードアプリケーションアカウント](#) (ct-0vdiy51oyrhbm) の変更タイプを使用して RFC を送信します。RFC で、オフボードするアプリケーションアカウントを指定します。また、ランディングゾーンへの Transit Gateway アタッチメントを削除または保持するかどうかを指定します。
5. AMS 請求が停止されていることを確認するには、アカウントをオフボードしたことを CSDM に通知します。

アプリケーションアカウントがオフボードされた後、以下が発生します。

- すべてのコンポーネントは AMS サービスとの関連付けが解除されますが、作成したリソースはアカウントに残ります。AMS オフボードアカウントを保持または閉鎖することを選択できます。
- コアアカウントおよびその他の残りのアプリケーションアカウントは通常、アプリケーションアカウントがオフボードされた後に機能します。
- AMS 請求は停止されますが、アカウントを閉鎖するまで AWS 請求は停止されません。詳細については、[「アカウントを閉鎖する前に知っておくべきこと」](#)を参照してください。
- アカウントが閉鎖されている場合、アカウントは suspended 状態で 90 日間組織に表示されます。90 日後、閉鎖されたアカウントは完全に削除され、組織に表示されなくなります。
- アカウントが閉鎖された後も、90 サポート 日間サインインしてサポートケースまたは連絡先を提出できます。
- 90 日後、アカウント内に残っているコンテンツはすべて完全に削除され、残りの AWS サービスは終了します。

アプリケーションアカウントのオフボーディングに関するよくある質問

Q: フェデレーティッド IAM ロールを使用して、AMS マルチアカウントランディングゾーンからオフボードしたアプリケーションアカウントに引き続きアクセスできますか？

はい。AMS が作成した[デフォルト AWS Identity and Access Management \(IAM\) ロール](#)は、AMS オフボーディング後もアカウントで引き続き使用できます。ただし、これらのロールとポリシーは、AMS アクセス管理で使用するよう設計されています。ユーザーに必要なアクセスを提供するには、独自の IAM リソースをデプロイする必要がある場合があります。

Q: AMS マルチアカウントランディングゾーンからオフボードしたアプリケーションアカウントへのフルアクセスを取得するにはどうすればよいですか？

オフボーディングされたアプリケーションアカウントは、AWS Organizations アカウント構造の非推奨組織単位 (OU) に移動されます。この移動により、以前にルートユーザーアクセスをブロックした SCP アクセス制限が解除されます。ルートユーザーの認証情報をリセットする方法については、[「紛失または忘れたルートユーザーのパスワードのリセット」](#)を参照してください。

Q: アプリケーションアカウントのオフボーディング中にどのような変更が行われますか？

サービスがアカウントをオフボードするときに AMS が実行するアクションの詳細については、「」を参照してください [オフボーディングの変更](#)。

Q: トランジットゲートウェイからデタッチせずにアプリケーションアカウントをオフボードできますか？

はい。 [管理アカウント | オフボードアプリケーションアカウント](#) (ct-0vdiy51oyrhbm) 変更タイプを使用して RFC を送信し、DeleteTransitGatewayAttachmentパラメータを として指定しますFalse。

Q: アプリケーションアカウントのオフボードにはどのくらいの時間がかかりますか？

[管理アカウント | オフボードアプリケーションアカウント](#) (ct-0vdiy51oyrhbm) の変更タイプを使用すると、RFCs 1 時間以内に完了します。

Q: オフボードされたアカウントを閉じることは必須ですか？

いいえ。AMS オフボーディング後のアカウント閉鎖は必須ではありません。オフボーディングプロセス中、AMS は AWS アカウントのアクセスと管理を削除しますが、アカウントとアカウント内のリソースは残ります。AMS オフボーディング後、AWS アカウントとリソースの管理と保守はお客様の責任となります。AMS は、オフボーディングプロセスの完了後にアカウントで発生する可能性のある問題、インシデント、またはサービスの中断について責任を負いません。詳細については、[AWS 「アカウントを閉じるにはどうすればよいですか？」](#)を参照してください。

Q: アカウント閉鎖リクエストを送信すると、既存のリソースはすべてすぐに削除されますか？

いいえ。アカウントを閉鎖してもリソースは終了しません。アカウントのリソースは、閉鎖リクエストから 90 日後に自動的に終了します。AMS 請求は停止しますが、AWS リソース請求はアカウントを閉鎖するまで停止しません。詳細については、[「アカウントを閉鎖する前に知っておくべきこと」](#)を参照してください。

Q: アプリケーションアカウントのオフボーディングをスケジュールできますか？

はい。RFCs を特定の時間に実行するようにスケジュールできます。ただし、管理 [アカウント | オフボードアプリケーションアカウント RFC](#) を [スケジュールする前に](#)、[アプリケーションアカウント | オフボード RFC](#) を確認する必要があります。詳細については、[「RFC スケジューリング」](#) を参照してください。

## RACI のアプリケーションアカウントのオフボーディング

- R: 責任者。リストされたタスクの完了を担当する当事者。
- A: 責任を負う当事者。完了したタスクを承認する当事者。
- C: 相談先。通常、対象分野の専門家として意見を求められ、双方向のコミュニケーションがある当事者。
- I: 情報提供者。多くの場合、タスクまたは成果物の完了時にのみ、進捗状況について通知される当事者。

| アクティビティ                                                   | お客様 | AWS Managed Services (AMS) |
|-----------------------------------------------------------|-----|----------------------------|
| 前提条件                                                      |     |                            |
| オフボードされる各 AWS アカウント ID のルート E メールアドレスへのアクセスを検証する          | R   | C                          |
| 推奨される顧客アクションに関する AMS ドキュメントを確認し、AMS オフボーディング用のアカウントを準備する  | R   | C                          |
| 必要に応じて、RFC を送信してデベロッパーモードを有効にし、AMS オフボーディング用のアカウントを準備します。 | R   | I                          |
| 必要に応じて、EC2 スタックアクセスの代替方法を選択します。                           | R   | I                          |
| オフボーディング                                                  |     |                            |

| アクティビティ                                                                    | お客様 | AWS Managed Services (AMS) |
|----------------------------------------------------------------------------|-----|----------------------------|
| RFCs を送信してアプリケーションアカウントのオフボーディングを確認してリクエストする                               | R   | I                          |
| アプリケーションアカウントから AMS コンポーネントをオフボードする                                        | I   | R                          |
| オフボーディングされたアカウントを AMS CSDM に通知して AMS 請求を停止する                               | R   | I                          |
| オフボード後                                                                     |     |                            |
| ルートユーザーアカウントのパスワードをリセットし、オフボードアカウントのルートアクセスを検証する                           | R   | C                          |
| アカウントを閉鎖するか、AMS オフボーディングドキュメントの推奨顧客アクションに関する AMS ガイダンスに従って、アカウントの運用を継続します。 | R   | C                          |

## オフボードコアアカウント

マルチアカウントランディングゾーン Core アカウントをオフボードするには、次の手順を実行します。

1. ランディングゾーン内のすべてのアプリケーションアカウントが AMS からオフボードされていることを確認します。
2. アカウントに開いている RFCs がないことを確認します。詳細については、「[RFCs の作成、クローン作成、更新、検索、キャンセル](#)」を参照してください。
3. すべての Core アカウントのプライマリまたはルートユーザーの E メールアドレスにアクセスできることを確認します。詳細については、「[マルチアカウントランディングゾーンアカウント](#)」を参照してください。
4. 管理アカウントのプライマリまたはルートユーザーの電話番号にアクセスできることを確認します。IAM AWSManagedServicesBillingRole ロールを使用して電話番号を更新します。詳細

については、[「アカウントに関連付けられている電話番号を更新するにはどうすればよいですか? AWS」](#)を参照してください。

5. AMS ランディングゾーン管理アカウントにログインし、AMS サービスリクエストを送信します。サービスリクエストで、 を指定してランディングゾーン全体をオフボードします。

Core アカウントがオフボードされた後、以下が発生します。

- すべてのコンポーネントは AMS サービスとの関連付けが解除されますが、一部の AWS リソースはアカウントに残ります。AMS オフボード Core アカウントを保持または閉鎖することを選択できます。
- AMS 請求は停止されますが、アカウントを閉鎖するまで AWS 請求は停止されません。詳細については、[「アカウントを閉鎖する前に知っておくべきこと」](#)を参照してください。
- アカウントが閉鎖されている場合、アカウントは suspended 状態で 90 日間組織に表示されます。90 日後、閉鎖されたメンバーアカウントは完全に削除され、組織に表示されなくなります。
- アカウントが閉鎖された後も、90 サポート 日間サインインしてサポートケースまたは連絡先を提出できます。
- アカウントが 90 日間閉鎖されると、アカウントに残っているコンテンツはすべて完全に削除され、残りの AWS サービスは終了します。

## コアアカウントのオフボーディングに関するよくある質問

Q: フェデレーティッド IAM ロールを使用して、オフボードされた Core アカウントに引き続きアクセスできますか?

はい。AMS が作成した[デフォルト AWS Identity and Access Management \(IAM\) ロール](#)は、オフボードされたアカウントで引き続き使用できます。ただし、これらのロールとポリシーは AMS アクセス管理で使用するよう設計されています。ユーザーに必要なアクセスを提供するには、独自の IAM リソースをデプロイする必要がある場合があります。

Q: AMS マルチアカウントランディングゾーンからオフボーディングした後、管理、共有サービス、ネットワーク、またはその他のアプリケーション [以外の MALZ](#) アカウントへのフルアクセスを取得するにはどうすればよいですか?

オフボーディング後、[「紛失または忘れたルートユーザーパスワードのリセット」](#)の手順に従って、プライマリ (ルート) ユーザー認証情報を使用して管理アカウント以外の Core アカウントにアクセスします。他のアカウントタイプとは異なり、管理アカウントは、ルートユーザーに関連

付けられているアクセスできない多要素認証 (MFA) デバイスを保持して、使用を防止します。  
ルートアクセスを回復するには、[失われた MFA デバイス復旧プロセス](#)に従う必要があります。

Q: Core アカウントのオフボーディング中にどのような変更が行われますか？

サービスがアカウントをオフボードするときに AMS が実行するアクションの詳細については、「」を参照してください[オフボーディングの変更](#)。

Q: Core アカウントのオフボーディングが完了するまでにどれくらいかかりますか？

Core アカウントのオフボーディングプロセスは通常、完了までに最大 30 日かかります。ただし、必要なすべてのステップが正しく完了していることを確認するには、オフボーディング開始の少なくとも 7 日前にオフボーディングリクエストを開始する必要があります。移行を容易にするには、事前に計画し、オフボーディングリクエストを事前に送信してください。

Q: AMS オフボーディング後に共有コンポーネントを管理するにはどうすればよいですか？

AMS Managed Active Directory およびその他の共有サービスインフラストラクチャコンポーネントは、AMS オペレーターアクセス用に設計されています。これらのコンポーネントへのフルアクセスを保持するには、Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループ、AWS Organizations サービスコントロールポリシー (SCP) の更新、またはその他の変更が必要になる場合があります。

Q: オフボーディングされた Core アカウントを閉鎖できますか？

デフォルトでは、アプリケーションアカウントには、AWS Organizations メンバーシップ、トランジットゲートウェイネットワーク接続、AMS Managed Active Directory 経由の DNS 解決など、MALZ Core アカウントへの複数の依存関係があります。これらの依存関係を解決したら、オフボードされた Core アカウントを廃止して閉鎖できます。詳細については、「[マルチアカウントランディングゾーンアカウント](#)」を参照してください。

## コアアカウントオフボーディング RACI

- R: 責任者。リストされたタスクの完了を担当する当事者。
- A: 責任を負う当事者。完了したタスクを承認する当事者。
- C: 相談者。通常、対象分野の専門家として意見を求められ、双方向のコミュニケーションがある当事者。
- I: 情報提供者。多くの場合、タスクまたは成果物の完了時にのみ、進捗状況について通知される当事者。

| アクティビティ                                                                    | お客様 | AWS Managed Services (AMS) |
|----------------------------------------------------------------------------|-----|----------------------------|
| 前提条件                                                                       |     |                            |
| オフボードされる各 AWS アカウント ID のルート E メールアドレスへのアクセスを検証する                           | R   | C                          |
| 管理アカウントのルートユーザーの電話番号へのアクセスを確認し、更新する                                        | R   | C                          |
| 推奨される顧客アクションに関する AMS ドキュメントを確認し、AMS オフボーディング用のアカウントを準備する                   | R   | C                          |
| オフボーディング                                                                   |     |                            |
| ランディングゾーンのオフボーディングをリクエストするサービスリクエストを送信する                                   | R   | I                          |
| Core アカウントから AMS コンポーネントをオフボードする                                           | I   | R                          |
| オフボード後                                                                     |     |                            |
| ルートユーザーアカウントのパスワードをリセットし、オフボードアカウントのルートアクセスを検証する                           | R   | C                          |
| アカウントを閉鎖するか、AMS オフボーディングドキュメントの推奨顧客アクションに関する AMS ガイダンスに従って、アカウントの運用を継続します。 | R   | C                          |

## オフボーディングの変更

次の表は、マルチアカウントランディングゾーンのオフボーディング、潜在的な影響、推奨されるアクションに対して AMS が実行するアクションを示しています。



| コンポーネント     | アカウントの種類      | オフボードのために実行されたアクション                                                                                                                                                                         | 潜在的な影響                                                                                                                                                                                                                | 推奨される顧客アクション                                                                                                                                                  |
|-------------|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アクセス管理      | アプリケーションアカウント | <p>オフボーディング後、just-in-timeの時間制限付きアクセス用のスタックアクセス RFCs を送信して、AMS 踏み台ホストを介して EC2 スタックにアクセスできなくなります。</p> <p>AMS は、既存の EC2 リソーススタック (PBIS Open エージェント、ドメイン結合スクリプト) のアクセス関連コンポーネントを管理しなくなりました。</p> | <p>RFS 経由で AMS 踏み台を使用して EC2 インスタンスにアクセスできない</p> <p>AMS 提供以外の AMIs から起動された EC2 インスタンスが Managed Active Directory ドメインに参加していない</p> <p>削除しない場合、既存のリソーススタックの AMS 起動スクリプトは、AMS 依存関係がないためエラーを生成し、別のドメインへの再参加を防ぐ可能性があります。</p> | <p>代替方法を使用して EC2 インスタンスにアクセスする (「」を参照<a href="#">代替手段にアクセスする</a>)</p> <p>既存の EC2 リソーススタックから AMS 起動スクリプトを削除する (「」を参照<a href="#">AMS EC2 起動スクリプトを無効にする</a>)</p> |
| アクセス管理 (続き) | コアアカウント       | PBIS Open から PBIS Enterprise (AD Bridge) に移行した場合、AMS はコアアカウントのオフボーディング後にライセンスを更新しなくなります。                                                                                                    | PBIS Enterprise ライセンスの有効期限が切れることが許可されている場合、Active Directory 認証情報は既存の Linux ベースの EC2 インスタンススタックでは無効です。                                                                                                                 | PBIS Enterprise (AD Bridge) に移行した場合は、ライセンスを維持するか廃止するかを決定します (「」を参照 <a href="#">PBIS Open/Enterprise (AD Bridge)</a> )。                                        |



| コンポーネント                   | アカウントの種類              | オフボードのために実行されたアクション                                                                                                                                                                                                                                                                           | 潜在的な影響                                                                                                                                                  | 推奨される顧客アクション                                                                                                                                                                       |
|---------------------------|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ログ記録、モニタリング、インシデント/イベント管理 | アプリケーションアカウントとコアアカウント | <p>デプロイする AMS コンポーネント <a href="#">AMS でのベースラインモニタリングからのアラート</a> が削除されます</p> <p>デプロイ済みの既存の Amazon CloudWatch アラームは残りますが、AMS インシデントは作成されなくなります</p> <p>AWS Config AMS と MALZ Core セキュリティアカウントからの集約認可が削除される</p> <p>AWS Config ルールはデプロイされたままで、Amazon GuardDuty は有効のままですが、AMS インシデントは作成されなくなります</p> | <p>新しく作成されたリソースには、AMS ベースラインモニタリングとアラームが適用されていません</p> <p>インフラストラクチャメトリクスアラームとセキュリティイベントが AMS インシデントを生成しなくなった</p> <p>AWS Config は中央アカウントに集約されなくなりました</p> | <p>オペレーションメトリクスを定義、キャプチャ、分析してワークロードイベントを表示し、適切なアクションを実行します。</p> <p>必要なアラートワークフローを実装して、必要な運用モニタリングとアラームを新しいリソースに引き続き適用し、AWS Config と Amazon GuardDuty からセキュリティアラートを受信できるようにします。</p> |
| 継続性管理 (バックアップと復元)         | アプリケーションアカウント         | <p>AMS はバックアップジョブをモニタリングしたり、バックアップおよび復元リクエストを実行したりしなくなりました</p> <p>AMS のデフォルトのバックアップポリシー、バックアップ暗号化キー、バックアップロールは残ります</p>                                                                                                                                                                        | バックアップオペレーションの失敗に気付かない場合があります                                                                                                                           | バックアッププラン設定のモニタリングとレビュー                                                                                                                                                            |

| コンポーネント  | アカウントの種類              | オフボードのために実行されたアクション                                                                                                                                                                                                            | 潜在的な影響                                                                                                                    | 推奨される顧客アクション                                                            |
|----------|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| パッチ管理    | アプリケーションアカウントとコアアカウント | <p>AMS は、パッチ適用オペレーションが正常に実行されるかどうかをモニタリングしたり、手動パッチ適用を実行したりしなくなりました。</p> <p>AMS は AMS インフラストラクチャコンポーネントを更新しなくなりました</p> <p>AMS が提供するパッチベースラインは保持されます</p> <p>AMS が提供する AWS Systems Manager パッチオートメーションランブックは共有解除され、使用できなくなります</p> | <p>パッチ適用オペレーションの失敗に気付かない場合があります</p> <p>AMS が提供する Systems Manager Automation ランブックに依存する既存のパッチ設定は、中断されないように再設定する必要があります</p> | 必要に応じてパッチ適用設定を確認して再設定する                                                 |
| ネットワーク管理 | アプリケーションアカウント         | 指定した場合、オフボーディングされたアプリケーションアカウントの Transit Gateway アタッチメントは削除されます。                                                                                                                                                               | オフボードアプリケーションアカウントは、Transit Gateway を使用して Managed Active Directory や他のアプリケーションアカウントなどの共有サービスにアクセスできなくなります。                | トランジットゲートウェイ接続を保持する False には、DeleteTransitGatewayAttachment として を指定します。 |

| コンポーネント  | アカウントの種類      | オフボードのために実行されたアクション                                                                                                                                                                                                                                      | 潜在的な影響                                                                                                              | 推奨される顧客アクション                                                                                |
|----------|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| セキュリティ管理 | アプリケーションアカウント | <p>アカウントは中央の Trend Micro DSM コンソールからデタッチされます。また、エンドポイントエージェントは AMS インシデントプロセスを通じてアラートを転送しなくなりました</p> <p>Trend Micro エージェントはインストールされたままですが、AMS によって管理または更新されなくなります。</p> <p>Trend Micro エージェントをデプロイする AMS が提供する AMI のカスタマイズは、AMS によって維持または更新されなくなりました。</p> | <p>EC2 インスタンスエンドポイントのマルウェア検出に気付かない可能性がある</p> <p>Trend micro エージェントは、AMS 提供以外の AMIs から起動された EC2 インスタンスにデプロイされません</p> | <p>Trend Micro を続行または中止するためのオプションを検討する (「」を参照<a href="#">Trend Micro Deep Security</a>)</p> |

| コンポーネント       | アカウントの種類              | オフボードのために実行されたアクション                                                                                                                                   | 潜在的な影響                                                                                                                     | 推奨される顧客アクション                                                                                     |
|---------------|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| セキュリティ管理 (続き) | コアアカウント               | <p>Trend Micro DSM インフラストラクチャは共有サービスアカウント内に残りますが、AMS によって維持または更新されなくなりました</p> <p>Trend Micro DSM は AMS インシデントプロセスを通じてアラートを転送しなくなりました</p>              | <p>EC2 インスタンスエンドポイントのマルウェア検出に気付かないことがある</p> <p>インフラストラクチャが維持されていない場合、EC2 インスタンスエンドポイントの保護に影響する可能性があります (定義の更新、ライセンスなど)</p> | <p>Trend Micro を継続するか中止するかを決定する (「」を参照 <a href="#">Trend Micro Deep Security</a>)</p>            |
| 変更管理          | アプリケーションアカウントとコアアカウント | <p>AMS RFC コンソールと API が削除されました</p> <p>アカウントレベルのアクセス制限を含む AMS カスタムサービスコントロールポリシー (SCPs) は、アプリケーションアカウントのオフボーディング中にデタッチされ、コアアカウントのオフボーディング中に削除されます。</p> | <p>新しいリソースの作成、既存のリソースの変更、または既存の CloudFormation スタックの更新には、ネイティブ AWS API を使用する必要があります。</p> <p>アクセス制限は、AMS が提供する SCPs。</p>    | <p>ユーザーロールが AWS サービスを使用するのに十分なアクセス権限を付与していることを確認します。</p> <p>SCPs を作成してアカウントレベルのアクセス許可制限を提供する</p> |

| コンポーネント                       | アカウントの種類              | オフボードのために実行されたアクション                                                                                                                                        | 潜在的な影響                                                                                                                                                                          | 推奨される顧客アクション                                                                  |
|-------------------------------|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| サービス管理用の AMS OS イメージとオートメーション | アプリケーションアカウントとコアアカウント | <p>AMS は、AMS が提供する EC2 AMIs</p> <p>AMS が提供する EC2 AMIs、オフボーディングされたアカウントで引き続き使用できます。</p> <p>AMS が提供する Systems Manager Automation ランブックは共有解除され、使用できなくなります</p> | <p>オフボーディング後、AMS コンポーネントへの依存関係がないため、AMS は cfn-signal CloudFormation の送信で起動FAILUREされた AMIs を提供しました</p> <p>AMS が提供する Systems Manager Automation ランブックに依存する運用プロセスが失敗する可能性があります</p> | AMS が提供する AMIs または Systems Manager Automation ランブックに依存するビルドまたは運用プロセスを確認して更新する |
| 共有サービスインフラストラクチャ              | コアアカウント               | AMS アクセスは削除され、AMS は AMS Managed Active Directory などの共有コンポーネントを管理しなくなります AWS Transit Gateway。AWS Organizations                                              | 共有インフラストラクチャに対する管理の喪失                                                                                                                                                           | AMS Managed Active Directory への管理者アクセスをリセットし、共有サービスコンポーネントの管理を引き受ける           |

| コンポーネント              | アカウントの種類              | オフボードのために実行されたアクション                                                 | 潜在的な影響                                                            | 推奨される顧客アクション                                            |
|----------------------|-----------------------|---------------------------------------------------------------------|-------------------------------------------------------------------|---------------------------------------------------------|
| 報告                   | アプリケーションアカウントとコアアカウント | AMS は、集計レポートのアカウントレベルまたはリソースレベルの詳細を収集しなくなりました                       | 運用メトリクスとビジネスメトリクス (バックアップとパッチの適用、変更管理、インシデントアクティビティ) に関するインサイトの喪失 | アカウント間で必要な集計データレポートを独自のソリューションに置き換える                    |
| AMS アカウントチームとサービスデスク | アプリケーションアカウントとコアアカウント | AMS アカウントチーム (CSDM、CA) と AMS オペレーションサービスデスクがオフボードアカウントをサポートしなくなりました | AMS 設計のマルチアカウントランディングゾーンアーキテクチャと関連コンポーネントの専門知識による運用サポートの喪失        | 環境内のオペレーションをサポートするのに十分な人員と、アカウント構造とリソースに精通していることを確認します。 |

## 代替手段にアクセスする

AMS アカウントをオフボードした後、EC2 スタックへのアクセスを保持するための代替方法は次のとおりです。

- Session Manager を使用して、踏み台やインバウンドネットワークアクセスを必要とせずに、昇格されたアクセス許可を持つ EC2 インスタンスにアクセスします。詳細については、「[AWS Systems Manager Session Manager](#)」を参照してください。
- 新しいドメイン認証情報を使用して、EC2 インスタンスを別の Active Directory ドメインに再結合します。を使用する場合は Directory Service、[EC2 インスタンスを AWS Managed Microsoft AD ディレクトリに結合する](#)」を参照してください。
- 他のいずれかのアクセス方法または [AWS Systems Manager Run Command](#) を使用して作成したローカルユーザーアカウントを使用します。

## AMS EC2 起動スクリプトを無効にする

### Linux オペレーティングシステム:

ディストリビューションのパッケージマネージャーを使用して、ams-modules パッケージをアンインストールします。例えば、Amazon Linux 2 の場合は `yum remove ams-modules` を使用します。

### Windows オペレーティングシステム

Windows で EC2 起動スクリプトを無効にするには、次の手順を実行します。

#### 1. Windows Server 2008/2012/2012r2/2016/2019:

マネージドサービス起動のスケジュールされたタスクをタスクスケジューラから無効化または削除します。スケジュールされたタスクを一覧表示するには、`Get-ScheduledTask -TaskName '*Ec2*'` コマンドを実行します。

#### Windows Server 2022:

[EC2Launch v2 タスク](#)を削除します。このタスクはInitialize-AMSBoot、インスタンスの `C:\ProgramData\Amazon\EC2Launch\config\agent-config.yml` のpostReadyステージで実行されます。以下は、の例のスニペットですagent-config.yml。

```
{
  "task": "executeScript",
  "inputs": [
    {
      "frequency": "always",
      "type": "powershell",
      "runAs": "localSystem"
    }
  ]
}
```

#### 2. (オプション) 次のファイルコンテンツを削除します。

```
C:\Program Files\WindowsPowerShell\Modules\AWSManagedServices.*
C:\Windows\System32\WindowsPowerShell\v1.0\Modules
\AWSManagedServices.Build.Utilities\*
```

## PBIS Open/Enterprise (AD Bridge)

PBIS Open または PBIS Enterprise (AD Bridge) エディションを使用しているかどうかを確認するには、Linux EC2 マネージドインスタンスで次のコマンドを実行します。

```
yum info | grep pbis
```

PBIS Enterprise (AD Bridge) を示す出力例を次に示します。

```
Name      : pbis-enterprise
From repo  : pbise
Name      : pbis-enterprise-devel
Repo      : pbise
Description : The pbis-enterprise-devel package includes the development
```

### PBIS オープン

PBIS Open は、BeyondTrust がサポートしなくなった非推奨製品です。詳細については、[BeyondTrust pbis-open ドキュメント](#)を参照してください。

### AD Bridge (PBIS Enterprise)

次のいずれかを試すことができます。

- ライセンスを更新し、AD Bridge の運用を継続します。ライセンスとサポートについては、BeyondTrust にお問い合わせください。
- AD Bridge の使用を中止します。次の Shell コマンドを実行して、Linux マネージドインスタンスから PBIS-Enterprise パッケージを削除します。詳細については、BeyondTrust ドキュメント「[ドメインを残して AD Bridge エージェントをアンインストール](#)する」を参照してください。

```
$ sudo /opt/pbis/bin/uninstall.sh purge
```

PBIS エージェントを削除せずに AMS マネージド Active Directory ドメインを残す

PBIS エージェントを削除せずに AMS マネージド Active Directory を離れるオプションがあります。オペレーティングシステムに応じて、次のいずれかのソリューションを使用します。



## Linux operating systems

AMS マネージド AD の PBIS を使用して、次のシェルコマンドを実行して Linux EC2 インスタンスの結合を解除します。詳細については、使用しているバージョンに応じて、[BeyondTrust pbis-open](#) または [BeyondTrust AD Bridge](#) のドキュメントを参照してください。

```
$ sudo /opt/pbis/bin/domainjoin-cli leave
```

次のようなエラーメッセージが表示される場合があります。

```
Error: LW_ERROR_KRB5_REALM_CANT_RESOLVE [code 0x0000a3e1]  
Cannot resolve network address for KDC in requested realm
```

このエラーが発生した場合は、次のコマンドを実行して AD プロバイダーレジストリを削除し、lwsmdサービスを再起動します。

```
$ /opt/pbis/bin/regshell dir '[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory\DomainJoin]'
```

前のコマンドから受け取ったディレクトリ ID 出力 (例: **A123EXAMPLE.AMAZONAWS.COM**) を使用して、次のコマンドを実行します。

```
$ /opt/pbis/bin/regshell delete_tree \  
'[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory\DomainJoin\  
\DIRECTORYID]'  
  
$ /etc/pbis/redhat/lwsmd restart  
  
$ /opt/pbis/bin/lwsm restart lwreg
```

## Windows operating systems

```
# Collect hostname and domain name using:  
  
Test-ComputerSecureChannel -verbose  
  
# Disjoin computer from the domain:  
  
netdom remove hostname /domain:domain name /force
```

**Note**

「」で説明されているように、Managed Services Startup スケジュールされたタスクを無効化または削除してください[AMS EC2 起動スクリプトを無効にする](#)。

## Trend Micro Deep Security

Trend Micro Deep Security の使用を続行または中止するには、次のいずれかのオプションを使用します。

### 使用を継続する

- (MALZ 全体をオフボーディングする場合) Core アカウントのオフボーディング後、オフボーディングされたアプリケーションアカウントを既存の Trend Micro Deep Security Manager (DSM) に再接続し、共有サービスアカウントのライセンスを維持します。詳細については、[AWS 「クラウドアカウントの追加」](#) および [「ライセンス情報の確認」](#) を参照してください。
  1. 共有サービスアカウントにログインし、Secrets Manager コンソールに移動します。
  2. `/ams/eps/` パスに保存されている DSM コンソール管理者認証情報を取得します。
  3. <https://dsm.sentinel.int> で DSM コンソールにログインします。
  4. クロスアカウントロールの使用 を選択し、 と入力します `arn:aws:iam::ACCOUNTID:role/mc_eps_cross_account_role`。ACCOUNTID をオフボーディングされたアプリケーションアカウント ID に置き換えます。
  5. [次へ] を選択します。
  6. DSM がアカウント検出を処理し、同期が成功したことを示すまで数分待ちます。
- オフボードのアプリケーションアカウントを新しい Trend Micro DSM インストールに再接続します。詳細については、[「エージェントのアクティブ化と保護」](#) および [「エージェントのアクティブ化」](#) を参照してください。
- オフボーディングされたアプリケーションアカウントを Trend Micro Cloud One に再接続します。詳細については、[「Migrate from Deep Security to Workload Security」](#) および [「Migrate from an on-premises DSM」](#) を参照してください。

## 使用の中止

- Trend Micro Deep Security Agents をオフボードされたアプリケーションアカウントからアンインストールします。詳細については、[「ディープセキュリティのアンインストール」](#)を参照してください。

# 変更管理モード

AWS Managed Services (AMS) は、変更管理モードを使用して AMS Advanced の変更を保護します。変更管理モードは、環境の高い運用基準を維持し、リスクを制御し、悪影響を防ぐのに役立ちます。AMS Advanced には、さまざまなレベルのコントロールとリスクを提供するさまざまなモードがあります。カスタマー管理モードを除くすべてのモードは、AMS によって管理されます。使用可能な変更管理モードは次のとおりです。

- RFC モード (以前の標準 CM モード): 「変更のリクエスト」 (RFC) システムと AMS カスタム変更タイプ (CTs)
- 直接変更モード: RFC モードと同じで、AWS APIs とコンソールを使用して AMS マネージドリソースを作成する
- AMS での AWS Service Catalog: Direct Change モードと同様ですが、AMS 変更管理システム (RFCs) を使用する代わりに、AWS Service Catalog を使用して AMS が管理するリソースを作成します。
- デベロッパーモード: 直接変更モードと同じですが、AWS APIs とコンソールで作成したリソースのみが AMS 管理対象ではなく、その管理はお客様の責任となります。
- セルフサービスプロビジョニング (SSP) モード: AMS 変更管理システムにアクセスできない (RFCs なし) 点を除き、デベロッパーモードと同じ
- カスタマーマネージドモード: AMS はマルチアカウントランディングゾーンランディングゾーンを提供しますが、すべてのリソース管理はお客様の責任となります。

AWS Managed Services (AMS) 変更管理システムは、変更管理 (CM) API を使用して、マルチアカウントランディングゾーン (MALZ) アカウントとシングルアカウントランディングゾーン (SALZ) アカウントの両方の変更リクエスト (RFCs) を作成および管理するためのオペレーションを提供します。

変更リクエスト (RFC) は、AMS インターフェイスを介してユーザーまたは AMS がマネージド環境に変更を加えるために作成したリクエストであり、特定のオペレーションの変更タイプ (CT) ID が含まれます。

AMS 変更管理 (CM) API は、変更リクエスト (RFCs) を作成および管理するためのオペレーションを提供します。RFCs を作成、更新、送信、承認、拒否、キャンセルできます。AMS 演算子は、RFCs を作成、更新、送信、承認、拒否、キャンセル、およびクローズとしてマークできます。

タグや他の名前で使用されない AMS リザーブドプレフィックスのリストについては、[「リザーブドプレフィックス」](#)を参照してください。

スキーマや例など、各変更タイプの詳細については、[「AMS 変更タイプリファレンス」](#)を参照してください。

**Note**

すべての変更管理 API コールは AWS CloudTrail に記録されます。詳細については、「[ログへのアクセス](#)」を参照してください。

## モードの概要

この情報を使用して、ビジネス成果を達成するための柔軟性と規範的なガバナンスの望ましい組み合わせに基づいて、アプリケーションをホストするための適切な AWS Managed Services (AMS) モードを選択します。

この情報の対象となる対象者は次のとおりです。

- ランディングゾーンの戦略とガバナンスを担当するカスタマーチーム。この情報は、チームが内部および外部の顧客に提供する AMS モードを使用して、AMS が管理するランディングゾーンの基盤を構築するのに役立ちます。
- アプリケーションの AMS への移行を担当するビジネスオーナーとアプリケーションオーナー。この情報は、アプリケーションの移行/ホストに適した AMS モードを使用して、アプリケーションの移行を計画するのに役立ちます。ソフトウェア開発ライフサイクル (SDLC) ライフサイクルのさまざまなフェーズで、同じアプリケーションを複数の AMS モードでホストできます。
- AMS パートナーには、AMS を構築して移行するためのさまざまなオプションについて顧客をガイドする役割があります。

この情報は、AMS マネージドプラットフォームを設定する基盤フェーズ中、および基盤からクラウド導入ジャーニーの移行フェーズに移行するときに、AMS へのオンボーディングが完了し、アプリケーションのガバナンスと運用に重点を置いている直後に最も役立ちます。

## AMS のモードとアカウントのタイプ

AWS Managed Services (AMS) モードは、各モードの特定のガバナンスフレームワークの下で AMS サービスとやり取りする方法として定義できます。ランディングゾーンの違い、マルチアカウントランディングゾーンまたは MALZ とシングルアカウントランディングゾーンまたは SALZ が記録されます。

**Note**

アプリケーションのデプロイと適切な AMS モードの選択の詳細については、[「AMS モードとアプリケーションまたはワークロード」](#)を参照してください。

さまざまなモードの実際のユースケースについては、[「AMS モードの実際のユースケース」](#)を参照してください。

次の表は、AMS サービスあたりのモードの説明です。

| AMS 機能                                    | RFC モード<br>(以前の標準<br>CM モード) /<br>OOD*        | 直接変更<br>モード                                                  | AWS Service<br>Catalog | セルフサービス<br>プロビジョニン<br>グ/デベロッパー<br>モード | カスタマー<br>管理              |
|-------------------------------------------|-----------------------------------------------|--------------------------------------------------------------|------------------------|---------------------------------------|--------------------------|
| ランディング<br>ゾーンの設定                          | MALZ と<br>SALZ                                | MALZ と<br>SALZ                                               |                        | MALZ と SALZ                           |                          |
| 変更管理                                      | 変更スケ<br>ジュール、<br>手動変更の<br>レビュー、<br>変更レコー<br>ド | IAM やセ<br>キュリティ<br>グループな<br>どの高リス<br>クの変更の<br>RFC モード<br>と同じ |                        | なし                                    |                          |
| ログ記録、<br>モニタリン<br>グ、ガード<br>レール、イ<br>ベント管理 | はい (サポートされているリソース)                            |                                                              |                        | いいえ                                   |                          |
| 継続性管理                                     | はい (サポートされているリソース)                            |                                                              |                        | 該当なし/いいえ                              | いいえ                      |
| セキュリ<br>ティ管理                              | インスタンスレベルのセキュリティコント<br>ロールとアカウントレベルのコントロール    |                                                              |                        | アカウントレ<br>ベルのコント<br>ロール               | AWS 組織レ<br>ベルのコン<br>トロール |

| AMS 機能              | RFC モード<br>(以前の標準<br>CM モード) /<br>OOD* | 直接変更<br>モード | AWS Service<br>Catalog | セルフサービス<br>プロビジョニン<br>グ/デベロッパー<br>モード | カスタマー<br>管理 |
|---------------------|----------------------------------------|-------------|------------------------|---------------------------------------|-------------|
| パッチ管理               | はい                                     |             |                        | 該当なし/いいえ                              | いいえ         |
| インシデントと問題の<br>管理    | AMS がサポートするリ<br>ソースの応答と解決の SLA         |             |                        | 結果のリソース<br>のレスポンス<br>SLA              | いいえ         |
| 報告                  | はい                                     |             |                        | いいえ                                   |             |
| サービスリ<br>クエスト管<br>理 | はい                                     |             |                        | サポートリクエ<br>ストのみ                       | いいえ         |

\*Operations On Demand (OOD) には、RFC モードを使用して、専用のリソースを通じて変更を管理するためのサービスがあります。詳細については、[「Operations on Demand catalog of offerings」](#) および「Cloud Service Delivery Manager (CSDM)」を参照してください。

#### Note

[AMS でのセルフサービスプロビジョニングモード](#) とはどちらも、ネイティブ AWS サービスに根ざした複雑なアーキテクチャを持つアプリケーションに適しているように見える [AMS Advanced Developer モード](#) 場合があります。ワークロードを設計するときは、ビジネスコンテキストに基づいて、運用上の優秀性と俊敏性のトレードオフを行います。これは、アプリケーションの SSP モードまたはデベロッパーモードの選択を検討する良い方法です。選択は、アプリケーションの SDLC フェーズに基づいて変更される場合があります。例: アプリケーションが本番環境に対応している場合、このモードでは AMS ガードレールが厳しくなるため、SSP モードの方が適切なオプションである可能性があります。ガードレールは、IAM 更新の RFC ベースの変更管理やアプリケーション OU レベルで SCPs などの予防的コントロールの形式で適用されます。これらのビジネス上の意思決定がエンジニアリングの優先度を左右する可能性があります。ガバナンスと運用サポートを犠牲にして、「事前生産」フェーズでアプリケーション所有者の柔軟性を高めるように最適化できます。

## MALZ アーキテクチャと関連する AMS モード

AMS マルチアカウントランディングゾーン (MALZ) では、デフォルトの組織単位 (OU)、カスタマーマネージド OU、マネージド OU、または開発 OU でアプリケーションアカウント (またはリソースアカウント) を自動的にプロビジョニングできます。これらの各 OUs で作成されたアプリケーションアカウントでプロビジョニングされるインフラストラクチャは、これらの基本 OUs によって提供される特定の AMS モードの対象となります。同じアプリケーションアカウントで 2 つ以上のモードの組み合わせを見つけるのが一般的です。例えば、RFC モードと SSP モードは、トリガー関数には API Gateway と Lambda、取り込みとオーケストレーションには EC2、S3、SQS で構成されるパイプラインアーキテクチャをホストする AMS マネージドアカウントに共存できます。この場合、SSP モードは Lambda と API Gateway に適用されます。

図 1 は、AMS の基本的な OUs を通じてさまざまなモードがどのように提供されるかを示しています。AMS で新しいアプリケーションアカウントをリクエストするときは、アカウントの OU を選択する必要があります。

## MALZ アーキテクチャと関連する AMS モード

AMS は、サービスコントロールポリシー (SCP) OUs を活用します。SCPs これは、各 AMS モードを使用してガバナンスフレームワークを適用する方法として機能します。基礎 OUs に適用されるガバナンスとセキュリティガードレール (SCPs の形式) も、カスタム/子 OUs に自動的に適用されます。子 OUs に追加の SCPs をリクエストできます。アプリケーションアカウントは モードと同じではないことを理解することが重要です。モードは、アカウント内でプロビジョニングされたインフラストラクチャに適用され、AMS と顧客間の運用責任を定義します。

## 図 1: MALZ アーキテクチャと関連する AMS モード

### Note

「制限 OUs のカスタムポリシーをリクエストできることを意味します。ポリシーは、AMS の機能に干渉して運用上の優秀性を提供しないように、case-by-case で AMS によって承認されます。AMS ガードレールの詳細なリストについては、ユーザーガイドの [「AMS ガードレール」](#) を参照してください。



## AMS モードとアプリケーションまたはワークロード

新しいアプリケーションアカウントをリクエストするか、既存のアプリケーションアカウントでアプリケーションをホストして、適切なモードを選択するときは、アプリケーションの運用要件とガバナンス要件を検討してください。各アプリケーションまたはワークロードに適した AMS モードの選択は、次の要因によって異なります。

- 環境が提供する SDLC ライフサイクル関数のタイプ (変更がモデル化されていないサンドボックス、頻繁に変更される UAT、最小限の変更と高度に規制された本番稼働など)
- 必要なガバナンスポリシー (OU レベルで SCPs を通じて実施)
- 運用モデル (運用責任を所有する場合、または AMS にそれを外部委託する場合)
- クラウドでの運用にかかる時間や運用コストなど、期待されるビジネス成果。

### Note

AMS サービスごとのモードタイプの詳細については、[「AMS のモードとアカウントのタイプ」](#)を参照してください。

さまざまなモードの実際のユースケースについては、[「AMS モードの実際のユースケース」](#)を参照してください。

次の表は、アプリケーション所有者が最適な AMS モードを決定するための重要な考慮事項の概要を示しています。アプリケーション所有者は、特定のアプリケーションに適用されるモードを完全に理解するために、アプリケーション移行の前に評価フェーズを含める必要があります。例: クラウドネイティブサービスまたはサーバーレスアーキテクチャに基づくアプリケーションの場合、最適なオプションは、開発者モードで構築と反復を開始し、AMS Managed – SSP モードを使用して最終的な Infrastructure as Code をデプロイすることです。この場合、自動デプロイ用に作成された CloudFormation テンプレートが AMS によって定められた取り込みガイドラインを確実に満たすために、軽いリファクタリングが必要になる場合があります。さらに、IAM アクセス許可は、最小特権モデルに従っていることを確認するために、AMS Security によって承認される必要があります。

アプリケーションをホストするために選択された AMS モードは、希望するクラウド運用モデルに向けて構築するのに役立ちます。

**Note**

複数のクラウド運用モデルは、アプリケーションをホストするために選択されたさまざまな AMS モードに基づいて、単一の AMS Managed Landing Zone に存在できます。

| 決定の問題 | 標準 CM<br>モード/<br>OOD* | AWS<br>Service<br>Catalog | 直接変更<br>モード | セルフサー<br>ビスプロビ<br>ジョニング | デベロッ<br>パーモード | カスタマー<br>管理 |
|-------|-----------------------|---------------------------|-------------|-------------------------|---------------|-------------|
|-------|-----------------------|---------------------------|-------------|-------------------------|---------------|-------------|

## 運用準備状況

|                                        |                                           |                                                            |                                                                                           |            |
|----------------------------------------|-------------------------------------------|------------------------------------------------------------|-------------------------------------------------------------------------------------------|------------|
| ログ記<br>録、モ<br>ニタリ<br>ング、イ<br>ベ<br>ント管理 | すべてのマネージドインフラストラク<br>チャを担当する AMS          | セルフサー<br>ビスプロ<br>ビジョニ<br>ングサー<br>ビス (SSP) を担<br>当するお客<br>様 | AMS CM シ<br>ステムの外<br>部で開発者<br>IAM ロール<br>を使用して<br>プロビジョ<br>ニングされ<br>たリソース<br>を担当する<br>お客様 | お客様の責<br>任 |
| 継続性管<br>理                              | お客様が選択したバックアッププラン<br>を実行する AMS 責任         | セルフサー<br>ビスプロ<br>ビジョニ<br>ングサー<br>ビス (SSP) を担<br>当するお客<br>様 | AMS CM シ<br>ステムの外<br>部で開発者<br>IAM ロール<br>を使用して<br>プロビジョ<br>ニングされ<br>たリソース<br>を担当する<br>お客様 |            |
| インスタ<br>ンスレベ                           | オンプレミスドメインによる一方向<br>AD 信頼を通じて AMS 管理。マネージ | 該当しない                                                      | AMS CM シ<br>ステムの外<br>部で開発者                                                                |            |

| 決定の問題                                        | 標準 CM<br>モード/<br>OOD*               | AWS<br>Service<br>Catalog | 直接変更<br>モード | セルフサー<br>ビスプロビ<br>ジョニング                                   | デベロッ<br>パーモード                                                                             | カスタマー<br>管理 |
|----------------------------------------------|-------------------------------------|---------------------------|-------------|-----------------------------------------------------------|-------------------------------------------------------------------------------------------|-------------|
| ルのアク<br>セス管理                                 | ドインフラストラクチャが AMS ドメ<br>インに参加する必要がある |                           |             |                                                           | IAM ロール<br>を使用して<br>プロビジョ<br>ニングされ<br>たりソース<br>を担当する<br>お客様                               |             |
| セキュリ<br>ティ管理<br>とアカウ<br>ントレベ<br>ルのアク<br>セス管理 | すべてのマネージドアカウントの AMS<br>責任           |                           |             | すべてのマ<br>ネージド<br>アカウント<br>を担当する<br>AMS                    | AMS CM シ<br>ステムの外<br>部で開発者<br>IAM ロール<br>を使用して<br>プロビジョ<br>ニングされ<br>たりソース<br>を担当する<br>お客様 |             |
| パッチ管<br>理                                    | すべてのマネージドアカウントの AMS<br>責任           |                           |             | セルフサー<br>ビスプロ<br>ビジョニン<br>グサービス<br>(SSP) を担<br>当するお客<br>様 | AMS CM シ<br>ステムの外<br>部で開発者<br>IAM ロール<br>を使用して<br>プロビジョ<br>ニングされ<br>たりソース<br>を担当する<br>お客様 |             |

| 決定の問題              | 標準 CM<br>モード/<br>OOD*                                     | AWS<br>Service<br>Catalog                                                                      | 直接変更<br>モード                                                    | セルフサー<br>ビスプロビ<br>ジョニング                                   | デベロッ<br>パーモード                                                                             | カスタマー<br>管理 |
|--------------------|-----------------------------------------------------------|------------------------------------------------------------------------------------------------|----------------------------------------------------------------|-----------------------------------------------------------|-------------------------------------------------------------------------------------------|-------------|
| 変更管理               | すべてのマネージドアカウントの AMS<br>責任                                 |                                                                                                |                                                                | セルフサー<br>ビスプロ<br>ビジョニン<br>グサービス<br>(SSP) を担<br>当するお客<br>様 | AMS CM シ<br>ステムの外<br>部で開発者<br>IAM ロール<br>を使用して<br>プロビジョ<br>ニングされ<br>たリソース<br>を担当する<br>お客様 |             |
| プロビ<br>ジョニン<br>グ管理 | AMS で提供<br>されるプロ<br>ビジョニン<br>グオプショ<br>ンの規範的<br>および標準<br>化 | AMS 規<br>範標準<br>に従っ<br>て AWS<br>Service<br>Catalog<br>用の AWS<br>サービス<br>API を直<br>接使用す<br>る柔軟性 | AMS 規<br>範標準に<br>従って<br>AWS サー<br>ビス API<br>を直接使<br>用する柔<br>軟性 | SSP サービ<br>スAPIs を直<br>接使用する<br>柔軟性                       | プロビジョ<br>ニングに<br>AWS サー<br>ビス API を<br>直接使用す<br>る柔軟性                                      |             |

| 決定の問題                                                                               | 標準 CM<br>モード/<br>OOD*        | AWS<br>Service<br>Catalog | 直接変更<br>モード | セルフサー<br>ビスプロビ<br>ジョニング | デベロッ<br>パーモード                                                                                  | カスタマー<br>管理                         |
|-------------------------------------------------------------------------------------|------------------------------|---------------------------|-------------|-------------------------|------------------------------------------------------------------------------------------------|-------------------------------------|
| インシデ<br>ント管理<br>と監査                                                                 | すべてのマネージドアカウントの AMS 責任       |                           |             |                         | AMS 変更<br>管理システ<br>ムの外部で<br>開発者 IAM<br>ロールを使<br>用してプロ<br>ビジョニン<br>グされたリ<br>ソースを担<br>当するお客<br>様 |                                     |
| GuardRail<br>s と共有<br>インフラ<br>ストラク<br>チャ (ネッ<br>トワーク)<br>とセキュ<br>リティ<br>フレーム<br>ワーク | AMS Core アカウントを活用した規範的および標準化 |                           |             |                         |                                                                                                | AMS Core<br>アカウント<br>を柔軟にカ<br>スタマイズ |

アプリケーションの準備状況

| 決定の問題                             | 標準 CM<br>モード/<br>OOD* | AWS<br>Service<br>Catalog | 直接変更<br>モード | セルフサー<br>ビスプロビ<br>ジョニング                        | デベロッ<br>パーモード                                                                    | カスタマー<br>管理                                                                    |
|-----------------------------------|-----------------------|---------------------------|-------------|------------------------------------------------|----------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| アプリ<br>ケーショ<br>ンのリ<br>ファクタ<br>リング | ライトリファクタリングが必要        |                           |             |                                                | ライトリ<br>ファクタ<br>リングが<br>必要 (AMS<br>Standard<br>CM を使用<br>してプロビ<br>ジョニング<br>した場合) | リファクタ<br>リングが不<br>要                                                            |
| AWS サー<br>ビスのサ<br>ポート             | AMS でサポートされているものに限定   |                           |             |                                                |                                                                                  | 無制限                                                                            |
| ビジネス上の考慮事項                        |                       |                           |             |                                                |                                                                                  |                                                                                |
| 運用準備<br>時間                        | 3 ~ 6 か月              |                           |             | 6 か月 + 顧客のアプリケー<br>ションオペレーションのコ<br>ンピテンシーに依存する |                                                                                  | お客様のイン<br>フラストラ<br>クチャと<br>アプリケー<br>ション運用<br>のコンピテ<br>ンシーに応<br>じて 6 ~ 18<br>か月 |
| コスト                               | \$\$\$\$              |                           |             | \$\$\$                                         | \$\$                                                                             | \$                                                                             |

| 決定的問題     | 標準 CM モード/<br>OOD*                        | AWS Service Catalog | 直接変更モード | セルフサービスプロビジョニング                                            | デベロッパーモード                                                | カスタマー管理                                           |
|-----------|-------------------------------------------|---------------------|---------|------------------------------------------------------------|----------------------------------------------------------|---------------------------------------------------|
| アプリケーション例 | 3 層スタックの Webserver、コンプライアンスと規制要件のアプリケーション |                     |         | API Gateway を使用する<br>ウェブサーバー、ECS/EKS を活用したコンテナ化されたアプリケーション | Lambda、Glue、Athena などを使用する<br>Data Lake アプリケーションでの反復/最適化 | サンドボックス、サードパーティーマネージドアプリケーションなどの分散型アカウント/アプリケーション |

\*Operations On Demand (OOD) には、標準 CM モードを使用して、専用のリソースを通じて変更を管理するためのサービスがあります。詳細については、[「Operations on Demand catalog of offerings」](#) および「Cloud Service Delivery Manager (CSDM)」を参照してください。

#### Note

SSP モードとデベロッパーモードの料金比較では、同じ AWS サービスがプロビジョニングされていることを前提としています。

## AMS モードとビジネス目標および IT 目標の比較

図に示すように、アプリケーション用に高度に制御され標準化されたガバナンスモデルをお探しの場合は、AMS 管理の標準変更モード、AWS Service Catalog モード、または直接変更モードが最適です。運用準備を必要とせずにアプリケーションのイノベーションに焦点を当てたカスタムガバナンスモデルが必要な場合は、カスタマーマネージドモードを選択します。カスタマーマネージドモードでは、インシデント管理、設定管理、プロビジョニング管理、セキュリティ管理、パッチ管理などの運用機能をサポートする人員、プロセス、ツールを確立する責任を負うため、アプリケーションの運用に時間がかかる場合があります。

## AMS モードの実際のユースケース

これらを調べて、AMS モードの使用方法を判断します。

- ユースケース 1 は、時間的制約のあるデータセンターの出口でコストを削減するためのビジネス上の課題です。データセンターの出口など、魅力的なビジネスイベントがある企業は、オンプレミスアプリケーションをクラウド上で再ホストすることに関心を持っています。オンプレミスイベントのほとんどは、オペレーティングシステムのバージョンが混在する Windows サーバーと Linux サーバーで構成されます。そうすることで、お客様はクラウドへの移行によるコスト削減を活用し、アプリケーションの技術的およびセキュリティ上の体制を改善したいと考えています。お客様は迅速に移行したいと考えていますが、社内のクラウド運用の専門知識はまだ構築されていません。お客様はリファクタリングのバランスを見つける必要があります。リファクタリングが多すぎると、厳しいタイムラインに対してリスクが高くなります。ただし、OS バージョンの更新やデータベースの最適化などのリファクタリングにより、アプリケーションは次のレベルのパフォーマンスを達成できます。この例では、お客様は AMS マネージド RFC モードを選択して、ほとんどのアプリケーションをリホストできます。AMS はインフラストラクチャオペレーションを提供し、クラウドでの安全な運用に関するベストプラクティスについてお客様の運用チームをガイドします。

AMS 管理の AWS Service Catalog および AMS 管理の Direct Change モードは、同じビジネス成果と目標を達成しながら、お客様にさらなる柔軟性を提供します。さらに、お客様は AMS Operations On Demand (OOD) サービスを使用して、専用の AMS オペレーションエンジニアが変更リクエスト (RFCs) の実行に優先順位を付けることができます。

差別化されていないインフラストラクチャの運用タスク (パッチ適用、バックアップ、アカウント管理など) を AMS にオフロードしながら、お客様は引き続きアプリケーションの最適化とクラウド運用に関する社内チームの強化に集中できます。AMS は、コスト削減に関する月次レポートを顧客に提供し、リソースの最適化に関するレコメンデーションを行います。このユースケースでは、Windows 2003 や 2008 などのレガシー OS バージョンでホストされている end-of-life アプリケーションがリファクタリングしないことを決定した場合、それらを AMS に移行し、カスタマー マネージドモードを利用するアカウントでホストすることもできます。

- ユースケース 2: 安全な AMS 境界内に Lambda、Glue、Athena を使用してデータレイクを構築する: 企業は、AMS の複数のアプリケーションのレポートニーズを満たすために Data Lake をセットアップしようとしています。お客様は、データセットの保存に S3 バケットを使用し、AWS Athena を使用して各レポートのデータセットに対してクエリを実行したいと考えています。S3 と AWS Athena は、別々の AMS マネージドアカウントにデプロイされます。S3 のアカウントには、データ取り込みパイプラインを構築するための Glue、Lambda、Step Functions などの他の



サービスもあります。この場合、Glue、Lambda、Athena、Step Functions はセルフサービスプロビジョニング (SSP) サービスと見なされます。顧客は、アドホックツール/スクリプトサーバーとして機能する EC2 インスタンスをアカウントにデプロイしました。まず、AMS マネージドアカウントで SSP サービスを有効にするように AMS にリクエストします。AMS は、ロールが顧客のフェデレーションソリューションにオンボーディングされると、顧客が引き受けることができるサービスごとに IAM ロールをプロビジョニングします。管理を容易にするために、お客様は個別の IAM ロールのポリシーを 1 つのカスタムロールに結合することもできます。これにより、AWS のサービス間で作業するときにロールを切り替える必要がなくなります。アカウントでロールを有効にすると、顧客は要件に従ってサービスを設定できます。ただし、お客様は AMS 変更管理システムと協力して、ユースケースに応じて追加のアクセス許可をリクエストする必要があります。

たとえば、Glue クローラにアクセスするには、Glue によって追加のアクセス許可が必要です。Lambda のイベントソースを作成するには、追加のアクセス許可も必要です。お客様は AMS と協力して IAM ロールを更新し、Athena が S3 バケットをクエリするためのクロスアカウントアクセスを許可します。サービスロールまたはサービスにリンクされたロールの更新も、Lambda が Step Functions サービスを呼び出し、Glue がすべての S3 バケットを読み書きするための AMS 変更管理を通じて必要になります。AMS はお客様と協力して、最小特権のアクセスモデルに従い、リクエストされた IAM の変更が過度に許容されず、環境が不要なリスクにさらされないようにします。顧客のデータレイクチームは、顧客のアーキテクチャに固有のサービスに必要なすべての IAM アクセス許可の計画に時間を費やし、それらを有効にするために AMS をリクエストします。これは、すべての IAM 変更が手動で処理され、AMS セキュリティチームからレビューされるためです。これらのリクエストを処理する時間は、アプリケーションのデプロイスケジュールで考慮する必要があります。

SSP サービスはアカウントで運用されているため、お客様は AMS インシデント管理とサービスリクエストを通じてサポートをリクエストし、問題を報告できます。ただし、AMS は Lambda のパフォーマンスと同時実行メトリクス、または Glue のジョブメトリクスを積極的にモニタリングしません。SSP サービスで適切なログ記録とモニタリングが有効になっていることを確認するのはお客様の責任です。アカウントの EC2 インスタンスと S3 バケットは、AMS によって完全に管理されます。

- ユースケース 3、AMS での CICD デプロイパイプラインの迅速かつ柔軟なセットアップ: お客様は、AMS 内のすべてのアプリケーションアカウントにコードパイプラインをデプロイするために Jenkins ベースの CICD パイプラインをセットアップしようとしています。お客様は、この CICD パイプラインを AMS 管理の直接変更モード (DCM) または AMS 管理のデベロッパーモードでホストするのが最も適している場合があります。これにより、EC2 で必要なカスタム設定で Jenkins サーバーを柔軟に設定し、アーティファクトリポジトリをホストする CloudFormation および S3 バケットにアクセスするための必要な IAM アクセス許可を付与できるためです。これは AMS 管

理 RFC モードで実行することもできますが、カスタマーチームは、IAM ロール用に複数の手動 RFCs を作成して、AMS によって手動でレビューされる、承認された最小限のアクセス許可のセットで反復する必要があります。DCM を使用すると、AMS マネージド RFCs モードを使用するときに、IAM ロール用に複数の手動 RFC を作成して、AMS によって手動でレビューされる最小限の許可セットを反復処理する必要がなくなります。これには時間がかかり、AMS プロセスとツールを強化するために顧客側の教育も必要です。開発者モードを使用すると、ネイティブ AWS APIs から始めることができます。このパイプラインをセットアップする最も迅速かつ柔軟な方法は、AMS Managed-Developer モードを使用することです。デベロッパーモードは、運用統合を犠牲にしながら、最も迅速かつ簡単な方法を提供します。一方、DCM は柔軟性が低くなりますが、RFC モードと同じレベルの運用サポートを提供します。

- ユースケース 4、AMS 基盤内のカスタマイズされた運用モデル: 顧客は、期限駆動型のデータセンターの終了を検討しており、エンタープライズアプリケーションの 1 つは、アプリケーション運用やインフラストラクチャ運用を含むサードパーティーの MSP によって完全に管理されています。このアプリケーションを AMS で操作できるようにリファクタリングする時間がスケジュールにないと仮定すると、カスタマーマネージドモードが適切なオプションです。お客様は、AMS マネージドランディングゾーンの自動的かつ迅速なセットアップを活用できます。一元化されたネットワークアカウントを通じて、アカウントの供給と接続を制御する一元化されたアカウント管理を活用できます。また、AMS Payer アカウントを通じてすべてのカスタマーマネージドアカウントの料金を統合することで、請求を簡素化します。お客様は、AMS マネージドアカウントに使用される標準アクセス管理とは別に、MSP を使用してカスタムアクセス管理モデルを柔軟に設定できます。これにより、カスタマーマネージドモードを使用して、オンプレミス環境から退避するというビジネス要件を満たしながら、AMS マネージド環境をセットアップできます。この場合、お客様がクラウドに移行する Windows ベースのアプリケーションも持っていて、それらをカスタマーマネージドアカウントに移動することを選択した場合、お客様はクラウド運用モデルを作成する責任があります。これは、従来の IT プロセスを変革し、人材をトレーニングする顧客の能力によっては、複雑でコストが高く、時間がかかる場合があります。お客様は、このようなワークロードを「リフトアンドシフト」して AMS マネージドアカウントにし、インフラストラクチャオペレーションを AMS にオフロードすることで、時間とコストを削減できます。

#### Note

お客様は、RFC または SSP モードのガバナンスフレームワークとデベロッパーモードの間でアプリケーションアカウントを移動する必要があると感じることがあります。たとえば、お客様は最初のリフトアンドシフト移行の一環として AMS マネージドモードでアプリケーションをホストできますが、時間の経過とともにアプリケーションを書き換えてクラウドネイティブの AWS サービス用に最適化したいと考えています。本番稼働前のアカウントのモードを AMS マネージド RFC から AMS マネージド開発者モードに変更し、イ

インフラストラクチャをプロビジョニングするための柔軟性と俊敏性を提供できます。ただし、「開発者ロール」を使用してインフラストラクチャのプロビジョニングが変更されると、同じインフラストラクチャを AMS マネージド RFC モードに戻すことはできません。これは、AMS が AMS 変更管理システムの外部でプロビジョニングされたインフラストラクチャのオペレーションを保証できないためです。お客様は、AMS マネージド RFC モードを提供する新しいアプリケーションアカウントを作成し、CloudFormation テンプレートまたは AMS マネージドアカウントに取り込まれたカスタム AMIs を使用して「最適化」インフラストラクチャ設定を再デプロイする必要がある場合があります。これは、本番稼働用設定をデプロイするためのクリーンな方法です。デプロイされると、アプリケーションは規範的な AMS ガバナンスと運用の下に置かれます。カスタマーマネージドモードと AMS マネージドモード間のモードの切り替えにも同じことが当てはまります。

## RFC モード

RFC モードは、AMS Advanced オペレーションプランのお客様向けのデフォルトモードです。これには、変更または RFCs のリクエストを含む変更管理システムと、アカウントに必要な追加または変更をリクエストするために使用する変更タイプのカタログが含まれます。この変更管理システムは、アカウントを変更できるユーザーを制限するためのセキュリティレベルを提供します。

AMS Advanced 変更タイプの詳細については、[「AMS 変更タイプとは」](#)を参照してください。

AMS Advanced へのオンボーディングの詳細については、[AWS Managed Services オンボーディングの概要](#)を参照してください。

変更タイプのウォークスルーの例については、AMS Advanced Change Type Reference [Change Types by Classification](#) セクションの関連する変更タイプの「追加情報」セクションを参照してください。

### Note

RFC モードは、以前は「変更管理モード」または「標準 CM モード」と呼ばれていました。

## トピック

- [RFCs の詳細](#)
- [変更タイプとは？](#)

- [AMS での RFC エラーのトラブルシューティング](#)

## RFCs の詳細

変更のリクエスト、または RFCs、2 つの方法で機能します。まず、RFC 自体に必要なパラメータがあります。これらは CreateRfc API のオプションです。次に、RFC のアクションに必要なパラメータ (実行パラメータ) があります。CreateRfc オプションの詳細については、AMS API リファレンスの [CreateRfc](#) セクションを参照してください。これらのオプションは通常、RFC ページの作成の追加設定領域に表示されます。

CreateRfc API、CLI、または AMS `aws amscm create-rfc` コンソールの RFC ページの作成を使用して、RFC を作成して送信できます。RFC の作成に関するチュートリアルについては、「」を参照してください [RFC を作成する](#)。

### トピック

- [RFC とは？](#)
- [AMS API/CLI を使用する場合は認証](#)
- [RFC セキュリティレビューを理解する](#)
- [RFC 変更タイプの分類を理解する](#)
- [RFC アクションとアクティビティの状態を理解する](#)
- [RFC ステータスコードを理解する](#)
- [RFC 更新 CTs と CloudFormation テンプレートドリフト検出を理解する](#)
- [RFCs](#)
- [RFCs](#)
- [RFC の制限された実行期間をリクエストする](#)
- [RFCs の作成、クローン作成、更新、検索、キャンセル](#)
- [RFCs](#)
- [一般的な RFC パラメータについて説明します。](#)
- [RFC の毎日の E メールにサインアップする](#)

### RFC とは？

変更のリクエスト、つまり RFC は、AMS が管理する環境を変更する方法、またはユーザーに代わって変更を行うように AMS に依頼する方法です。RFC を作成するには、AMS 変更タイプが

ら選択し、RFC パラメータ (スケジュールなど) を選択し、AMS コンソールまたは API コマンド [CreateRfc](#) と [SubmitRfc](#) を使用してリクエストを送信します。

RFC には 2 つの仕様が含まれています。1 つは RFC 自体用で、もう 1 つは変更タイプ (CT) パラメータ用です。コマンドラインでは、インライン RFC コマンド、または作成した CT JSON スキーマファイル (CT パラメータに基づく) とともに入力して送信する JSON 形式の標準の CreateRfc テンプレートを使用できます。CT 名は、CT の非公式な説明です。CSIO (カテゴリ、サブカテゴリ、項目、オペレーション) は、CT のより正式な説明です。RFC を作成するときは、CT ID のみを指定する必要があります。

RFCs、検証と実行の 2 つの主要な段階があります。

1. 検証段階では、AMS は RFC リクエストの完全性と正確性を確認します。AMS は、セキュリティ [技術標準に従ってセキュリティ](#) のリクエストも評価します。AMS は、リクエストされた変更が有効で実行可能であることを確認します。
2. 実行ステージでは、AMS はアカウントでリクエストされた変更を試みます。

AMS は、自動プロセス、手動プロセス、またはその両方の組み合わせを通じて両方のステージを処理します。手動プロセスは AMS オペレーションチームによって処理されます。詳細については、「[自動 CT と手動 CTs](#)」を参照してください。

AMS には、リクエストを処理するための 3 つの実行モードがあります。

- (AMS 推奨) 実行モード: 自動。これらの CTs RFC の検証と実行に自動化を使用します。これは、ビジネス成果を達成するための最も迅速な方法です。
- (AMS 推奨) 実行モード: 手動および指定: マネージドオートメーション。これらの CTs、RFC の検証と実行のための自動プロセスと手動プロセスの組み合わせを使用します。オートメーションがリクエストされた変更を実行できない場合、RFC は手動処理のために (自動ルーティングまたは代替 RFC の作成によって) AMS オペレーションチームに転送されます。これらの CTs を送信すると、リクエストをより構造化し、AMS オートメーションで補完して、処理と実行の結果の時間枠を改善できます。
- 実行モード: 手動および指定: レビューが必要。 [ct-1e1xtak34nx76 管理 | その他 | その他 | 更新 \(レビューが必要\)](#) または [ct-0xdawir96cy7k 管理 | その他 | その他 | 作成 \(レビューが必要\)](#) を通じてリクエストされた変更。これらの CTs、検証と実行の手動処理に依存しています。これらの CTs は、変更リクエストの手動解釈によって異なります。

AMS は、変更が正常に完了したとき (成功) または失敗したとき (失敗) に通知します。



**Note**

RFC 障害のトラブルシューティングについては、「」を参照してください[AMS での RFC エラーのトラブルシューティング](#)。

次の図は、ユーザーが送信した RFC のワークフローを示しています。

## AMS API/CLI を使用する場合は認証

AMS API/CLI を使用する場合は、一時的な認証情報を使用して認証する必要があります。フェデレーティッドユーザーの一時的なセキュリティ認証情報をリクエストするには、`cal` [GetFederationToken](#)、[AssumeRole](#)、[AssumeRoleWithSAML](#)、または [AssumeRoleWithWebIdentity](#) AWS セキュリティトークンサービス (STS) APIs。

一般的な選択肢は SAML です。セットアップ後、呼び出す各オペレーションに 引数を追加します。  
例: `aws --profile saml amscm list-change-type-categories`。

SAML 2.0 プロファイルのショートカットは、を使用して各 API/CLI の開始時にプロファイル変数を設定することです `set AWS_DEFAULT_PROFILE=saml` (Windows の場合、Linux の場合、 `export AWS_DEFAULT_PROFILE=saml` )。CLI 環境変数の設定については、「[AWS コマンドラインインターフェイスの設定、環境変数](#)」を参照してください。

## RFC セキュリティレビューを理解する

AWS Managed Services (AMS) 変更管理承認プロセスにより、アカウントに加えた変更のセキュリティレビューを確実に実行できます。

AMS は、AMS 技術標準に照らしてすべての変更リクエスト (RFCs) を評価します。技術標準から逸脱してアカウントのセキュリティ体制を低下させる可能性のある変更は、セキュリティレビューの対象となります。セキュリティレビュー中、AMS は関連するリスクを強調し、セキュリティリスクが高い、または非常に高い場合は、承認されたセキュリティ担当者が RFC を承認または拒否します。すべての変更は、AMS の運用能力への悪影響を評価するためにも評価されます。潜在的な悪影響が見つかった場合は、AMS 内で追加のレビューと承認が必要です。

## AMS 技術標準

AMS 技術標準は、アカウントのベースラインセキュリティを確立するための最小限のセキュリティ基準、設定、プロセスを定義します。これらの標準には、AMS とユーザーの両方が従う必要があります。

技術標準から逸脱することでアカウントのセキュリティ体制を低下させる可能性のある変更は、リスク受理プロセスを経て、関連するリスクが AMS によって強調表示され、承認されたセキュリティ担当者がユーザーから承認または拒否します。そのような変更はすべて、アカウントを運用する AMS の能力に悪影響があるかどうかを評価するために評価され、その場合は AMS 内で追加のレビューと承認が必要になります。

### RFC カスタマーセキュリティリスク管理 (CSRM) プロセス

組織の誰かがマネージド環境への変更をリクエストすると、AMS は変更を確認して、リクエストが技術標準に違反してアカウントのセキュリティ体制を悪化させる可能性があるかどうかを判断します。リクエストによってアカウントのセキュリティ体制が低下した場合、AMS はセキュリティチームの連絡先に関連リスクについて通知し、変更を実行します。または、変更によって環境に高いまたは非常に高いセキュリティリスクが発生する場合、AMS はセキュリティチームの連絡先にリスク承諾の形式で明示的な承認を求めます (次に説明)。AMS 顧客リスク承諾プロセスは、以下を目的として設計されています。

- リスクが明確に特定され、適切な所有者に伝えられるようにする
- 環境に対する特定されたリスクを最小限に抑える
- 組織のリスクプロファイルを理解している指定されたセキュリティ担当者から承認を取得して文書化する
- 特定されたリスクに対する継続的な運用オーバーヘッドを削減する

### 技術標準と高リスクまたは非常に高いリスクにアクセスする方法

AMS 技術標準ドキュメントをレポートとして <https://console.aws.amazon.com/artifact/> で参照できるようにしました。AMS 技術標準ドキュメントを使用して、変更リクエスト (RFC) を送信する前に、承認されたセキュリティ担当者からの変更のリスク承諾が必要かどうかを理解します。

デフォルトの AWS Managed Services (AMS) Technical Standards」を検索して、技術標準レポートを検索します。AWS Artifact `AWSManagedServicesChangeManagementRole`

**Note**

AMS 技術標準ドキュメントは、単一アカウントランディングゾーンの `Customer_ReadOnly_Role` からアクセスできます。マルチアカウントランディングゾーンでは、セキュリティ管理者が使用する `AWSManagedServicesAdminRole` と、アプリケーションチームが使用する `AWSManagedServicesChangeManagementRole` を使用して、ドキュメントにアクセスできます。チームがカスタムロールを使用している場合は、その他 | その他の RFC を作成してアクセスをリクエストすると、指定されたカスタムロールが更新されます。

## RFC 変更タイプの分類を理解する

RFC の送信時に使用する変更タイプは、次の 2 つのカテゴリに分かれています。

- デプロイ: この分類はリソースの作成用です。
- 管理: この分類は、リソースを更新または削除するために使用します。管理カテゴリには、インスタンスへのアクセス、AMIs暗号化または共有、スタックの開始、停止、再起動、または削除のための変更タイプも含まれています。

## RFC アクションとアクティビティの状態を理解する

`RfcActionState` (API) / `Activity State` (コンソール) は、RFC に対する人間の介入またはアクションのステータスを理解するのに役立ちます。手動 RFCs に主に使用される は、ユーザーまたは AMS オペレーションに必要なアクションがいつ必要か `RfcActionState` を理解し、AMS オペレーションが RFC でアクティブに動作しているかを確認するのに役立ちます。これにより、RFC のライフサイクル中に RFC に対して実行されるアクションの透明性が向上します。

`RfcActionState` (API) / アクティビティ状態 (コンソール) 定義:

- `AwsOperatorAssigned`: AWS オペレーターが RFC でアクティブに作業しています。
- `AwsActionPending`: AWS からのレスポンスまたはアクションが必要です。
- `CustomerActionPending`: 顧客からのレスポンスまたはアクションが想定されます。
- `NoActionPending`: AWS または顧客からのアクションは必要ありません。
- `NotApplicable`: この状態は AWS オペレーターまたはお客様が設定することはできません。この機能がリリースされる前に作成された RFCs にのみ使用されます。



RFC アクションの状態は、送信された変更タイプが手動レビューを必要とし、スケジュールが ASAP に設定されているかどうかによって異なります。

- RFC ActionState は、遅延スケジューリングを使用した手動変更タイプのレビュー、承認、開始中に変更されます。
- スケジュールされた手動 RFC を送信すると、ActionState は自動的に AwsActionPending に変更され、オペレータが RFC を確認して承認する必要があることを示します。
- オペレーターが RFC のアクティブレビューを開始すると、ActionState は AwsOperatorAssigned に変わります。
- オペレーターが RFC を承認すると、RFC ステータスはスケジュール済みに変わり、ActionState は自動的に NoActionPending に変わります。
- RFC のスケジュールされた開始時刻に達すると、RFC ステータスは InProgress に変わり、ActionState は自動的に AwsActionPending に変わり、RFC のレビューのためにオペレータを割り当てる必要があることを示します。
- オペレーターが RFC のアクティブ実行を開始すると、ActionState が AwsOperatorAssigned に変更されます。
- 完了すると、オペレータは RFC を閉じます。これにより、ActionState が自動的に NoActionPending に変更されます。

#### Important

- アクションの状態を設定することはできません。RFC の変更に基づいて自動的に設定されるか、AMS 演算子によって手動で設定されます。
- RFC にレスポンスを追加すると、ActionState は自動的に AwsActionPending に設定されます。
- RFC が作成されると、ActionState は自動的に NoActionPending に設定されます。
- RFC が送信されると、ActionState は自動的に AwsActionPending に設定されます。
- RFC が拒否、キャンセル、または完了し、ステータスが Success または Failure の場合、ActionState は自動的に NoActionPending にリセットされます。
- アクション状態は自動 RFCs の両方で有効になりますが、これらのタイプの RFCs では通信が必要になることが多いため、主に手動 RFCs では重要です。

## RFC アクションの状態を確認するユースケースの例

### ユースケース: 手動 RFC プロセスの可視性

- 手動 RFC を送信すると、RFC アクションの状態は自動的に に変わり `AwsActionPending`、オペレーターが RFC を確認して承認する必要があることを示します。オペレーターが RFC のアクティブレビューを開始すると、RFC アクションの状態は に変わります `AwsOperatorAssigned`。
- 承認およびスケジュールされ、実行を開始する準備ができている手動 RFC を検討してください。RFC ステータスが に変わると `InProgress`、RFC アクションの状態は自動的に に変わります `AwsActionPending`。オペレーター `AwsOperatorAssigned` が RFC のアクティブ実行を開始すると、再び に変わります。
- 手動 RFC が完了 (「成功」または「失敗」としてクローズ) すると、RFC アクションの状態は に変わり `NoActionPending`、顧客またはオペレーターからそれ以上のアクションが不要であることを示します。

### ユースケース: RFC 対応

- 手動 RFC が の場合 `Pending Approval`、AMS オペレーターからさらに情報が必要になる場合があります。オペレーターは RFC にコレスポンスを投稿し、RFC アクションの状態を に変更します `CustomerActionPending`。新しい RFC 対応を追加して応答すると、RFC アクションの状態は自動的に に変わります `AwsActionPending`。
- 自動または手動 RFC が失敗した場合は、RFC の詳細にコレスポンスを追加して、RFC が失敗した理由を AMS オペレーターに尋ねることができます。コレスポンスが追加されると、RFC アクションの状態は自動的に に設定されます `AwsActionPending`。AMS オペレーターが RFC をピックアップしてコレスポンスを表示すると、RFC アクションの状態は に変わります `AwsOperatorAssigned`。オペレーターが新しい RFC コレスポンスを追加して応答すると、RFC アクションの状態を に設定して `CustomerActionPending`、顧客からの別の応答が予想されることを示すか、 に設定して `NoActionPending`、顧客からの応答が不要または予想されることを示すことができます。

## RFC ステータスコードを理解する

RFC ステータスコードは、リクエストの追跡に役立ちます。これらのステータスコードは、CLI 出力で RFC を実行するとき、またはコンソールで RFC リストページを更新することで確認できます。

RFC のコードは、RFC の詳細ページでも確認できます。

送信していない RFC がリストに表示される場合があります。AMS 演算子が内部専用 CT を使用する場合は、RFC に送信され、RFC リストに表示されます。詳細については、「[内部のみの変更タイプ](#)」を参照してください。

#### Important

RFC の状態変更の通知をリクエストできます。詳細については、「[RFC 状態変更通知](#)」を参照してください。

### RFC ステータスコード

| Success                                                                                          | 失敗                                                                                                       |
|--------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| 編集中: RFC は作成されていますが、送信されていません                                                                    | 拒否: RFCsは通常、検証に失敗するため拒否されます。たとえば、使用できないリソース、つまりサブネットが指定されます。                                             |
| PendingApproval / Submitted: RFC が送信され、システムは承認が必要かどうかを判断し、必要に応じてその承認を取得します。                      | キャンセル済み: RFCsは通常、設定された開始時刻が経過する前に検証に合格しないためキャンセルされます。                                                    |
| AWS による承認/顧客による承認: RFC が承認されました。自動 RFCsは AWS によって承認され、手動 RFCsはオペレーター、場合によっては顧客によって承認されます。        | Failure: RFC が失敗しました。失敗の理由については出力の StatusReason を参照してください。AMS オペレーションは自動的にトラブルチケットを作成し、必要に応じてユーザーと通信します。 |
| スケジュール済み: RFC は構文と要件チェックに合格し、実行がスケジュールされています                                                     |                                                                                                          |
| InProgress: RFC が実行されています。複数のリソースをプロビジョニングする、または UserData が長時間実行される RFCs の実行には時間がかかることに注意してください。 |                                                                                                          |
| 実行済み: RFC が実行されました                                                                               |                                                                                                          |
| Success/Succeeded: RFC が正常に完了しました                                                                |                                                                                                          |

**Note**

キャンセルまたは拒否された RFCs 「」も参照してください[RFCsを更新する](#)。 [UpdateRfc](#)

RFC が必要なすべての条件に合格した場合 (たとえば、すべての必須パラメータが指定されている場合)、ステータスは に変わります PendingApproval (自動 CTsでも承認が必要で、構文とパラメータチェックが合格すると自動的に行われます)。合格しない場合、ステータスは に変わります Rejected。StatusReason は拒否に関する情報を提供し、ExecutionOutputフィールドは承認と完了に関する情報を提供します。エラーコードには以下が含まれます。

- InvalidRfcStateException: RFC は、呼び出されたオペレーションを許可しないステータスです。たとえば、RFC が送信済み状態に移行した場合、変更できなくなります。
- InvalidRfcScheduleException: StartTime、EndTime、または TimeoutInMinutes パラメータが超過しました。
- InternalServerError: システムに問題が発生しました。
- InvalidArgumentException: パラメータが正しく指定されていません。たとえば、許容できない値が使用されます。
- ResourceNotFoundException: スタック ID などの値が見つかりません。

変更が承認される前に、スケジュールされたリクエストの開始時刻と終了時刻 (変更実行ウィンドウとも呼ばれます) が発生した場合、RFC ステータスは に変わります Canceled。変更が承認されると、RFC ステータスは に変わります Scheduled。ASAP RFCs の変更実行ウィンドウは、送信された時刻に CT ExpectedExecutionDurationの値を加えたものです。

変更実行ウィンドウの到着前であればいつでも、スケジュールされた変更 (CLI RequestedStartTimeの で送信) を変更またはキャンセルできます。スケジュールされた変更が変更された場合は、再送信する必要があります。

変更の開始時刻 (スケジュールまたは ASAP) が到着し、承認が完了すると、ステータスは に変わり InProgress、変更を加えることはできません。指定された変更実行ウィンドウ内に変更が完了すると、ステータスは に変わります Success。変更の一部が失敗した場合、または変更実行ウィンドウの終了時に変更がまだ進行中である場合、ステータスは に変わります Failure。

**Note**

InProgress、SuccessまたはFailureの状態、RFC を変更またはキャンセルすることはできません。

次の図は、CreateRFC 呼び出しから解決までの CreateRFCステータスを示しています。

## RFC 更新 CTs と CloudFormation テンプレートドリフト検出を理解する

AMS でプロビジョニングされたリソースは、変更された CloudFormation テンプレートを使用します。リソースのパラメータがサービスの AWS マネジメントコンソールから直接変更された場合、そのリソースの CloudFormation 作成レコードは同期しなくなります。この場合、AMS 更新変更タイプを使用して AMS のリソースを更新しようとする、AMS は元のリソース設定を参照し、変更されたパラメータをリセットする可能性があります。このリセットはダメージを与える可能性があるため、追加の AMS 設定の変更が検出された場合、AMS は更新変更タイプの RFCs を禁止します。

更新変更タイプのリストについては、コンソールフィルターを使用します。

### ドリフト修復FAQs

AMS ドリフト修復に関する質問と回答。ドリフト修復を開始するために使用できる変更タイプは 2 つあります。1 つは実行モード = 手動または「マネージドオートメーション」で、もう 1 つは実行モード = 自動です。

### ドリフト修復でサポートされているリソース (ct-3king0u4l33zf)

これらは、ドリフト修復変更タイプ (ct-3king0u4l33zf) でサポートされているリソースです。リソースを修正するには、代わりに「マネージドオートメーション」(ct-34sxf053yuzah) 変更タイプを使用します。

```
AWS::EC2::Instance
AWS::EC2::SecurityGroup
AWS::EC2::VPC
AWS::EC2::Subnet
AWS::EC2::NetworkInterface
AWS::EC2::EIP
AWS::EC2::InternetGateway
AWS::EC2::NatGateway
```

```
AWS::EC2::NetworkAcl
AWS::EC2::RouteTable
AWS::EC2::Volume
AWS::AutoScaling::AutoScalingGroup
AWS::AutoScaling::LaunchConfiguration
AWS::AutoScaling::LifecycleHook
AWS::AutoScaling::ScalingPolicy
AWS::AutoScaling::ScheduledAction
AWS::ElasticLoadBalancing::LoadBalancer
AWS::ElasticLoadBalancingV2::Listener
AWS::ElasticLoadBalancingV2::ListenerRule
AWS::ElasticLoadBalancingV2::LoadBalancer
AWS::CloudWatch::Alarm
```

## ドリフト修復の変更タイプ

AMS ドリフト修復変更タイプの使用に関する質問と回答。

ドリフト修復機能でサポートされているリソースのリストについては、「」を参照してください [ドリフト修復でサポートされているリソース \(ct-3king0u4l33zf\)](#)。

### Important

ドリフト修復はスタックテンプレートやパラメータを変更し、最新のスタックテンプレートやパラメータを使用するようにローカルテンプレートリポジトリまたはこれらのスタックを更新するオートメーションを更新する必要があります。同期せずに古いテンプレートやパラメータを使用すると、基盤となるリソースに有害な変更が生じる可能性があります。マネージドオートメーションなし、自動、CT (ct-3king0u4l33zf) は、RFC あたり 10 個のリソースの修復のみをサポートします。残りのリソースを 10 個のバッチで修正するには、すべてのリソースが修正されるまで新しい RFCs を作成します。

## どのドリフト修復変更タイプを使用すべきですか？

以下の場合、マネージドオートメーションなしの自動 CT (ct-3king0u4l33zf) を使用することをお勧めします。

- 自動 CT を使用して既存のスタックリソースの更新を実行しようとする、スタックが であるため RFC が拒否されます DRIFTED。
- 過去に Update CT を使用していて、スタックが DRIFTED になったため失敗しました。更新を再試行する必要はなく、代わりにマネージドオートメーション、手動、CT を使用できます。



マネージドオートメーション、手動 CT (ct-34sxfo53yuzah) を使用するの、ドリフト修復でドリフトリソースタイプがサポートされていない場合、マネージドオートメーション、自動、CT (ct-3king0u4l33zf) がない場合、またはドリフト修復でマネージドオートメーション、自動、CT が失敗した場合のみです。

修復中にスタックにどのような変更が実行されますか？

修復には、ドリフトするプロパティに応じて、スタックテンプレートやパラメータの更新が必要です。修復は、修復中にスタックのスタックポリシーを更新し、修復が完了するとスタックポリシーを以前の値に復元します。

スタックテンプレートやパラメータに対して実行された変更を確認するにはどうすればよいですか？

RFC へのレスポンスでは、変更の概要に以下の情報が表示されます。

- **ChangeSummaryJson**: ドリフト修復の一環として、スタックテンプレートやパラメータの変更の概要が含まれます。修復は複数のフェーズで実行されます。この変更の概要は、個々のフェーズの変更で構成されます。修復が成功した場合は、最後のフェーズの変更を確認します。順番に実行されるフェーズについては、JSON の **ExecutionPlan** を参照してください。たとえば、**RestoreReferences** セクションが存在する場合、常に最後に実行され、修正後の変更のための JSON が含まれます。DryRun モードで修復が実行された場合、これらの変更はスタックに適用されません。
- **PreRemediationStackTemplateAndConfigurationJson**: スタックで修復がトリガーされる前に、テンプレート、パラメータ、出力、**StackPolicyBody** を含む CloudFormation スタックの設定スナップショットが含まれます。

修復が実行されたら、何をする必要がありますか？

#### Important

RFC の概要で提供されている最新のテンプレートとパラメータを使用して、修復されたスタックを更新するローカルテンプレートリポジトリまたはオートメーションを更新する必要があります。古いテンプレートやパラメータを使用すると、スタックリソースにさらに破壊的な変更が生じる可能性があるため、これを行うことが重要です。

この修復中にアプリケーションは有効になりますか？

修復は、CloudFormation スタック設定でのみ実行されるオフラインプロセスです。基盤となるリソースでは更新は実行されません。

管理 | その他 | その他の RFCs を引き続き使用して、修復後にリソースの更新を実行できますか？

使用可能な自動 Update CTs を使用して、スタックリソースの更新を常に行うことをお勧めします。利用可能な Update CTs がユースケースをサポートしていない場合は、管理 | その他 | その他のリクエストを使用します。

修復によってスタックに新しいリソースが作成されますか？

修復では、スタックに新しいリソースは作成されません。ただし、修復は新しい出力を作成し、スタックテンプレート [メタデータ](#) セクションを更新して、参照用に修復の概要を保存します。

修復は常に成功しますか？

修復には、テンプレート設定を慎重に分析して検証し、実行できるかどうかを判断する必要があります。これらの検証が失敗した場合、修復プロセスは停止され、スタックテンプレートまたはパラメータに変更は実行されません。また、修復はサポートされているリソースタイプでのみ実行できます。

修復が成功しなかった場合にスタックリソースの更新を実行するにはどうすればよいですか？

Management | Other | Other | Update CT (ct-0xdawir96cy7k) を使用して変更をリクエストできます。AMS はこのようなシナリオをモニタリングし、修復ソリューションの改善に取り組んでいます。

サポートされているリソースタイプとサポートされていないリソースタイプの両方を持つスタックを修復できますか？

はい。ただし、修復は、サポートされているリソースタイプがスタックで DRIFTED が見つかった場合にのみ実行されます。サポートされていないリソースタイプが DRIFTED の場合、修復は続行されません。

CFN 以外の取り込み CTs を使用して作成されたスタックの修復をリクエストできますか？

はい。修正は、スタックの作成に使用される変更タイプに関係なく、スタックで実行できます。

修復前にスタックに実行される変更を知ることはできますか？

はい。どちらの変更タイプも、スタックが修正された場合に実行される変更をリクエストするために使用できる DryRun オプションを提供します。ただし、最終的な修復の変更は、修復時にスタックに存在するドリフトによって異なる場合があります。

## RFCs

スケジュール機能を使用すると、RFCs の開始時間を選択できます。スケジューリング機能では、次のオプションを使用できます。



- この変更をできるだけ早く実行する: AMS は、承認されるとすぐに RFC を実行します。ほとんどの CTs は自動的に承認されます。RFC を特定の時間に開始しない場合は、このオプションを使用します。
- この変更をスケジュールする: RFC を実行する日、時刻、タイムゾーンを設定します。自動変更タイプの場合、RFC の送信予定から少なくとも 10 分後に開始時刻をリクエストするのがベストプラクティスです。マネージドオートメーションの変更タイプでは、RFC の送信予定から少なくとも 24 時間後に開始時刻をリクエストする必要があります。RFC が設定された開始時刻までに承認されない場合、RFC は拒否されます。

## RFC スケジュールを設定する

RFC をスケジュールするには、次のいずれかの方法を使用します。

この変更をできるだけ早く実行します。

- コンソール: 何もしません。これはデフォルトの RFC スケジュールを使用します。
- API または CLI: RFC の作成オペレーションで RequestedStartTime および RequestedEndTime オプションを削除します。

ASAP RFCs は、送信後 30 日以内に承認されない場合、自動拒否されます。

この変更をスケジュールします。

- コンソール: この変更のスケジュールラジオボタンを選択します。開始時間領域が開きます。手動で日を入力するか、カレンダーウィジェットを使用して日を選択します。ISO 8601 形式で表される時刻を UTC で入力し、ドロップダウンリストを使用して場所を選択します。デフォルトでは、AMS は ISO 8601 形式 YYYYMMDDThhmmssZ または YYYY-MM-DDThh:mm:ssZ を使用します。どちらの形式も使用できます。

### Note

デフォルトの終了時刻は、入力した開始時刻から 4 時間です。スケジュールされた変更の終了時刻を 4 時間を超えて設定するには、API または CLI を使用して変更を実行します。

- API または CLI: RFC の作成オペレーションで RequestedStartTime および RequestedEndTime パラメータの値を送信します。設定済みの `RequestedEndTime` としても、既に開始されている自動変更タイプの実行は停止されません。「マネージドオートメーション」の変更タイプで、AMS オペレーションの研究がまだ進行中に `RequestedEndTime` に到達

し、AMS と通信している場合は、拡張機能をリクエストするか、RFC の再送信を求められる場合があります。

#### Tip

UTC タイムリードアウトの例については、Time-is ウェブサイトの [「UTC」](#) を参照してください。2:20pm: 2016-2016-12-05T14:20:00Z 2016-12-05 の日付/時刻値の ISO 8601 形式の例。20161205T142000Z

指定した場合..

- のみRequestedStartTime、RFC はスケジュール済みと見なされ、RequestedEndTimeは ExecutionDurationInMinutes値を使用して入力されます。
- のみRequestedEndTime、InvalidArgumentException をスローします。
- RequestedStartTime と の両方でRequestedEndTime、指定された開始時刻に ExecutionDurationInMinutes値を加えたRequestedEndTime値で を上書きします。
- RequestedStartTime も も、RequestedEndTimeこれらの値は null のままで、RFC は ASAP RFC として扱われます。

#### Note

スケジュールされたすべての RFCs について、未指定の終了時刻は、指定された時刻に、送信された変更タイプの ExpectedExecutionDurationInMinutes 属性RequestedStartTimeを加えた時刻として書き込まれます。たとえば、ExpectedExecutionDurationInMinutesが「60」(分)で、指定された RequestedStartTimeが 2016-12-05T14:20:00Z (2016 年 12 月 5 日午前 4 時 20 分) の場合、実際の終了時刻は 2016 年 12 月 5 日午前 5 時 20 分に設定されます。ExpectedExecutionDurationInMinutes 特定の変更タイプの を検索するには、次のコマンドを実行します。

```
aws amscm --profile sam1 get-change-type-version --  
change-type-id CHANGE_TYPE_ID --query "ChangeTypeVersion.  
{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

## RFC Priority オプションを使用する

execution mode = manual 変更タイプで Priority オプションを使用して、リクエストの緊急性を AMS オペレーションに警告します。

の Priority オプション execution mode = manual:

手動 RFC の優先度を High、Medium、または Low に指定します。High に分類され RFCs は、RFCs サービスレベル目標 (SLOs) とその送信時間に従って、Medium に分類される RFC の前にレビューおよび承認されます。優先度が低い、または優先度が指定されていない RFCs は、送信された順序で処理されます。

## RFCs

承認が必要な (手動) CTs で送信される RFCs は、ユーザーまたは AMS によって承認される必要があります。事前承認 CTs は自動的に処理されます。詳細については、「[CT 承認要件](#)」を参照してください。

### Note

手動 CTs を使用する場合、AMS では ASAP スケジューリングオプション (コンソールで ASAP を選択し、API/CLI で開始時刻と終了時刻を空白のままにする) を使用することをお勧めします。これらの CTs では、AMS オペレータが RFC を調べ、承認して実行する前にお客様と通信する必要があるためです。これらの RFCs スケジュールする場合は、少なくとも 24 時間かかります。スケジュールされた開始時刻より前に承認が行われない場合、RFC は自動的に拒否されます。

承認が必要な RFC が AMS によって正常に送信された場合は、明示的に承認する必要があります。または、承認が必要な RFC を送信する場合は、AMS によって承認される必要があります。AMS が送信した RFC を承認する必要がある場合は、承認をリクエストする E メールまたはその他の事前定義された通信が送信されます。通信には RFC ID が含まれます。通信が送信されたら、次のいずれかを実行します。

- コンソールの承認または拒否: 関連する RFC の RFC 詳細ページを使用します。
- API / CLI 承認: [ApproveRfc](#) は変更を承認済みとしてマークします。アクションは、所有者とオペレーターの両方が必要な場合に実行する必要があります。以下は、CLI 承認コマンドの例です。次の例では、RFC\_ID を適切な RFC ID に置き換えます。

```
aws amscm approve-rfc --rfc-id RFC_ID
```

- API / CLI 拒否: [RejectRfc](#) は変更を拒否済みとしてマークします。CLI 拒否コマンドの例を示します。次の例では、RFC\_ID を適切な RFC ID に置き換えます。

```
aws amscm reject-rfc --rfc-id RFC_ID --reason "no longer relevant"
```

## RFC の制限された実行期間をリクエストする

以前はブラックアウトデーと呼ばれていましたが、特定の期間の制限をリクエストできます。この間の変更を実行できません。

制限された実行期間を設定するには、[UpdateRestrictedExecutionTimes](#) API オペレーションを使用して、UTC で特定の期間を設定します。指定した期間は、指定した以前の期間よりも優先されます。指定された制限された実行時間内に RFC を送信すると、送信は無効な RFC スケジュールというエラーで失敗します。最大 200 の制限期間を指定できます。デフォルトでは、制限された期間は設定されていません。以下は、リクエストコマンドの例です (SAML 認証が設定されている)。

```
aws amscm --profile saml update-restricted-execution-times --restricted-execution-times='[{"TimeRange":{"StartTime":"2018-01-01T12:00:00Z","EndTime":"2018-01-01T12:00:01Z"}}]'
```

RestrictedExecutionTimes API オペレーションを実行して、現在の RestrictedExecutionTimes 設定を表示することもできます。 [ListRestrictedExecutionTimes](#) 例:

```
aws amscm --profile saml list-restricted-execution-times
```

指定された制限された実行時間内に RFC を送信する場合は、OverrideRestrictedTimeRanges の値を持つ RestrictedExecutionTimesOverrideId を追加し、通常どおり RFC を送信します。この方法は、緊急または緊急の RFC にのみ使用するのがベストプラクティスです。詳細については、[SubmitRfc](#) の API リファレンスを参照してください。

## RFCs の作成、クローン作成、更新、検索、キャンセル

以下の例では、さまざまな RFC オペレーションについて説明します。

### トピック

- [RFC を作成する](#)

- [AMS コンソールを使用して RFCs のクローンを作成する \(再作成\)](#)
- [RFCsを更新する](#)
- [RFCs の検索](#)
- [RFCs](#)

## RFC を作成する

### コンソールを使用した RFC の作成

以下は、AMS コンソールでの RFC 作成プロセスの最初のページです。クイックカードが開き、変更タイプの参照がアクティブになっています。

以下は、AMS コンソールで RFC 作成プロセスの最初のページで、カテゴリ別に選択がアクティブになっています。

#### 仕組み:

1. RFC の作成ページに移動します。AMS コンソールの左側のナビゲーションペインで RFCs をクリックして RFCs リストページを開き、RFC の作成をクリックします。
2. デフォルトの変更タイプ参照ビューで一般的な変更タイプ (CT) を選択するか、カテゴリ別選択ビューで CT を選択します。
  - 変更タイプ別に参照: クイック作成エリアで一般的な CT をクリックすると、すぐに RFC の実行ページを開くことができます。クイック作成で古い CT バージョンを選択することはできません。

CTs をソートするには、カードビューまたはテーブルビューですべての変更タイプエリアを使用します。どちらのビューでも、CT を選択し、RFC の作成をクリックして RFC の実行ページを開きます。必要に応じて、RFC の作成ボタンの横に古いバージョンで作成オプションが表示されます。

  - カテゴリ別に選択: カテゴリ、サブカテゴリ、項目、オペレーションを選択すると、CT 詳細ボックスが開き、必要に応じて古いバージョンで作成するオプションが表示されます。RFC の作成をクリックして、RFC の実行ページを開きます。
3. RFC の実行ページで、CT 名エリアを開き、CT の詳細ボックスを表示します。件名は必須です (変更タイプの参照ビューで CT を選択した場合は入力されます)。追加設定エリアを開き、RFC に関する情報を追加します。

実行設定領域で、使用可能なドロップダウンリストを使用するか、必要なパラメータの値を入力します。オプションの実行パラメータを設定するには、追加設定エリアを開きます。

- 完了したら、実行 をクリックします。エラーがない場合、RFC が正常に作成されたページに、送信された RFC の詳細と最初の実行出力が表示されます。
- Run parameters 領域を開き、送信した設定を確認します。ページを更新して RFC 実行ステータスを更新します。必要に応じて、RFC をキャンセルするか、ページ上部のオプションを使用して RFC のコピーを作成します。

## CLI を使用した RFC の作成

仕組み:

- インライン作成 (すべての RFC と実行パラメータを含む create-rfc コマンドを発行) またはテンプレート作成 (2 つの JSON ファイルを作成し、1 つは RFC パラメータ用、もう 1 つは実行パラメータ用) のいずれかを使用し、2 つのファイルを入力として create-rfc コマンドを発行します。どちらの方法もここで説明します。
- 返された RFC ID を使用して RFC: `aws amscm submit-rfc --rfc-id ID` コマンドを送信します。

RFC: `aws amscm get-rfc --rfc-id ID` コマンドをモニタリングします。

変更タイプのバージョンを確認するには、次のコマンドを使用します。

```
aws amscm list-change-type-version-summaries --filter
Attribute=ChangeTypeId,Value=CT_ID
```

### Note

変更タイプのスキーマの一部であるかどうかにかかわらず、任意の RFC で任意の CreateRfc パラメータを使用できます。たとえば、RFC ステータスが変更されたときに通知を受け取るには、リクエストの RFC パラメータ部分 (実行パラメータではなく) `--notification "{\"Email\": {\"EmailRecipients\": [\"email@example.com\"]}}\"` にこの行を追加します。すべての CreateRfc パラメータのリストについては、[AMS 変更管理 API リファレンス](#) を参照してください。

## インライン作成:

インラインで指定された実行パラメータ (インラインで実行パラメータを指定する場合は引用符をエスケープ) を指定して create RFC コマンドを発行し、返された RFC ID を送信します。たとえば、コンテンツを次のような内容に置き換えることができます。

```
aws amscm create-rfc --change-type-id "CT_ID" --change-type-version "VERSION" --title "TITLE" --execution-parameters "{\\"Description\": \\"example\\"}"
```

## テンプレートの作成:

### Note

RFC を作成するこの例では、Load Balancer (ELB) スタック変更タイプを使用します。

1. 関連する CT を見つけます。次のコマンドは、項目名に「ELB」が含まれている CT 分類の概要を検索し、Category、Item、Operation、ChangeTypeId の出力をテーブル形式で作成します (両方のサブカテゴリは ですAdvanced stack components)。

```
aws amscm list-change-type-classification-summaries --query "ChangeTypeClassificationSummaries[?contains(Item,'ELB')]. [Category,Item,Operation,ChangeTypeId]" --output table
```

```
-----
|                               CtSummaries                               |
+-----+-----+-----+-----+-----+-----+
| Deployment| Load balancer (ELB) stack | Create | ct-123h45t6uz7j1 |
| Management| Load balancer (ELB) stack | Update | ct-01tm873rsebx9 |
+-----+-----+-----+-----+-----+-----+

```

2. CT の最新バージョンを見つけてます。

ChangeTypeId および ChangeTypeVersion: このウォークスルーの変更タイプ ID は ct-123h45t6uz7j1 (ELB を作成) です。最新バージョンを確認するには、次のコマンドを実行します。

```
aws amscm list-change-type-version-summaries --filter Attribute=ChangeTypeId,Value=ct-123h45t6uz7j1
```



3. オプションと要件について説明します。次のコマンドは、CreateElbParams.json.

```
aws amscm get-change-type-version --change-type-id "ct-123h45t6uz7jl" --query
"ChangeTypeVersion.ExecutionInputSchema" --output text > CreateElbParams.json
```

4. 実行パラメータ JSON ファイルを変更して保存します。この例では、CreateElbParams.json.

プロビジョニング CT の場合、StackTemplateId はスキーマに含まれ、実行パラメータで送信する必要があります。

TimeoutInMinutes の場合、RFC が失敗するまでにスタックの作成に許可される分数。この設定は RFC の実行を遅らせませんが、十分な時間を与える必要があります (たとえば、「5」を指定しないでください)。UserData: Create EC2 and Create ASG が長時間実行される CTs」～「360」です。他のすべてのプロビジョニング CTs」をお勧めします。

スタックを作成する VPC の ID を指定します。VPC ID は CLI コマンド で取得できます `aws amsskms list-vpc-summaries`。

```
{
  "Description":      "ELB-Create-RFC",
  "VpcId":            "VPC_ID",
  "StackTemplateId":  "stm-sdhopv000000000000",
  "Name":             "MyElbInstance",
  "TimeoutInMinutes": 60,
  "Parameters": {
    "ELBSubnetIds":    ["SUBNET_ID"],
    "ELBHealthCheckHealthyThreshold": 4,
    "ELBHealthCheckInterval": 5,
    "ELBHealthCheckTarget": "HTTP:80/",
    "ELBHealthCheckTimeout": 60,
    "ELBHealthCheckUnhealthyThreshold": 5,
    "ELBScheme":       false
  }
}
```

5. RFC JSON テンプレートを CreateElbRfc.json:

```
aws amscm create-rfc --generate-cli-skeleton > CreateElbRfc.json
```

6. CreateElbRfc.json ファイルを変更して保存します。実行パラメータを別のファイルに作成したため、ExecutionParameters行を削除します。たとえば、コンテンツを次のような内容に置き換えることができます。



```
{
  "ChangeTypeVersion":    "2.0",
  "ChangeTypeId":         "ct-123h45t6uz7jl",
  "Title":                 "Create ELB"
}
```

7. RFC を作成します。次のコマンドは、実行パラメータファイルと RFC テンプレートファイルを指定します。

```
aws amscm create-rfc --cli-input-json file://CreateElbRfc.json --execution-
parameters file://CreateElbParams.json
```

レスポンスで新しい RFC の ID を受け取り、それを使用して RFC を送信およびモニタリングできます。送信するまで、RFC は編集状態のままであり、開始されません。

## ヒント

### Note

AMS API/CLI を使用して、RFC JSON ファイルまたは CT 実行パラメータ JSON ファイルを作成せずに RFC を作成できます。これを行うには、`create-rfc` コマンドを使用し、必要な RFC および実行パラメータをコマンドに追加します。これは「インライン作成」と呼ばれます。すべてのプロビジョニング CTs には、リソースのパラメータを含む `Parameters` 配列が `execution-parameters` ブロックに含まれていることに注意してください。パラメータには、バックスラッシュ (\) でエスケープされた引用符が必要です。RFC を作成する他の文書化された方法は、「テンプレートの作成」と呼ばれます。ここでは、RFC パラメータ用の JSON ファイルと実行パラメータ用の別の JSON ファイルを作成し、`create-rfc` コマンドを使用して 2 つのファイルを送信します。これらのファイルはテンプレートとして機能し、将来の RFCs に再利用できます。

テンプレートを使用して RFCs を作成する場合、コマンドを使用して、次に示すようにコマンドを発行することで、必要な内容の JSON ファイルを作成できます。コマンドは、表示された内容で「`parameters.json`」という名前のファイルを作成します。これらのコマンドを使用して RFC JSON ファイルを作成することもできます。

AMS コンソールを使用して RFCs のクローンを作成する (再作成)

AMS コンソールを使用して、既存の RFC のクローンを作成できます。

AMS コンソールを使用して RFC のクローンを作成または再作成するには、次の手順に従います。

1. 関連する RFC を見つけます。左側のナビゲーションで、RFCs をクリックします。

RFCs が開きます。

2. クローンを作成する RFC が見つかるまでページをスクロールします。フィルターオプションを使用してリストを絞り込みます。クローンを作成する RFC を選択します。

RFC の詳細ページが開きます。

3. コピーの作成をクリックします。

変更リクエストの作成ページが開き、すべてのオプションが元の RFC でとして設定されます。

4. 必要な変更を加えます。追加のオプションを設定するには、ベーシックオプションをアドバンストに変更します。すべてのオプションを設定したら、送信を選択します。

アクティブな RFC の詳細ページが開き、クローン RFC の新しい RFC ID が表示され、クローン RFC が RFC ダッシュボードに表示されます。

## RFCs を更新する

RFC を更新して送信するか、再送信することで、拒否された RFC またはまだ送信されていない RFC を再送信できます。ほとんどの RFCs は拒否されることに注意してください。これは、指定された RequestedStartTime が送信前に渡されたか、指定された TimeoutInMinutes が RFC の実行に不十分であるためです (TimeoutInMinutes は成功した RFC を延長しないため、Amazon EC2 または長時間実行される UserData を持つ Amazon EC2 Auto Scaling グループでは、常にこれを「60」以上「360」以下に設定することをお勧めします)。このセクションでは、UpdateRfc コマンドの CLI バージョンを使用して、新しい RFC パラメータで RFC を更新する方法、または文字列化された JSON または更新されたパラメータファイルを使用して新しいパラメータを更新する方法について説明します。

この例では、AMS UpdateRfc API の CLI バージョンの使用について説明します ([「RFC の更新」](#)を参照)。一部のリソース (DNS プライベートおよびパブリック、ロードバランサースタック、スタックパッチ適用設定) を更新するための変更タイプがありますが、RFC を更新する CT はありません。

一度に 1 つの UpdateRfc オペレーションを送信することをお勧めします。DNS スタックなどで複数の更新を送信すると、更新が同時に DNS を更新しようとして失敗する可能性があります。

必須データ: RfcId: 更新する RFC。

オプションデータ: `ExecutionParameters`: などの必須でないフィールドを更新しない限り `Description`、RFC が拒否またはキャンセルされた原因となった問題に対処するために、変更された実行パラメータを送信します。送信された NULL 以外の値はすべて、元の RFC の値を上書きします。

1. 関連する拒否またはキャンセルされた RFC を検索するには、このコマンドを使用できます (値を `Canceled` に置き換えることができます)。

```
aws amscm list-rfc-summaries --filter Attribute=RfcStatusId,Value=Rejected
```

2. 次のいずれかの RFC パラメータを変更できます。

```
{
  "Description": "string",
  "ExecutionParameters": "string",
  "ExpectedOutcome": "string",
  "ImplementationPlan": "string",
  "RequestedEndTime": "string",
  "RequestedStartTime": "string",
  "RfcId": "string",
  "RollbackPlan": "string",
  "Title": "string",
  "WorstCaseScenario": "string"}
```

説明フィールドを更新するコマンドの例：

```
aws amscm update-rfc --description "AMSTestNoOpsActionRequired" --rfc-id "RFC_ID"
--region us-east-1
```

`ExecutionParameters VpcId` フィールドを更新するコマンドの例：

```
aws amscm update-rfc --execution-parameters "{\"VpcId\": \"VPC_ID\"}" --rfc-id
"RFC_ID" --region us-east-1
```

RFC を、更新を含む実行パラメータファイルで更新するコマンドの例。[EC2 スタック | 作成](#)：」のステップ 2 の実行パラメータファイルの例を参照してください。

```
aws amscm update-rfc --execution-parameters file://CreateEc2ParamsUpdate.json --
rfc-id "RFC_ID" --region us-east-1
```

3. `submit-rfc` と RFC が最初に作成されたときと同じ RFC ID を使用して RFC を再送信します。

```
aws amscm submit-rfc --rfc-id RFC_ID
```

RFC が成功した場合、コマンドラインに確認メッセージやエラーメッセージは表示されません。

4. リクエストのステータスをモニタリングし、実行出力を表示するには、次のコマンドを実行します。

```
aws amscm get-rfc --rfc-id RFC_ID
```

## RFCs の検索

### コンソールで変更リクエスト (RFC) を検索する

AMS コンソールを使用して RFC を検索するには、次の手順に従います。

#### Note

この手順は、スケジュールされた RFCs つまり ASAP オプションを使用しなかった RFCs にも適用されます。

1. 左側のナビゲーションで、RFCs をクリックします。

RFCs が開きます。

2. リストをスクロールするか、フィルターオプションを使用してリストを絞り込みます。

RFC リストはフィルター条件ごとに変わります。

3. 目的の RFC のサブジェクトリンクを選択します。

RFC の詳細ページが開き、RFC ID などの情報が表示されます。

4. ダッシュボードに多数の RFCs がある場合は、フィルターオプションを使用して RFC で検索できます。

- 件名: RFC の作成時に指定された件名またはタイトル (API/CLI の場合)。

- RFC ID: RFC の識別子。
- アクティビティ状態: RFC の状態がわかっている場合は、オペレータが現在 RFC を見ていることを示す `AwsOperatorAssigned`、`AwsActionPending` のいずれかを選択できます。つまり、AMS オペレータは RFC 実行を続行する前に何かを実行する必要があります。`CustomerActionPending` は、RFC 実行を続行する前に何らかのアクションを実行する必要がありますことを意味します。
- ステータス: RFC ステータスがわかっている場合は、次のいずれかを選択できます。
  - スケジュール: スケジュールされた RFCs。
  - キャンセル済み: キャンセルされた RFCs。
  - 進行中: RFCs が進行中です。
  - Success: RFCs。
  - 拒否: 拒否された RFCs。
  - 編集: 編集の RFCs。
  - Failure: 失敗した RFCs。
  - 承認保留中: AMS またはユーザーが承認するまで続行できない RFCs。通常、これは RFC を承認する必要があることを示します。サービスリクエストリストにこのサービス通知が表示されます。
- 変更タイプ: `Category`、`Subcategory`、`Item`、`Operation` を選択すると、変更タイプ ID が自動的に取得されます。
- リクエストされた開始時刻またはリクエストされた終了時刻: このフィルターオプションでは、前または後を選択し、日付と、オプションで時刻 (hh:mm とタイムゾーン) を入力できます。このフィルターは、スケジュールされた RFCs (ASAP RFCs)。
- ステータス: スケジュール済み、キャンセル済み、進行中、成功、拒否済み、編集、または失敗。
- 件名: RFC にした件名 (または RFC が API/CLI で作成された場合はタイトル)。
- 変更タイプ ID: RFC で送信された変更タイプの識別子を使用します。

次のスクリーンショットに示すように、検索ではフィルターを追加できます。

## 5. 目的の RFC の件名リンクをクリックします。

RFC の詳細ページが開き、RFC ID などの情報が表示されます。

## CLI を使用した変更リクエスト (RFC) の検索

複数のフィルターを使用して RFC を検索できます。

変更タイプのバージョンを確認するには、次のコマンドを使用します。

```
aws amscm list-change-type-version-summaries --filter
Attribute=ChangeTypeId,Value=CT_ID
```

 **Note**

変更タイプのスキーマの一部であるかどうかにかかわらず、任意の RFC で任意の CreateRfc パラメータを使用できます。たとえば、RFC ステータスが変更されたときに通知を受け取るには、リクエストの RFC パラメータ部分 (実行パラメータではなく) --notification '{"Email\\": {"EmailRecipients\\": [\\"email@example.com\\"]}}'にこの行を追加します。すべての CreateRfc パラメータのリストについては、[AMS 変更管理 API リファレンス](#)を参照してください。

RFC ID を書き留めず、後で見つける必要がある場合は、AMS 変更管理 (CM) システムを使用して ID を検索し、フィルターまたはクエリを使用して結果を絞り込むことができます。

- CM API [ListRfcSummaries](#) オペレーションにはフィルターがあります。論理 AND オペレーションで Attribute と Value を組み合わせて、または Attribute、 、に基づいて Condition 結果を [フィルタリング](#)できますValues。

### RFC フィルタリング

| 属性            | 有効値                                      | 有効な条件 | デフォルトの条件 | 注意事項                                                                                           |
|---------------|------------------------------------------|-------|----------|------------------------------------------------------------------------------------------------|
| ActualEndTime | ISO8601 日時を表す文字列 (例: 「20170101T000000Z」) | 前、後、間 | なし       | Before または After 条件は、Values フィールドで 1 つの値のみを受け入れます。Between 条件には、Values フィールドに正確に 2 つの値が必要です。最初の |

| 属性                 | 有効値                                      | 有効な条件        | デフォルトの条件 | 注意事項                                                                                                                     |
|--------------------|------------------------------------------|--------------|----------|--------------------------------------------------------------------------------------------------------------------------|
|                    |                                          |              |          | 値は、2 番目の値より前の日付を表す必要があります。                                                                                               |
| ActualStartTime    | ISO8601 日時を表す文字列 (例: 「20170101T000000Z」) | 前、後、間        | なし       | Before または After 条件は、Values フィールドで 1 つの値のみを受け入れます。Between 条件には、Values フィールドに正確に 2 つの値が必要です。最初の値は、2 番目の値より前の日付を表す必要があります。 |
| AutomationStatusId | 手動、自動                                    | Equals (等しい) | Equals   | 自動化ステータスは 2 つだけです                                                                                                        |
| ChangeTypeId       | 任意の有効な変更タイプ ID。例: ct-123h45t6uz7jl       | Equals (等しい) | Equals   | <a href="#">変更タイプまたは CSIO の検索</a>                                                                                        |
| ChangeTypeVersion  | 有効な変更タイプ ID。例: 1.0                       | Equals (等しい) | Equals   | <a href="#">変更タイプまたは CSIO の検索</a>                                                                                        |
| CreatedBy          | 任意の文字列 (最大許容長は 2048 文字)                  | Contains     | Contains | RFC の CreatedBy フィールドには、RFC を作成したユーザーの ARN が含まれます。                                                                       |

| 属性               | 有効値                                       | 有効な条件 | デフォルトの条件 | 注意事項                                                                                                                     |
|------------------|-------------------------------------------|-------|----------|--------------------------------------------------------------------------------------------------------------------------|
| CreatedTime      | ISO8601 日時を表す文字列 (例 : 「20170101T000000Z」) | 前、後、間 | なし       | Before または After 条件は、Values フィールドで 1 つの値のみを受け入れます。Between 条件には、Values フィールドに正確に 2 つの値が必要です。最初の値は、2 番目の値より前の日付を表す必要があります。 |
| LastModifiedTime | ISO8601 日時を表す文字列 (例 : 「20170101T000000Z」) | 前、後、間 | なし       | Before または After 条件は、Values フィールドで 1 つの値のみを受け入れます。Between 条件には、Values フィールドに正確に 2 つの値が必要です。最初の値は、2 番目の値より前の日付を表す必要があります。 |



| 属性                | 有効値                                       | 有効な条件 | デフォルトの条件 | 注意事項                                                                                                                     |
|-------------------|-------------------------------------------|-------|----------|--------------------------------------------------------------------------------------------------------------------------|
| LastSubmittedTime | ISO8601 日時を表す文字列 (例 : 「20170101T000000Z」) | 前、後、間 | なし       | Before または After 条件は、Values フィールドで 1 つの値のみを受け入れます。Between 条件には、Values フィールドに正確に 2 つの値が必要です。最初の値は、2 番目の値より前の日付を表す必要があります。 |
| RequestedEndTime  | ISO8601 日時を表す文字列 (例 : 「20170101T000000Z」) | 前、後、間 | なし       | Before または After 条件は、Values フィールドで 1 つの値のみを受け入れます。Between 条件には、Values フィールドに正確に 2 つの値が必要です。最初の値は、2 番目の値より前の日付を表す必要があります。 |

| 属性                 | 有効値                                                        | 有効な条件        | デフォルトの条件 | 注意事項                                                                                                                     |
|--------------------|------------------------------------------------------------|--------------|----------|--------------------------------------------------------------------------------------------------------------------------|
| RequestedStartTime | ISO8601 日時を表す文字列 (例: 「20170101T000000Z」)                   | 前、後、間        | なし       | Before または After 条件は、Values フィールドで 1 つの値のみを受け入れます。Between 条件には、Values フィールドに正確に 2 つの値が必要です。最初の値は、2 番目の値より前の日付を表す必要があります。 |
| RfcStatusId        | キャンセル済み、編集中、失敗、InProgress、PendingApproval、拒否済み、スケジュール済み、成功 | Equals (等しい) | Equals   | AMS コンソールで RFC リストを更新するか、 <a href="#">GetRfc</a> を実行します。                                                                 |
| タイトル               | 有効な RFC タイトル                                               | Contains     | Contains | 個々のフィールドの正規表現はサポートされていません。大文字と小文字を区別しない検索                                                                                |

例:

SQS (SQS が CT のアイテム部分に含まれている) に関連するすべての RFCs の IDs を見つけるには、次のコマンドを使用できます。

```
list-rfc-summaries --query 'RfcSummaries[?contains(Item.Name,`SQS`)].
[Category.Id,Subcategory.Id,Type.Id,Item.Id,RfcId]' --output table
```

これは次のようなものを返します。

```

-----
|                               ListRfcSummaries                               |
+-----+-----+-----+-----+-----+-----+
|Deployment| Advanced Stack Components      |SQS    |Create |ct-123h45t6uz7j1|
|Management| Monitoring & Notification    |SQS    |Update |ct-123h45t6uz7j1|
+-----+-----+-----+-----+-----+-----+

```

で利用できるもう 1 つのフィルター `list-rfc-summaries` は `AutomationStatusId`、自動または手動 RFCs を検索する です。

```
aws amscm list-rfc-summaries --filter Attribute=AutomationStatusId,Value=Automated
```

で利用できるもう 1 つのフィルター `list-rfc-summaries` は `Title` (コンソールの件名) です。

```
Attribute=Title,Value=RFC-TITLE
```

RFCs を返す JSON の新しいリクエスト構造の例は次のとおりです。

- (タイトル 「Windows 2012」 または 「Amazon Linux」 というフレーズが含まれます)
- (RfcStatusId EQUALS "Success" OR "InProgress") AND
- (20170101T000000Z <= RequestedStartTime <= 20170103T000000Z) AND (ActualEndTime <= 20170103T000000Z)

```
{
  "Filters": [
    {
      "Attribute": "Title",
      "Values": ["Windows 2012", "Amazon Linux"],
      "Condition": "Contains"
    },
    {
      "Attribute": "RfcStatusId",
      "Values": ["Success", "InProgress"],
      "Condition": "Equals"
    },
    {
      "Attribute": "RequestedStartTime",

```

```
    "Values": ["20170101T000000Z", "20170103T000000Z"],
    "Condition": "Between"
  },
  {
    "Attribute": "ActualEndTime",
    "Values": ["20170103T000000Z"],
    "Condition": "Before"
  }
]
```

#### Note

より高度な では Filters、AMS は今後のリリースで次のフィールドを廃止する予定です。

- Value: Value フィールドは Filters フィールドの一部です。より高度な機能をサポートする Values フィールドを使用します。
- RequestedEndTimeRange: より高度な機能をサポートするフィルターフィールド内で RequestedEndTime を使用します。
- RequestedStartTimeRange: より高度な機能をサポートする Filters フィールド内で RequestedStartTime を使用します。

CLI クエリの使用の詳細については、[「--query オプションで出力をフィルタリングする方法」](#) および「クエリ言語リファレンス」の[JMESPath 仕様](#)を参照してください。

## 2. AMS コンソールを使用している場合:

RFCs リストページに移動します。必要に応じて、RFC サブジェクトをフィルタリングできます。これは、RFC の作成 Title 時に RFC として入力した内容です。

## ヒント

#### Note

この手順は、スケジュールされた RFCs つまり ASAP オプションを使用しなかった RFCs にのみ適用されます。

## RFCs

コンソールまたは AMS API/CLI を使用して RFC をキャンセルできます。

コンソールで RFC をキャンセルするには、RFC リストで RFC を見つけて開きます。キャンセルをクリックします。

必要なデータ：

- Reason: RFC をキャンセルする理由。
- RfcId: キャンセルする RFC。

1. 通常、RFC は送信直後にキャンセルします (そのため、RFC ID は便利です)。そうしないと、スケジュールして指定した開始時刻より前でない限りキャンセルできません。RFC ID を見つける必要がある場合は、このコマンドを使用できます (手動で承認された RFC ValuePendingApprovalの代わりに 使用できます)。

```
aws amscm list-rfc-summaries --filter Attribute=RfcStatusId,Value=Scheduled
```

2. RFC をキャンセルするコマンドの例：

```
aws amscm cancel-rfc --reason "Bad Stack ID" --rfc-id "RFC_ID" --profile saml --region us-east-1
```

## RFCs

AMS コンソールには、RFCs。

RFC リストページを使用する (コンソール)

AMS コンソールRFCs リストページには、次のオプションがあります。

- フィルターによる高度な RFC 検索。詳細については、「[RFCs の検索](#)」を参照してください。
- RFC が最後に変更された時刻を検索します。この値は、RFC ステータスが最後に変更された時刻を表します。
- RFC サブジェクトを使用した RFC の詳細の表示。このリンクを選択すると、その RFC の詳細ページが開きます。

- RFC ステータスの表示。詳細については、「[RFC ステータスコードを理解する](#)」を参照してください。

## RFC クイック作成を使用する (コンソール)

RFC クイック作成カードまたはリストテーブルを使用するか、分類別に RFCs の変更タイプを選択します。

詳細については[RFC を作成する](#)を参照してください。

## RFC コレスポンドンスとアタッチメントを追加する (コンソール)

コレスポンドンスは、送信後、承認前に RFC に追加できます。例えば、「PendingApproval」の状態です。RFC が承認されると (「スケジュール済み」または「InProgress」の状態)、リクエストの変更として解釈される可能性があるため、コレスポンドンスを追加できません。RFC が完了すると (「キャンセル済み」、「拒否済み」、「成功」、または「失敗」の状態)、通信は再度有効になりますが、RFC が 30 日以上閉じられると通信は無効になります。

### Note

各コレスポンドンスは 5,000 文字に制限されています。

## 添付ファイルの制限:

- コレスポンドンスごとに 3 つの添付ファイルのみ。
- RFC ごとに 50 個のアタッチメントを制限します。
- 各アタッチメントのサイズは 5 MB 未満である必要があります。
- プレーンテキスト (.txt)、カンマ区切り値 (), JSON (.csv)、YAML (.json) などのテキストファイルのみが受け入れられます。yaml。YAML 形式の場合は、ファイル拡張子を使用してファイルをアタッチする必要があります。yaml。

### Note

XML コンテンツを含むテキストファイルは禁止されています。AMS と共有する XML コンテンツがある場合は、サービスリクエストを使用します。

- ファイル名は 255 文字に制限されており、数字、文字、スペース、ダッシュ (-)、アンダースコア (\_)、ドット (.) のみを使用できます。
- RFC での添付ファイルの更新と削除は現在サポートされていません。

RFC にコレスポンドンスと添付ファイルを追加するには、次の手順に従います。

1. AMS コンソールの RFC の詳細ページで、ページの下部にある「Correspondence」セクションを見つけます。

通信前:

いくつかの通信の後:

2. 新しいコレスポンドンスを追加するには、返信テキストボックスにメッセージを入力します。対応に関連するファイルをアタッチするには、添付ファイルの追加を選択し、必要なファイルを選択します。
3. 完了したら、送信を選択します。

新しいコレスポンドンスは、添付ファイルへのリンクとともに、RFC の詳細ページのコレスポンドンスリストに表示されます。

## RFC E メール通知を設定する (コンソール)

AMS コンソールの変更リクエストの作成ページには、RFC の状態変更の通知を受信する E メールアドレスを追加するオプションがあります。

さらに、次のような変更タイプに通知用の E メールアドレスを追加できます。

```
aws amscm create-rfc --change-type-id <Change type ID>
                        --change-type-version 1.0 --title "TITLE"
                        --notification "{\"Email\": {\"EmailRecipients\": [\"email@example.com\"]}}"
```

パラメータ部分ではなく、RFC パラメータ部分の任意の変更タイプのインラインリクエストまたはテンプレートリクエストに同様の行 (`--notification "{\"Email\": {\"EmailRecipients\": [\"email@example.com\"]}}\"`) を追加します。

一般的な RFC パラメータについて説明します。

以下は、送信する必要がある RFC パラメータと、RFCs。

- 変更タイプ情報: `ChangeTypeId` と `ChangeTypeVersion`。変更タイプ IDs [「変更タイプリファレンス」](#) を参照してください。

CLI `list-change-type-classification-summaries` で `query` 引数を使用して を実行し、結果を絞り込みます。たとえば、結果を絞り込んで、Item 名前に「アクセス」を含むタイプを変更します。

```
aws amscm list-change-type-classification-summaries --query
  "ChangeTypeClassificationSummaries [?contains (Item, 'access')].
  [Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
```

を実行し `get-change-type-version`、変更タイプ ID を指定します。次のコマンドは、`ct-2tylseo8rxfs` の CT バージョンを取得します。

```
aws amscm get-change-type-version --change-type-id ct-2tylseo8rxfs
```

- タイトル: RFC の名前。これは AMS コンソール RFC リストの RFC のサブジェクトになり、`GetRfc` コマンドとフィルターを使用して検索できます。Title
- スケジュール: スケジュールされた RFC が必要な場合は、パラメータ `RequestedStartTime` と `RequestedEndTime` パラメータを含めるか、この変更のスケジュールコンソールオプションを使用する必要があります。ASAP RFC (承認されるとすぐに実行される) の場合、CLI を使用するときは、`RequestedStartTime` と `RequestedEndTime` null のままにします。コンソールを使用する場合は、ASAP オプションを受け入れます。

`RequestedStartTime` が見つからない場合、RFC は拒否されます。

- CT のプロビジョニング CTs: 実行パラメータ、または `Parameters` は、リソースのプロビジョニングに必要な特定の設定です。CT によって大きく異なります。
- 非プロビジョニング CTs: アクセス CTs やその他 | その他などのリソースをプロビジョニングしない CT、またはスタックを削除しない CTs は、最小限の実行パラメータを持ち、`Parameters` ブロックはありません。



- RFCs、 を指定するかTimeoutInMinutes、 RFC が失敗するまでにスタックの作成に何分かかかるかも指定する必要があります。長時間実行される UserData の有効な値は 60 (分) から 360 までです。を超える前に実行を完了できない場合、RFC TimeoutInMinutes は失敗します。ただし、この設定では RFC の実行が遅延することはありません。
- S3 バケットや ELB などのインスタンスを作成する RFCs は、通常、最大 7 つのタグ (キーと値のペア) を追加できるスキーマを提供します。デプロイ | 高度なスタックコンポーネント | タグ | 変更タイプの作成 (ct-3cx7we852p3af) を使用して RFC を送信することで、S3 バケットにタグを追加できます。EC2、EFS、RDS、および多層 (HA 2 階層および HA 1 階層) スキーマでは、最大 50 個のタグを使用できます。タグはスキーマの ExecutionParameters部分で指定されます。タグを提供することは大きな価値があります。詳細については、「[Amazon EC2 リソースにタグを付ける](#)」を参照してください。

AMS コンソールを使用する場合は、タグを追加するには追加設定エリアを開く必要があります。

#### Tip

多くの CT スキーマには、スキーマの上部近くに Description および Nameフィールドがあります。これらのフィールドは、スタックまたはスタックコンポーネントに名前を付けるために使用されます。作成するリソースには名前を付けません。一部のスキーマは、作成するリソースに名前を付けるパラメータを提供し、そうでないスキーマもあります。たとえば、Create EC2 スタックの CT スキーマは、EC2 インスタンスに名前を付けるパラメータを提供しません。そのためには、キー「Name」と名前の値を持つタグを作成する必要があります。このようなタグを作成しない場合、EC2 インスタンスは EC2 コンソールに名前属性なしで表示されます。

## RFC AWS リージョンオプションを使用する

AMS API および CLI (amscm および amsskms) エンドポイントは `us-east-1` にあります。Security Assertion Markup Language (SAML) とフェデレーションする場合、AWS リージョンを `us-east-1` に設定するスクリプトがオンボーディング時に提供されます。SAML を使用する場合、コマンドを発行するときに `--region` オプションを指定する必要はありません。SAML が `us-east-1` を使用するように設定されていても、アカウントがその AWS リージョンにない場合は、他の AWS コマンド (例: ) を発行するときに、アカウントオンボーディングリージョンを指定する必要があります `aws s3`。

**Note**

このガイドに記載されているコマンド例のほとんどには、`--region` オプションは含まれていません。

## RFC の毎日の E メールにサインアップする

RFC ダイジェスト機能を使用して、過去 24 時間のアカウントの RFC アクティビティをまとめた毎日の E メールにサインアップできます。RFC ダイジェスト機能は、アカウントの RFCs。RFC ダイジェストは、応答を保留しているアクションを見逃す可能性を減らす可能性があります。

RFC ダイジェスト機能を有効にするには、AMS Cloud Service Delivery Manager (CSDM) にお問い合わせください。CSDM がサブスクライブします。RFC ダイジェスト E メールリストに含める E メールアドレス (またはエイリアス) を最大 20 個リクエストできます。現在の E メールスケジュールは 09:00 UTC-8 に固定されています。

RFC ダイジェスト機能をオフにするには、CSDM に連絡してリクエストしてください。

RFC ダイジェストを設定せず、RFCs に関する通知が必要な場合、または RFCs ダイジェストが提供する情報よりも RFC に関する詳細情報が必要な場合は、変更管理システムを使用して、情報が必要な個々の RFC ごとに CloudWatch Events 通知または E メール通知を設定します。RFC 通知の設定については、[「RFC 状態変更通知」](#)を参照してください。

RFC ダイジェストに含まれるトピックは次のとおりです。

- Pending Customer Approval: PendingApproval ステータスの RFCs を一覧表示し、承認待ちにします
- Pending Customer Reply: RFCs を待っている RFC を一覧表示します
- 保留中の AWS 承認または応答: AMS が応答または承認を待っている RFCs を一覧表示します
- 完了: 成功、失敗、キャンセル、拒否のステータス RFCs を一覧表示します

RFC ダイジェストの例を次に示します。

## 変更タイプとは？

変更タイプとは、AWS Managed Services (AMS) による変更リクエスト (RFC) が実行し、変更アクション自体、および変更のタイプを手動と自動で含めるアクションを指します。AMS には、他の

Amazon ウェブサービスでは使用されていない変更タイプの大規模なコレクションがあります。これらの変更タイプは、リソースをデプロイ、管理、またはアクセスするための変更リクエスト (RFC) を送信するときに使用します。

## トピック

- [自動 CT と手動 CTs](#)
- [CT 承認要件](#)
- [変更タイプバージョン](#)
- [変更タイプを作成する](#)
- [変更タイプを更新する](#)
- [内部のみの変更タイプ](#)
- [変更タイプスキーマ](#)
- [変更タイプのアクセス許可の管理](#)
- [変更タイプから機密情報を編集する](#)
- [クエリオプションを使用した変更タイプの検索](#)

## 自動 CT と手動 CTs

変更タイプの制約は、自動か手動かです。これは、AMS コンソールで実行モードと呼ばれる変更タイプのAutomationStatusId属性です。

自動変更タイプには期待される結果と実行時間があり、通常は 1 時間以内に AMS 自動システムを通じて実行されます (これは CT がプロビジョニングするリソースに大きく依存します)。手動変更タイプは一般的ではありませんが、実行する前に AMS オペレーターが RFC を操作する必要があるため、扱いが異なります。つまり、RFC 送信者と通信する場合があるため、手動の変更タイプでは、完了までにさまざまな時間がかかることがあります。

スケジュールされたすべての RFCs について、未指定の終了時刻は、指定された時刻に、送信された変更タイプの ExpectedExecutionDurationInMinutes 属性RequestedStartTimeを加えた時刻として書き込まれます。たとえば、ExpectedExecutionDurationInMinutesが「60」(分)で、指定された RequestedStartTimeが 2016-12-05T14:20:00Z (2016 年 12 月 5 日午前 4 時 20 分) の場合、実際の終了時刻は 2016 年 12 月 5 日午前 5 時 20 分に設定されます。ExpectedExecutionDurationInMinutes 特定の変更タイプの を検索するには、次のコマンドを実行します。

```
aws amscm --profile sam1 get-change-type-version --change-type-id CHANGE_TYPE_ID --  
query "ChangeTypeVersion.{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

#### Note

スケジュールされた RFCs の実行モード = コンソールでは、少なくとも 24 時間後に実行するように設定する必要があります。

#### Note

手動 CTs を使用する場合、AMS では ASAP スケジューリングオプション (コンソールで ASAP を選択し、API/CLI で開始時刻と終了時刻を空白のままにする) を使用することをお勧めします。これらの CTs では、AMS オペレータが RFC を調べ、承認して実行する前にお客様と通信する必要があるためです。これらの RFCs スケジュールする場合は、少なくとも 24 時間かかります。スケジュールされた開始時刻より前に承認が行われない場合、RFC は自動的に拒否されます。

AMS は手動 CT に 4 時間以内に応答することを目指しており、できるだけ早く対応しますが、RFC が実際に実行されるまでにかなり時間がかかる場合があります。

手動であり、AMS レビューが必要な CTs 「変更タイプ CSV ファイル」を参照してください。

YouTube Video: [AMS RFCs の自動変更タイプを見つけるにはどうすればよいですか？](#)

AMS コンソールで CT の実行モードを見つけるには、変更タイプの参照検索オプションを使用する必要があります。結果には、一致する変更タイプまたは変更タイプの実行モードが表示されます。

AMS CLI を使用して AutomationStatus 特定の変更タイプの を検索するには、次のコマンドを実行します。

```
aws amscm --profile sam1 get-change-type-version --change-type-id CHANGE_TYPE_ID --  
query "ChangeTypeVersion.{AutomationStatus:AutomationStatus.Name}"
```

すべての [AMS 変更タイプに関する情報を提供する AMS 変更タイプリファレンス](#) で変更タイプを検索することもできます。

 Note

AMS API/CLI は現在 AWS API/CLI の一部ではありません。AMS API/CLI にアクセスするには、AMS コンソールから AMS SDK をダウンロードします。

CT 承認要件

AMS CTs には、常に AwsApprovalId と CustomerApprovalId の 2 つの承認条件があり、RFC が実行を承認するために AMS またはユーザー、あるいは誰かを必要とするかどうかを示します。

承認条件は実行モードと多少関連しています。詳細については、「」を参照してください[自動 CT と手動 CTs](#)。

CT の承認条件を確認するには、[AMS 変更タイプリファレンス](#)を参照するか、[GetChangeTypeVersion](#) を実行します。どちらも CT モードAutomationStatusIdまたは実行モードも提供します。

RFCs、AMS コンソールを使用するか、次のコマンドを使用します。

```
aws amscm approve-rfc --rfc-id RFC_ID
```

CT 承認条件

| CT 承認条件が の場合                          | からの承認が必要です                                             | And                                                        |
|---------------------------------------|--------------------------------------------------------|------------------------------------------------------------|
| AwsApprovalId: Required               | AMS 変更タイプシステム、                                         | アクションは必要ありません。この条件は、自動 CTs。                                |
| AwsApprovalId: NotRequiredIfSubmitter | 送信された RFC が送信されたアカウント用である場合、AMS 変更タイプシステムであり、他に誰もいません。 | アクションは必要ありません。この条件は、AMS 演算子によって常にレビューされるため、手動 CTs では一般的です。 |

| CT 承認条件が の場合                                  | からの承認が必要です                                   | And                                                                             |
|-----------------------------------------------|----------------------------------------------|---------------------------------------------------------------------------------|
| CustomerApprovalId:<br>NotRequired            | AMS 変更タイプシステム、                               | RFC が構文チェックとパラメータチェックに合格すると、自動承認されます。                                           |
| CustomerApprovalId:<br>Required               | AMS 変更タイプシステムとユーザー                           | 通知が送信され、通知に応答するか、 <a href="#">ApproveRfc</a> オペレーションを実行して、RFC を明示的に承認する必要があります。 |
| CustomerApprovalId:<br>NotRequiredIfSubmitter | RFC を送信した場合は、AMS 変更タイプシステムであり、他のユーザーではありません。 | RFC が構文チェックとパラメータチェックに合格すると、自動承認されます。                                           |
| 緊急のセキュリティインシデントまたはパッチ                         | AMS                                          | 自動承認され、実装されています。                                                                |

## 変更タイプバージョン

変更タイプはバージョン管理され、バージョンは変更タイプにメジャーな更新が行われたときに変更されます。

AMS コンソールを使用して変更タイプを選択したら、追加設定エリアを開き、変更タイプバージョンを選択するオプションがあります。API/CLI コマンドラインで変更タイプバージョンを指定することもできます。これは、次のようなさまざまな理由で実行できます。

- 更新する変更タイプのバージョンは、更新するリソースの作成に使用した変更タイプの作成バージョンと一致する必要があります。たとえば、ELB Create change type version 1 で作成した Elastic Load Balancer (ELB) インスタンスがあるとしします。更新するには、ELB 更新バージョン 1 を選択します。
- 最新の変更タイプとは異なるオプションを含む変更タイプバージョンを使用します。AMS は主にセキュリティ上の理由から変更タイプを更新するため、これはお勧めしません。常に最新バージョンを選択することをお勧めします。

## 変更タイプを作成する

変更タイプの作成は、version-to-version 更新変更タイプと一致します。つまり、リソースのプロビジョニングに使用する変更タイプバージョンは、後でそのリソースを変更するために使用する更新変更タイプのバージョンと一致する必要があります。例えば、Create S3 Bucket change type version 2.0 で S3 バケットを作成し、後で RFC を送信してその S3 バケットを変更する場合は、バージョン 3.0 の Update S3 Bucket change type version 2.0 があっても、Update S3 Bucket change type version 2.0 も使用する必要があります。

後で Update 変更タイプを使用してリソースを変更する場合に備えて、Create 変更タイプでリソースをプロビジョニングするときに使用する変更タイプ ID とバージョンを記録しておくことをお勧めします。

## 変更タイプを更新する

AMS には、Create change types で作成されたリソースを更新するための Update change types が用意されています。更新変更タイプは、リソースのプロビジョニングに最初に使用された変更タイプの作成と version-to-version 一致させる必要があります。

更新しやすいように、リソースをプロビジョニングするときに使用する変更タイプ ID とバージョンを記録しておくことをお勧めします。

YouTube 動画: [更新 CTs を使用して AWS Managed Services \(AMS\) アカウントのリソースを変更する方法を教えてください。](#)

## 内部のみの変更タイプ

内部使用のみの変更タイプを確認できます。これにより、AMS が実行できる、または実行するアクションがわかります。使用できる内部のみの変更タイプがある場合は、サービスリクエストを送信します。

例えば、管理 | モニタリングと通知 | CloudWatch アラーム抑制 | CT の更新は内部専用です。AMS はこれを使用してインフラストラクチャの更新 (パッチ適用など) をデプロイし、更新が誤ってトリガーされる可能性のあるアラーム通知をオフにします。この CT が送信されると、RFC リストに CT の RFC が表示されます。RFC にデプロイされている内部専用 CT は、RFC リストに表示されません。

## 変更タイプスキーマ

すべての変更タイプは、リソースの作成、変更、またはアクセスの入力に JSON スキーマを提供します。スキーマは、変更リクエスト (RFC) を作成するためのパラメータとその説明を提供します。



RFC が正常に実行されると、実行出力になります。RFCs プロビジョニングの場合、実行出力には CloudFormation のスタックを表す「stack\_id」が含まれ、CloudFormation コンソールで検索できます。実行出力には、作成されたインスタンスの ID の出力が含まれる場合があり、その ID を使用して、対応する AWS コンソールでインスタンスを検索できます。例えば、Create ELB CT 実行出力には、CloudFormation で検索可能な「stack\_id」が含まれ、Elastic Load Balancing の Amazon EC2 コンソールで検索可能な key=ELB value=<stack-xxxx> を出力します。

CT スキーマを見てみましょう。これは、かなり小さなスキーマである CodeDeploy Application Create のスキーマです。一部のスキーマには、非常に大きな Parameter 領域があります。

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "name": "Create CodeDeploy application",
  "description": "Use to create an AWS CodeDeploy application
on
resource with the specified name.",
  "type": "object",
  "properties": {
    "Description": {
      "description": "The reason for the request.",
      "type": "string",
      "minLength": 1,
      "maxLength": 500
    },
    "VpcId": {
      "description": "ID of the vpc to use, in the form
vpc-0123abcd or vpc-01234567890abcdef.",
      "type": "string",
      "pattern": "^vpc-[a-z0-9]{8}$"
    },
    "StackTemplateId": {
      "description": "Must be stm-sft6rv000000000000",
      "type": "string",
      "enum": ["stm-sft6rv000000000000"]
    },
    "Name": {
      "description": "A name for the stack or stack component
;
this becomes the Stack Name.",
      "type": "string",
      "minLength": 1,
      "maxLength": 255
    }
  }
}
```

スキーマの最初の部分は、リクエストされた変更タイプに関する情報を AMS に提供します。



```

},
"Tags": {
  "description": "Up to seven tags (key/value pairs) to
  categorize the resource.",
  "type": "array",
  "items": {
    "type": "object",
    "properties": {
      "Key": {
        "type": "string",
        "minLength": 1,
        "maxLength": 127
      },
      "Value": {
        "type": "string",
        "minLength": 1,
        "maxLength": 255
      }
    },
    "additionalProperties": false,
    "required": [
      "Key",
      "Value"
    ]
  },
  "minItems": 1,
  "maxItems": 7
},
"TimeoutInMinutes": {
  "description": "The maximum amount of time, in minutes,
  to
  allow for execution of the change. This will not prolong
  execution,
  but the RFC fails if the change is not completed in the
  specified time.
  Valid values are 60 up to 360, for long-running
  UserData.",
  "type": "number",
  "minimum": 0,
  "maximum": 60
},
"Parameters": {
  "description": "Specifications for the stack.",
  "type": "object",

```

TimeoutInMinutes パラメータを使用すると、変更タイプを実行する境界時間を指定できます。長時間実行される UserData の有効な値は 60 ~ 360 です。

Parameters セクションは、作成するリソースの設定、またはリクエストするアクションを指定する場所です。

「追加プロパティ」セクションでは、どのパラメータが必要

```
"properties": {
  "CodeDeployApplicationName": {
    "description": "The name of an AWS CodeDeploy
application.",
    "type": "string",
    "minLength": 1,
    "maxLength": 100,
    "pattern": "^[a-zA-Z0-9._+=,@-]{1,100}$"
  }
},
"additionalProperties": false,
"required": [
  "CodeDeployApplicationName"
]
},
"additionalProperties": false,
"required": [
  "Description",
  "VpcId",
  "StackTemplateId",
  "Name",
  "TimeoutInMinutes",
  "Parameters"
]
}
```

で、どれがオプションかがわかります。

#### Note

このスキーマでは最大 7 つのタグを使用できますが、EC2、EFS、RDS、および多層作成スキーマでは最大 50 個のタグを使用できます。

## 変更タイプのアクセス許可の管理

カスタムポリシーを使用して、異なるグループまたはユーザーが使用できる変更タイプ (CTs) を制限できます。

これを行う方法の詳細については、「AMS ユーザーガイド」セクション「アクセス[許可の設定](#)」を参照してください。

## 変更タイプから機密情報を編集する

AMS 変更タイプスキーマ `"metadata": "ams:sensitive": "true"` は、パスワードなどの機密情報を含むパラメータに使用されるパラメータ属性を提供します。この属性を設定すると、指定された入力は不明瞭になります。このパラメータ属性は設定できないことに注意してください。ただし、AMS を使用して変更タイプを作成し、入力時に不明瞭にするパラメータがある場合は、これをリクエストできます。

## クエリオプションを使用した変更タイプの検索

この例では、AMS コンソールを使用して、送信する RFC の適切な変更タイプを見つける方法を示します。

コンソールまたは API/CLI を使用して、変更タイプ ID (CT) またはバージョンを検索できます。検索または分類の選択の 2 つの方法があります。どちらの選択タイプでも、最も頻繁に使用される、最近使用された、またはアルファベットのいずれかを選択して検索をソートできます。

YouTube 動画: [AWS Managed Services CLI を使用して RFC を作成する方法と、CT スキーマの場所を教えてください。](#)

AMS コンソールの RFCs -> RFC の作成ページで、次の操作を行います。

- 変更タイプによる参照 (デフォルト) を選択した場合、次のいずれかを実行します。
  - クイック作成エリアを使用して、AMS の最も一般的な CTs から選択します。ラベルをクリックすると、RFC の実行ページが開き、件名オプションが自動的に入力されます。必要に応じて残りのオプションを完了し、実行をクリックして RFC を送信します。
  - または、すべての変更タイプ領域までスクロールダウンし、オプションボックスに CT 名を入力し始めます。変更タイプ名を完全または完全に設定する必要はありません。関連する単語を入力して、変更タイプ ID、分類、または実行モード (自動または手動) で CT を検索することもできます。

デフォルトのカードビューを選択すると、入力時に一致する CT カードが表示され、カードを選択して RFC の作成をクリックします。テーブルビューを選択し、関連する CT を選択し、RFC の作成をクリックします。どちらの方法でも、RFC の実行ページが開きます。

- または、変更タイプの選択肢を確認するには、ページ上部の「カテゴリ別に選択」をクリックして、一連のドロップダウンオプションボックスを開きます。
- カテゴリ、サブカテゴリ、項目、オペレーションを選択します。その変更タイプの情報ボックスは、ページの下部にパネルが表示されます。

- 準備ができたら、Enter キーを押すと、一致する変更タイプのリストが表示されます。
- リストから変更タイプを選択します。その変更タイプの情報ボックスがページの下部に表示されます。
- 正しい変更タイプを取得したら、RFC の作成を選択します。

#### Note

これらのコマンドを機能させるには、AMS CLI をインストールする必要があります。AMS API または CLI をインストールするには、AMS コンソールのデベロッパーリソースページに移動します。AMS CM API または AMS SKMS API のリファレンスマテリアルについては、「ユーザーガイド」の「AMS 情報リソース」セクションを参照してください。認証 `--profile` のオプションを追加する必要がある場合があります。例: `aws amsskms ams-cli-command --profile SAML`。また、など、すべての AMS コマンドが `us-east-1` を使い果たすため、`--region` オプションを追加する必要がある場合があります `aws amscm ams-cli-command --region=us-east-1`。

#### Note

AMS API/CLI (`amscm` および `amsskms`) エンドポイントは、AWS N. Virginia リージョンにあります `us-east-1`。認証の設定方法や、アカウントとリソースが存在する AWS リージョンによっては、コマンドの発行 `--region us-east-1` 時に追加が必要になる場合があります。認証方法である場合は `--profile saml`、を追加する必要がある場合もあります。

AMS CM API ([ListChangeTypeClassificationSummaries](#) を参照) または CLI を使用して変更タイプを検索するには：

フィルターまたはクエリを使用して検索できます。ListChangeTypeClassificationSummaries オペレーションには、Category、SubcategoryItem、およびの [フィルター](#) オプションがありますが Operation、値は既存の値と完全に一致する必要があります。CLI を使用する際のより柔軟な結果を得るには、`--query` オプションを使用できます。

## AMS CM API/CLI を使用した変更タイプのフィルタリング

| 属性           | 有効値                                          | 有効/デフォルト条件   | 注意                                                                                                |
|--------------|----------------------------------------------|--------------|---------------------------------------------------------------------------------------------------|
| ChangeTypeld | ChangeTypeld を表す任意の文字列 (例: ct-abc123xyz7890) | Equals (等しい) | 変更タイプ IDs <a href="#">「変更タイプリファレンス」</a> を参照してください。<br><br>変更タイプ IDs 「変更タイプまたは CSIO の検索」を参照してください。 |
| カテゴリ         | 任意の自由形式のテキスト                                 | を含む          | 個々のフィールドの正規表現はサポートされていません。大文字と小文字を区別しない検索                                                         |
| サブカテゴリ       |                                              |              |                                                                                                   |
| Item         |                                              |              |                                                                                                   |
| Operation    |                                              |              |                                                                                                   |

## 1. 変更タイプの分類を一覧表示する例をいくつか示します。

次のコマンドは、すべての変更タイプカテゴリを一覧表示します。

```
aws amscm list-change-type-categories
```

次の コマンドは、指定されたカテゴリに属するサブカテゴリを一覧表示します。

```
aws amscm list-change-type-subcategories --category CATEGORY
```

次の コマンドは、指定されたカテゴリとサブカテゴリに属する項目を一覧表示します。

```
aws amscm list-change-type-items --category CATEGORY --subcategory SUBCATEGORY
```

## 2. CLI クエリで変更タイプを検索する例をいくつか示します。

次のコマンドは、項目名に「S3」が含まれている CT 分類の概要を検索し、カテゴリ、サブカテゴリ、項目、オペレーション、変更タイプ ID の出力をテーブル形式で作成します。

```
aws amscm list-change-type-classification-summaries --query
  "ChangeTypeClassificationSummaries [?contains(Item, 'S3')].
  [Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
```

```
+-----+
|               ListChangeTypeClassificationSummaries               |
+-----+-----+-----+-----+-----+-----+
|Deployment|Advanced Stack Components|S3|Create|ct-1a68ck03fn98r|
+-----+-----+-----+-----+-----+-----+-----+
```

- その後、変更タイプ ID を使用して CT スキーマを取得し、パラメータを調べることができます。次のコマンドは、CreateS3Params.schema.json。

```
aws amscm get-change-type-version --change-type-id "ct-1a68ck03fn98r"
  --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
  CreateS3Params.schema.json
```

CLI クエリの使用の詳細については、[「--query Option で出力をフィルタリングする方法」](#)および「クエリ言語リファレンス」の[JMESPath Specification](#)を参照してください。

- 変更タイプ ID を取得したら、変更タイプのバージョンを検証して最新バージョンであることを確認することをお勧めします。次のコマンドを使用して、指定された変更タイプのバージョンを検索します。

```
aws amscm list-change-type-version-summaries --filter
  Attribute=ChangeTypeId,Value=CHANGE_TYPE_ID
```

AutomationStatus 特定の変更タイプの を検索するには、次のコマンドを実行します。

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --
  query "ChangeTypeVersion.{AutomationStatus:AutomationStatus.Name}"
```

ExpectedExecutionDurationInMinutes 特定の変更タイプの を検索するには、次のコマンドを実行します。

```
aws amscm --profile saml get-change-type-version --change-type-id ct-14027q0sjyt1h
--query "ChangeTypeVersion.{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

## AMS での RFC エラーのトラブルシューティング

多くの AMS プロビジョニング RFC 障害は、CloudFormation ドキュメントを通じて調査できます。[AWS CloudFormation のトラブルシューティング: エラーのトラブルシューティング](#) を参照してください。

追加のトラブルシューティングの提案については、以下のセクションで説明します。

### AMS の「管理」RFC エラー

AMS "Management" カテゴリ変更タイプ (CTs) を使用すると、リソースへのアクセスをリクエストしたり、既存のリソースを管理したりできます。このセクションでは、いくつかの一般的な問題について説明します。

#### RFC アクセスエラー

- RFC で指定したユーザー名と FQDN が正しく、ドメインに存在することを確認します。FQDN の検索については、[「FQDN の検索」](#) を参照してください。
- アクセス用に指定したスタック ID が EC2-related スタックであることを確認します。ELB や Amazon Simple Storage Service (S3) などのスタックは、アクセス RFCs の候補ではなく、読み取り専用アクセスロールを使用してこれらのスタックリソースにアクセスします。スタック ID の検索については、[「スタック IDs」](#) を参照してください。
- 指定したスタック ID が正しく、関連するアカウントに属していることを確認します。

その他のアクセス RFC 障害については、[「アクセス管理」](#) を参照してください。

YouTube 動画: [拒否や失敗を避けるために、変更リクエスト \(RFC\) を適切に作成するにはどうすればよいですか？](#)

#### RFC (手動) CT スケジューリングエラー

ほとんどの変更タイプは ExecutionMode=Automated ですが、一部は ExecutionMode=Manual であり、RFC の失敗を避けるためのスケジューリング方法に影響します。

ExecutionMode=Manual のスケジュールされた RFCs は、AMS コンソールを使用して RFC を作成する場合は、少なくとも 24 時間後に実行するように設定する必要があります。

AMS は手動 CT に 8 時間以内に応答することを目指しており、できるだけ早く対応しますが、RFC が実際に実行されるまでにかなり時間がかかる場合があります。

### 手動更新 CT RFCs の使用 CTs

AMS オペレーションは、更新するスタックタイプの更新変更タイプがある場合、管理 | その他 | スタックの更新に関するその他の RFCs を拒否します。

### RFC スタック削除エラー

RFC 削除スタックの失敗: Management | Standard stacks | Stack | Delete CT を使用する場合、AMS スタック名を持つスタックの詳細なイベントが CloudFormation コンソールに表示されます。スタックは、AMS コンソールの名前と照合することで識別できます。CloudFormation コンソールには、障害の原因に関する詳細が表示されます。

スタックを削除する前に、スタックの作成方法を考慮する必要があります。AMS CT を使用してスタックを作成し、スタックリソースを追加または編集しなかった場合、問題なく削除できます。ただし、削除スタック RFC を送信する前に、手動で追加されたリソースをスタックから削除することをお勧めします。たとえば、フルスタック CT (HA Two Tier) を使用してスタックを作成する場合、セキュリティグループ - SG1 が含まれます。次に AMS を使用して別のセキュリティグループ SG2 を作成し、フルスタックの一部として作成された SG1 内の新しい SG2 を参照し、削除スタック CT を使用してスタックを削除した場合、SG2 SG1 は削除しません。SG1

#### Important

スタックを削除すると、望ましくない結果や予期しない結果が生じる可能性があります。AMS は、この理由から、お客様に代わってスタックまたはスタックリソースを \*削除しない\* ことを優先します。AMS は、ユーザーに代わって (送信された管理 | その他 | その他 | 変更タイプの更新を通じて)、削除する適切な自動変更タイプを使用して削除できないリソースのみを削除することに注意してください。追加の考慮事項:

- リソースが「削除保護」に対して有効になっている場合、管理 | その他 | その他 | 変更タイプを更新し、削除保護を削除した後、自動 CT を使用してそのリソースを削除することで、AMS はこれをブロック解除できます。
- スタックに複数のリソースがあり、スタックリソースのサブセットのみを削除する場合は、CloudFormation Update 変更タイプを使用します ([CloudFormation Ingest Stack](#):



[Updatedating](#)」を参照)。管理 | その他 | その他 | 更新変更タイプを送信することもできます。AMS エンジニアは、必要に応じて変更セットの作成を支援します。

- ドリフトが原因で CloudFormation Update CT の使用に問題がある場合、AMS は、管理 | その他 | その他 | 更新を送信してドリフトを解決し (AWS CloudFormation サービスでサポートされる限り)、自動 CT、管理/カスタムスタック/CloudFormation テンプレートからのスタック/変更セットと更新の承認を使用して検証および実行できる ChangeSet を提供できます。

AMS は、予期しない、または予期しないリソースの削除がないように、上記の制限を維持します。

詳細については、[AWS CloudFormation のトラブルシューティング: スタックの削除が失敗する](#)」を参照してください。

## RFC 更新 DNS エラー

DNS ホストゾーンを更新する複数の RFCs は、理由なしに失敗する可能性があります。DNS ホストゾーン (プライベートまたはパブリック) を更新するために複数の RFCs を同時に作成すると、同じスタックを同時に更新しようとしているために、一部の RFCs が失敗する可能性があります。AMS 変更管理は、スタックが別の RFCs によって既に更新されているため、スタックを更新できない RFC を拒否または失敗します。AMS では、一度に 1 つの RFC を作成し、RFC が成功するのを待ってから、同じスタック用に新しい RFC を作成することをお勧めします。

## RFC IAM エンティティエラー

AMS は、ニーズを満たすように設計されたいくつかのデフォルトの IAM ロールとプロファイルを AMS アカウントにプロビジョニングします。ただし、追加の IAM リソースをリクエストする必要がある場合があります。

カスタム IAM リソースをリクエストする RFCs を送信するプロセスは、手動 RFCs の標準ワークフローに従いますが、承認プロセスには、適切なセキュリティコントロールが実施されていることを確認するためのセキュリティレビューも含まれています。したがって、通常、このプロセスは他の手動 RFCs よりも時間がかかります。これらの RFCs のサイクル時間を短縮するには、次のガイドラインに従ってください。

IAM レビューの意味と、それが技術標準およびリスク許容プロセスにどのようにマッピングされるかについては、「」を参照してください[RFC セキュリティレビューを理解する](#)。

## 一般的な IAM リソースリクエスト:

- CloudEndure などの主要なクラウド互換アプリケーションに関連するポリシーをリクエストする場合は、AMS の事前承認された IAM CloudEndure ポリシー: [WIGs Cloud Endure ランディングゾーンの例](#) ファイルを解凍し、customer\_cloud\_endure\_policy.json

### Note

より寛容なポリシーが必要な場合は、CloudArchitect/CSDM とニーズについて話し合い、必要に応じて、ポリシーを実装する RFC を送信する前に AMS セキュリティレビューとサインオフを取得します。

- デフォルトでは、アカウントに AMS によってデプロイされたリソースを変更する場合は、既存のリソースに変更を加えるのではなく、そのリソースの修正されたコピーをリクエストすることをお勧めします。
- (ユーザーに許可をアタッチするのではなく) 人間のユーザーの許可をリクエストする場合は、その許可をロールにアタッチし、そのロールを引き受ける許可をユーザーに付与します。これを行う方法の詳細については、[「一時的な AMS Advanced コンソールアクセス」](#)を参照してください。
- 一時的な移行またはワークフローに例外的なアクセス許可が必要な場合は、リクエストでそれらのアクセス許可の終了日を指定します。
- リクエストの件名についてセキュリティチームとすでに話し合っている場合は、CSDM に承認の証拠をできるだけ詳しく提供します。

AMS が IAM RFC を拒否した場合、拒否の明確な理由を指定します。例えば、IAM ポリシー作成リクエストを拒否し、ポリシーについて不適切な点を説明する場合があります。その場合は、特定された変更を行い、リクエストを再送信できます。リクエストのステータスをさらに明確にする必要がある場合は、サービスリクエストを送信するか、CSDM にお問い合わせください。

次のリストは、IAM RFCs を確認するときに AMS が軽減を試みる一般的なリスクを示しています。IAM RFC にこれらのリスクがある場合、RFC が拒否される可能性があります。例外が必要な場合、AMS はセキュリティチームの承認を求めます。このような例外を求めるには、CSDM と調整します。

**Note**

AMS は、何らかの理由で、アカウント内の IAM リソースへの変更を拒否することがあります。RFC 拒否に関する懸念については、サービスリクエストを介して AMS オペレーションに問い合わせるか、CSDM にお問い合わせください。

- 独自のアクセス許可を変更したり、アカウント内の他のリソースのアクセス許可を変更したりできるアクセス許可など、権限のエスカレーション。例:
  - 別のより特権的なロール `iam:PassRole` で を使用する。
  - ロールまたはユーザーから IAM ポリシーをアタッチ/デタッチするアクセス許可。
  - アカウントの IAM ポリシーの変更。
  - 管理インフラストラクチャのコンテキストで API コールを行う機能。
- AMS サービスを提供するために必要なリソースまたはアプリケーションを変更するアクセス許可。例:
  - 踏み台、管理ホスト、EPS インフラストラクチャなどの AMS インフラストラクチャの変更。
  - ログ管理 AWS Lambda 関数、またはログストリームの削除。
  - デフォルトの CloudTrail モニタリングアプリケーションの削除または変更。
  - Directory Services Active Directory (AD) の変更。
  - CloudWatch (CW) アラームを無効にする。
  - ランディングゾーンの一部としてアカウントにデプロイされたプリンシパル、ポリシー、名前空間の変更。
- 情報セキュリティを危険にさらす状態でインフラストラクチャを作成できるアクセス許可など、ベストプラクティス外のインフラストラクチャのデプロイ。例:
  - パブリックまたは暗号化されていない S3 バケットの作成または EBS ボリュームのパブリック共有。
  - パブリック IP アドレスのプロビジョニング。
  - 広範なアクセスを許可するようにセキュリティグループを変更しました。
- データ損失、整合性損失、不適切な設定、インフラストラクチャおよびアカウント内のアプリケーションのサービスの中断につながる可能性のあるアクセス許可など、アプリケーションに影響を与える可能性のある過度に広範なアクセス許可。例:
  - やなどの APIs を介したネットワークトラフィックの無効

- マネージドホストからボリュームをデタッチしてマネージドインフラストラクチャを無効にする。
- AMS サービスの説明の一部ではなく、AMS でサポートされていないサービスのアクセス許可。

AMS サービスの説明に記載されていないサービスは、AMS アカウントでは使用できません。機能またはサービスのサポートをリクエストするには、CSDM にお問い合わせください。

- 過度に寛大であるか、控えめであるか、間違っただけのリソースに適用されるため、指定された目標を達成できないアクセス許可。例:
  - 関連するキーへのアクセス `s3:PutObject` 許可のない、必須の KMS 暗号化を持つ S3 バケットへのアクセス `KMS:Encrypt` 許可のリクエスト。
  - アカウントに存在しないリソースに関連するアクセス許可。
  - RFCs の説明がリクエストと一致しないように思われる IAM RFC。

## 「デプロイ」 RFC エラー

AMS "Deployment" カテゴリ変更タイプ (CTs) を使用すると、AMS がサポートするさまざまなリソースをアカウントに追加することをリクエストできます。

リソースを作成するほとんどの AMS CTs は、CloudFormation テンプレートに基づいています。お客様は、CloudFormation コンソールを使用して CloudFormation、CloudFormation スタックの説明に基づいてスタックを表すスタックをすばやく特定できます。障害が発生したスタックは `DELETE_COMPLETE` 状態である可能性があります。CloudFormation スタックを特定すると、イベントには作成に失敗した特定のリソースとその理由が表示されます。

### CloudFormation ドキュメントを使用したトラブルシューティング

ほとんどの AMS プロビジョニング RFCs は CloudFormation テンプレートを使用しており、そのドキュメントはトラブルシューティングに役立ちます。その CloudFormation テンプレートのドキュメントを参照してください。

- アプリケーションロードバランサーの作成の失敗: [AWS::ElasticLoadBalancingV2::LoadBalancer \(Application Load Balancer\)](#)
- Auto [Scaling グループ](#)の作成: [AWS::AutoScaling::AutoScalingGroup \(Auto Scaling グループ\)](#)
- memcached キャッシュの作成: [AWS::ElastiCache::CacheCluster \(キャッシュクラスター\)](#)
- Redis キャッシュの作成: [AWS::ElastiCache::CacheCluster \(キャッシュクラスター\)](#)

- DNS ホストゾーンの作成 (DNS プライベート/パブリックの作成で使用):  
[AWS::Route53::HostedZone \(R53 ホストゾーン\)](#)
- DNS レコードセットの作成 (DNS プライベート/パブリックの作成で使用):  
[AWS::Route53::RecordSet \(リソースレコードセット\)](#)
- EC2 スタックの作成: [AWS::EC2::Instance \(Elastic Compute Cloud\)](#)
- Elastic File System (EFS): [AWS::EFS::FileSystem \(Elastic File System\)](#)
- ロードバランサーの作成: [AWS::ElasticLoadBalancing::LoadBalancer \(Elastic Load Balancer\)](#)
- RDS DB の作成: [AWS::RDS::DBInstance \(リレーショナルデータベース\)](#)
- Amazon S3 の作成: [AWS::S3::Bucket \(Simple Storage Service\)](#)
- キューの作成: [AWS::SQS::Queue \(簡易キューサービス\)](#)

## RFC AMI AMIs の作成エラー

Amazon マシンイメージ (AMI) は、ソフトウェア構成 (オペレーティングシステム、アプリケーションサーバー、アプリケーションなど) を記録したテンプレートです。AMI から、クラウドで仮想サーバーとして実行される AMI のコピーであるインスタンスを起動します。AMIs は非常に有用であり、EC2 インスタンスまたは Auto Scaling グループの作成に必要ですが、いくつかの要件に従う必要があります。

- に指定するインスタンスは、RFC が成功するためには停止状態 `Ec2InstanceId` である必要があります。ASG は停止したインスタンスを終了するため、このパラメータに Auto Scaling グループ (ASG) インスタンスを使用しないでください。
- AMS Amazon マシンイメージ (AMI) を作成するには、AMS インスタンスから始める必要があります。インスタンスを使用して AMI を作成する前に、インスタンスが停止され、そのドメインから接続解除されていることを確認することで、インスタンスを準備する必要があります。詳細については、「[Sysprep を使用して標準 Amazon マシンイメージを作成する](#)」を参照してください。
- 新しい AMI に指定する名前は、アカウント内で一意である必要があります。そうしないと、RFC は失敗します。これを行う方法については、「[AMI | Create](#)」で説明されています。詳細については、「[AMI | Create](#)」および「[AWS AMI Design](#)」を参照してください。

### Note

AMI 作成の準備の詳細については、「[AMI | Create](#)」を参照してください。

## EC2s または ASGs エラーを作成する RFCs

タイムアウトを伴う EC2 または ASG 障害の場合、AMS では、使用する AMI がカスタマイズされているかどうかを確認することをお勧めします。その場合は、このガイドに含まれている AMI 作成手順 ([「AMI」作成](#)) を参照して、AMI が正しく作成されたことを確認してください。カスタム AMI を作成する際の一般的な間違いは、ガイドの手順に従って Sysprep の名前を変更または呼び出すことではありません。

## RDS エラーを作成する RFCs

Amazon Relational Database Service (RDS) の障害は、RDS の作成時にさまざまなエンジンを使用でき、各エンジンには独自の要件と制限があるため、さまざまな理由で発生する可能性があります。AMS RDS スタックを作成する前に、AWS RDS パラメータ値を慎重に確認してください。[CreateDBInstance](#)」を参照してください。

サイズのレコメンデーションなど、Amazon RDS 全般の詳細については、[Amazon Relational Database Service ドキュメント](#)」を参照してください。

## Amazon S3s エラーを作成する RFCs

S3 ストレージバケットを作成する際の一般的なエラーの 1 つは、バケットに一意の名前を使用しないことです。以前に送信したものと同名前の S3 バケット Create CT を送信した場合、その BucketName を持つ S3 バケットがすでに存在するため、失敗します。これは CloudFormation コンソールで詳しく説明され、スタックイベントにバケット名がすでに使用されていることが示されます。

## RFC 検証エラーと実行エラー

RFC の失敗と関連するメッセージは、選択した RFC の AMS コンソール RFC の詳細ページの出力メッセージによって異なります。

- 検証失敗の理由は、ステータスフィールドでのみ使用できます。
- 実行失敗の理由は、実行出力とステータスフィールドで使用できます。

## RFC エラーメッセージ

リストされた変更タイプ (CTs) で次のエラーが発生した場合は、これらのソリューションを使用して問題の原因を見つけて修正できます。



```
{"errorMessage": "An error has occurred during RFC execution. We are investigating the issue.", "errorType": "InternalError"}
```

以下のトラブルシューティングオプションを参照してさらにサポートが必要な場合は、RFC 通信を通じて AMS をエンゲージしてください。詳細については、[「RFC の通信と添付ファイル \(コンソール\)」](#)を参照してください。

## ワークロード取り込み (WIGS) エラー

### Note

Windows と Linux の両方の検証ツールは、オンプレミスサーバーと AWS の EC2 インスタンスに直接ダウンロードして実行できます。これらは、「AMS Advanced Application Developer's Guide [Migrating workloads: Linux pre-ingestion validation](#)」および「[Migrating workloads: Windows pre-ingestion validation](#)」で確認できます。

- EC2 インスタンスがターゲット AMS アカウントに存在することを確認します。たとえば、AMS 以外のアカウントから AMS アカウントに AMI を共有している場合は、ワークロード取り込み RFC を送信する前に、共有 AMI を使用して AMS アカウントに EC2 インスタンスを作成する必要があります。
- インスタンスにアタッチされたセキュリティグループで送信トラフィックが許可されているかどうかを確認します。SSM エージェントはパブリックエンドポイントに接続できる必要があります。
- インスタンスに SSM エージェントに接続するための適切なアクセス許可があるかどうかを確認します。これらのアクセス許可には `customer-mc-ec2-instance-profile` が付属しています。これは EC2 コンソールで確認できます。

## EC2 インスタンススタック停止エラー

- インスタンスが既に停止状態か終了状態かを確認します。
- EC2 インスタンスがオンラインであり、InternalErrorエラーが表示された場合は、AMS が調査するためのサービスリクエストを送信します。
- 変更タイプ Management | Advanced stack components | EC2 instance stack | Stop `ct-3mvt2zkyvej` を使用して Auto Scaling グループ (ASG) インスタンスを停止することはできません。ASG インスタンスを停止する必要がある場合は、サービスリクエストを送信します。

## EC2 インスタンススタックの作成エラー

メッセージは CloudFormation からの InternalError ものです。CREATION\_FAILED ステータスの理由です。CloudWatch スタックイベントでスタックの障害に関する詳細を確認するには、次の手順に従います。

- AWS マネジメントコンソールでは、スタックの作成、更新、または削除中にスタックイベントのリストを表示できます。このリストから失敗イベントを探して、そのイベントのステータスの理由を確認します。

ステータスの理由には、問題を理解するのに役立つ AWS CloudFormation または特定のサービスからのエラーメッセージが含まれている場合があります。

- スタックイベントの表示の詳細については、[「AWS マネジメントコンソールでの AWS CloudFormation スタックデータとリソースの表示」](#)を参照してください。

## EC2 インスタンスボリュームの復元エラー

EC2 インスタンスボリュームの復元が失敗すると、AMS は内部トラブルシューティング RFC を作成します。これは、EC2 インスタンスボリュームの復元がディザスタリカバリ (DR) の重要な部分であり、AMS によってこの内部トラブルシューティング RFC が自動的に作成されるためです。

内部トラブルシューティング RFC が作成されると、バナーが表示され、RFC へのリンクが表示されます。この内部トラブルシューティング RFC は、RFC の障害をより詳細に可視化し、同じエラーにつながる再試行 RFCs を送信したり、この障害について AMS に手動で連絡したりするのではなく、変更を追跡して、障害が AMS によって処理されていることを知ることができます。これにより、AMS Operators がリクエストを待つ代わりに RFC 障害にプロアクティブに取り組むため、変更の time-to-recovery (TTR) メトリクスも短縮されます。

## RFC のヘルプを取得する方法

AMS に連絡して、障害の根本原因を特定できます。AMS の営業時間は、1 日 24 時間、1 週間 7 日、1 年 365 日です。

AMS には、サポートを求めるための手段がいくつか用意されています。

- オープン RFC または完了しても正しくない RFC のサポートが必要な場合は、RFC 双方向通信を通じて AMS をエンゲージします。詳細については、[「RFC の通信と添付ファイル \(コンソール\)」](#)を参照してください。



- マネージド環境に影響する AWS または AMS サービスのパフォーマンスの問題を報告するには、AMS コンソールを使用してインシデントレポートを送信します。詳細については、[「インシデントの報告」](#)を参照してください。AMS インシデント管理の一般的な情報については、[「インシデント対応」](#)を参照してください。
- お客様またはお客様のリソースやアプリケーションが AMS とどのように連携しているかに関する具体的な質問、またはインシデントのエスカレーションについては、以下のうち 1 つ以上を E メールで送信してください。
  1. まず、サービスリクエストまたはインシデントレポートのレスポンスに満足できない場合は、CSDM に E メールを送信してください: [ams-csdm@amazon.com](mailto:ams-csdm@amazon.com)
  2. 次に、エスカレーションが必要な場合は、AMS Operations Manager に E メールを送信できます (CSDM はおそらくこれを行います): [ams-opsmanager@amazon.com](mailto:ams-opsmanager@amazon.com)
  3. さらにエスカレーションは、AMS Director: [ams-director@amazon.com](mailto:ams-director@amazon.com) に行われます。
  4. 最後に、AMS VP にいつでもアクセスできます: [ams-vp@amazon.com](mailto:ams-vp@amazon.com)

## AMS の直接変更モード

### トピック

- [直接変更モードの開始方法](#)
- [セキュリティとコンプライアンス](#)
- [Direct Change モードでの変更管理](#)
- [Direct Change モードを使用したスタックの作成](#)
- [直接変更モードのユースケース](#)

AWS Managed Services (AMS) Direct Change Mode (DCM) は、リソースをプロビジョニングおよび更新するための AMS Advanced Plus および Premium アカウントへのネイティブ AWS アクセスを提供することで、AMS Advanced 変更管理を拡張します AWS。DCM では、ネイティブ AWS API (コンソールまたは CLI/SDK) または AMS Advanced Change Management Request for Change (RFCs) を使用するオプションがあり、いずれの場合も、リソースと変更がモニタリング、パッチ、バックアップ、インシデント対応管理など、AMS によって完全にサポートされています。DCM を介してプロビジョニングされたリソースは、AMS サービスナレッジ管理システム (SKMS) に登録され、AMS マネージド Active Directory ドメイン (該当する場合) に結合され、AMS 管理エージェントを実行します。既存のツール (CloudFormation、AWS SDK、CDK など) を使用して、AMS 管理の CloudFormation スタックを開発およびデプロイします。

**Note**

直接変更モードでは、AMS 変更管理 RFCsは削除されません。DCM を使用して AMS RFCs にフルアクセスできます。

[詳細については、Akash の動画をご覧ください \(6:30\)](#)

## 直接変更モードの開始方法

まず前提条件を確認してから、対象となる AMS Advanced アカウントで変更リクエスト (RFC) を送信します。

1. DCM で使用するアカウントが要件を満たしていることを確認します。
  - アカウントは AMS Advanced Plus または Premium です。
  - アカウントで Service Catalog が有効になっていません。現在、DCM と Service Catalog の両方へのアカウントのオンボーディングはサポートされていません。Service Catalog に既にオンボーディングされているが DCM に関心がある場合は、クラウドサービスデリバリーマネージャー (CSDM) とニーズについて話し合ってください。Service Catalog から DCM に切り替える場合は、Service Catalog をオフボードして変更を依頼してください。AMS での Service Catalog の詳細については、「[AMS と Service Catalog](#)」を参照してください。
2. Management | Managed Account | Direct Change Mode | Enable change type (ct-3rd4781c2nnhp) を使用して、変更リクエスト (RFC) を送信します。チュートリアル の例については、「[直接変更モード | 有効化](#)」を参照してください。

CT が処理されると、事前定義された IAM ロール `AWSManagedServicesCloudFormationAdminRole` と `AWSManagedServicesUpdateRole` が指定されたアカウントにプロビジョニングされます。

3. 内部フェデレーションプロセスを使用して DCM アクセスを必要とするユーザーに適切なロールを割り当てます。

**Note**

ロールを引き受けるには、任意の数の `SAMLIdentityProviders`、AWS Services、IAM エンティティ (ロール、ユーザーなど) を指定できます。、`SAMLIdentityProviderARNs`、`IAMEntityARNs` または の少なくとも 1 つを指定

する必要がありますAWSServicePrincipals。詳細については、会社の IAM 部門または AMS クラウドアーキテクト (CA) にお問い合わせください。

## 直接変更モードの IAM ロールとポリシー

アカウントで直接変更モードが有効になっている場合、これらの新しい IAM エンティティがデプロイされます。

**AWSManagedServicesCloudFormationAdminRole:** このロールは、CloudFormation コンソールへのアクセス、CloudFormation スタックの作成と更新、ドリフトレポートの表示、CloudFormation ChangeSets の作成と実行を許可します。このロールへのアクセスは、SAML プロバイダーを通じて管理されます。

ロールAWSManagedServicesCloudFormationAdminRoleにデプロイおよびアタッチされる管理ポリシーは次のとおりです。

- AMS Advanced マルチアカウントランディングゾーン (MALZ) アプリケーションアカウント
  - AWSManagedServices\_CloudFormationAdminPolicy1
  - AWSManagedServices\_CloudFormationAdminPolicy2
  - このポリシーは、に付与されたアクセス許可を表しますAWSManagedServicesCloudFormationAdminRole。このポリシーを使用して、アカウント内の既存のロールへのアクセスを許可し、そのロールがアカウント内の CloudFormation スタックを起動および更新できるようにします。これには、他の IAM エンティティが CloudFormation スタックを起動できるように、追加の AMS サービスコントロールポリシー (SCP) 更新が必要になる場合があります。
- AMS Advanced シングルアカウントランディングゾーン (SALZ) アカウント
  - AWSManagedServices\_CloudFormationAdminPolicy1
  - AWSManagedServices\_CloudFormationAdminPolicy2
  - cdk-legacy-mode-s3-access [インラインポリシー]
  - AWS ReadOnlyAccess ポリシー

**AWSManagedServicesUpdateRole:** このロールは、ダウストリーム AWS サービス APIs への制限付きアクセスを許可します。ロールは、変更および非変更 API オペレーションを提供する マネージドポリシーでデプロイされますが、一般的には、IAM、KMS、GuardDuty、VPC、AMS インフ

ラストラクチャリソースや設定などの特定のサービスに対して変更オペレーション (Create/Delete/PUT など) を制限します。このロールへのアクセスは、SAML プロバイダーを通じて管理されます。

ロールAWSManagedServicesUpdateRoleにデプロイおよびアタッチされる管理ポリシーは次のとおりです。

- AMS Advanced マルチアカウントランディングゾーンアプリケーションアカウント
  - AWSManagedServicesUpdateBasePolicy
  - AWSManagedServicesUpdateDenyPolicy
  - AWSManagedServicesUpdateDenyProvisioningPolicy
  - AWSManagedServicesUpdateEC2AndRDSPolicy
  - AWSManagedServicesUpdateDenyActionsOnAMSInfraPolicy
- AMS Advanced シングルアカウントランディングゾーンアカウント
  - AWSManagedServicesUpdateBasePolicy
  - AWSManagedServicesUpdateDenyProvisioningPolicy
  - AWSManagedServicesUpdateEC2AndRDSPolicy
  - AWSManagedServicesUpdateDenyActionsOnAMSInfraPolicy1
  - AWSManagedServicesUpdateDenyActionsOnAMSInfraPolicy2

これらに加えて、マネージドポリシーAWSManagedServicesUpdateRoleロールには AWS マネージドポリシーもViewOnlyAccessタッチされています。

## セキュリティとコンプライアンス

セキュリティとコンプライアンスは、AMS Advanced とお客様との間の責任共有です。AMS Advanced Direct Change モードは、この責任共有を変更しません。

### 直接変更モードのセキュリティ

AMS Advanced は、規範的なランディングゾーン、変更管理システム、アクセス管理で追加の値を提供します。Direct Change モードを使用する場合、この責任モデルは変更されません。ただし、追加のリスクに注意する必要があります。

Direct Change Mode の「Update」ロール (「」を参照[直接変更モードの IAM ロールとポリシー](#)) は、エンティティがアクセスできるようにする昇格されたアクセス許可を提供し、アカウント内の AMS がサポートするサービスのインフラストラクチャリソースを変更します。アクセス許可が引き上げられると、リソース、サービス、アクションに応じてさまざまなリスクが存在します。特に、監

視、ミス、または内部プロセスとコントロールフレームワークへの準拠の欠如が原因で誤った変更が行われた状況では、リスクが異なります。

AMS 技術標準に従って、以下のリスクが特定され、次のようにレコメンデーションが行われます。AMS 技術標準の詳細については、「」を参照してください AWS Artifact。アクセスするには AWS Artifact、CSDM に連絡して手順を確認するか、[「 の開始方法 AWS Artifact」](#)を参照してください。

AMS-STD-001: タグ付け

| [Standards] (標準)                                                                                                         | 壊れていますか？                                                                                                                                                                                                                                                             | リスク                                                                                | 推奨事項                                                                      |
|--------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| <div>すべての AMS 所有リソースには、次のキーと値のペアが必要です</div> <div>上記のタグ以外のすべての AMS 所有タグには、upper/lower/mixMC*の AMS*やなどのプレフィックスが必要です。</div> | <div>はい。CloudFormation、CloudTrail、EFS、OpenSearch、CloudWatch Logs、SQS、SSM、タグ付け API のブレーク - これらのサービスは AMS 名前空間のタグ付けを制限するaws:TagsKey 条件をサポートしていないため。</div> <div>次の表 AMS-STD-003 の標準では、AppId、Environment、AppName は変更できますが、AMS 所有のリソースは変更できません。IAM アクセス許可では達成できません。</div> | <div>AMS リソースのタグ付けが正しくないと、リソースのレポート、アラート、パッチ適用オペレーションに AMS 側で悪影響が及ぶ可能性があります。</div> | <div>AMS チーム以外のすべてのユーザーの AMS のデフォルトのタグ付け要件を変更するには、アクセスを復元する必要があります。</div> |
| AMS 所有スタックのタグは、変更リクエ                                                                                                     | はい。CloudFormation は、AMS                                                                                                                                                                                                                                              |                                                                                    |                                                                           |

| [Standards] (標準)                              | 壊れていますか？                                                                                                                                                                                                                             | リスク | 推奨事項 |
|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|------|
| ストに基づいて削除しないでください。                            | 名前空間のタグを制限するaws:TagsKey 条件をサポートしていません。                                                                                                                                                                                               |     |      |
| 次の表 AMS-AMS-STD-002 タグの命名規則を使用することは許可されていません。 | はい。CloudFormation、CloudTrail、Amazon Elastic File System (EFS)、OpenSearch、CloudWatch Logs、Amazon Simple Queue Service (SQS)、Amazon EC2 Systems Manager (SSM)、Tagging API のブレイク。これらのサービスは、AMS 名前空間のタグ付けを制限するaws:TagsKey 条件をサポートしていません。 |     |      |

## AMS-STD-002: Identity and Access Management (IAM)

| [Standards] (標準)                                               | 壊れていますか？                                               | リスク                                                      | 推奨事項                                                  |
|----------------------------------------------------------------|--------------------------------------------------------|----------------------------------------------------------|-------------------------------------------------------|
| 4.7 変更管理プロセス (RFC) をバイパスするアクションは、インスタンスの起動または停止、S3 バケットまたは RDS | はい。セルフサービスアクションの目的は、AMS RFC システムをバイパスしてアクションを実行することです。 | セキュアアクセスモデルは AMS の主要な技術的側面であり、コンソールまたはプログラムによるアクセス用の IAM | IAM ユーザーには、最小特権と need-to-know ことに基づいて、時間制限があり、アクセス許可が |

| [Standards] (標準)                                                                                           | 壊れていますか？ | リスク                                                                                        | 推奨事項            |
|------------------------------------------------------------------------------------------------------------|----------|--------------------------------------------------------------------------------------------|-----------------|
| インスタンスの作成などを許可してはいけません。デベロッパーモードアカウントとセルフサービスプロビジョンドモードサービス (SSPS) は、アクションが割り当てられたロールの境界内で実行される限り、除外されません。 |          | ユーザーがこのアクセスコントロールを回避します。IAM ユーザーのアクセスは、AMS 変更管理によってモニタリングされません。アクセスは CloudTrail にのみ記録されます。 | 付与されている必要があります。 |

## AMS-STD-003: ネットワークセキュリティ

| [Standards] (標準)                                                           | 壊れていますか？                                                            | リスク                                                                             | 推奨事項                                                                                                          |
|----------------------------------------------------------------------------|---------------------------------------------------------------------|---------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| S2。EC2 インスタンスの Elastic IP は、正式なリスク承諾契約、または内部チームによる有効なユースケースでのみ使用する必要があります。 | はい。セルフサービスアクションを使用すると、Elastic IP アドレス (EIP) の関連付けと関連付け解除を行うことができます。 | Elastic IP をインスタンスに追加すると、その IP はインターネットに公開されます。これにより、情報開示や不正なアクティビティのリスクが高まります。 | セキュリティグループを介してそのインスタンスへの不要なトラフィックをブロックし、セキュリティグループがインスタンスにアタッチされていることを確認し、ビジネス上の理由で必要な場合にのみトラフィックを許可するようにします。 |
| S14。同じ顧客に属するアカウント間の VPC ピアリングとエ                                            | はい。IAM ポリシーでは実行できません。                                               | AMS アカウントから出るトラフィックは、アカウントの境                                                    | 所有している AMS アカウントとのみピア接続することをお勧めします。ユース                                                                        |



| [Standards] (標準)                                                                           | 壊れていますか？ | リスク                                         | 推奨事項                                                                          |
|--------------------------------------------------------------------------------------------|----------|---------------------------------------------|-------------------------------------------------------------------------------|
| エンドポイント接続を許可できます。                                                                          |          | 界から出るとモニタリングされません。                          | ケースでこれが必要な場合は、セキュリティグループとルートテーブルを使用して、関連する接続を介して出力できるトラフィック範囲、リソース、タイプを制限します。 |
| AMS ベース AMIs は、AMS が管理するアカウントとアンマネージドアカウントの間に共有できます。ただし、それらが同じ AWS 組織によって所有されていることを確認できます。 |          | AMIs 機密データが含まれており、意図しないアカウントに公開される可能性があります。 | 組織が所有するアカウントのみと AMIs を共有するか、組織外で共有する前にユースケースとアカウント情報を検証します。                   |

## AMS-STD-007: ログ記録

| [Standards] (標準)                                | 壊れていますか？                                                    | リスク                                        | 推奨事項                                                                                |
|-------------------------------------------------|-------------------------------------------------------------|--------------------------------------------|-------------------------------------------------------------------------------------|
| 19. ログは、ある AMS アカウントから同じ顧客の別の AMS アカウントに転送できます。 | はい。同じ組織内の顧客アカウントの検証による顧客ログの潜在的なセキュリティ低下は、IAM ポリシーでは達成できません。 | ログには機密データが含まれており、意図しないアカウントに公開される可能性があります。 | AWS 組織によって管理されているアカウントのみとログを共有するか、組織外と共有する前にユースケースとアカウント情報を検証します。これは複数の方法で検証できます。クラ |
| 20. ログは、AMS 以外のアカウントが同じ AMS 顧客によって所有されている (同じ   |                                                             |                                            |                                                                                     |



| [Standards] (標準)                                                                                                     | 壊れていますか？ | リスク | 推奨事項                                |
|----------------------------------------------------------------------------------------------------------------------|----------|-----|-------------------------------------|
| AWS Organizations アカウントにあることを確認するか、E メールドメインを顧客の会社名と PAYER リンクアカウントと照合する) 場合にのみ、内部ツールを使用して AMS から非 AMS アカウントに転送できます。 |          |     | ウドサービスデリバリーマネージャー (CSDM) に確認してください。 |

内部認可および認証チームと協力して、それに応じて Direct Change モードロールへのアクセス許可を制御します。

## 直接変更モードのコンプライアンス

Direct Change モードは、本番ワークロードと非本番ワークロードの両方と互換性があります。コンプライアンス標準 (PHI、HIPAA、PCI など) を確実に順守し、Direct Change モードの使用が内部管理フレームワークと標準に準拠していることを確認するのはお客様の責任です。

## Direct Change モードでの変更管理

変更管理は、AMS Advanced が変更リクエストを実装するために使用するプロセスです。変更リクエスト (RFC) は、ユーザーまたは AMS Advanced インターフェイスを介して AMS Advanced によって作成されたリクエストで、マネージド環境に変更を加え、特定のオペレーションの AMS Advanced 変更タイプ (CT) ID が含まれます。詳細については、[「変更管理」](#)を参照してください。

### Note

直接変更モードでは、AMS 変更管理 RFCs は削除されません。DCM を使用して AMS RFCs にフルアクセスできます。

AMS Direct Change Mode (DCM) は、リソースをプロビジョニングおよび更新するための AMS Advanced Plus および Premium アカウントへのネイティブ AWS アクセスを提供することで、AMS

Advanced 変更管理を拡張します AWS 。IAM ロールを通じて直接変更モードのアクセス許可を付与されたユーザーは、ネイティブ AWS API アクセスを使用して、AMS Advanced アカountのリソースをプロビジョニングおよび変更できます。ユーザーは、同じ IAM ロールを使用して AMS Advanced 変更管理 RFCs を引き続き使用できます。どちらの場合も、リソースとその変更は、モニタリング、パッチ、バックアップ、インシデント対応管理など、AMS によって完全にサポートされています。これらのアカウントで適切なロールを持たないユーザーは、AMS Advanced 変更管理 RFC プロセスを使用して変更を行う必要があります。

## 変更管理のユースケース

セキュリティ上の理由から、AMS Advanced の一部の変更は、変更管理の変更リクエスト (RFC) プロセスを通じてのみ行うことができます。AWSManagedServicesCloudFormationAdminRole は、CloudFormation (CFN) を通じて実行されるアクションに制限されます。DCM を使用してスタックを作成する方法の詳細については、「[直接変更モードを使用したスタックの作成](#)」を参照してください。AWSManagedServicesUpdateRole は、次のアクションに制限されています。

管理 | マネージドアカウント | 直接変更モード | 有効化 (ct-3rd4781c2nnhp) 変更タイプを含む各変更タイプのチュートリアルについては、「AMS Advanced Change Type Reference [Change Types by Classification](#)」セクションの「Additional Information」セクションを参照してください。

| サービス                                     | アクション          |
|------------------------------------------|----------------|
| AWS Key Management Service (AWS KMS)     | 更新             |
| AWS Certificate Manager                  | 作成             |
| AWS Identity and Access Management (IAM) | いずれか           |
| Site-to-Site VPN                         | すべて            |
| AMS リソーススケジューラ                           |                |
| AWS Backup                               | バックアッププランを作成する |
| AMS ワークロード取り込み (WIGs)                    | いずれか           |
| AMS Advanced MALZ アカountの変更              |                |
| Amazon GuardDuty                         |                |

| サービス                                        | アクション            |
|---------------------------------------------|------------------|
| AMS アドバンスドスタックアクセス                          | いずれか             |
| Amazon Elastic Block Store (EBS) ボリューム      | Delete           |
| Amazon Elastic Block Store (EBS) のデフォルトの暗号化 | デフォルトの暗号化を有効にする  |
| Amazon Elastic Compute Cloud (Amazon EC2)   | ホスト名の変更          |
| Amazon マシンイメージ (AMI)                        | 削除、共有            |
| Amazon EC2 セキュリティグループ                       | いずれか             |
| AMS Advanced SSPS                           |                  |
| AWS Managed Microsoft AD                    |                  |
| AMS Advanced デベロッパーモード                      |                  |
| Amazon Simple Storage Service (Amazon S3)   | S3 バケットポリシーを作成する |
| AWS Systems Manager                         | 作成               |

## Direct Change モードを使用したスタックの作成

を使用して CloudFormation でスタックを起動する場合

合AWSManagedServicesCloudFormationAdminRole、スタックを AMS で管理するには、次の 2 つの要件があります。

- テンプレートには が含まれている必要がありますAmsStackTransform。
- スタック名はプレフィックスで始まり、その後に 17 文字の英数字文字列がstack-続く必要があります。

### Note

を正常に使用するにはAmsStackTransform、 CloudFormation (CFN) がスタックを作成または更新するために、スタックテンプレートに CAPABILITY\_AUTO\_EXPAND機能が含

まれていることを確認する必要があります。これを行うには、`create-stack` リクエスト `CAPABILITY_AUTO_EXPAND` の一部として渡します。がテンプレートに含まれているときにこの機能が確認されない場合、CFN `AwsStackTransform` はリクエストを拒否します。CFN コンソールでは、テンプレートに 変換がある場合にこの機能を渡すことができますが、APIs を介して CFN とやり取りしている場合、この機能が失われる可能性があります。

この機能は、次の CFN API コールを使用するたびに渡す必要があります。

- [CreateChangeSet](#)
- [CreateStack](#)
- [UpdateStack](#)

DCM を使用してスタックを作成または更新する場合、CFN Ingest および Stack Update CTs [CloudFormation 「Ingest Guidelines」](#)、[「Best Practices」](#)、および [「Limitations」](#) を参照してください。ただし、AMS デフォルトセキュリティグループ (SGs) は Auto Scaling グループ (ASGs) のスタンドアロン EC2 インスタンスまたは EC2 インスタンスにはアタッチされません。スタンドアロン EC2 インスタンスまたは ASGs を使用して CloudFormation テンプレートを作成する場合、デフォルトの SGs をアタッチできます。

#### Note

IAM ロールを で作成および管理できるようになりました `AWSManagedServicesCloudFormationAdminRole`。

AMS デフォルト SGs には、インスタンスが正常に起動し、後で AMS オペレーションとユーザーによる SSH または RDP を介してアクセスできるようにする進入および退出ルールがあります。で AMS のデフォルトのセキュリティグループが許容されすぎることがわかった場合は、より制限の厳しいルールを使用して独自の SGs を作成し、インスタンスにアタッチできます。ただし、インシデント発生時にユーザーと AMS オペレーションがインスタンスにアクセスできる場合に限りです。

AMS のデフォルトのセキュリティグループは次のとおりです。

- `SentinelDefaultSecurityGroupPrivateOnly`: この SSM パラメータを使用して CFN テンプレートでアクセスできます `/ams/${VpcId}/SentinelDefaultSecurityGroupPrivateOnly`

- SentinelDefaultSecurityGroupPrivateOnlyEgressAll: この SSM パラメータを使用して CFN テンプレートでアクセスできます /ams/\${VpcId}/SentinelDefaultSecurityGroupPrivateOnlyEgressAll

## AMS 変換

CloudFormation テンプレートに Transform ステートメントを追加します。これにより、起動時にスタックを検証して AMS に登録する CloudFormation マクロが追加されます。

### JSON の例

```
"Transform": {
  "Name": "AmsStackTransform",
  "Parameters": {
    "StackId": {"Ref" : "AWS::StackId"}
  }
}
```

### YAML の例

```
Transform:
  Name: AmsStackTransform
  Parameters:
    StackId: !Ref 'AWS::StackId'
```

また、既存のスタックのテンプレートを更新するときに Transform ステートメントを追加します。

### JSON の例

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description" : "Create an SNS Topic",
  "Transform": {
    "Name": "AmsStackTransform",
    "Parameters": {
      "StackId": {"Ref" : "AWS::StackId"}
    }
  },
  "Parameters": {
    "TopicName": {
      "Type": "String",
```

```
    "Default": "HelloWorldTopic"
  },
  "Resources": {
    "SnsTopic": {
      "Type": "AWS::SNS::Topic",
      "Properties": {
        "TopicName": {"Ref": "TopicName"}
      }
    }
  }
}
```

## YAML の例

```
AWSTemplateFormatVersion: '2010-09-09'
Description: Create an SNS Topic
Transform:
  Name: AmsStackTransform
  Parameters:
    StackId: !Ref 'AWS::StackId'
Parameters:
  TopicName:
    Type: String
    Default: HelloWorldTopic
Resources:
  SnsTopic:
    Type: AWS::SNS::Topic
    Properties:
      TopicName: !Ref TopicName
```

## スタック名

スタック名はプレフィックスで始まり、その後に 17 文字の英数字文字列が stack-続く必要があります。これは、AMS スタック IDs。

互換性のあるスタック IDs を生成する方法の例を次に示します。

Bash:

```
echo "stack-$(env LC_CTYPE=C tr -dc 'a-z0-9' < /dev/urandom | head -c 17)"
```

Python:

```
import string
import random

'stack-' + ''.join(random.choices(string.ascii_lowercase + string.digits, k=17))
```

Powershell:

```
"stack-" + ( -join ((0x30..0x39) + ( 0x61..0x7A) | Get-Random -Count 17 | %
{[char]$_})) )
```

## 直接変更モードのユースケース

以下は、直接変更モードのユースケースです。

によるリソースのプロビジョニングと管理 CloudFormation

- 既存の CloudFormation ベースのツールとプロセスを統合します。

継続的なリソース管理と更新

- リスクの低い小さなアトミック変更。
- 手動または自動 RFC を通じて実行される変更。
- ネイティブ AWS API アクセスを必要とするツール。
- DCM ロールは、移行段階にある場合に使用できます。移行チームは、DCM のアクセス許可を活用してスタックを作成または変更します。
- DCM ロールは、CI/CD パイプラインで新しい AMIs の構築、Amazon ECS タスクの作成などに使用できます。

## AMS Advanced Developer モード

トピック

- [AMS Advanced Developer モードの開始方法](#)
- [デベロッパーモードでのセキュリティとコンプライアンス](#)
- [デベロッパーモードでの変更管理](#)
- [AMS Developer モードでのインフラストラクチャのプロビジョニング](#)
- [AMS デベロッパーモードでの検出コントロール](#)

- [AMS Developer モードでのログ記録、モニタリング、イベント管理](#)
- [AMS デベロッパーモードでのインシデント管理](#)
- [AMS デベロッパーモードでのパッチ管理](#)
- [AMS デベロッパーモードでの継続管理](#)
- [AMS Developer モードでのセキュリティとアクセスの管理](#)

AWS Managed Services (AMS) デベロッパーモードでは、AMS Advanced Plus および Premium アカウントの昇格されたアクセス許可を使用して、AMS Advanced 変更管理プロセス外の AWS リソースをプロビジョニングおよび更新します。AMS Advanced Developer モードは、AMS Advanced Virtual Private Cloud (VPC) 内のネイティブ AWS API コールを活用して、マネージド環境でインフラストラクチャとアプリケーションを設計および実装できるようにします。

デベロッパーモードが有効になっているアカウントを使用する場合、AMS Advanced 変更管理プロセスまたは AMS Amazon マシンイメージ (AMI) を使用してプロビジョニングされたリソースには、継続性管理、パッチ管理、変更管理が提供されます。ただし、これらの AMS 管理機能は、ネイティブ AWS APIs を介してプロビジョニングされたリソースには提供されません。

AMS Advanced 変更管理プロセス外でプロビジョニングされるインフラストラクチャリソースをモニタリングする責任があります。デベロッパーモードは、本番ワークロードと非本番ワークロードの両方と互換性があります。アクセス許可が引き上げられると、内部管理を確実に順守する責任が増大します。

#### Important

デベロッパーモードを使用して作成したリソースは、AMS Advanced 変更管理プロセスを使用して作成された場合にのみ、AMS Advanced によって管理できます。

デベロッパーモードは、使用できる AMS Advanced モードの 1 つです。詳細については、「[モードの概要](#)」を参照してください。

## AMS Advanced Developer モードの開始方法

AMS Advanced Developer モードを使用したさまざまな AMS Advanced アカウントと、Developer モードを正常に実装する方法について説明します。

### トピック



- [AMS デベロッパーモードを開始する前に](#)
- [AMS デベロッパーモードの前提条件](#)
- [AMS Advanced Developer モードを実装する方法](#)
- [AMS Advanced Developer モードのアクセス許可](#)

## AMS デベロッパーモードを開始する前に

デベロッパーモードを実装する前に、知っておくべきことがいくつかあります。

AMS Advanced は、変更リクエスト (RFCs) を通じて AMS Advanced 変更管理プロセス外で作成された DevMode アカountの既存のスタックまたはリソースを管理することはできません。ただし、アカウントが DevMode にある間、AMS Advanced は AMS Advanced 変更管理プロセスを通じてプロビジョニングされたリソースを RFCs。

DevMode アカountから始めて、後で AMS Advanced が管理するアプリケーションアカountに隠すことはできません。

## AMS デベロッパーモードの前提条件

デベロッパーモードを実装するための前提条件は次のとおりです。

- 少なくとも 1 つのオンボードされた AMS Advanced Plus または Premium アカountを持つ AMS Advanced のお客様である必要があります。
- 使用するアカウントは、AMS Advanced Plus または Premium アカountである必要があります。
- マルチアカウントランディングゾーン (MALZ): AWSManagedServicesDevelopmentRole事前定義された AWS Identity and Access Management (IAM) ロールを使用する必要があります。このロールをリクエストします。次のセクションでは、デベロッパーモードのアクセス許可を取得する方法について説明します。
- 単一アカウントランディングゾーン (SALZ): customer\_developer\_role事前定義された AWS Identity and Access Management (IAM) ロールを使用する必要があります。このロールをリクエストします。次のセクションでは、デベロッパーモードのアクセス許可を取得する方法について説明します。

## AMS Advanced Developer モードを実装する方法

デベロッパーモードを実装するには、対象の AMS Advanced アカountを事前定義された IAM ロールでプロビジョニングするようにリクエストします。

- MALZ: AWSManagedServicesDevelopmentRole
- SALZ: customer\_developer\_role

次に、フェデレーティッドネットワーク内の関連するユーザーにロールを割り当てます。

デベロッパーモードを使用すると、AMS Advanced マネージドリソースの AMS Advanced 変更管理と、カスタマーが管理するリソースのカスタマーマネージドロールフェデレーションの 2 つの変更ベクトルが作成されるため、AMS Advanced では、デベロッパーモードの使用が内部コントロールフレームワークと標準に準拠していることを確認することをお勧めします。AMS Advanced プロセスは宣言に準拠していますが、顧客プロセスとコントロールフレームワークを更新する必要がある場合があります。

AMS Advanced アカウントにデベロッパーモードを実装するには

1. デベロッパーモードで使用するアカウントが、「」に記載されている要件を満たしていることを確認します[AMS デベロッパーモードの前提条件](#)。
2. 変更タイプ (CT) 管理 | マネージドアカウント | デベロッパーモード | 有効化 (マネージドオートメーション) を使用して、変更リクエスト (RFC) を送信します。この CT の使用方法の例については、「[デベロッパーモード | 有効 \(マネージドオートメーション\)](#)」を参照してください。

CT が処理されると、事前定義された IAM ロール

(AWSManagedServicesDevelopmentRoleMALZ の場合は、SALZ

customer\_developer\_roleの場合は) がリクエストされたアカウントにプロビジョニングされます。

3. 内部フェデレーションプロセスを使用して、開発者モードアクセスを必要とするユーザーに適切なロールを割り当てます。

AMS Advanced では、リソースの望ましくないまたは未承認のプロビジョニングや変更を防ぐためにアクセスを制限することをお勧めします。

## AMS Advanced Developer モードのアクセス許可

事前定義されたロール (AWSManagedServicesDevelopmentRoleMALZ の場合は MALZ、SALZ customer\_developer\_roleの場合は) は、AMS Advanced によって運用されている共有サービスコンポーネント (管理ホスト、ドメインコントローラー、Trend Micro EPS、踏み台、サポートされていない AWS サービスなど) へのアクセスを制限しながら、IAM ロールを含む AMS Advanced VPC 内にアプリケーションインフラストラクチャリソースを作成するアクセス許可を付与しま

す。このロールは、AWS のサービス Amazon GuardDuty、AWS Organizations、AWS Directory Service APIs、AMS Advanced ログへのアクセスも制限します。

ロールでは追加の IAM ロールを作成できますが、デベロッパーモードアクセスに含まれるのと同じアクセス許可の境界は、によって作成されたすべての IAM ロールに適用されます `AWSManagedServicesDevelopmentRole`。

## デベロッパーモードでのセキュリティとコンプライアンス

セキュリティとコンプライアンスは、AMS Advanced とお客様との間の責任共有です。AMS アドバンスドデベロッパーモードは、変更管理プロセス外でプロビジョニングされたリソース、または変更管理を通じてプロビジョニングされたリソースに対して、デベロッパーモードのアクセス許可で更新されたリソースに対する責任共有を移行します。責任共有の詳細については、[AWS Managed Services](#)」を参照してください。

注意：

- DevMode を使用すると、ユーザーと承認されたチームは、AMS セキュリティの中核となる deny-by-default の原則を回避できます。利点、セルフサービス、AMS の待機時間の短縮は欠点と照らし合わせて検討する必要があります。セキュリティチームの知識がなくても、誰でも予期しない破壊的なアクションを実行できます。開発モードと直接変更モードを有効にする自動変更タイプが公開され、組織内の承認されたユーザーがこれらの CTs を実行してこれらのモードを有効にすることができます。
- ユーザーベースからの CT 実行のアクセス許可を管理する責任があります。
- AMS は CT 実行アクセス許可を管理しません

推奨事項:

- 保護
  - お客様は、アクセス許可によってこの CT へのアクセスを防ぐことができます。 [「IAM ロールポリシーステートメントによるアクセス許可の制限」](#)を参照してください。
  - ITSM システムなどのプロキシを実装してこの CT へのアクセスを防止する
  - 必要に応じてポリシーと動作を防止するサービスコントロールポリシー (SCPs) [「AMS Preventative and Detective Controls Library」](#)を参照してください。
- 検出
  - これらの CTs の RFC をモニタリングし (開発者モード `ct-1opjmhuddw194` と直接変更モードを有効にする、`ct-3rd4781c2nnhp` を有効にする)、それに応じて応答します。

- アカウントで IAM リソースの有無を確認および/または監査して、デベロッパーモードまたは直接変更モードがデプロイされているアカウントを特定します。
- 応答
  - 必要に応じてデベロッパーモードでアカウントを削除する

## デベロッパーモードのセキュリティ

AMS Advanced は、規範的なランディングゾーン、変更管理システム、アクセス管理で追加の値を提供します。デベロッパーモードを使用する場合、AMS Advanced のセキュリティ値は、ベースライン AMS Advanced セキュリティ強化ネットワークを確立する標準 AMS Advanced アカウントと同じアカウント設定を使用して保持されます。ネットワークは、ロール (AWSManagedServicesDevelopmentRoleMALZ の場合は MALZ、SALZ customer\_developer\_roleの場合は ) で強制されるアクセス許可の境界によって保護されます。これにより、ユーザーは、アカウントの設定時に確立されたパラメータ保護を破ることが制限されます。

たとえば、ロールを持つユーザーは Amazon Route 53 にアクセスできますが、AMS Advanced の内部ホストゾーンは制限されています。によって作成された IAM ロールにも同じアクセス許可の境界が適用されAWSManagedServicesDevelopmentRole、アカウントAWSManagedServicesDevelopmentRoleが AMS Advanced にオンボーディングされたときに確立されたパラメータ保護をユーザーが壊すことを制限するアクセス許可の境界が に強制されます。

## デベロッパーモードでのコンプライアンス

デベロッパーモードは、本番ワークロードと非本番ワークロードの両方と互換性があります。コンプライアンス標準 (PHI、HIPAA、PCI など) を確実に順守し、デベロッパーモードの使用が内部管理フレームワークと標準に準拠していることを確認するのはお客様の責任です。

## デベロッパーモードでの変更管理

変更管理は、AMS Advanced サービスが変更リクエストを実装するために使用するプロセスです。変更リクエスト (RFC) は、AMS Advanced インターフェイスを介してユーザーまたは AMS Advanced によって作成され、マネージド環境に変更を加えるリクエストであり、特定のオペレーションの変更タイプ (CT) ID が含まれます。詳細については、「[変更管理モード](#)」を参照してください。

開発者モードのアクセス許可が付与されている AMS Advanced アカウントでは、変更管理は適用されません。IAM ロール (AWSManagedServicesDevelopmentRoleMALZ の場合は、SALZ customer\_developer\_roleの場合は) でデベロッパーモードのアクセス許可を付与されたユーザーは、ネイティブ AWS API アクセスを使用して、AMS Advanced アカウントのリソースをプロビジョニングおよび変更できます。これらのアカウントで適切なロールを持たないユーザーは、AMS Advanced 変更管理プロセスを使用して変更を行う必要があります。

#### Important

デベロッパーモードを使用して作成したリソースは、AMS Advanced 変更管理プロセスを使用して作成された場合にのみ、AMS Advanced によって管理できます。AMS Advanced 変更管理プロセス外で作成されたリソースについて AMS Advanced に送信された変更のリクエストは、ユーザーが処理する必要があるため、AMS Advanced によって拒否されます。

## セルフサービスプロビジョニングサービス API の制限

すべての AMS Advanced セルフプロビジョニングサービスは、デベロッパーモードでサポートされています。セルフプロビジョニングサービスへのアクセスには、それぞれのユーザーガイドセクションで説明されている制限が適用されます。デベロッパーモードロールでセルフプロビジョニングサービスを使用できない場合は、デベロッパーモードの変更タイプを使用して更新されたロールをリクエストできます。

以下のサービスは、サービス APIs へのフルアクセスを提供しません。

デベロッパーモードで制限されるセルフプロビジョニングサービス

| サービス                     | 注意                                                            |
|--------------------------|---------------------------------------------------------------|
| Amazon API Gateway       | を除くすべての Gateway APIs コールが許可されますSetWebACL。                     |
| Application Auto Scaling | スケーラブルターゲットの登録または登録解除、スケーリングポリシーの配置または削除のみが可能です。              |
| AWS CloudFormation       | というプレフィックスが付いた名前の CloudFormation スタックにアクセスまたは変更することはできませんmc-。 |

| サービス                      | 注意                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AWS CloudTrail            | ams- および/または というプレフィックスが付いた名前の CloudTrail リソースにアクセスまたは変更することはできませんmc-。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Amazon Cognito (ユーザープール ) | <p>ソフトウェアトークンを関連付けることはできません。</p> <p>ユーザープール、ユーザーインポートジョブ、リソースサーバー、または ID プロバイダーを作成することはできません。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| AWS Directory Service     | <p>Connect および WorkSpaces サービスでは、次の Directory Service アクションのみが必要です。他のすべての Directory Service アクションは、デベロッパーモードのアクセス許可境界ポリシーによって拒否されます。</p> <ul style="list-style-type: none"><li>• ds:AuthorizeApplication</li><li>• ds:CreateAlias</li><li>• ds&gt;CreateIdentityPoolDirectory</li><li>• ds&gt;DeleteDirectory</li><li>• ds:DescribeDirectories</li><li>• ds:GetAuthorizedApplicationDetails</li><li>• ds:ListAuthorizedApplications</li><li>• ds:UnauthorizeApplication</li></ul> <p>シングルアカウントランディングゾーンアカウントでは、境界ポリシーは、開発モードが有効なアカウントへのアクセスを維持するために AMS Advanced が使用する AMS Advanced マネージドディレクトリへのアクセスを明示的に拒否します。</p> |

| サービス                         | 注意                                                                                                                                                                                       |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Amazon Elastic Compute Cloud | <p>、DhcpOptions、Gateway、Subnet、VPCおよび の文字列を含む Amazon EC2 APIs にはアクセスできませんVPN。</p> <p>、AMS、ManagementHostASG および/または のプレフィックスが付いたタグを持つ Amazon EC2 mcリソースにアクセスまたは変更することはできませんsentinel。</p> |
| Amazon EC2 (レポート )           | <p>ビューアクセスのみが付与されます (変更できません )。注: Amazon EC2 レポートは移動中です。レポートメニュー項目は Amazon EC2 コンソールのナビゲーションメニューから削除されます。削除された Amazon EC2 使用状況レポートを表示するには、AWS Billing およびコスト管理コンソールを使用します。</p>           |

| サービス                                     | 注意                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AWS Identity and Access Management (IAM) | <p>既存のアクセス許可の境界を削除したり、IAM ユーザーパスワードポリシーを変更したりすることはできません。</p> <p>正しい IAM ロール (AWSManagedServicesDevelopmentRole MALZ の場合は、SALZ customer_developer_role の場合は) を使用しない限り、IAM リソースを作成または変更することはできません。</p> <p>プレフィックスが ams、customer_deny_policy、および/または の IAM mc リソースを変更することはできません sentinel。</p> <p>新しい IAM リソース (ロール、ユーザー、またはグループ) を作成するときは、アクセス許可の境界 (MALZ: AWSManagedServicesDevelopmentRolePermissionsBoundary、SALZ: ams-app-infra-permissions-boundary) をアタッチする必要があります。</p> |
| AWS Key Management Service (AWS KMS)     | AMS Advanced マネージド KMS キーにアクセスまたは変更することはできません。                                                                                                                                                                                                                                                                                                                                                                                                                             |
| AWS Lambda                               | プレフィックスが の AWS Lambda 関数にアクセスまたは変更することはできません AMS。                                                                                                                                                                                                                                                                                                                                                                                                                          |
| CloudWatch Logs                          | 、mc、lambda および/または というプレフィックスが付いた名前の CloudWatch aws ログストリームにはアクセスできません AMS。                                                                                                                                                                                                                                                                                                                                                                                                |



| サービス                                            | 注意                                                                                                                                             |
|-------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Amazon Relational Database Service (Amazon RDS) | というプレフィックスが付いた名前の Amazon Relational Database Service (Amazon RDS) データベース (DBs) にアクセスまたは変更することはできません。mc-                                        |
| AWS Resource Groups                             | Get、Listおよび Searchリソースグループ API アクションにのみアクセスできます。                                                                                               |
| Amazon Route 53                                 | Route53 AMS Advanced が管理するリソースにアクセスまたは変更することはできません。                                                                                            |
| Amazon S3                                       | 、ams-*、ms-aまたは というプレフィックスが付いた名前の Amazon S3 amsバケットにはアクセスできませんmc-a。                                                                             |
| AWS Security Token Service                      | 許可されるセキュリティトークンサービス API は のみですDecodeAuthorizationMessage 。                                                                                     |
| Amazon SNS                                      | 、AMS-、Energon-Topic または というプレフィックスが付いた名前の SNS トピックにはアクセスできませんMMS-Topic 。                                                                       |
| AWS Systems Manager マネージャー (SSM)                | ams、mcまたは のプレフィックスが付いた SSM パラメータを変更することはできません SVC。<br><br>ams または のプレフィックスが付いたタグを持つ Amazon EC2 インスタンスSendCommand に対して SSM API を使用することはできませんmc。 |
| AWS タグ付け                                        | プレフィックスが の AWS タグ付け API アクションにのみアクセスできますGet。                                                                                                   |

| サービス                           | 注意                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AWS Lake Formation             | <p>次の AWS Lake Formation API アクションは拒否されます。</p> <ul style="list-style-type: none"> <li>lakeformation:DescribeResource</li> <li>lakeformation:GetDataLakeSettings</li> <li>lakeformation:DeregisterResource</li> <li>lakeformation:RegisterResource</li> <li>lakeformation:UpdateResource</li> <li>lakeformation:PutDataLakeSettings</li> </ul> |
| Amazon Elastic Inference       | <p>Elastic Inference API アクション のみを呼び出すことができますelastic-inference:Connect 。このアクセス許可は、 にアタッチcustomer_sagemaker_admin_policy されている に含まれていますcustomer_sagemaker_admin_role 。このアクションにより、Elastic Inference アクセラレーターにアクセスできます。</p>                                                                                                                      |
| AWS Shield                     | <p>このサービスの APIs またはコンソールにはアクセスできません。</p>                                                                                                                                                                                                                                                                                                      |
| Amazon Simple Workflow Service | <p>このサービスの APIs またはコンソールにはアクセスできません。</p>                                                                                                                                                                                                                                                                                                      |

## AMS Developer モードでのインフラストラクチャのプロビジョニング

デベロッパーモードが有効になっているアカウントAWSManagedServicesDevelopmentRoleで、デベロッパーモード IAM ロール を持たないユーザーは、AMS Advanced AMIs を活用する AMS Advanced 変更管理プロセスに従う必要があります。正しいロール (MALZ: AWSManagedServicesDevelopmentRole、SALZ: customer\_developer\_role) を持つユー

ザーは、AMS Advanced 変更管理システムと AMS Advanced AMIs を使用できますが、必須ではありません。

 Note

AMS Advanced ワークロードの取り込みによって処理されていない、または AMS Advanced アカウントで作成された AWS AMI には、AMS Advanced に必要な設定は含まれません。

## AMS デベロッパーモードでの検出コントロール

このセクションは、機密性の高い AMS セキュリティ関連情報が含まれているため、編集されています。この情報は、AMS コンソールのドキュメントから入手できます。AWS Artifact にアクセスするには、CSDM に連絡して手順を確認するか、[「AWS Artifact の開始方法」](#)を参照してください。

## AMS Developer モードでのログ記録、モニタリング、イベント管理

ログ記録、モニタリング、イベント管理は、AMS Advanced 変更管理プロセス外でプロビジョニングされたリソースや、変更管理を通じてプロビジョニングされ、デベロッパーモードのアクセス許可を使用してアカウントによって変更されたリソースでは使用できません。

## AMS デベロッパーモードでのインシデント管理

インシデント対応時間に変更はありません。インシデント解決は、変更管理プロセス外でプロビジョニングされたリソース、または変更管理を通じてプロビジョニングされ、デベロッパーモードのアクセス許可を使用してアカウントによって変更されたリソースのベストエフォートです。

 Note

AMS サービスレベルアグリーメント (SLA) は、AMS 変更管理システムの外部で作成または更新されたリソース (変更または RFCs のリクエスト) には適用されません。デベロッパーモードが含まれるため、デベロッパーモードで更新または作成されたリソースは自動的に P3 に低下し、AMS サポートがベストエフォートです。

## AMS デベロッパーモードでのパッチ管理

パッチ管理は、AMS Advanced 変更管理プロセス外でプロビジョニングされたリソース、または変更管理を通じてプロビジョニングされ、デベロッパーモードのアクセス許可を使用してアカウントによって変更されたリソースでは使用できません。パッチ適用時間：

- 重要なセキュリティ更新の場合: ベンダーによるリリースから 10 営業日以内に、変更管理によってプロビジョニングされ、デベロッパーモードのアクセス許可を使用してアカウントによって変更されたリソース。
- 重要な更新の場合: ベンダーによるリリースから 2 か月以内に、変更管理によってプロビジョニングされ、デベロッパーモードのアクセス許可を使用してアカウントによって変更されたリソース。

## AMS デベロッパーモードでの継続管理

継続性管理は、AMS Advanced 変更管理プロセス外でプロビジョニングされたリソース、または変更管理を通じてプロビジョニングされ、デベロッパーモードのアクセス許可を使用してアカウントによって変更されたリソースでは使用できません。

環境復旧の開始時間は、AMS Advanced 変更管理プロセス外でプロビジョニングされたリソース、または変更管理を通じてプロビジョニングされ、デベロッパーモードのアクセス許可を使用してアカウントによって変更されたリソースの場合、最大 12 時間かかることがあります。

## AMS Developer モードでのセキュリティとアクセスの管理

マルウェア対策保護は、AMS Advanced 変更管理プロセス外でプロビジョニングされたリソース、または変更管理を通じてプロビジョニングされ、デベロッパーモードのアクセス許可を使用してアカウントによって変更されたリソースについて、お客様の責任となります。AMS Advanced 変更管理によってプロビジョニングされていない Amazon Elastic Compute Cloud (Amazon EC2) インスタンスへのアクセスは、フェデレーティッドアクセスを提供する代わりに、キーペアによって制御される場合があります。

## AMS でのセルフサービスプロビジョニングモード

AWS Managed Services (AMS) セルフサービスプロビジョニング (SSP) モードは、AMS マネージドアカウントのネイティブ AWS サービスと API 機能へのフルアクセスを提供します。標準化、スコープダウン、AWS Identity and Access Management ロールを通じてサービスにアクセスします。AMS はサービスリクエストとインシデント管理を提供します。アラート、モニタリング、ログ

記録、パッチ適用、バックアップ、変更管理はお客様の責任となります。多くの場合、セルフサービスプロビジョニングサービス (SSPS) はセルフマネージド型またはサーバーレスであり、パッチ適用などの特定の運用タスクを管理する必要はありません。AMS ガードレールで定義された環境境界内でこれらのサービスを使用すると、プラットフォームのベースラインセキュリティを維持するために、IAM の変更 (サービスにリンクされたロール、サービスロール、クロスアカウントロール、ポリシーの更新を含む) を AMS オペレーションで承認する必要があります。テンプレートを活用して CloudFormation これらのサービスのデプロイを自動化できますが、これはすべての SSP サービスでサポートされているわけではありません。

#### Important

AWS Managed Services (AMS) アカウントで SSP モードを使用して、サービスにアクセスして採用します。ただし AWS、記載されている制限があります。

AMS アカウントには、AMS 管理なしで AWS のサービス 使用できるものもあります。セルフサービスプロビジョニングモードサービス、つまり略して SSPS を AMS アカウントに追加する方法とそれぞれのよくある質問FAQs「」セクションで説明します。

セルフサービスプロビジョニングサービスはそのまま提供され、管理するのはお客様の責任です。AMS は、これらのサービスに関連付けられたリソースに対してアラート、モニタリング、ログ記録、またはパッチ適用を行いません。AMS には、AMS アカウントでサービスを安全に使用できる IAM ロールが用意されています。AMS SLAs は適用されません。

セルフサービスでプロビジョニングするリソースの場合、AMS は、インシデント管理、検出コントロールとガードレール、レポート、指定リソース (Cloud Service Delivery Manager と Cloud Architect)、セキュリティとアクセス、サービスリクエストによるテクニカルサポートを提供します。さらに、該当する場合、AMS 変更管理システムの外部でプロビジョニングまたは設定されたリソースの継続管理、パッチ管理、インフラストラクチャモニタリング、変更管理に責任を負います。

## AMS での SSP モードの開始方法

セルフサービスプロビジョニングは、マルチアカウントランディングゾーン (MALZ) に使用できる AMS モードの 1 つです。詳細については、「[モードの概要](#)」を参照してください。

セルフサービスプロビジョニング機能を提供するために、AMS は、直接 AWS のサービス アクセスからの意図しない変更を制限するためのアクセス許可の境界を持つ昇格された IAM ロールを作成しました。ロールによってすべての変更が妨げられるわけではなく、内部コントロールとコンプライアンスポリシーに準拠し、使用されているすべての AWS のサービス が必須の証明書を満たしている

ことを確認する必要があります。これはセルフサービスプロビジョニングモードです。AWS コンプライアンス要件の詳細については、[AWS「コンプライアンス」](#)を参照してください。

マルチアカウントランディングゾーンアプリケーションアカウントにセルフサービスプロビジョニングサービスを追加するには、サービスの指示に従って、Management | AWS service | Self-provisioned service | Add change type (CT) を使用します。

#### Note

AMS に追加のセルフサービスプロビジョニングサービスを提供するようにリクエストするには、サービスリクエストを提出します。

## AMS SSP を使用して AMS アカウントに Amazon API Gateway をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon API Gateway 機能に直接アクセスします。[Amazon API Gateway](#) は、デベロッパーがあらゆる規模で API の公開、保守、モニタリング、セキュリティ保護を簡単に行えるフルマネージドサービスです。を使用すると AWS マネジメントコンソール、アプリケーションが Amazon Elastic Compute Cloud (Amazon [Amazon EC2](#)) で実行されているワークロード、で実行されているコード、ウェブアプリケーション、リアルタイム通信アプリケーションなど、バックエンドサービスからデータ、ビジネスロジック、機能にアクセスするためのフロントドアとして機能する [AWS Lambda](#) REST および WebSocket APIs を作成できます。

API Gateway は、トラフィック管理、認可とアクセスコントロール、モニタリング、API バージョン管理など、最大数十万の同時 API コールの受け入れと処理に関連するすべてのタスクを処理します。API Gateway には最低料金やスタートアップコストはありません。支払いは、受信した API コールと転送されたデータ量に対してのみ発生し、API Gateway 階層型料金モデルを使用すると、API 使用量が拡大するにつれてコストを削減できます。詳細については、[Amazon API Gateway](#)」を参照してください。

### よくある質問: AMS の API Gateway

Q: AMS アカウントの Amazon API Gateway へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) change type で RFC を送信して API Gateway へのアクセスをリクエストします。この RFC は、

customer\_apigateway\_author\_role および の IAM ロールをアカウントにプロビジョニングします customer\_apigateway\_cloudwatch\_role。アカウントでプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon API Gateway の使用にはどのような制限がありますか？

- API Gateway の設定は、AMS インフラストラクチャへの変更を防ぐために、MC-AMS-またはプレフィックスのないリソースに制限されます。
- CREATE Elastic Load Balancer の規制されていない作成を防ぐために、VPCLink の 権限は無効になっています。VPCLinks [Application Load Balancer | Create](#)」を参照してください。

Q: AMS アカウントで Amazon API Gateway を使用するための前提条件または依存関係は何ですか？

デプロイする API Gateway のタイプによって異なります。スタンドアロンサービスでもかまいませんが、既存のサービス (Network Load Balancer など) へのアクセスをリクエストすることもできます。

## AMS SSP を使用して AMS アカウントで Alexa for Business をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Alexa for Business 機能に直接アクセスします。Alexa for Business は、組織と従業員が Alexa を使用してより多くの作業を完了できるようにするサービスです。Alexa for Business を使用すると、Alexa をインテリジェントアシスタントとして使用して、会議室、デスク、自宅や外出先で既に使用している Alexa デバイスでも生産性を高めることができます。IT および施設マネージャーは、Alexa for Business を使用して、職場の既存の会議室の使用率を測定し、向上させることができます。

詳細については、[Alexa for Business](#)」を参照してください。

## AWS Managed Servicesでの Alexa for Business に関するよくある質問

Q: AMS アカウントで Alexa for Business へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (マネージドオートメーション) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします:



customer\_alex\_console\_role。customer\_alex\_device\_setup\_user は、Alexa for Business が提供する Device Setup Tool にも作成されます。その後、この Device Setup Tool を使用してデバイスをセットアップできます。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Alexa for Business ゲートウェイを使用すると、Alexa for Business を Cisco Webex エンドポイントと Poly Group Series エンドポイントに接続して、音声で会議を制御できます。ゲートウェイソフトウェアは、オンプレミスのハードウェアで実行され、Alexa for Business から Cisco エンドポイントへの会議ディレクティブを安全にプロキシします。ゲートウェイは、Alexa for Business と通信するために 2 組の AWS 認証情報を必要とします。アクセスが制限され customer\_alex\_gateway\_execution\_user した IAM ユーザーを 2 人用意しています。customer\_alex\_gateway\_installer\_user1 つは Alexa for Business ゲートウェイのインストール用、もう 1 つはゲートウェイの運用用です。これらは、デプロイ | 高度なスタックコンポーネント | Identity and Access Management (IAM) | Create entity or policy (managed automation) change type (ct-3dpg8mdd9jn1r) を使用して RFC を送信することでリクエストできます。

#### Note

使用状況レポートを生成して Amazon S3 に送信するには、セルフプロビジョニングサービス RFC で Amazon S3 バケット名を指定します。

Q: AMS アカウントで Alexa for Business を使用するにはどのような制限がありますか？

制限はありません。Alexa for Business の全機能は、Alexa for Business の自己プロビジョニング型サービスロールで使用できます。

Q: AMS アカウントで Alexa for Business を使用する際の前提条件または依存関係は何ですか？

- WPA2 Enterprise Wi-Fi を使用して共有デバイスをセットアップする場合は、AWS Private Certificate Authority が必要な Device Setup Tool でこのネットワークセキュリティタイプを指定します。
- AMS は、名前空間「A4B」で始まるシークレットキーのみを作成します。これは、この名前空間にのみ制限されます。

Q: Alexa for Business のどの機能に個別の RFCsが必要ですか？

Alexa Voice Service (AVS) デバイスを Alexa for Business に登録するには、Alexa 組み込みデバイスメーカーへのアクセスを提供します。これを行うには、管理 | その他 | その他の変更タイプを使用し



でデプロイできる IAM ロールを Alexa for Business コンソールで作成する必要があります。これにより、AVS デバイスメーカーはユーザーに代わって Alexa for Business にデバイスを登録および管理できます。

## AMS SSP を使用して AMS アカウントで Amazon WorkSpaces アプリケーションをプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon WorkSpaces アプリケーション (WorkSpaces アプリケーション) 機能に直接アクセスします。WorkSpaces アプリケーションを使用すると、デスクトップアプリケーションを書き換えることなく AWS に移動できます。WorkSpaces アプリケーションにアプリケーションをインストールしたり、起動設定を設定したり、ユーザーがアプリケーションを使用できるようにしたりできます。WorkSpaces Applications には、さまざまな仮想マシンオプションが用意されているため、アプリケーションの要件に最適なインスタンスタイプを選択し、エンドユーザーのニーズに合わせて簡単に自動スケーリングパラメータを設定できます。WorkSpaces アプリケーションを使用すると、独自のネットワークでアプリケーションを起動できます。つまり、アプリケーションは既存の AWS リソースとやり取りできます。

Amazon WorkSpaces アプリケーションを使用すると、Image Builder を使用してアプリケーションをすばやく簡単にインストール、テスト、更新できます。Microsoft Windows Server 2012 R2、Windows Server 2016、または Windows Server 2019 で実行されるアプリケーションはサポートされており、変更を加える必要はありません。テストが完了したら、アプリケーションの起動設定、デフォルトのユーザー設定を設定し、ユーザーがアクセスできるようにイメージを公開できます。

詳細については、[WorkSpaces アプリケーション](#)」を参照してください。

### AWS Managed Services での WorkSpaces アプリケーションに関するよくある質問

Q: AMS アカウントの WorkSpaces アプリケーションへのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (ct-3qe6io8t6jtny) 変更タイプで RFC を送信して、WorkSpaces アプリケーションへのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_appstream_console_role`。

`customer_appstream_stream_role` は、Active Directory ログイン認証情報を使用してユーザーを認証する必要があるアプリケーションをストリーミングするためにもデプロイされます。

アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの WorkSpaces アプリケーションの使用にはどのような制限がありますか？

- 以下の機能は AMS サポートチームが設定する必要があり、特定の RFCs が必要です。追加機能のリクエスト手順については、セクション 4 を参照してください。
- インターフェイス VPC エンドポイントからの作成とストリーミング。
- プライベートネットワークでのホームフォルダとアプリケーション設定の永続化のための Amazon S3 エンドポイントのサポート。
- すべてのフリートストリーミングインスタンスで利用できる IAM ロールを作成して選択します。
- WorkSpaces アプリケーションフリートと Image Builder の Microsoft Active Directory ドメインへの参加。
- WorkSpaces アプリケーションカスタム使用状況レポートの作成。
- カスタムブランドは現在サポートされていません。

Q: AMS アカウントで WorkSpaces アプリケーションを使用するための前提条件または依存関係は何ですか？

WorkSpaces アプリケーションのオンボードに RFC を送信するときは、WorkSpaces アプリケーションの使用状況レポートに使用する Amazon S3 バケット名を含めます。バケット名は、WorkSpaces アプリケーションのオンボーディング時に `customer-appstream-usagereports-policy` 作成される に追加されます。

Q: 個別の RFC を必要とする WorkSpaces アプリケーション機能は何ですか？ RFCs

- WorkSpaces アプリケーションのインターフェイス VPC エンドポイントを選択するには、管理 | その他 | その他 | 変更タイプ RFC を更新して、アカウントに VPC エンドポイントを作成します。WorkSpaces アプリケーションのカスタムエンドポイントを作成する手順については、[「WorkSpaces アプリケーションユーザーガイド」の「インターフェイス VPC エンドポイントからの作成とストリーミング」](#)を参照してください。WorkSpaces
- ホームフォルダの Amazon S3 エンドポイントとプライベートネットワークでのアプリケーション設定の永続性のサポートは、管理 | その他 | その他 | 変更タイプ RFC の作成で Amazon S3 VPC エンドポイントをリクエストすることで設定できます。RFC には、ホームフォルダのコンテンツをホストするターゲット Amazon S3 バケット、またはアプリケーション設定 Amazon S3 バケットをそれぞれ含める必要があります。この RFC は、Amazon S3 VPC エンドポイントにアクセス

するために必要なアクセス許可を WorkSpaces アプリケーションに提供します。ストリームのカスタムエンドポイントを作成する手順については、WorkSpaces アプリケーションユーザーガイドの「[ホームフォルダの Amazon S3 VPC エンドポイントの使用](#)」と「[アプリケーション設定の永続化](#)」を参照してください。WorkSpaces

- すべてのフリートストリーミングインスタンスで利用できる IAM ロールを作成して選択するには、デプロイ | 高度なスタックコンポーネント | Identity and Access Management (IAM) | エンティティまたはポリシー (マネージドオートメーション) 変更タイプ (ct-3dpd8mdd9jn1r) RFC を作成して、必要なポリシーで IAM ロールをリクエストします。IAM ロール名は常にプレフィックス「customer\_appstream」で始まる必要があります。
- Amazon WorkSpaces アプリケーションフリートと Image Builder は、Active Directory (AD) でサービスアカウントを作成するための管理 | その他 | その他 | 更新変更タイプ RFC を送信することで、Microsoft Active Directory のドメインに参加できます。Microsoft Active Directory に参加するために必要な最小限のアクセス許可は、「Active Directory コンピュータオブジェクトを作成および管理するためのアクセス許可の付与」の WorkSpaces [アプリケーションドキュメントで定義されています](#)。
- カスタム WorkSpaces アプリケーション使用状況レポートを作成するには、管理 | その他 | その他 | 以下をリクエストする変更タイプ RFC を作成します。
  - AppStreamUsageReports」CFN スタックの作成
  - アカウントで「customer\_appstream\_usagereports\_role」をプロビジョニングする
  - また、以下の詳細を指定します。
    - クローラの実行をスケジュールする CRON 式を指定します。デフォルトでは、毎日 23:00 UTC です。
    - Athena クエリ結果に使用される Amazon S3 バケット ARN。このバケットにはプレフィックスが必要です。aws-athena-query-results
    - WorkSpaces アプリケーション使用状況レポートログの Amazon S3 バケット ARN。

ロールがプロビジョニングされたら、フェデレーションソリューションとログインにロールをオンボードし、AWS GlueAWS Glue と Athena にアクセスして、使用状況レポートロールを使用してカスタムレポートを生成します。WorkSpaces アプリケーション使用状況レポートの使用の詳細については、[WorkSpaces アプリケーションドキュメントの「カスタムレポートの作成」](#)および「[WorkSpaces アプリケーション使用状況データの分析](#)」を参照してください。WorkSpaces

# AMS SSP を使用して AMS アカウントに Amazon Athena をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Athena (Athena) 機能に直接アクセスします。Athena は、標準 SQL を使用して Amazon S3 内のデータを分析するためのインタラクティブなクエリサービスです。Athena はサーバーレスであることから管理するインフラストラクチャがなく、実行したクエリの料金のみを支払います。Amazon S3 のデータにポイントし、スキーマを定義して、標準 SQL を使用してクエリを開始します。ほとんどの結果は数秒以内に配信されます。Athena を使用すると、複雑な extract-transform-load (ETL) ジョブでデータを分析用に準備する必要はありません。これにより、SQL スキルを持つすべてのユーザーが大規模なデータセットをすばやく分析できます。詳細については、[Amazon Athena](#)」を参照してください。

## よくある質問: AMS の Athena

Q: AMS アカウントの Amazon Athena へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) change type で RFC を送信して、Athena へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_athena_console_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon Athena の使用にはどのような制限がありますか？

制限はありません。Amazon Athena の完全な機能は、AMS アカウントで使用できます。

Q: AMS アカウントで Amazon Athena を使用するための前提条件または依存関係は何ですか？

Athena は、で作成されたデータカタログ/メタストアを使用するため、AWS Glue サービスに大きく依存します AWS Glue。したがって、AWS Glue アクセス許可は成功した Athena RFC に含まれます。

ロールには、Amazon S3 バケットの前提条件 `customer_athena_console_role` があります。新しいバケットを作成するには、自動 CT `ct-1a68ck03fn98r` (デプロイ | 高度なスタックコンポーネント | S3 ストレージ | 作成) を使用します。この自動 CT を使用して Athena の S3 バケットを作成する場合、バケット名はプレフィックス で始まる必要があります `athena-query-results-*`。

# AMS SSP を使用して AMS アカウントに Amazon Bedrock をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Bedrock 機能に直接アクセスします。Amazon Bedrock は、主要な AI スタートアップから高性能な基盤モデル (FMs) を提供し、統合された API AWS を通じて使用できるフルマネージドサービスです。さまざまな基盤モデルから選択して、ユースケースに最適なモデルを見つけることができます。Amazon Bedrock には、セキュリティ、プライバシー、責任のある AI を備えた生成 AI アプリケーションを構築するためのさまざまな機能も用意されています。Amazon Bedrock を使用すると、ユースケースに適した最善の基盤モデルを簡単に試して評価したり、ファインチューニングや検索拡張生成 (RAG) などの手法を使用して基盤モデルをデータでプライベートにカスタマイズしたり、エンタープライズシステムやデータソースを使用してタスクを実行するエージェントを構築したりできます。

Amazon Bedrock のサーバーレスエクスペリエンスを使用すると、インフラストラクチャを管理することなく、すばやく開始し、独自のデータを使用して基盤モデルをプライベートにカスタマイズし、AWS ツールを使用してアプリケーションに簡単かつ安全に統合してデプロイできます。詳細については、「[Amazon Bedrock とは](#)」を参照してください。

## よくある質問: AMS の Amazon Bedrock

Q: AMS アカウントの Amazon Bedrock へのアクセスをリクエストするにはどうすればよいですか？

Amazon Bedrock へのアクセスをリクエストするには、管理 | AWS サービス | セルフプロビジョニングサービス | (マネージドオートメーション) (ct-3qe6io8t6jtny) 変更タイプを使用して RFC を送信します。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_bedrock_console_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon Bedrock の使用にはどのような制限がありますか？

- Amazon Bedrock ナレッジベースは、現在 AMS でサポートされていない Amazon OpenSearch Service Serverless に依存しているため、SSPS ロールの一部としてデフォルトではサポートされていません。
- Bedrock Studio は、Amazon DataZone などのサポートされていないサービスに依存しているため、サポートされていません。

Q: AMS アカウントで Amazon Bedrock を使用するための前提条件または依存関係は何ですか？



- AWS Marketplace アクセス許可を必要とするサードパーティーモデルのサブスクリプションは、デフォルトのロール (AWSManagedServicesAdminRoleMALZ では、SALZ Customer\_ReadOnly\_Roleでは) で実行する必要があります。これは、デフォルトのロールに AWS Marketplace アクセス許可が含まれているためです。
- データ暗号化を使用する場合は、コンソールロールの作成をリクエストするときに AWS KMS キー ARN を指定する必要があります。また、使用する Amazon S3 バケットの名前に「bedrock」が含まれている必要があります。

## AMS SSP を使用して AMS アカウントで Amazon CloudSearch をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon CloudSearch 機能に直接アクセスします。Amazon CloudSearch は、ウェブサイトまたはアプリケーションの検索ソリューションのセットアップ、管理、スケーリングを費用対効果の高い方法で行うために使用する AWS クラウド内のマネージドサービスです。Amazon CloudSearch は、34 の言語と、強調表示、オートコンプリート、地理空間検索などの一般的な検索機能をサポートしています。詳細については、[Amazon CloudSearch](#)」を参照してください。

### Note

AWS は、2024 年 7 月 25 日に Amazon CloudSearch への新しい顧客アクセスを閉鎖しました。Amazon CloudSearch の既存のお客様は、引き続きこのサービスを通常どおり使用できます。AWS は引き続き Amazon CloudSearch のセキュリティ、可用性、パフォーマンスの向上に投資しますが、新機能を導入する予定はありません。

Amazon CloudSearch と Amazon OpenSearch Service の違いと OpenSearch Service への移行方法を理解するには、クラウドアーキテクト (CA) に連絡してガイダンスを受けてください。OpenSearch Service への移行の詳細については、[Amazon CloudSearch から Amazon OpenSearch Service サービスへの移行](#)」を参照してください。

## AWS Managed Servicesでの Amazon CloudSearch に関するよくある質問

Q: AMS アカウントの Amazon CloudSearch へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) change type  
で RFC を送信して、Amazon CloudSearch へのアクセスをリクエストします。この RFC は、

customer\_csearch\_admin\_role および の IAM ロールをアカウントにプロビジョニングし、customer\_csearch\_dev\_role。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon CloudSearch の使用にはどのような制限がありますか？

Amazon CloudSearch の全機能は、AMS アカウントで使用できます。AMS がサポートするすべてのデータベースソリューションは、現在 Amazon CloudSearch でサポートされています。現在、インデックスを作成できないマネージド AWS データベースソリューションは DynamoDB のみです。

Q: AMS アカウントで Amazon CloudSearch を使用するための前提条件または依存関係は何ですか？

Amazon CloudSearch は Amazon S3 が ID プロバイダーと連携して入力データを自動的に分析し、テーブルフィールドを決定します。Amazon S3 へのアクセスはこの RFC では提供されておらず、サービスリクエストで個別にリクエストする必要があります。

## AMS SSP を使用して AMS アカウントで Amazon CloudWatch Synthetics をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon CloudWatch Synthetics 機能に直接アクセスします。Amazon CloudWatch Synthetics を使用して「canaryAPIs をモニタリングできます。

Canary は、Node.js または Python で記述された設定可能なスクリプトで、スケジュールに従って実行されます。Node.js または Python をフレームワークとして使用する Lambda 関数をアカウント内に作成します。Canary は、HTTP プロトコルと HTTPS プロトコルの両方で動作します。Canary はエンドポイントの可用性とレイテンシーをチェックし、ロードタイムデータと UI スクリーンショットを保存できます。REST API、URL、ウェブサイトのコンテンツをモニターリングし、フィッシング、コードインジェクション、およびクロスサイトスクリプティングによる不正な変更をチェックできます。

Canary は顧客と同じルートに従って同じアクションを実行するため、アプリケーションに顧客トラフィックがない場合でもカスタマーエクスペリエンスを継続的に検証できます。Canary を使用すると、顧客が問題を検出する前に問題を検出できます。詳細については、[Amazon CloudWatch: 合成モニタリングの使用](#)を参照してください。

## AWS Managed Services の Amazon CloudWatch Synthetics に関するよくある質問

Q: AMS アカウントの Amazon CloudWatch Synthetics へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) 変更タイプで RFC を送信して、Amazon CloudWatch Synthetics へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: 'customer\_cw\_synthetics\_console\_role' および 'customer\_cw\_synthetics\_canary\_lambda\_role'。アカウントにプロビジョニングされたら、フェデレーションソリューションで「customer\_cw\_synthetics\_console\_role」ロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon CloudWatch Synthetics の使用にはどのような制限がありますか？

AMS アカウントでの Amazon CloudWatch Synthetics の使用に制限はありません。AMS が提供するサービスロールcustomer\_cw\_synthetics\_canary\_lambda\_role」以外の Canary のロールの作成は禁止されています。

Q: AMS アカウントで Amazon CloudWatch Synthetics を使用するための前提条件または依存関係は何ですか？

Canary は、デフォルトの Amazon CloudWatch Synthetics S3 バケットを作成および使用します。cw-syn-results-*-\${accountnumber}-\${default-region}*」

## AMS SSP を使用して AMS アカウントに Amazon Cognito ユーザープールをプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Cognito ユーザープール機能に直接アクセスします。Amazon Cognito ユーザープールは、何億人ものユーザーにスケールする安全なユーザーディレクトリを提供します。フルマネージドサービスである Amazon Cognito ユーザープールは、サーバーインフラストラクチャの立ち上げを心配することなくセットアップできます。このサービスを使用すると、内部アプリケーションとの統合に使用できる最終ユーザーのプールを管理できます。このサービスでは、カスタマイズされたデータベースまたはウェブアプリケーションやモバイルアプリケーションの最終ユーザーのディレクトリの代わりに使用できます。同時に、Amazon Cognito ユーザープールは、パスワードポリシー、多要素認証、パスワード復旧、サービスへの自己サインアップなど、ディレクトリサービスのフルセットの機能を提供します。また、アプリケーションは OpenID、Facebook、Amazon、Google などの一般的なパブリックサービスでアクセスをフェデレーションすることもできます。



Amazon Cognito は 2 つの主要製品に分かれています。Amazon Cognito ユーザープールと Amazon Cognito ID プロバイダー。このセクションでは、Amazon S3 や DynamoDB などの他のサービスへのアクセスを提供する Amazon Cognito ユーザープールに焦点を当てます。AWS Amazon S3 DynamoDB このサービスでは、Amazon Cognito ユーザープールまたはサードパーティーの ID プロバイダーを使用して、AWS サービスへのアクセスを提供できます。また、匿名ゲストアクセスを使用して AWS サービスへのアクセスも提供します。Amazon Cognito ユーザープールの強力な性質により、アカウントへの潜在的なセキュリティ侵害を避けるために、運用手動サービスとして case-by-case で手動で管理されます。詳細については、[Amazon Cognito ユーザープール](#)」を参照してください。

## AWS Managed Services の Amazon Cognito ユーザープールに関するよくある質問

よくある質問と回答：

Q: AMS アカウントの Amazon Cognito ユーザープールへのアクセスをリクエストするにはどうすればよいですか？

AMS での Amazon Cognito ユーザープールの実装は、2 ステップのプロセスです。

1. 管理を送信する | その他 | その他 | 変更タイプ (ct-1e1xtak34nx76) を作成し、AMS アカウントで Amazon Cognito ユーザープールの作成をリクエストします。次の情報を含めてください。
  - AWS リージョン。
  - Cognito ユーザープールの名前。
  - デフォルトの内部 Cognito メールサービスの代わりに Amazon Simple Email Service (Amazon SES) を使用してメッセージと通知を送信する場合、お客様はアカウントで Amazon SES Service の検証済みの E メールアドレスを提供する必要があります。このアドレスは、メッセージの「From」フィールドと「REPLY-TO」フィールドに使用されます。また、Amazon SES がアクティブ化されたリージョン (us-east-1、eu-west-1、または us-west-2) も指定する必要があります。
  - ワンタイムパスワードと検証に SMS メッセージを使用する場合は、顧客が指定する必要があります。
2. Management | AWS service | Self-provisioned service | Add change type (ct-1w8z66n899dct) を送信してユーザーアクセスをリクエストします。この RFC は、customer\_cognito\_admin\_role および の IAM ロールをアカウントにプロビジョニングします customer\_cognito\_importjob\_role。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。これらのロールを使用すると、Amazon Cognito ユーザープールの管理、プール内のユーザーとグループの管理、ユーザー

のインポートジョブの作成、通知メッセージとサブスクリプションメッセージの変更、ユーザープールへのアプリケーションの関連付け、プールへのフェデレーションサービスの追加の自己管理、および既に作成されたプールの削除を行うことができます。

Q: AMS アカウントでの Amazon Cognito ユーザープールの使用にはどのような制限がありますか？

Amazon Cognito ユーザープールを作成することはできません。このアクションでは、Amazon SES や Amazon Cognito が使用するサービスを活用するための IAM ロールを作成する必要があります。Amazon SNS

Q: AMS アカウントで Amazon Cognito ユーザープールを使用するための前提条件または依存関係は何ですか？

Amazon SES を使用してユーザープールに E メールでメッセージと通知を送信する場合は、アカウントで Amazon SES サービスをアクティブ化し、送信された Eメールの「FROM」フィールドと「REPLY-TO」フィールドで使用する E メールアドレスを既に検証する必要があります。Amazon SES を使用した E メールアドレスの検証の詳細については、[Amazon SES での E メールアドレスの検証](#)」を参照してください。

## AMS SSP を使用して AMS アカウントに Amazon Comprehend をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Comprehend 機能に直接アクセスします。Amazon Comprehend は、機械学習を使用してテキストでインサイトや関係を見つける自然言語処理 (NLP) サービスであり、機械学習の経験は必要ありません。Amazon Comprehend は機械学習を使用して、非構造化データ内のインサイトと関係を明らかにするのに役立ちます。このサービスは、テキストの言語の識別、キーフレーズ、場所、人物、ブランド、またはイベントの抽出、テキストがどの程度肯定的または否定的であるかの理解、トークン化と音声部分を使ったテキスト分析、テキストファイルコレクションのトピックごとの自動整理を行います。Amazon Comprehend の AutoML 機能を使用すると、組織のニーズに合わせて独自にカスタマイズしたエンティティまたはテキスト分類モデルのカスタムセットを構築することもできます。詳細については、[Amazon Comprehend](#)」を参照してください。

## AWS Managed Services の Amazon Comprehend に関するよくある質問

Q: AMS アカウントで Amazon Comprehend へのアクセスをリクエストするにはどうすればよいですか？

Amazon Comprehend コンソールとデータアクセスロールは、2 つの AMS Service RFCs を送信することでリクエストできます。

Management | AWS service | Self-provisioned service | Add (マネージドオートメーション) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_comprehend_console_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon Comprehend の使用にはどのような制限がありますか？

Amazon Comprehend コンソールを使用して新しい IAM ロールを作成する機能は制限されています。それ以外の場合は、Amazon Comprehend の全機能が AMS アカウントで使用できます。

Q: AMS アカウントで Amazon Comprehend を使用するための前提条件または依存関係は何ですか？

Amazon S3 バケットが AWS KMS キーで暗号化されている場合、Amazon Comprehend を使用するには Amazon S3 と AWS Key Management Service (AWS KMS) が必要です。

## AMS SSP を使用して AMS アカウントに Amazon Connect をプロビジョニングする

### Note

慎重に検討した結果、2026 年 5 月 20 日をもって Amazon Connect Voice ID のサポートを終了することになりました。Amazon Connect Voice ID は、2025 年 5 月 20 日以降、新規のお客様を受け入れません。2025 年 5 月 20 日より前にサービスにサインアップしたアカウントを持つ既存のお客様は、引き続き Amazon Connect Voice ID の機能を使用できます。2026 年 5 月 20 日以降は、Amazon Connect Voice ID を使用できなくなります。

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Connect 機能に直接アクセスします。Amazon Connect は、企業が優れたカスタマーサービスを低コストで提供できるようにするオムニチャネルクラウドコンタクトセンターです。Amazon Connect は顧客とエージェントに音声とチャットのチャネル全体でシームレスなエクスペリエンスを提供します。これには、スキルベースのルーティング、強力なリアルタイム分析と履歴分析、easy-to-use 直感的な管理ツールのセットが含まれます。これらはすべて pay-as-you-go です。

仮想コンタクトセンターインスタンスの 1 つ以上のインスタンスは、AMS マルチアカウントランディングゾーンまたはシングルアカウントランディングゾーンアカウントに作成できます。エージェ

ントアクセスには既存の SAML 2.0 ID プロバイダーを使用するか、ユーザーライフサイクル管理には Amazon Connect ネイティブサポートを使用できます。

さらに、Amazon Connect コンソールから各 Amazon Connect インスタンスの通話料無料/直通ダイヤルの電話番号を要求できます。Amazon Connect 豊富な問い合わせフローを作成して、easy-to-use グラフィカルユーザーインターフェイスを使用して、望ましいカスタマーエクスペリエンスとルーティングを実現できます。問い合わせフローは、AWS Lambda 関数を活用して、オンプレミスのデータストアや API と統合できます。Kinesis Streams と Firehose を使用してデータストリーミングを有効にすることもできます。

通話録音、チャットトランスクリプト、およびレポートは、AWS KMS キーを使用して暗号化された Amazon S3 バケットに保存されます。問い合わせフローログは CloudWatch ロググループに保存できます。

詳細については、[Amazon Connect](#)」を参照してください。

## AWS Managed Services での Amazon Connect に関するよくある質問

Q: AMS アカウントで Amazon Connect へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (マネージドオートメーション) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、customer\_connect\_console\_role および の IAM ロールをアカウントにプロビジョニングします customer\_connect\_user\_role。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon Connect の使用にはどのような制限がありますか？

制限はありません。Amazon Connect の完全な機能は、AMS アカウントで使用できます。

Q: AMS アカウントで Amazon Connect を使用するための前提条件または依存関係は何ですか？

- 標準の AMS RFCs を使用して AWS KMS キーと Amazon S3 バケットを作成する必要があります。通話録音とチャットトランスクリプトを保存するには Amazon S3 バケットが必要です。
- Active Directory (AD) と統合する場合は、AMS がホストする Amazon Connect インスタンスとオンプレミスのディレクトリサービスの統合に AD Connector が必要です。AD Connector は、「Management | Other | Other」RFC をリクエストすることで、アカウントで設定できます。
- 問い合わせフローの要件に基づいて、以下のオプションのセルフプロビジョニングサービスを有効にできます。

- AWS Lambda: Lambda 関数を使用して問い合わせフローを拡張し、既存のオンプレミスデータストアまたは APIs を活用できます。Lambda 自己プロビジョニングサービスを使用して Lambda 関数を作成できます。
- Amazon Kinesis Data Streams: データストリームを作成して、外部アプリケーションへのデータストリーミングを有効にできます。問い合わせトレースレコードまたはエージェントイベントをストリーミングできます。
- Amazon Kinesis Data Firehose: Data Firehose を作成して、大量の問い合わせトレースレコードを外部アプリケーションにストリーミングできます。
- Amazon Lex: Amazon Lex Chatbots を活用して、Amazon Alexa サービスを活用したスマートな問い合わせフローを作成し、豊富なカスタマーエクスペリエンスと自動化を実現できます。
- Q: 発信通話または着信通話の国のリストの追加をリクエストするにはどうすればよいですか？

アウトバウンド通話またはインバウンド通話の国のリストを追加するには、サービスリクエストを AMS に送信します。

## AMS SSP を使用して AMS アカウントに Amazon Data Firehose をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Data Firehose 機能に直接アクセスします。Firehose は、ストリーミングデータをデータレイク、データストア、分析ツールに確実にロードする最も簡単な方法です。Amazon S3、Amazon Redshift、Amazon OpenSearch Service、[Splunk](#) にストリーミングデータをキャプチャ、変換、ロードできるため、現在既に使用している既存のビジネスインテリジェンスツールやダッシュボードでほぼリアルタイムの分析が可能になります。完全マネージド型サービスのため、データスループットに応じて自動的にスケールされ、継続的な管理は不要です。また、データをロードする前にバッチ処理、圧縮、変換、および暗号化を行うことができるため、送信先で使用されるストレージ量を最小限に抑え、セキュリティを強化できます。詳細については、[「Amazon Data Firehose とは」を参照してください。](#)

### AWS Managed Services の Firehose に関するよくある質問

一般的な質問と回答:

Q: AMS アカウントの Amazon Data Firehose へのアクセスをリクエストするにはどうすればよいですか？



Management | AWS service | Self-provisioned service | Add (マネージドオートメーション)

(ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_kinesis_firehose_user_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Firehose の使用にはどのような制限がありますか？

制限はありません。Amazon Data Firehose の全機能は、AMS アカウントで使用できます。

Q: AMS アカウントで Firehose を使用するための前提条件または依存関係は何ですか？

配信ストリームごとに新しいサービスにリンクされた IAM ロールをリクエストする必要があります。また、必要なリソースアクセス許可 (S3 バケット/KMS キー/Lambda 関数/Kinesis ストリームを含む) でロールポリシーを更新することで、すべてのストリームに対して単一のサービスにリンクされたロールを再利用することもできます。

RFC を送信して Firehose を追加すると、AMS オペレーションエンジニアが Data Firehose に接続するリソース (S3 AWS KMS、Lambda、Kinesis Streams など) の ARNs のサービスリクエストを通じてお客様に連絡します。

## AMS SSP を使用して AMS アカウントに Amazon DevOps Guru をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon DevOps Guru 機能に直接アクセスします。Amazon DevOps Guru は、開発者やオペレーターがアプリケーションのパフォーマンスと可用性を簡単に改善できるようにするフルマネージド型のオペレーションサービスです。DevOps Guru は、運用上の問題の特定に関連する管理タスクをオフロードし、アプリケーションを改善するためのリコメンデーションを迅速に実装できるようにします。DevOps Guru は、アプリケーションを今すぐ改善するために使用できる事後対応型のインサイトを作成します。また、将来アプリケーションに影響を与える可能性のある運用上の問題を回避するために事前対応型インサイトを作成します。DevOps Guru は、機械学習を適用して、運用データとアプリケーションのメトリクスおよびイベントを分析し、通常の運用パターンから逸脱する動作を特定します。DevOps Guru が運用上の問題またはリスクを検出すると通知が行われます。DevOps Guru は、各問題について、現在および予測される将来の運用上の問題に対処するためのインテリジェントなレコメンデーションを提示します。

詳細については、[「Amazon DevOps Guru とは」](#)を参照してください。

## AWS Managed Servicesでの Amazon DevOps Guru に関するよくある質問

Q: AMS アカウントの Amazon DevOps Guru へのアクセスをリクエストするにはどうすればよいですか？

アクセスをリクエストするには、管理 | AWS サービス | セルフプロビジョニングサービス | (マネージドオートメーション) (ct-3qe6io8t6jtny) 変更タイプを追加します。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_devopsguru_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon DevOps Guru の使用にはどのような制限がありますか？

制限はありません。Amazon DevOps Guru の全機能は、AMS アカウントで使用できます。

Q: AMS アカウントで Amazon DevOps Guru を使用するための前提条件または依存関係は何ですか？

前提条件はありません。DevOps Guru は、Amazon CloudWatch Logs、RDS Insights AWS X-Ray、および AWS Lambda AWS のサービスを活用します AWS CloudTrail。

## AMS SSP を使用して AMS アカウントに Amazon DocumentDB (MongoDB 互換) をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon DocumentDB (MongoDB 互換) 機能に直接アクセスします。Amazon DocumentDB (MongoDB 互換) は、MongoDB ワークロードをサポートする、高速、スケーラブル、高可用性、完全マネージド型のドキュメントデータベースサービスです。Amazon DocumentDB は、ミッションクリティカルな MongoDB ワークロードを大規模に運用するために必要なパフォーマンス、スケーラビリティ、可用性を提供します。Amazon DocumentDB は、MongoDB クライアントが MongoDB サーバーに期待するレスポンスをエミュレートすることで、Apache 2.0 オープンソースの MongoDB 3.6 API を実装し、Amazon DocumentDB で既存の MongoDB ドライバーとツールを使用できます。MongoDB Amazon DocumentDB では、ストレージとコンピューティングが分離され、それぞれが独立してスケールできるようになります。データのサイズに関係なく、最大 15 個の低レイテンシーのリードレプリカを追加することで、読み取り容量を 1 秒あたり数百万リクエストに増やすことができます。Amazon DocumentDB は 99.99% の可用性を実現するように設計されており、データの 6 つのコピーを 3 つの AWS アベイラビリティゾーン (AZs) にレプリケートします。AWS Database Migration Service (DMS) を無料で (6 か月間) 使用して、オンプレミスまたは Amazon Elastic Compute Cloud (Amazon EC2) MongoDB データベースを Amazon DocumentDB にほぼダウンタイムなしで移行できます。詳細については、[Amazon DocumentDB \(MongoDB 互換\)](#) を参照してください。

## AWS Managed Services の Amazon DocumentDB に関するよくある質問

Q: AMS アカウントの Amazon DocumentDB へのアクセスをリクエストするにはどうすればよいですか？

Amazon DocumentDB コンソールとデータアクセスロールは、コンソールアクセスとデータアクセスの 2 つの AMS RFCs を送信することでリクエストできます。

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (ct-1w8z66n899dct) 変更タイプで RFC を送信して Amazon DocumentDB へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_documentdb_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon DocumentDB の使用にはどのような制限がありますか？

Amazon DocumentDB には、Amazon RDS 固有のアクセス許可が必要です。AMS は Amazon RDS を完全に管理するため、Amazon DocumentDB の IAM ロールには Amazon RDS でのアクションに対するいくつかの制限が含まれています。以下の制限が適用されます。

- DeleteDBInstance および DeleteDBCluster APIs へのアクセスが制限されています。これらの削除 APIs を使用するには、管理 | 高度なスタックコンポーネント | Identity and Access Management (IAM) | 更新エンティティまたはポリシー (マネージドオートメーション) 変更タイプ (ct-27tuth19k52b4) で RFC を送信します。
- Amazon RDS インスタンスにタグを追加または削除することはできません。
- Amazon DocumentDB インスタンスを公開することはできません。

Q: AMS アカウントで Amazon DocumentDB を使用するための前提条件または依存関係は何ですか？

Amazon S3 バケット AWS KMS が AWS KMS キーで暗号化されている場合、Amazon DocumentDB を使用するには Amazon S3 と が必要です。

## AMS SSP を使用して AMS アカウントに Amazon DynamoDB をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon DynamoDB (DynamoDB) 機能に直接アクセスします。Amazon DynamoDB は、あらゆる規模で 1 桁ミリ秒のパフォーマンスを実現するキー値およびドキュメントデータベースです。これ



は、セキュリティ、バックアップと復元、インターネットスケールアプリケーション用のインメモリキャッシュが組み込まれた、フルマネージド型のマルチリージョンのマルチアクティブデータベースです。詳細については[Amazon DynamoDB](#)を参照してください。

Amazon DynamoDB Accelerator (DAX) は、DynamoDB テーブルにキャッシュを追加するプロセスを簡素化するために設計された書き込みスルーキャッシュサービスです。DAX は、高パフォーマンスの読み込みを必要とするアプリケーションを対象としています。

## AWS Managed Services の DynamoDB に関するよくある質問

Q: AMS アカウントの DynamoDB と DAX へのアクセスをリクエストするにはどうすればよいですか？

管理 | サービス | AWS セルフプロビジョニングサービス | 追加 (ct-1w8z66n899dct) 変更タイプで RFC を送信して、DynamoDB と DAX へのアクセスをリクエストします。この RFC は、次の IAM ロールとポリシーをアカウントにプロビジョニングします。

- DynamoDB ロール名: `customer_dynamodb_role`

DAX サービスロール名: `customer_dax_service_role`

- DynamoDB ポリシー名: `customer_dynamodb_policy`

DAX サービスポリシー: `customer_dax_service_policy`

アカウントにプロビジョニングされたら、フェデレーションソリューション `customer_dynamodb_role` で をオンボードする必要があります。

Q: AMS アカウントでの DynamoDB の使用にはどのような制限がありますか？

DynamoDB Accelerator (DAX) を含むすべての DynamoDB 機能がサポートされています。

特定のテーブルに対してアラームを作成する場合、アラーム名には「customer\*」というプレフィックスを付ける必要があります `customer-employee-table-high-put-latency`。たとえば、。

DynamoDB 用の Amazon SNS トピックを作成するときは、 という名前にする必要があります `dynamodb`。

DynamoDB によって作成された Amazon SNS トピックを削除するには、管理 | その他 | その他 | 更新変更タイプ RFC を送信します。

Q: AMS アカウントで DynamoDB を使用するための前提条件または依存関係は何ですか？

AMS アカウントで DynamoDB を使用するための前提条件や依存関係はありません。

## AMS SSP を使用して AMS アカウントに Amazon Elastic Container Registry をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Elastic Container Registry (Amazon ECR) 機能に直接アクセスします。Amazon Elastic Container Registry は、開発者が [Docker](#) コンテナイメージを簡単に保存、管理、デプロイできるようにするフルマネージド型の Docker コンテナレジストリです。Amazon ECR は [Amazon Elastic Container Service \(Amazon ECS\)](#) と統合されているため、本番環境への開発ワークフローが簡素化されます。Amazon ECR を使用すると、独自のコンテナリポジトリを運用したり、基盤となるインフラストラクチャのスケールリングを心配する必要がなくなります。Amazon ECS は、高可用性でスケラブルなアーキテクチャでイメージをホストするため、アプリケーションのコンテナを確実にデプロイできます。AWS Identity and Access Management (IAM) との統合により、各リポジトリのリソースレベルの制御が可能になります。Amazon ECR では、前払い料金やコミットメントはありません。リポジトリに保存したデータの量とインターネットに転送されたデータに対してのみ料金が発生します。

詳細については、[「Amazon Elastic Container Registry」](#) を参照してください。

## AWS Managed Services の Amazon Elastic Container Registry に関するよくある質問

Q: AMS アカウントの Amazon ECR へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) change type で RFC を送信して Amazon ECR へのアクセスをリクエストします。この RFC は、次の IAM ロールをアカウントにプロビジョニングします: `customer_ecr_console_role`、および関連する IAM ポリシー `customer_ecr_poweruser_instance_profile` を持つ `customer_ecr_poweruser_instance_profile_policy`、`customer_ecr_console_policy` および。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon ECR の使用にはどのような制限がありますか？

AMS アカウントでの Amazon ECR の使用には、AMS 名前空間に関する制限があります。コンテナイメージには「AMS-」または「Sentinel-」のプレフィックスを付けることはできません。

Q: AMS アカウントで Amazon ECR を使用するための前提条件または依存関係は何ですか？

AMS アカウントで Amazon ECR を使用するための前提条件や依存関係はありません。

## AMS SSP を使用して AMS アカウントに EC2 Image Builder をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで EC2 Image Builder 機能に直接アクセスします。EC2 Image Builder は、カスタマイズされ、安全で up-to-date 「ゴールデン」サーバーイメージの作成、管理、デプロイを簡単に自動化できるフルマネージド AWS サービスです。これらのイメージは、特定の IT 標準を満たすためのソフトウェアと設定がプリインストールされ、事前設定されています。

AWS マネジメントコンソール、AWS CLI、または APIs を使用して、AWS アカウントにカスタムイメージを作成できます。を使用すると AWS マネジメントコンソール、Amazon EC2 Image Builder ウィザードが以下のステップをガイドします。

- 開始アーティファクトを指定する
- ソフトウェアの追加と削除
- 設定とスクリプトをカスタマイズ
- 選択したテストを実行する
- AWS イメージをリージョンに配布する

ビルドするイメージはアカウントで作成され、オペレーティングシステムのパッチ用に継続的に設定できます。詳細については、[EC2 Image Builder](#) を参照してください。

### AWS Managed Services の EC2 Image Builder に関するよくある質問

一般的な質問と回答:

Q: AMS アカウントの EC2 Image Builder へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (マネージドオートメーション) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC を通じて、次の IAM ロールがアカウントにプロビジョニングされます: `customer_ec2_imagebuilder_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: EC2 Image Builder にはどのような制限がありますか？

AMS は、インフラストラクチャ設定でのサービスデフォルトの使用をサポートしていません。新しいインフラストラクチャ設定を作成することも、既存の設定を使用することもできます。

AMS は現在、コンテナレシピの作成をサポートしていません。

Q: EC2 Image Builder を有効にするための前提条件または依存関係は何ですか？

- EC2 Image Builder サービスにリンクされたロール: サービスにリンクされたロールを手動で作成する必要はありません。、 CLI AWS マネジメントコンソール、または AWS API で最初の Image Builder AWS リソースを作成すると、Image Builder によってサービスにリンクされたロールが作成されます。
- Image Builder を使用してイメージを構築し、テストを実行するために使用されるインスタンスは、Systems Manager サービスにアクセスできる必要があります。SSM エージェントは、ソースイメージがまだ存在しない場合はインストールされ、イメージが作成される前に削除されます。
- AWS IAM: インスタンスプロファイルに関連付ける IAM ロールには、イメージに含まれるビルドコンポーネントとテストコンポーネントを実行するアクセス許可が必要です。インスタンスプロファイルに関連付けられている IAM ロールには、EC2InstanceProfileForImageBuilder および の IAM ロールポリシーをアタッチする必要があります AmazonSSMManagedInstanceCore。IAM ロール名には \*imagebuilder\* キーワードを含める必要があります。
- ロギングを設定する場合、インフラストラクチャ構成で指定されたインスタンスプロファイルは、ターゲットバケット(arn:aws:s3:::{bucket-name}/\*)に対して s3:PutObject の権限を持っている必要があります。例えば、次のようになります。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::{bucket-name}/*"
    }
  ]
}
```

- EC2 Image Builder からアラートと通知を受信するには、「imagebuilder」という名前の SNS トピックを作成します。

## AMS SSP を使用して AMS アカウントの AWS Fargate で Amazon ECS をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS Fargate 機能で Amazon ECS に直接アクセスします。AWS Fargate は、Amazon EC2 インスタンスの Amazon EC2 で使用できるテクノロジーです (「[のコンテナ AWS](#)」を参照)。を使用すると AWS Fargate、コンテナを実行するために仮想マシンのクラスターをプロビジョニング、設定、またはスケーリングする必要がなくなります。これにより、サーバータイプの選択、クラスターをスケーリングするタイミングの決定、クラスターのパッキングの最適化を行う必要がなくなります。

詳細については、「[Amazon ECS on AWS Fargate](#)」を参照してください。

### AWS Managed Services での Fargate での Amazon ECS に関するよくある質問

Q: AMS アカウントの Fargate で Amazon ECS へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (ct-1w8z66n899dct) 変更タイプで RFC を送信して、Fargate で Amazon ECS へのアクセスをリクエストします。この RFC は、次の IAM ロールをアカウントにプロビジョニングします: `customer_ecs_fargate_console_role` (ECS ポリシーを関連付けるための既存の IAM ロールが指定されていない場合) `customer_ecs_fargate_events_service_role`、`customer_ecs_task_execution_service_role` および `AWSManagedServiceRoleForApplicationAutoScaling_ECSService`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントで Fargate で Amazon ECS を使用することにはどのような制限がありますか？

- Amazon ECS タスクのモニタリングとログ記録は、コンテナレベルのアクティビティがハイパーバイザーを超えて発生し、Fargate の Amazon ECS によってログ記録機能が制限されるため、お客様の責任と見なされます。Fargate 上の Amazon ECS のユーザーは、Amazon ECS タスクのログ記録を有効にするために必要な手順を実行することをお勧めします。詳細については、「[コンテナの awslogs ログドライバーの有効化](#)」を参照してください。
- コンテナレベルでのセキュリティとマルウェアの保護もお客様の責任と見なされます。Fargate の Amazon ECS には、Trend Micro または事前設定されたネットワークセキュリティコンポーネントは含まれていません。

- このサービスは、マルチアカウントランディングゾーンとシングルアカウントランディングゾーンの両方の AMS アカウントで使用できます。
- Amazon ECS [Service Discovery](#) は、Route 53 プライベートホストゾーンの作成には昇格されたアクセス許可が必要であるため、セルフプロビジョニングロールではデフォルトで制限されています。サービスでサービス検出を有効にするには、[管理 | その他 | その他 | 変更タイプ](#)を更新します。Amazon ECS サービスのサービス検出を有効にするために必要な情報については、「[サービス検出マニュアル](#)」を参照してください。
- AMS は現在、Amazon ECS Fargate へのコンテナのデプロイに使用されるイメージを管理または制限していません。Amazon ECR、Docker Hub、またはその他のプライベートイメージリポジトリからイメージをデプロイできます。したがって、パブリックイメージやセキュリティで保護されていないイメージは、アカウントで悪意のあるアクティビティが発生する可能性があるため、デプロイしないことをお勧めします。

Q: AMS アカウントで Fargate で Amazon ECS を使用する際の前提条件または依存関係は何ですか？

- 以下は、Fargate 上の Amazon ECS の依存関係です。ただし、自己プロビジョニングロールでこれらのサービスを有効にするための追加のアクションは必要ありません。
  - CloudWatch ログ
  - CloudWatch events
  - CloudWatch アラーム
  - CodeDeploy
  - App Mesh
  - クラウドマップ
  - Route 53
- ユースケースに応じて、Amazon ECS が依存するリソースを次に示します。アカウントで Fargate で Amazon ECS を使用する前に必要になる場合があります。
  - Amazon ECS サービスで使用するセキュリティグループ。デプロイ | 高度なスタックコンポーネント | セキュリティグループ | 作成 (自動) (ct-3pc215bnwb6p7) を使用するか、セキュリティグループで特別なルールが必要な場合は、デプロイ | 高度なスタックコンポーネント | セキュリティグループ | 作成 (マネージドオートメーション) (ct-10xx2g2d7hc90) を使用できます。  
注: Amazon ECS で選択したセキュリティグループは、Amazon ECS サービスまたはクラスターが存在する Amazon ECS 専用に作成する必要があります。詳細については、「Security Group」セクションの「[Setting Up with Amazon ECS](#) and [Security in Amazon Elastic Container Service](#)」を参照してください。



- Application Load Balancer (ALB)、Network Load Balancer (NLB)、Classic Load Balancer (ELB)。
- ALBs のターゲットグループ。
- Amazon ECS クラスターと統合するためのアプリメッシュリソース (仮想ルーター、仮想サービス、仮想ノードなど)。
- 現在、標準 AMS 変更タイプ以外で作成された場合、AMS がセキュリティグループのアクセス許可のサポートに関連するリスクを自動的に軽減する方法はありません。Amazon ECS で使用するために指定されていないセキュリティグループを使用する可能性を制限するために、Fargate クラスターで使用する特定のセキュリティグループをリクエストすることをお勧めします。

## AMS SSP を使用して AMS アカウントの AWS Fargate で Amazon EKS をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS Fargate 機能で Amazon EKS に直接アクセスします。AWS Fargate は、コンテナに適したサイズのコンピューティングキャパシティをオンデマンドで提供するテクノロジーです (コンテナを理解するには、[「コンテナとは」](#)を参照してください)。を使用すると AWS Fargate、コンテナを実行するために仮想マシンのグループをプロビジョニング、設定、またはスケールする必要がなくなります。これにより、サーバータイプの選択、ノードグループをスケールするタイミングの決定、クラスターのパッキングの最適化を行う必要がなくなります。

Amazon Elastic Kubernetes Service (Amazon EKS) は、Kubernetes が提供するアップストリームの拡張可能なモデル AWS Fargate を使用して構築されたコントローラー AWS を使用して、Kubernetes をと統合します。これらのコントローラーは、Amazon EKS が管理する Kubernetes コントロールプレーンの一部として実行され、ネイティブ Kubernetes ポッドを Fargate にスケジューリングします。Fargate コントローラーには、いくつかの変更と検証アドミSSION コントローラーに加えて、デフォルトの Kubernetes スケジューラーとともに実行される新しいスケジューラーが含まれています。Fargate で実行する条件を満たすポッドを起動すると、クラスターで実行されている Fargate コントローラーはポッドを認識し、更新し、Fargate にスケジューリングします。

詳細については、[「Amazon EKS on AWS Fargate Now generally Available」](#) および [「Amazon EKS Best Practices Guide for Security」](#) (「Review and revoke unnecessary anonymous access」などの「Recommendations」を含む) を参照してください。

**i** Tip

AMS には、Amazon EKS で使用できる変更タイプである Deployment | Advanced stack components | Identity and Access Management (IAM) | Create OpenID Connect provider (ct-30ecvfi3tq4k3) があります。例については、[「Identity and Access Management \(IAM\) | Create OpenID Connect Provider」](#)を参照してください。

## AWS Managed Services AWS Fargate のでの Amazon EKS に関するよくある質問

Q: AMS アカウントの Fargate で Amazon EKS へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (マネージドオートメーション) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、次の IAM ロールをアカウントにプロビジョニングします。

- customer\_eks\_fargate\_console\_role.

アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

- これらのサービスロールは、ユーザーに代わって他の AWS サービスを呼び出すアクセス許可を Amazon EKS on Fargate に付与します。

- customer\_eks\_pod\_execution\_role
- customer\_eks\_cluster\_service\_role

Q: AMS アカウントで Fargate で Amazon EKS を使用することにはどのような制限がありますか？

- [マネージド](#) EC2 ノードグループまたは[セルフマネージド](#) EC2 ノードグループの作成は、AMS ではサポートされていません。EC2 EC2 ワーカーノードの使用が必要な場合は、AMS Cloud Service Delivery Manager (CSDM) または Cloud Architect (CA) にお問い合わせください。
- AMS には、Trend Micro またはコンテナイメージ用に事前設定されたネットワークセキュリティコンポーネントは含まれません。デプロイ前に悪意のあるコンテナイメージを検出するために、独自のイメージスキャンサービスを管理する必要があります。
- CloudFormation の相互依存関係のため、EKSCtl はサポートされていません。
- クラスターの作成中に、クラスターコントロールプレーンのログ記録を無効にするアクセス許可があります。詳細については、[「Amazon EKS コントロールプレーンのログ記録」](#)を参照してくだ



さい。クラスターの作成時に、すべての重要な API、認証、監査ログを有効にすることをお勧めします。

- クラスターの作成中、Amazon EKS クラスターのクラスターエンドポイントアクセスはデフォルトでパブリックになります。詳細については、[「Amazon EKS クラスターエンドポイントアクセスコントロール」](#)を参照してください。Amazon EKS エンドポイントをプライベートに設定することをお勧めします。パブリックアクセスにエンドポイントが必要な場合は、特定の CIDR 範囲に対してのみパブリックに設定することをお勧めします。
- AMS には、Amazon EKS Fargate のコンテナへのデプロイに使用されるイメージを強制および制限する方法はありません。Amazon ECR、Docker Hub、またはその他のプライベートイメージリポジトリからイメージをデプロイできます。したがって、アカウントで悪意のあるアクティビティを実行する可能性のあるパブリックイメージをデプロイするリスクがあります。
- Cloud Development Kit (CDK) または CloudFormation Ingest を使用した EKS クラスターのデプロイは、AMS ではサポートされていません。
- [ct-3pc215bnwb6p7 デプロイ | 高度なスタックコンポーネント | セキュリティグループ](#) | イングレス作成用のマニフェストファイルの作成と参照を使用して、必要なセキュリティグループを作成する必要があります。これは、ロールにセキュリティグループを作成する権限 `customer-eks-alb-ingress-controller-role` がないためです。

Q: AMS アカウントで Fargate で Amazon EKS を使用するための前提条件または依存関係は何ですか？

サービスを使用するには、次の依存関係を設定する必要があります。

- サービスに対して認証するには、KUBECTL と aws-iam-authenticator の両方をインストールする必要があります。詳細については、[「クラスター認証の管理」](#)を参照してください。
- Kubernetes は「サービスアカウント」と呼ばれる概念に依存しています。EKS 上の kubernetes クラスター内のサービスアカウント機能を利用するには、次の入力で管理 | その他 | その他 | RFC を更新する必要があります。
  - [必須] Amazon EKS クラスター名
  - [必須] サービスアカウント (SA) がデプロイされる Amazon EKS クラスター名前空間。
  - [必須] Amazon EKS クラスター SA 名。
  - [必須] 関連付ける IAM ポリシー名とアクセス許可/ドキュメント。
  - [必須] リクエストされている IAM ロール名。
  - [オプション] OpenID Connect プロバイダー URL。詳細については、以下を参照してください。
    - [クラスターでサービスアカウントの IAM ロールを有効にする](#)

- [サービスアカウントのきめ細かな IAM ロールの紹介](#)
- Config ルールを設定してモニタリングすることをお勧めします。
- パブリッククラスターエンドポイント
- 無効化された API ログ記録

これらの Config ルールをモニタリングして修正するのはユーザーの責任です。

[ALB Ingress](#) Controller をデプロイする場合は、管理 | その他 | その他の更新 RFC を送信して、ALB Ingress Controller ポッドで使用するために必要な IAM ロールをプロビジョニングします。ALB Ingress Controller (RFC にこれらを含める) に関連付ける IAM リソースを作成するには、次の入力が必要です。

- [必須] Amazon EKS クラスター名
- [オプション] OpenID Connect プロバイダー URL
- [オプション] Application Load Balancer (ALB) Ingress Controller サービスをデプロイする Amazon EKS クラスター名前空間。〔デフォルト: kube-system〕
- [オプション] Amazon EKS クラスターサービスアカウント (SA) 名。〔デフォルト: aws-load-balancer-controller〕

クラスターでエンベロープシークレットの暗号化を有効にする場合は (推奨)、使用する KMS キー IDs を RFC の説明フィールドに入力してサービスを追加します (Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct))。エンベロープ暗号化の詳細については、[「Amazon EKS adds envelope encryption for secrets with AWS KMS」](#)を参照してください。

## AMS SSP を使用して AMS アカウントに Amazon EMR をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon EMR 機能に直接アクセスします。Amazon EMR は、Apache Spark、Apache Hive、Apache HBase、Apache Flink、Apache Hudi、Presto などのオープンソースツールを使用して大量のデータを処理するための、業界をリードするクラウドビッグデータプラットフォームです。Amazon EMR を使用すると、従来のオンプレミスソリューションのコストの半分未満で、標準の Apache Spark の 3 倍以上の速度で Petabyte スケール分析を実行できます。実行時間の短いジョブでは、クラスターをスピンアップおよびスピンドアウンし、使用したインスタンスに対して 1 秒あ

たりの料金を支払うことができます。長時間実行されるワークロードの場合、需要に合わせて自動的にスケーリングする高可用性クラスターを作成できます。

Amazon EMR クラスターの 1 つ以上のインスタンスを AMS マルチアカウントランディングゾーンまたはシングルアカウントランディングゾーンアカウントに作成して、一時的および永続的な Amazon EMR クラスターの両方をサポートできます。Kerberos 認証を有効にして、オンプレミスの Active Directory ドメインからユーザーを認証することもできます。

Amazon EMR クラスターで複数のデータストアを活用して、ユースケース固有の Hadoop ツールとライブラリをサポートできます。Amazon EMR クラスターは、OnDemand インスタンスまたはスポットインスタンスを使用して作成し、容量を管理し、コストを削減するように自動スケーリングを設定できます。

クラスターログファイルは、ログ記録とデバッグのために Amazon S3 バケットにアーカイブできます。Amazon EMR クラスターでホストされているウェブインターフェイスにアクセスして、hadoop 管理要件をサポートしたり、顧客のノートブックエクスペリエンスをサポートしたりすることもできます。

詳細については、「[Amazon EMR](#)」を参照してください。

## AWS Managed Services での Amazon EMR に関するよくある質問

Q: AMS アカウントの Amazon EMR へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (マネージドオートメーション)  
(ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、次の IAM ロールをアカウントにプロビジョニングします。

- customer\_emr\_cluster\_instance\_profile
- customer\_emr\_cluster\_autoscaling\_role
- customer\_emr\_console\_role
- customer\_emr\_cluster\_service\_role

アカウントにプロビジョニングされたら、フェデレーションソリューションで customer\_emr\_console\_role をオンボードする必要があります。

Q: AMS アカウントでの Amazon EMR の使用にはどのような制限がありますか？

AWS コンソールから EC2 クラスターに Amazon EMR を作成するときは、クラスターの作成 – 詳細オプションを使用することをお勧めします。Amazon EMR クラスターは、キー-for-use-with-

amazon-emr-managed-policies」と値「true」のタグを追加して作成する必要があります。セキュリティオプションで次の設定を選択します。

- クラスターのカスタムロールを選択します。
  - EMR ロール: customer\_emr\_cluster\_service\_role
  - EC2 インスタンスプロファイル: customer\_emr\_cluster\_instance\_profile
  - Auto Scaling ロール: customer\_emr\_cluster\_autoscaling\_role
- EC2 セキュリティグループ:
  - マスター: ams-emr-master-security-group
  - コアとタスク: ams-emr-worker-security-group
  - サービスアクセス: ams-emr-serviceaccess-security-group

Q: AMS アカウントで Amazon EMR を使用するための前提条件または依存関係は何ですか？

AMS は、Amazon EMR マスター、ワーカー、およびサービスノードのデフォルトのセキュリティグループを作成します。

Amazon EMR クラスターで使用する起動テンプレートとセキュリティグループには、値「true」のタグキーfor-use-with-amazon-emr-managed-policies」が必要です。

デフォルトの Amazon EMR クラスターインスタンスプロファイルでは、名前に「emr」が含まれている s3 バケットや dynamodb テーブルなどのリソースにアクセスできます。Amazon EMR で使用する追加のリソースを使用するように、追加の IAM ポリシーをリクエストできます。customer\_emr\_cluster\_instance\_profile を使用して、Amazon EMR ジョブで次のリソース ARN を使用できます。

- arn:aws:dynamodb:\*:\*:table/\*emr\*
- arn:aws:kinesis:\*:\*:stream/\*emr\*
- arn:aws:sns:\*:\*:\*emr\*arn:aws:sqs:\*:\*:\*emr\*
- arn:aws:sqs:\*:\*:\*emr\*
- arn:aws:sqs:\*:\*:AWS-ElasticMapReduce-\*
- arn:aws:sdb:\*:\*:domain:\*emr\*
- arn:aws:s3:\*:\*:\*emr\*

Amazon EMR クラスターに kerberos 認証が必要な場合:

- カーバライズされた各 Amazon EMR クラスターに使用する領域名とオンプレミスの Active Directory IP アドレスを指定します。
- インフラストラクチャ要件:

マルチアカウントランディングゾーン (MALZ): RFC を送信して、新しいマネージドアプリケーションアカウントまたは既存のアプリケーションアカウントに新しい VPC を作成します。

単一アカウントランディングゾーン (SALZ): RFC を送信して VPC に新しいサブネットを作成します。

- オンプレミス Active Directory でクラスターの領域に対する受信信頼を設定します。
- マネージド AD の領域に DNS ゾーンを設定するには、RFC を送信します。
- 領域設定:

MALZ: 管理 | その他 | その他 | 更新 (ct-0xdawir96cy7k) RFC を送信して、ドメイン名のサフィックスに領域名を使用するように設定された VPC DHCP オプションを更新します。

SALZ: 管理 | その他 | その他 | 更新 (ct-0xdawir96cy7k) RFC を送信して、ドメイン名のサフィックスに特定の領域を使用する新しい Amazon EMR AMI を生成します。

Amazon EMR Studio をデプロイするには、ロールに Amazon Simple Storage Service バケットの前提条件 `customer_emr_cluster_service_role` があります。バケットを作成するには、自動 CT `ct-1a68ck03fn98r` (デプロイ | 高度なスタックコンポーネント | S3 ストレージ | 作成) を使用します。この自動 CT を使用して Amazon EMR 用の Amazon S3 バケットを作成する場合、バケット名はプレフィックスで始まる必要があります `customer-emr-*`。また、Amazon EMR クラスターと同じ AWS リージョンにバケットを作成する必要があります。

## AMS SSP を使用して AMS アカウントに Amazon EventBridge をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon EventBridge 機能に直接アクセスします。Amazon EventBridge は、アプリケーションをさまざまなイベントソースのデータに簡単に接続できるようにするサーバーレスイベントバスサービスです。EventBridge は、独自のアプリケーション、Software-as-a-Service (SaaS) アプリケーション、および AWS のサービスからリアルタイムデータのストリームを配信し、そのデータをなどのターゲットにルーティングします AWS Lambda。お客様は、データの送信先を判断するためのルーティングルールを設定して、すべてのデータソースにリアルタイムで反応するアプリケーションアー

キテクチャを構築できます。EventBridge を使用すると、疎結合かつ分散型のイベント駆動型アーキテクチャの構築が可能になります。

詳細については、「[Amazon EventBridge](#)」を参照してください。

## AWS Managed Services の EventBridge に関するよくある質問

Q: AMS アカウントの EventBridge へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (ct-1w8z66n899dct) 変更タイプで RFC を送信して EventBridge へのアクセスをリクエストします。この RFC は、customer\_eventbridge\_role および の IAM ロールをアカウントにプロビジョニングします customer\_eventbridge\_scheduler\_execution\_role。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

実行ロール customer\_eventbridge\_scheduler\_execution\_role は、EventBridge スケジューラが AWS のサービス ユーザーに代わって他の とやり取りするために引き受ける IAM ロールです。このロールにアタッチされたアクセス許可ポリシーは EventBridge スケジューラにターゲットを呼び出すためのアクセス許可を付与します。

### Note

デフォルトでは、EventBridge スケジューラは EventBridge の AWS 所有キーを使用してデータを暗号化します。EventBridge のカスタマーマネージドキーを使用してデータを暗号化するには、管理 | AWS サービス | セルフプロビジョニングサービス | サービスプロビジョニングに [\(マネージドオートメーション\) 変更タイプ \(ct-3qe6io8t6jtny\)](#) を追加します。

Q: AMS アカウントでの EventBridge の使用にはどのような制限がありますか？

AMS RFCs を送信し、次のリソースを作成する必要があります。バッチジョブ、SQS キュー、CodeBuild、CodePipeline、および SSM コマンドをトリガーするサービスロール。

Q: AMS アカウントで EventBridge を使用するための前提条件または依存関係は何ですか？

EventBridge を使用して Lambda、Amazon SNS、Amazon SQS AWS Batch、Amazon CloudWatch Logs リソースなどの他の AWS リソースをトリガーする前に、デプロイ | 高度なスタックコンポーネント | Identity and Access Management (IAM) | Create entity or policy (マネージドオートメーション) change type (ct-3dpd8mdd9jn1r) を使用して RFC で EventBridge サービスロールをリクエストする必要があります。Amazon SNS Amazon SQS サービスロールをリクエストするときに呼び出す



サービスを指定します。ターゲットの呼び出しに必要なアクセス許可については、[EventBridge のリソースベースのポリシーの使用](#)」を参照してください。

EventBridge は AWS CloudTrail、EventBridge のユーザー、ロール、または によって実行されたアクションを記録するサービスである EventBridge と統合 AWS のサービス されています。CloudTrail を有効にして、ログファイルを S3 バケットに保存できるようにする必要があります。注: すべての AMS アカウントで CloudTrail が有効になっているため、アクションは必要ありません。

Q: ロール `customer_eventbridge_scheduler_execution_role` には、AWS Key Management Service キーの前提条件があります (暗号化に使用される場合はオプション)。保管時/転送時のデータ暗号化に AWS KMS CMKs を採用するにはどうすればよいですか？

デフォルトでは、EventBridge スケジューラは、AWS 所有キーに保存するイベントメタデータとメッセージデータを暗号化します (保管時の暗号化)。EventBridge スケジューラは、Transport Layer Security (TLS) (転送中の暗号化) を使用して、EventBridge スケジューラと他の サービスの間を通過するデータも暗号化します。

特定のユースケースで、EventBridge スケジューラでデータを保護する暗号化キーを管理および監査する必要がある場合は、カスタマーマネージドキーを使用できます。

Amazon EventBridge を使用してアクセス AWS KMS 許可をオンボードする前に、管理 | AWS のサービス | セルフプロビジョニングサービス | (マネージドオートメーション) 変更タイプを使用して RFC をリクエストする必要があります。

## AMS SSP を使用して AMS アカウントに Amazon Forecast をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Forecast (Forecast) 機能に直接アクセスします。Amazon Forecast は、機械学習を使用して高精度の予測を提供するフルマネージドサービスです。

### Note

AWS は、2024 年 7 月 29 日に Amazon Forecast への新しい顧客アクセスを閉鎖しました。Amazon Forecast の既存のお客様は、通常どおりサービスを引き続き使用できます。AWS は引き続き Amazon Forecast のセキュリティ、可用性、パフォーマンスの向上に投資しますが、新機能を導入する予定 AWS はありません。

Amazon Forecast を使用する場合は、CSDM に連絡して、Amazon [Forecast の使用を Amazon SageMaker Canvas に移行する](#) 方法について詳しく説明してもらいます。

Amazon.com で使用されているのと同じテクノロジーに基づいて、Forecast は機械学習を使用して時系列データと追加の変数を組み合わせて予測を構築します。Forecast では、開始するために機械学習の経験は必要ありません。履歴データに加えて、予測に影響を与える可能性があると思われる追加データを提供するだけで済みます。例えば、シャツの特定の色の需要は、季節や店舗の場所によって変わる可能性があります。この複雑な関係を単独で判断することは困難ですが、機械学習はそれを認識するのに最適です。データを指定すると、Forecast はデータを自動的に調査し、意味のあるものを特定し、時系列データだけを見るよりも最大 50% 正確な予測を行うことができる予測モデルを生成します。

詳細については、「[Amazon Forecast](#)」を参照してください。

## AWS Managed Services での Amazon Forecast に関するよくある質問

Q: AMS アカウントの Forecast へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) change type を使用して RFC を送信 AWS Firewall Manager して、へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_forecast_admin_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントで Forecast を使用することにはどのような制限がありますか？

デフォルトの S3 バケットアクセスでは、「customer-forecast-\*」という名前のバケットにのみアクセスできます。データバケットの独自の命名規則がある場合は、Cloud Architect (CA) でバケットの命名と関連するアクセス設定について説明します。例:

- 「AmazonForecast-ExecutionRole-\*」などの名前と、関連する適切な S3 バケットアクセスを使用して、特定の Amazon Forecast サービスロールを定義できます。ExecutionRole S3 IAM コンソールの「サービスロール - AmazonForecast-ExecutionRole-Admin」および「IAM ポリシー - customer\_forecast\_default\_s3\_access\_policy」を参照してください。
- 関連する S3 バケットアクセスを IAM フェデレーションロールに関連付ける必要がある場合があります。IAM コンソールの「IAM ポリシー - customer\_forecast\_default\_s3\_access\_policy」を参照してください。

Q: AMS アカウントで Forecast を使用するための前提条件または依存関係は何ですか？

- Forecast を使用する前に、適切な Amazon S3 バケット (複数可) を作成する必要があります。特に、デフォルトの S3 バケットアクセスは命名パターン「customer-forecast-\*」です。



- 「customer-forecast-\*」以外の S3 バケットに命名パターンを使用する場合は、バケットに対する S3 アクセス許可を持つ新しいサービスロールを作成する必要があります。
  1. 「AmazonForecast-ExecutionRole-{suffix}」という名前で作成される新しいサービスロール。
  2. customer\_forecast\_default\_s3\_access\_policy に似ており、新しいサービスロールおよび関連するフェデレーション管理者ロール (「customer\_forecast\_admin\_role」など) に関連付けられている新しい IAM ポリシーを作成する

Q: Amazon Forecast の使用中にデータセキュリティを強化するにはどうすればよいですか？

- 保管中のデータ暗号化の場合、AWS KMS を使用してカスタマー管理の CMK をプロビジョニングし、Amazon S3 サービス上のデータストレージを保護できます。
- プロビジョニングキーを使用してバケットでデフォルトの暗号化を有効にし、データの配置中に AWS KMS データ暗号化を受け入れるようにバケットポリシーを設定します。
- AWS KMS キーユーザーとして Amazon Forecast サービスロール AmazonForecast-ExecutionRole-\* とフェデレーション管理者ロール (「customer\_forecast\_admin\_role」など) を有効にします。
- 転送中のデータ暗号化の場合、Amazon S3 バケットポリシーでオブジェクトを転送するときに必要な HTTPS プロトコルを設定できます。
- アクセスコントロールのさらなる制限により、Amazon Forecast サービスロール AmazonForecast-ExecutionRole-\* と管理者ロール (「customer\_forecast\_admin\_role」など) の承認済みアクセスのバケットポリシーを有効にします。

Q: Amazon Forecast を使用する際のベストプラクティスは何ですか？

- Amazon Forecast で S3 バケットを使用する際は、データ分類のプラクティスを十分に理解し、関連するデータセキュリティのニーズをマッピングする必要があります。
- Amazon S3 バケット設定では、S3 バケットポリシーで HTTPS 適用を有効にすることを強くお勧めします。
- Amazon S3 バケットに対する「customer-forecast\_admin\_role」サポートの管理者ロール「customer-forecast-\*」という名前のアクセス許可 (Get/Delete/Put Amazon S3 オブジェクト) に注意する必要があります。注: 複数のチームにきめ細かなアクセスコントロールが必要な場合は、次のプラクティスに従ってください。
- 関連する Amazon S3 バケットへの最小特権アクセスを持つチームベースのアクセス IAM ID (ロール/ユーザー) を定義します。

- チーム/プロジェクトベースの AWS KMS CMKs 対応する IAM ID への適切なアクセスが許可されます (ユーザーアクセスと AmazonForecast-ExecutionRole-{team/project})'。
- 作成した CMK を使用して S3 バケットのデフォルトの暗号化を設定します。AWS KMS CMKs
- S3 バケットポリシーで HTTPS プロトコルを使用して S3 API トラフィックを強制します。
- 関連する IAM ID (ユーザーアクセスと AmazonForecast-ExecutionRole-{team/project}) がバケットに承認されたアクセスのために S3 バケット設定を適用します。
- 汎用に「customer\_forecast\_admin\_role」を使用する場合は、前述のポイントを考慮して S3 バケットを保護します。

Q: Amazon Forecast に関するコンプライアンス情報はどこにありますか？

「[AWS サービスコンプライアンスプログラム](#)」を参照してください。

## AMS SSP を使用して AMS アカウントに Amazon FSx をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon FSx 機能に直接アクセスします。Amazon FSx は、フルマネージド型のサードパーティファイルシステムを提供します。Amazon FSx は、Windows ベースのストレージ、ハイパフォーマンスコンピューティング (HPC)、機械学習、電子設計自動化 (EDA) などのワークロード用の機能セットを備えたサードパーティのファイルシステムのネイティブ互換性を提供します。Amazon FSx は、ハードウェアのプロビジョニング、ソフトウェア設定、パッチ適用、バックアップなど、時間のかかる管理タスクを自動化します。Amazon FSx は、ファイルシステムをクラウドネイティブ AWS サービスと統合するため、より広範なワークロードのセットでさらに役立ちます。

Amazon FSx には、Windows ベースのアプリケーション用の Amazon FSx for Windows File Server と、コンピューティング負荷の高いワークロード用の Amazon FSx for Lustre の 2 つのファイルシステムがあります。詳細については、「[Amazon FSx](#)」を参照してください。

## AWS Managed Services での Amazon FSx に関するよくある質問

Q: AMS アカウントの Amazon FSx へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (ct-1w8z66n899dct) 変更タイプで RFC を送信して、Amazon FSx へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: customer\_fsx\_admin\_role。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon FSx の使用にはどのような制限がありますか？

制限はありません。サービスの完全な機能を利用できます。

Q: AMS アカウントで Amazon FSx を使用するための前提条件または依存関係は何ですか？

前提条件はありません。ただし、マルチ AZ などの事前設定を行うには、DFS レプリケーションおよび DFS 名前空間サービスをインストールおよび管理する必要があります。詳細については、[「マルチ AZ ファイルシステムのデプロイ」](#)を参照してください。

Q: Amazon FSx ファイルシステムをマルチアカウントランディングゾーン Managed AD と統合するにはどうすればよいですか？

Amazon FSx ファイルシステムを作成するときは、MALZ Managed AD を Windows 認証用のAWS「マネージド Microsoft Active Directory」として指定できます。詳細については、[「Microsoft Active Directory での Amazon FSx の使用 AWS Directory Service」](#)を参照してください。

また、最初に Managed AD をアプリケーションアカウントと共有する必要があります。これを行うには、Management | Directory Service | Directory | Share directory change type (ct-369odask0pd9w)を使用して RFC を送信します。

Q: AWS 委任 FSx 管理者グループに属するユーザーはどれですか？

IT ファイルサーバー管理者のみ。このグループには、すべてのファイル共有に対するフルアクセス権限があります。

Q: FSx システムがプロビジョニングされたときに作成されるデフォルトのファイル共有、共有を使用する必要がありますか？

いいえ。プロビジョニングされたデフォルトのファイル共有、共有を使用することはお勧めしません。最小特権の原則に違反するフルアクセスをすべてのユーザーに付与します。代わりに、ビジネスニーズに合った小さなカスタムファイル共有を作成します。

Q: ビジネス内の特定の組織のカスタムファイル共有を作成するにはどうすればよいですか？

カスタム[ファイル共有の作成手順](#)については、「ファイル共有」を参照してください。最小特権の原則を使用して、各ファイル共有へのアクセスを制限します。

## AMS SSP を使用して AMS アカウントで Amazon FSx for OpenZFS をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon FSx for OpenZFS 機能に直接アクセスします。FSx for OpenZFS は、フルマネージド型のファイルストレージサービスです。これにより、アプリケーションコードやデータ管理方法を変更することなく、オンプレミスの ZFS やその他の Linux ベースのファイルサーバーにあるデータを AWS に簡単に移動できます。オープンソースの OpenZFS ファイルシステム上に構築された、信頼性、スケーラビリティ、パフォーマンス、機能豊富なファイルストレージを提供し、OpenZFS ファイルシステムの使い慣れた機能と機能に、フルマネージド AWS サービスの俊敏性、スケーラビリティ、シンプルさを提供します。クラウドネイティブアプリケーションを構築するデベロッパー向けに、データを操作するための豊富な機能を備えたシンプルで高性能なストレージを提供します。

FSx for OpenZFS ファイルシステムは、業界標準の NFS プロトコル (v3、v4.0、v4.1、v4.2) を使用して、Linux、Windows、macOS コンピューティングインスタンスおよびコンテナから広くアクセスできます。Graviton AWS プロセッサと最新の AWS ディスクおよびネットワークテクノロジー (AWS スケーラブルな信頼性の高い Datagram ネットワークと AWS Nitro システムを含む) を搭載した FSx for OpenZFS は、数百マイクロ秒のレイテンシーで最大 100 万 IOPS を提供します。FSx for OpenZFS は、インスタンtpoint-in-timeスナップショットやデータクローン作成などの OpenZFS 機能を完全にサポートしているため、オンプレミスのファイルサーバーを使い慣れたファイルシステム機能を提供する AWS ストレージに簡単に置き換えることができます。これにより、長時間の認定や既存のアプリケーションやツールの変更や再設計を行う必要がなくなります。OpenZFS また、OpenZFS データ管理機能の能力と最新の AWS テクノロジーの高パフォーマンスとコスト効率を組み合わせることで、FSx for OpenZFS では、高性能でデータ集約型のアプリケーションを構築して実行できます。

フルマネージドサービスである FSx for OpenZFS を使用すると、オンプレミスで実行しているファイルサーバーを置き換え AWS のフルマネージドファイルシステムの起動、実行、スケーリングが簡単になり、俊敏性とコスト削減に役立ちます。FSx for OpenZFS を使用すると、ファイルサーバーとストレージボリュームのセットアップとプロビジョニング、データのレプリケーション、ファイルサーバーソフトウェアのインストールとパッチ適用、ハードウェア障害の検出と対処、バックアップの手動実行について心配する必要がなくなりました。また、AWS Identity and Access Management (IAM)、AWS Key Management Service ()、AWS KMS Amazon CloudWatch、などの他の AWS サービスとの豊富な統合も提供します AWS CloudTrail。

Amazon FSx には、Windows ベースのアプリケーション用の Amazon FSx for Windows File Server と、コンピューティング負荷の高いワークロード用の Amazon FSx for Lustre の 2 つのファイルシステムがあります。詳細については、[「Amazon FSx」](#)を参照してください。

## AWS Managed Services での Amazon FSx for OpenZFS に関するよくある質問

Q: AMS アカウントで FSx for OpenZFS を使用するためのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) 変更タイプで RFC を送信して、Amazon FSx OpenZFS へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_fsx_ontap_admin_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントで FSx for OpenZFS を使用することにはどのような制限がありますか？

Amazon FSx Elastic Network Interface (ENIs) のセキュリティグループを置き換えるには、管理 | その他 | その他 | RFCs を更新する必要があります。これは、セキュリティグループが AMS 環境にとって重要な境界であるためです。これが唯一の制限です。

Q: AMS アカウントで FSx for OpenZFS を使用するための前提条件または依存関係は何ですか？

前提条件はありません。ただし、[AMS SSP を使用して AMS アカウントに Amazon FSx をプロビジョニングする](#)がインストールされている必要があります。

## AMS SSP を使用して AMS アカウントで Amazon FSx for NetApp ONTAP をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon FSx for NetApp ONTAP 機能に直接アクセスします。Amazon FSx for NetApp ONTAP は、NetApp の人気ある ONTAP ファイルシステム上に構築された、高い信頼性、拡張性、パフォーマンス、機能豊富なファイルストレージを提供するフルマネージド型サービスです。NetApp ファイルシステムの使い慣れた機能、パフォーマンス、機能、APIs に、フルマネージド型の俊敏性、スケーラビリティ、シンプルさを提供します AWS のサービス。

Amazon FSx for NetApp ONTAP は、AWS またはオンプレミスで実行されている Linux、Windows、macOS コンピューティングインスタンスから幅広くアクセスできる、機能豊富で高速、柔軟な共有ファイルストレージを提供します。FSx for ONTAP は、ミリ秒未満のレイテンシーを備えた高性能 SSD ストレージを提供し、ボタンをクリックするだけでファイルのスナップショット作成、クローン作成、複製を行えるため、データをすばやく簡単に管理できます。また、データを低コストで伸縮性のあるストレージに自動的に階層化することで、容量のプロビジョニングや管理が不要になり、ごく一部のデータに対して SSD ストレージの費用を支払うのみで、ワークロードに対して SSD レベルのパフォーマンスを実現することができます。フルマネージドバック



アップとクロスリージョン災害対策のサポートにより、可用性と耐久性に優れたストレージを提供し、一般的なデータセキュリティおよびアンチウイルスアプリケーションをサポートし、データの保護とセキュリティをさらに容易にします。NetApp ONTAP をオンプレミスで使用するお客様にとって、FSx for ONTAP は、アプリケーションコードやデータの管理方法を変更 AWS することなく、ファイルベースのアプリケーションをオンプレミスからに移行、バックアップ、またはバーストするための理想的なソリューションです。

フルマネージドサービスとして、Amazon FSx for NetApp ONTAP は、クラウドでの信頼性、パフォーマンス、安全な共有ファイルストレージを簡単に起動および拡張できます。Amazon FSx for NetApp ONTAP を使用すると、ファイルサーバーとストレージボリュームの設定とプロビジョニング、データのレプリケーション、ファイルサーバーソフトウェアのインストールとパッチ適用、ハードウェア障害の検出と対応、フェイルオーバーとフェイルバックの管理、バックアップの手動実行について心配する必要がなくなります。また、Amazon WorkSpaces AWS のサービスや AWS Identity and Access Management など AWS Key Management Service、他の どの豊富な統合も提供します AWS CloudTrail。

Amazon FSx には、Windows ベースのアプリケーション用の Amazon FSx for Windows File Server と、コンピューティング負荷の高いワークロード用の Amazon FSx for Lustre の 2 つのファイルシステムがあります。詳細については、[「Amazon FSx」](#)を参照してください。

## AWS Managed Services での Amazon FSx for NetApp ONTAP に関するよくある質問

Q: AMS アカウントで Amazon FSx for NetApp ONTAP へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (ct-1w8z66n899dct) 変更タイプで RFC を送信して、Amazon FSx for NetApp ONTAP へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_fsx_ontap_admin_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントで Amazon FSx for NetApp ONTAP を使用することにはどのような制限がありますか？

Amazon FSx for NetApp ONTAP Elastic Network Interface (ENIs) のセキュリティグループを置き換えるには、管理 | その他 | その他 | RFCs を更新する必要があります。これは、セキュリティグループが AMS 環境にとって重要な境界であるためです。これが唯一の制限です。

Q: AMS アカウントで Amazon FSx for NetApp ONTAP を使用する際の前提条件または依存関係は何ですか？

前提条件はありません。ただし、[AMS SSP を使用して AMS アカウントに Amazon FSx をプロビジョニングする](#)がインストールされている必要があります。

## AMS SSP を使用して AMS アカウントに Amazon Inspector Classic をプロビジョニングする

### Note

サポート終了通知: 2026 年 5 月 20 日に、AWS は Amazon Inspector Classic のサポートを終了します。2026 年 5 月 20 日以降、Amazon Inspector Classic コンソールまたは Amazon Inspector Classic リソースにアクセスできなくなります。Amazon Inspector Classic は、新しいアカウント、および過去 6 か月間に評価を完了していないアカウントで利用できなくなります。他のすべてのアカウントでは、アクセスは 2026 年 5 月 20 日まで有効です。その後、Amazon Inspector Classic コンソールまたは Amazon Inspector Classic リソースにアクセスできなくなります。詳細については、[Amazon Inspector Classic のサポート終了](#)」を参照してください。

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Inspector Classic 機能に直接アクセスします。Amazon Inspector Classic は、デプロイされたアプリケーションのセキュリティとコンプライアンスの向上に役立つ自動セキュリティ評価サービスです。AWS。Amazon Inspector Classic は、アプリケーションの露出、脆弱性、ベストプラクティスからの逸脱を自動的に評価します。評価を実行すると、Amazon Inspector Classic は重要度レベル別に優先順位が付けられたセキュリティ検出結果の詳細なリストを作成します。これらの検出結果は、直接レビューすることも、Amazon Inspector Classic コンソールまたは API から入手できる詳細な評価レポートの一部としてレビューすることもできます。詳細については、[Amazon Inspector Classic](#)」を参照してください。

### AWS Managed Services の Amazon Inspector に関するよくある質問

Q: AMS アカウントで Amazon Inspector Classic へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) 変更タイプで RFC を送信して、Amazon Inspector Classic へのアクセスをリクエストします。この RFC は、IAM `customer_inspector_admin_role` ロールをアカウントにプロビジョニングします。ロールには AWS、管理の `AmazonInspectorFullAccess` ポリシーが含まれます。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。



Q: AMS アカウントでの Amazon Inspector Classic の使用にはどのような制限がありますか？

制限はありません。Amazon Inspector Classic の完全な機能は、AMS アカウントで使用できます。

Q: AMS アカウントで Amazon Inspector Classic を使用するための前提条件または依存関係は何ですか？

AMS アカウントで Amazon Inspector Classic を使用するための前提条件や依存関係はありません。

## AMS で新しい Amazon Inspector を使用する

AMS アカウントで新しい Amazon Inspector を使用できるようになりました。

Amazon Inspector Classic では、`customer-inspector-admin-role-ssm-inspector-agent-policy`と `AmazonInspectorFullAccess`が必要でした。ただし、SSPS ロールが更新され`customer-inspector-admin-role`、追加の `AmazonInspector2FullAccess`が含まれるようになりました。この新しいポリシーは、Amazon Inspector の新しいバージョンの API アクセス許可を付与します。

## AMS SSP を使用して AMS アカウントに Amazon Kendra をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Kendra 機能に直接アクセスします。Amazon Kendra は、自然言語処理と高度な機械学習アルゴリズムを使用して、データからの検索質問に対する特定の回答を返すインテリジェントな検索サービスです。従来のキーワードベースの検索とは異なり、Amazon Kendra はセマンティックおよびコンテキスト理解機能を使用して、ドキュメントが検索クエリに関連しているかどうかを判断します。Amazon Kendra は質問に対する特定の回答を返すため、エクスペリエンスは人間の専門家とのやり取りに近いです。Amazon Kendra はスケーラビリティが高く、パフォーマンスの需要を満たすことができ、Amazon S3 や Amazon Lex などの他の AWS サービスと緊密に統合されており、エンタープライズレベルのセキュリティを提供します。詳細については、[「Amazon Kendra」](#)を参照してください。

## AWS Managed Services の Amazon Kendra に関するよくある質問

Q: AMS アカウントの Amazon Kendra へのアクセスをリクエストするにはどうすればよいですか？

Amazon Inspector Classic へのアクセスをリクエストするには、`Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny)` 変更タイプを使用して RFC を送信します。この RFC

は、IAM `customer_kendra_console_role` ロールをアカウントにプロビジョニングします。アカウントでプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon Kendra の使用にはどのような制限がありますか？

制限はありません。Amazon Kendra の完全な機能は、AMS アカウントで使用できます。

Q: AMS アカウントで Amazon Kendra を使用するための前提条件または依存関係は何ですか？

Amazon Kendra の使用を開始するための前提条件や依存関係はありません。ただし、特定のユースケースによっては、他の AWS サービスへのアクセスが必要になる場合があります。

## AMS SSP を使用して AMS アカウントに Amazon Kinesis Data Streams をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Kinesis Data Streams (KDS) 機能に直接アクセスします。Amazon Kinesis Data Streams は、スケーラビリティと耐久性に優れたリアルタイムのデータストリーミングサービスです。KDS は、ウェブサイトのクリックストリーム、データベースイベントストリーム、金融取引、ソーシャルメディアフィード、IT ログ、位置追跡イベントなど、数十万のソースから 1 秒あたり数ギガバイトのデータを継続的にキャプチャできます。収集されたデータはミリ秒単位で利用でき、リアルタイムダッシュボード、リアルタイム異常検出、動的料金設定などのリアルタイム分析のユースケースを可能にします。詳細については、[Amazon Kinesis Data Streams](#)」を参照してください。

## AWS Managed Services での Kinesis Data Streams に関するよくある質問

よくある質問と回答：

Q: AMS アカウントの Amazon Kinesis Data Streams へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 変更タイプを追加 (ct-1w8z66n899dct) で RFC を送信して、Amazon Kinesis Data Streams へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします：  
`customer_kinesis_data_streaming_user_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon Kinesis Data Streams の使用にはどのような制限がありますか？

制限はありません。Amazon Kinesis Data Streams のフル機能は、AMS アカウントで使用できません。

Q: AMS アカウントで Amazon Kinesis Data Streams を使用するための前提条件または依存関係は何か？

AMS アカウントで Amazon Kinesis Data Streams を使用するための前提条件や依存関係はありません。

## AMS SSP を使用して AMS アカウントに Amazon Kinesis Video Streams をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Kinesis Video Streams (KVS) 機能に直接アクセスします。Amazon Kinesis Video Streams を使用すると、接続されたデバイスからビデオを安全にストリーミングして、AWS 分析、機械学習 (ML)、再生、その他の処理を行うことができます。Kinesis Video Streams は、何百万ものデバイスからストリーミングビデオデータを取り込むために必要なすべてのインフラストラクチャを自動的にプロビジョニングし、伸縮自在にスケールリングします。また、ビデオデータをストリームに永続的に保存、暗号化、インデックス化し、easy-to-use APIs を通じてデータにアクセスできます。Kinesis Video Streams を使用すると、ライブおよびオンデマンド視聴用のビデオを再生し、Amazon Rekognition Video との統合、および Apache MxNet、TensorFlow、OpenCV などの ML フレームワーク用のライブラリを通じて、コンピュータビジョンとビデオ分析を活用するアプリケーションをすばやく構築できます。詳細については、[Amazon Kinesis Video Streams](#)」を参照してください。

## AWS Managed Services での Amazon Kinesis Video Streams に関するよくある質問

一般的な質問と回答：

Q: AMS アカウントの Amazon Kinesis Video Streams へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 変更タイプを追加 (ct-1w8z66n899dct) で RFC を送信して、Amazon Kinesis Video Streams へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします：customer\_kinesis\_video\_streaming\_user\_role。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon Kinesis Video Streams の使用にはどのような制限がありますか？

制限はありません。Amazon Kinesis Video Streams のフル機能は、AMS アカウントで使用できます。

Q: AMS アカウントで Amazon Kinesis Video Streams を使用するための前提条件または依存関係は何ですか？

AMS アカウントで Amazon Kinesis Video Streams を使用するための前提条件や依存関係はありません。

## AMS SSP を使用して AMS アカウントに Amazon Lex をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Lex 機能に直接アクセスします。Amazon Lex は、音声とテキストを使用して会話型インターフェイスを任意のアプリケーションに構築するためのサービスです。Amazon Lex は、音声をテキストに変換するための自動音声認識 (ASR) の高度な深層学習機能と、テキストの意図を認識するための自然言語理解 (NLU) を提供し、非常に魅力的なユーザーエクスペリエンスとリアルな会話インタラクションでアプリケーションを構築できるようにします。Amazon Lex では、Amazon Alexa を強化するのと同じ深層学習テクノロジーをすべての開発者が利用できるようになりました。これにより、洗練された自然言語の会話ボットやチャットボットを迅速かつ簡単に構築できます。詳細については、[Amazon Lex](#) を参照してください。

## AWS Managed Services の Amazon Lex に関するよくある質問

一般的な質問と回答：

Q: AMS アカウントの Amazon Lex へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add change type (ct-1w8z66n899dct) を送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_lex_author_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon Lex の使用にはどのような制限がありますか？

Amazon Lex と Lambda の統合は、AMS インフラストラクチャへの変更を防ぐために、「AMS-」プレフィックスのない Lambda 関数に制限されています。

Q: AMS アカウントで Amazon Lex を使用するための前提条件または依存関係は何ですか？

AMS アカウントで Amazon Lex を使用するための前提条件や依存関係はありません。

# AMS SSP を使用して AMS アカウントに Amazon MQ をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon MQ 機能に直接アクセスします。Amazon MQ は Apache ActiveMQ のマネージドメッセージブローカーサービスで、クラウドでのメッセージブローカーのセットアップと運用に役立ちます。メッセージブローカーを使用すると、多くの場合、異なるプログラミング言語と異なるプラットフォームで異なるソフトウェアシステムを使用して、情報を通信および交換できます。Amazon MQ は、一般的なオープンソースメッセージブローカーである ActiveMQ のプロビジョニング、セットアップ、メンテナンスを管理することで、運用負荷を軽減します。現在のアプリケーションを Amazon MQ に接続すると、JMS、NMS、AMQP、STOMP、MQTT、WebSocket などの業界標準 APIs とプロトコルがメッセージングに使用されます。標準を使用すると、ほとんどの場合、移行時にメッセージングコードを書き直す必要はありません AWS。詳細については、[Amazon MQ とは](#)」を参照してください。

## AWS Managed Services の Amazon MQ に関するよくある質問

一般的な質問と回答：

Q: AMS アカウントの Amazon MQ へのアクセスをリクエストするにはどうすればよいですか？

AMS アカウントでの Amazon MQ の使用には、2 つのステップがあります。

1. Amazon MQ ブローカーをプロビジョニングします。これを行うには、Amazon MQ ブローカーを含む CFN テンプレートを、デプロイ | Ingestion | Stack from CloudFormation Template | Create change type (ct-36cn2avfrj9v) の RFC を介して送信するか、Management | Other | Other | Create change type (ct-1e1xtak34nx76) change type を使用して RFC を送信して Amazon MQ ブローカーをアカウントにプロビジョニングするようにリクエストします。
2. Amazon MQ コンソールにアクセスします。Amazon MQ ブローカーがプロビジョニングされたら、管理 | AWS サービス | セルフプロビジョニングサービス | 変更タイプを追加 (ct-1w8z66n899dct) で RFC を送信して Amazon MQ コンソールへのアクセスを取得します。この RFC は、アカウントに次の IAM ロールをプロビジョニングします：  
customer\_mq\_console\_role。

アカウントにロールがプロビジョニングされたら、フェデレーションソリューションにロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon MQ の使用にはどのような制限がありますか？



Amazon MQ の完全な機能は AMS アカウントで使用できますが、必要なアクセス許可が昇格しているため、ポリシーを通じて Amazon MQ ブローカーをプロビジョニングすることはできません。アカウントで Amazon MQ ブローカーをプロビジョニングする方法の詳細については、上記を参照してください。

Q: AMS アカウントで Amazon MQ を使用する際の前提条件または依存関係は何ですか？

AMS アカウントで Amazon MQ を使用するための前提条件や依存関係はありません。

## AMS SSP を使用して AMS アカウントで Amazon Managed Service for Apache Flink をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Managed Service for Apache Flink 機能に直接アクセスします。Managed Service for Apache Flink は、ストリーミングデータを分析し、実用的なインサイトを取得し、ビジネスと顧客のニーズにリアルタイムで対応するための最も簡単な方法です。Amazon Managed Service for Apache Flink は、ストリーミングアプリケーションの構築、管理、他の AWS サービスとの統合の複雑さを軽減します。SQL ユーザーは、テンプレートとインタラクティブな SQL エディタを使用して、ストリーミングデータのクエリやストリーミングアプリケーション全体の構築を簡単に行うことができます。Java 開発者は、オープンソースの Java ライブラリと AWS 統合を使用して高度なストリーミングアプリケーションをすばやく構築し、データをリアルタイムで変換および分析できます。Amazon Managed Service for Apache Flink は、リアルタイムアプリケーションを継続的に実行するために必要なすべてを処理し、受信データのボリュームとスループットに合わせて自動的にスケールリングします。Amazon Managed Service for Apache Flink では、ストリーミングアプリケーションが消費するリソースに対してのみ料金が発生します。最低料金やセットアップ料金はかかりません。詳細については、[「Amazon Managed Service for Apache Flink」](#)を参照してください。

## AWS Managed Services の「Managed Service for Apache Flink」に関するよくある質問

一般的な質問と回答:

Q: AMS アカウントの Amazon Managed Service for Apache Flink へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (マネージドオートメーション) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします:

customer\_kinesis\_analytics\_application\_role。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントで Amazon Managed Service for Apache Flink を使用する際の制限は何ですか？

- AMS インフラストラクチャへの変更を防ぐため、設定は「AMS-」または「MC-」プレフィックスのないリソースに限定されます。
- 新しい Kinesis Data Streams または Firehose を削除または作成するアクセス許可がポリシーから削除されました。これを許可する別のポリシーがあります。

Q: AMS アカウントで Amazon Kinesis Data Streams を使用するための前提条件または依存関係は何ですか？

いくつかの依存関係があります。

- Amazon Managed Service for Apache Flink では、Managed Service for Apache Flink でアプリケーションを設定する前に、Kinesis Data Streams または Firehose を作成する必要があります。
- リソースベースのポリシーのアクセス許可は、特定の入力データソースを示す必要があります。

## AMS SSP を使用して AMS アカウントに Amazon Managed Streaming for Apache Kafka をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Managed Streaming for Apache Kafka (Amazon MSK) 機能に直接アクセスします。Amazon Managed Streaming for Apache Kafka は、フルマネージド型の AWS ストリーミングデータサービスです。これにより、Apache Kafka クラスターの運用に関するエキスパートになることなく、Apache Kafka を使用してストリーミングデータを処理するアプリケーションを簡単に構築および実行できます。Amazon MSK は、Apache Kafka クラスターと Apache ZooKeeper ノードのプロビジョニング、設定、メンテナンスを管理します。Amazon MSK は AWS、コンソールに主要な Apache Kafka パフォーマンスメトリクスも表示します。

Amazon MSK は、VPC ネットワークの分離、コントロールプレーン API 認可のための AWS IAM、保管時の暗号化、転送中の TLS 暗号化、TLS ベースの証明書認証、で保護された SASL/SCRAM 認証など、Apache Kafka クラスターに複数のレベルのセキュリティを提供します AWS Secrets Manager。詳細については、[「Amazon MSK」](#)を参照してください。



## AWS Managed Services での Amazon MSK に関するよくある質問

一般的な質問と回答:

Q: AMS アカウントの Amazon MSK へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (マネージドオートメーション) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、次の IAM ポリシーとロールをアカウントにプロビジョニングします。

- customer-msk-admin-policy.json
- AmazonMSKFullAccess
- customer-msk-admin-role.json

アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: Amazon MSK の使用にはどのような制限がありますか？

Amazon MSK が設定した宛先にブローカーログを配信するには、AmazonMSKFullAccess ポリシーが IAM ロールに添付されていることを確認してください。そのため、フルアクセス許可はすでに設定されています。

Q: Amazon MSK を使用する際の前提条件または依存関係は何ですか？

MSK クラスターを作成する前に、その VPC 内に VPC とサブネットが必要です。デフォルトでは、AMS はこれをデフォルトの [AMS VPC 作成](#) の一部として扱います。

Amazon MSK の制限については、[「Amazon MSK の制限」](#) を参照してください。

## AMS SSP を使用して AMS アカウントで Amazon Managed Service for Prometheus をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Managed Service for Prometheus (AMP) 機能に直接アクセスします。Amazon Managed Service for Prometheus は、コンテナメトリクスをモニタリングするためのサーバーレスの Prometheus 互換のサービスであり、コンテナ環境の大規模かつ安全なモニタリングを簡単に行えるようになります。Amazon Managed Service for Prometheus では、現在使用されているものと同じオープンソースの Prometheus データモデルとクエリ言語を使用して、コンテナ化されたワーク

ロードのパフォーマンスをモニタリングできます。また、基盤のインフラストラクチャを管理する必要なく、スケーラビリティ、可用性、セキュリティを強化できます。

Amazon Managed Service for Prometheus は、ワークロードのスケールアップとスケールダウンに応じて、運用メトリクスの取り込み、ストレージ、クエリを自動的にスケーリングします。これは AWS セキュリティサービスと統合され、データへの高速で安全なアクセスを可能にします。詳細については、[「Amazon Managed Service for Prometheus とは」を参照してください。](#)

## AWS Managed Services での Amazon Managed Service for Prometheus に関するよくある質問

一般的な質問と回答:

Q: AMS アカウントで Amazon Managed Service for Prometheus へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (マネージドオートメーション) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer-prometheus-console-role`。アカウントにプロビジョニングされたら、フェデレーションソリューションで `customer-prometheus-console-role` ロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon Managed Service for Prometheus の使用にはどのような制限がありますか？

すべての機能がサポートされています。

Q: AMS アカウントで Amazon Managed Service for Prometheus を使用するための前提条件または依存関係は何ですか？

Amazon Managed Service for Prometheus の使用を開始するための前提条件や依存関係はありません。ただし、特定のユースケースによっては、他の AWS サービスへのアクセスが必要になる場合があります。

## AMS SSP を使用して AMS アカウントに Amazon Personalize をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Personalize 機能に直接アクセスします。Amazon Personalize は、開発者がアプリケーション

ンを使用する顧客向けに個別のレコメンデーションを簡単に作成できるようにする機械学習サービスです。

機械学習は、パーソナライズされた製品とコンテンツのレコメンデーション、カスタマイズされた検索結果、ターゲットを絞ったマーケティングプロモーションを強化することで、カスタマーエンゲージメントを向上させるためにますます使用されています。ただし、これらの高度なレコメンデーションシステムを生成するために必要な機械学習機能の開発は、複雑さのため、現在のほとんどの組織の手の届かないところにあります。Amazon Personalize を使用すると、これまで機械学習の経験がない開発者は、Amazon.com で長年使用されていた機械学習テクノロジーを使用して、アプリケーションに高度なパーソナライゼーション機能を簡単に構築できます。

Amazon Personalize では、クリック、ページビュー、サインアップ、購入など、アプリケーションからのアクティビティストリームと、記事、製品、動画、音楽などの推奨アイテムのインベントリを提供します。年齢や位置情報などのユーザーの人口統計情報を Amazon Personalize に提供することもできます。Amazon Personalize は、データの処理と調査、意味のあるものの特定、適切なアルゴリズムの選択、データに合わせてカスタマイズされたパーソナライゼーションモデルのトレーニングと最適化を行います。Amazon Personalize が分析したすべてのデータについては、プライバシーとセキュリティが確保され、お客様に合わせたレコメンデーションの提供にのみ使用されます。シンプルな API コールを使用して、パーソナライズされたレコメンデーションの提供を開始できます。使用した分だけ料金が発生します。最低料金や初期費用は不要です。

詳細については、[「Amazon Personalize」](#) を参照してください。

## AWS Managed Services での Amazon Personalize に関するよくある質問

Q: AMS アカウントで Amazon Personalize へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (マネージドオートメーション) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。また、AWS パーソナライズによってレコメンデーションの生成に使用されるデータを含む S3 バケットを指定する必要があります。この RFC は、customer\_personalize\_console\_role および の IAM ロールをアカウントにプロビジョニングします customer\_personalize\_service\_role。

- アカウントで customer\_personalize\_console\_role がプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。以外の既存のロール customer\_personalize\_console\_policy に をアタッチすることもできます Customer\_ReadOnly\_Role。

- `customer_personalize_service_role` がアカウントに提供されたら、新しいデータセットグループを作成するときに ARN を参照できます。

この時点で、AMS Operations はこのサービスロールをアカウント にもデプロイします `aws_code_pipeline_service_role_policy`。

Q: AMS アカウントでの Amazon Personalize の使用にはどのような制限がありますか？

Amazon Personalize の設定は、AMS インフラストラクチャへの変更を防ぐために、「ams-」または「mc-」プレフィックスのないリソースに限定されます。

Q: AMS アカウントで Amazon Personalize を使用する際の前提条件または依存関係は何ですか？

- データが保存されている S3 バケットが暗号化されている場合、Amazon Personalize がバケットを復号化するために使用するロールを許可できるように、KMS キー ID を指定する必要があります。

Amazon Personalize は、デフォルトの KMS S3 キーをサポートしていません。KMS を使用する必要がある場合は、カスタムキーを作成し、変更タイプ KMS キー | 作成 (マネージドオートメーション) の RFC を開いて次のポリシーを追加します。

JSON

```
{
  "Version": "2012-10-17",
  "Id": "key-consolepolicy-3",
  "Statement": [
    {
      "Sid": "Enable IAM User Permissions",
      "Effect": "Allow",
      "Principal": {
        "Service": "personalize.amazonaws.com"
      },
      "Action": "kms:*",
      "Resource": "*"
    }
  ]
}
```

- S3 バケットは、次のバケットポリシーを使用して作成する必要があります。これを行うには、変更タイプ S3 ストレージ | ポリシーの作成で RFC を送信します。このポリシーは、Amazon

Personalize がデータにアクセスすることを許可します。そのバケットには、Amazon Personalize が使用するデータが含まれます。

JSON

```
{
  "Version": "2012-10-17",
  "Id": "PersonalizeS3BucketAccessPolicy",
  "Statement": [
    {
      "Sid": "PersonalizeS3BucketAccessPolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "personalize.amazonaws.com"
      },
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::bucket-name",
        "arn:aws:s3:::bucket-name/*"
      ]
    }
  ]
}
```

## AMS SSP を使用して AMS アカウントに Amazon Quick をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントでクイック機能に直接アクセスします。Quick は、組織内のすべてのユーザーにインサイトを提供する、高速でクラウドを活用したビジネスインテリジェンスサービスです。フルマネージドサービスである Quick を使用すると、機械学習 (ML) インサイトを含むインタラクティブなダッシュボードを簡単に作成して公開できます。詳細については、[「Amazon Quick」](#) を参照してください。

### AWS Managed Services クイックに関するよくある質問

一般的な質問と回答:

Q: AMS アカウントの Quick へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add change type (ct-1w8z66n899dct) を送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_quicksight_console_admin_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Quick の使用にはどのような制限がありますか？

- AWS Quick の リソース設定には、IAM ポリシーの依存関係のためアクセスできません。ただし、AMS チームはリクエストに応じて各リソースを有効にし、サービスを有効にします。
- この機能により、ユーザーは AMS インフラストラクチャを侵害する可能性のある IAM アクセス許可を変更できるため、個々のユーザーとグループのリソースアクセスはこのモデルではサポートされていません。
- QuickSight 内から IAM アイデンティティを招待する機能は、IAM オブジェクトの変更に伴うリスクのためサポートされていません。
- クイックサービスには、Enterprise と Standard の 2 つのエディションがあります。どちらも、AMS でサポートされているシングルサインオン (SSO) オプションを提供します。ただし、Enterprise Edition には、Quick と Active Directory (AD) を統合するオプションがあります。AMS のクイックは、AMS アカウント構造とクイック信頼要件との互換性がないため、AD との統合をサポートしていません。

Q: AMS アカウントで Quick を使用するための前提条件または依存関係は何ですか？

- AMS がこの RFC を受信して Quick を追加すると、追加情報のサービスリクエストが送信され、以下を提供します。
  - クイックアカウント名 (例: *CustomerName*-quicksight)
  - Quick Edition (Standard と Enterprise)
  - クイックサービスを有効にする AWS リージョン (デフォルトは AMS AWS リージョン)。
  - クイックアカウントの通知 E メールアドレス。
  - (オプション) 分析するデータファイルがある S3 バケット。
  - Quick に接続する VPC とサブネット IDs は、VPC 接続を追加する機能をサポートしています。これにより、Quick とアカウント内のリソース間のプライベート接続が可能になります。

AMS オペレーターは、ユーザーに代わってサインアッププロセスを実行し、2 つの QuickSight 機能を設定します。

- データソースへの[自動検出](#)。
- [VPC 接続](#)。

#### Note

これらのアクションは、サインインプロセス中に昇格された IAM および VPC アクセス許可が必要なため、AMS オペレーターが実行する必要があります。

## AMS SSP を使用して AMS アカウントに Amazon Rekognition をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Rekognition 機能に直接アクセスします。Amazon Rekognition を使用すると、機械学習の専門知識を必要としない、実証済みの高度にスケーラブルな深層学習テクノロジーを使用して、アプリケーションにイメージ分析とビデオ分析を簡単に追加できます。Amazon Rekognition を使用すると、イメージやビデオ内のオブジェクト、人物、テキスト、シーン、アクティビティを特定し、不適切なコンテンツを検出できます。Amazon Rekognition は、高精度の顔分析および顔検索機能も提供しており、ユーザー認証、人数カウント、公共安全など、幅広いユースケースで顔を検出、分析、比較できます。

Amazon Rekognition Custom Labels を使用すると、ビジネスニーズに固有のイメージ内のオブジェクトやシーンを特定できます。例えば、アセンブリライン上の特定の機械部品を分類したり、育ちの悪い植物を検出したりするモデルを構築できます。Amazon Rekognition Custom Labels はモデル開発の面倒な作業を処理するため、機械学習の経験は必要ありません。識別するオブジェクトまたはシーンの画像を提供するだけで、サービスが残りの作業を処理します。

詳細については、[Amazon Rekognition](#)」を参照してください。

## AWS Managed Services の Amazon Rekognition に関するよくある質問

一般的な質問と回答:

Q: AMS アカウントで Amazon Rekognition へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (マネージドオートメーション)  
(ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、アカウント



トに次の IAM ロールをプロビジョニングします: `customer_rekognition_console_role` & `customer_rekognition_service_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon Rekognition の使用にはどのような制限がありますか？

Amazon Rekognition の完全な機能は、Amazon Rekognition の自己プロビジョニング型サービスロールで使用できます。

Q: AMS アカウントで Amazon Rekognition を使用するための前提条件または依存関係は何ですか？

Amazon Rekognition Video ストリームプロセッサまたはデータストリームのソースストリーミングビデオを提供する Kinesis Video Streams を Kinesis Data Streams にデータを書き込む送信先として使用する場合は、RFC の作成 `kinesisStreamName` 時に AMS に を提供してください。

## AMS SSP を使用して AMS アカウントに Amazon SageMaker AI をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon SageMaker AI 機能に直接アクセスします。SageMaker AI は、すべての開発者とデータサイエンティストに、機械学習モデルを迅速に構築、トレーニング、デプロイする機能を提供します。Amazon SageMaker AI は、データのラベル付けと準備、アルゴリズムの選択、モデルのトレーニング、デプロイのための調整と最適化、予測、アクションを実行するための機械学習ワークフロー全体をカバーするフルマネージドサービスです。モデルは、はるかに少ない労力と低コストで本番環境に迅速に移行できます。詳細については、[Amazon SageMaker AI](#)」を参照してください。

## AWS Managed Services での SageMaker AI に関するよくある質問

一般的な質問と回答:

Q: AMS アカウントの SageMaker AI へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) change type を送信してアクセスをリクエストします。この RFC は、IAM ロール `customer_sagemaker_admin_role` とサービスロール をアカウントにプロビジョニングします AmazonSageMaker-ExecutionRole-Admin。SageMaker AI がアカウントにプロビジョニングされたら、フェデレーションソリューションで `customer_sagemaker_admin_role` ロールをオンボードする必要があります。サービスロールに直接アクセスすることはできません。SageMaker AI サービスは、「[ロールの受け渡し](#)」で説明されているように、[さまざまなアクションを実行する際にサービスロール](#)を使用します。

Q: AMS アカウントでの SageMaker AI の使用にはどのような制限がありますか？

- AMS Amazon SageMaker AI IAM ロールでは、次のユースケースはサポートされていません。
  - SageMaker AI Studio は現在サポートされていません。
  - SageMaker AI Ground Truth は、プライベートワークフォースを管理するためのサポート対象外です。この機能では、Amazon Cognito リソースへの過度に寛容なアクセスが必要になるためです。プライベートワークフォースの管理が必要な場合は、SageMaker AI と Amazon Cognito アクセス許可を組み合わせたカスタム IAM ロールをリクエストできます。それ以外の場合は、データのラベル付けにパブリックワークフォース (Amazon Mechanical Turk がサポート) または AWS Marketplace サービスプロバイダーを使用することをお勧めします。
- SageMaker AI サービス (aws.sagemaker.{region}.notebook、com.amazonaws.{region}.sagemaker.api & com.amazonaws.{region}.sagemaker.runtime) への API コールをサポートする VPC エンドポイントの作成は、アクセス許可を SageMaker AI 関連サービスのみに限定することはできないためサポートされていません。このユースケースをサポートするには、管理 | その他 | その他の RFC を送信して、関連する VPC エンドポイントを作成します。
- SageMaker AI エンドポイントの自動スケーリングはサポートされていません。SageMaker AI には (「\*」) リソースに対する DeleteAlarm アクセス許可が必要なためです。エンドポイントの自動スケーリングをサポートするには、管理 | その他 | その他の RFC を送信して、SageMaker AI エンドポイントの自動スケーリングを設定します。

Q: AMS アカウントで SageMaker AI を使用する際の前提条件または依存関係は何ですか？

- 次のユースケースでは、使用前に特別な設定が必要です。
  - S3 バケットを使用してモデルアーティファクトとデータを保存する場合は、デプロイ | 高度なスタックコンポーネント | S3 ストレージ | RFC の作成で、必要なキーワード (SageMaker、Sagemaker、sagemaker、または aws-glue) を含む という名前の S3 バケットをリクエストする必要があります。
  - Elastic File Store (EFS) を使用する場合は、EFS ストレージを同じサブネットに設定し、セキュリティグループで許可する必要があります。
  - 他のリソースが SageMaker AI サービス (ノートブック、API、ランタイムなど) に直接アクセスする必要がある場合は、次の方法で設定をリクエストする必要があります。
    - RFC を送信してエンドポイントのセキュリティグループを作成する (デプロイ | 高度なスタックコンポーネント | セキュリティグループ | 作成 (自動))。
    - 管理の送信 | その他 | その他 | RFC を作成して関連する VPC エンドポイントを設定します。

Q: が直接`customer_sagemaker_admin_role`アクセスできるリソースでサポートされている命名規則は何ですか? (更新および削除のアクセス許可については、以下を参照してください。リソースでサポートされている追加の命名規則が必要な場合は、AMS Cloud Architect に連絡して相談してください。)

- リソース: `AmazonSageMaker-ExecutionRole-*` ロールを渡す
  - アクセス許可: SageMaker AI セルフプロビジョニングサービスロールは、AWS Glue、AWS RoboMaker、およびでの SageMaker AI サービスロール (`AmazonSageMaker-ExecutionRole-*`) の使用をサポートします AWS Step Functions。
- リソース: Secrets Manager の AWS シークレット
  - アクセス許可: `AmazonSageMaker-*` プレフィックスを使用してシークレットを記述、作成、取得、更新します。
  - アクセス許可: SageMaker リソースタグが に設定されているときにシークレットを取得するについて説明します `true`。
- リソース: 上のリポジトリ AWS CodeCommit
  - アクセス許可: `AmazonSageMaker-*` プレフィックスを持つリポジトリを作成/削除します。
  - アクセス許可: Git Pull/Push on repositories with following prefixes, `*sagemaker*`, `*SageMaker*`, and `*Sagemaker*`。
- リソース: Amazon ECR (Amazon Elastic Container Registry) リポジトリ
  - アクセス許可: アクセス許可: 次のリソース命名規則が使用されている場合、リポジトリポリシーを設定、削除し、コンテナイメージをアップロードします `*sagemaker*`。
- リソース: Amazon S3 バケット
  - アクセス許可: リソースにプレフィックス、`*sagemaker*` がある場合、オブジェクトの取得、配置、削除 `*SageMaker*` `*Sagemaker*`、マルチパートアップロード S3 オブジェクトの中止を行います `aws-glue`。
  - アクセス許可: SageMaker タグが に設定されているときに S3 オブジェクトを取得します `true`。
- リソース: Amazon CloudWatch Log Group
  - アクセス許可: ロググループまたはストリームの作成、ログイベントの入力、一覧表示、更新、の作成、プレフィックス を使用したログ配信の削除 `/aws/sagemaker/*`。
- リソース: Amazon CloudWatch メトリクス

- アクセス許可: 、AWS/SageMaker、AWS/SageMaker/、 、aws/SageMaker、 、および のプレフィックスを使用する場合はaws/SageMaker/aws/sagemakeraws/sagemaker/、メトリクスデータを配置します/aws/sagemaker/。
- リソース: Amazon CloudWatch Dashboard
  - アクセス許可: プレフィックス が使用されているときにダッシュボードを作成/削除しますcustomer\_\*。
- リソース: Amazon SNS (Simple Notification Service) トピック
  - アクセス許可: 、 \*sagemaker\*、および のプレフィックスを使用する場合\*SageMaker\*にトピックをサブスクライブ/作成します\*Sagemaker\*。

Q: **AmazonSageMakerFullAccess**と の違いは何ですか**customer\_sagemaker\_admin\_role**?

customer\_sagemaker\_admin\_role とは、以下を除き、AmazonSageMakerFullAccess とほぼ同じアクセス許可customer\_sagemaker\_admin\_policyを提供します。

- AWS RoboMaker、Amazon Cognito、および AWS Glue リソースに接続するためのアクセス許可。
- SageMaker AI エンドポイントの自動スケーリング。管理 | 高度なスタックコンポーネント | Identity and Access Management (IAM) | エンティティまたはポリシー (マネージドオートメーション) の変更タイプ (ct-27tuth19k52b4) を更新して、自動スケーリングのアクセス許可を一時的または永続的に昇格させる必要があります。これは、自動スケーリングには CloudWatch サービスへの許可付きアクセスが必要なためです。

Q: 保管中のデータ暗号化に AWS KMS カスタマーマネージドキーを採用するにはどうすればよいですか?

関連する IAM ユーザーまたはロールがキーを使用できるように、カスタマーマネージドキーでキーポリシーが正しく設定されていることを確認する必要があります。詳細については、[AWS KMS 「キーポリシー」ドキュメント](#)を参照してください。

## AMS SSP を使用して AMS アカウントに Amazon Simple Email Service をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Simple Email Service (Amazon SES) 機能に直接アクセスします。Amazon Simple Email Service は、デジタルマーケティング担当者やアプリケーション開発者、マーケティング、通知、ト

ランザクション E メール送信を支援するように設計されたクラウドベースの E メール送信サービスです。

SMTP インターフェイスまたはいずれかの AWS SDKs を使用して、Amazon SES を既存のアプリケーションに直接統合できます。Amazon SES の E メール送信機能を、チケットシステムや E メールクライアントなど、既に使用しているソフトウェアに統合することもできます。

詳細については、[「Amazon Simple Email Service」](#) を参照してください。

## AWS Managed Services での Amazon SES に関するよくある質問

Q: AMS アカウントの Amazon SES へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (ct-1w8z66n899dct) 変更タイプで RFC を送信して、Amazon SES へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_ses_admin_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントで Amazon SES を使用するための前提条件または依存関係は何ですか？

- Amazon SES がバケットにイベントを発行できるようにするには、S3 バケットポリシーを設定する必要があります。
- Amazon AWS SES が E メールを暗号化し、アカウントに属する Amazon S3、Amazon SES、Amazon SNS を使用するか、CMK キーを設定する必要があります。

Q: AMS アカウントでの Amazon SES の使用にはどのような制限がありますか？

次のリソースを作成するには RFCs を生成する必要があります。

- Kinesis Firehose ストリームへの PutEvents アクセス許可を持つ SMTP ユーザーと IAM サービスロール。
- Amazon SES ルールと設定セットの送信先がそれらの AWS リソースと連携するには、AMS 変更タイプを使用して S3 バケット、Firehose ストリーム、SNS トピックなどの新しいリソースを作成する必要があります。Amazon SES
- SMTP 認証情報。新しい SMTP 認証情報をリクエストするには、変更タイプ (管理 | その他 | その他 | 作成) を使用します。AMS は認証情報を作成し、Secrets Manager に追加します。

# AMS SSP を使用して AMS アカウントに Amazon Simple Workflow Service をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Simple Workflow Service (Amazon SWF) 機能に直接アクセスします。Amazon Simple Workflow Service は、デベロッパーが並列またはシーケンシャルなステップを持つバックグラウンドジョブを構築、実行、スケーリングするのに役立ちます。Amazon SWF は、クラウドでフルマネージド型のステートトラッカーおよびタスクコーディネーターと考えることができます。アプリケーションのステップが完了するまでに 500 ミリ秒以上かかる場合、処理の状態を追跡する必要がある場合、またはタスクが失敗した場合に復旧または再試行する必要がある場合、Amazon SWF が役立ちます。詳細については、[「Amazon Simple Workflow Service」](#)を参照してください。

## AWS Managed Services の Amazon SWF に関するよくある質問

一般的な質問と回答：

Q: AMS アカウントの Amazon SWF へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add change type (ct-1w8z66n899dct) を送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_swf_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon SWF の使用にはどのような制限がありますか？

Lambda アクセス `InvokeFunction` 許可はこのサービスに含まれていますが、すべての AMS カスタマーロールに追加された `AMS customer_deny_policy` は、AMS Lambda 関数と AMS 所有リソースへのアクセスを明示的に拒否します。Amazon SWF 内のリソースにタグ付けまたはタグ付け解除するには、管理 | その他 | その他の変更タイプを送信します。

Q: AMS アカウントで Amazon SWF を使用するための前提条件または依存関係は何ですか？

Amazon SWF は AWS Lambda サービスに依存するため、このロールの一部として Lambda を呼び出すためのアクセス許可が提供されており、Amazon SWF から Lambda を呼び出すための追加のアクセス許可は必要ありません。それ以外の場合は、Amazon SWF を使用するための前提条件はありません。



## AMS SSP を使用して AMS アカウントに Amazon Textract をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Textract 機能に直接アクセスします。Amazon Textract は、スキャンされたドキュメントから印刷されたテキスト、手書き、その他のデータを自動的に抽出するフルマネージド型の機械学習サービスで、シンプルな光学文字認識 (OCR) を超えて、フォームやテーブルからデータを識別、理解、抽出します。詳細については、「[Amazon Textract](#)」を参照してください。

### AWS Managed Services の Amazon Textract に関するよくある質問

一般的な質問と回答:

Q: AMS アカウントで Amazon Textract をセットアップするようにリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (マネージドオートメーション) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、customer\_textract\_console\_role、customer\_textract\_human\_review\_execution\_role などの IAM ロールをアカウントにプロビジョニングします。また、customer\_ec2\_textract\_instance\_profile を作成し、customer\_textract\_console\_role でロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon Textract の使用にはどのような制限がありますか？

AMS アカウントでの Amazon Textract の使用に制限はありません。

Q: AMS アカウントで Amazon Textract を使用するための前提条件または依存関係は何ですか？

RFC デプロイ | 高度なスタックコンポーネント | S3 ストレージ | 作成 (ct-1a68ck03fn98r) を送信して、S3 バケットの作成をリクエストする必要があります。

## AMS SSP を使用して AMS アカウントに Amazon Transcribe をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Transcribe 機能に直接アクセスします。Amazon Transcribe は、オーディオファイルからタイムスタンプ付きのテキストトランスクリプトを自動的に生成する、フルマネージドで継続的にト



レーニングされた自動音声認識サービスです。Amazon Transcribe を使用すると、開発者はアプリケーションにspeech-to-text機能を簡単に追加できます。コンピュータがオーディオデータを検索して分析することは事実上不可能です。したがって、記録された音声は、アプリケーションで使用する前にテキストに変換する必要があります。これまで、顧客は文字起こしプロバイダーと連携する必要があり、高価な契約に署名する必要があり、このタスクを実行するためにテクノロジースタックに統合するのが困難でした。これらのプロバイダーの多くは、コンタクトセンターで一般的な低忠実度の電話オーディオなど、さまざまなシナリオにうまく適応しない古いテクノロジーを使用しているため、精度が低下します。

Amazon Transcribe は、自動音声認識 (ASR) と呼ばれる深層学習プロセスを使用して、音声をテキストに迅速かつ正確に変換します。Amazon Transcribe を使用して、カスタマーサービスへの電話の文字起こし、クローズドキャプションと字幕の自動化、メディアアセットのメタデータの生成を行い、完全に検索可能なアーカイブを作成できます。Amazon Transcribe Medical を使用して、臨床ドキュメントアプリケーションに医療speech-to-text機能を追加できます。詳細については、[Amazon Transcribe](#)」を参照してください。

## AWS Managed Services での Amazon Transcribe に関するよくある質問

一般的な質問と回答:

Q: Amazon Transcribe を AMS アカウントでセットアップするようにリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (マネージドオートメーション) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_transcribe_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon Transcribe の使用にはどのような制限がありますか？

RA と特に指定がない限り、文字起こしを操作するときは、バケットのプレフィックスとして「customer-transcribe\*」を使用する必要があります。

Amazon 文字起こし内で IAM ロールを作成することはできません。

デフォルトの SSPS の出力データにサービスマネージド S3 バケットを使用することはできません (必要な場合は、アカウント CA にお問い合わせください)。

AMS 名前空間に属さないカスタマー管理の KMS キーを使用する場合は、リスク承諾を送信する必要があります。

Q: AMS アカウントで Amazon Transcribe を使用するための前提条件または依存関係は何ですか？

S3 は、「customer-transcribe\*」という名前のバケットにアクセスできる必要があります。S3 バケットが KMS キーで暗号化されている場合、Amazon Transcribe を使用するには KMS が必要です。バケットを暗号化する必要がない場合は、「KMStranscribeAllow」を削除できます。

## AMS SSP を使用して AMS アカウントに Amazon WorkSpaces をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで WorkSpaces 機能に直接アクセスします。WorkSpaces を使用すると、WorkSpaces と呼ばれる仮想クラウドベースの Microsoft Windows または Amazon Linux デスクトップをユーザーにプロビジョニングできます。WorkSpaces は、ハードウェアの調達とデプロイ、または複雑なソフトウェアのインストールの必要性を排除します。必要に応じてユーザーをすばやく追加または削除できます。ユーザーは、サポートされているデバイスからクライアントアプリケーションを使用するか、Windows WorkSpaces の場合はウェブブラウザを使用して WorkSpaces にアクセスし、既存のオンプレミス Active Directory (AD) 認証情報を使用してログインします。WorkSpaces

詳細については、[Amazon WorkSpaces](#) を参照してください。

## AWS Managed Services の WorkSpaces に関するよくある質問

一般的な質問と回答:

Q: AMS アカウントの WorkSpaces へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (マネージドオートメーション) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_workspaces_console_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの WorkSpaces の使用にはどのような制限がありますか？

WorkSpaces の完全な機能は、Amazon WorkSpaces のセルフプロビジョニングサービスロールで使用できます。

Q: AMS アカウントで WorkSpaces を使用するための前提条件または依存関係は何ですか？

- WorkSpaces は AWS リージョンによって制限されるため、AD Connector は WorkSpaces インスタンスがホストされているのと同じ AWS リージョンで設定する必要があります。

お客様は、次の 2 つの方法のいずれかを使用して WorkSpaces をカスタマー AD に接続できます。

1. AD コネクタを使用して認証をオンプレミス Active Directory サービスにプロキシする (推奨):

WorkSpaces インスタンスをオンプレミスのディレクトリサービスと統合する前に、AMS アカウントに Active Directory (AD) Connector を設定します。AD Connector は、既存の AD ユーザー (ドメインから) のプロキシとして機能し、既存のオンプレミス AD 認証情報を使用して WorkSpaces に接続します。WorkSpaces はお客様のオンプレミスドメインに直接結合され、リソースフォレストとユーザーフォレストの両方として機能し、お客様側でより細かく制御できるため、これが推奨されます。

詳細については、[Amazon WorkSpaces をデプロイするためのベストプラクティス \(シナリオ 1\)](#)」を参照してください。

2. AWS Microsoft AD、共有サービス VPC、オンプレミスへの一方向の信頼で AD Connector を使用する:

また、まず AMS 管理 AD からオンプレミス AD への一方向の送信信頼を確立することで、オンプレミスディレクトリでユーザーを認証することもできます。WorkSpaces は AD Connector を使用して AMS マネージド AD に参加します。その後、WorkSpaces アクセス許可は AMS マネージド AD を介して WorkSpaces インスタンスに委任されます。オンプレミス環境との双方向の信頼を確立する必要はありません。このシナリオでは、ユーザーフォレストはカスタマー AD にあり、リソースフォレストは AMS マネージド AD にあります (AMS マネージド AD への変更は RFC 経由でリクエストできます)。WorkSpaces VPC と AMS マネージド AD を実行している MALZ 共有サービス VPC 間の接続は、Transit Gateway を介して確立されることに注意してください。

詳細については、[Amazon WorkSpaces をデプロイするためのベストプラクティス \(シナリオ 6\)](#)」を参照してください。

 Note

AD Connector は、管理 | その他 | その他 | 前提条件の AD 設定の詳細を含む変更タイプ RFC を送信することで設定できます。詳細については、「[AD Connector の作成](#)」を参照してください。メソッド 2 を使用して AMS マネージド AD でリソースフォレストを作成する場合は、別の管理 | その他 | その他 | AMS マネージド AD を実行して AMS 共有サービスアカウントに変更タイプ RFC を作成します。

## AMS SSP を使用して AMS アカウントで AMS Code サービスをプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで AMS Code サービス機能に直接アクセスします。AMS Code サービスは、次に示すように、AWS コード管理サービスの独自のバンドルです。AMS Code サービスを使用して AMS のすべてのサービスをデプロイするか、AMS に個別にデプロイするかを選択できます。

AMS Code サービスには、次のサービスが含まれます。

- AWS CodeCommit: セキュアな Git ベースのリポジトリをホストするフルマネージド型の [ソースコントロール](#) サービス。これにより、チームは安全でスケーラブルなエコシステムでコードでコラボレーションできます。CodeCommit を使用することにより、独自のソース管理システムを運用したり、そのインフラストラクチャをスケールしたりする必要がなくなります。CodeCommit を使用すると、ソースコードからバイナリまで、あらゆるものを安全に保存でき、既存の Git ツールとシームレスに連携します。詳細については、「[AWS CodeCommit](#)」を参照してください。

AMS Code サービスとは別に AMS アカウントにこれをデプロイするには、「」を参照してください [AMS SSP を使用して AMS アカウント AWS CodeCommit でプロビジョニングする](#)。

- AWS CodeBuild: ソースコードをコンパイルし、テストを実行し、デプロイ可能なソフトウェアパッケージを生成するフルマネージドの継続的統合サービス。CodeBuild により、ビルドサーバーのプロビジョニング、管理、スケーリングが不要になります。CodeBuild では、継続的にスケールされ、複数のビルドが同時にプロセスされるため、ビルドの実行までキューで待機することはありません。パッケージ済みのビルド環境を使用、またはご自分のビルドツールを使用するカスタムビルド環境を作成できることですぐに開始できます。CodeBuild では毎分ごとに使用するコンピューティングリソースの使用量が有料になります。詳細については、「[AWS CodeBuild](#)」を参照してください。

AMS Code サービスとは別に AMS アカウントにこれをデプロイするには、「」を参照してください [AMS SSP を使用して AMS アカウント AWS CodeBuild でプロビジョニングする](#)。

- AWS CodeDeploy: Amazon EC2 やオンプレミスサーバーなどのさまざまなコンピューティングサービスへのソフトウェアデプロイを自動化するフルマネージドデプロイサービス。AWS CodeDeploy は、新機能を迅速にリリースし、アプリケーションのデプロイ中のダウンタイムを回避し、アプリケーションの更新の複雑さを処理するのに役立ちます。AWS CodeDeploy を使用してソフトウェアのデプロイを自動化できるため、エラーが発生しやすい手動操作が不要になります。サービスは、デプロイのニーズに合わせてスケールされます。詳細については、「[AWS CodeDeploy](#)」を参照してください。

AMS Code サービスとは別に AMS アカウントにこれをデプロイするには、「」を参照してください [AMS SSP を使用して AMS アカウント AWS CodeDeploy でプロビジョニングする](#)。

- AWS CodePipeline: 完全マネージド型の[継続的デリバリー](#)サービス。リリースパイプラインを自動化して、アプリケーションとインフラストラクチャを迅速かつ確実に更新できます。CodePipeline はお客様が定義したリリースモデルに基づき、コードチェンジがあった場合のフェーズの構築、テスト、およびデプロイを自動化します。機能とアップデートをすばやく、信頼性の高い方法で配信できます。GitHub などの AWS CodePipeline サードパーティーサービスと、または独自のカスタムプラグインと簡単に統合できます。では AWS CodePipeline、使用した分のみお支払いいただきます。前払い金や長期契約はありません。詳細については、「[AWS CodePipeline](#)」を参照してください。

AMS Code サービスとは別に AMS アカウントにこれをデプロイするには、「」を参照してください [AMS SSP を使用して AMS アカウント AWS CodePipeline でプロビジョニングする](#)。

## AWS Managed Services の AMS Code サービスに関するよくある質問

Q: AMS アカウントの AMS Code サービスへのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (マネージドオートメーション) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_code_suite_console_role`。アカウントでプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。この時点で、AMS Operations は `CodeBuildcustomer_codebuild_service_role`、`CodeDeploy`、`CodePipelineaws_code_pipeline_service_role` サービスのアカウントに `customer_codedeploy_service_role`、サービスロールもデプロイします。CodeBuild に追加の IAM アクセス許可が必要な場合は `customer_codebuild_service_role`、AMS サービスリクエストを送信します。

### Note

これらのサービスを個別に追加することもできます。詳細については、[AMS SSP を使用して AMS アカウント AWS CodeBuild でプロビジョニングする](#)「」、[AMS SSP を使用して AMS アカウント AWS CodeDeploy でプロビジョニングする](#)「」、および [AMS SSP を使用](#)



[して AMS アカウント AWS CodePipeline でプロビジョニングする「」](#)をそれぞれ参照してください。

Q: AMS アカウントでの AMS Code サービスの使用にはどのような制限がありますか？

- AWS CodeCommit: CodeCommit のトリガー機能は、SNS トピックを作成する権限が関連付けられているため無効になっています。CodeCommit に対する直接認証は制限されています。ユーザーは 認証情報ヘルパーで認証する必要があります。一部の KMS コマンドも制限されています。kms:Encrypt、kms:Decrypt、kms:ReEncrypt、kms:GenerateDataKey、kms:GenerateDataKeyWithoutEntropy および kms:DescribeKey。
- CodeBuild: AWS CodeBuild コンソール管理者アクセスの場合、アクセス許可はリソースレベルで制限されます。たとえば、CloudWatch アクションは特定のリソースに制限され、iam:PassRole アクセス許可は制御されます。
- CodeDeploy: 現在、CodeDeploy は Amazon EC2/オンプレミスでのデプロイのみをサポートしています。CodeDeploy を介した ECS および Lambda でのデプロイはサポートされていません。
- CodePipeline: CodePipeline の機能、ステージ、プロバイダーは以下に限定されます。
  - デプロイステージ: Amazon S3 および AWS CodeDeploy
  - ソースステージ: Amazon S3、AWS CodeCommit、ビットバケット、GitHub
  - ビルドステージ: AWS CodeBuild および Jenkins
  - 承認ステージ: Amazon SNS
  - テストステージ: AWS CodeBuild、Jenkins、BlazeMeter、Ghost Inspector UI テスト、Micro Focus StormRunner Load、Runscope API Monitoring
  - ステージの呼び出し: Step Functions と Lambda

#### Note

AMS オペレーションは `customer_code_pipeline_lambda_policy` をアカウントにデプロイします。Lambda 呼び出しステージの Lambda 実行ロールにアタッチする必要があります。このポリシーを追加する Lambda サービス/実行ロール名を指定します。カスタム Lambda サービス/実行ロールがない場合、AMS は という名前の新しいロールを作成します。これは `customer_code_pipeline_lambda_execution_role` `customer_lambda_basic_execution_role` とのコピーです `customer_code_pipeline_lambda_policy`。

Q: AMS アカウントで AMS Code サービスを使用するための前提条件または依存関係は何ですか？

- CodeCommit: S3 バケットが AWS KMS キーで暗号化されている場合は、S3 と AWS KMS を使用する必要があります AWS CodeCommit。
- CodeBuild: 定義された AWS CodeBuild サービスロールに追加の IAM アクセス許可が必要な場合は、AMS サービスリクエストを通じてリクエストします。
- CodeDeploy: なし。
- CodePipeline: None. AWS supported services—AWS CodeCommit, AWS CodeBuild, AWS CodeDeploy—は、CodePipeline の起動前または起動時に起動する必要があります。ただし、これは AMS エンジニアによって行われます。

## AMS SSP を使用して AMS アカウント AWS Amplify でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントの AWS Amplify 機能に直接アクセスします。AWS Amplify は、フロントエンドのウェブおよびモバイル開発者がフルスタックアプリケーションを簡単に構築、接続、ホストできるようにする完全なソリューションです。Amplify は、ユースケースの進化に応じて幅広い AWS サービスを活用する柔軟性を提供します。Amplify は、フルスタックの iOS、Android、Flutter、Web、React Native アプリケーションを構築するための製品を提供しています。詳細については[AWS Amplify](#)を参照してください。

### AWS Amplify AWS Managed Servicesに関するよくある質問

一般的な質問と回答:

Q: AMS アカウントでの設定 AWS Amplify をリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (マネージドオートメーション) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_amplify_console_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

さらに、にはインフラストラクチャの変更許可 AWS Amplify があるため、リスク承諾を提供する必要があります。これを行うには、Cloud Service Delivery Manager (CSDM) を使用します。

Q: AMS アカウント AWS Amplify で を使用することにはどのような制限がありますか？



特に RA と が指定されていない限り、Amplify を使用するときは、バケットのプレフィックス 'amplify\*' として を使用する必要があります。

Q: AMS アカウント AWS Amplify で を使用するための前提条件または依存関係は何ですか？

AMS アカウント AWS Amplify で を使用するための前提条件はありません。

Malz 環境のみ: Amplify のデフォルトのオンボードロールは「customer\_amplify\_console\_role」です。カスタムロールを使用するには、まず IAM エンティティをデプロイします。次に、追加の RFC を作成して、アプリケーションアカウントのサービスコントロールポリシーの許可リストにカスタムロールを追加します。

## AMS SSP を使用してプロビジョニングする AWS AppSync

AMS Self-Service Provisioning (SSP) モードを使用して、AMS マネージドアカウント内の AWS AppSync 機能に直接アクセスします。 は、1 つ以上のデータソースのデータに安全にアクセスし、操作し、結合するための柔軟な API を作成できるようにすることで、アプリケーション開発 AWS AppSync を簡素化します。AWS AppSync は、GraphQL を使用してアプリケーションが必要とするデータを正確に取得できるようにするマネージドサービスです。

を使用すると AWS AppSync、リアルタイムの更新を必要とするアプリケーションを含むスケーラブルなアプリケーションを、NoSQL データストア、リレーショナルデータベース、HTTP APIs、カスタムデータソースなどのさまざまなデータソースで構築できます AWS Lambda。モバイルアプリとウェブアプリの場合、 は AWS AppSync さらに、デバイスがオフラインになったときにローカルデータアクセスを提供し、オンラインに戻ったときにカスタマイズ可能な競合解決によるデータ同期を提供します。詳細については[AWS AppSync](#)を参照してください。

## AWS AppSync AWS Managed Servicesに関するよくある質問

よくある質問と回答：

Q: AMS アカウントのアクセス AWS AppSync をリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add change type (ct-1w8z66n899dct) を送信してアクセスをリクエストします。この RFC は、customer\_appsync\_service\_roleおよび の IAM ロールをアカウントにプロビジョニングしますcustomer\_appsync\_author\_role。アカウントにプロビジョニングされたら、フェデレーションソリューションcustomer\_appsync\_author\_roleで をオンボードする必要があります。

Q: の使用にはどのような制限がありますか AWS AppSync？

- AppSync でデータソースを作成する場合、お客様は以前に作成したサービスロールを指定する必要があります。新しいロールの作成は許可されないため、アクセス拒否が返されます。
- AppSync ロールは、AMS インフラストラクチャへの変更を防ぐために、「AMS-」または「MC-」プレフィックスを含むリソースへのアクセス許可を制限するように設定されています。

Q: を使用するための前提条件または依存関係は何ですか AWS AppSync ?

このサービスでは、他の複数の サービスをデータソースとして使用できます。これらのサービスを使用するための基本的なアクセス許可はサービスロール (customer\_appsync\_service\_role) に含まれていますが、サービスを使用するときはサービスロールを手動で選択する必要があります。

## AMS SSP を使用して AMS アカウント AWS App Mesh でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS App Mesh 機能に直接アクセスします。は、複数のタイプのコンピューティングインフラストラクチャ間でサービスが相互に通信しやすいように、アプリケーションレベルのネットワーク AWS App Mesh を提供します。App Mesh は、サービスの通信方法を標準化し、end-to-end 可視性を提供し、アプリケーションの高可用性を確保します。

AWS App Mesh は、複数のタイプのコンピューティングインフラストラクチャにまたがって構築されたサービスの一貫した可視性とネットワークトラフィック制御を提供することで、サービスの実行を容易にします。App Mesh を使用すると、アプリケーションコードを更新して、モニタリングデータの収集方法やサービス間のトラフィックのルーティング方法を変更する必要がなくなります。App Mesh は、モニタリングデータをエクスポートするように各サービスを設定し、アプリケーション全体で一貫した通信制御ロジックを実装します。これにより、エラーの正確な場所をすばやく特定し、障害が発生したときやコード変更をデプロイする必要があるときにネットワークトラフィックを自動的に再ルーティングすることが容易になります。詳細については[AWS App Mesh](#)を参照してください。

## AWS App Mesh AWS Managed Servicesに関するよくある質問

よくある質問と回答：

Q: AMS アカウントのアクセス AWS App Mesh をリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add change type (ct-1w8z66n899dct) を送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニング

します: `customer_app_mesh_console_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: の使用にはどのような制限がありますか AWS App Mesh ?

のフル機能は AWS App Mesh 、 AMS アカウントで使用できます。

Q: を使用するための前提条件または依存関係は何ですか AWS App Mesh ?

AMS アカウント AWS App Mesh で使用する前提条件や依存関係はありません。

## AMS SSP を使用して AMS アカウント AWS Audit Manager でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Audit Manager 機能に直接アクセスします。Audit Manager は、AWS 使用状況を継続的に監査し、リスクと規制や業界標準への準拠を評価する方法を簡素化するのに役立ちます。Audit Manager はエビデンスの収集を自動化するため、ポリシー、手順、アクティビティが効果的に機能しているかどうかの評価が容易になります。監査の時期になると、Audit Manager はコントロールのステークホルダーレビューを管理し、手動作業を大幅に削減して監査対応レポートを構築するのに役立ちます。詳細については、[「Audit Manager」](#)を参照してください。

## AWS Audit Manager AWS Managed Servicesに関するよくある質問

一般的な質問と回答:

Q: AWS Audit Manager AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか?

AWS サービス RFC 管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (マネージドオートメーション) (ct-3qe6io8t6jtny) の送信を通じてアクセスをリクエストできます。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer-audit-manager-admin-Role`。アカウントでプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: の使用にはどのような制限がありますか AWS Audit Manager?

AMS アカウント AWS Audit Manager での の使用に制限はありません。の完全な機能 AWS Audit Manager が提供されます。

Q: を使用するための前提条件または依存関係は何ですか AWS Audit Manager?

1. レポート/評価を配置する s3 バケットを AMS に提供する必要があります。
2. サービスで暗号化する場合は、使用する KMS CMK ARN を AMS に提供する必要があります。
3. トピックに SNS 通知を送信する場合は、トピックまたは ARN の名前を指定する必要があります。
4. (オプション) Audit Manager のマルチアカウントランディングゾーンの一部として Organizations を有効にし、委任された管理者アカウントが必要な場合は、追加の前提条件があります。RFC の説明フィールド (Management | AWS service | Compatible Service| Add) で、Audit Manager Setup の一部として委任された管理者アカウントを使用するように指定し、以下の詳細を指定します。
  - KMS CMK ARN (最初は Audit Manager のセットアップに使用)
  - Audit Manager がこのマルチアカウントランディングゾーンの一部として使用する委任管理者アカウント ID (MALZ アプリケーションアカウントでもかまいません)

## AMS SSP を使用して AMS アカウント AWS Batch でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS Batch 機能に直接アクセスします。AWS Batch は、開発者、サイエンティスト、エンジニアが数十万のバッチコンピューティングジョブを簡単かつ効率的に実行できるようにします AWS。は、送信されたバッチジョブのボリュームと特定のリソース要件に基づいて、最適な量とタイプのコンピューティングリソース (CPU またはメモリ最適化インスタンスなど) を AWS Batch 動的にプロビジョニングします。を使用すると AWS Batch、ジョブの実行に使用するバッチコンピューティングソフトウェアやサーバークラスターをインストールおよび管理する必要がなくなるため、結果の分析と問題の解決に集中できます。詳細については[AWS Batch](#)を参照してください。

### AWS Batch AWS Managed Servicesに関するよくある質問

よくある質問と回答：

Q: AWS Batch AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか？

1. へのアクセスをリクエストするには AWS Batch、RFC 管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (ct-1w8z66n899dct) を送信します。この RFC は、アカウントに次の IAM ロールとポリシーをプロビジョニングします。

IAM ロール：

- `customer_batch_console_role`
- `customer_batch_ecs_instance_role`
- `customer_batch_events_service_role`
- `customer_batch_service_role`
- `customer_batch_ecs_task_role`

ポリシー:

- `customer_batch_console_role_policy`
- `customer_batch_service_role_policy`
- `customer_batch_events_service_role_policy`

2. アカウントでプロビジョニングされたら、フェデレーションソリューション `customer_batch_console_role` でロールをオンボードする必要があります。

Q: の使用にはどのような制限がありますか AWS Batch ?

コンピューティング環境を作成するときは、EC2 インスタンスを「`customer_batch`」または「`customer-batch`」としてタグ付けする必要があります。インスタンスにタグが付けられていない場合、ジョブの完了時にインスタンスはバッチで終了されません。

Q: を使用するための前提条件または依存関係は何ですか AWS Batch ?

AMS アカウント AWS Batch で使用する前提条件や依存関係はありません。

## AMS SSP を使用して AMS アカウント AWS Certificate Manager でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで AWS Certificate Manager (ACM) 機能に直接アクセスします。AWS Certificate Manager は、サービスおよび内部接続リソースで使えるように、パブリックおよびプライベートの Secure Sockets Layer/Transport Layer Security (SSL/TLS) 証明書をプロビジョニング、管理、デプロイできる AWS サービスです。SSL/TLS 証明書は、ネットワーク通信を保護し、インターネット上のウェブサイトとプライベートネットワーク上のリソースのアイデンティティを確立するために使用されます。は、SSL/TLS 証明書を購入、アップロード、更新する時間のかかる手動プロセス AWS Certificate Manager を削除します。

を使用すると AWS Certificate Manager、証明書をリクエストし、Elastic Load Balancer、Amazon CloudFront デイストリビューション、API Gateway APIs などの ACM 統合 AWS リソースにデプロイし、が証明書の更新 AWS Certificate Manager を処理できます。内部リソースのプライベート証明書を作成し、証明書のライフサイクルを一元管理することもできます。ACM 統合サービスで利用できる AWS Certificate Manager 用に でプロビジョニングされたパブリック証明書とプライベート証明書は無料です。アプリケーションを実行するために作成した AWS リソースに対してのみ料金が発生します。では[AWS Private Certificate Authority](#)、 のオペレーション AWS Private CA と発行するプライベート証明書に対して毎月お支払いいただきます。詳細については、[AWS Certificate Manager 「- AWS Documentation」](#)を参照してください。

## AWS Managed Services の ACM に関するよくある質問

一般的な質問と回答:

Q: AWS Certificate Manager AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add change type (ct-1w8z66n899dct) を送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: customer\_acm\_create\_role。このロールを使用して、ACM 証明書を作成および管理できます。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

ACM 証明書は、IAM customer\_acm\_create\_role ロールを追加していない場合でも、次の変更タイプを使用して作成できます。

- [ACM | パブリック証明書の作成](#)
- [ACM | プライベート証明書の作成](#)
- [追加の SANs を含む ACM 証明書 | 作成](#)

Q: の使用にはどのような制限がありますか AWS Certificate Manager?

既存の証明書を削除または変更するには、変更リクエスト (RFC) を AMS に送信する必要があります。これらのアクションには完全な管理者アクセスが必要です (管理 | 高度なスタックコンポーネント | ACM | 証明書変更タイプの削除 (ct-1q8q56cmwqj9m) を使用 )。IAM ポリシーでは、タグ名 (mc\*、ams\* など) に基づいて権限を除外できないことに注意してください。証明書にはコストが発生しないため、未使用の証明書を削除しても時間的制約はありません。

Q: Certificate Manager を使用するための前提条件または依存関係は何ですか？



既存のパブリック DNS 名、および DNS CNAME レコードを作成するためのアクセス。ただし、マネージドアカウントでホストする必要はありません。

## AMS SSP を使用して AMS アカウント AWS Private Certificate Authority でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントの AWS Private Certificate Authority 機能に直接アクセスします。プライベート証明書は、サーバー、モバイル、IoT デバイス、アプリケーションなどのプライベートネットワーク上の接続されたリソース間の通信を識別して保護するために使用されます。AWS Private CA は、プライベート証明書のライフサイクルを簡単かつ安全に管理できるマネージドプライベート CA サービスです。は、独自のプライベート CA を運用するための事前投資と継続的なメンテナンスコストなしで、高可用性のプライベート CA サービス AWS Private CA を提供します。は、ACM の証明書管理機能をプライベート証明書に AWS Private CA 拡張し、パブリック証明書とプライベート証明書を一元的に作成および管理できるようにします。AWS マネジメントコンソールまたは ACM API を使用して、AWS リソースのプライベート証明書を簡単に作成およびデプロイできます。EC2 インスタンス、コンテナ、IoT デバイス、オンプレミスリソースの場合、プライベート証明書を簡単に作成して追跡し、独自のクライアント側のオートメーションコードを使用してデプロイできます。また、プライベート証明書を作成して、カスタム証明書の有効期間、キーアルゴリズム、またはリソース名を必要とするアプリケーション用に自分で管理することもできます。詳細については、「」を参照してください[AWS Private CA](#)。

### AWS Private CA AWS Managed Servicesに関するよくある質問

一般的な質問と回答:

Q: AMS アカウントのアクセス AWS Private CA をリクエストするにはどうすればよいですか？

AWS サービス RFC (管理 | AWS サービス | 互換サービス) の送信を通じてアクセスをリクエストします。この RFC を通じて、次の IAM ロールがアカウントにプロビジョニングされます: `customer_acm_pca_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: の使用にはどのような制限がありますか AWS Private CA？

現在、AWS Resource Access Manager (AWS RAM) を使用してクロスアカウントを共有 AWS Private CA することはできません。

Q: を使用するための前提条件または依存関係は何ですか AWS Private CA？



1. CRL を作成する場合は、保存先の S3 バケットが必要です。AWS Private CA は指定した Amazon S3 バケットに CRL を自動的に預金し、定期的に更新します。CRL を設定する前に、S3 バケットに以下のバケットポリシーがあることが前提条件です。このリクエストを続行するには、次のように `ct-0fpjlxa808sh2` (管理 | 高度なスタックコンポーネント | S3 ストレージ | 更新ポリシー) を使用して RFC を作成します。

- S3 バケット名または ARN を指定します。
- 以下のポリシーを RFC にコピーし、を目的の S3 バケット名 `bucket-name` に置き換えます。

## JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "acm-pca.amazonaws.com"
      },
      "Action": [
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation"
      ],
      "Resource": [
        "arn:aws:s3:::bucket-name/*",
        "arn:aws:s3:::bucket-name"
      ]
    }
  ]
}
```

2. 上記の S3 バケットが暗号化されている場合、サービスプリンシパル `acm-pca.amazonaws.com` には復号するためのアクセス許可が必要です。このリクエストを続行するには、次のように `ct-3ovo7px2vsa6n` (管理 | 高度なスタックコンポーネント | KMS キー | 更新) を使用して RFC を作成します。

- ポリシーを更新する必要がある KMS キー ARN を指定します。

- 以下のポリシーを RFC にコピーし、を目的の S3 バケット名bucket-nameに置き換えます。

```
{
  "Sid": "Allow ACM-PCA use of the key",
  "Effect": "Allow",
  "Principal": {
    "Service": "acm-pca.amazonaws.com"
  },
  "Action": [
    "kms:GenerateDataKey",
    "kms:Decrypt"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:EncryptionContext:aws:s3:arn": [
        "arn:aws:s3:::bucket_name/acm-pca-permission-test-key",
        "arn:aws:s3:::bucket_name/acm-pca-permission-test-key-private",
        "arn:aws:s3:::bucket_name/audit-report/*",
        "arn:aws:s3:::bucket_name/crl/*"
      ]
    }
  }
}
```

3. AWS Private CA CRLs 「新しいアクセスコントロールリスト (ACLs)」をサポートしていません。S3 「ACM プライベート CA の AWS Private CA CRL を安全に作成して保存する方法」で説明されているように、S3 アカウントとバケットでこの設定を無効にする必要があります。無効にするには、ct-0xdawir96cy7k (管理 | その他 | その他 | 更新) を使用して新しい RFC を作成し、リスク許容をアタッチします。CRLs <https://aws.amazon.com/blogs/security/how-to-securely-create-and-store-your-crl-for-acm-private-ca/> リスクの受け入れについてご質問がある場合は、クラウドアーキテクトにお問い合わせください。

## AMS SSP を使用して AMS アカウントで AWS CloudEndure をプロビジョニングする

### Note

の起動に成功すると AWS Application Migration Service、CloudEndure Migration サービスはすべての AWS リージョンでサポート終了となります。GovCloud リージョンと商用リー

ジョンへの移行 AWS Application Migration Service には、を使用することをお勧めします。詳細については、「[とは AWS Application Migration Service](#)」を参照してください。を使用する場合は AWS Application Migration Service、CA に連絡して指示を受けてください。

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで AWS CloudEndure 機能に直接アクセスします。AWS CloudEndure 移行は、物理、仮想、クラウドベースのインフラストラクチャから への大規模な移行を簡素化、迅速化、自動化します AWS。CloudEndure デイザスタリカバリ (DR) は、ランサムウェアやサーバーの破損などの脅威によるダウンタイムやデータ損失から保護します。

## AWS Managed Services でのAWS CloudEndure に関するよくある質問

Q: AMS アカウントの CloudEndure へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (マネージドオートメーション) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、次の IAM ユーザーをアカウントにプロビジョニングします: `customer_cloud_endure_user`。アカウントでプロビジョニングされると、ユーザーのアクセスキーとシークレットキーは AWS Secrets Manager で共有されます。

これらのポリシーは、`customer_cloud_endure_policy`および のアカウントにもプロビジョニングされます `customer_cloud_endure_deny_policy`。

さらに、アプリケーション統合用の CloudEndure DR ソリューションにはインフラストラクチャ変更のアクセス許可があるため、リスク承諾を提供する必要があります。これを行うには、クラウドサービスデリバリーマネージャー (CSDM) を使用します。

Q: AMS アカウントでの CloudEndure の使用にはどのような制限がありますか？

クラウド耐久性レプリケーションおよび変換インスタンスは、指定したサブネットでのみ起動できます。

Q: AMS アカウントで CloudEndure を使用するための前提条件または依存関係は何ですか？ RFC 双方向通信を介して以下を共有します。

- 起動するレプリケーションインスタンスと変換インスタンスの VPC サブネットの詳細。
- EBS ボリュームが暗号化されている場合の KMS キー Amazon リソースネーム (ARN)。

# AMS SSP を使用して AMS アカウント AWS CloudHSM でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで AWS CloudHSM 機能に直接アクセスします。AWS CloudHSM 企業、契約上の AWS クラウド内で専用のハードウェアセキュリティモジュール (HSM) インスタンスを使用して、データセキュリティに関する および の規制コンプライアンス要件 AWS。 および AWS Marketplace パートナー、は、AWS プラットフォーム内の機密データを保護するためのさまざまなソリューションを提供します。ただし、暗号化キーの管理に関する契約上または規制上の義務の対象となるアプリケーションやデータについては、追加の保護が必要になる場合があります。は既存のデータ保護ソリューションを AWS CloudHSM 補完し、安全なキー管理のために政府の標準に従って設計および検証された HSMs 内の暗号化キーを保護することができます。AWS CloudHSM を使用すると、保存、は、データ暗号化に使用される暗号化キーを、ユーザーのみがキーにアクセスできるように管理します。詳細については[AWS CloudHSM](#)を参照してください。

## AWS CloudHSM AWS Managed Servicesに関するよくある質問

一般的な質問と回答：

Q: AWS CloudHSM AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか？

AMS アカウントでの の使用には 2 つのステップがあります。

1. AWS CloudHSM クラスターをリクエストします。これを行うには、管理 | その他 | その他 | 作成 (ct-1e1xtak34nx76) 変更タイプを使用して RFC を送信します。次の詳細を含めます。
  - AWS リージョン。
  - VPC ID/ARN。送信する RFC と同じアカウントにある VPC ID/VPC ARN を指定します。
  - クラスターに少なくとも 2 つのアベイラビリティゾーンを指定します。
  - HSM クラスターに接続する Amazon EC2 インスタンス ID。
2. AWS CloudHSM コンソールにアクセスします。これを行うには、管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (ct-1w8z66n899dct) 変更タイプで RFC を送信します。この RFC は、アカウントに次の IAM ロールをプロビジョニングします：  
customer\_cloudhsm\_console\_role。

アカウントでロールがプロビジョニングされたら、フェデレーションソリューションにロールをオンボードする必要があります。

Q: AMS アカウント AWS CloudHSM で を使用することにはどのような制限がありますか？

AWS CloudHSM コンソールへのアクセスでは、クラスターを作成、終了、または復元することはできません。これらの操作を行うには、管理 | その他 | その他 | 変更タイプの作成 (ct-1e1xtak34nx76) 変更タイプを送信します。

Q: AMS アカウント AWS CloudHSM で を使用するための前提条件または依存関係は何ですか？

VPC 内のクライアント Amazon EC2 インスタンスを介してポート 2225 を使用する TCP トラフィックを許可するか、HSM クラスターへのアクセスを必要とするオンプレミスサーバーに Direct Connect VPN を使用する必要があります。AWS CloudHSM は、セキュリティグループとネットワークインターフェイスの Amazon EC2 に依存します。ログのモニタリングまたは監査では、HSM はすべてのローカル HSM デバイスアクティビティで CloudTrail (AWS API オペレーション) と CloudWatch Logs に依存します。

Q: AWS CloudHSM クライアントおよび関連するソフトウェアライブラリに更新を適用するのは誰ですか？

ライブラリとクライアントの更新を適用する責任はお客様にあります。リリースの [CloudHSM バージョン履歴](#) ページをモニタリングし、[CloudHSM クライアントアップグレード](#) を使用して更新を適用します。

 Note

HSM アプライアンスのソフトウェアパッチは、常にサービスによって AWS CloudHSM 自動的に適用されます。

## AMS SSP を使用して AMS アカウント AWS CodeBuild でプロビジョニングする

AMS Self-Service Provisioning (SSP) モードを使用して、AMS マネージドアカウント内の AWS CodeBuild 機能に直接アクセスします。AWS CodeBuild は、ソースコードをコンパイルし、テストを実行し、デプロイ可能なソフトウェアパッケージを生成するフルマネージドの継続的統合サービスです。CodeBuild により、ビルドサーバーのプロビジョニング、管理、スケーリングが不要になります。CodeBuild では、継続的にスケーリングされ、複数のビルドが同時にプロセスされるため、ビルドの実行までキューで待機することはありません。パッケージ済みのビルド環境を使用、またはご自分のビルドツールを使用するカスタムビルド環境を作成できることですぐに開始できま

す。CodeBuild では毎分ごとに使用するコンピューティングリソースの使用量が有料になります。詳細については[AWS CodeBuild](#)を参照してください。

#### Note

CodeCommit、CodeBuild、CodeDeploy、および CodePipeline を単一の RFC でオンボードするには、管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (マネージドオートメーション) (ct-3qe6io8t6jtny) 変更タイプを送信し、CodeBuild、CodeDeploy、および CodePipeline の 3 つのサービスをリクエストします。次に、`customer_codebuild_service_role`、`customer_codedeploy_service_role`、`aws_code_pipeline_service_role` の 3 つのロールすべてがアカウントにプロビジョニングされます。アカウントでプロビジョニングした後、フェデレーションソリューションでロールをオンボードする必要があります。

## AWS Managed Services での CodeBuild に関するよくある質問

一般的な質問と回答:

Q: AWS CodeBuild AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか？

AMS アカウント AWS CodeBuild での の使用には 2 つのステップがあります。

1. S3 バケット、Amazon CloudWatch、ロググループと AWS 調整する CodeBuild Service Role ビルドプロセスの をプロビジョニングする
2. CodeBuild コンソールへのアクセスをリクエストする

管理 | AWS サービス | セルフプロビジョニングサービス | 変更タイプの追加 (ct-1w8z66n899dct) を使用して RFC を送信することで、両方の設定を AMS アカウントでリクエストできます。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウント AWS CodeBuild で を使用することにはどのような制限がありますか？

AWS CodeBuild コンソール管理者アクセスの場合、アクセス許可はリソースレベルで制限されます。たとえば、CloudWatch アクションは特定のリソースに制限され、`iam:PassRole` アクセス許可は制御されます。

Q: AMS アカウントで CodeBuild を使用するための前提条件または依存関係は何ですか？

定義された AWS CodeBuild サービスロールに追加の IAM アクセス許可が必要な場合は、AMS サービスリクエストを通じてリクエストします。

## AMS SSP を使用して AMS アカウント AWS CodeCommit でプロビジョニングする

### Note

AWS は AWS CodeCommit、2024 年 7 月 25 日以降、への新しいお客様のアクセスを閉鎖しました。AWS CodeCommit 既存のお客様は、引き続きこのサービスを通常どおり使用できます。AWS は引き続きセキュリティ、可用性、パフォーマンスの向上に投資しますが AWS CodeCommit、新機能を導入する予定はありません。

AWS CodeCommit Git リポジトリを他の Git プロバイダーに移行するには、クラウドアーキテクト (CA) に連絡してガイダンスを受けてください。Git リポジトリの移行の詳細については、[AWS CodeCommit リポジトリを別の Git プロバイダーに移行する方法](#)を参照してください。

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS CodeCommit 機能に直接アクセスします。AWS CodeCommit は、セキュアな Git ベースのリポジトリをホストするフルマネージド型の[ソースコントロール](#)サービスです。これは、安全でスケーラブルなエコシステムでチームがコードでコラボレーションするのに役立ちます。CodeCommit を使用することにより、独自のソース管理システムを運用したり、そのインフラストラクチャをスケールしたりする必要がなくなります。CodeCommit を使用すると、ソースコードからバイナリまで、あらゆるものを安全に保存でき、既存の Git ツールとシームレスに連携します。詳細については[AWS CodeCommit](#)を参照してください。

### Note

CodeCommit、CodeBuild、CodeDeploy、および CodePipeline を単一の RFC でオンボードするには、管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (マネージドオートメーション) (ct-3qe6io8t6jtny) 変更タイプを送信し、CodeBuild、CodeDeploy、および CodePipeline の 3 つのサービスをリクエストします。次に、、、customer\_codebuild\_service\_role、customer\_codedeploy\_service\_roleaws\_code\_pipeline\_service\_roleの 3 つのロールすべてがアカウントにプロビジョニングされます。アカウントでプロビジョニングした後、フェデレーションソリューションでロールをオンボードする必要があります。



## AWS Managed Services の CodeCommit に関するよくある質問

Q: AMS アカウントの CodeCommit へのアクセスをリクエストするにはどうすればよいですか？

AWS CodeCommit コンソールとデータアクセスロールは、2 つの AWS Service RFCs、コンソール アクセス、データアクセスを送信することでリクエストできます。

- Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) change type を使用して RFC を送信 AWS CodeCommit して、へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_codecommit_console_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

データアクセス (トレーニングやエンティティリストなど) には、S3 データソース (必須)、出力バケット (必須)、KMS (オプション) を指定する個別の CTs がデータソースごとに必要です。すべてのデータソースにアクセスロールが付与されている限り、AWS CodeCommit ジョブの作成に制限はありません。データアクセスをリクエストするには、管理 | その他 | その他 | 作成 (ct-1e1xtak34nx76) を使用して RFC を送信します。

Q: AMS アカウント AWS CodeCommit で を使用することにはどのような制限がありますか？

SNS トピックを作成する権限が関連付けられているため、CodeCommit のトリガー機能は無効になっています。CodeCommit に対する直接認証は制限されているため、ユーザーは 認証情報ヘルパーで認証する必要があります。、`kms:Encrypt`、`kms:Decrypt`、`kms:ReEncrypt`、`kms:GenerateDataKey`、`kms:GenerateDataKeyWithoutPlaintext`などの KMS コマンドも制限されています。`kms:DescribeKey`。

Q: AMS アカウント AWS CodeCommit で を使用するための前提条件または依存関係は何ですか？

S3 バケットが KMS キーで暗号化されている場合、 を使用するには S3 と KMS が必要です AWS CodeCommit。

## AMS SSP を使用して AMS アカウント AWS CodeDeploy でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS CodeDeploy 機能に直接アクセスします。AWS CodeDeploy は、Amazon EC2、AWS

Fargate AWS Lambda、オンプレミスサーバーなどのさまざまなコンピューティングサービスへのソフトウェアデプロイを自動化するフルマネージドデプロイサービスです。AWS CodeDeploy は、新機能を迅速にリリースし、アプリケーションのデプロイ中のダウンタイムを回避し、アプリケーションの更新の複雑さに対処します。AWS CodeDeploy を使用してソフトウェアのデプロイを自動化できるため、エラーが発生しやすい手動操作が不要になります。サービスは、デプロイのニーズに合わせてスケーリングされます。詳細については[AWS CodeDeploy](#)を参照してください。

#### Note

CodeCommit、CodeBuild、CodeDeploy、および CodePipeline を単一の RFC でオンボードするには、管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (マネージドオートメーション) (ct-3qe6io8t6jtny) 変更タイプを送信し、CodeBuild、CodeDeploy、および CodePipeline の 3 つのサービスをリクエストします。次に、`customer_codebuild_service_role`、`customer_codedeploy_service_role`、`aws_code_pipeline_service_role` の 3 つのロールすべてがアカウントにプロビジョニングされます。アカウントでプロビジョニングした後、フェデレーションソリューションでロールをオンボードする必要があります。

## AWS Managed Services での CodeDeploy に関するよくある質問

Q: AMS アカウントの CodeDeploy へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (ct-1w8z66n899dct) 変更タイプで RFC を送信して CodeDeploy へのアクセスをリクエストします。この RFC は、`customer_codedeploy_console_role` および の IAM ロールをアカウントにプロビジョニングします `customer_codedeploy_service_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションで `customer_codedeploy_console_role` ロールをオンボードする必要があります。

Q: AMS アカウントでの CodeDeploy の使用にはどのような制限がありますか？

現在、Compute Platform は Amazon EC2/オンプレミスとしてのみサポートされています。ブルー/グリーンデプロイはサポートされていません。

Q: AMS アカウントで CodeDeploy を使用するための前提条件または依存関係は何ですか？

AMS アカウントで CodeDeploy を使用するための前提条件や依存関係はありません。

# AMS SSP を使用して AMS アカウント AWS CodePipeline でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS CodePipeline 機能に直接アクセスします。AWS CodePipeline はフルマネージド型の[継続的デリバリー](#)サービスであり、リリースパイプラインを自動化して、アプリケーションとインフラストラクチャを迅速かつ確実に更新できます。CodePipeline はお客様が定義したリリースモデルに基づき、コードチェンジがあった場合のフェーズの構築、テスト、およびデプロイを自動化します。機能とアップデートをすばやく、信頼性の高い方法で配信できます。GitHub などの AWS CodePipeline サードパーティーサービスと、または独自のカスタムプラグインと簡単に統合できます。では AWS CodePipeline、使用した分のみお支払いいただきます。前払い金や長期契約はありません。詳細については[AWS CodePipeline](#)を参照してください。

## Note

CodeCommit、CodeBuild、CodeDeploy、および CodePipeline を単一の RFC でオンボードするには、管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (マネージドオートメーション) (ct-3qe6io8t6jtny) 変更タイプを送信し、CodeBuild、CodeDeploy、および CodePipeline の 3 つのサービスをリクエストします。次に、`customer_codebuild_service_role`、`customer_codedeploy_service_role`、`aws_code_pipeline_service_role` の 3 つのロールすべてがアカウントにプロビジョニングされます。アカウントでプロビジョニングした後、フェデレーションソリューションでロールをオンボードする必要があります。AMS の CodePipeline は、「ソースステージの Amazon CloudWatch Events」をサポートしていません。これは、最小特権モデルと AMS 変更管理プロセスをバイパスするサービスロールとポリシーを作成するための昇格されたアクセス許可が必要なためです。

## AWS Managed Services の CodePipeline に関するよくある質問

Q: AMS アカウントの CodePipeline へのアクセスをリクエストするにはどうすればよいですか？

関連するアカウントの のサービスリクエストを送信して、CodePipeline `customer_code_pipeline_console_role` へのアクセスをリクエストします。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

この時点で、AMS Operations はこのサービスロールをアカウントにもデプロイします `aws_code_pipeline_service_role_policy`。

Q: AMS アカウントでの CodePipeline の使用にはどのような制限がありますか？

はい。CodePipeline の機能、ステージ、プロバイダーは以下に限定されます。

1. デプロイステージ: Amazon S3 に限定、および AWS CodeDeploy
2. ソースステージ: Amazon S3、AWS CodeCommit、BitBucket、GitHub に限定
3. ビルドステージ: AWS CodeBuild および Jenkins に限定
4. 承認ステージ: Amazon SNS に限定
5. テストステージ: Jenkins AWS CodeBuild、BlazeMeter、Ghost Inspector UI テスト、Micro Focus StormRunner Load、Runscope API Monitoring に限定
6. 呼び出しステージ: Step Functions と Lambda に限定

 Note

AMS オペレーションは `customer_code_pipeline_lambda_policy` アカウントにデプロイされます。Lambda 呼び出しステージの Lambda 実行ロールにアタッチする必要があります。このポリシーを追加する Lambda サービス/実行ロール名を指定してください。カスタム Lambda サービス/実行ロールがない場合、AMS は という名前の新しいロールを作成します。これは `customer_code_pipeline_lambda_execution_role` `customer_lambda_basic_execution_role` と一緒に のコピーになります `customer_code_pipeline_lambda_policy`。

Q: AMS アカウントで CodePipeline を使用するための前提条件または依存関係は何ですか？

AWS がサポートする サービスは AWS CodeCommit AWS CodeBuild、CodePipeline の起動前または起動と同時に起動 AWS CodeDeploy する必要があります。

## AMS SSP を使用して AMS アカウント AWS Compute Optimizer でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS Compute Optimizer 機能に直接アクセスします。は、ワークロードに最適な AWS コンピューティングリソース AWS Compute Optimizer を推奨し、機械学習を使用して過去の使用率メトリク

ス进行分析し、コストを削減し、パフォーマンスを向上させます。コンピューティング (Amazon EC2 および ASGs) の過剰プロビジョニングにより、不要なインフラストラクチャコストが発生し、コンピューティングのプロビジョニングが不足すると、アプリケーションのパフォーマンスが低下する可能性があります。Compute Optimizer は、使用率データに基づいて Amazon EC2 Auto Scaling グループの一部であるインスタンスタイプを含め、最適な Amazon EC2 インスタンスタイプを選択するのに役立ちます。詳細については[AWS Compute Optimizer](#)を参照してください。

## AWS Managed Services の Compute Optimizer に関するよくある質問

Q: AMS アカウントの Compute Optimizer へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (マネージドオートメーション) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_compute_optimizer_readonly_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Compute Optimizer の使用にはどのような制限がありますか？

制限はありません。の完全な機能は AWS Compute Optimizer、AMS アカウントで使用できます。

Q: AMS アカウントで Compute Optimizer を使用するための前提条件または依存関係は何ですか？

- アカウントでサービスを有効にするには、AMS Ops を承認する RFC (管理 | その他 | その他 | 更新) を送信する必要があります。デプロイ中に、メトリクスの収集とレポートの生成を可能にするサービスリンクロール (SLR) が作成されます。SLR には `AWSServiceRoleForComputeOptimizer` というラベルが付けられています。詳細については、[「のサービスにリンクされたロールの使用」](#)を参照してください。 [AWS Compute Optimizer](#)
- CloudWatch メトリクスは、次のメトリクスに対して有効にする必要があります。
  - CPU 使用率: インスタンスで使用されている割り当てられた Amazon EC2 コンピューティングユニットの割合。このメトリクスは、選択したインスタンスでアプリケーションを実行するために必要な処理能力を識別します。
  - メモリ使用率: サンプル期間中に何らかの方法で使用されたメモリの量。このメトリクスは、選択したインスタンスでアプリケーションを実行するために必要なメモリを識別します。メモリ使用率は、統合 CloudWatch エージェントがインストールされているリソースについてのみ分析されます。詳細については、CloudWatch エージェントによるメモリ使用率の有効化」 (p. 10) を参照してください。

- **Network in:** インスタンスがすべてのネットワークインターフェイスで受信したバイト数。このメトリクスは、単一のインスタンスへの受信ネットワークトラフィックのボリュームを識別します。
- **ネットワーク出力:** インスタンスによってすべてのネットワークインターフェイスで送信されたバイト数。このメトリクスは、1 つのインスタンスからの送信ネットワークトラフィックの量を識別します。
- **ローカルディスク入出力 (I/O):** ローカルディスクの入出力オペレーションの数。このメトリクスは、インスタンスのルートボリュームのパフォーマンスを識別します。

## AMS SSP を使用して AMS アカウント AWS DataSync でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS DataSync 機能に直接アクセスします。は、オンプレミスストレージと Amazon S3、Amazon Elastic File System (Amazon Elastic File System)、または Amazon FSx の間で大量のデータをオンライン AWS DataSync に移動します。Amazon Elastic File System データ転送に関連する手動タスクは、移行を遅らせ、IT 運用に負担をかける可能性があります。DataSync は、コピージョブのスク립ト作成、転送のスケジュールとモニタリング、データの検証、ネットワーク使用率の最適化など、これらのタスクの多くを排除または自動的に処理します。DataSync ソフトウェアエージェントはネットワークファイルシステム (NFS) およびサーバーメッセージブロック (SMB) ストレージに接続するため、アプリケーションを変更する必要はありません。DataSync は、インターネットまたは AWS Direct Connect リンク経由で、オープンソースツールの最大 10 倍の速度で数百テラバイトと数百万のファイルを転送できます。DataSync を使用して、アクティブなデータセットまたはアーカイブをに移行したり AWS、データをクラウドに転送してタイムリーな分析と処理を行ったり、ビジネス継続 AWS 性のためにデータを にレプリケートしたりできます。

詳細については[AWS DataSync](#)を参照してください。

### AWS Managed Services での DataSync に関するよくある質問

Q: AMS アカウントの DataSync へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (マネージドオートメーション)  
(ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_datasync_console_role`。



アカウントでプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

タスクログをストリーミングするために使用する CloudWatch ロググループは「/aws/datasync」です。

Q: AMS アカウントでの DataSync の使用にはどのような制限がありますか？

の完全な機能は AWS DataSync、AMS アカウントで使用できます。

Q: AMS アカウントで DataSync を使用するための前提条件または依存関係は何ですか？

- Amazon S3 サービスロール を使用して実行される DataSync タスクに関連付けられたすべての S3 バケットには、Amazon DataSync S3 ARNs (Amazon リソースネーム) が必要です `customer_datsync_service_role`。
- DataSync エージェントの VPC エンドポイントとセキュリティグループは、VPC エンドポイントを使用する前に、管理 | その他 | その他 | 作成 (ct-1e1xtak34nx76) 変更タイプを使用して RFC でリクエストする必要があります。
- AWS DataSync エージェントはアプライアンスとして AMS で実行されます。AWS DataSync エージェントにパッチが適用され、サービスによって更新されます。詳細については、[AWS DataSync 「よくある質問」](#) を参照してください。
- AWS DataSync エージェントを起動するには、管理 | その他 | その他 | 作成 (ct-1e1xtak34nx76) 変更タイプを使用して RFC を送信し、エージェントのデプロイをリクエストします。AWS DataSync Amazon EC2 AMI ID、インスタンスタイプ、サブネット、セキュリティグループを指定し、既存の Amazon EC2 キーペアを参照するか、新しいキーペアの作成をリクエストします。

#### Note

AMS は、お客様に代わって AWS DataSync エージェントを手動でプロビジョニングするため、AWS DataSync Amazon EC2 AMI での WIGS 取り込みプロセスは必要ありません。

## AMS SSP を使用して AMS アカウント AWS Device Farm でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS Device Farm 機能に直接アクセスします。AWS Device Farm は、テストインフラストラク



チャをプロビジョニングおよび管理することなく、幅広いデスクトップブラウザと実際のモバイルデバイスでテストすることで、ウェブおよびモバイルアプリケーションの品質を向上させるアプリケーションテストサービスです。このサービスを使用すると、複数のデスクトップブラウザまたは実際のデバイスでテストを同時に実行してテストスイートの実行を高速化し、ビデオとログを生成して、アプリの問題をすばやく特定できます。

詳細については[AWS Device Farm](#)を参照してください。

## AWS Device Farm AWS Managed Servicesに関するよくある質問

Q: AWS Device Farm AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (マネージドオートメーション) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_devicefarm_role`。

アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウント AWS Device Farm で を使用することにはどのような制限がありますか？

AWS Device Farm サービスへのフルアクセスは、「Name」タグで AMS 名前空間を使用することを除いて提供されます。

Q: AMS アカウント AWS Device Farm で を使用するための前提条件または依存関係は何ですか？

なし。

## AMS SSP を使用して AMS アカウント AWS Elastic Disaster Recovery でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS Elastic Disaster Recovery 機能に直接アクセスします。は、手頃な価格のストレージ、最小限のコンピューティング、point-in-timeリカバリを使用して、オンプレミスおよびクラウドベースのアプリケーションの高速で信頼性の高いリカバリにより、ダウンタイムとデータ損失 AWS Elastic Disaster Recovery を最小限に抑えます。を使用して、サポートされているオペレーティングシステムで実行されているオンプレミスまたはクラウドベースのアプリケーションをレプリケートする場合 AWS Elastic Disaster Recovery 、IT レジリエンスを高めることができます。AWS マネジメントコ

ンソール を使用して、レプリケーションと起動の設定、データレプリケーションのモニタリング、ドリルまたはリカバリ用のインスタンスの起動を行います。

詳細については[AWS Elastic Disaster Recovery](#)を参照してください。

## AWS Elastic Disaster Recovery AWS Managed Servicesに関するよくある質問

Q: AWS Elastic Disaster Recovery AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (マネージドオートメーション) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_drs_console_role`。

アカウントでプロビジョニングされたロールは、フェデレーションソリューションでオンボードする必要があります。

Q: AMS アカウント AWS Elastic Disaster Recovery で を使用することにはどのような制限がありますか？

AMS アカウント AWS Elastic Disaster Recovery で使用する制限はありません。

Q: AMS アカウント AWS Elastic Disaster Recovery で を使用するための前提条件または依存関係は何ですか？

- コンソールロールにアクセスしたら、Elastic Disaster Recovery サービスを初期化して、アカウント内で必要な IAM ロールを作成する必要があります。
- インスタンスプロファイルのクローンを作成して `AWSElasticDisasterRecoveryEc2InstancePolicy` ポリシーを `customer-mc-ec2-instance-profile` にアタッチするには、変更タイプ管理 | アプリケーション | IAM インスタンスプロファイル | 変更タイプ `ct-0ixp4ch2tiu04` RFC を作成 (マネージドオートメーション) する必要があります。新しいポリシーをアタッチするマシンを指定する必要があります。
- インスタンスがデフォルトのインスタンスプロファイルを使用していない場合、AMS は自動化 `AWSElasticDisasterRecoveryEc2InstancePolicy` を通じてアタッチできます。
- クロスアカウントリカバリには、顧客所有の KMS キーを使用する必要があります。ターゲットアカウントへのアクセスを許可するには、ソースアカウントの KMS キーをポリシーに従って更新する必要があります。詳細については、[「EBS 暗号化キーをターゲットアカウントと共有する」](#)を参照してください。

- ロール `customer_drs_console_role` の表示を切り替える場合は、KMS キーポリシーを更新して、ポリシーの表示を許可する必要があります。
- クロスアカウント、クロスリージョンディザスタリカバリの場合、AMS はソースアカウントとターゲットアカウントを信頼されたアカウントとして設定し、[フェイルバックロールとAWS 右サイジングロール](#)をデプロイする必要があります CloudFormation。

## AMS SSP を使用して AMS アカウント AWS Elemental MediaConvert でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS Elemental MediaConvert 機能に直接アクセスします。AWS Elemental MediaConvert は、ブロードキャストグレードの機能を持つファイルベースのビデオトランスコーディングサービスです。これにより、ブロードキャストおよびマルチスクリーン配信用の video-on-demand (VOD) コンテンツを大規模に作成できます。このサービスは、高度なビデオおよびオーディオ機能と、シンプルなウェブサービスインターフェイスと従量制料金。を使用すると AWS Elemental MediaConvert、独自のビデオ処理インフラストラクチャの構築と運用の複雑さを心配することなく、魅力的なメディアエクスペリエンスの提供に集中できます。

詳細については[AWS Elemental MediaConvert](#)を参照してください。

### AWS Managed Services での MediaConvert に関するよくある質問

Q: AMS アカウントの MediaConvert へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (マネージドオートメーション) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_mediaconvert_author_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

2 番目のロール が提供されます。これは `customer_MediaConvert_Default_Role`、ソース S3 バケットから読み取り、出力を送信先 S3 バケットに書き込むため、およびデジタル著作権管理 (DRM) が必要な場合に API ゲートウェイを呼び出すために MediaConvert によって使用されます。

Q: AMS アカウントでの MediaConvert の使用にはどのような制限がありますか？

AMS での MediaConvert の使用に制限はありません。

Q: AMS アカウントで MediaConvert を使用するための前提条件または依存関係は何ですか？

AMS アカウントで MediaConvert を使用するための前提条件や依存関係はありません。

## AMS SSP を使用して AMS アカウント AWS Elemental MediaLive でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントの AWS Elemental MediaLive 機能に直接アクセスします。AWS Elemental MediaLive はブロードキャストグレードのライブビデオ処理サービスです。これにより、接続されたテレビ、タブレット、スマートフォン、セットトップボックスなどTVs、ブロードキャストテレビやインターネットに接続されたマルチスクリーンデバイスに配信するための高品質のビデオストリームを作成できます。このサービスは、ライブビデオストリームをリアルタイムでエンコードし、より大きなサイズのライブビデオソースを取得し、視聴者に配信するためにより小さなバージョンに圧縮することで機能します。を使用すると AWS Elemental MediaLive、高度なブロードキャスト機能、高可用性、pay-as-you-go で、ライブイベントと 24 時間 365 日対応のチャンネルの両方にストリームを簡単に設定できます。AWS Elemental MediaLive では、ブロードキャストグレードのビデオ処理インフラストラクチャの構築と運用を複雑にすることなく、視聴者に魅力的なライブビデオエクスペリエンスの作成に集中できます。

詳細については[AWS Elemental MediaLive](#)を参照してください。

### AWS Managed Services での MediaLive に関するよくある質問

Q: AMS アカウントの MediaLive へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (マネージドオートメーション) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_medialive_author_role`。

この RFC の一部として、2 番目のロールがアカウントにデプロイされます。 `customer_medialive_service_role` このロールは、Amazon S3、MediaStore、CloudWatch Logs などの他のサービスとやり取りするために、Media Live チャンネルと入力に割り当てることができます。 CloudWatch

アカウントにロールがプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの MediaLive の使用にはどのような制限がありますか？

AMS での MediaLive の使用に制限はありません。

Q: AMS アカウントで MediaLive を使用するための前提条件または依存関係は何ですか？

AMS アカウントで MediaLive を使用するための前提条件や依存関係はありません。

## AMS SSP を使用して AMS アカウント AWS Elemental MediaPackage でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS Elemental MediaPackage 機能に直接アクセスします。は、インターネット経由で配信するためのビデオ AWS Elemental MediaPackage を確実に準備して保護します。AWS Elemental MediaPackage は 1 つのビデオ入力から、接続されたテレビ、携帯電話、コンピュータ、タブレット、ゲームコンソールで再生するようにフォーマットされたビデオストリームを作成します。これにより、DVRs で一般的に見られるような、視聴者向けの一般的な動画機能 (起動、一時停止、巻き戻しなど) を簡単に実装できます。AWS Elemental MediaPackage は、デジタル著作権管理 (DRM) を使用してコンテンツを保護することもできます。は負荷に応じて自動的に AWS Elemental MediaPackage スケーリングするため、視聴者は必要な容量を事前に正確に予測することなく、常に優れたエクスペリエンスを得ることができます。

詳細については[AWS Elemental MediaPackage](#)を参照してください。

## AWS Managed Servicesでの MediaPackage に関するよくある質問

Q: AWS Elemental MediaPackage AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (マネージドオートメーション) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_mediapackage_author_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

2 番目のロール が提供されます。これは `customer_mediapackage_service_role`、S3 や Secrets Manager などの他のサービスとやり取りするための Media Live チャンネルと入力に割り当てることができます。

Q: AMS アカウントでの MediaPackage の使用にはどのような制限がありますか？

AMS での MediaPackage の使用に制限はありません。

Q: AMS アカウントで MediaPackage を使用するための前提条件または依存関係は何ですか？

AMS アカウントで MediaPackage を使用するための前提条件や依存関係はありません。

## AMS SSP を使用して AMS アカウント AWS Elemental MediaStore でプロビジョニングする

### Note

慎重に検討した結果、AWS は 2025 年 11 月 13 日に MediaStore の廃止を決定しました。MediaStore のアクティブなお客は、サービスのサポートが終了する 2025 年 11 月 13 日まで MediaStore を通常どおり使用できます。この日以降、MediaStore またはこのサービスが提供する機能を使用できなくなります。

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS Elemental MediaStore 機能に直接アクセスします。AWS Elemental MediaStore は、メディア用に最適化された AWS ストレージサービスです。これにより、ライブストリーミングビデオコンテンツを配信するために必要なパフォーマンス、一貫性、低レイテンシーが得られます。AWS Elemental MediaStore は、ビデオワークフローのオリジンストアとして機能します。その高性能機能は、最も要求の厳しいメディア配信ワークロードのニーズを満たすとともに、長期的で費用対効果の高いストレージを提供します。詳細については[AWS Elemental MediaStore](#)を参照してください。

### AWS Managed Services の MediaStore に関するよくある質問

Q: AMS アカウントの MediaStore へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (ct-1w8z66n899dct) 変更タイプで RFC を送信して MediaStore へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_mediastore_author_role`。この RFC の一部として、2 番目のロールがアカウントにデプロイされます。ロールは `MediaStoreAccessLogs`、この機能を有効にすることを選択した場合、MediaStore サービスが CloudWatch でアクティビティをログに記録するために使用されます。アカウントにプロビジョニングされたら、フェデレーションリレーションでロールをオンボードする必要があります。

この時点で、AMS Operations はこのサービスロールをアカウントにもデプロイします `aws_code_pipeline_service_role_policy`。

Q: AMS アカウントでの MediaStore の使用にはどのような制限がありますか？

AMS での MediaStore の使用に制限はありません。



Q: AMS アカウントで MediaStore を使用するための前提条件または依存関係は何ですか？

AMS アカウントで MediaStore を使用するための前提条件や依存関係はありません。

## AMS SSP を使用して AMS アカウント AWS Elemental MediaTailor でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS Elemental MediaTailor 機能に直接アクセスします。AWS Elemental MediaTailor は、ブロードキャストレベルのquality-of-serviceを犠牲にすることなく、ビデオプロバイダーが個別にターゲットを絞った広告をビデオストリームに挿入します。を使用すると AWS Elemental MediaTailor、ライブビデオまたはオンデマンドビデオの視聴者は、コンテンツとパーソナライズされた広告を組み合わせたストリームを受け取ります。ただし、他のパーソナライズされた広告ソリューションとは異なり、動画と広告は AWS Elemental MediaTailor、視聴者のエクスペリエンスを向上させるためにブロードキャストグレードの動画品質で配信されます。は、クライアント側とサーバー側の広告配信メトリクスの両方に基づいて自動レポート AWS Elemental MediaTailor を提供し、広告のインプレッションと視聴者の動作を正確に測定します。を使用して、前払いコストなしで、予期しない需要の高い視聴イベントを簡単に収益化できます AWS Elemental MediaTailor。また、広告配信レートも向上し、すべての動画からより多くの収益を得るのに役立ちます。また、さまざまなコンテンツ配信ネットワーク、広告決定サーバー、クライアントデバイスで動作します。

詳細については[AWS Elemental MediaTailor](#)を参照してください。

## AWS Managed Services の MediaTailor に関するよくある質問

Q: AMS アカウントの MediaTailor へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (ct-1w8z66n899dct) 変更タイプで RFC を送信して、MediaTailor へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: customer-mediatailor-role。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの MediaTailor の使用にはどのような制限がありますか？

AMS での MediaTailor の使用に制限はありません。

Q: AMS アカウントで MediaTailor を使用するための前提条件または依存関係は何ですか？

AMS アカウントで MediaTailor を使用するための前提条件や依存関係はありません。



## AMS SSP を使用して AMS アカウント AWS Global Accelerator でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Global Accelerator 機能に直接アクセスします。Global Accelerator は、世界中のユーザーが使用するインターネットアプリケーションの可用性とパフォーマンスを向上させるアクセラレーターを作成するネットワークレイヤーサービスです。詳細については、「[Global Accelerator](#)」を参照してください。

### AWS Managed Services での Global Accelerator に関するよくある質問

よくある質問と回答：

Q: Global Accelerator を AMS アカウントでセットアップするようにリクエストするにはどうすればよいですか？

AWS サービス RFC (管理 | AWS サービス | セルフプロビジョニングサービス) の送信を通じてアクセスをリクエストします。この RFC を通じて、次の IAM ロールがアカウントにプロビジョニングされます: `customer_global_accelerator_console_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでコンソールロールをオンボードする必要があります。

Q: AMS アカウントでの Global Accelerator の使用にはどのような制限がありますか？

Global Accelerator は、[AWS リージョン表](#)に記載されている複数の AWS リージョンのエンドポイントをサポートするグローバルサービスです。

Q: AMS アカウントで Global Accelerator を使用するための前提条件または依存関係は何ですか？

Global Accelerator でアクセラレーターを設定するときは、静的 IP アドレスを 1 つ以上の AWS リージョンのリージョンエンドポイントに関連付けます。標準アクセラレーターの場合、エンドポイントは Network Load Balancer、Application Load Balancer、Amazon EC2 インスタンス、または Elastic IP アドレスです。カスタムルーティングアクセラレーターの場合、エンドポイントは 1 つ以上の EC2 インスタンスを持つ Virtual Private Cloud (VPC) サブネットです。

## AMS SSP を使用して AMS アカウント AWS Glue でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS Glue 機能に直接アクセスします。AWS Glue は、分析用のデータの準備とロードに役立つフルマネージド型の抽出、変換、ロード (ETL) サービスです。数回クリックするだけで、ETL ジョブ

を作成して実行できます AWS マネジメントコンソール。に保存されている AWS Glue データをポイントすると AWS、はデータ AWS Glue を検出し、関連するメタデータ (テーブル定義やスキーマなど) を に保存します AWS Glue Data Catalog。カタログ化されると、データはすぐに検索可能で、クエリ可能で、ETL アクションに使用できます。詳細については[AWS Glue](#)を参照してください。

## AWS Glue AWS Managed Servicesに関するよくある質問

よくある質問と回答：

Q: AMS アカウントでの設定 AWS Glue をリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 変更タイプを追加 (ct-1w8z66n899dct) で RFC を送信 AWS Glue して、へのアクセスをリクエストします。この RFC は、次の IAM ロールをアカウントにプロビジョニングします。

- customer\_glue\_console\_role
- customer\_glue\_service\_role

上記のロールには、以下のアタッチされたポリシーが含まれます。

- customer\_glue\_secrets\_manager\_policy
- customer\_glue\_deny\_policy

アカウントでロールがプロビジョニングされたら、フェデレーションソリューションにロールをオンボードする必要があります。

クローラ、ジョブ、開発エンドポイント (特定のユースケースに必要なロール) にアクセスするには、デプロイ | 高度なスタックコンポーネント | Identity and Access Management (IAM) | エンティティまたはポリシーの作成 (ct-3dpg8mdd9jn1r) を使用して RFC を送信します。

Q: AMS アカウント AWS Glue でを使用することにはどのような制限がありますか？

制限はありません。の完全な機能は AWS Glue、AMS アカウントで使用できます。ETL スクリプトを作成およびテストできるインタラクティブな環境では、AWS Glue Studio で Notebooks を使用します。AWS Glue インタラクティブセッションとジョブノートブックは、で使用する AWS Glue AWS Glue のサーバーレス機能であり、AWS Glue サービスロールを使用します。

AWS Glue 2.0 より前：AWS Glue ノートブックは、アカウントで Amazon EC2 インスタンスを起動する非マネージドリソースです。ベストプラクティスとして、独自の Amazon EC2 インスタンス

を起動し、ノートブック環境と開発をサポートするために必要なソフトウェアをインストールします。詳細については、[「チュートリアル: ETL スクリプトをテストおよびデバッグするためのローカル Apache Zeppelin ノートブックのセットアップ」](#) および [「スクリプトの開発に開発エンドポイントを使用する」](#) を参照してください。

Q: AMS アカウント AWS Glue で 使用するための前提条件または依存関係は何ですか？

AWS Glue は、Amazon S3、CloudWatch、CloudWatch Logs に依存しています。推移的な依存関係はデータソースによって異なり、他の AWS Glue サービス機能が とやり取りしている可能性があります (Amazon Redshift、Amazon RDS、Athena など)。

## AMS SSP を使用して AMS アカウント AWS Lake Formation でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS Lake Formation 機能に直接アクセスします。AWS Lake Formation は、安全なデータレイクを数日で簡単にセットアップできるサービスです。データレイクは、分析用に準備および選別され、セキュリティ保護されたリポジトリで、すべてのデータを元の形式で保存します。データレイクを使用すると、データサイロを分解し、さまざまな種類の分析を組み合わせることでインサイトを獲得し、優れたビジネス意思決定を導くことができます。

Lake Formation を使用したデータレイクの作成は、データソースおよび適用するデータアクセスとセキュリティポリシーを定義するのと同様に簡単です。Lake Formation は、データベースやオブジェクトストレージからのデータの収集とカタログ化、新しい Amazon S3 データレイクへのデータの移動、Machine Learning アルゴリズムを使用したデータのクリーンアップと分類、機密データへの安全なアクセスを支援します。ユーザーは、利用可能なデータセットとその適切な使用状況を説明する一元化されたデータカタログにアクセスできます (詳細については、[AWS Glue 「よくある質問」](#) を参照してください)。その後、ユーザーはこれらのデータセットを、[Amazon Redshift](#)、[Amazon Athena](#)、Amazon [EMR](#) for Apache Spark (ベータ版) などの分析サービスと機械学習サービスの選択で活用します。Lake Formation は、 で利用可能な機能に基づいています[AWS Glue](#)。

詳細については[AWS Lake Formation](#)を参照してください。

## AWS Managed Services での Lake Formation に関するよくある質問

Q: AWS Lake Formation AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (マネージドオートメーション)

(ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_lakeformation_data_analyst_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

さらに、次の 2 つのロールはオプションです。

- `customer_lakeformation_admin_role`
- `customer_lakeformation_workflow_role`

管理者権限の場合、同じ SSPS 変更タイプ (ct-3qe6io8t6jtny)

`customer_lakeformation_admin_role`の一部としてロールをオンボードすることを選択できます。

AWS Lake Formation コンソールでブループリントを作成する場合は、管理 |

AWS サービス | セルフプロビジョニングサービス | (マネージドオートメーション)

(ct-3qe6io8t6jtny) 変更タイプを追加し、明示的に を追加して をデプロイする必要があります

`customer_lakeformation_workflow_role`。RFC では、ブループリントの作成時にバ

ケットがソースである場合は、S3 バケット名を指定する必要があります。S3 バケットは AWS

CloudTrail、設計図タイプが Classic Load Balancer Logs または Application Load Balancer Logs の場合に適用されます。

Q: AMS アカウント AWS Lake Formation で を使用することにはどのような制限がありますか？

Lake Formation の全機能は AMS で利用できます。

Q: AMS アカウント AWS Lake Formation で を使用するための前提条件または依存関係は何ですか？

Lake Formation は AWS Glue サービスと統合されるため、AWS Glue ユーザーは Lake Formation

アクセス許可を持つデータベースとテーブルにのみアクセスできます。さらに、AWS Athena およ

び Amazon Redshift ユーザーは、Lake Formation アクセス許可を持つ AWS Glue データベースと

テーブルのみをクエリできます。

## AMS SSP を使用して AMS アカウント AWS Lambda でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントの

AWS Lambda 機能に直接アクセスします。サーバーをプロビジョニングまたは管理せずにコードを

実行する AWS Lambda。消費したコンピューティング時間に対してのみ料金が発生します。コードが実行されていない場合は料金は発生しません。Lambda を使用すると、ほぼあらゆるタイプのアプリケーションまたはバックエンドサービスのコードを、すべて管理なしで実行できます。はコードをアップロードし、Lambda はコードの実行とスケールに必要なすべてを高可用性で処理します。他のサービスから自動的にトリガーするようにコードを設定することも AWS、ウェブやモバイルアプリから直接呼び出すこともできます。詳細については[AWS Lambda](#)を参照してください。

## AWS Managed Services の Lambda に関するよくある質問

Q: AWS Lambda AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (マネージドオートメーション) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、customer\_lambda\_admin\_roleおよび の IAM ロールをアカウントにプロビジョニングしますcustomer\_lambda\_basic\_execution\_role。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウント AWS Lambda で を使用することにはどのような制限がありますか？

- Lambda 関数は、イベントソースによって呼び出されるように設計されています。Lambda イベントソースとして使用できるサービスのリストについては、「[Using AWS Lambda with Other Services](#)」を参照してください。現在、これらのサービスの一部が AMS アカウントで利用できるわけではありません。利用できないサービスが必要な場合は、AMS CSDM と連携して例外を申請します。
- デフォルトでは、AMS は AWSLambdaBasicExecutionRoleおよび アクセスAWSXrayWriteOnlyAccess許可を含む基本的な Lambda 開始ロールを提供します。詳細については、[AWS Lambda 「開始ロール」](#)を参照してください。AMS VPC 内で Lambda 関数をプロビジョニングする機能など、追加のアクセス許可が必要な場合は、管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (マネージドオートメーション)(ct-3qe6io8t6jtny) 変更タイプを使用して RFC を送信します。

Q: AMS アカウント AWS Lambda で を使用するための前提条件または依存関係は何ですか？

開始するための前提条件や依存関係はありません AWS Lambdaが、特定のユースケースによっては、イベントソースを作成するために他の AWS サービスへのアクセスや、関数がさまざまなアクションを実行するための追加のアクセス許可が必要になる場合があります。追加のアクセス許可が必要な場合は、管理 | AWS サービス | セルフプロビジョニングサービス | (マネージドオートメーション) 変更タイプを追加 (ct-3qe6io8t6jtny) で RFC を送信します。



Q: いずれかのアカウントで Lambda 関数を実行するにはどうすればよいですか？

Lambda 関数をコアアカウントにデプロイするには、次のガイドラインを使用します。

- の SSPS AWS Lambda がオンボードされていることを確認します。
- AMS リソースが保護および準拠している限り、AMS の責任の下でこのデプロイを禁止する特定の制限はありません。
- AMS で Lambda 関数を作成する場合は、まず指定された SSPS ロールを使用する必要があります AWS Lambda。次に、AMS のサポートで関数をデプロイまたはサポートする場合は、CA に連絡して範囲外 (OOS) プロセスを開始します。

## AMS SSP を使用して AMS アカウント AWS License Manager でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS License Manager 機能に直接アクセスします。は AWS サービスと AWS License Manager 統合して、1 つの AWS アカウントを通じて複数の AWS アカウント、IT カタログ、オンプレミスのライセンスの管理を簡素化します。AWS License Manager では、管理者はライセンス契約の条件をエミュレートするカスタマイズされたライセンスルールを作成し、Amazon EC2 のインスタンスが起動されたときにこれらのルールを適用できます。のルール AWS License Manager では、インスタンスの起動を物理的に停止するか、侵害について管理者に通知することで、ライセンス違反を制限できます。詳細については[AWS License Manager](#)を参照してください。

### AWS Managed Services の License Manager に関するよくある質問

一般的な質問と回答：

Q: AMS アカウントでの設定 AWS License Manager をリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) change type を使用して RFC を送信 AWS License Manager して、へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: customer\_license\_manager\_role。License Manager IAM ロールがアカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウント AWS License Manager でを使用することにはどのような制限がありますか？

所有する AMI に AWS License Manager ルールを関連付けることができます (「Owned by me」でフィルタリングされます)。AMIs AMI に制限の関連付けを適用することを選択した場合 (例: はこ

の AMI の 100 個の vCPU のみをサポートできます )、制限を使い果たすと、その AMI での今後の起動はブロックされ、「ライセンスなし」というエラーが返されます。これは、このサービスの意図した動作です (ライセンスを使い果たすことはできません )。制限を使い果たしても AMI を再度起動する必要がある場合は、 で設定されたルールを変更する必要があります AWS License Manager。

Q: AMS アカウント AWS License Manager で 使用するための前提条件または依存関係は何ですか？

AMS アカウント AWS License Manager で使用する前提条件や依存関係はありません。

## AMS SSP を使用して AMS アカウント AWS Migration Hub でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS Migration Hub 機能に直接アクセスします。 は、複数の AWS およびパートナーソリューション間のアプリケーション移行の進行状況を追跡できる単一の場所 AWS Migration Hub を提供します。 Migration Hub を使用すると、アプリケーションポートフォリオ全体の移行のステータスを可視化しながら、ニーズに最適な AWS およびパートナー移行ツールを選択できます。 Migration Hub は、移行に使用されているツールに関係なく、個々のアプリケーションの主要なメトリクスと進行状況も提供します。これにより、すべての移行の進行状況の更新をすばやく取得し、問題を簡単に特定してトラブルシューティングし、移行プロジェクトに費やす全体的な時間と労力を削減できます。詳細については [AWS Migration Hub](#) を参照してください。

## AWS Managed Services の Migration Hub に関するよくある質問

一般的な質問と回答：

Q: AMS アカウントの Migration Hub へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (ct-1w8z66n899dct) 変更タイプで RFC を送信して Migration Hub へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: customer\_migrationhub\_author\_role。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: Migration Hub にはどのような制限がありますか？

なし。

Q: Migration Hub を有効にするための前提条件は何ですか？



AMS アカウントで Migration Hub の使用を開始するための前提条件はありません。ただし、Migration Hub 以外のアクセス許可は、サーバー情報をアップロードするためのアクセス許可を Amazon S3 に書き込むなど、サービスの管理中に必要になる場合があります。

## AMS SSP を使用して AMS アカウント AWS Outposts でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS Outposts 機能に直接アクセスします。AWS Outposts は、AWS インフラストラクチャ、AWS サービス、APIs、ツールを事実上あらゆるデータセンター、コロケーションスペース、またはオンプレミス施設に拡張し、一貫したハイブリッドエクスペリエンスを実現します。AWS Outposts は、オンプレミスシステム、ローカルデータ処理、またはローカルデータストレージへの低レイテンシーアクセスを必要とするワークロードに適しています。詳細については[AWS Outposts](#)を参照してください。

### AWS Outposts AWS Managed Servicesに関するよくある質問

一般的な質問と回答：

Q: AMS アカウントでの設定 AWS Outposts をリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) change type を使用して RFC を送信 AWS Outposts して、へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_outposts_role`。アカウントにロールがプロビジョニングされたら、フェデレーションソリューションにロールをオンボードする必要があります。

Q: AMS アカウント AWS Outposts でを使用することにはどのような制限がありますか？

AMS アカウント AWS Outposts での の使用に制限はありません。

Q: AMS アカウント AWS Outposts でを使用するための前提条件または依存関係は何ですか？

AMS アカウント AWS Outposts で使用する前提条件や依存関係はありません。

## AMS SSP を使用して AMS アカウント AWS Resilience Hub でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS Resilience Hub 機能に直接アクセスします。AWS Resilience Hub を使用すると、AWS アプ

リケーションを事前に準備し、中断から保護できます。Resilience Hub は、ソフトウェア開発ライフサイクルに統合される耐障害性評価と検証を提供し、耐障害性の弱点を明らかにします。Resilience Hub は、アプリケーションが目標復旧時間 (RTO) と目標復旧時点 (RPO) の目標を達成できるかどうかを推定し、本番環境にリリースされる前に問題を解決するのに役立ちます。AWS アプリケーションを本番環境にデプロイした後、Resilience Hub を使用してアプリケーションの回復体制の追跡を続行できます。停止が発生した場合、Resilience Hub はオペレーターに通知を送信して、関連する復旧プロセスを起動します。

## AWS Resilience Hub AWS Managed Servicesに関するよくある質問

一般的な質問と回答：

Q: AWS Resilience Hub AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (ct-1w8z66n899dct) 変更タイプで RFC を送信して、Resilience Hub へのアクセスをリクエストします。この RFC は、次の IAM ロールとポリシーをアカウントにプロビジョニングします。

IAM; ロール

- `customer_resiliencehub_console_role`
- `customer_resiliencehub_service_role`

ポリシー

- `customer_resiliencehub_console_policy`
- `customer_resiliencehub_service_policy`

アカウントでロールがプロビジョニングされたら、フェデレーションソリューション `customer_resiliencehub_console_role` でロールをオンボードする必要があります。

Q: AMS アカウント AWS Resilience Hub で を使用することにはどのような制限がありますか？

制限はありません。Resilience Hub のフル機能は、AMS アカウントで使用できます。

Q: AMS アカウント AWS Resilience Hub で を使用するための前提条件または依存関係は何ですか？

AMS アカウントで Resilience Hub を使用するための前提条件や依存関係はありません。

# AMS SSP を使用して AMS アカウント AWS Secrets Manager でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントの AWS Secrets Manager 機能に直接アクセスします。アプリケーション、サービス、IT リソースへのアクセスに必要なシークレットを保護する AWS Secrets Manager のに役立ちます。このサービスを使用すると、データベースクレデンシャル、API キー、およびその他のシークレットをライフサイクル全体で簡単にローテーション、管理、および取得できます。ユーザーとアプリケーションは Secrets Manager APIs を呼び出すことでシークレットを取得するため、機密情報をプレーンテキストでハードコードする必要がなくなります。Secrets Manager には、Amazon RDS、Amazon Redshift、Amazon DocumentDB の統合機能が組み込まれたシークレットローテーションが用意されています。また、このサービスは API キーや OAuth トークンなど、他のタイプのシークレットにも拡張できます。詳細については[AWS Secrets Manager](#)を参照してください。

## Note

デフォルトでは、AMS 演算子は、アカウントのデフォルト AWS KMS キー (CMK) を使用して暗号化 AWS Secrets Manager された のシークレットにアクセスできます。シークレットを AMS オペレーションにアクセスできるようにするには、シークレットに保存されているデータに適したアクセス許可を定義する AWS Key Management Service (AWS KMS) キーポリシーを持つカスタム CMK を使用します。

## AWS Managed Services の Secrets Manager に関するよくある質問

Q: AWS Secrets Manager AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (ct-3qe6io8t6jtny) 変更タイプで RFC を送信して Secrets Manager へのアクセスをリクエストします。この RFC は、customer\_secrets\_manager\_console\_role および の IAM ロールをアカウントにプロビジョニングしますcustomer-rotate-secrets-lambda-role。customer\_secrets\_manager\_console\_role は、シークレットをプロビジョニングおよび管理するための管理者ロールとして使用され、シークレットをローテーションする Lambda 関数の Lambda 実行ロールとしてcustomer-rotate-secrets-lambda-role使用されます。アカウントにプロビジョニングされたら、フェデレーションソリューションでcustomer\_secrets\_manager\_console\_role ロールをオンボードする必要があります。

Q: AMS アカウント AWS Secrets Manager で を使用することにはどのような制限がありますか？

のフル機能は、シークレットの自動ローテーション機能とともに、AMS アカウントで AWS Secrets Manager 使用できます。ただし、「ローテーションを実行するための新しい Lambda 関数の作成」を使用してローテーションを設定することはサポートされていません。これは、変更管理プロセスをバイパスする CloudFormation スタックの作成 (IAM ロールと Lambda 関数の作成) に昇格されたアクセス許可が必要なためです。AMS Advanced は、「既存の Lambda 関数を使用してローテーションを実行する」のみをサポートします。ここでは、Lambda 関数を管理して AWS Lambda SSPS 管理者ロールを使用してシークレットをローテーションします。AMS Advanced は、シークレットを更新するために Lambda を作成または管理しません。

Q: AMS アカウント AWS Secrets Manager で を使用するための前提条件または依存関係は何ですか？

次の名前空間は AMS が使用するために予約されており、への直接アクセスの一部としては使用できません AWS Secrets Manager。

- `arn:aws:secretsmanager:*:*:secret:ams-shared/*`
- `arn:aws:secretsmanager:*:*:secret:customer-shared/*`
- `arn:aws:secretsmanager:*:*:secret:ams/*`

## Secrets Manager (AMS SSPS) を使用したキーの共有

RFC、サービスリクエスト、またはインシデントレポートのプレーンテキストでシークレットを AMS と共有すると、情報開示インシデントが発生し、AMS はケースからの情報とキーを再生成するリクエストを編集します。

[AWS Secrets Manager](#) (Secrets Manager) は、この名前空間 で使用できます `customer-shared`。

Secrets Manager を使用したキーの共有に関するよくある質問

Q: Secrets Manager を使用して共有する必要があるシークレットのタイプは何ですか？

例としては、VPN 作成用の事前共有キー、認証キー (IAM、SSH)、ライセンスキー、パスワードなどの機密キーなどがあります。

Q: Secrets Manager を使用して AMS とキーを共有するにはどうすればよいですか？

1. フェデレーティッドアクセスと適切なロールを使用して、AWS マネジメントコンソールにログインします。

SALZ の場合は、Customer\_ReadOnly\_Role

MALZ の場合は、AWSManagedServicesChangeManagementRole。

2. [AWS Secrets Manager コンソール](#)に移動し、新しいシークレットを保存するをクリックします。
3. [その他のシークレット] を選択します。
4. シークレット値をプレーンテキストとして入力し、デフォルトの KMS 暗号化を使用します。[次へ] をクリックします。
5. シークレット名と説明を入力します。名前は常に customer-shared/ で始まります。たとえば、customer-shared/mykey2022 などです。[次へ] をクリックします。
6. 自動ローテーションを無効にしたまま、次へをクリックします。
7. Store を確認してクリックし、シークレットを保存します。
8. シークレットを識別して取得できるように、サービスリクエスト、RFC、またはインシデントレポートを通じてシークレット名を返信してください。

Q: Secrets Manager を使用してキーを共有するには、どのようなアクセス許可が必要ですか？

SALZ: customer\_secrets\_manager\_shared\_policy マネージド IAM ポリシーを探し、ポリシードキュメントが以下の作成ステップでアタッチされているものと同じであることを確認します。ポリシーが次の IAM ロールにアタッチされていることを確認します: Customer\_ReadOnly\_Role。

MALZ: ams-shared 名前空間で GetSecretValue アクションを許可する AWSManagedServicesChangeManagementRole ロールに AMSSecretsManagerSharedPolicy がアタッチされていることを確認します。

例:

```
{
  "Action": "secretsmanager:*",
  "Resource": [
    "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
    "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
  ],
  "Effect": "Allow",
```

```
"Sid": "AllowAccessToSharedNameSpaces"  
}
```

#### Note

セルフサービスでプロビジョニングされたサービス AWS Secrets Manager として を追加すると、必要なアクセス許可が付与されます。

## AMS SSP を使用して AMS アカウント AWS Security Hub CSPM でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS Security Hub CSPM 機能に直接アクセスします。AWS Security Hub CSPM では、内のセキュリティ状態 AWS と、セキュリティ業界標準およびベストプラクティスへの準拠を包括的に把握できます。Security Hub CSPM は、AWS アカウント、サービス、およびサポートされているサードパーティーパートナー間のセキュリティとコンプライアンスの検出結果を一元化して優先順位付けし、セキュリティの傾向を分析し、最も優先度の高いセキュリティ問題を特定するのに役立ちます。詳細については[AWS Security Hub CSPM](#)を参照してください。

### AWS Managed Services の Security Hub CSPM に関するよくある質問

Q: AWS Security Hub CSPM AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (ct-1w8z66n899dct) 変更タイプで RFC を送信して、Security Hub CSPM へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_securityhub_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントで Security Hub CSPM を使用することにはどのような制限がありますか？

アーカイブ機能は、潜在的なセキュリティおよび運用上のリスクとして認識されており、自己プロビジョニングサービスセキュリティロールの一部として制限されています。

Q: AMS アカウント AWS Security Hub CSPM で を使用するための前提条件または依存関係は何ですか？



AMS アカウント AWS Security Hub CSPM で使用する前提条件や依存関係はありません。

## AMS SSP を使用して AMS アカウント AWS Service Catalog AppRegistry でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで AppRegistry 機能に直接アクセスします。AppRegistry を使用すると、アプリケーションの検索、レポート、管理アクションを一元的に実行できます。ビルダーが 1 つの AWS アカウントでアプリケーションを作成することはめったにありません。通常、アプリケーションリソースは、開発、テスト、本番稼働などのライフサイクルフェーズごとに分離されます。AppRegistry を使用すると、定義した AWS アカウント全体ですべてのリソースコレクションをグループ化して表示できます。

AppRegistry を使用すると、AWS アプリケーション、アプリケーションに関連付けられているリソースのコレクション、およびアプリケーション属性グループを保存できます。詳細については、[AppRegistry とは](#)」を参照してください。

### よくある質問: AMS AWS Service Catalog AppRegistry 内

Q: AWS Service Catalog AppRegistry AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | (マネージドオートメーション)  
(ct-3qe6io8t6jtny) 変更タイプで RFC を送信して AppRegistry へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: customer-appregistry-console-role。アカウントでプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウント AWS Service Catalog AppRegistry で を使用することにはどのような制限がありますか？

'Name' タグで AMS 名前空間を使用する場合を除き、AppRegistry サービスへのフルアクセスが提供されます。

Q: AMS アカウント AWS Service Catalog AppRegistry で を使用するための前提条件または依存関係は何ですか？

AMS アカウントで AppRegistry を使用するための前提条件や依存関係はありません。



# AMS SSP を使用して AMS アカウント AWS Shield Advanced でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS Shield Advanced 機能に直接アクセスします。AWS Shield Advanced は、で実行されているアプリケーションを保護するマネージド型分散型サービス拒否 (DDoS) 保護サービスです。AWS Shield Advanced は、アプリケーションのダウンタイムとレイテンシーを最小限に抑える常時オンの検出と自動インライン緩和を提供するため、DDoS 保護のメリットを享受するために AWS Support を関与させる必要はありません。Standard AWS Shield と Advanced の 2 つの階層があります。AMS には Shield Advanced が用意されています。詳細については、[「Shield Advanced」](#) を参照してください。

すべての AWS お客様は AWS Shield Standard、追加料金なしで自動保護を利用できます。は、ウェブサイトまたはアプリケーションをターゲットとする最も一般的な、頻繁に発生するネットワークおよびトランスポートレイヤーの DDoS 攻撃に対して AWS Shield Standard 防御します。Amazon CloudFront および Amazon Route 53 AWS Shield Standard でを使用すると、すべての既知のインフラストラクチャ (レイヤー 3 および 4) 攻撃に対する包括的な可用性保護が得られます。

Amazon Elastic Compute Cloud (Amazon EC2)、Elastic Load Balancing (ELB)、Amazon CloudFront AWS Global Accelerator、Amazon Route 53 リソースで実行されているアプリケーションをターゲットとする攻撃に対する保護レベルを高めるには、にサブスクライブできます AWS Shield Advanced。

に付属するネットワークおよびトランスポートレイヤーの保護に加えて AWS Shield Standard、は、大規模で高度な DDoS 攻撃に対する追加の検出と軽減、攻撃に対するほぼリアルタイムの可視性、およびウェブアプリケーションファイアウォールとの統合 AWS Shield Advanced を提供します。AWS Shield Advanced または AWS WAF、は AWS Shield 、レスポンスチーム (SRT) への 24 時間 365 日アクセス、および Amazon Elastic Compute Cloud (Amazon EC2)、Elastic Load Balancing (Elastic Load Balancing)、Amazon CloudFront AWS Global Accelerator、および Amazon Route 53 料金の DDoS 関連のスパイクに対する保護も提供します。

## AWS Managed Servicesでの Shield Advanced に関するよくある質問

Q: AMS アカウントで Shield Advanced へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) 変更タイプで RFC を送信して、Shield Advanced へのアクセスをリクエストします。この RFC

は、`customer_shield_role`および の IAM ロールをアカウントにプロビジョニングします`aws_drt_shield_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

ロールがアカウントにデプロイされたら、`customer_shield_role` を使用してアカウントの AWS Shield Advanced へのサブスクリプションを確認できます。

 Note

の使用には、月額料金と 1 年間のコミットメントがあることに注意してください AWS Shield Advanced。さらに、AMS AWS Shield Advanced で を使用すると、AMS が AWS Shield (SRT) にエスカレートすることを許可します。SRT は、エスカレートされた分散サービス拒否 (DDoS) インシデント中にウェブアプリケーションファイアウォール (AWS WAF) ルールを変更する可能性があります。これらの変更は、AMS と連携して行われます。

Q: AMS アカウントでの Shield Advanced の使用にはどのような制限がありますか？

制限ではありませんが、Shield Advanced を使用すると がデプロイされるため`aws_drt_shield_role`、AWS Shield チーム (SRT) はエスカレーションされた DDoS インシデント中に AMS アカウント内の AWS WAF ルールに緊急変更を加えることができます。これは、DDoS 攻撃の迅速な修復のために AMS によって推奨され、SRT への AMS エスカレーション後に行われます。

Q: AMS アカウントで Shield Advanced を使用するための前提条件または依存関係は何ですか？

AMS アカウントで Shield Advanced を使用するための前提条件や依存関係はありません。

## AMS SSP を使用して AMS アカウント AWS Snowball Edge でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Snowball Edge 機能に直接アクセスします。Snowball Edge はペタバイト規模のデータ転送ソリューションで、安全なデバイスを使用して大量のデータを AWS クラウドとの間で転送します。Snowball Edge は、高いネットワークコスト、長い転送時間、セキュリティ上の懸念など、大規模なデータ転送に関する一般的な課題に対処します。Snowball Edge を使用して、分析データ、ゲノムデータ、ビデオライブラリ、イメージリポジトリ、バックアップを移行し、データセンターのシャットダウン、テープ交換、またはアプリケーション移行プロジェクトの一部をアーカイブできます。Snowball

Edge によるデータ転送はシンプル、高速、より安全であり、高速インターネットによるデータ転送コストの 5 分の 1 にすぎません。

Snowball Edge では、データを転送するためにコードを記述したり、ハードウェアを購入したりする必要はありません。まず、AWS マネジメントコンソールを使用して Snowball の [インポートジョブを作成する](#) と、Snowball デバイスが自動的に配送されます。到着したら、デバイスをローカルネットワークに接続し、Snowball クライアント (「クライアント」) をダウンロードして実行して接続を確立し、クライアントを使用してデバイスに転送するファイルディレクトリを選択します。次に、クライアントはファイルを暗号化し、高速でデバイスに転送します。転送が完了し、デバイスを返却する準備ができると、E Ink 配送ラベルが自動的に更新され、Amazon Simple Notification Service (Amazon SNS)、テキストメッセージ、または コンソールで直接ジョブステータスを追跡できます。詳細については [AWS Snowball Edge](#) を参照してください。

## AWS Managed Services での Snowball Edge に関するよくある質問

一般的な質問と回答：

Q: AWS Snowball Edge AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか？

AMS での Snowball Edge の実装は、2 ステップのプロセスです。

1. 管理を送信する | その他 | その他 | 変更タイプ (ct-1e1xtak34nx76) を作成し、AMS アカウントの Snowball Edge のサービスロールをリクエストします。
2. Management | AWS service | Self-provisioned service | Add change type (ct-1w8z66n899dct) を送信してユーザーアクセスをリクエストします。この RFC は、customer\_snowball\_console\_role、customer\_snowball\_export\_role およびの IAM ロールをアカウントにプロビジョニングします customer\_snowball\_import\_role。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウント AWS Snowball Edge で を使用することにはどのような制限がありますか？

の完全な機能は AWS Snowball Edge 、AMS アカウントで使用できます。

Q: AMS アカウント AWS Snowball Edge で を使用するための前提条件または依存関係は何ですか？

上記のように、サービスロールアカウントが必要です。

# AMS SSP を使用して AMS アカウント AWS Step Functions でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS Step Functions 機能に直接アクセスします。AWS Step Functions は、ビジュアルワークフローを使用して分散アプリケーションとマイクロサービスのコンポーネントを調整できるウェブサービスです。それぞれ別個の関数 (タスク) を実行する個々のコンポーネントからアプリケーションを構築することで、簡単にアプリケーションをスケールおよび変更できます。Step Functions を使えば、安心してコンポーネントを調整し、アプリケーションの関数を配置できます。Step Functions には、アプリケーションのコンポーネントを一連のステップとして視覚化するためのグラフィカルコンソールが用意されています。各ステップを自動的にトリガーして追跡し、エラーが発生したときに再試行するため、アプリケーションは毎回、想定どおりに順番に実行されます。また、Step Functions では各ステップの状態がログに記録されるため、問題が発生した場合は、問題を簡単に診断およびデバッグできます。詳細については[AWS Step Functions](#)を参照してください。

## AWS Managed Services の Step Functions に関するよくある質問

一般的な質問と回答：

Q: AWS Step Functions AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add change type (ct-1w8z66n899dct) を使用して RFC を送信 AWS Step Functions して、 へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_step_functions_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウント AWS Step Functions で を使用することにはどのような制限がありますか？

の完全な機能は AWS Step Functions 、AMS アカウントで使用できます。

Q: AMS アカウント AWS Step Functions で を使用するための前提条件または依存関係は何ですか？

実行時に、Step Functions で使用されるロールは、ステップ関数で使用されるサービスにアクセスできる必要があります。たとえば、ステップ関数は Lambda 関数に依存することができます。ステップ関数を作成するユーザーは、Lambda 関数を同時に作成している可能性があり、そのサービスへのアクセスもリクエストする必要があります。

# AMS SSP を使用して AMS AWS Systems Manager アカウントに Parameter Store をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで AWS Systems Manager Parameter Store 機能に直接アクセスします。AWS Systems Manager Parameter Store は、設定データ管理とシークレット管理のための安全な階層型ストレージを提供します。パスワード、データベース文字列、およびライセンスコードなどのデータをパラメータ値として保存することができます。値はプレーンテキストまたは暗号化されたデータとして保存できます。次に、パラメータの作成時に指定した一意の名前を使用して値を参照できます。スケーラビリティ、可用性、耐久性に優れた Parameter Store は AWS クラウドでサポートされています。詳細については、[AWS Systems Manager 「Parameter Store」](#) を参照してください。

## Note

ライフサイクル管理を備えた専用シークレットストアが必要な場合は、Parameter Store [AMS SSP を使用して AMS アカウント AWS Secrets Manager でプロビジョニングする](#) の代わりにを使用します。Secrets Manager は、シークレットを自動的にローテーションできるようにすることで、セキュリティとコンプライアンスの要件を満たすのに役立ちます。Secrets Manager は、Amazon RDS 上の MySQL、PostgreSQL、Amazon Aurora の統合を組み込み、Lambda 関数をカスタマイズすることで他のタイプのシークレットに拡張できます。

## AWS Systems Manager AWS Managed Services のパラメータストアに関するよくある質問

一般的な質問と回答：

Q: AMS アカウントの Systems Manager パラメータストアへのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add change type (ct-1w8z66n899dct) を使用して RFC を送信して、AWS Systems Manager Parameter Store へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_systemsmanager_parameterstore_console_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。



Q: AMS アカウントでの AWS Systems Manager Parameter Store の使用にはどのような制限がありますか？

AWS マネージドキーを使用する必要があります。アクセスはカスタム KMS キーの作成に制限されます。ただし、カスタムキーが必要な場合は、RFC を送信して、Deployment | Advanced Stack Components | KMS Key | Create change type (ct-1d84keiri1jhg) with this IAM role, customer\_systemsmanager\_parameterstore\_console\_role as the value for the IAMPrincipalsRequiringDecryptPermissions および IAMPrincipalsRequiringEncryptPermissionsPrincipal parameters を使用してカスタムマネージドキー (CMK) を作成します。KMS キーを作成したら、それを使用して Secure String を作成できます。

Q: AMS アカウントで AWS Systems Manager Parameter Store を使用するための前提条件または依存関係は何ですか？

前提条件はありませんが、SSM パラメータストアは KMS に依存して Secure String を作成するため、パラメータストアに保存されている値を暗号化および復号できます。

## AMS SSP を使用して AMS アカウントに AWS Systems Manager オートメーションをプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで AWS Systems Manager オートメーション機能に直接アクセスします。AWS Systems Manager Automation は、ランブック、アクション、サービスクォータを使用して、Amazon Elastic Compute Cloud インスタンスおよびその他の AWS リソースの一般的なメンテナンスおよびデプロイタスクを簡素化します。これにより、自動化を大規模に構築、実行、モニタリングできます。Systems Manager Automation は、Systems Manager がマネージドインスタンスで実行するアクションを定義する Systems Manager ドキュメントの一種です。マネージドインスタンス内でコマンドやオートメーションスクリプトを実行するなど、一般的なメンテナンスおよびデプロイタスクを実行するために使用されるランブック。Systems Manager には、Amazon Elastic Compute Cloud タグを使用してインスタンスの大規模なグループをターゲットにするのに役立つ機能と、定義した制限に従って変更をロールアウトするのに役立つ速度制御が含まれています。ランブックは、JavaScript Object Notation (JSON) または YAML を使用して記述されます。ただし、Systems Manager Automation コンソールの [Document Builder (ドキュメントビルダー)] を使用すると、ネイティブの JSON または YAML で作成しなくても、ランブックを作成できます。または、Systems Manager が提供するランブックを、ニーズに合った事前定義されたステップで使用することもできます。詳細については、AWS Systems Manager ドキュメントの「[ランブックの使用](#)」を参照してください。

**Note**

Systems Manager Automation は、ランブックで利用できる 20 のアクションタイプをサポートしていますが、AMS Advanced アカウントで使用するランブックの作成時に利用できるアクションの数は限られています。同様に、Systems Manager が提供するランブックは、限られた数だけ、直接使用することも、独自のランブック内から使用することもできます。詳細については、次の FAQ の制限を参照してください。

## AWS Systems Manager AWS Managed Services での自動化に関するよくある質問

一般的な質問と回答：

Q: AMS アカウントの Systems Manager Automation へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add change type (ct-1w8z66n899dct) を使用して RFC を送信して、AWS Systems Manager オートメーションへのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします：customer\_systemsmanager\_automation\_console\_role。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの AWS Systems Manager オートメーションの使用にはどのような制限がありますか？

マネージドインスタンス内でコマンドやスクリプトを実行するためだけに、自動化のために Systems Manager がサポートするアクションのセットを制限してランブックを作成する必要があります。使用できるアクションと制限の概要は次のとおりです。

### AWS Systems Manager 自動化の制限

| アクション                           | 説明                           | 制限           |
|---------------------------------|------------------------------|--------------|
| aws:assertAwsResourceProperty – | AWS リソースの状態またはイベントの状態をアサートする | EC2 インスタンスのみ |
| aws:aws:branch –                | 条件付きオートメーションステップを実行する        | 制限なし         |



| アクション                            | 説明                    | 制限                                                                                       |
|----------------------------------|-----------------------|------------------------------------------------------------------------------------------|
| aws:createTags –                 | AWS リソースのタグを作成する      | 作成した SSM オートメーションランブックのみ                                                                 |
| aws:executeAutomation –          | 別のオートメーションを実行する       | 作成したオートメーションランブックのみ                                                                      |
| aws:executeScript –              | スクリプトを実行する            | サービスに対して API コールを行わないスクリプトのみ                                                             |
| aws:pause –                      | オートメーションを一時停止する       | 制限なし                                                                                     |
| aws:runCommand –                 | マネージドインスタンスでコマンドを実行する | System Manager が提供するドキュメントのみを使用する<br>- AWS-RunShellScript および<br>AWS-RunPowerShellScript |
| aws:sleep –                      | オートメーションの遅延           | 制限なし                                                                                     |
| aws:waitForAwsResourceProperty – | AWS リソースプロパティを待機する    | EC2 インスタンスのみ                                                                             |

Systems Manager コンソール内から「Run Command」機能を使用して、Systems Manager が提供するランブック AWS-RunShellScript および AWS-RunPowerShellScript でコマンドまたはスクリプトを直接実行することもできます。これらのランブックをランブック内にネストして、追加の検証前や検証後、または複雑な自動化ロジックに対応することもできます。

ロールは最小特権の原則に従い、マネージドインスタンス内でコマンドやスクリプトを実行することを目的としたランブックの実行の詳細を作成、実行、取得するために必要なアクセス許可のみを提供します。AWS Systems Manager サービスが提供する他の機能に対するアクセス許可は付与されません。この機能を使用すると自動化ランブックを作成できますが、ランブックの実行を AMS 所有リソースの対象にすることはできません。

Q: AMS アカウントで AWS Systems Manager オートメーションを使用するための前提条件または依存関係は何ですか？

前提条件はありませんが、ランブックの作成中は、内部プロセスやコンプライアンスコントロールが準拠していることを確認する必要があります。また、本番稼働用リソースに対してランブックを実行する前に、ランブックを徹底的にテストすることをお勧めします。

Q: Systems Manager ポリシーを他の IAM ロールにアタッ

チ `customer_systemsmanager_automation_policy` できますか？

いいえ。他のセルフプロビジョニング対応サービスとは異なり、このポリシーはプロビジョニングされたデフォルトロールにのみ割り当てることができません `customer_systemsmanager_automation_console_role`。

他の SSPS ロールのポリシーとは異なり、この SSM SSPS ポリシーは他のカスタム IAM ロールと共有できません。これは、この AMS サービスがマネージドインスタンス内でコマンドまたはオートメーションスクリプトを実行する場合のみであるためです。これらのアクセス許可を他のカスタム IAM ロールにアタッチすることが許可され、他ののサービスに対するアクセス許可がある場合、許可されるアクションの範囲はマネージドサービスにまで及ぶ可能性があり、アカウントのセキュリティ体制が低下する可能性があります。

AMS 技術標準に照らして変更リクエスト (RFCs [「RFC セキュリティレビュー」](#)) を参照してください。

#### Note

AWS Systems Manager では、アカウントと共有されているランブックを使用できます。共有ランブックを使用する場合は注意を払い、デューディリジェンスチェックを実行することをお勧めします。ランブックを実行する前に、必ずコンテンツを確認して、それらが実行するコマンド/スクリプトを理解してください。詳細については、[「共有 SSM ドキュメントのベストプラクティス」](#) を参照してください。

## AMS SSP を使用して AMS アカウント AWS Transfer Family でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで AWS Transfer Family (Transfer Family) 機能に直接アクセスします。AWS Transfer Family は、セキュアファイル転送プロトコル (SFTP) 経由で Amazon Simple Storage Service (Amazon S3) ストレージとの間でファイルを転送できるフルマネージド AWS サービスです。SFTP は、Secure Shell (SSH) ファイル転送プロトコルとも呼ばれています。SFTP は、金融サービス、医療、広告、リテールなどのさまざまな業界間におけるデータ交換ワークフローに使用されます。

SFTP を使用すると、サーバーインフラストラクチャを実行する AWS ことなく、AWS の SFTP サーバーにアクセスできます。このサービスを使用して、エンドユーザーのクライアントと設定をそのまま維持 AWS しながら、SFTP ベースのワークフローをに移行できます。まずホスト名を SFTP サーバーエンドポイントに関連付け、ユーザーを追加して適切なレベルのアクセスでプロビジョニングします。これを行うと、ユーザーの転送リクエストは SFTP AWS サーバーエンドポイントから直接処理されます。詳細については、[AWS Transfer for SFTP](#)「」、[「SFTP 対応サーバーの作成」](#)を参照してください。

## AWS Transfer for SFTP AWS Managed Servicesに関するよくある質問

よくある質問と回答：

Q: AWS Transfer for SFTP AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add change type (ct-1w8z66n899dct) を使用して RFC を送信 AWS Transfer for SFTP して、 へのアクセスをリクエストします。この RFC を通じて、次の IAM ロールとポリシーがアカウントにプロビジョニングされます。

- `customer_transfer_author_role`。このロールは、コンソールを使用して SFTP サービスを管理するように設計されています。
- `customer_transfer_sftp_server_logging_role`。このロールは、SFTP サーバーにアタッチされるように設計されています。これにより、SFTP サーバーは CloudWatch にログをプルできます。
- `customer_transfer_sftp_user_role`。このロールは、SFTP ユーザーにアタッチされるように設計されています。これにより、SFTP ユーザーは S3 バケットとやり取りできます。
- `policy_customer_transfer_scope_down_policy`。このポリシーは、SFTP ユーザーに適用して、S3 バケットへのアクセスをホームフォルダに制限できるスコープダウンポリシーです。
- `customer_transfer_sftp_efs_user_role`。このロールは、SFTP ユーザーにアタッチされるように設計されています。これにより、SFTP ユーザーは EFS ファイルシステムとやり取りできます。

アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウント AWS Transfer for SFTP で を使用することにはどのような制限がありますか？

AWS SFTP 設定の転送は、AMS インフラストラクチャへの変更を防ぐために、「AMS-」または「MC-」プレフィックスのないリソースに制限されます。

Q: AMS アカウント AWS Transfer for SFTP で を使用するための前提条件または依存関係は何ですか？

- AWS Transfer for SFTP サーバーとユーザーを作成する前に、キーワード「転送」を含む名前の Amazon S3 バケットが必要です。
- 「顧客識別プロバイダー」を使用するには、API Gateway、Lambda 関数、ユーザーリポジトリ (AD、Secrets Manager など) をデプロイする必要があります。詳細については、「ID [プロバイダー AWS Transfer for SFTP の使用と操作のパスワード認証 AWS Secrets Manager](#)を有効にする」を参照してください。 <https://docs.aws.amazon.com/transfer/latest/userguide/authenticating-users.html>

## AMS SSP を使用して AMS アカウント AWS Transit Gateway でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントの AWS Transit Gateway 機能に直接アクセスします。AWS Transit Gateway は、Amazon Virtual Private Cloud (VPCs) とオンプレミスネットワークを単一のゲートウェイに接続できるサービスです。で実行されているワークロードの数が増えるにつれて AWS、増加に対応するために、複数のアカウントと Amazon VPCs にネットワークをスケールする必要があります。現在、ピアリングを使用して Amazon VPCs のペアを接続できます。ただし、接続ポリシーを一元管理することなく、多くの Amazon VPCs point-to-point 接続を管理することは、運用コストが高く、面倒な作業になる可能性があります。オンプレミス接続の場合は、AWS VPN を個々の Amazon VPC にアタッチする必要があります。このソリューションは、構築に時間がかかり、VPCs 増えた場合の管理が困難になる可能性があります。詳細については [AWS Transit Gateway](#) を参照してください。

## AWS Transit Gateway AWS Managed Services に関するよくある質問

一般的な質問と回答：

Q: AWS Transit Gateway AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add change type (ct-1w8z66n899dct) で RFC を送信 AWS Transit Gateway して、 へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: customer\_tgw\_console\_role。アカウントにプロ

ビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウント AWS Transit Gateway で を使用することにはどのような制限がありますか？

のフル機能は AWS Transit Gateway 、Transit Gateway ルーティングのルートテーブルの変更を除き、AMS シングルアカウントランディングゾーンアカウントで使用できます。管理 | その他 | その他 | 変更タイプの作成 (ct-1e1xtak34nx76) を送信してルートテーブルの変更をリクエストします。

**Note**

このサービスは、マルチアカウントランディングゾーン (MALZ) ではなく、シングルアカウントランディングゾーン (SALZ) でのみサポートされています。

Q: AMS アカウント AWS Transit Gateway で を使用するための前提条件または依存関係は何ですか？

AMS アカウント AWS Transit Gateway で使用する前提条件や依存関係はありません。

## AMS SSP を使用して AMS アカウントで AWS WAF ウェブアプリケーションファイアウォールをプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS WAF 機能に直接アクセスします。AWS WAF は、アプリケーションの可用性に影響を与えたり、セキュリティを侵害したり、過剰なリソースを消費したりする一般的なウェブエクスポイトからウェブアプリケーションを保護するウェブアプリケーションファイアウォール (AWS WAF) です。は、カスタマイズ可能なウェブセキュリティルールを定義することで、ウェブアプリケーションに対して許可またはブロックするトラフィックを制御します。を使用して AWS WAF、SQL インジェクションやクロスサイトスクリプティングなどの一般的な攻撃パターンをブロックするカスタムルールと、特定のアプリケーション用に設計されたルールを作成できます。

詳細については、「[AWS WAF - Web Application Firewall](#)」を参照してください。

AMS は、 のモニタリング (CloudWatch アラーム/イベント/MMS アラート) をサポートしていません AWS WAF。の性質上 AWS WAF、アプリケーションのカスタムルールを作成する必要があります。AMS はアプリケーションのコンテキストなしではアラームを定量化して作成できません。詳細については、「[AWS WAF - Web Application Firewall](#)」を参照してください。

## AWS WAF AWS Managed Servicesに関するよくある質問

一般的な質問と回答：

Q: AMS アカウントでの設定 AWS WAF をリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 変更タイプを追加 (ct-1w8z66n899dct) で RFC を送信 AWS WAF して、へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_waf_role`。アカウントに IAM AWS WAF ロールがプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: の使用にはどのような制限がありますか AWS WAF？

アクセス許可がプロビジョニングされたら、のすべての機能を使用できます AWS WAF。

Q: を使用するための前提条件または依存関係は何ですか AWS WAF？

AMS アカウント AWS WAF で使用する前提条件や依存関係はありません。

## AMS SSP を使用して AMS アカウント AWS Well-Architected Tool でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントの AWS Well-Architected Tool 機能に直接アクセスします。AWS Well-Architected Tool は、ワークロードの状態を確認し、最新の AWS アーキテクチャのベストプラクティスと比較するのに役立ちます。このツールは、クラウドアーキテクトが安全で高性能、回復力があり、効率的なアプリケーションインフラストラクチャを構築できるように開発された [AWS Well-Architected フレームワーク](#)に基づいています。このフレームワークは、アーキテクチャを評価するための一貫したアプローチを提供し、ソリューションアーキテクチャチームによって AWS 数万件のワークロードレビューに使用され、時間の経過とともにアプリケーションのニーズに合わせてスケールする設計を実装するためのガイダンスを提供します。詳細については[AWS Well-Architected Tool](#)を参照してください。

## AWS WA Tool AWS Managed Servicesに関するよくある質問

一般的な質問と回答：

Q: AWS Well-Architected Tool AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか？



管理 | AWS サービス | セルフプロビジョニングサービス | 変更タイプを追加 (ct-1w8z66n899dct) で RFC を送信 AWS Well-Architected Tool して、へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_well_architected_tool_console_admin_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウント AWS Well-Architected Tool でを使用することにはどのような制限がありますか？

の完全な機能は AWS Well-Architected Tool、AMS アカウントで使用できます。

Q: AMS アカウント AWS Well-Architected Tool でを使用するための前提条件または依存関係は何ですか？

AMS アカウント AWS Well-Architected Tool で使用する前提条件や依存関係はありません。

## AMS SSP を使用して AMS アカウント AWS X-Ray でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで AWS X-Ray (X-Ray) 機能に直接アクセスします。開発者 AWS X-Ray は、マイクロサービスアーキテクチャを使用して構築されたアプリケーションなど、本番稼働用の分散アプリケーションを分析およびデバッグできます。X-Ray を使用すると、アプリケーションとその基盤となるサービスのパフォーマンスを理解し、パフォーマンスの問題やエラーの根本原因を特定してトラブルシューティングできます。X-Ray は、アプリケーションを通過するリクエストの end-to-end ビューを提供し、アプリケーションの基礎となるコンポーネントのマップを表示します。X-Ray を使用して、シンプルな 3 層アプリケーションから数千のサービスで構成される複雑なマイクロサービスアプリケーションまで、開発中と本番環境の両方のアプリケーションを分析できます。詳細については [AWS X-Ray](#) を参照してください。

### AWS Managed Services での X-Ray に関するよくある質問

一般的な質問と回答：

Q: AWS X-Ray AMS アカウントのへのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) change type を送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_xray_console_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。さらに、Amazon EC2 インス



タンスから X-Ray にデータをプッシュ `customer_xray_daemon_write_instance_profile` するには、が必要です。このインスタンスプロファイルは、を受け取ると作成されます `customer_xray_console_role`。

AMS Operations にサービスリクエストを送信して、 `customer_xray_daemon_write_policy` を既存のインスタンスプロファイルに割り当てることも、AMS Operations が X-Ray を有効にしたときに作成されるインスタンスプロファイルを使用することもできます。

Q: AMS アカウント AWS X-Ray で を使用することにはどのような制限がありますか？

のフル機能は、KMS キー (AWS KMS キー) による暗号化を除き、AMS アカウントで使用できます。AWS X-Ray はデフォルトですべてのトレースデータを AWS X-Ray 暗号化します。デフォルトでは、X-Ray はトレースと関連データを保管中に暗号化します。保管中のデータをキーで暗号化する必要がある場合は、AWS マネージド KMS キー (`aws/xray`) または KMS カスタマー マネージド キーを選択できます。X-Ray 暗号化用の KMS カスタマー マネージド キーの場合は、管理 | その他 | その他 | 変更タイプ の作成 (`ct-1e1xtak34nx76`) を送信します。

Q: AMS アカウント AWS X-Ray で を使用するための前提条件または依存関係は何ですか？

AWS X-Ray は、AMS アカウントに既に実装されている Amazon S3、CloudWatch、CloudWatch Logs に依存しています。推移的な依存関係は、機能がやり取り AWS X-Ray しているデータソースやその他の AWS サービス (Amazon Redshift、Amazon RDS、Athena など) によって異なります。

## AMS SSP を使用して AMS アカウントで VM Import/Export をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで VM Import/Export 機能に直接アクセスします。VM Import/Export を使用すると、仮想マシンイメージを既存の環境から Amazon EC2 インスタンスに簡単にインポートし、オンプレミス環境にエクスポートし直すことができます。この機能により、IT セキュリティ、設定管理、コンプライアンス要件を満たすために構築した仮想マシンへの既存の投資を活用できます。これらの仮想マシンを `ready-to-use` インスタンスとして Amazon EC2 に取り込むことができます。インポートしたインスタンスをオンプレミスの仮想化インフラストラクチャにエクスポートして、IT インフラストラクチャ全体にワークロードをデプロイすることもできます。詳細については、[「VM Import/Export」](#) を参照してください。

## AWS Managed Services での VM Import/Export に関するよくある質問

よくある質問と回答：

Q: AMS アカウントの VM Import/Export へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add change type (ct-1w8z66n899dct) で RFC を送信して VM Import/Export へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ポリシーをプロビジョニングします: `customer_vmimport_policy`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

サービスがアカウントでアクションを実行するには、VM Import/Export サービスロールという追加のロールが必要です。

Q: AMS アカウントでの VM Import/Export の使用にはどのような制限がありますか？

- カスタムマシンイメージとデータボリュームをインポートする機能は、どちらも AMS VM Import/Export で使用できます。ただし、S3 へのアクセス許可は、アカウント内の情報へのアクセスを制限 `customer-vmimport-*` するために、名前に一致するバケットにアクションを制限するようにスコープダウンされています。
- イメージとスナップショットのインポートは、AMS VM Import/Export でサポートされています。ただし、セキュリティ対策のため、インスタンスのインポートおよびインスタンスのエクスポート機能は利用できません。
- さらに、制限されたデータや機密データをエクスポートするリスクを軽減するために、エクスポート機能が無効になっています。

Q: AMS アカウントで VM Import/Export を使用するための前提条件または依存関係は何ですか？

- AWS 環境にインポートするには、サポートされているディスクイメージを指定する必要があります。詳細については、[「VM Import/Export Requirements」](#)を参照してください。
- VM Import/Export には AWS コンソールからアクセスできません。このサービスには AWS CLI、AWS Tools for PowerShell、または AWS SDKs からアクセスする必要があります。または、変更タイプ `ct-117rmp64d5mnb: Deployment | Advanced stack components | Identity and Access Management (IAM) | Create EC2 instance profile` を送信して、インスタンスプロファイルのリクエストすることもできます。このインスタンスプロファイルにより、ツールはインスタンスからコマンドを実行できます。

# カスタマーマネージドモード

AWS Managed Services (AMS) カスタマーマネージドモードは、柔軟で要件に適応できるガバナンスモデルを提供します。これは、AMS が動作できないサービスやアプリケーションのフォールバックオプションと考えることができます。AMS は、このモードで作成されたアカウントでホストされるインフラストラクチャを運用しません。ただし、このモードでは、一元化されたマルチアカウント管理を活用できます。このモードでは、次のマルチアカウントランディングゾーン機能を活用できます。

- 自動アカウントデプロイ
- ネットワークアカウントの Transit Gateway を介した接続
- AMS Config ルールライブラリ
- ログ記録アカウントにログのコピーを保存する
- セキュリティアカウントへのカスタマーマネージド Guard Duty アラートの集約
- 一括請求
- カスタムサービスコントロールポリシーの有効化。

例: AMS によって管理されるオペレーティングシステムではない Ubuntu Pro でワークロードを実行する場合は、カスタマーマネージドアカウントを使用してワークロードをホストできます。また、カスタマーマネージドアカウントを通じてワークロードを統合し、AWS 組織全体での共有を通じて利用可能なリザーブドインスタンス/共有プランの一括割引を利用することもできます。

## カスタマーマネージドモードの開始方法

AMS カスタマーマネージドモードは、特別なマルチアカウントランディングゾーンアプリケーションアカウントを通じて使用できます。

カスタマーマネージドアプリケーションアカウントの作成方法などの詳細については、[「カスタマーマネージドアプリケーションアカウント」](#)を参照してください。

## AMS と AWS Service Catalog

AWS Managed Services (AMS) のサービスカタログを使用すると、組織は AWS 情報テクノロジー (IT) サービスのカタログを作成および管理でき、IT 管理者は承認された製品のカタログを作成、管理、およびアカウントのエンドユーザーに配布できます。エンドユーザーは、パーソナライズされ

たサービスのポータルで必要な製品にアクセスできます。管理者は、どのユーザーが各製品にアクセスできるかを制御して、組織のビジネスポリシーへの準拠を強制できます。管理者は、承認されたりソースをデプロイするためにエンドユーザーが Service Catalog への IAM アクセスのみを必要とするようにロールを設定することもできます。Service Catalog を使用すると、エンドユーザーが管理するカタログから必要な製品のみを見つけて起動できるため、組織は俊敏性とコスト削減の恩恵を受けることができます。

Service Catalog では、AMS マネージドアカウント (複数可) でリソースをプロビジョニングおよび更新するための AMS 変更リクエスト (RFC) プロセスの代わりに使用できます。AMS は、セキュリティ、コンプライアンス、プロビジョニング、可用性、パッチ、モニタリング、アラート、レポート、インシデント対応、コスト最適化など、Service Catalog を通じてプロビジョニングされたすべてのインフラストラクチャリソースに対して AWS を大規模に実行するために必要なすべてのインフラストラクチャオペレーションタスクを管理します。AMS マネージドアカウントで Service Catalog を使用すると、一般的にデプロイされる IT サービスを一元管理するためのメカニズムが提供され、ユーザーが必要とする承認済みの IT サービスのみをマネージド環境にすばやくデプロイしながら、一貫したガバナンスを実現できます。

## Service Catalog の開始方法

AMS で Service Catalog の使用を開始するには、AMS コンソールからサービスリクエストを送信して、Service Catalog へのアクセスをリクエストします。リクエストを送信すると、3 つの IAM ロールがアカウント (複数可) にデプロイされ、AMS (前 Transform 述) を呼び出す CloudFormation マクロを含む AMS マネージドスタックとともにデプロイされます。これにより、システムに製品を登録し、Service Catalog を介してプロビジョニングされたインフラストラクチャに対してオペレーションを実行できます。デプロイされた 3 つの IAM ロールには、IT 管理者が Service Catalog 管理者として製品を管理するためのロール、アプリケーション所有者とエンドユーザーが製品を設定、起動、管理するためのロール、および製品の起動または更新時に Service Catalog が使用するアクセス許可を定義する起動制約として使用されるロールが含まれます。

## 開始する前に AMS の Service Catalog

Service Catalog は、既存の AMS 変更リクエスト (RFC) プロセスを置き換えますか？

Service Catalog が有効になっているアカウントでは、事前定義された製品カタログを使用して AMS アカウントで IT サービスをプロビジョニングおよび更新する変更管理システムとして機能します。AMS はデフォルトのポートフォリオ/製品カタログを提供し、IT 管理者は独自の を作成および設定できます。Service Catalog は、Service Catalog を介してプロビジョニングされたスタックのみを承認します。同様に、Service Catalog を介してプロビジョニングされたサービスは

AMS RFC プロセスを通じて変更できません。Service Catalog の外部で変更すると、承認された製品設定からスタックがドリフトするためです。

AMS コンソールでサービスカタログを通じてプロビジョニングされたスタックを確認できますか？

はい。AMS コンソールで、サービスカタログを通じてプロビジョニングされたすべてのスタックを表示できます。サービスカタログを介してプロビジョニングされたスタックは、スタック ID 「SC-」によって簡単に識別できます。スタックは AMS コンソールで表示できますが、AMS RFC プロセスを通じて更新することはできません。AMS 変更管理システム (RFCs) へのアクセスは、アクセスリクエスト、パッチオーケストレーション、バックアップ RFCs。

Service Catalog を使用してスタックをプロビジョニングまたは更新する場合、対応する RFC が AMS コンソールにありますか？

AMS コンソールに表示される唯一の RFC は、スタックが最初にプロビジョニングされたときにスタックを AMS に登録する RFC です。この RFC は、Service Catalog を介してスタックが起動されたときにトリガーされる AMS 検証プロセスによって自動的にファイルされます。その他のプロビジョニングと変更は Service Catalog で直接追跡され、Service Catalog コンソールで表示できます。さらに、Service Catalog のプロビジョニング済み製品プラン機能を使用して、製品のプロビジョニングまたは更新の前にリソースに加えられる変更のリストを表示できます。

AMS マネージドアカウントで製品をプロビジョニングするために、特定の操作を行う必要がありますか？

はい。AMS アカウントでプロビジョニングされるすべての Service Catalog 製品には、その製品を定義する CFN テンプレートにこの JSON 行が含まれている必要があります。

```
"Transform":{"Name":"AmsStackTransform","Parameters":{"StackId":
{"Ref":"AWS::StackId"}}}
```

この CloudFormation コードスニペットは、リソースを AMS マネージドアカウントでプロビジョニングするために必要な AMS 検証をトリガーします。このコード行を製品定義の一部として含めるのはお客様の責任です。含まれていない場合、プロビジョニングは失敗し、「製品の作成に失敗しました」というエラーメッセージが表示されます。このアカウントは AMS によって管理されます。AMS アカウントのすべての製品には、テンプレートに AMS Transformコードが必要です。」

起動時に AMS のお客様に利用できない、または制限されている Service Catalog 機能はありますか？

はい。AMS のお客様は、初回起動時に以下の SC 機能を使用できません。

- Service Catalog によるアカウントの作成

- Service Catalog を介してすべての AWS サービスを AMS マネージドアカウントで起動する機能。AWS サービスの可用性は、AMS がサポートするサービス (マネージド型およびセルフプロビジョニング型) に限定されます。AMS がサポートするサービスの詳細については、AMS サービスの説明を参照してください。
- Service Catalog IT サービスマネージャー (ITSM) コネクタは、AMS インシデントレポートやサービスリクエストと通信しません。
- Service Catalog のクイックスタートとリファレンスアーキテクチャを、変更なしで活用する機能。AMS アカウントの Service Catalog 製品には、次の JSON コード行が含まれている必要があることに注意してください。

```
"Transform":{"Name":"AmsStackTransform","Parameters":{"StackId":{"Ref":"AWS::StackId"}}}
```

CNF テンプレートの。この行は一般的な AWS CloudFormation テンプレートの一部ではなく、明示的に追加する必要があることに注意してください。

- Terraform は現在、Service Catalog 製品のプロビジョニングのために AMS でサポートされていません。
- AWS CFN スタックセットは AMS ではサポートされていません。
- カスタム IAM ロールを作成することはできません。
- サービスアクションは以下に限定されます。
  - [AWS-RebootRdsInstance](#)
  - [AWS-RestartEC2Instance](#)
  - [AWS-StartEC2Instance](#)
  - [AWS-StartRdsInstance](#)
  - [AWS-StopEC2Instance](#)
  - [AWS-StopRdsInstance](#)
  - [AWS-CreatelImage](#)
  - [AWS-CreateRdsSnapshot](#)
  - [AWS-CreateSnapshot](#)

 Note

サービスアクションを作成するときは、実行ロールをエンドユーザーのアクセス許可、起動ロール、または選択したカスタム IAM ロールに設定できます。



選択した実行ロールには、サービスアクションを実行するための十分なアクセス許可が必要であり、Service Catalog による引き受けを許可する TrustPolicy が必要です。そうしないと、サービスアクションは実行時に失敗します。サービスアクションとして使用する正しいアクセス許可と信頼ポリシーを持つ `AWSManagedServicesServiceCatalogLaunchRole` を使用することをお勧めします。

AMS RFC システムの使用にはまだ何が必要ですか？

一般提供 (GA) では、RFCS を使用して以下のアクションを実行する必要があります。

- パッチオーケストレーターの設定
- バックアップポリシーの設定
- インスタンスアクセスのリクエスト
- AMS ガイドラインの範囲外のセキュリティグループを作成して割り当てる。
- ワークロード取り込みの実行 (WIGS)
- 「IAM ロールの作成」

Service Catalog CLI を使用して AMS マネージドアカウントの Service Catalog にアクセスすることはできますか？

はい。Service Catalog APIs は CLI で使用および有効化できます。Service Catalog アーティファクトの管理から、それらのアーティファクトのプロビジョニングと終了までのアクションを使用できます。詳細については、[AWS Service Catalog リソース](#)」を参照するか、最新の AWS SDK または CLI をダウンロードしてください。

顧客の承認済み製品のカatalogを作成、管理、配布するのは誰ですか？

お客様のCatalog管理者および/または IT 管理者、または割り当てられたリソースは、Service Catalog Catalog および承認済み製品の管理を担当します。

AMS AMIs?

2020 年 3 月以降に販売された AMS AMIs は、AWS Service Catalog を通じてデプロイできます。

Service Catalog を使用して AMS に移行するにはどうすればよいですか？

Service Catalog を使用してワークロードを AMS に移行するには、まず[ワークロード取り込み \(WIGs\)](#) プロセスに従って AMS に AMI を作成します。WIGS によって生成された AMI を使用して、Service Catalog で製品を作成します。これを行う方法については、[AWS Service Catalog - 開始方法](#)を参照してください。



# 必要なデータ (SKMS)、AMS の検索

AWS Managed Services (AMS) アカウントを使用するときに必要なデータを見つけるには、AMS サービスナレッジ管理または SKMS システムで呼び出します。AMS。

SKMS はサービスナレッジ管理システムの略で、お客様の AWS Managed Services (AMS) サービスに関連するすべての情報を指します。AMS には、データを検索するための SKMS API があります。

## トピック

- [サービスナレッジ管理とは](#)
- [AMS での VPC IDs の検索](#)
- [AMS でのサブネット IDs の検索](#)
- [AMI IDs、AMS の検索](#)
- [セキュリティグループ \(SG\) IDs、AMS を検索する](#)
- [AMS で IAM エンティティを検索する](#)
- [AMS でスタック IDs を検索する](#)
- [AMS でインスタンス IDs または IP アドレスを検索する](#)
- [AMS で Amazon リソースネーム \(ARNs\) を検索する](#)
- [AMS で ARN 別にリソースを検索する](#)
- [AMS アカウント設定の検索](#)

## サービスナレッジ管理とは

サービスナレッジ管理は、AMS アカウントのすべての情報の保存です。以下に関する情報は、AMS サービスナレッジ管理システム (SKMS)、AMS SKMS API、または AMS コンソールから取得されます。

- VPC
- マネージドサブネット
- Amazon EC2 インスタンスやその他のリソースを含むスタックとスタックコンポーネント
- Amazon マシンイメージ (AMI)

SKMS からの情報を使用して、管理対象のインフラストラクチャを理解し、インフラストラクチャを作成、変更、または削除するための変更管理およびサービスリクエストの入力として使用できます。

#### Note

すべての AMS SKMS API コールが記録されます AWS CloudTrail。

AMS SKMS API を使用して SKMS にアクセスします。これにより、環境 (VPCs とサブネット) とそこにデプロイできるアプリケーションリソース (スタック、Amazon EC2 インスタンス、インスタンスイメージまたは AMIs) に関する情報を検出するオペレーションが提供されます。

VPCs とインスタンスイメージは、オンボーディング中に必要なアクセス許可を持つアカウントで設定されます。それらが確立されたら、変更管理システムを使用して VPCs に作業スタックを入力できます。

## AMS での VPC IDs の検索

Virtual Private Cloud (VPC) には 1 つ以上のサブネットがあります。AMS では、VPC は にあり AWS リージョン、プライベートサブネットとパブリックサブネットがあります。

「[AMS でのサブネット IDs の検索](#)」も参照してください。

一部の CTs VpcId が必要です。VPC ID をを見つけるには、AMS コンソールまたは API/CLI を使用できます。

AMS コンソール：

ナビゲーションペインで、VPCs と関連する VPC を選択します。選択した VPC の VPC の詳細ページが開き、VPC ID などの情報が表示されます。

AMS SKMS API ListVpcSummaries または CLI:

#### Note

これらのコマンドを機能させるには、AMS CLI をインストールする必要があります。AMS API または CLI をインストールするには、AMS コンソールのデベロッパーリソースページに移動します。AMS CM API または AMS SKMS API のリファレンスマテリアルについては、「ユーザーガイド」の「AMS 情報リソース」セクションを参照してください。認証--

profile のオプションを追加する必要がある場合があります。例: `aws amsskms ams-cli-command --profile SAML`。また、など、すべての AMS コマンドが `us-east-1` を使い果たすため、`--region` オプションを追加する必要がある場合があります `aws amscm ams-cli-command --region=us-east-1`。

#### Note

AMS API/CLI (amscm および amsskms) エンドポイントは、AWS N. Virginia リージョンにあります `us-east-1`。認証の設定方法や、アカウントとリソースが存在する AWS リージョンによっては、コマンドの発行 `--region us-east-1` 時に追加が必要になる場合があります。認証方法である場合は `--profile saml`、を追加する必要がある場合もあります。

1. 次の例では、最初のコマンドはアカウント内のすべての VPCs の概要のリストをリクエストします。2 番目のコマンドは VPCs のリストをリクエストし、2016 年に作成された VPCs のみを一覧表示するクエリフィルターを使用して、`CreatedTime`、`VpcId`、および `Name` を出力します。

#### Note

AMS SKMS CLI は、AMS コンソールのデベロッパーのリソースページから取得できません。

```
aws amsskms list-vpc-summaries --output table
```

```
-----
|                               ListVPCSummaries                               |
+-----+
|                               VPCSummaries                                |
|+-----+-----+-----+-----+-----+-----+
| CreatedTime | 2016-01-15T18:50:11Z |
| VpcId       | vpc-01234567890abcdef |
| LastModifiedTime | 2016-01-15T18:50:11Z |
| Name        | 952444781316-initial-vpc |
|+-----+-----+-----+-----+-----+-----+
|                               Visibility                               |
|-----|
```

| Id   | PrivateAndPublic |
|------|------------------|
| Name | PrivateAndPublic |

## 2. 今回はクエリを使用します。

```
aws amsskms list-VPC-summaries --query "VPCSummaries[?starts_with(@.CreatedTime,to_string(`2016`))].[CreatedTime, VpcId, Name]" --output table
```

| ListVPCSummaries     |                       |                          |
|----------------------|-----------------------|--------------------------|
| 2016-01-15T18:50:11Z | vpc-01234567890abcdef | 952444781316-initial-VPC |

## AMS でのサブネット IDs の検索

いくつかのリソースでは、設定時にサブネットまたはサブネットのリストを指定する必要があります。サブネットを見つけるには、AMS コンソールまたは AMS SKMS API/CLI を使用できます。AMS SKMS API/CLI はプライベートであり、使用する前にインストールする必要があります。

AMS コンソール：

1. ナビゲーションペインで、VPCsと関連する VPC を選択します。選択した VPC の VPC 詳細ページがサブネットのテーブルで開き、サブネット ID をクリックして詳細ページを開き、ID を見つけます。

AMS SKMS API ListSubnetSummaries または CLI:

### Note

これらのコマンドを機能させるには、AMS CLI をインストールする必要があります。AMS API または CLI をインストールするには、AMS コンソールのデベロッパーリソースページに移動します。AMS CM API または AMS SKMS API のリファレンスマテリアルについては、「ユーザーガイド」の「AMS 情報リソース」セクションを参照してください。認証--profileのオプションを追加する必要がある場合があります。例: `aws amsskms ams-`

*cli-command* --profile SAML。また、など、すべての AMS コマンドが us-east-1 を使い果たすため、--region オプションを追加する必要がある場合があります `aws amscm ams-cli-command --region=us-east-1`。

 Note

AMS API/CLI (amscm および amsskms) エンドポイントは、AWS N. Virginia リージョンにあります us-east-1。認証の設定方法や、アカウントとリソースが存在する AWS リージョンによっては、コマンドの発行 --region us-east-1 時に追加が必要になる場合があります。認証方法である場合は --profile saml、を追加する必要がある場合もあります。

VPC のサブネットを検索するには、次に示すように list-subnet-summaries コマンドで検索します。

 Note

AMS アカウントにないサブネットを探している場合は、を試すことができます `aws ec2 describe-subnets --region us-west-2`。

1. SKMS API/CLI ListSubnetSummaries オペレーション :

シンプルなリスト :

```
aws amsskms list-subnet-summaries
```

テーブルへの出力 :

```
aws amsskms list-subnet-summaries --output table
```

2. SKMS API ListSubnetSummaries オペレーションには、可視性に基づいて結果を絞り込むためのパラメータがあります。さらに、名前に基づいて結果を [フィルタリング](#) できます。CLI を使用している場合は、--query オプションを使用して出力を絞り込んだり、値の一部を検索したりすることもできます。たとえば、特定の VPC のすべてのサブネットを検索するには、次のコマンドを使用できます。

```
aws amsskms list-subnet-summaries --query
  "SubnetSummaries.sort_by(@,&Visibility.Name)[].[Visibility.Name,SubnetId,Name]" --
output table
```

これは次のようなものを返します。

```
-----
|                               ListSubnetSummaries                               |
+-----+-----+-----+-----+
| Private| subnet-01234567890abcdef | Demo Deployment Zone #1 |
| Private| subnet-01234567890abcdef | Demo Deployment Zone #1 |
| Public | subnet-01234567890abcdef | Demo DMZ #1             |
| Public | subnet-01234567890abcdef | Demo DMZ #1             |
+-----+-----+-----+-----+
```

CLI クエリの使用の詳細については、[「--query オプションで出力をフィルタリングする方法」](#) および「クエリ言語リファレンス」の[JMESPath 仕様](#)を参照してください。

- 複数の VPCs がある場合は、コマンドに VPC フィルターを含め、各 VPC に対してコマンドを実行します。例:

```
list-subnet-summaries --filter Attribute=VpcId,Value=vpc-xxxxxxx --query
  "SubnetSummaries.sort_by(@,&Visibility.Name)[].[Visibility.Name,SubnetId,Name]" --
output table
```

- AWS では、[describe-subnets](#) を使用します。

CLI クエリの使用の詳細については、[「--query Option で出力をフィルタリングする方法」](#) および「クエリ言語リファレンス」の[JMESPath Specification](#)を参照してください。

## サブネット名

AMS サブネットは、入力が集められ、システムに追加されると自動的に作成されます。AMS は式を使用してサブネット名 **AACCOUNT\_ID-SUBNET-TYPE-AZ-IDENTIFIER** を作成します。サブネットタイプは、dmz、shared-services、または のいずれかになりますcustomer-application。複数のカスタマーアプリケーションサブネットがある場合、オプション識別子をアカウント ID の後にサブネット名に追加して、サブネットが「追加」または「予約済み」サブネットであることを示すことができます。

## AMI IDs、AMS の検索

Amazon マシンイメージ、つまり AMI は、Amazon EC2 インスタンスから作成された Amazon EC2 インスタンスのテンプレートです。は、更新された AMIs (パッチ付きなど) を毎月 AWS 提供します。ただし、AWS Managed Services (AMS) では、AMS 用に変更された AMIs が必要です。AMS は、毎月パッチ火曜日の直後に使用できる新しい AMIs をリリースします。

Amazon マシンイメージ (AMIs) は、AWS で EC2 インスタンスを作成するために使用されるインスタンス設定テンプレートです。AMS では、AMS マネージドリソースに特定の AMIs を使用する必要があります。EC2 インスタンスと EC2 Auto Scaling グループを作成するための変更タイプでは、変更タイプが作成するインスタンスの基礎として使用する AMS の AMI を指定する必要があります。AMS では、利用可能な最新の AMI を常に選択することをお勧めします。

AWS AMIs [AWS 「AMI 設計」](#) を参照してください。

AMS アカウントの Amazon EC2 スタックまたは Amazon EC2 Auto Scaling グループを作成するときは、Amild で AMI を指定する必要があります。AMIs に限定されているため、常に最新の AMI を選択することをお勧めします。

アカウントの最新の AMI を検索するには、AMS SKMS CLI コマンドで検索するか、関連する VPC の AMS コンソールの詳細ページを使用します。

- AMS コンソールを使用する: 使用可能な AMIs は、AMS コンソールの AMI ページに表示されます。名前が AMIs から選択します。
- AMS SKMS API/CLI ListAmis オペレーションを使用します。

### Note

これらのコマンドを機能させるには、AMS CLI をインストールする必要があります。AMS API または CLI をインストールするには、AMS コンソールのデベロッパーリソースページに移動します。AMS CM API または AMS SKMS API のリファレンスマテリアルについては、「ユーザーガイド」の「AMS 情報リソース」セクションを参照してください。認証 `--profile` のオプションを追加する必要がある場合があります。たとえば、`aws amsskms ams-cli-command --profile SAML`。また、など、すべての AMS コマンドが `us-east-1` を使い果たすため、`--region` オプションを追加する必要がある場合があります `aws amscm ams-cli-command --region=us-east-1`。

結果をお客様の AMI に制限する `query` オプション付きの CLI の例を次に示します。AMIs



```
aws amsskms list-amis --vpc-id VPC_ID --query "Amis.sort_by(@,&Name)[?starts_with(Name,'customer')].[Name,AmiId]" --output table
```

この例では、`filter` オプションと `query` オプションを使用して、「customerAMIs」を検索します。

```
aws amsskms list-amis --vpc-id VPC_ID --query "Amis.sort_by(@,&Name)[?starts_with(Name,'customer')].[Name,AmiId]" --filter Attribute=Platform,Value=windows --output table
```

- CLI クエリの使用の詳細については、[「--query オプションで出力をフィルタリングする方法」](#)および「クエリ言語リファレンス」の[JMESPath 仕様](#)を参照してください。

## セキュリティグループ (SG) IDs、AMS を検索する

Amazon EC2 作成および OpenSearch 作成ドメイン CTsには、セキュリティグループ ID が必要です。これは の形式になります `sg-02ce123456e7893c7`。アカウントに少なくとも 2 つのデフォルトのセキュリティグループがあります。「」を参照してください [セキュリティグループ](#)。さらに、特定の目的で作成したセキュリティグループがある場合があります。セキュリティグループを検出するには：

- AWS コンソール: EC2 または VPC コンソールを使用して、選択した VPC のすべてのセキュリティグループを表示します。
- API/CLI (AMS アカウントにログインしている場合):

セキュリティグループを一覧表示します。

```
aws ec2 describe-security-groups
```

## AMS で IAM エンティティを検索する

アカウントにはデフォルトの IAM ロールとポリシーがあります。[AMS の IAM ユーザーロール](#)「」と「IAM インスタンスプロファイルのデフォルト」を参照してください。「」と「ポリシー [EC2 IAM インスタンスプロファイル](#)のデフォルト」を参照してください。IAM ロールとポリシーを検出するには：

- コンソール: IAM コンソールを使用して、アカウントのすべての IAM ポリシーとロールを表示します。
- API/CLI (AMS アカウントにログインしている場合):

#### Note

これらのコマンドを機能させるには、AMS CLI をインストールする必要があります。AMS API または CLI をインストールするには、AMS コンソールのデベロッパーリソースページに移動します。AMS CM API または AMS SKMS API のリファレンスマテリアルについては、「ユーザーガイド」の「AMS 情報リソース」セクションを参照してください。認証 `--profile` のオプションを追加する必要がある場合があります。たとえば、`aws amsskms ams-cli-command --profile SAML`。また、`us-east-1` など、すべての AMS コマンドが `us-east-1` を使い果たすため、`--region` オプションを追加する必要がある場合があります `aws amscm ams-cli-command --region=us-east-1`。

ロールを一覧表示します。

```
aws --profile saml iam list-roles
```

ポリシーを一覧表示します。

```
aws --profile saml iam list-role-policies --role-name ROLE_NAME
```

## AMS でスタック IDs を検索する

スタック ID をを見つけるには、Amazon EC2 コンソール、AMS コンソール、または AMS SKMS API/CLI のいずれかを使用できます。

AMS コンソール :

- ナビゲーションペインで RFCs を選択し、スタックを作成した RFC をクリックします。上部のフィルターオプションを使用して、リストを減らします。RFC の詳細ページが開き、スタック ID を含む実行出力が含まれます。
- または、ナビゲーションペインでスタックを選択してスタックリストページを開き、スタックリストを目的のスタックにページスルーすることもできます。この方法は、探しているスタックのサブジェクトがわかっている場合に便利です。

## Amazon EC2 コンソール :

ナビゲーションペインで、インスタンス、ロードバランサー、または Auto Scaling グループを選択します。

AMS SKMS API ListStackSummaries または CLI:

### Note

これらのコマンドを機能させるには、AMS CLI をインストールする必要があります。AMS API または CLI をインストールするには、AMS コンソールのデベロッパーリソースページに移動します。AMS CM API または AMS SKMS API のリファレンスマテリアルについては、「ユーザーガイド」の「AMS 情報リソース」セクションを参照してください。認証--profileのオプションを追加する必要がある場合があります。たとえば、`aws amsskms ams-cli-command --profile SAML`。また、など、すべての AMS コマンドが us-east-1 を使い果たすため、--regionオプションを追加する必要がある場合があります`aws amscm ams-cli-command --region=us-east-1`。

### Note

AMS API/CLI (amscm および amsskms) エンドポイントは、AWS N. Virginia リージョンにありますus-east-1。認証の設定方法、およびアカウントとリソースがどの AWS リージョンにあるかによっては、コマンドの発行--region us-east-1時に追加する必要がある場合があります。認証方法である場合は--profile saml、を追加する必要がある場合もあります。

現在のアカウントのスタックのリストを表示するには、SKMS API (CLI: ) の ListStackSummaries オペレーションを実行しますlist-stack-summaries。StackId で特定のスタックインスタンスに関する完全な情報を取得するには、GetStack を実行します。

- 次の例では、最初のコマンドは、アカウント内のすべてのスタックインスタンスの概要のリストをリクエストします。2 番目のコマンドは、スタックインスタンスのリストをリクエストし、クエリフィルターを使用して特定のスタックテンプレートのリストのみを表示し、VpcId、Name、および StackId を出力します。

```
aws amsskms list-stack-summaries --output table
```

```

-----
|                                     ListStackSummaries          |
|                                     StackSummaries              |
+-----+-----+-----+-----+
| VpcId      | StackId      | StackTemplateId  | Name      |
+-----+-----+-----+-----+
| vpc-0123abcd| stack-1fb7fe2212345678| stm-sdhopvbb123456789| Test ELB |
| vpc-0123abcd| stack-8323cc0e12345678| stm-s2b72beb123456789| S3 store |
| vpc-0123abcd| stack-2309fa0712345678| stm-sdhopvbb123456789| ELB      |
| vpc-0123abcd| stack-5e61a70512345678| stm-sdpabqbb123456789| PatchSim |
| vpc-0123abcd| stack-bd0e080d12345678| stm-s2b72beb123456789| CLI demo |
+-----+-----+-----+-----+

```

CLI クエリの使用の詳細については、[「--query オプションで出力をフィルタリングする方法」](#) および「クエリ言語リファレンス」の[JMESPath 仕様](#)を参照してください。

#### Note

アクセスにインスタンス IDs 「」も参照してください [踏み台を使用したインスタンスへのアクセス](#)。

## AMS でインスタンス IDs または IP アドレスを検索する

- インスタンスへのアクセスをリクエストする、インスタンスにログインする、または AMI を作成するには、インスタンス ID が必要です。EC2 インスタンス (スタンドアロンインスタンスまたはスタックの一部) またはデータベースインスタンスの場合は、いくつかの異なる方法で ID を見つけることができます。
- ASG スタック内のインスタンスの AMS コンソール: スタックを作成した RFC の RFC 詳細ページを確認します。実行出力セクションには、ASG スタックのスタック ID が表示され、EC2 コンソールの Auto Scaling Groups ページに移動してそのスタック ID を検索し、そのスタックのインスタンスを検索できます。インスタンスを見つけたら、そのインスタンスを選択すると、IP アドレスなどの詳細を含むエリアがページの下部に表示されます。
- スタンドアロン EC2 またはデータベース (DB) インスタンスの AMS コンソール: EC2 スタックまたは DB インスタンスを作成した RFC の RFC 詳細ページを確認します。実行出力セクションには、インスタンス ID と IP アドレスが表示されます。

- AWS EC2 コンソール :
  1. ナビゲーションペインで、[インスタンス] を選択します。インスタンスページが開きます。
  2. ID が必要なインスタンスをクリックします。インスタンスの詳細ページが開き、ID と IP アドレスが表示されます。
- AWS データベースコンソール :
  1. ホームページで、DB インスタンスを選択します。インスタンスページが開きます。
  2. ID が必要な DB インスタンスをフィルタリングします。インスタンスの詳細ページが開き、ID が表示されます。
- AMS CLI/API。

 Note

これらのコマンドを機能させるには、AMS CLI をインストールする必要があります。AMS API または CLI をインストールするには、AMS コンソールのデベロッパーリソースページに移動します。AMS CM API または AMS SKMS API のリファレンスマテリアルについては、「ユーザーガイド」の「AMS 情報リソース」セクションを参照してください。認証--profileのオプションを追加する必要がある場合があります。たとえば、`aws amsskms ams-cli-command --profile SAML`。また、など、すべての AMS コマンドが us-east-1 を使い果たすため、--regionオプションを追加する必要がある場合があります`aws amscm ams-cli-command --region=us-east-1`。

 Note

AMS API/CLI (amscm および amsskms) エンドポイントは、AWS N. Virginia リージョン にありますus-east-1。認証の設定方法、およびアカウントとリソースがどの AWS リージョンにあるかによっては、コマンドの発行--region us-east-1時に追加する必要がある場合があります。認証方法である場合は--profile saml、を追加する必要がある場合もあります。

次のコマンドを実行して、スタック実行出力の詳細を取得します。

```
aws amsskms get-stack --stack-id STACK_ID
```

出力は次のようになります。InstanceId は下部の の下に表示されます Outputs (値は例です )。

```
{
  "Stack": {
    "StackId": "stack-7fa52bd5eb8240123",
    "Status": {
      "Id": "CreateCompleted",
      "Name": "CreateCompleted"
    },
    "VpcId": "vpc-01234567890abcdef",
    "Description": "Amazon",
    "Parameters": [
      {
        "Value": "sg-01234567890abcdef,sg-01234567890abcdef",
        "Key": "SecurityGroups"
      },
      {
        "Value": "subnet-01234567890abcdef",
        "Key": "InstanceSubnetId"
      },
      {
        "Value": "t2.large",
        "Key": "InstanceType"
      },
      {
        "Value": "ami-01234567890abcdef",
        "Key": "InstanceAmiId"
      }
    ],
    "Tags": [],
    "Outputs": [
      {
        "Value": "i-0b22a22eec53b9321",
        "Key": "InstanceId"
      },
      {
        "Value": "10.0.5.000",
        "Key": "InstancePrivateIP"
      }
    ]
  }
}
```

```
    ],  
    "StackTemplateId": "stm-s6xvs000000000000",  
    "CreatedTime": "1486584508416",  
    "Name": "Amazon"  
  }  
}
```

## AMS で Amazon リソースネーム (ARNs) を検索する

Amazon リソースネーム (ARN) は、EC2 インスタンス、S3 バケット、アカウント、Lambda 関数などの AWS リソースを一意に識別する文字列です。IAM ポリシー、Amazon Relational Database Service (Amazon RDS) タグ、API コールなど AWS、すべての でリソースを明確に指定するには、ARN AWS が必要です。ARNs は、サービス、リージョン、アカウント、その他の情報を指定する識別子から構築されます。3 つの ARN 形式があります。

```
arn:aws:service:region:account-id:resource-id  
arn:aws:service:region:account-id:resource-type/resource-id  
arn:aws:service:region:account-id:resource-type:resource-id
```

### Note

ARN の正確な形式は、サービスとリソースのタイプによって異なります。ARN の詳細については、[「Amazon リソースネーム \(ARNs AWS 「サービス名前空間と ARN 形式」を参照してください。 https://docs.aws.amazon.com/quicksight/latest/APIReference/qs-arn-format.html](#)

リソース別の ARN 形式の例については、AWS 「サービス認可リファレンス [リソースタイプの表](#)」を参照してください。

AWS オブジェクトの ARN をを見つけるのは難しい場合があります。試す方法は 3 つあります。

- AWS サービスコンソール: 関連する AWS サービスコンソールに移動し、リソースを見つけて、リソースの詳細で ARN を見つけます。
- AWS API/CLI (最初に AWS CLI をインストールする必要があります): [AWS CLI コマンドリファレンス](#)で関連するサービスを探し、AWS サービスに応じて、describeや などの関連するオペレーションを探getします。たとえば、すべての IAM ロール、ポリシー、ユーザーについて、以下を使用して CLI からの出力で ARN を取得できます。



```
aws iam get-role --role-name EMR_DefaultRole
```

- 関連する形式に基づいて ARN を作成します。[AWS サービスのアクション、リソース、および条件キー](#) ページを確認し、関連するサービスを検索してから、リソース ARN 形式にドリルダウンして、リソースの ARN 形式を検索します。形式を取得したら、変数を関連する設定に置き換えます。

ARN は、適切な形式 (サービスおよびリソースタイプごとに形式が変更される) に従い、情報を入力して自分で構築できます。ARN の例を次に示します。

- AWS アカウント ARN には次の構文があります。

```
arn:aws:iam::ACCOUNT-ID:root
```

- S3 ARN には、バケットと関連するオブジェクトのフラット階層があります。

```
arn:aws:s3:::ams-bucket
```

- EC2 ARN には、イメージ、セキュリティグループ、インスタンスなどのサブリソースタイプがあります。この例では、最後にインスタンス ID を含めます。

```
arn:aws:ec2:us-east-1:123456789012:instance/i-012abcd34efghi56
```

- Lambda ARN には resource-id 部分の関数名があり、次の例に示すように、末尾にバージョン番号を含める必要がある場合があります。

```
arn:aws:lambda:us-east-1:123456789012:function:api-function:1
```

この AWS Key Management Service サービスは、キー [ID とキー ARN を検索する](#) という情報を提供します。

DynamoDB テーブルの ARN を検索するには、DynamoDB [describe-table](#) CLI を使用します。

アウトサイダーによる AWS ARNs の詳細については、[AWS 「ARN Explained: Amazon リソースネームガイド」](#) を参照してください。

## AMS で ARN 別にリソースを検索する

Amazon リソースネーム (ARNs) は AWS リソースを一意に識別します。ARN と ARN 形式の詳細については、「[Amazon リソースネーム \(ARNs AWS 「サービス名前空間と ARN 形式」](https://docs.aws.amazon.com/quicksight/latest/APIReference/qs-arn-format.html)」を参照してください。 <https://docs.aws.amazon.com/quicksight/latest/APIReference/qs-arn-format.html>

### Note

ARN からリソースに関する詳細を取得するには、リソースを作成したアカウントにアクセスできる必要があります。

サービスにはさまざまな関連情報を含む複数のリソースタイプがあるため、リソース ARN からすべてのリソースの詳細 AWS を検索する直接パスにはありません。リソースの ARN がある場合は、以下を確認できます。

- 関連 AWS サービス (3 番目の ARN セグメント) は、リソースを見つけるためにどの AWS コンソールを確認するかを示します。
- リソース ID (6 番目または 7 番目の ARN セグメント) は、適切なリソースが見つかったことを確認します。

または、リソースの詳細を取得する方法については、AWS CLI コマンド [AWS リファレンスでそのサービスで使用できる CLI コマンド](#)を検索できます。

たとえば、次の ARN から、サービスが lambda、アカウントが 123456789012、リソースタイプが function、関数の名前が TestFunction であると判断できます。

```
arn:aws:lambda:us-east-1:123456789012:function:TestFunction
```

ここから、[AWS Lambda サービスの CLI ドキュメント](#)を確認して、get-function や などのさまざまなコマンドで詳細を取得する方法を確認できます get-function-configuration。

たとえば、Lambda 関数の名前または ARN がある場合は、次のコマンドを使用して Lambda 関数に関する詳細情報を取得できます。

```
aws lambda get-function-configuration --function-name TestFunction
```

```
aws lambda get-function-configuration --function-name arn:aws:lambda:us-east-1:123456789012:function:TestFunction
```

## AMS アカウント設定の検索

AMS RFCs の作成、スケジュールの設定、通知の受信者の決定に使用されるアカウント設定。

一部の設定はオンボーディング中に作成され、変更するにはサービスリクエストが必要です。AMS と通信するときに使用するため、これらのアカウントの詳細を書き留めておく必要があります。

- 認証情報: AMS ユーザー名またはパスワードを取得する必要がある場合は、ローカル IT 管理者にお問い合わせください。--AMS は会社の Active Directory を使用します。
- Cloud Service Delivery Manager (CSDM): このユーザーは AMS との連絡係であり、サービスの質問に回答できます。このユーザーの連絡先情報はオンボーディング時に提供され、AMS を操作する組織内のすべてのユーザーが利用できるようにする必要があります。このユーザーから AMS サービスに関する月次レポートを受け取ることを期待できます。
- コンソールアクセス: アカウント専用設定された URL で AMS コンソールにアクセスします。URL は CSDM から取得できます。
- AMS CLI: AMS CLI は、AMS コンソール開発者のリソースページ、または CSDM から取得したディストリビューションパッケージから取得できます。頒布可能パッケージを入手したら、[「AMS CLI のインストールまたはアップグレード」](#)で説明されているステップに従います。
- メンテナンスウィンドウ: メンテナンスウィンドウは、EC2 インスタンスのパッチ適用がいつ行われるかを決定します。AWS Managed Servicesメンテナンスウィンドウ (またはメンテナンスウィンドウ) は、AWS Managed Services (AMS) のメンテナンスアクティビティを実行し、毎月第 2 木曜日の太平洋標準時の午後 3 時から午後 4 時まで繰り返します。AMS は、48 時間前に通知することでメンテナンスウィンドウを変更する場合があります。オンボーディング時に別のウィンドウを選択している可能性があります。選択したメンテナンスウィンドウの記録を保持します。
- モニタリング: AMS はデフォルトで一連の CloudWatch メトリクスを提供しますが、追加のメトリクスをリクエストすることもできます。その場合は、記録しておきます。
- ログ: デフォルトでは、ログは `ams-a-ACCOUNT_ID-log-management-REGION` に保存されます。`REGION` はログが生成されたリージョンです。
- 緩和策: リソースに対するマルウェア攻撃が特定された場合、AMS はオンボーディング時に選択した緩和アクションを記録します。たとえば、特定のユーザーに連絡します。AMS を操作する組織内のすべてのユーザーがこの情報を利用できるようにします。

- リージョン: AMS コンソールの VPC の詳細ページを確認できます。AMS SKMS CLI をインストールした後にこのコマンドを実行することもできます (このコマンドは SAML プロファイルを使用し、認証方法が異なる場合は を削除します)。

```
aws --profile saml amsskms get-vpc --vpc-id VPC_ID
```

### ⚠ Important

#### Note

AMS API/CLI (amscm および amsskms) エンドポイントは、AWS N. Virginia リージョン にあります us-east-1。認証の設定方法や、アカウントとリソースが存在する AWS リージョンによっては、コマンドの発行 --region us-east-1 時に追加が必要になる場合があります。認証方法である場合は --profile saml、 を追加する必要がある場合もあります。

## AMS で FQDNs を検索する

AWS Managed Services (AMS) アクセス変更タイプ (CTs) には、AMS が信頼するドメインの完全修飾ドメイン名または FQDN が の形式で必要です C844273800838.amazonaws.com。FQDN AWS を検出するには、次のいずれかを実行します。

- AWS コンソール: ディレクトリ名列の AWS Directory Service コンソールを確認します。
- CLI: ドメインにログインしている間は、次のコマンドを使用します。

Windows (ユーザーと FQDN を返します):

```
whoami /upn
```

または (DC+DC+DC=FQDN)

```
whoami /fqdn
```

Linux:

```
hostname --fqdn
```

### Note

AMS API/CLI (amscm および amsskms) エンドポイントは、AWS N. Virginia リージョンにあります us-east-1。認証の設定方法や、アカウントとリソースが存在する AWS リージョンによっては、コマンドの発行 `--region us-east-1` 時に追加が必要になる場合があります。認証方法である場合は `--profile saml`、を追加する必要がある場合もあります。

## AMS でアベイラビリティーゾーン (AZs) を検索する

アベイラビリティーゾーン: すべてのアカウントに少なくとも 2 つのアベイラビリティーゾーンがあります。アベイラビリティーゾーン名を正確に検索するには、まず関連付けられたサブネット ID を知る必要があります。

- AMS コンソール: ナビゲーションペインで VPCs をクリックし、必要に応じて関連する VPC をクリックします。VPCs の詳細ページで、サブネットのテーブルで関連するサブネットを選択し、関連するアベイラビリティーゾーンの名前を含むサブネットの詳細ページを開きます。
- AMS SKMS API/CLI:

```
aws amsskms list-subnet-summaries --output table
```

```
aws amsskms get-subnet --subnet-id SUBNET_ID
```

### Note

AMS API/CLI (amscm および amsskms) エンドポイントは、AWS N. Virginia リージョンにあります us-east-1。認証の設定方法や、アカウントとリソースが存在する AWS リージョンによっては、コマンドの発行 `--region us-east-1` 時に追加が必要になる場合があります。認証方法である場合は `--profile saml`、を追加する必要がある場合もあります。

## AMS で SNS トピックを検索する

SNS トピックは、さまざまな状況で通知されるユーザーを決定します。AMS は、AMI 通知 (SNS を使用した [AMS AMI 通知を参照](#))、CloudWatch アラーム、EC2 リソース (AMS によって生成されたアラートの受信を参照) などの SNS <https://docs.aws.amazon.com/managedservices/latest/userguide/sent-alert-views.html> トピックを提供します。CloudWatch EC2 既存の SNS トピックを検出するには：

- AWS コンソール: SNS コンソールを使用して、すべてのトピック、アプリケーション、サブスクリプション、およびメッセージのグラフを表示します。また、トピックを作成、削除、サブスクライブ、公開します。
- API/CLI (AMS アカウントにログインする場合、には AWS CLI が必要です)。

SNS トピックを一覧表示します。

```
aws sns list-topics
```

SNS サブスクリプションを一覧表示します。

```
aws sns list-subscriptions
```

### Note

AMS API/CLI (amscm および amsskms) エンドポイントは、AWS N. Virginia リージョンにあります us-east-1。認証の設定方法、およびアカウントとリソースがどの AWS リージョンにあるかによっては、コマンドの発行 `--region us-east-1` 時に追加する必要がある場合があります。認証方法である場合は `--profile saml`、を追加する必要がある場合もあります。

## AMS でバックアップ設定を検索する

バックアップとスナップショットは、ネイティブ [AWS Backup](#) サービスを通じて AMS によって管理されます。

設定は AWS Backup 計画を通じて管理されます。タグ付けされたリソースをバックアップスケジュールと保持ポリシーに関連付ける複数の AWS Backup プランを持つことができます。AMS アカ

AWS Backup 設定を検索するには、<https://console.aws.amazon.com/backup> コンソールを使用するか、[バックアップ](#) コマンドの AWS CLI コマンドリファレンスを使用します。

AMS の詳細については AWS Backup、[「継続性管理」](#) を参照してください。



# AMS でのアクセス管理

SSH またはリモートデスクトッププロトコル (RDP) を使用して リソースにアクセスする方法と、踏み台を使用する方法について説明します。

AWS Managed Services (AMS) アクセス管理システムは、オンボーディング中に設定されます。AMS IAM ユーザーロールを持つユーザーのみが、アカウントの AMS リソースにアクセスできます。

次に説明するフェデレーティッドトラストに加えて、AMS セキュリティグループはプライベートおよびパブリックアプリケーションアクセスにおける重要な要素です。AMS セキュリティグループとその変更方法については、「」を参照してください[セキュリティグループ](#)。

## トピック

- [アクセス管理とは](#)
- [AMS でルートユーザーアカウントを使用する方法とタイミング](#)
- [AMS Advanced コンソールと Amazon EC2 アクセス](#)
- [AWS マネジメントコンソールと AMS コンソールへのアクセス](#)
- [踏み台を使用したインスタンスへのアクセス](#)

## アクセス管理とは

アクセス管理とは、承認されたアクセスと認証されたアクセスのみを許可することで、AMS がリソースを保護する方法です。AMS は、デフォルトの IAM ユーザーロールとインスタンスプロファイル、多要素認証、セキュリティグループ、DNS フレンドリーな踏み台名などを使用して、リソースを保護します。

AMS は、管理が必要な 3 種類のアクセスに焦点を当てています。

- コンソールアクセス: アカウントの Active Directory のユーザーは、フェデレーションを活用して、シングルサインオン (SSO) を使用してコンソールにアクセスできます。これらのアカウントに多要素認証を設定している場合、コンソールへのアクセスを MFA に引き続き要求できます。
- RDP または SSH によるインスタンスアクセス: Active Directory の信頼を活用すると、アカウントの既存の Active Directory のユーザーはインスタンスへのアクセスをリクエストし、既存の企業認証情報を使用して踏み台とインスタンスに対して正常に認証できます。これらのアカウントに多要素認証を設定している場合、インスタンスへのアクセスをリクエストするために MFA を引き続き

要求できます。AMS は独自の MFA ソリューションを使用して、AMS エンジニアのインスタンスへのアクセスを制限します。

- アプリケーションアクセス: ユースケースによって異なります。

## トピック

- [AMS がアカウントにアクセスする理由とタイミング](#)

## AMS がアカウントにアクセスする理由とタイミング

AWS Managed Services (AMS) は AWS インフラストラクチャを管理し、特定の理由で AMS オペレーターと管理者がアカウントにアクセスすることがあります。これらのアクセスイベントは、AWS CloudTrail (CloudTrail) ログに記録されます。

AMS がアカウントにアクセスする理由、タイミング、および方法については、以下のトピックで説明します。

### AMS カスタマーアカウントアクセストリガー

AMS カスタマーアカウントアクセスアクティビティは、トリガーによって駆動されます。今日のトリガーは、Amazon CloudWatch (CloudWatch) アラームとイベントに応答して問題管理システムで作成された AWS チケット、および送信したインシデントレポートまたはサービスリクエストです。アクセスごとに複数のサービス呼び出しとホストレベルのアクティビティが実行される場合があります。

アクセスの根拠、トリガー、トリガーのイニシエータを次の表に示します。

#### アクセストリガー

| アクセス            | イニシエータ | Trigger トリガー)                             |
|-----------------|--------|-------------------------------------------|
| パッチ適用           | AMS    | パッチの問題                                    |
| インフラストラクチャのデプロイ | AMS    | デプロイの問題                                   |
| 内部問題調査          | AMS    | 問題 (システムとして特定された問題)                       |
| アラートの調査と修復      | AMS    | AWS Systems Manager 運用作業項目 (SSM OpsItems) |

| アクセス                     | イニシエータ | Trigger トリガー)                                                              |
|--------------------------|--------|----------------------------------------------------------------------------|
| 手動 RFC 実行                | You    | Request for Change (RFC) の問題。(自動化されていない RFCs リソースへの AMS アクセスが必要になる場合があります) |
| インシデントの調査と修復             | You    | インバウンドサポートケース (送信したインシデントまたはサービスリクエスト)                                     |
| インバウンドサービスリクエストのフルフィルメント | You    |                                                                            |

## AMS カスタマーアカウントアクセス IAM ロール

トリガーされると、AMS は AWS Identity and Access Management (IAM) ロールを使用してカスタマーアカウントにアクセスします。アカウントのすべてのアクティビティと同様に、ロールとその使用状況は CloudTrail に記録されます。

### Important

これらのロールを変更または削除しないでください。

## カスタマーアカウントへの AMS アクセスの IAM ロール

| ロール名                            | アカウントタイプ (SALZ、MALZ 管理、MALZ アプリケーションなど) | 説明                                                    |
|---------------------------------|-----------------------------------------|-------------------------------------------------------|
| ams-service-admin               | SALZ、MALZ                               | AMS サービスの自動化アクセスと、パッチ、バックアップ、自動修復などの自動インフラストラクチャデプロイ。 |
| ams-application-infra-read-only | SALZ、MALZ アプリケー                         | オペレーターの読み取り専用アクセス                                     |

| ロール名                             | アカウントタイプ (SALZ、MALZ 管理、MALZ アプリケーションなど) | 説明                          |
|----------------------------------|-----------------------------------------|-----------------------------|
| ams-application-infra-operations | シヨン、MALZ Tools-Application              | インシデント/サービスリクエストのオペレーターアクセス |
| ams-application-infra-admin      |                                         | AD 管理者アクセス                  |
| ams-primary-read-only            | MALZ 管理                                 | オペレーターの読み取り専用アクセス           |
| ams-primary-operations           |                                         | インシデント/サービスリクエストのオペレーターアクセス |
| ams-primary-admin                |                                         | AD 管理者アクセス                  |
| ams-logging-read-only            | MALZ ログ記録                               | オペレーターの読み取り専用アクセス           |
| ams-logging-operations           |                                         | インシデント/サービスリクエストのオペレーターアクセス |
| ams-logging-admin                |                                         | AD 管理者アクセス                  |
| ams-networking-read-only         | MALZ ネットワーキング                           | オペレーターの読み取り専用アクセス           |
| ams-networking-operations        |                                         | インシデント/サービスリクエストのオペレーターアクセス |
| ams-networking-admin             |                                         | AD 管理者アクセス                  |
| ams-shared-services-read-only    | MALZ 共有サービス                             | オペレーターの読み取り専用アクセス           |
| ams-shared-services-operations   |                                         | インシデント/サービスリクエストのオペレーターアクセス |

| ロール名                                            | アカウントタイプ (SALZ、MALZ 管理、MALZ アプリケーションなど)             | 説明                                   |
|-------------------------------------------------|-----------------------------------------------------|--------------------------------------|
| ams-shared-services-admin                       |                                                     | AD 管理者アクセス                           |
| ams-security-read-only                          |                                                     | オペレーターの読み取り専用アクセス                    |
| ams-security-operations                         | MALZ セキュリティ                                         | インシデント/サービスリクエストのオペレーターアクセス          |
| ams-security-admin                              |                                                     | AD 管理者アクセス                           |
| ams-access-security-analyst                     | SALZ、MALZ アプリケーション、MALZ Tools-Application、MALZ Core | AMS セキュリティアクセス                       |
| ams-access-security-analyst-read-only           |                                                     | AMS セキュリティ、読み取り専用アクセス                |
| Sentinel_AdminUser_Role_PXHazRQadu0PVcCDcMbHE   | SALZ                                                | [BreakGlassRole]breakGlassするために使用します |
| Sentinel_PowerUser_Role_wZuPuS0ROOI0IazDbRI9    |                                                     | RFC 実行のためのユーザーアカウントへのパワーユーザーアクセス     |
| Sentinel_ReadOnlyUser_Role_Pd4L6Rw9RD0InLkD5JOo | SALZ、MALZ                                           | RFC 実行のためのカスタマーアカウントへのReadOnlyアクセス   |
| ams_admin_role                                  |                                                     | RFC 実行のためのカスタマーアカウントへの管理者アクセス        |

| ロール名                                               | アカウントタイプ (SALZ、MALZ 管理、MALZ アプリケーションなど) | 説明                                                                           |
|----------------------------------------------------|-----------------------------------------|------------------------------------------------------------------------------|
| AWSManagedServices_Provisioning_CustomerStacksRole |                                         | CloudFormation Ingest を通じて顧客に代わって CFN スタックを起動および更新するために使用されます                |
| customer_ssm_automation_role                       |                                         | ランブック実行のために CT 実行によって SSM Automation に渡されるロール                                |
| ams_ssm_automation_role                            | SALZ、MALZ アプリケーション、MALZ Core            | ランブック実行のために AMS サービスによって SSM Automation に渡されるロール                             |
| ams_ssm_iam_deployment_role                        | MALZ アプリケーション                           | IAM カタログで使用されるロール                                                            |
| ams_ssm_shared_services_intermediary_role          | MALZ 共有サービス                             | 共有サービスアカウントで特定の SSM ドキュメントを実行するためにアプリケーション ams_ssm_automation_role で使用されるロール |
| AmsOpsCenterRole                                   |                                         | カスタマーアカウントで OpsItems を作成および更新するために使用されます                                     |
| AMSOpsItemAutoExecutionRole                        | SALZ、MALZ                               | SSM ドキュメントの取得、リソースタグの説明、OpsItems の更新、自動化の開始に使用されます。                          |
| customer-mc-ec2-instance-profile                   |                                         | デフォルトのカスタマー EC2 インスタンスプロファイル (ロール)                                           |

## インスタンスアクセスのリクエスト

リソースにアクセスするには、まずそのアクセスの変更リクエスト (RFC) を送信する必要があります。リクエストできるアクセスには、admin (読み取り/書き込みアクセス許可) と読み取り専用 (標準

ユーザーアクセス) の 2 種類があります。デフォルトでは、アクセスは 8 時間続きます。この情報は必須です。

- アクセスするインスタンスのスタック ID、またはスタック IDs のセット。
- AMS 信頼ドメインの完全修飾ドメイン名。
- アクセスを希望するユーザーの Active Directory ユーザー名。
- アクセスするスタックがある VPC の ID。

アクセス権限が付与されたら、必要に応じてリクエストを更新できます。

アクセスをリクエストする方法の例については、[「スタック管理者アクセス | 許可」](#) または [「スタック読み取り専用アクセス | 許可」](#) を参照してください。

## AMS でルートユーザーアカウントを使用する方法とタイミング

[ルートユーザー](#)は、アカウント AWS 内のスーパーユーザーです。AMS はルートの使用状況をモニタリングします。ルートは、アカウント設定の変更、請求とコスト管理への (IAM) アクセスの有効化 AWS Identity and Access Management、ルートパスワードの変更、多要素認証 (MFA) の有効化など、必要ないくつかのタスクにのみ使用することをお勧めします。[「ユーザーガイド」の「ルートユーザー認証情報を必要とするタスク」](#) を参照してください。AWS Identity and Access Management

### Note

MFA は AMS Advanced オンボーディング中に有効になり、特にルートユーザーアクセスを禁止します。AMS マネージドアカウントのルートアクセスは他の AWS アカウントとは異なり、AMS マネージド環境全体のセキュリティにとって重要です。設定された MFA は仮想 MFA であり、AMS 所有のデバイスを使用して実行されます。仮想 MFA が AMS の支援で設定されると、仮想トークンは直ちに削除されます。これにより、ユーザーも AMS もルートユーザーとしてアカウントにログインできなくなります。ルートログインは特別なリクエスト (次に説明) でのみ再有効化でき、AMS はそのようなアクセスが絶対に必要な場合にのみ使用されることを期待します。MFA の詳細については、[「多要素認証による新しいアカウントの保護」](#) を参照してください。



ルートアクセスは常に AMS セキュリティおよび運用チームのレスポンスをトリガーします。AMS は API コールのルートアクセスをモニタリングし、そのようなアクセスが検出されるとアラームがトリガーされます。

ルートアクセスのリクエストは、AMS アカウントタイプによって若干異なります。

AMS Advanced シングルアカウントランディングゾーンによるルートアクセス：

シングルアカウントランディングゾーンがある場合は、クラウドサービスの配信マネージャー (CSDM) とクラウドアーキテクト (CAs) に連絡して、必要なルートアクセス作業についてアドバイスしてください。提案されたアクティビティの前に 24 時間前に通知することをお勧めします。

AMS Advanced マルチアカウントランディングゾーンによるルートアクセス：

マルチアカウントランディングゾーンアプリケーション、共有サービス、セキュリティ、またはネットワークアカウントの場合は、管理 | その他 | その他 (ct-1e1xtak34nx76) 変更タイプを使用します。ルートユーザーの認証情報を使用する日付、時刻、目的を含め、アクティビティが提案される 24 時間前に必ず通知するように RFC をスケジュールします。マルチアカウントランディングゾーン管理アカウントを使用して RFC を送信します。

さらに、24 時間前に CSDM と CAs に連絡して、必要なルートアクセス作業についてアドバイスしてください。

AMS オペレーションとルート使用状況に対するセキュリティ対応：

ルートユーザーアカウントが使用されると、AMS はアラームを受け取ります。ルート認証情報の使用がスケジュールされていない場合は、AMS セキュリティチームおよびアカウントチームに連絡して、これが予想されるアクティビティであるかどうかを確認します。アクティビティが想定されていない場合、AMS はセキュリティチームと協力して問題を調査します。

## AMS Advanced コンソールと Amazon EC2 アクセス

AMS Advanced コンソールへのアクセス。

Amazon EC2 インスタンスへのアクセス。

アクセスリクエストの送信:

AMS Amazon EC2 インスタンスへのログイン:

## AWS マネジメントコンソールと AMS コンソールへのアクセス

オンボーディング中、AWS マネジメントコンソールへのログインが提供されます (権限が制限されています。AMS コンソールに書き込むことができ、顧客情報ページの一部のフィールドを入力できます)。AWS マネジメントコンソールでマネージドサービスリンクを選択すると、AMS コンソールにアクセスできます。フェデレーティッドアクセスまたは共有認証情報 (ユーザー名/パスワード) は、IT 管理チームとの合意に従って準備されます。アカウントまたはグループをさらに作成するには、サービスリクエストを AMS に送信します。

AWS マネジメントコンソールへのアクセスについては、[AWS 「マネジメントコンソールの使用」](#)を参照してください。

AMS コンソールの使用に関するヒントについては、[「AMS コンソールの使用」](#)を参照してください。

### AMS コンソールへの一時的なアクセス

AMS に対して認証するための ID プロバイダー (SAML など) をまだ設定していない場合は、AMS コンソールに一時的にアクセスできます。CSDM に連絡して、デプロイ | 高度なスタックコンポーネント | Identity and Access Management (IAM) | エンティティまたはポリシー変更リクエスト (ct-3dpgd8mdd9jn1r) を以下の値で送信してもらいます。

- UserName: 作成する IAM ユーザーエンティティの名前
- AccessType: "コンソールアクセス"
- UserPermissions: **#USERNAME** (一時アクセスを希望するユーザー) の一時 AMS コンソールアクセス」
- E メール通知: AMS が リクエストしたときにリクエストを承認できるように E メールアドレス

#### Note

この一時的な AMS コンソールアクセス用の RFC には、内部セキュリティチームと AMS グローバルセキュリティの両方によるセキュリティレビューと承認が必要です。

このリクエストが完了し、ログインできるようになると、作成された RFC を承認し、承認を追跡して AMS チームが作業を終了できるようにする必要があります。RFC を承認するには、RFC のリ

ストページで検索し (その横に承認保留中フラグが表示されます)、RFC を選択してその RFC の RFC 詳細ページを開き、承認を選択します。RFC が承認されるまで AMS を使用することはできません。

RFC が正常に完了すると、AMS オペレーションによって新しい IAM ユーザーとパスワードが提供されます。次に、以下のステップに従います。

1. AWS マネジメントコンソールに移動し、提供された認証情報でログインします。新しいパスワードを作成するように求められます。また、ログイン時に多要素認証 (MFA) を設定する必要があります。詳細については、「[でのMulti-Factor Authentication \(MFA\) AWSの使用](#)」を参照してください。
2. AWS マネジメントコンソールで、を指定された IAM ロール () に変更します `customer_CustomerCode_readonly_user_role`。
3. AMS マネージドサービスコンソールを開きます。

#### Note

一時的なアクセスのデフォルトは 60 日ですが、CSDM に連絡して 30 日間の延長をリクエストできます。

## 踏み台を使用したインスタンスへのアクセス

顧客と AMS オペレーターの両方の AMS マネージドアカウント内のリソースへのすべてのアクセスは、踏み台ホストの使用によってゲートされます。マルチアカウントランディングゾーン (MALZ) とシングルアカウントランディングゾーン (SALZ) の両方の AMS Advanced アカウントにアクセスするために、Linux と Windows RDP の両方の踏み台を維持します。

踏み台には、プライベート接続 (VPN または Direct Connect)DX 経由でのみアクセスできます。インバウンドトラフィックを防ぐためのファイアウォールに加えて、踏み台は固定スケジュールで定期的に再プロビジョニングされます (既存の認証情報を使用)。

#### Note

EC2 インスタンスへのファイルの移動については、「[ファイル転送: Local Windows または MAC PC から Linux Amazon EC2](#)」を参照してください。

## MALZ

アカウントインスタンスにアクセスするには、Active Directory (AD) 認証情報を使用して踏み台インスタンスにログインします。Amazon は境界ネットワーク VPC (ネットワークアカウント) にある踏み台を使用し、共有サービスアカウントの Customer Bastions サブネットにあるカスタマー踏み台を使用します。

AMS 環境が最初にオンボーディングされると、選択に応じて 2 つの SSH 踏み台と 2 つの RDP 踏み台があります。

## SALZ

アカウントインスタンスにアクセスするには、Active Directory (AD) 認証情報を使用して踏み台インスタンスにログインします。AMS は境界ネットワークサブネットにある踏み台を使用し、プライベートサブネットにある踏み台を使用します。

アカウントが最初にオンボーディングされると、デフォルトで 2 つの RDP と 2 つの SSH 踏み台があります。

### Note

シングルアカウントランディングゾーンの一部として、AMS はスタックにアクセスするための RDP (Windows) 踏み台と SSH (Linux) 踏み台の両方を提供します。ただし、RDP 踏み台のみを使用するか、SSH 踏み台のみを使用するかを選択できます。RDP のみ、または SSH 踏み台のみを維持するようにリクエストするには、サービスリクエストを送信します。

インスタンスにアクセスするには、以下が必要です。

- スタックに付与されたアクセス。スタックへのアクセス許可を取得するには、[「スタック管理者アクセス | 許可」](#)または[「スタック読み取り専用アクセス | 許可」](#)を参照してください。
- インスタンスへのアクセスを許可できるように、アクセスするスタック ID。スタック ID を検索するには、「」を参照してください[AMS でスタック IDs を検索する](#)。
- アクセスするインスタンス IP。インスタンス IP を検索するには、「」を参照してください[AMS でインスタンス IDs または IP アドレスを検索する](#)。
- DNS フレンドリ踏み台名または踏み台 IP。次に、DNS フレンドリな踏み台名の使用方法と踏み台 IP を見つける方法について説明します。

# DNS フレンドリ踏み台名

AWS Managed Services (AMS) は、DNS フレンドリな踏み台名を使用します。

## MALZ

マルチアカウントランディングゾーン (MALZ) の場合、AMS マネージド Active Directory の FQDN の踏み台に DNS レコードが作成されます。AMS は、必要に応じて Linux と Windows の踏み台を置き換えます。たとえば、デプロイする必要がある新しい踏み台 AMI がある場合、踏み台 DNS レコードは新しい有効な踏み台を指すように動的に更新されます。

1. SSH (Linux) 踏み台にアクセスするには、次のような DNS レコードを使用します。  
`sshbastion(1-4).Your_Domain.com`

たとえば、ドメインが の場合Your\_Domain :

- `sshbastion1.Your_Domain.com`
- `sshbastion2.Your_Domain.com`
- `sshbastion3.Your_Domain.com`
- `sshbastion4.Your_Domain.com`

2. RDP (Windows) 踏み台にアクセスするには、 のような DNS レコードを使用します  
`rdp-Username.Your_Domain.com`。

たとえば、ユーザー名が alex、test、demo、または でbob、ドメインが の場合Your\_Domain.com :

- `rdp-alex.Your_Domain.com`
- `rdp-test.Your_Domain.com`
- `rdp-demo.Your_Domain.com`
- `rdp-bob.Your_Domain.com`

## SALZ

シングルアカウントランディングゾーン (SALZ) は、必要に応じて Linux と Windows の踏み台を置き換えます。たとえば、デプロイする必要がある新しい踏み台 AMI がある場合、踏み台 DNS レコードは新しい有効な踏み台を指すように動的に更新されます。

1. SSH (Linux) 踏み台にアクセスするには、次のような DNS レコードを使用します。  
`sshbastion(1-4).AAccountNumber.amazonaws.com.`

たとえば、123456789012はアカウント番号です。

- `sshbastion1.A123456789012.amazonaws.com`
- `sshbastion2.A123456789012.amazonaws.com`
- `sshbastion3.A123456789012.amazonaws.com`
- `sshbastion4.A123456789012.amazonaws.com`

2. RDP (Windows) 踏み台にアクセスするには、 のような DNS レコードを使用します  
`rdpbastion(1-4).ACCOUNT_NUMBER.amazonaws.com.`

たとえば、123456789012はアカウント番号です。

- `rdpbastion1.A123456789012.amazonaws.com`
- `rdpbastion2.A123456789012.amazonaws.com`
- `rdpbastion3.A123456789012.amazonaws.com`
- `rdpbastion4.A123456789012.amazonaws.com`

## 単一アカウントランディングゾーン (SALZ) 踏み台でのコスト削減

AMS は、Amazon EC2 インスタンスに接続するためのデフォルト設定で 2 つの SSH 踏み台と 2 つの RDP 踏み台を提供し、サービスオペレーションのデフォルト設定で 2 つの DMZ 踏み台をデプロイします。踏み台はデフォルトで m4. large Amazon EC2 インスタンスを使用します。踏み台に使用される Amazon EC2 インスタンスを t3.small に変更し、コストを削減することもできます。

オンデマンドインスタンス、スポットインスタンス、または Savings Plans を使用している場合は、この機能を検討し、コストを削減する必要があります。リザーブドインスタンスを使用する場合は、t3.small インスタンスを使用するとコストを削減できるかどうかを検討してください。インスタンスタイプを変更するには、AMS アカウントから [管理 | 高度なスタックコンポーネント | EC2 インスタンススタック | サイズ変更 \(ct-15mazjj88xc69\) CT](#) を使用して RFC を送信します。

その他の質問については、クラウドサービスデリバリーマネージャー (CSDM) にお問い合わせください。または、この機能のメリットを享受できるかどうかを確認してください。

## 踏み台 IP アドレスの使用

AMS のお客様は、[DNS フレンドリ踏み台名](#) 前述の または踏み台 IP アドレスのいずれかの SSH および RDP 踏み台を使用できます。

アカウントの踏み台 IP アドレス、SSH、RDP を見つけるには：

1. マルチアカウントランディングゾーンのみ: 共有サービスアカウントにログインします。
2. EC2 コンソールを開き、インスタンスの実行を選択します。

インスタンスページが開きます。

3. 上部のフィルターボックスに、ssh-bastion または rdp-bastion を入力します。

上部のフィルターボックスに、customer-ssh または customer-rdp を入力します。

アカウントの SSH および/または RDP 踏み台が表示されます。

SSH 踏み台に加えて、リストに AMS 境界ネットワーク踏み台が表示される場合がありますが、これは利用できません。

4. SSH または RDP 踏み台を選択します。Windows コンピュータを使用していて、Linux インスタンスにログインする場合は、SSH 踏み台を使用します。Windows インスタンスにログインする場合は、RDP 踏み台を使用します。Linux OS で Windows インスタンスにログインする場合は、RDP トンネルを介して SSH 踏み台を使用します (これにより Windows デスクトップにアクセスできます)。Linux OS から Linux インスタンスにアクセスするには、SSH 踏み台を使用します。

## AMS でのインスタンスアクセスの例

これらの例は、RFC を通じてアクセス権が付与された後に踏み台を使用して AMS アカウントのインスタンスにログインする方法を示しています。アクセス許可の取得については、「」を参照してください [インスタンスアクセスのリクエスト](#)。

### Note

EC2 インスタンスへのファイルの移動については、[「ファイル転送: Local Windows または MAC PC から Linux Amazon EC2」](#) を参照してください。



## 必要なデータ :

- 踏み台 DNS フレンドリ名または IP アドレス: 「」で説明されているように DNS フレンドリ名を使用する [DNS フレンドリ踏み台名](#) か、「」で説明されているように踏み台 IP アドレスを見つけて [す踏み台 IP アドレスの使用](#)。

### Note

Amazon EC2 Auto Scaling グループを介して作成された Amazon EC2 インスタンスには、入出力をサイクルする IP アドレスがあり、Amazon EC2 コンソールを使用してその IP アドレスを見つける必要があります。

- ユーザー名 ([DOMAIN\\_FQDN\USERNAME](#) など) とパスワード: アカウントの認証情報。 [USERNAME](#) は Active Directory ユーザー名である必要があります。

username@customerdomain.com 形式のユーザー名を使用できますが、PBIS の設定に問題がある可能性があります。

- スタック IP アドレス: スタックを起動するために送信した RFC の実行出力を確認するか、Amazon EC2 コンソールで Amazon EC2 インスタンス IP アドレスを検索します。単一の Amazon EC2 インスタンスの場合、AMS SKMS コマンド ListStackSummaries を使用してスタック ID を検索し、GetStack を使用してスタック IP アドレスを検索することもできます。AMS SKMS API リファレンスについては、AWS Artifact コンソールのレポートタブを参照してください。

必要に応じて踏み台 IP アドレス SSH または RDP にアクセスし、次のいずれかの手順を使用してログインします。

### Note

RDP 踏み台では、2 つの同時接続のみが許可されます。したがって、最適なシナリオでは、同時に Windows スタックに接続できるのは 4 人の管理者のみです。RDP 用にさらに接続が必要な場合は、[「AMS オンボーディングガイド」の「アプリケーション移行/オンボーディング中の AMS 踏み台オプション」](#)を参照してください。

## Linux コンピュータから Linux インスタンスへ

SSH を使用して SSH 踏み台に接続し、次に Linux インスタンスに接続します。

## MALZ

フレンドリ踏み台名の詳細については、[「DNS 踏み台」](#)を参照してください。

Linux インスタンスに接続するには、まず SSH 踏み台に接続する必要があります。

1. シェルウィンドウを開き、次のように入力します。

```
ssh Domain_FQDN\\Username@SSH_bastion_name  
or SSH_bastion_IP
```

Domain\_FQDN が「corp.domain.com」、アカウント番号が「123456789123」、Your\_Domain が「amazonaws.com」、踏み台「4」、ユーザー名が「JoeSmith」の場合、次のようになります。

```
ssh corp.domain.com\\JoeSmith sshbastion4.A123456789123.amazonaws.com
```

2. 会社の Active Directory 認証情報を使用してログインします。
3. Bash プロンプトが表示されたら、インスタンスに SSH インし、次のように入力します。

```
ssh Domain_FQDN\\Username@Instance_IP
```

または、Login フラグ (-l) を使用できます。

```
ssh -l Domain_FQDN\\Username@Instance_IP
```

## SALZ

フレンドリ踏み台名の詳細については、[「DNS 踏み台」](#)を参照してください。

Linux インスタンスに接続するには、まず SSH 踏み台に接続する必要があります。

1. シェルウィンドウを開き、次のように入力します。

```
ssh DOMAIN_FQDN\\USERNAME@SSH_BASTION_name  
or SSH_BASTION_IP
```

アカウント番号が 123456789123 で、踏み台 4 を選択し、ユーザー名が JoeSmith の場合、次のようになります。

```
ssh corp.domain.com\\JoeSmith sshbastion1.A123456789123.amazonaws.com
```

2. 会社の Active Directory 認証情報を使用してログインします。
3. Bash プロンプトが表示されたら、インスタンスに SSH インし、次のように入力します。

```
ssh DOMAIN_FQDN\\USERNAME@INSTANCE_IP
```

または、Login フラグ (-l) を使用できます。

```
ssh -l DOMAIN_FQDN\\USERNAME@INSTANCE_IP
```

## Linux コンピュータから Windows インスタンスへ

SSH トンネルと RDP クライアントを使用して、Linux コンピュータから Windows インスタンスに接続します。

### MALZ

この手順では、Linux 用のリモートデスクトップ接続クライアントが必要です。この例では、Microsoft リモートデスクトップ (Windows リモートデスクトップサービスに接続するためのオープンソースの UNIX クライアント) を使用します。Rdesktop は代替手段です。

#### Note

Windows インスタンスへのログイン方法は、使用しているリモートデスクトップクライアントによって異なる場合があります。

まず SSH トンネルを確立してからログインします。

フレンドリ踏み台名の詳細については、「」を参照してください [DNS フレンドリ踏み台名](#)。

開始する前に:

- 接続するインスタンスへのアクセスをリクエストします。詳細については、[「アクセスリクエスト」](#)を参照してください。
- 接続するわかりやすい DNS SSH 踏み台名を選択します。次に例を示します。

```
sshbastion(1-4).Your_Domain
```

Domain\_FQDN が「corp.domain.com」で、AMS が管理する Your\_Domain が「amazonaws.com」で、踏み台「4」を選択し、ユーザー名が JoeSmith の場合、次のようになります。

```
ssh corp.domain.com\\JoeSmith sshbastion4.amazonaws.com
```

- 接続するインスタンスの IP アドレスを見つけます。詳細については、[「インスタンス ID または IP アドレスの検索」](#)を参照してください。

1. Linux デスクトップから Windows インスタンスへの SSH トンネル経由で RDP を設定します。正しい値で ssh コマンドを発行するには、いくつかの方法があります。

- Linux シェルで変数を設定し、SSH 接続コマンドを入力します。

```
BASTION="sshbastion(1-4).Your_Domain"  
WINDOWS="Windows_Instance_Private_IP"  
AD="AD_Account_Number"  
USER="AD_Username"  
ssh -L 3389:$WINDOWS:3389 A$AD\\\\$USER@$BASTION
```

たとえば、次の値を使用する場合です。

```
BASTION="sshbastion4.A123456789123.amazonaws.com"
```

```
WINDOWS="172.16.3.254"
```

```
AD="ACORP_example"
```

```
USER="john.doe"
```

- 変数値を ssh コマンドに直接追加します。

いずれの場合も、レンダリングされたリクエストは次のようになります (変数値の同じセットを想定)。

```
ssh -L 3389:172.16.3.254:3389 ACORP_example\\\\john.doe@myamsadomain.com
```

2. どちらか: リモートデスクトップクライアントを開き、ループバックアドレスとポート 127.0.0.1:3389 を入力し、接続を開きます。

または、新しい Linux デスクトップシェルから Windows インスタンスにログインします。RDesktop を使用する場合、コマンドは次のようになります。

```
rdesktop 127.0.0.1:3389
```

Windows インスタンスのリモートデスクトップウィンドウが Linux デスクトップに表示されます。

 Tip

リモートデスクトップセッションの開始に失敗した場合、SSH 踏み台からの Windows インスタンスへのネットワーク接続が、ステップ 1 のシェルからのポート 3389 で許可されていることを確認します (private\_ip\_address\_of\_windows\_instance 適切に置き換えてください)。

```
nc private_ip_address_of_windows_instance 3389 -v -z
```

成功 :

```
nc 172.16.0.83 3389 -v -z
Connection to 172.16.0.83 3389 port [tcp/ms-wbt-server] succeeded
netstat -anvp | grep 3389
tcp    0      0 172.16.0.253:48079 172.16.3.254:3389 ESTABLISHED
```

## SALZ

シングルアカウントランディングゾーンのこの手順では、Linux 用のリモートデスクトップ接続クライアントが必要です。この例では、Microsoft リモートデスクトップ (Windows リモートデスクトップサービスに接続するためのオープンソースの UNIX クライアント) を使用します。Rdesktop は代替手段です。

**Note**

Windows インスタンスへのログイン方法は、使用しているリモートデスクトップクライアントによって異なる場合があります。

まず SSH トンネルを確立してからログインします。

フレンドリ踏み台名の詳細については、「」を参照してください[DNS フレンドリ踏み台名](#)。

開始する前に:

- 接続するインスタンスへのアクセスをリクエストします。詳細については、[「アクセスリクエスト」](#)を参照してください。
- 接続するわかりやすい DNS SSH 踏み台名を選択します。次に例を示します。

```
sshbastion(1-4).AMSAccountNumber.amazonaws.com
```

アカウント番号が 123456789123 で、踏み台 4 を選択した場合、次のようになります。

```
sshbastion4.A123456789123.amazonaws.com
```

- 接続するインスタンスの IP アドレスを見つけます。詳細については、[「インスタンス ID または IP アドレスの検索」](#)を参照してください。

1. Linux デスクトップから Windows インスタンスへの SSH トンネル経由で RDP を設定します。正しい値でsshコマンドを発行するには、いくつかの方法があります。

- Linux シェルで変数を設定し、SSH 接続コマンドを入力します。

```
BASTION="sshbastion(1-4).AMSAccountNumber.amazonaws.com"
WINDOWS="WINDOWS_INSTANCE_PRIVATE_IP"
AD="AD_ACCOUNT_NUMBER"
USER="AD_USERNAME"
ssh -L 3389:$WINDOWS:3389 A$AD\\$USER@$BASTION
```

たとえば、次の値を使用する場合です。

```
BASTION="sshbastion4.A123456789123.amazonaws.com"
```

```
WINDOWS="172.16.3.254"
```

```
AD="ACORP_example"
```

```
USER="john.doe"
```

- 変数値を ssh コマンドに直接追加します。

いずれの場合も、レンダリングされたリクエストは次のようになります (変数値の同じセットを想定)。

```
ssh -L 3389:172.16.3.254:3389 ACORP_example\\\
\john.doe@sshbastion4.A123456789123.amazonaws.com
```

2. どちらか: リモートデスクトップクライアントを開き、ループバックアドレスとポート 127.0.0.1:3389 を入力し、接続を開きます。

または、新しい Linux デスクトップシェルから Windows インスタンスにログインします。RDesktop を使用する場合、コマンドは次のようになります。

```
rdesktop 127.0.0.1:3389
```

Windows インスタンスのリモートデスクトップウィンドウが Linux デスクトップに表示されます。

#### Tip

リモートデスクトップセッションの開始に失敗した場合、SSH 踏み台からの Windows インスタンスへのネットワーク接続が、ステップ 1 のシェルからのポート 3389 で許可されていることを確認します (private\_ip\_address\_of\_windows\_instance 適切に置き換えてください)。

```
nc private_ip_address_of_windows_instance 3389 -v -z
```

成功 :

```
nc 172.16.0.83 3389 -v -z
Connection to 172.16.0.83 3389 port [tcp/ms-wbt-server] succeeded
netstat -anvp | grep 3389
```



```
tcp    0    0 172.16.0.253:48079 172.16.3.254:3389 ESTABLISHED
```

## Windows コンピュータから Windows インスタンスへ

Windows リモートデスクトップ接続クライアントを使用して、Windows コンピュータから Windows インスタンスに接続します。

### MALZ

フレンドリ踏み台名の詳細については、「」を参照してください[DNS フレンドリ踏み台名](#)。

1. 標準の Windows プログラムであるリモートデスクトップ接続プログラムを開き、ホスト名フィールドに Windows 踏み台の名前を入力します。
2. 接続 を選択します。リモートデスクトップ接続は、踏み台への RDP 接続を試みます。

成功すると、認証情報ダイアログボックスが開きます。アクセスを取得するには、Windows インスタンスと同様に、会社の Active Directory 認証情報を使用します。

3. 踏み台でリモートデスクトップ接続プログラムを開き、接続する Windows インスタンスの IP アドレス (10.0.0.100 など) を入力し、接続を選択します。Windows インスタンスに接続する前に、会社の Active Directory 認証情報が再度必要です。

### SALZ

フレンドリ踏み台名の詳細については、「」を参照してください[DNS フレンドリ踏み台名](#)。

1. 標準の Windows プログラムであるリモートデスクトップ接続プログラムを開き、ホスト名フィールドに Windows 踏み台の名前を入力します。たとえば、です。アカウント番号が 123456789123 で `rdpbastion(1-4).AMSAccountNumber.amazonaws.com`、踏み台 4、を選択した場合、このようになります `rdpbastion4.A123456789123.amazonaws.com`。
2. 接続 を選択します。リモートデスクトップ接続は、踏み台への RDP 接続を試みます。

成功すると、認証情報ダイアログボックスが開きます。アクセスを取得するには、Windows インスタンスと同様に、会社の Active Directory 認証情報を使用します。

3. 踏み台でリモートデスクトップ接続プログラムを開き、接続する Windows インスタンスの IP アドレス (10.0.0.100 など) を入力し、接続を選択します。Windows インスタンスに接続する前に、会社の Active Directory 認証情報が再度必要です。

## Windows コンピュータから Linux インスタンスへ

Windows 環境から SSH 踏み台に RDP を送信するには、次の手順に従います。

### MALZ

開始する前に:

- 接続するインスタンスへのアクセスをリクエストします。詳細については、[「アクセスリクエスト」](#)を参照してください。
- 接続するわかりやすい DNS SSH 踏み台名を選択します。次に例を示します。

```
sshbastion(1-4).YOUR_DOMAIN
```

YOUR\_DOMAIN が "myamsaddomain.com" で、踏み台 4 を選択した場合、次のようになります。

```
sshbastion4.myamsaddomain.com
```

- 接続するインスタンスの IP アドレスを見つけます。詳細については、[「インスタンス ID または IP アドレスの検索」](#)を参照してください。

Windows マシンから Linux インスタンスに接続するには、まず SSH 踏み台に接続する必要があります。

ネイティブの Windows [OpenSSH クライアント](#)を使用するか、ローカルマシンに [PuTTY](#) をインストールします。OpenSSH の詳細については、[「Windows での OpenSSH」](#)を参照してください。

1. ネイティブ Windows を使用するか PuTTY を開き、SSH 踏み台ホスト名または SSH 踏み台 IP アドレスを入力します。たとえば、10.65.2.214 (22 は SSH に使用されるポートで、デフォルトで設定されます) です。
2. OpenSSH または PuTTY は踏み台への SSH 接続を試み、シェルウィンドウを開きます。
3. 会社の Active Directory 認証情報は、RDP ホストと同じように使用してアクセスできるようにします。
4. Bash プロンプトが表示されたら、インスタンスに SSH します。次のとおりに入力します。

```
ssh DOMAIN_FQDN\USERNAME@INSTANCE_IP
```

## SALZ

開始する前に:

- 接続先のインスタンスへのアクセスをリクエストします。詳細については、[「アクセスリクエスト」](#)を参照してください。
- 接続するわかりやすい DNS SSH 踏み台名を選択します。次に例を示します。

```
sshbastion(1-4).AMSAccountNumber.amazonaws.com
```

アカウント番号が 123456789123 で、踏み台 4 を選択した場合、次のようになります。

```
sshbastion4.A123456789123.amazonaws.com
```

- 接続するインスタンスの IP アドレスを見つけます。詳細については、[「インスタンス ID または IP アドレスの検索」](#)を参照してください。

Windows マシンから Linux インスタンスに接続するには、まず SSH 踏み台に接続する必要があります。

ネイティブ Windows [OpenSSH クライアント](#) を使用するか、ローカルマシンに [PuTTY](#) をインストールします。OpenSSH の詳細については、[「Windows での OpenSSH」](#)を参照してください。

1. ネイティブ Windows を使用するか PuTTY を開き、SSH 踏み台ホスト名または SSH 踏み台 IP アドレスを入力します。たとえば、10.65.2.214 (22 は SSH に使用されるポートで、デフォルトで設定されます) です。

2. OpenSSH または PuTTY は踏み台への SSH 接続を試み、シェルウィンドウを開きます。
3. 会社の Active Directory 認証情報は、RDP ホストと同じように使用してアクセスできるようにします。
4. Bash プロンプトが表示されたら、インスタンスに SSH します。次のとおりに入力します。

```
ssh DOMAIN_FQDN\USERNAME@INSTANCE_IP
```

## AMS アカウントのチームまたはロールベースのアクセスコントロール

シナリオ: 2 つのアプリケーションチーム A と B は、それぞれアプリケーション「AA」と「BB」に 1 つの AMS アカウントを使用します。チーム A はアプリ「AA」のリソースにのみアクセスし、チーム B はアプリ「BB」のリソースにのみアクセスします。設定方法を教えてください。

ITSM のツールを使用して、チームベースのアクセスコントロール (TBAC) を実装します。例えば、AMS API との統合に AMS ServiceNow Connector アプリを使用できます APIs 。この実装の大まかなガイダンスについては、CSDM にお問い合わせください。

# AMS Advanced の自動インスタンス設定

AMS Advanced 自動インスタンス設定サービスは毎日実行され、マネージド EC2 インスタンスの SSM エージェントと CloudWatch エージェントと設定ファイルを自動的にスキャンして更新します。更新は、必要に応じて以下に適用されます。

- SSM エージェントと CloudWatch エージェント
- CloudWatch 設定ファイル

これらの更新により、AMS は AMS が管理する EC2 インスタンスにアクセスし、適切な[ログ](#)とメトリクスを出力するようにインスタンスを設定できます。

## トピック

- [自動インスタンス設定の前提条件](#)
- [SSM エージェントの自動インストール](#)
- [自動変更](#)

## 自動インスタンス設定の前提条件

変更管理を使用してインスタンスをデプロイする AMS Advanced のお客様は、次の前提条件を満たす必要があります。

- SSM エージェントがインストールされ、管理状態になります。
- インスタンスはマネージドインスタンスとしてタグ付けされます。  
( aws:cloudformation:stack-name タグには stack- または で始まる値があります ) sc-。

SSM エージェントがまだインスタンスにインストールされていない場合は、AMS SSM エージェントの自動インストール機能を使用してインストールできます。詳細については、「[SSM エージェントの自動インストール](#)」を参照してください。

または、SSM エージェントを手動でインストールすることもできます。詳細については次を参照してください:

- Linux: [Linux の EC2 インスタンスに SSM エージェントを手動でインストールする - AWS Systems Manager](#)

- Windows: [Windows Server の EC2 インスタンスに SSM エージェントを手動でインストールする - AWS Systems Manager](#)

SSM エージェントの詳細については、AWS ドキュメント「[SSM エージェントの使用](#)」を参照してください。

## SSM エージェントの自動インストール

### Important

SSM エージェントの自動インストールは、アジアパシフィック (マレーシア) リージョンをサポートしていません。

AMS で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理するには、各インスタンスに AWS Systems Manager SSM エージェントをインストールする必要があります。インスタンスに SSM Agent がインストールされていない場合は、AMS SSM Agent 自動インストール機能を使用できます。

### Note

- この機能は、Auto Scaling グループになく、AMS でサポートされている Linux オペレーティングシステムを実行する EC2 インスタンスでのみ使用できます。
- AMS SSM エージェントの自動インストール機能は、デフォルトで無効になっています。有効にするには、CA または CSDM にお問い合わせください。

## SSM エージェント使用の前提条件

- ターゲットインスタンスに関連付けられたインスタンスプロファイルに、次のいずれかのポリシー (またはそれらに許可リストされている同等のアクセス許可) があることを確認します。
  - AmazonSSMManagedEC2InstanceDefaultPolicy
  - AmazonSSMManagedInstanceCore
- 上記のポリシーにリストされているアクセス許可を明示的に拒否する AWS Organizations レベルのサービスコントロールポリシーがないことを確認します。

詳細については、「[Systems Manager に必要なインスタンスのアクセス許可を設定する](#)」を参照してください。

- アウトバウンドトラフィックをブロックするには、ターゲットインスタンスが存在する VPC で次のインターフェイスエンドポイントが有効になっていることを確認します (URL の「リージョン」を適切に置き換えます)。
  - ssm.<region>.amazonaws.com
  - ssmmessages.<region>.amazonaws.com
  - ec2messages.<region>.amazonaws.com

詳細については、「[Systems Manager のために VPC エンドポイントを使用して EC2 インスタンスのセキュリティを強化する](#)」を参照してください。

マネージドノードの可用性の有効化またはトラブルシューティングに関する一般的なヒントについては、「[解決策 2: インスタンスに IAM インスタンスプロファイルが指定されていることを確認する \(EC2 インスタンスのみ\)](#)」を参照してください。

#### Note

AMS は、自動インストールプロセスの一環として各インスタンスを停止および開始します。インスタンスが停止すると、インスタンスストアボリュームに保存されているデータと RAM に保存されているデータは失われます。詳細については、「[インスタンスを停止するとどうなるか](#)」を参照してください。

## インスタンスへの SSM エージェントの自動インストールをリクエストする

アカウントが AMS Accelerate Patch アドオンにオンボードされている場合は、インスタンスのパッチメンテナンスウィンドウ (MW) を設定します。パッチプロセスを完了するには、作業中の SSM エージェントが必要です。インスタンスに SSM エージェントがない場合、AMS はパッチメンテナンスウィンドウ中に自動的にインストールしようとします。

#### Note

AMS は、自動インストールプロセスの一環として各インスタンスを停止および開始します。インスタンスが停止すると、インスタンスストアボリュームに保存されているデータと RAM



に保存されているデータは失われます。詳細については、[「インスタンスを停止するとどうなるか」](#)を参照してください。

## SSM Agent 自動インストールの仕組み

AMS は EC2 ユーザーデータを使用して、インスタンスでインストールスクリプトを実行します。ユーザーデータスクリプトを追加してインスタンスで実行するには、AMS が各インスタンスを停止して起動する必要があります。

インスタンスに既存のユーザーデータスクリプトがすでにある場合、AMS は自動インストールプロセス中に次の手順を実行します。

1. 既存のユーザーデータスクリプトのバックアップを作成します。
2. 既存のユーザーデータスクリプトを SSM エージェントのインストールスクリプトに置き換えます。
3. インスタンスを再起動して SSM エージェントをインストールします。
4. インスタンスを停止し、元のスクリプトを復元します。
5. 元のスクリプトを使用してインスタンスを再起動します。

## 自動変更

AMS Advanced 自動インスタンス設定サービスは、必要に応じて EC2 インスタンスを変更します。

変更点：

- [Linux インスタンスでコードを自動的に更新する](#)
- [Linux インスタンスで PBIS を自動的に更新する](#)
- [SSM エージェントの最小バージョンと CloudWatch エージェントを自動的に更新する](#)
- [CloudWatch 設定ファイル、更新の詳細](#)
- [自動的に設定されたログ](#)

## Linux インスタンスでコードを自動的に更新する

AMS は Linux インスタンスのインスタンスコードを自動的に更新します。これにより、AMS コンポーネントと環境の運用上の安定性とセキュリティが完全に向上します。

よくある質問：

Linux のインスタンスコード (OIC) には何が含まれていますか？

OIC には、ams-toolkit パッケージと、いくつかの設定ファイルと cron ジョブが含まれています。AMS では、統合のためにこれらのファイルとパッケージが必要です (Active Directory、CloudFormation、およびその他の依存関係)。これらのファイルを AMS 提供の AMIs するか、ワークロードの取り込み中にインスタンスに をインストールします。

AMS はいつ OIC を更新しますか？

AMS は、バグ修正やその他の改善を加えて新しいバージョンをリリースするときに OIC を更新します。OIC のバージョンと更新を確認するワークフローは、毎日実行されます。

## Linux インスタンスで PBIS を自動的に更新する

AMS は Power Broker Identity Service (PBIS) モジュールを使用して、Linux インスタンスを AMS マネージド Active Directory に結合します。

AMS は Linux インスタンスで PBIS を自動的に更新します。

よくある質問：

AMS はいつ PBIS を更新しますか？

AMS は再起動時に PBIS 更新を有効にします。使用可能な新しい PBIS バージョンがある場合、AMS は次のインスタンスの再起動中に新しいバージョンをインストールしようとします。

PBIS 更新はオフにできますか？

PBIS 更新は、インスタンスレベルまたはアカウントレベルでオフにできます。

- アカウントレベル：SSM パラメータストアにパラメータを作成します: 名前: /ams/skip-pbis-update、値: true (大文字と小文字は問いません)。

### Note

インスタンスプロファイルには、SSM パラメータを読み取るアクセス許可が必要です。フラグがない場合、デフォルトの動作は更新を実行することです。

- インスタンスレベル：

- タグベース: インスタンスに次のタグを追加します: キー: `skip_pbis_update`、値: `true` (大文字と小文字は問いません)。
- Config ファイル: `/opt/aws/ams/etc/ams.conf.d/state.ini` ファイルに次のフラグを追加します。 `skip_pbis_update = true`。

#### Note

タグの優先度は SSM パラメータよりも高くなります。PBIS 更新は、パラメータを使用してアカウントレベルで無効にできますが、タグ `Key:skip_pbis_update`、を追加することで、単一 (または複数の) インスタンスで無効にできます `Value: false`。

説明されているオプションのいずれかを設定するには、AMS 環境の標準変更管理プロセスに従います。

## SSM エージェントの最小バージョンと CloudWatch エージェントを自動的に更新する

AMS Advanced の最小バージョン (SSM または CloudWatch エージェント) は、AMS サービスチームによってテストされ、オペレーティングシステム用に事前に承認されているバージョンです。プロアクティブに保ち、最新の安定した互換性のあるバージョンを実行しようとするため、バージョン番号は時間の経過とともに変化します。現在の最小バージョンは、サービスリクエストを AMS に発行することで確認できます。

### • SSM エージェント管理

Amazon SSM エージェントは、インスタンスでリモートコマンドを実行する責任があります。インスタンス設定の自動化により、SSM エージェントが最小バージョンを実行していることが保証されます。

### • Cloudwatch エージェント管理

Amazon CloudWatch エージェントは、OS ログとメトリクスの出力を担当します。自動インスタンス設定は以下を実行します。

- 必要に応じて、レガシー CloudWatch Log エージェントを無効にし、設定を新しい統合 CloudWatch エージェントに移行します。

- インスタンスがレガシー CloudWatch Log Agent を実行している場合、自動インスタンス設定はレガシー CloudWatch Log エージェントサービスを無効にし、その設定を統合 CloudWatch エージェントに移行します。
- CloudWatch 設定をカスタマイズして、適切なログとメトリクスを出力します。

影響を受けるファイルとディレクトリ：

- Windows
  - %ProgramData%\Amazon\AmazonCloudWatchAgent\
  - %ProgramData%\Amazon\AmazonCloudWatchAgent\Configs\
- リナックス
  - /opt/aws/amazon-cloudwatch-agent/etc/
  - /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/
  - /opt/aws/ams/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json

## CloudWatch 設定ファイル、更新の詳細

次の CloudWatch ディレクトリ ([推奨](#)ディレクトリを参照) からカスタム CloudWatch 設定 (JSON のみ) を読み取り、それらを標準の AMS CloudWatch 設定とマージします。

- CloudWatch ファイル
  - インスタンスの場合：
    - Windows
      - %ProgramData%\Amazon\AmazonCloudWatchAgent\Configs\
      - %ProgramFiles%\WindowsPowerShell\Modules\AWSManagedServices.Logging.Utilities\Files\Config.json
    - リナックス
      - /opt/aws/ams/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json
  - Amazon S3 の場合：
    - Windows:
      - [https://ams-configuration-artifacts-REGION\\_NAME.s3.REGION\\_NAME.amazonaws.com/configurations/cloudwatch/latest/windows-cloudwatch-config.json](https://ams-configuration-artifacts-REGION_NAME.s3.REGION_NAME.amazonaws.com/configurations/cloudwatch/latest/windows-cloudwatch-config.json)
    - Linux:

- [https://ams-configuration-artifacts-REGION\\_NAME.s3.REGION\\_NAME.amazonaws.com/configurations/cloudwatch/latest/linux-cloudwatch-config.json](https://ams-configuration-artifacts-REGION_NAME.s3.REGION_NAME.amazonaws.com/configurations/cloudwatch/latest/linux-cloudwatch-config.json)

## 自動的に設定されたログ

次のログを書き込むようにインスタンスを設定します。

- Windows:
  - AmazonSSMAgentLog
  - AmazonCloudWatchAgentLog
  - AmazonSSMErrorLog
  - AmazonCloudFormationLog
  - ApplicationEventLog
  - EC2ConfigServiceEventLog
  - MicrosoftWindowsAppLockerEXEAndDLLEventLog
  - MicrosoftWindowsAppLockerMSIAndScriptEventLog
  - MicrosoftWindowsGroupPolicyOperationalEventLog
  - SecurityEventLog
  - SystemEventLog
- Linux:
  - /var/log/amazon/ssm/amazon-ssm-agent.log
  - /var/log/amazon/ssm/errors.log
  - /var/log/audit/audit.log
  - /var/log/cloud-init-output.log
  - /var/log/cloud-init.log
  - /var/log/cron
  - /var/log/dpkg.log
  - /var/log/maillog
  - /var/log/messages
  - /var/log/secure
  - /var/log/spooler
  - /var/log/syslog

- /var/log/yum.log
- /var/log/zypper.log

# AMS でのモニタリングとイベント管理

## トピック

- [モニタリングとは](#)
- [AMS モニタリングシステムは何をモニタリングしますか？](#)
- [モニタリングの仕組み](#)
- [AMS アカウントのモニタリング設定の表示](#)
- [AMS アカウントのモニタリング設定の変更](#)
- [AMS でのアプリケーション対応インシデント通知](#)
- [AMS での OpsCenter の使用](#)
- [AMS からのアラート通知](#)
- [AMS での追加の CloudWatch アラームの作成](#)
- [AMS でのカスタム CloudWatch メトリクスとアラームの作成](#)
- [AMS での .Net および SQL Server 用の CloudWatch Application Insights の使用](#)
- [AMS での Amazon EventBridge マネージドルールの使用](#)
- [AMS の信頼できる修復](#)

AWS Managed Services (AMS) モニタリングシステムは、AMS リソースの障害、パフォーマンスの低下、セキュリティの問題を監視します。AMS モニタリングシステムは、Amazon CloudWatch(CloudWatch)、Amazon GuardDuty、Amazon Macie、などの AWS のサービスに依存しています AWS Health。AMS は、モニタリングシステムに加えて、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのマルウェアに対する保護のために TrendMicro DeepSecurity もデプロイします。エンドポイントセキュリティ (EPS) のデフォルトについては、「」を参照してください [エンドポイントセキュリティ \(EPS\)](#)。

AMS モニタリングには以下の利点があります。

- モニタリングベースライン。マネージドアカウントの他のモニタリングを設定していない場合でも、デフォルトの保護レベルを維持できます。詳細については、「[AMS でのベースラインモニタリングからのアラート](#)」を参照してください。
- 調査アラートを使用して、適切なアクションを決定します。例えば、GuardDuty が Amazon EC2 インスタンスに対するブルートフォース試行を示すアクティビティを検出した場合、AMS は VPC フローログを分析してアクティビティのオリジンとコンテキストを理解します。



- アプリケーションへの影響を防止または軽減するために、可能な場合はアラートを修正します。たとえば、スタンダードの Amazon EC2 インスタンスを使用していて、システムヘルスチェックに失敗した場合、AMS はインスタンスを停止して再起動することでインスタンスの復旧を試みます。詳細については、「[アラートの AMS 自動修復](#)」を参照してください。
- OpsCenter を使用して、アクティブで以前に解決されたアラートへの透明性。例えば、Amazon EC2 インスタンスで予期しない CPU 使用率が高い場合、AWS Systems Manager コンソールへのアクセス (OpsCenter コンソールへのアクセスを含む) をリクエストし、OpsCenter コンソールで OpsItem を直接表示できます。OpsCenter

## モニタリングとは

AMS モニタリングシステムは、障害、パフォーマンスの低下、セキュリティの問題がないか AWS リソースをモニタリングします。マネージドアカウントとして、AMS は該当する AWS リソースのアラームを設定およびデプロイし、モニタリングして、必要に応じて修復を実行します。

AMS モニタリングシステムは、アカウントのモニタリング設定に基づいてアラートを生成します。アカウントのモニタリング設定は、アラートを作成するアカウントのすべてのリソースパラメータを指します。リソースパラメータの詳細については、「」を参照してください[AMS でのベースラインモニタリングからのアラート](#)。アカウントのモニタリング設定には、CloudWatch アラーム定義と、アラート (アラームまたはイベント) を生成する CloudWatch イベントルールが含まれます。

ベースラインモニタリング設定は、マネージドアカウントのリソースをモニタリングするために AMS によってキュレートされたアラーム定義のセット ([AMS でのベースラインモニタリングからのアラート](#)) です。アカウントのモニタリング設定は、ユーザーがリクエストした変更の結果として、ベースライン設定とは異なる場合があります。

アカウントで設定されたベースラインモニタリングによって生成された差し迫った、進行中の、後退中の、または潜在的な障害、パフォーマンスの低下、またはセキュリティの問題の通知は、アラートと呼ばれます。アラートの例としては、Amazon CloudWatch アラーム、Amazon CloudWatch イベント、イベント、Amazon GuardDuty などの AWS サービスからの検出結果、Trend Micro Deep Security からのイベントまたはアラートなどがあります。

Amazon GuardDuty Amazon Macie、Trend Micro Deep Security などのセキュリティ関連の AWS サービスからのアラートは、セキュリティアラートと呼ばれ、他のタイプのアラートと区別されます。

AMS モニタリングには以下の利点があります。

- 要件を満たすようにベースラインリソースアラームをカスタマイズする機能。
- アプリケーションへの影響を防止または軽減するために、可能な場合はアラートを自動的に修復します。たとえば、スタンダードの Amazon EC2 インスタンスを使用していて、システムヘルスチェックに失敗した場合、AMS はインスタンスを停止して再起動することでインスタンスの復旧を試みます。詳細については、「[アラートの AMS 自動修復](#)」を参照してください。
- OpsCenter を使用して、アクティブで以前に解決されたアラートへの透明性。例えば、Amazon EC2 インスタンスで予期しない CPU 使用率が高い場合、コンソールへのアクセス AWS Systems Manager (OpsCenter コンソールへのアクセスを含む) をリクエストし、OpsCenter コンソールで OpsItem を直接表示できます。OpsCenter
- アラートを調査して、適切なアクションを決定します。
- アカウントの設定とサポートされている AWS サービスに基づいて生成されたアラート。アカウントのモニタリング設定は、アラートを作成するアカウント内のすべてのリソースパラメータを指します。アカウントのモニタリング設定には、CloudWatch アラーム定義と、アラート (アラームまたはイベント) を生成する EventBridge (旧 CloudWatch Events) が含まれます。リソースパラメータの詳細については、「」を参照してください[AMS でのベースラインモニタリングからのアラート](#)。
- 差し迫った障害、継続的障害、後退障害、潜在的な障害、パフォーマンスの低下、またはアカウントで設定されたベースラインモニタリングによって生成されたセキュリティ問題 (アラートと呼ばれる) の通知。アラートの例には、CloudWatch アラーム、イベント、GuardDuty や などの AWS サービスからの検出結果などがあります AWS Health。

## AMS モニタリングシステムは何をモニタリングしますか？

AWS Managed Services (AMS) 共有サービス責任モデルに従って、AMS モニタリングシステムは AWS インフラストラクチャをモニタリングします。モニタリング対象の AWS リソースや各リソースのアラートのタイプなど、AMS でのベースラインモニタリングの詳細については、「」を参照してください[AMS でのベースラインモニタリングからのアラート](#)。Amazon EC2 インスタンスの場合、AMS はオペレーティングシステムをモニタリングし、CPU 使用率やルートボリューム使用率などの OS メトリクスに基づいてベースラインモニタリングを提供します。

アプリケーションに合わせた AWS のサービスを使用した追加のモニタリングで AMS モニタリングを補足することをお勧めします。可用性のモニタリングに関するガイダンスについては、このホワイトペーパー[信頼性の柱](#)の「モニタリングとアラーム」セクションを参照してください。運用上のニーズに合わせて独自のモニタリングを設定できます。これを行う方法については、[AMS での追加の CloudWatch アラームの作成](#)「」および「」を参照してください[AMS でのカスタム CloudWatch メトリクスとアラームの作成](#)。

# AMS での Active Directory Trust の単一アカウントランディングゾーンのプロアクティブモニタリング

AMS シングルアカウントランディングゾーン (SALZ) は、AMS マネージドアカウントの Managed Active Directory (AD) と企業ドメイン間の一方向信頼 (複数可) のステータスをモニタリングします。Managed AD との一方向の信頼は、アクセスリクエストとインスタンスログオンリクエストにとって重要です。この新しいモニタリングにより、AMS は信頼関連の問題にプロアクティブに対応し、アクセス関連のインシデントを検出する平均時間を短縮できるようになりました。

この機能は、AWS Managed Services (AMS) アカウントで自動的に有効になります。

コストへの影響はわずかです。この機能は、4 つの AWS CloudWatch メトリクスと 2 つの AWS CloudWatch アラームを 1 つの信頼に使用します。

## モニタリングの仕組み

AWS Managed Services (AMS) のモニタリングアーキテクチャについては、次の図を参照してください。

次の図は、AMS マルチアカウントランディングゾーンと AMS シングルアカウントランディングゾーンのモニタリングワークフローの概要を示しています。

- 生成: アカウントのオンボーディング時に、AMS はマネージドアカウントで作成されたすべてのリソースのベースラインモニタリング (CloudWatch (CW) アラームと CW イベントルールの組み合わせ) を設定します。ベースラインモニタリング設定は、CW アラームがトリガーされたとき、または CW イベントが生成されたときにアラートを生成します。
- 集計:
  - マルチアカウントランディングゾーン: アラートは、アプリケーションおよびコア組織単位アカウント内のリソースによって生成され、セキュリティアカウントを通じて AMS モニタリングシステムに送信されます。
  - 単一アカウントランディングゾーン: リソースによって生成されたすべてのアラートは、アカウントの SNS トピックに誘導することで AMS モニタリングシステムに送信されます。
  - AMS が EC2 アラートをグループ化する方法を設定することもできます。AMS は、同じ EC2 インスタンスに関連するすべてのアラートを 1 つのインシデントにグループ化するか、必要に応じてアラートごとに 1 つのインシデントを作成します。この設定は、Cloud Service Delivery

Manager または Cloud Architect を使用していつでも変更できます。これは、マルチアカウントランディングゾーンとシングルアカウントランディングゾーンのどちらを使用している場合でも同じように機能します。

- 処理: AMS はアラートを分析し、影響の可能性に基づいてアラートを処理します。アラートは次に示すように処理されます。
- 既知の顧客への影響があるアラート: 新しいインシデントレポートと AMS の作成は、インシデント管理プロセスに従います。インシデント管理の詳細については、「」を参照してください [AMS インシデント対応](#)。

アラートの例: Amazon EC2 インスタンスはシステムヘルスチェックに失敗し、AMS はインスタンスを停止して再起動することでインスタンスの復旧を試みます。

- 顧客への影響が不明なアラート: これらのタイプのアラートの場合、AMS はインシデントレポートを送信します。多くの場合、AMS がアクションを実行する前に影響を検証するように求められます。ただし、インフラストラクチャ関連のチェックに合格した場合、AMS はインシデントレポートを送信しません。

例えば、Amazon EC2 インスタンスで 10 分以上の >85% CPU 使用率のアラートは、この動作が使用状況に基づいて予想される可能性があるため、すぐにインシデントとして分類することはできません。この例では、AMS Automation はリソースに対してインフラストラクチャ関連のチェックを実行します。これらのチェックに合格した場合、CPU 使用率が 99% を超えた場合でも、AMS はアラート通知を送信しません。インフラストラクチャ関連のチェックがリソースで失敗していることをオートメーションが検出した場合、AMS はアラート通知を送信し、緩和が必要かどうかを確認します。アラート通知については、このセクションで詳しく説明します。AMS は、通知で緩和オプションを提供します。アラートがインシデントであることを確認する通知に返信すると、AMS は新しいインシデントレポートを作成し、AMS インシデント管理プロセスが開始されます。「顧客への影響なし」または 3 日間応答なしの応答を受信するサービス通知は、解決済みとしてマークされ、対応するアラートは解決済みとしてマークされます。

- 顧客への影響がないアラート: 評価後、AMS がアラートに顧客への影響がないと判断した場合、アラートはクローズされます。

たとえば、は置き換えが必要な EC2 インスタンス AWS Health を通知しますが、そのインスタンスはその後終了しています。

## EC2 インスタンスグループ化通知

同じ EC2 インスタンスからのアラートを 1 つのインシデントにグループ化するように AMS モニタリングを設定できます。Cloud Service Delivery Manager または Cloud Architect がこれを設定できます。AMS 管理アカウントごとに設定できるパラメータは 4 つあります。

1. スコープ: アカウント全体またはタグベースのいずれかを選択します。
  - そのアカウントのすべての EC2 インスタンスに適用される設定を指定するには、スコープ = アカウント全体を選択します。
  - 特定のタグを持つそのアカウントの EC2 インスタンスにのみ適用される設定を指定するには、スコープ = タグベースを選択します。
2. グループ化ルール: クラシックまたはインスタンスを選択します。
  - アカウント内のすべてのリソースに対してインスタンスレベルのグループ化を設定するには、スコープ = アカウント全体、グループ化ルール = インスタンスを選択します。
  - インスタンスレベルのグループ化を使用するようにアカウント内の特定のリソースを設定するには、それらのインスタンスにタグを付け、スコープ = タグベース、グループ化ルール = インスタンスレベルを選択します。
  - アカウントのアラートにインスタンスグループ化を使用しないには、グループ化ルール = クラシックを選択します。
3. エンゲージメントオプション: なし、レポートのみ、またはデフォルトのいずれかを選択します。
  - 設定がアクティブな間、AMS がインシデントを作成したり、それらのリソースからアラームのオートメーションを実行したりしない場合は、なしを選択します。
  - 設定のアクティブ中に AMS がインシデントを作成したり、それらのリソースからアラームの自動化を実行したりせず、自動ヒーリング Systems Manager ドキュメントを実行したりせず、これらのイベントのレコードをレポートに含めるには、レポートのみを選択します。これは、やり取りするインシデントサポートケースの量を減らしたい場合や、非本番稼働用アカウントのインシデントなど、一部のリソースからのインシデントに即時の対応が必要ない場合に便利です。
  - AMS がアラートを処理し、オートメーションを実行し、必要に応じてインシデントケースを作成するには、デフォルトを選択します。
4. 解決: 24 時間、48 時間、または 72 時間のいずれかを選択します。最後に、インシデントケースが自動的にクローズされるタイミングを設定します。最後のケースのコレスポンスからの時間が、設定された解決後値に達すると、インシデントはクローズされます。

## アラート通知

アラート処理の一環として、AWS AWS Managed Services (AMS) は影響分析に基づいてインシデントを作成し、影響を特定できる場合に、修復のためのインシデント管理プロセスを開始します。影響が判断できない場合、AMS はサービス通知を通じてアカウントに関連付けられた E メールアドレスにアラート通知を送信します。一部のシナリオでは、このアラート通知は送信されません。たとえば、インフラストラクチャ関連のチェックが CPU 使用率の高いアラートを渡す場合、アラート通知は送信されません。詳細については、 のアラート処理プロセスの AMS モニタリングアーキテクチャの図を参照してください [モニタリングの仕組み](#)。

## タグベースのアラート通知

タグを使用して、リソースのアラート通知をさまざまな E メールアドレスに送信します。1 つの E メールアドレスに送信される通知は、複数のデベロッパーチームが同じアカウントを使用する場合に混乱を引き起こす可能性があるため、タグベースのアラート通知を使用するのがベストプラクティスです。タグベースのアラート通知は、選択した [EC2 インスタンスグループ化通知](#) 設定の影響を受けません。

タグベースのアラート通知を使用すると、次のことができます。

- 特定の E メールアドレスにアラートを送信する: 、を使用して `key = OwnerTeamEmail`、特定の E メールアドレスに送信する必要があるアラートを含むリソースにタグ付けします `value = EMAIL_ADDRESS`。
- 複数の E メールアドレスにアラートを送信する: 複数の E メールアドレスを使用するには、値のカンマ区切りリストを指定します。例えば、`key = OwnerTeamEmail` や `value = EMAIL_ADDRESS_1, EMAIL_ADDRESS_2, EMAIL_ADDRESS_3, ...` などです。値フィールドの合計文字数は 260 を超えることはできません。
- カスタムタグキーを使用する: カスタムタグキーを使用するには、タグベースの通信の自動通知を有効にすることを明示的に同意する E メールで CSDM にカスタムタグキー名を指定します。すべてのインスタンスとリソースで問い合わせタグに同じタグ付け戦略を使用するのがベストプラクティスです。

### Note

`OwnerTeamEmail` のキー値はキャメルケースである必要はありません。ただし、タグでは大文字と小文字が区別されるため、推奨形式を使用することをお勧めします。



ローカル部分をドメインから分離するには、E メールアドレスを完全に指定し、「アットマーク」 (@) を指定する必要があります。無効な E メールアドレスの例: *Team.AppATabc.xyz* または *john.doe*。タグ付け戦略の一般的なガイダンスについては、「[AWS リソースのタグ付け](#)」を参照してください。タグに個人を特定できる情報 (PII) を追加しないでください。可能な限り、ディストリビューションリストまたはエイリアスを使用します。

タグベースのアラート通知は、次の Amazon サービスのリソースでサポートされています。EC2、Elastic Block Store (EBS)、Elastic Load Balancing (ELB)、Application Load Balancer (ALB)、Network Load Balancer、リレーショナルデータベースサービス (RDS)、OpenSearch、Elastic File System (EFS)、FSx、Site-to-Site VPN。

## AMS アカウントのモニタリング設定の表示

アカウントのモニタリング設定には、表示できる 2 つの主要な部分があります。

- CloudWatch アラーム: CloudWatch コンソールに移動し、目的のさまざまなサービスを選択することで、アカウント内のすべての CW アラームを表示できます。
- CloudWatch Events:
  - マルチアカウントランディングゾーン: アカウントでモニタリングされる CloudWatch Events は、文字列 ですべての CW イベントルールをフィルタリングすることで確認できます "ams-"。
  - 単一アカウントランディングゾーン: アカウントでモニタリングされる CloudWatch Events は、文字列 ですべての CW イベントルールをフィルタリングすることで確認できます "mc-"。

## AMS アカウントのモニタリング設定の変更

Amazon EC2 リソースのベースラインモニタリング設定を変更できます。設定できるアラートについては、「」を参照してください[AMS でのベースラインモニタリングからのアラート](#)。アラートがアプリケーションの運用要件を満たすように、ベースラインモニターのアラーム定義、アラーム送信先、またはアラーム通知のオプトアウトを変更できます。マネジメント | その他 | その他 | 更新 CT (ct-0xdawir96cy7k) を以下の詳細とともに送信することで、前述の変更の一部またはすべてをリクエストできます。

- インスタンス IDs [オプション、記載されていない場合はアカウント内のすべてのインスタンスが対象範囲内]



- CloudWatch メトリクス名。CPU 使用率/スワップフリー/IOWait など
- ターゲット - SMS/SNS トピックの E メール ID/電話番号

ベースラインモニタリング設定でリクエストできる変更のタイプの詳細については、[Amazon CloudWatch ドキュメント](#)」を参照してください。

## AMS でのアプリケーション対応インシデント通知

アプリケーション対応の自動インシデント通知を使用して、AMS がユーザーに代わって作成するサポートケースのコミュニケーションエクスペリエンスをカスタマイズします。この機能を使用すると、AMS は [AWS Service Catalog AppRegistry](#) からカスタムワークロード設定を取得し、アプリケーションに関するメタデータを使用して AMS インシデント通信を強化し、ユーザーに代わって AMS によって作成されたサポートケースの重要度をカスタマイズします。この機能を使用するには、まず AMS アカウントで AWS Service Catalog AppRegistry をプロビジョニングする必要があります。

AMS モニタリングのデフォルトの詳細については、「」を参照してください[AMS でのモニタリングとイベント管理](#)。

## AMS アカウントに AppRegistry をプロビジョニングし、アプリケーションを作成する

AppRegistry サービスは、AMS アカウントのセルフサービスプロビジョニング (SSP) モードで使用できます。アクセスをリクエストする方法については、「[AMS SSP を使用して AMS アカウント AWS Service Catalog AppRegistry でプロビジョニングする](#)」を参照してください。

AppRegistry をプロビジョニングしたら、次のいずれかの方法を使用してアプリケーションを作成します。

1. AWS コンソール：AWS コンソールを使用して AppRegistry でアプリケーションを作成する方法の詳細については、AWS Service Catalog AppRegistry 管理者ガイドの「[アプリケーションの作成](#)」を参照してください。
2. CloudFormation: AppRegistry アプリケーションは、他のリソースを定義するのと同じように定義できます。詳細については、「CloudFormation ユーザーガイド」の[AWS Service Catalog AppRegistry リソースタイプのリファレンス](#)」を参照してください。

## タグを作成してケースエンリッチメントを有効にする

AMS がアプリケーションメタデータにアクセスする前に、アプリケーションにタグを付ける必要があります。次の表に、必要なタグを示します。

| タグキー      | タグ値  |
|-----------|------|
| ams マネージド | true |

## アプリケーションの AMS サポートケースの重要度をカスタマイズする

アプリケーションが組織にとってどの程度重要であるかを指定することで、AMS が作成したサポートケースの重要度をカスタマイズできます。この設定は、AppRegistry のアプリケーションに関連付けられた属性グループによって制御されます。属性グループ名の名前は、次のパターンと一致する必要があります。

```
AMS.<ApplicationName>.CommunicationOptions
```

前述のパターンでは、 はアプリケーションの作成時に AppRegistry で使用される名前と一致する ApplicationName 必要があります。

コンテンツの例：

```
{
  "SchemaVersion": "1.0",
  "Criticality": "low"
}
```

### SchemaVersion

これにより、使用しているスキーマバージョンと使用可能な機能のサブセットが決まります。

| スキーマバージョン | 機能                            |
|-----------|-------------------------------|
| 1.0       | 重要度値に基づいてカスタマイズされたサポートケースの重要度 |

## 重要度

このアプリケーションの重要度によって、AMS 自動システムによって作成されたサポートケースの重要度が決まります。

有効な値:

```
low|normal|high|urgent|critical
```

重要度レベルの詳細については、AWS サポート API リファレンスの[SeverityLevel](#)」を参照してください。

必須: はい

## 必要なアクセス許可を確認する

この機能を使用するには、AMS は次のアクセス AWS Identity and Access Management 許可にアクセスする必要があります。

- iam:ListRoleTags
- iam:ListUserTags
- resourcegroupstaggingapi:GetResources
- servicecatalog-appregistry:GetApplication
- servicecatalog-appregistry:ListAssociatedAttributeGroups
- servicecatalog-appregistry:GetAttributeGroup

### Important

上記のアクションを拒否する IAM ポリシーまたはサービスコントロールポリシー (SCP) がないことを確認します。

API コールは `ams-access-admin` ロールによって行われます。以下は、表示される可能性のある内容の例です。

```
arn:aws:sts::111122223333:assumed-role/ams-access-admin/AMS-AMSAppMetadataLookup-*
```

# AMS での OpsCenter の使用

AWS Managed Services (AMS) オペレーションチームは、[AWS Systems Manager OpsCenter](#) を使用して、リソースに関連する多くのアラートを診断および修復します。

OpsCenter を使用すると、AMS オペレーションチームの運用キューを透過的に表示しながら、平均解決時間 (MTTR) を短縮できます。

OpsCenter を使用すると、AMS は、[OpsItems](#) と呼ばれる運用作業項目を透過的に把握し、自動化ソリューションに加えて、AMS チームによって積極的に作業されています。

OpsCenter と OpsItems の詳細については、[AWS Systems Manager OpsCenter](#)」を参照してください。AWS マネジメントコンソールへのアクセスについては、[「AWS マネジメントコンソールの使用」](#)を参照してください。AWS マネジメントコンソールから、AWS Systems Manager コンソールと OpsCenter に移動できます。詳細については、[AWS Systems Manager 「Session Manager」](#)を参照してください。OpsCenter には、使用できる API も用意されています。詳細については、[OpsCenter の詳細](#)」を参照してください。

OpsCenter は、10 USD 未満の OpsItems を最大 1,000 個含む料金設定の機能です。詳細については、[「AWS Systems Manager の料金表」](#)を参照してください。

## AMS からのアラート通知

アラート処理の一環として、AWS AWS Managed Services (AMS) は影響分析に基づいてインシデントを作成し、影響を特定できる場合に、修復のためのインシデント管理プロセスを開始します。影響が判断できない場合、AMS はサービス通知を通じてアカウントに関連付けられた E メールアドレスにアラート通知を送信します。のアラート処理プロセスの AMS モニタリングアーキテクチャの図を参照してください[モニタリングの仕組み](#)。

## AMS によって生成されたアラートの受信

AWS Managed Services (AMS) を使用すると、Amazon EC2 リソースのアラート通知を直接受信して、通信の遅延を軽減できます。Amazon EC2 アラートを直接受信するには、管理 | モニタリングと通知 | SNS | サブスクライブ変更タイプ (ct-3rc19u1k017wu) を使用して、ターゲット (優先 E メール) を Amazon SNS トピック Direct-Customer-Alerts にサブスクライブします。

### Note

デフォルトでは、すべてのベースラインアラートが Direct-Customer-Alerts トピックに送信されるわけではありません。AMS モニタリングシステムによって生成されたすべてのアラート

トを表示するには、AMS モニタリングシステムの Amazon SNS トピックをサブスクライブします。リクエストで、「AMS モニタリングトピック」をリクエストし、アラートを受信するサブスクリプションチャンネル (Lambda、Amazon SQS、HTTP/S、E メール、SMS) を指定し、アラートを受信するエンドポイント (E メールプロトコルを選択した場合は E メールアドレスなど) を指定します。

AMS モニタリングトピックは、AMS 共有サービスで使用されるアラートを受信するため、ノイズが多い可能性があります。

詳細については、Amazon Simple Notification Service [Subscribe](#) API リファレンスの「Subscribe」セクションを参照してください。

AMS が提供するベースラインアラートのリストについては、「」を参照してください [AMS でのベースラインモニタリングからのアラート](#)。

## AMS でのタグベースのアラート通知

タグを使用して、リソースのアラート通知をさまざまな E メールアドレスに送信します。1 つの E メールアドレスに送信される通知は、複数のデベロッパーチームが同じアカウントを使用する場合に混乱を引き起こす可能性があるため、タグベースのアラート通知を使用するのがベストプラクティスです。

### Important

タグベースのアラート通知は、Amazon EC2、Amazon EBS、Elastic Load Balancing、Network Load Balancer、Application Load Balancer、Amazon RDS、Amazon Redshift、OpenSearch に関連する通知でのみ機能します。  
タグに個人を特定できる情報 (PII) を追加しないでください。

### 特定の E メールアドレスにアラートを送信する

、を使用して、特定の E メールアドレスに送信する必要があるアラートがあるリソースにタグ `key = OwnerTeamEmail` を付けます `value = EMAIL_ADDRESS`。

### 複数の E メールアドレスにアラートを送信する

複数の E メールアドレスを使用するには、値のカンマ区切りリストを指定します。例えば、`key = OwnerTeamEmail` や `value = EMAIL_ADDRESS_1, EMAIL_ADDRESS_2,`

`EMAIL_ADDRESS_3`, ... などです。値フィールドの合計文字数は 260 を超えることはできません。

カスタムタグキーを使用する

カスタムタグキーを使用するには、タグベースの通信の自動通知をアクティブ化する同意を提供する E メールで、カスタムタグキー名を CSDM に提供します。すべてのインスタンスとリソースで問い合わせタグに同じタグ付け戦略を使用するのがベストプラクティスです。

ローカル部分をドメインから分離するには、E メールアドレスを完全に指定し、「アットマーク」 (@) を指定する必要があります。無効な E メールアドレスの例: `Team.AppATabc.xyz` または `john.doe`。タグ付け戦略の一般的なガイダンスについては、「[タグの使用](#)」を参照してください。既存のリソースにタグを付けるには、デプロイ | 高度なスタックコンポーネント | タグ | 作成 (自動) (ct-3cx7we852p3af) 変更タイプを使用して RFC を送信します。

 Note

`OwnerTeamEmail` のキー値はキャメルケースである必要はありません。ただし、タグでは大文字と小文字が区別されるため、推奨形式を使用することをお勧めします。

アラートの AMS 自動修復

検証後、AWS Managed Services (AMS) は、このセクションで説明されている特定の条件とプロセスに従って、特定のアラートを自動的に修復します。

| アラート名       | 説明                                                                              | しきい値                                | アクション                                                                                                                     |
|-------------|---------------------------------------------------------------------------------|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| 壊れたセキユアチャネル | 壊れたセキユアチャネルアラームは、インスタンスが AD ドメインコントローラーとの接続を失ったときに Windows EC2 インスタンスでトリガーされます。 | しきい値は、過去 15 分間に定義された値を 10 回上回っています。 | AMS 自動修復は、インスタンスが SSM でオンラインであること、ホスト名が重複していないこと、AD コンピュータオブジェクトが CloudFormation スタックと整列していることを検証します。この修復により、セキユアチャネル接続が修 |

| アラート名             | 説明                                                               | しきい値                                       | アクション                                                                                                                                                                                       |
|-------------------|------------------------------------------------------------------|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                   |                                                                  |                                            | 復され、インスタンスへのアクセスが復元されます。                                                                                                                                                                    |
| ステータスチェックに失敗しました  | インスタンスのハードウェア障害または障害状態が発生する可能性があります。                             | システムは、過去 15 分以内に少なくとも 1 回失敗したステータスを検出しました。 | AMS 自動修復は、最初にインスタンスにアクセスできるかどうかを検証します。インスタンスにアクセスできない場合、インスタンスは停止して再起動されます。停止と起動により、インスタンスは新しい基盤となるハードウェアに移行できます。詳細については、次のセクション「EC2 Status Check Failure Remediation Automation」を参照してください。 |
| AMSLinuxDiskUsage | EC2 インスタンスの 1 つのマウントポイント (ボリュームの指定領域) のディスク使用量がいっぱいになるとトリガーされます。 | しきい値は、過去 30 分間に定義された値を 6 回上回っています。         | AMS 自動修復は、まず一時ファイルを削除します。十分なディスク容量が解放されない場合は、ボリュームがいっぱいになった場合のダウンタイムを防ぐためにボリュームを拡張します。                                                                                                      |



| アラート名                       | 説明                                                         | しきい値                               | アクション                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------|------------------------------------------------------------|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AMSWindow<br>sDiskUsag<br>e | EC2 インスタンスの 1 つのマウントポイント (ボリュームの指定領域) のディスク使用量がいっぱいになったとき。 | しきい値は、過去 30 分間に定義された値を 6 回上回っています。 | AMS 自動修復は、まず一時ファイルを削除します。十分なディスク容量が解放されない場合は、ボリュームがいっぱいになった場合のダウンタイムを防ぐためにボリュームを拡張します。                                                                                                                                                                                                                                                       |
| RDS-<br>EVENT<br>-0089      | DB インスタンスは割り当てられたストレージの 90% 以上を使用しています。                    | ストレージが 90% 以上割り当てられている。            | <p>AMS 自動修復は、まず DB が変更可能で使用可能、またはストレージフル状態であることを検証します。次に、CloudFormation の変更セットを通じて、割り当てられたストレージ、IOPS、ストレージスループットの向上を試みます。スタックドリフトが既に検出されている場合、ダウンタイムを防ぐために RDS API にフォールバックします。</p> <p>この機能は、RDS DB インスタンスに次のタグを追加することでオプトアウトできます。<br/>"Key: <code>ams:rt:ams-rds-max-allocated-storage-policy</code>, Value: <code>ams-opt-out</code>".</p> |

| アラート名          | 説明                                                       | しきい値                  | アクション                                                                                                                                                                                                                                                                                                              |
|----------------|----------------------------------------------------------|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RDS-EVENT-0007 | DB インスタンスに割り当てられたストレージが使い果たされました。解決するには、追加のストレージを割り当てます。 | ストレージは 100% 割り当てられます。 | <p>AMS 自動修復は、まず DB が変更可能で使用可能、またはストレージフル状態であることを検証します。次に、CloudFormation の変更セットを通じて、割り当てられたストレージ、IOPS、ストレージスループットの向上を試みます。スタックドリフトが既に検出されている場合、ダウンタイムを防ぐために RDS API にフォールバックします。</p> <p>この機能は、RDS DB インスタンスに次のタグを追加することでオプトアウトできます。<br/>"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".</p> |

| アラート名          | 説明                                                | しきい値                                                  | アクション                                                                                                                                                                                                                                                                                                                                                           |
|----------------|---------------------------------------------------|-------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RDS-EVENT-0224 | リクエストされた割り当てられたストレージが、設定された最大ストレージしきい値に達するか、超えます。 | DB インスタンスの最大ストレージしきい値が枯渇したか、リクエストされた割り当てられたストレージ以上です。 | <p>AMS 自動修復は、最初に、リクエストされた RDS ストレージの量が最大ストレージしきい値を超えていることを検証します。確認された場合、AMS は CloudFormation 変更セットを使用して最大ストレージしきい値を 30% 引き上げようとしています。または、CloudFormation を介してリソースがプロビジョニングされていない場合は RDS API を指示します。</p> <p>この機能は、RDS DB インスタンスに次のタグを追加することでオプトアウトできます。<br/>"Key: <code>ams:rt:ams-rds-max-allocated-storage-policy</code>, Value: <code>ams-opt-out</code>".</p> |

| アラート名                | 説明                                     | しきい値                  | アクション                                                                                                                                                                                                                                                                                                              |
|----------------------|----------------------------------------|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RDS-Storage-Capacity | DB インスタンスに割り当てられたストレージに 1GB 未満が残っています。 | ストレージは 99% が割り当てられます。 | <p>AMS 自動修復は、まず DB が変更可能で使用可能、またはストレージフル状態であることを検証します。次に、CloudFormation の変更セットを通じて、割り当てられたストレージ、IOPS、ストレージスループットの向上を試みます。スタックドリフトが既に検出されている場合、ダウンタイムを防ぐために RDS API にフォールバックします。</p> <p>この機能は、RDS DB インスタンスに次のタグを追加することでオプトアウトできます。<br/>"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".</p> |

| アラート名                               | 説明                                                                     | しきい値                                                   | アクション                                                                                                                                                                                                                            |
|-------------------------------------|------------------------------------------------------------------------|--------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AMSFSXONAPVolumeCapacityUtilization | Amazon FSx for NetApp ONTAP ボリュームが、デフォルトの割り当てストレージ (80%) よりも多く消費されました。 | FSx for ONTAP ボリューム容量使用率が 2 時間 (デフォルト値) で 80% を超えています。 | AMS 自動修復は、まずボリュームライフサイクルの状態が変更可能な状態であることを検証し、ファイルシステムの最大容量に対して検証しながらボリュームサイズを 10% 拡張します。ファイルシステムにボリューム拡張のための十分なストレージ容量がない場合、ボリュームとファイルシステムの両方が一緒に拡張されます。この拡張は、任意の 7 日間に最大 3 回に制限されます。AMS Automation が拡張する最大ストレージ制限は 5120 GiB です。 |

 **Note**

ボリュームの上に iSCSI LUN が設定されている場合は、オペレーティングシステムレベルで iSCSI LUN を展開します。詳細については、[FSx for ONTAP LUN が読み取り専用モードであるのはなぜで](#)

| アラート名 | 説明 | しきい値 | アクション                           |
|-------|----|------|---------------------------------|
|       |    |      | <a href="#">すか?</a> 」を参照してください。 |

## Amazon EC2 の壊れたセキュアチャネル: 修復の自動化に関する注意事項

AWS Managed Services (AMS) 自動修復が Amazon EC2 Windows 壊れたセキュアチャネルの問題に対して修復を実行する前に、自動化は次の事前チェックを実行し、さらに調査するためのインシデントレポートを作成します。

- Amazon EC2 インスタンスの SSM ステータスが「オンライン」であることを確認します。
- Amazon EC2 インスタンスが Auto Scaling グループの一部であるかどうか、および Auto Scaling グループ内のすべてのインスタンスに同じホスト名があるかどうかを検証します。
- Amazon EC2 インスタンスが、プロビジョニングに使用された CloudFormation スタックの一部かどうかを確認します。インスタンスが CloudFormation スタックから削除された場合、オートメーションは、関連付けられた Active Directory Organizational Unit (OU) がまだスタックを参照しているかどうかを検証します。

上記の検証に合格すると、自動化は Broken Secure チャネルの修正に進みます。

### 修復手順:

- 自動修復は、EC2 インスタンスと AD ドメイン間の安全なチャネルを修復し、インスタンスへのアクセスを復元しようとします。
- 修復後、オートメーションはセキュアチャネルが確立されていることを確認します。失敗した場合、AMS はインシデントを作成し、AMS オペレーションに調査を依頼します。

## EC2 ステータスチェックの失敗: 修復オートメーションに関する注意事項

EC2 ステータスチェックの失敗の問題に対する AMS 自動修復の仕組み:

- Amazon EC2 インスタンスにアクセスできなくなった場合は、インスタンスを停止して再度起動し、新しいハードウェアに移行して復旧できるようにする必要があります。
- 問題のルートが OS 内にある場合 (fstab のデバイスの欠落、カーネルの破損など)、オートメーションはインスタンスを復旧できません。

- インスタンスが Auto Scaling グループに属している場合、自動化はアクションを実行しません。AutoScalingGroup スケーリングアクションはインスタンスを置き換えます。
- インスタンスで EC2 Auto Recovery が有効になっている場合、修復はアクションを実行しません。

## EC2 ボリューム使用量修復の自動化

EC2 ボリュームの使用状況の問題に対する AWS Managed Services (AMS) 自動修復の仕組み:

- オートメーションはまず、ボリュームの拡張が必要かどうか、および実行できるかどうかを検証します。拡張が適切であると判断された場合、自動化によりボリューム容量が増加する可能性があります。この自動化されたプロセスは、制御された限定的な拡張で成長の必要性のバランスを取ります。
- ボリュームを拡張する前に、オートメーションはインスタンスでクリーンアップタスク (Windows: Disk Cleaner、Linux: Logrotate + Simple Service Manager エージェントログの削除) を実行して、領域を解放しようとします。

### Note

クリーンアップタスクは、継続的な機能のために CPU クレジットに依存するため、EC2 の「T」ファミリーインスタンスでは実行されません。

- Linux では、オートメーションは EXT2, EXT3, EXT4XFS タイプの拡張ファイルシステムのみをサポートします。
- Windows では、自動化は新しいテクノロジーファイルシステム (NTFS) とレジリエントファイルシステム (ReFS) のみをサポートします。
- 自動化は、Logical Volume Manager (LVM) または RAID アレイの一部であるボリュームを拡張しません。
- 自動化はインスタンスストアボリュームを拡張しません。
- 影響を受けるボリュームがすでに 2 TiB を超えている場合、オートメーションはアクションを実行しません。
- 自動化による拡張は、システムの存続期間中、週に最大 3 回、合計 5 回に制限されています。
- 前の拡張が過去 6 時間以内に発生した場合、オートメーションはボリュームを拡張しません。



これらのルールによってオートメーションがアクションを実行できない場合、AMS はアウトバウンドサービスリクエストを通じてお客様に連絡し、次に実行するアクションを決定します。

## Amazon RDS の低ストレージイベント修復の自動化

AWS Managed Services (AMS) 自動修復が Amazon RDS の低ストレージイベントの問題とどのように連携するか:

- Amazon RDS インスタンスストレージを拡張する前に、オートメーションはいくつかのチェックを実行して、Amazon RDS インスタンスが変更可能で使用可能、またはストレージフル状態であることを確認します。
- CloudFormation スタックドリフトが検出された場合、修復は Amazon RDS API を通じて行われます。
- トリガーイベントに応じて、修復によってプロパティ `MaxAllocatedStorage`、`AllocatedStorage`、`Iops`、または `StorageThroughput` が変更されます。他の Amazon RDS インスタンスのプロパティは変更されません。詳細については、[「DB インスタンスの設定」](#)を参照してください。
- 修復アクションは、次のシナリオでは実行されません。
  - Amazon RDS インスタンスのステータスが「使用可能」または「ストレージフル」ではありません。
  - Amazon RDS インスタンスストレージは現在変更できません (過去 6 時間以内にストレージが変更された場合など)。
  - Amazon RDS インスタンスでは、自動スケーリングストレージが有効になっています。
- 修復は 6 時間あたり 1 回の拡張に制限され、14 日間に 3 回まで拡張できます。
- これらのシナリオが発生すると、AMS はアウトバウンドインシデントでお客様に連絡し、次のアクションを決定します。

## ONTAP ボリューム容量修復の自動化

ONTAP ボリューム容量の問題に対する AWS Managed Services (AMS) 自動修復の仕組み:

- ボリュームを拡張する前に、オートメーションはボリュームのライフサイクル状態が変更可能な状態であることを確認します。
- 自動化により、ボリュームサイズが 10% 拡張され、ファイルシステムの最大容量に対して検証されます。

- ファイルシステムにボリューム拡張に対応するのに十分なストレージ容量がない場合、ボリュームとファイルシステム容量の両方が拡張されます。
- 修復は、7 日間に 3 回以下の更新に制限されます。
- AMS Automation が拡張する最大ストレージ制限は 5120 GiB です。
- ボリュームの上に iSCSI LUN が設定されている場合は、自動修復の完了後に OS レベルで iSCSI LUN を手動で拡張する必要があります。詳細については、[FSx for ONTAP LUN が読み取り専用モードであるのはなぜですか?](#)」を参照してください。

## AMS での追加の CloudWatch アラームの作成

AWS Managed Services (AMS) デプロイ | モニタリングと通知 | CloudWatch | アラーム変更タイプの作成を使用して、新しい CloudWatch アラームを作成できます。

### Important

AMS は、ユーザーが作成した CloudWatch アラームをモニタリングしません。

Amazon EC2 インスタンスのカスタム CloudWatch メトリクスとアラームの使用 (Auto Scaling グループにデプロイされた更新された AMLs に依存しない変更可能なデプロイでのみ動作します)。

1. アプリケーションモニタリングスクリプトとカスタムメトリクスを生成します。スクリプト例の詳細とアクセスについては、[Amazon EC2 Linux インスタンスのメモリとディスクのメトリクスのモニタリング](#)」を参照してください。Linux Amazon EC2 インスタンスの Amazon CloudWatch モニタリングスクリプトは、Amazon CloudWatch カスタムメトリクスを生成して使用方法を示しています。これらの Perl スクリプトのサンプルは、Linux インスタンスのメモリ、スワップ、およびディスクスペースの使用状況メトリクスをレポートする、完全に機能する例で構成されます。
2. モニタリングスクリプトをアップロードします。モニタリングスクリプトを Auto Scaling グループまたは Amazon EC2 インスタンス設定にアップロードするには、Auto Scaling グループまたは Amazon EC2 インスタンスを設定するときに UserData を使用できます。また、アプリケーションが CodeDeploy でデプロイされている場合は、デプロイ | アプリケーション | CodeDeploy アプリケーション | デプロイ CT (ct-2edc3sd1"rb) を使用して設定を変更できます。
3. カスタムメトリクスを CloudWatch にパブリッシュする (新しいカスタムメトリクスのデータポイントを初めてパブリッシュすると作成されます)。[「カスタムメトリクスのパブリッシュ」](#)を参照してください。

- CloudWatch アラームを作成します。[「インスタンスの CloudWatch アラームを作成する」](#)を参照してください。

**⚠ Important**

モニタリングデータは、このパス [infra/INSTANCE\_ID/YOUR\_CUSTOM\_METRIC] に送信する必要があります

CloudWatch アラームを変更または削除するには、「Amazon CloudWatch API リファレンス [PutMetricAlarm](#)」で説明されているように、管理 | その他 | その他 | 更新変更タイプ (ct-0xdawir96cy7k) を使用して RFC を送信します。

CloudWatch イベントストリームを使用できます。AMS は CloudWatch と統合されており、AWS API コールが CloudWatch イベントをトリガーするようにリクエストできます。

これを行うには、関心のある API コールを使用して、管理 | その他 | その他 | 更新 CT (ct-0xdawir96cy7k) を送信します。AMS オペレーターから要件を収集するための連絡があります。詳細については、[Amazon CloudWatch ドキュメント](#)を参照してください。

CloudWatch イベントストリームにアクセスするには、管理 | その他 | その他 | CT の更新 (ct-0xdawir96cy7k) を送信して、SNS 通知トピックにパーティを追加します。AMS オペレーターから要件を収集するための連絡があります。

## AMS でのカスタム CloudWatch メトリクスとアラームの作成

ビジネスメトリクスとアプリケーションメトリクスを Amazon CloudWatch に保存できます。CloudWatch が AWS Managed Services (AMS) リソース用に既に保存しているメトリクスと同様に、グラフを表示したり、これらのメトリクスに基づいてアラームを設定したりできます。CloudWatch の詳細については、[Amazon CloudWatch の概念](#)を参照してください。

Amazon SNS を使用すると、アプリケーションは、アラームが発行される AMS Managed Monitoring System または MMS、Amazon SNS (SNS) トピック、この場合は MMS、SQS キューに対して、「プッシュ」メカニズムを介して複数のサブスクライバーにタイムクリティカルなメッセージを送信できます。CloudWatch を使用してカスタムメトリクスを作成し、SNS トピックを通じて AMS アラームを適切に設定できます。これを実行するには、次の手順を実行します。

**Note**

このプロセスは、Auto Scaling グループにデプロイされた更新された AMIs に依存する変更不可能なデプロイでは機能せず、変更可能なアプリケーション (ASG ではなく) のデプロイに適しています。

AMS Advanced の制限内でカスタムメトリクスを設定するのは、複雑なタスクです。CloudWatch の例については、[「例: 用語の出現回数をカウントする」](#)を参照してください。

1. アプリケーションモニタリングスクリプトとカスタムメトリクス (カウント発生 の例など) を生成します。スクリプト例の詳細とアクセスについては、[Amazon EC2 Linux インスタンスのメモリとディスクのメトリクスのモニタリング](#)を参照してください。
2. モニタリングスクリプトをアップロードします。モニタリングスクリプトを Auto Scaling グループまたは Amazon EC2 インスタンス設定にアップロードするには、Auto Scaling グループまたは Amazon EC2 インスタンスを設定するときに UserData を使用できます。または、アプリケーションが CodeDeploy でデプロイされている場合は、デプロイ | アプリケーション | CodeDeploy アプリケーション | CT (ct-2edc3sd1"rb) を使用して設定を変更できます。
3. カスタムメトリクスを CloudWatch にパブリッシュする (新しいカスタムメトリクスのデータポイントを初めてパブリッシュすると作成されます)。[「カスタムメトリクスのパブリッシュ」](#)を参照してください。
4. カスタマーメトリクスをアプリケーションモニタリングシステムに統合するには、デプロイ | モニタリングと通知 | SNS | 変更タイプの作成 (ct-3dfnglm4ombbs) で RFC を送信して、メトリクスの SNS トピックの作成を AMS にリクエストします。
5. CloudWatch アラームを作成します。[Amazon CloudWatch アラームの作成](#)を参照してください。

**Important**

モニタリングデータは、このパス [infra/*INSTANCE\_ID*/*YOUR\_CUSTOM\_METRIC*] に送信する必要があります。

# AMS での .Net および SQL Server 用の CloudWatch Application Insights の使用

Amazon CloudWatch Application Insights を使用して、AWS Managed Services (AMS) アプリケーションリソースのモニターを設定し、アプリケーションの問題の兆候についてデータを継続的に分析し、アプリケーションの問題のトラブルシューティング時に平均修復時間 (MTTR) を短縮できます。CloudWatch Application Insights の詳細については、[CloudWatch Application Insights for .NET and SQL Server](#)」を参照してください。

## Important

AMS は CloudWatch Application Insights から問題をモニタリングしません。これらはユーザーが制御するアプリケーションコード用であるためです。

CloudWatch Application Insights を使用するには、デプロイ | 高度なスタックコンポーネント | Identity and Access Management (IAM) | エンティティまたはポリシー (マネージドオートメーション) 変更タイプ (ct-3dpg8mdd9jn1r) をリクエストとともに送信し、CloudWatch Application Insights を設定するアクセス許可を付与する IAM ロールを作成します。特定された問題を受信するには、SNS トピックを使用するか、CloudWatch イベントルールのターゲットを使用するかの 2 つのオプションがあります。RFC で、必要なものを指定します。CloudWatch Event ルールを使用する場合は、RFC でルール定義も指定します。CloudWatch Application Insights をセットアップすると、考えられる根本原因をポイントするインサイトなど、潜在的な問題の通知を受け取ります。

ロールを引き受ける方法については、「AMS オンボーディングガイド」の「[AMS IAM ロールを使用して Active Directory をフェデレーションする](#)」を参照してください。

## AMS での Amazon EventBridge マネージドルールの使用

AMS Advanced は Amazon EventBridge マネージドルールを使用します。マネージドルールは、AMS に直接リンクされた一意のタイプのルールです。これらのルールは受信イベントに一致し、処理のためにターゲットに送信します。マネージドルールは AMS によって事前定義されており、カスタマーアカウントを管理するためにサービスが必要とするイベントパターンが含まれています。特に定義されている場合を除き、所有サービスのみがこれらのマネージドルールを使用できます。

AMS マネージドルールは `events.managedservices.amazonaws.com` サービスプリンシパルにリンクされています。これらのマネージドルール

は、[AWSServiceRoleForManagedServices\\_Events](#)サービスにリンクされたロールを通じて管理されます。これらのルールを削除するには、顧客による特別な確認が必要です。詳細については、「[AMS のマネージドルールの削除](#)」を参照してください。

ルールの詳細については、「Amazon EventBridge ユーザーガイド」の「[ルール](#)」を参照してください。

## AMS によってデプロイされた Amazon EventBridge マネージドルール

### Amazon EventBridge マネージドルール

| ルール名                | 説明                                                                                                      | 定義                                                                                                             |
|---------------------|---------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| AMSAdvancedCoreRule | このルールは、Amazon CloudWatch アラームを AMS Monitoring に転送します。Amazon CloudWatch イベントは CloudWatch アラームをモニタリングします。 | <pre>{   {     "source": ["aws.cloudwatch"],     "detail-type": ["CloudWatch Alarm State Change"],   } }</pre> |

## AMS のマネージドルールの作成

Amazon EventBridge マネージドルールを手動で作成する必要はありません。AWS マネジメントコンソール、AWS CLIまたは AWS API で AMS にオンボードすると、AMS によって自動的に作成されます。

## AMS のマネージドルールの編集

AMS では、マネージドルールを編集することはできません。各マネージドルールの名前とイベントパターンは、AMS によって事前定義されています。



## AMS のマネージドールの削除

マネージドールを手動で削除する必要はありません。AWS マネジメントコンソール、または AWS API で AMS からオフボードすると、AMS はリソースをクリーンアップし AWS CLI、AMS が所有するすべてのマネージドールを削除します。

AMS がオフボーディング中にマネージドールを削除できない場合は、Amazon EventBridge コンソール、AWS CLI または AWS API を使用して、マネージドールを手動で削除することもできます。これを行うには、まず AMS からオフボードし、マネージドールの強制削除を実行する必要があります。

## AMS の信頼できる修復

Trusted Remediator は、[AWS Trusted Advisor](#)、[AWS Security Hub CSPM](#) および [レコメンデーション](#) [AWS Compute Optimizer](#) の修復を自動化する AWS Managed Services ソリューションです。Trusted Remediator は Trusted Advisor、Security Hub CSPM と Compute Optimizer がコストを削減し、システムの可用性を向上させ、パフォーマンスを最適化し、セキュリティギャップを埋める機会を示している場合にレコメンデーションを作成します AWS アカウント。Trusted Remediator を使用すると、確立されたベストプラクティスを使用する安全で標準化された方法で、これらのセキュリティ、パフォーマンス、コスト最適化、耐障害性、サービス制限の推奨事項に対処できます。Trusted Remediator を使用すると、修復ソリューションを設定し、作成したスケジュールで自動的に実行されるため、修復プロセスが簡素化されます。この合理化されたアプローチは、手動による介入なしで、一貫して効率的に問題に対処します。

## 信頼できる修復の主な利点

Trusted Remediator の主な利点は次のとおりです。

- セキュリティ、パフォーマンス、コストの最適化の向上: Trusted Remediator は、アカウントの全体的なセキュリティ体制の強化、リソース使用率の最適化、運用コストの削減に役立ちます。
- セルフサービスのセットアップと設定: 要件と設定に合わせて信頼できる修復を設定できます。
- 自動 Trusted Advisor チェック、Security Hub CSPM コントロール、[レコメンデーション](#) [AWS Compute Optimizer](#) コメンデーションの修正: 設定後、信頼された修復者は選択したチェックの修正アクションを自動的に実行します。この自動化により、手動による介入が不要になります。
- ベストプラクティスの実装: 修復アクションは確立されたベストプラクティスに基づいているため、問題は標準化された効果的な方法で対処されます。



- スケジュールされた実行: day-to-day運用ワークフローに沿った修復スケジュールを選択できます。

Trusted Remediator を使用すると、AWS 環境内で特定された問題に積極的に対処し、ベストプラクティスに従い、安全で高性能、費用対効果の高いクラウドインフラストラクチャを維持できます。

## Trusted Remediator の仕組み

以下は、信頼できる修復ワークフローの図です。

Trusted Remediator は Trusted Advisor、 の評価、Security Hub CSPM、Compute Optimizer の推奨事項 AWS アカウント を評価し、AWS Systems Manager OpsCenter で [OpsItems](#) を作成します。OpsCenter その後、信頼された修復の自動化ドキュメントを使用して、OpsItems を自動または手動で修復できます。以下は、各タイプの修復の詳細です。

- 自動修復: Trusted Remediator は自動化ドキュメントを実行し、実行をモニタリングします。自動化ドキュメントが完了すると、信頼された修復者は Opsitem を解決します。
- 手動修復: Trusted Remediator は、確認できるように OpsItem を作成します。確認したら、自動 RFC、[信頼された修復者 | 検出結果 | 修復](#)、変更タイプを作成してリソースを修復できます。手動修復手順の詳細については、「」を参照してください[信頼できる修復ツールで手動修復を実行する](#)。

修復ログは Amazon S3 バケットに保存されます。S3 バケット内のデータを使用して、レポート用のカスタムクイックダッシュボードを構築できます。AMS は、信頼できる修復業者のオンリクエストレポートも提供します。これらのレポートを受け取るには、CSDM にお問い合わせください。

## 信頼できる修復の主な用語

以下は、AMS で信頼された修復を使用するときに役立つ用語です。

- AWS Trusted Advisor、AWS Security Hub および AWS Compute Optimizer: が提供するクラウド最適化サービス AWS。Trusted Advisor、Security Hub CSPM、および Compute Optimizer は、AWS 環境を検査し、次の 6 つのカテゴリのベストプラクティスに基づいて推奨事項を提供します。
  - コスト最適化
  - パフォーマンス

- セキュリティ
- 耐障害性
- オペレーショナルエクセレンス
- サービス制限

詳細については、[AWS Trusted Advisor](#)「[セキュリティ](#)」、「[パフォーマンス](#)」、および[AWS Security Hub](#)「[セキュリティ](#)」を参照してください。[AWS Compute Optimizer](#)。

- Trusted Remediator: [Trusted Advisor](#)チェック、[AWS Security Hub CSPM](#)レコメンデーション、[レコメン](#)[AWS Compute Optimizer](#)レーションのための AMS 修復ソリューション。Trusted Remediator は、セキュリティ、パフォーマンスを向上させ、コストを削減するための既知のベストプラクティスを使用して、Trusted Advisor チェック、Security Hub CSPM コントロール、Compute Optimizer レコメンデーションを安全に修復するのに役立ちます。Trusted Remediator は簡単にセットアップおよび設定できます。を 1 回設定すると、Trusted Remediator は任意のスケジュール (毎日または毎週) で修復を実行します。
- AWS Systems Manager SSM ドキュメント: が AWS リソースに対して AWS Systems Manager 実行するアクションを定義する JSON または YAML ファイル。SSM ドキュメントは、複数の AWS リソースとインスタンスにわたる運用タスクを自動化するための宣言仕様として機能します。
- AWS Systems Manager OpsCenter OpsItem: 環境内の AWS 運用上の問題の追跡と解決に役立つクラウド運用上の問題管理リソース。OpsItems は、 および AWS のサービス リソース全体の運用データと問題の一元化されたビューと管理システムを提供します。各 OpsItem は、潜在的なセキュリティリスク、パフォーマンスの問題、運用インシデントなどの運用上の問題を表します。
- 設定: 設定は、 の一[AWS AppConfig機能である に保存されている属性のセットです AWS Systems Manager](#)。の信頼された修復アプリケーション AWS AppConfig は、アカウントレベルで修復を設定するのに役立ちます。
- 実行モード: 実行モードは、Compute Optimizer と Security Hub CSPM からの各 Trusted Advisor チェック結果と推奨事項に対して修復を実行する方法を決定する設定属性です。サポートされている実行モードは、自動、手動、条件付き、非アクティブの 4 つです。
- リソースの上書き: この機能は、リソースタグを使用して特定のリソースの設定を上書きします。
- 修復項目ログ: Trusted Remediator 修復 S3 ログバケットのログファイル。修復項目ログは、修復 OpsItems の作成時に作成されます。このログファイルには、手動実行修復 OpsItems と自動実行修復 OpsItems が含まれています。このログファイルを使用して、すべての修復項目を追跡します。
- 自動修復実行ログ: Trusted Remediator 修復 S3 ログバケットのログファイル。自動修復実行ログは、自動 SSM ドキュメント実行が完了すると作成されます。このログには、自動実行修復

OpsItems の SSM 実行の詳細が含まれています。このログファイルを使用して、自動修復を追跡します。

## AMS で信頼された修復の使用を開始する

Trusted Remediator は AMS で追加料金なしで利用できます。Trusted Remediator は、単一アカウントとマルチアカウントの設定をサポートしています。

### 信頼できる修復にオンボードする

AMS アカウントを信頼された修復者にオンボードするには、Cloud Architects または Cloud Service Delivery Manager (CSDMs) に E メールを送信します。E メールには、以下の情報を記載してください。

- AWS アカウント: 12 桁のアカウント識別番号。Trusted Remediator にオンボードするすべてのアカウントは、同じ AMS Advanced カスタマーに属している必要があります。
- 委任管理者アカウント: 単一または複数のアカウントの Trusted Advisor Compute Optimizer および Security Hub CSPM チェック設定に使用されるアカウント。
- メンバーアカウント: 委任管理者アカウントにリンクされたアカウントです。これらのアカウントは、委任管理者アカウントから設定を継承します。1 つのメンバーアカウントまたは複数のメンバーアカウントを持つことができます。

#### Note

メンバーアカウントは、委任管理者アカウントから設定を継承します。特定のアカウントに対して異なる設定が必要な場合は、複数の委任管理者アカウントを任意の設定でオンボードします。オンボーディングする前に、Cloud Architects でアカウント構造と設定を計画します。

- AWS リージョン: リソース AWS リージョン が配置されている。のリストについては AWS リージョン、[AWS のサービス「リージョン別」](#)を参照してください。
- 修復スケジュールと時刻: 希望する修復スケジュール (毎日または毎週)。Trusted Remediator は、スケジュールされた時刻に Trusted Advisor チェックを収集し、修復を開始します。たとえば、オーストラリア東部標準時の毎週日曜日の午前 1 時に修復スケジュールを設定できます。
- 通知 E メール: Trusted Remediator は、通知 E メールを使用して、修復があれば毎日通知します。通知 Eメールの件名は「信頼できる修復者修復の概要」で、内容は過去 24 時間以内に実行された信頼できる修復者修復に関する情報を提供します。

**Note**

スケジュールされた修復のたびに、アプリケーションとリソースを確認します。その他のサポートについては、AMS にお問い合わせください。

必要な詳細を含むオンボードリクエストを CA または CSDM に送信すると、AMS は信頼された修復者にアカウントをオンボードします。Trusted Remediator は AWS AppConfig、の一機能であるを使用して AWS Systems Manager、Trusted Advisor チェックの設定を定義します。これらの設定は、に保存されている一連の属性です AWS AppConfig。リソースへの不正請求を防ぐため、アカウントが信頼された修復者にオンボーディングされると、サポートされているすべての Trusted Advisor チェックは非アクティブに設定されます。これらの設定は、特定の Trusted Advisor チェックを自動的に修正したり、残りのチェックを評価および手動で修正したりするのに役立ちます。設定は高度にカスタマイズ可能で、Trusted Advisor チェックごとに設定を適用できます。詳細については、「[Trusted Remediator で Trusted Advisor チェック修復を設定する](#)」を参照してください。

## で信頼された修復を設定する AWS アカウント

オンボーディングが完了すると、CA または CDSM から通知され、委任された管理者にデフォルト設定が作成されます AWS アカウント。設定は、信頼された修復アプリケーションの AWS AppConfig に保存されます。RFC [管理 | 信頼できる修復者 | 修復設定 | 更新](#)を使用して設定の更新をリクエストできます。詳細については、「[Trusted Remediator で Trusted Advisor チェック修復を設定する](#)」を参照してください。

デフォルトの信頼された修復の設定を表示するには、次の手順を実行します。

1. <https://console.aws.amazon.com/systems-manager/> で AWS Systems Manager コンソールを開きます。

**Note**

委任管理者アカウントにいることを確認します。

2. アプリケーション管理、AppConfig を選択します。
3. アプリケーションのリストから信頼された修復を選択します。

信頼された修復の設定を示す AWS AppConfig コンソールの例を次に示します。

## 修復するチェックとレコメンデーションを選択する

デフォルトでは、修復実行モードは、設定内のすべての Trusted Advisor チェック、Compute Optimizer レコメンデーション、および Security Hub CSPM レコメンデーションに対して非アクティブです。これにより、不正な修復が防止され、リソースが保護されます。AMS は、Trusted Advisor チェック修復用に厳選された SSM 自動化ドキュメントを提供します。

Trusted Remediator で修復するチェックを選択するには、次の手順を実行します。

1. サポートされている [Trusted Advisor](#) のリスト、[Compute Optimizer のレコメンデーション](#)、[Security Hub CSPM のレコメンデーション](#)、および関連する SSM オートメーションドキュメントの名前を確認して、信頼できる修復方法で修復するチェックとレコメンデーションを決定します。
2. [管理を送信する | 信頼できる修復者 | 修復設定 | 選択したチェックの設定を更新するようにリクエストを更新します](#)。Trusted Advisor チェックを選択する方法については、「」を参照してください [Trusted Remediator で Trusted Advisor チェック修復を設定する](#)。

## Trusted Remediator で修復を追跡する

アカウントレベルの設定を更新すると、Trusted Remediator は修復ごとに OpsItems を作成します。Trusted Remediator は、修復スケジュールに従って OpsItems の自動修復のために SSM ドキュメントを実行します。Systems Manager OpsCenter コンソールからすべての修復 OpsItems を表示する方法については、「」を参照してください [Trusted Remediator で修復を追跡する](#)。OpsCenter

## 信頼できる修復ツールで手動修復を実行する

自動 RFC を使用して、手動で Trusted Advisor チェックを修復できます。手動修復を選択すると、信頼された修復者は手動実行 OpsItem を作成します。詳細については、「[信頼できる修復ツールで手動修復を実行する](#)」を参照してください。

## 信頼できる修復者がサポートする Compute Optimizer の推奨事項

次の表に、サポートされている Compute Optimizer の推奨事項、SSM オートメーションドキュメント、事前設定されたパラメータ、およびオートメーションドキュメントの期待される成果を示します。SSM オートメーションドキュメントをチェック修復を有効にする前に、期待される結果を確認して、ビジネス要件に基づいて考えられるリスクを理解するのに役立ちます。

修復を有効にするサポートされているチェックについて、Compute Optimizer の各チェックに対応する設定ルールが存在することを確認します。詳細については、[Trusted Advisor 「チェック AWS Compute Optimizer のオプトイン」](#)を参照してください。

| 最適化オプション                                    | SSM ドキュメント名と期待される成果                                                                                                                                                                                                                                        | サポートされている事前設定済みパラメータと制約                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 適切なサイズ設定                                    |                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                |
| <a href="#">Amazon EC2 インスタンスのレコメンデーション</a> | <p>AWSManagedServices-TrustedRemediatorResizeInstanceByComputeOptimizerRecommendation</p> <p>Compute Optimizer の推奨事項に従って Amazon EC2 インスタンスタイプが更新されました。オプションが存在する場合、最適なオプションは、同じプラットフォームパラメータ (アーキテクチャ、ハイパーバイザー、ネットワークインターフェイス、仮想化タイプなど) を維持しながら選択されます。</p> | <ul style="list-style-type: none"> <li>MinimumDaysSinceLastChange: 前回のインスタンスタイプ変更からの最小日数を指定するパラメータ。デフォルトは 7 日です。</li> </ul> <p>制約なし</p> <ul style="list-style-type: none"> <li>CreateAMIBeforeResize: サイズ変更前にインスタンス AMI をバックアップとして作成するには、を「true」に設定します。バックアップを作成しない場合は、を「false」に設定します。デフォルトは 'true' です。</li> </ul> <p>制約なし</p> |
| <a href="#">Amazon EBS ボリュームレコメンデーション</a>   | <p>AWSManagedServices-ModifyEBSVolume</p> <p>Amazon EBS ボリュームは、Compute Optimizer の推奨事項に従って変更されます。変更には、ボリュームタイプ、サイズ、IOPS、ボリューム生成 (gp2、gp3 など) が含まれる場合があります。</p>                                                                                             | <ul style="list-style-type: none"> <li>CreateSnapshot: ボリュームを変更する前にスナップショットを作成するには、を「true」に設定します。スナップショットを作成しない場合は、を「false」に設定します。デフォルトは「true」です。</li> </ul> <p>制約なし</p> <ul style="list-style-type: none"> <li>VolumeType: 目的のボリュームタイプ。タイプが指定されていない場合、既存のタイプは保持されます。</li> </ul>                                               |



| 最適化オプション | SSM ドキュメント名と期待される成果 | サポートされている事前設定済みパラメータと制約                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          |                     | <p>制約なし</p> <ul style="list-style-type: none"><li>• VolumeSize: ボリュームの希望するサイズ。GiB 単位。ターゲットボリュームサイズは、ボリュームの既存のサイズ以上である必要があります。サイズが指定されていない場合、既存のサイズは保持されます。</li></ul> <p>制約なし</p> <ul style="list-style-type: none"><li>• Iops: リクエストされた 1 秒あたりの I/O オペレーション数 (IOPS)。このパラメータは、io1、io2、および gp3 ボリュームでのみ有効です。</li></ul> <p>制約なし</p> <ul style="list-style-type: none"><li>• スループット: ボリュームにプロビジョニングするスループット。最大 1000 MiB/秒。このパラメータは gp3 ボリュームでのみ有効です。</li></ul> <p>制約なし</p> <ul style="list-style-type: none"><li>• RemediateStackDrift: ボリュームの変更によってドリフトが発生した場合にドリフト修復を開始するには、を「true」に設定します。ドリフト修復を試行しない場合は、を「false」に設定します。デフォルトは 'true' です。</li></ul> <p>制約なし</p> |



| 最適化オプション                            | SSM ドキュメント名と期待される成果                                                                                                        | サポートされている事前設定済みパラメータと制約                                              |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|
| <a href="#">Lambda 関数のレコメンデーション</a> | <p>AWSManagedServices-TrustedRemediatorOptimizeLambdaMemory</p> <p>AWS Lambda Compute Optimizer の推奨事項に従って最適化された 関数メモリ。</p> | <p>RecommendedMemorySize: 推奨オプションと異なる場合は、カスタムメモリサイズ。</p> <p>制約なし</p> |

## アイドル状態のリソース

|                                           |                                                                                            |                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------------|--------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">アイドル状態の Amazon EBS ボリューム</a>  | <p>AWSManagedServices-DeleteUnusedEBSVolume</p> <p>アタッチされていない Amazon EBS ボリュームは削除されます。</p> | <ul style="list-style-type: none"> <li>• CreateSnapshot: ボリュームを削除する前にスナップショットを作成するには、を「true」に設定します。スナップショットを作成しない場合は、を「false」に設定します。デフォルトは「true」です。</li> </ul> <p>制約なし</p> <ul style="list-style-type: none"> <li>• MinimumUnattachedDays: 最大 62 日間、削除する Amazon EBS ボリュームのアタッチされていない最小日数。デフォルトは 7 です。</li> </ul> <p>制約なし</p> |
| <a href="#">アイドル状態の Amazon EC2 インスタンス</a> | <p>AWSManagedServices-StopEC2Instance</p> <p>アイドル状態の Amazon EC2 インスタンスは停止します。</p>          | <p>ForceStopWithInstanceStore: インスタンスストアを使用してインスタンスを強制的に停止するには、を「true」に設定します。強制停止しない場合は、を「false」に設定します。デフォルト値の「false」は、インスタンスの停止を防ぎます。</p> <p>制約なし</p>                                                                                                                                                                       |

| 最適化オプション                                  | SSM ドキュメント名と期待される成果                                                                                                                                                                                                                                 | サポートされている事前設定済みパラメータと制約                  |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| <a href="#">アイドル状態の Amazon RDS インスタンス</a> | <p>AWSManagedServices-StopIdle RDSInstance</p> <p>アイドル状態の Amazon RDS インスタンスを停止します。サポートされているエンジンは、MariaDB、Microsoft SQL Server、MySQL、Oracle、PostgreSQL です。このドキュメントは、Aurora MySQL および Aurora PostgreSQL には適用されません。インスタンスは最大 7 日間停止され、自動的に再起動されます。</p> | <p>事前設定済みのパラメータは許可されません。</p> <p>制約なし</p> |

## Trusted Advisor Trusted Remediator でサポートされている チェック

次の表に、サポートされている Trusted Advisor チェック、SSM オートメーションドキュメント、事前設定されたパラメータ、およびオートメーションドキュメントの期待される結果を示します。SSM オートメーションドキュメントをチェック修復を有効にする前に、期待される結果を確認して、ビジネス要件に基づいて考えられるリスクを理解するのに役立ちます。

修復を有効にするサポートされている Trusted Advisor チェックについて、各チェックに対応する設定ルールが存在することを確認します。詳細については、[「View AWS Trusted Advisor checks powered by AWS Config」](#)を参照してください。チェックに対応する AWS Security Hub CSPM コントロールがある場合は、Security Hub CSPM コントロールが有効になっていることを確認します。詳細については、[「Security Hub CSPM でのコントロールの有効化」](#)を参照してください。事前設定済みパラメータの管理については、[「Trusted Remediator」の「Configure Trusted Advisor check remediation」](#)を参照してください。

## Trusted Advisor Trusted Remediator でサポートされているコスト最適化チェック

| ID と名前を確認する                                                              | SSM ドキュメント名と期待される成果                                                                                                   | サポートされている事前設定済みパラメータと制約                                                                                                                                                                                                                                                 |
|--------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Z4AUBRNSmz</a><br><br>関連付けられていない Elastic IP Address          | AWSManagedServices-TrustedRemediatorReleaseElasticIP<br><br>リソースに関連付けられていない Elastic IP アドレスを解放します。                    | 事前設定済みのパラメータは許可されません。<br><br>制約なし                                                                                                                                                                                                                                       |
| <a href="#">c18d2gz150</a> - Amazon EC2 インスタンスが停止しました                    | AWSManagedServices-TerminateEC2InstanceStoppedForPeriodOfTime - 日間停止された Amazon EC2 インスタンスは終了します。                      | <ul style="list-style-type: none"> <li>• CreateAMIBeforeTermination: Amazon EC2 インスタンスを終了する前にインスタンス AMI をバックアップとして作成するには、 を選択します true。終了する前にバックアップを作成しない場合は、 を選択します false。デフォルトは true です。</li> <li>• AllowedDays: インスタンスが終了するまでに停止状態にある日数。デフォルトは 30 です。</li> </ul> 制約なし |
| <a href="#">c18d2gz128</a><br><br>ライフサイクルポリシーが設定されていない Amazon ECR リポジトリ。 | AWSManagedServices-TrustedRemediatorPutECRLifecyclePolicy<br><br>ライフサイクルポリシーがまだ存在しない場合は、指定されたリポジトリのライフサイクルポリシーを作成します。 | ImageAgeLimit: Amazon ECR リポジトリ内の「任意の」イメージの最大有効期間 (1 ~ 365)。<br><br>制約なし                                                                                                                                                                                                |
| <a href="#">DAvU99Dc4C</a><br><br>利用頻度の低い Amazon EBS ボリューム               | AWSManagedServices-DeleteUnusedEBSVolume<br><br>ボリュームが過去 7 日間アタッチされていない場合、使用率の低い                                      | <ul style="list-style-type: none"> <li>• CreateSnapshot: に設定すると true、オートメーションは削除する前に Amazon EBS ボリュームのスナップショットを作成しま</li> </ul>                                                                                                                                          |

| ID と名前を確認する                                             | SSM ドキュメント名と期待される成果                                                                                                  | サポートされている事前設定済みパラメータと制約                                                                                                                                                                                                                                                                                            |
|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                         | Amazon EBS ボリュームを削除します。Amazon EBS スナップショットはデフォルトで作成されます。                                                             | <p>す。デフォルトの設定は true です。有効な値は true と false (大文字と小文字が区別されます) です。</p> <ul style="list-style-type: none"> <li>MinimumUnattachedDays: 削除する EBS ボリュームのアタッチされていない最小日数。最大 62 日間です。に設定すると 0、SSM ドキュメントはアタッチされていない期間をチェックせず、ボリュームが現在アタッチされていない場合はボリュームを削除します。デフォルト値は 7 です。</li> </ul> <p>制約なし</p>                            |
| <a href="#">hjLMh88uM8</a><br><br>アイドル状態の Load Balancer | AWSManagedServices-DeleteIdleClassicLoadBalancer<br><br>アイドル状態の Classic Load Balancer が未使用で、インスタンスが登録されていない場合は削除します。 | <p>IdleLoadBalancerDays: Classic Load Balancer がアイドル状態と見なす前に 0 個のリクエストされた接続がある日数。デフォルトは 7 日間です。</p> <p>自動実行が有効になっている場合、アクティブなバックエンドインスタンスがない場合、オートメーションはアイドル状態の Classic Load Balancer を削除します。アクティブなバックエンドインスタンスがあるが、正常なバックエンドインスタンスがないすべてのアイドル状態の Classic Load Balancer では、自動修復は使用されず、手動修復用の OpsItems が作成されます。</p> |

| ID と名前を確認する                                                         | SSM ドキュメント名と期待される成果                                                                                             | サポートされている事前設定済みパラメータと制約                                                                                                                                                        |
|---------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Ti39halfu8</a><br><br>Amazon RDS アイドル DB インスタンス         | AWSManagedServices-StopIdleRDSInstance<br><br>過去 7 日間アイドル状態であった Amazon RDS DB インスタンスは停止します。                     | 事前設定済みのパラメータは許可されません。<br><br>制約なし                                                                                                                                              |
| <a href="#">COr6dfpM05</a><br><br>AWS Lambda メモリサイズの過剰プロビジョニングされた関数 | AWSManagedServices-ResizeLambdaMemory<br><br>AWS Lambda 関数のメモリサイズは、 が提供する推奨メモリサイズに変更されます Trusted Advisor。       | RecommendedMemorySize: Lambda 関数に推奨されるメモリ割り当て。値の範囲は 128 ~ 10240 です。<br><br>自動化の実行前に Lambda 関数のサイズが変更された場合、この自動化によって推奨値で設定が上書きされる可能性があります Trusted Advisor。                      |
| <a href="#">Qch7DwouX1</a><br><br>低稼働率の Amazon EC2 インスタンス           | AWSManagedServices-StopEC2Instance (自動実行モードと手動実行モードの両方のデフォルト SSM ドキュメント)<br><br>使用率の低い Amazon EC2 インスタンスは停止します。 | ForceStopWithInstanceStore: インスタンスストアを使用してインスタンスを強制停止trueするには、 に設定します。それ以外の場合は、false に設定します。デフォルト値のは、インスタンスの停止falseを防ぎます。有効な値は true または false (大文字と小文字が区別されます) です。<br><br>制約なし |

| ID と名前を確認する                                                      | SSM ドキュメント名と期待される成果                                                                                                                                                                                                                       | サポートされている事前設定済みパラメータと制約                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><a href="#">Qch7DwouX1</a></p> <p>低稼働率の Amazon EC2 インスタンス</p> | <p>AWSManagedServices-ResizeInstanceByOneLevel</p> <p>Amazon EC2 インスタンスは、同じインスタンスファミリータイプで 1 つのインスタンスタイプダウンでサイズ変更されます。サイズ変更オペレーション中にインスタンスが停止および開始され、SSM ドキュメントの実行が完了した後、初期状態に戻ります。この自動化は、Auto Scaling グループ内のインスタンスのサイズ変更をサポートしていません。</p> | <ul style="list-style-type: none"> <li>• <b>MinimumDaysSinceLastChange:</b> 前回のインスタンスタイプ変更からの最小日数。インスタンスタイプが指定された時間内に変更された場合、インスタンスタイプは変更されません。を使用して、この検証をスキップします。デフォルトは 7 です。</li> <li>• <b>CreateAMIBeforeResize:</b> サイズ変更前にインスタンス AMI をバックアップとして作成するには、を選択します <code>true</code>。バックアップを作成しない場合は、を選択します <code>false</code>。デフォルトは <code>false</code> です。有効な値は <code>true</code> および <code>false</code> (大文字と小文字が区別されます) です。</li> <li>• <b>ResizeIfStopped:</b> インスタンスが停止状態であっても、インスタンスサイズの変更を続行するには、を選択します <code>true</code>。停止状態でインスタンスのサイズを自動的に変更しない場合は、を選択します <code>false</code>。有効な値は <code>true</code> と <code>false</code> (大文字と小文字が区別されます) です。</li> </ul> <p>制約なし</p> |

| ID と名前を確認する                                                             | SSM ドキュメント名と期待される成果                                                                                                                                    | サポートされている事前設定済みパラメータと制約                                                                                                                                                      |
|-------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Qch7DwouX1</a><br><br>低稼働率の Amazon EC2 インスタンス               | AWSManagedServices-TerminateInstance<br><br>使用率の低い Amazon EC2 インスタンスは、Auto Scaling グループの一部ではなく、終了保護が有効になっていない場合に終了します。AMI はデフォルトで作成されます。               | CreateAMIBeforeTermination: EC2 インスタンスを終了する前にバックアップとしてインスタンス AMI false を作成するには、このオプションを true または に設定します。デフォルトは true です。有効な値は true および false (大文字と小文字が区別されます) です。<br><br>制約なし |
| <a href="#">G31sQ1E9U</a><br><br>使用率の低い Amazon Redshift クラスター           | AWSManagedServices-PauseRedshiftCluster<br><br>Amazon Redshift クラスターは一時停止しています。                                                                        | 事前設定済みのパラメータは許可されません。<br><br>制約なし                                                                                                                                            |
| <a href="#">c1cj39rr6v</a><br><br>Amazon S3 で不完全なマルチパートアップロードを中止するための設定 | AWSManagedServices-TrustedRemediatorEnableS3AbortIncompleteMultipartUpload<br><br>Amazon S3 バケットには、特定の日が経過しても不完全なマルチパートアップロードを中止するライフサイクルルールが設定されています。 | DaysAfterInitiation: Amazon S3 が不完全なマルチパートアップロードを停止するまでの日数。デフォルトは 7 日間に設定されています。<br><br>制約なし                                                                                 |
| <a href="#">c1z7kmr00n</a><br><br>Amazon EC2 インスタンスのコスト最適化に関する推奨事項      | から Amazon EC2 インスタンスのレコメンデーションとアイドル状態の Amazon EC2 インスタンスを使用します <a href="#">信頼できる修復者がサポートする Compute Optimizer の推奨事項</a> 。                               | 事前設定済みのパラメータは許可されません。<br><br>制約なし                                                                                                                                            |



| ID と名前を確認する                                                       | SSM ドキュメント名と期待される成果                                                                                                    | サポートされている事前設定済みパラメータと制約           |
|-------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
| <a href="#">c1z7kmr02n</a><br>Amazon EBS ボリュームのコスト最適化に関する推奨事項     | から Amazon EBS ボリュームのレコメンデーションとアイドル状態の Amazon EBS ボリュームを使用します <a href="#">信頼できる修復者がサポートする Compute Optimizer の推奨事項</a> 。 | 事前設定済みのパラメータは許可されません。<br><br>制約なし |
| <a href="#">c1z7kmr03n</a><br>Amazon RDS DB インスタンスのコスト最適化に関する推奨事項 | からアイドル状態の Amazon RDS インスタンスを使用します <a href="#">信頼できる修復者がサポートする Compute Optimizer の推奨事項</a> 。                            | 事前設定済みのパラメータは許可されません。<br><br>制約なし |
| <a href="#">c1z7kmr05n</a><br>AWS Lambda 関数のコスト最適化に関する推奨事項        | から Lambda 関数のレコメンデーションを使用します <a href="#">信頼できる修復者がサポートする Compute Optimizer の推奨事項</a> 。                                 | 事前設定済みのパラメータは許可されません。<br><br>制約なし |

## Trusted Advisor Trusted Remediator でサポートされているセキュリティチェック

| ID と名前を確認する                              | SSM ドキュメント名と期待される成果                                                                            | サポートされている事前設定済みパラメータと制約                                              |
|------------------------------------------|------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|
| <a href="#">12Fnkpl8Y5</a><br>露出したアクセスキー | AWSManagedServices-TrusteRemediatorDeactivateIAMAccessKey<br><br>公開された IAM アクセスキーは非アクティブ化されます。 | 事前設定済みのパラメータは許可されません。<br><br>公開された IAM アクセスキーで設定されたアプリケーションは認証できません。 |

| ID と名前を確認する                                                                                                                                             | SSM ドキュメント名と期待される成果                                                                                                      | サポートされている事前設定済みパラメータと制約                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Hs4Ma3G127</p> <p>- API Gateway REST および WebSocket API 実行ログを有効にする必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">APIGateway.1</a></p>    | <p>AWSManagedServices-TrustedR<br/>emediatorEnableAPIGateWayEx<br/>ecutionLogging</p> <p>実行ログ記録は API ステージで有効になっています。</p> | <p>LogLevel: 実行ログ記録を有効にするログ記録レベル ERROR - ログ記録はエラーに対してのみ有効になります。INFO- ログ記録はすべてのイベントで有効になっています。</p> <p>実行ログを有効にするには、アカウントの CloudWatch にログを読み書きするアクセス許可を API Gateway に付与する必要があります。詳細については、<a href="#">「API Gateway で REST API の CloudWatch ログ記録を設定する APIs」</a>を参照してください。</p> |
| <p>Hs4Ma3G129</p> <p>- API Gateway REST API ステージでは AWS X-Ray トレースを有効にする必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">APIGateway.3</a></p> | <p>AWSManagedServices-EnableAp<br/>iGateWayXRayTracing</p> <p>X-Ray トレースは API ステージで有効になっています。</p>                        | <p>事前設定済みのパラメータは許可されません。</p> <p>制約なし</p>                                                                                                                                                                                                                                  |

| ID と名前を確認する                                                                                                                                            | SSM ドキュメント名と期待される成果                                                                                                                                              | サポートされている事前設定済みパラメータと制約                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Hs4Ma3G202 - API Gateway REST API キャッシュデータは保管時に暗号化する必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">APIGateway.5</a></p>                | <p>AWSManagedServices-EnableAPIGatewayCacheEncryption</p> <p>API Gateway REST API ステージでキャッシュが有効になっている場合、API Gateway REST API キャッシュデータの保管時の暗号化を有効にします。</p>        | <p>事前設定済みのパラメータは許可されません。</p> <p>制約なし</p>                                                                                                                                                                                                                                                                                                                               |
| <p>Hs4Ma3G177 -</p> <p>対応する AWS Security Hub CSPM チェック - ロードバランサーに関連付けられた Auto Scaling グループは、ロードバランサーのヘルスチェック</p> <p><a href="#">AutoScaling.1</a></p> | <p>AWSManagedServices-TrustedR<br/>emediatorEnableAutoScalingG<br/>roupELBHealthCheck</p> <p>Auto Scaling グループに対して Elastic Load Balancing ヘルスチェックが有効になっています。</p> | <p>HealthCheckGracePeriod: サービスを開始した Amazon Elastic Compute Cloud インスタンスのヘルスステータスをチェックするまでに Auto Scaling が待機する秒単位の時間。</p> <p>Elastic Load Balancing ヘルスチェックをオンにすると、Auto Scaling グループにアタッチされた Elastic Load Balancing ロードバランサーのいずれかが異常と報告した場合、実行中のインスタンスが置き換えられる可能性があります。詳細については、<a href="#">Elastic Load Balancing ロードバランサーを Auto Scaling グループにアタッチする</a>を参照してください。</p> |

| ID と名前を確認する                                                                                                                                                                                                               | SSM ドキュメント名と期待される成果                                                                                                                                                  | サポートされている事前設定済みパラメータと制約                                                                                                                                                                                |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p data-bbox="115 275 347 638">Hs4Ma3G245 - CloudFormation スタックは Amazon Simple Notification Service と統合する必要があります</p> <p data-bbox="115 684 324 911">対応する AWS Security Hub CSPM チェック: <a href="#">CloudFormation.1</a></p> | <p data-bbox="399 275 881 352">AWSManagedServices-EnableCFNStackNotification</p> <p data-bbox="399 399 922 531">CloudFormation スタックを通知用の Amazon SNS トピックに関連付けます。</p> | <p data-bbox="974 275 1495 401">NotificationARNs 選択した CloudFormation スタックに関連付ける Amazon SNS トピックの ARNs。</p> <p data-bbox="974 447 1490 623">自動修復を有効にするには、NotificationARNs 事前設定されたパラメータを指定する必要があります。</p> |

| ID と名前を確認する                                                                                                                           | SSM ドキュメント名と期待される成果                                                                                                 | サポートされている事前設定済みパラメータと制約                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Hs4Ma3G210 - CloudFront デイストリビューションではログ記録が有効になっている必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">CloudFront.2</a></p> | <p>AWSManagedServices-EnableCloudFrontDistributionLogging</p> <p>ログ記録は Amazon CloudFront デイストリビューションで有効になっています。</p> | <ul style="list-style-type: none"><li>• BucketName: アクセスログを保存する Amazon S3 バケットの名前。</li><li>• S3KeyPrefix: theAmazonCloudFront デイストリビューションログの S3 バケット内の場所のプレフィックス。</li><li>• IncludeCookies: アクセスログに Cookie を含めるかどうかを示します。</li></ul> <p>自動修復を有効にするには、以下の事前設定済みパラメータを指定する必要があります。</p> <ul style="list-style-type: none"><li>• BucketName</li><li>• S3KeyPrefix</li><li>• IncludeCookies</li></ul> <p>この修復の制約については、<a href="#">CloudFront デイストリビューションのログ記録を有効にするにはどうすればよいですか？</a>を参照してください。</p> |

| ID と名前を確認する                                                                                                                                 | SSM ドキュメント名と期待される成果                                                                                            | サポートされている事前設定済みパラメータと制約                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Hs4Ma3G109 - CloudTrail ログファイルの検証を有効にする必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">CloudTrail.4</a></p>                  | <p>AWSManagedServices-TrustedRolemediatorEnableCloudTrailLogValidation</p> <p>CloudTrail 証跡ログの検証を有効にします。</p>   | <p>事前設定済みのパラメータは許可されません。</p> <p>制約なし</p>                                                                                                                                                                                                                                                                                                                                                                                                    |
| <p>Hs4Ma3G108 - CloudTrail 証跡は Amazon CloudWatch Logs と統合する必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">CloudTrail.5</a></p> | <p>AWSManagedServices-IntegrateCloudTrailWithCloudWatch</p> <p>AWS CloudTrail は CloudWatch Logs と統合されています。</p> | <ul style="list-style-type: none"> <li>CloudWatchLogsLogGroupName: CloudTrail ログが配信される CloudWatch Logs ロググループの名前。アカウントにあるロググループを使用する必要があります。</li> <li>CloudWatchLogsRoleName: ユーザーのロググループに書き込むために引き受ける CloudWatch Logs エンドポイントの IAM ロールの名前。アカウントにあるロールを使用する必要があります。</li> </ul> <p>自動修復を有効にするには、以下の事前設定済みパラメータを指定する必要があります。</p> <ul style="list-style-type: none"> <li>CloudWatchLogsLogGroupName</li> <li>CloudWatchLogsRoleName</li> </ul> |

| ID と名前を確認する                                                                                                                            | SSM ドキュメント名と期待される成果                                                                                                                            | サポートされている事前設定済みパラメータと制約                  |
|----------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| <p>Hs4Ma3G217 - CodeBuild プロジェクト環境にはログ記録 AWS 設定が必要です</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">CodeBuild.4</a></p>           | <p>AWSManagedServices-TrustedRolemediatorEnableCodeBuildLoggingConfig</p> <p>CodeBuild プロジェクトのログ記録を有効にします。</p>                                 | <p>事前設定済みのパラメータは許可されません。</p> <p>制約なし</p> |
| <p>Hs4Ma3G306 - Neptune DB クラスターでは削除保護を有効にする必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">DocumentDB.3</a></p>           | <p>AWSManagedServices-TrustedRolemediatorDisablePublicAccessOnDocumentDBSnapshot</p> <p>Amazon DocumentDB 手動クラスターナップショットからパブリックアクセスを削除します。</p> | <p>事前設定済みのパラメータは許可されません。</p> <p>制約なし</p> |
| <p>Hs4Ma3G308 - Amazon DocumentDB クラスターでは削除保護が有効になっている必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">DocumentDB.5</a></p> | <p>AWSManagedServices-TrustedRolemediatorEnableDocumentDBClusterDeletionProtection</p> <p>Amazon DocumentDB クラスターの削除保護を有効にします。</p>             | <p>事前設定済みのパラメータは許可されません。</p> <p>制約なし</p> |



| ID と名前を確認する                                                                                                                                      | SSM ドキュメント名と期待される成果                                                                                                              | サポートされている事前設定済みパラメータと制約                  |
|--------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| <p>Hs4Ma3G323 - DynamoDB テーブルでは削除保護を有効にする必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">DynamoDB.6</a></p>                          | <p>AWSManagedServices-TrustedR<br/>emediatorEnableDynamoDBTableDeletionProtection</p> <p>AMS 以外の DynamoDB テーブルの削除保護を有効にします。</p>  | <p>事前設定済みのパラメータは許可されません。</p> <p>制約なし</p> |
| <p><a href="#">ePs02jT06w</a> - Amazon EBS パブリックスナップショット</p>                                                                                     | <p>AWSManagedServices-TrustedR<br/>emediatorDisablePublicAccessOnEBSSnapshot</p> <p>Amazon EBS スナップショットのパブリックアクセスは無効になっています。</p> | <p>事前設定済みのパラメータは許可されません。</p> <p>制約なし</p> |
| <p>Hs4Ma3G118 - VPC のデフォルトのセキュリティグループは、インバウンドトラフィックまたはアウトバウンドトラフィックを許可しないでください</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">EC2.2</a></p> | <p>AWSManagedServices-TrustedR<br/>emediatorRemoveAllRulesFromDefaultSG</p> <p>デフォルトのセキュリティグループ内のすべての進入ルールと退出ルールが削除されます。</p>     | <p>事前設定済みのパラメータは許可されません。</p> <p>制約なし</p> |

| ID と名前を確認する                                                                                                             | SSM ドキュメント名と期待される成果                                                                                                          | サポートされている事前設定済みパラメータと制約                                                                                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Hs4Ma3G117 - アタッチされた EBS ボリュームは保管時に暗号化する必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">EC2.3</a></p>    | <p>AWSManagedServices-EncryptInstanceVolume</p> <p>インスタンスにアタッチされた Amazon EBS ボリュームは暗号化されます。</p>                              | <ul style="list-style-type: none"><li>• ボリュームを暗号化する<br/>KMSKeyId: AWS KMS key ID または ARN。</li><li>• DeleteStaleNonEncryptedSnapshotBackups: 暗号化されていない古いボリュームのスナップショットバックアップを削除するかどうかを決定するフラグ。</li></ul> <p>インスタンスは修復の一部として再起動され、DeleteStaleNonEncryptedSnapshotBackups が復元falseに役立つ に設定されている場合はロールバックが可能です。</p> |
| <p>Hs4Ma3G120 - 停止した EC2 インスタンスは、指定された期間後に削除する必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">EC2.4</a></p> | <p>AWSManagedServices-TerminateInstance (自動実行モードと手動実行モードの両方のデフォルトの SSM ドキュメント)</p> <p>30 日間停止した Amazon EC2 インスタンスは終了します。</p> | <p>CreateAMIBeforeTermination:。EC2 インスタンスを終了する前にインスタンス AMI をバックアップとして作成するには、 を選択しますtrue。終了する前にバックアップを作成しない場合は、 を選択しますfalse。デフォルトは true です。</p> <p>制約なし</p>                                                                                                                                                      |

| ID と名前を確認する                                                                                                             | SSM ドキュメント名と期待される成果                                                                                                                        | サポートされている事前設定済みパラメータと制約                                                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Hs4Ma3G120 - 停止した EC2 インスタンスは、指定された期間後に削除する必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">EC2.4</a></p> | <p>AWSManagedServices-TerminateEC2InstanceStoppedForPeriodOfTime - Security Hub で定義された日数の間停止された Amazon EC2 インスタンス (デフォルト値は 30) は終了します。</p> | <p>CreateAMIBeforeTermination: EC2 インスタンスを終了する前にインスタンス AMI をバックアップとして作成するには、 <code>を</code> 選択します <code>true</code>。終了する前にバックアップを作成しない場合は、 <code>を</code> 選択します <code>false</code>。デフォルトは <code>true</code> です。</p> <p>制約なし</p> |
| <p>Hs4Ma3G121 - EBS のデフォルトの暗号化を有効にする必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">EC2.7</a></p>           | <p>AWSManagedServices-EncryptEBSByDefault</p> <p>特定の <code>に対して</code> Amazon EBS 暗号化がデフォルトで有効になっている AWS リージョン</p>                         | <p>事前設定済みのパラメータは許可されません。</p> <p>デフォルトでの暗号化はリージョン固有の設定です。リージョンに対して有効にした場合、そのリージョンの個々のボリュームまたはスナップショットに対して無効にすることはできません。</p>                                                                                                      |

| ID と名前を確認する                                                                                                                                             | SSM ドキュメント名と期待される成果                                                                                                                  | サポートされている事前設定済みパラメータと制約                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Hs4Ma3G124</p> <p>- Amazon EC2 インスタンスはインスタンスメタデータサービスバージョン 2 (IMDSv2) を使用する必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">EC2.8</a></p> | <p>AWSManagedServices-TrustedRemediatorEnableEC2InstanceIMDSv2</p> <p>Amazon EC2 インスタンスは、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用します。</p> | <ul style="list-style-type: none"> <li>• IMDSv1MetricCheckPeriod: CloudWatch で IMDSv1 使用状況メトリクスを分析する日数 (42-455)。Amazon EC2 インスタンスが指定された期間内に作成された場合、分析はインスタンスの作成日から開始されます。</li> <li>• HttpPutResponseHopLimit: インスタンスメタデータトークンに許可されるネットワークホップの最大数。この値は、1 と 2 ホップの間で設定できます。のホップ制限は、インスタンスで直接実行されるプロセスへのトークンアクセス1を制限し、のホップ制限は、インスタンスで実行されているコンテナからのアクセス2を許可します。</li> </ul> <p>制約なし</p> |
| <p>Hs4Ma3G207 - EC2 サブネットはパブリック IP アドレスを自動的に割り当てないでください</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">EC2.15</a></p>                              | <p>AWSManagedServices-UpdateAutoAssignPublicIpv4Addresses</p> <p>VPC サブネットは、パブリック IP アドレスを自動的に割り当てないように設定されています。</p>                 | <p>事前設定済みのパラメータは許可されません。</p> <p>制約なし</p>                                                                                                                                                                                                                                                                                                                                            |

| ID と名前を確認する                                                                                                               | SSM ドキュメント名と期待される成果                                                         | サポートされている事前設定済みパラメータと制約                  |
|---------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|------------------------------------------|
| <p>Hs4Ma3G209 - 未使用のネットワークアクセスコントロールリストが削除されました</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">EC2.16</a></p>        | <p>AWSManagedServices-DeleteUnusedNACL</p> <p>未使用のネットワーク ACL を削除する</p>      | <p>事前設定済みのパラメータは許可されません。</p> <p>制約なし</p> |
| <p>Hs4Ma3G215 - 未使用の Amazon EC2 セキュリティグループを削除する必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">EC2.22</a></p> | <p>AWSManagedServices-DeleteSecurityGroups</p> <p>未使用のセキュリティグループを削除します。</p> | <p>事前設定済みのパラメータは許可されません。</p> <p>制約なし</p> |

| ID と名前を確認する                                                                                                                                      | SSM ドキュメント名と期待される成果                                                                                                                                  | サポートされている事前設定済みパラメータと制約                  |
|--------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| <p>Hs4Ma3G247 - Amazon EC2 Transit Gateway は VPC アタッチメントリクエストを自動的に受け入れないでください</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">EC2.23</a></p> | <p>AWSManagedServices-TrustedR<br/>emediatorDisableTGWAutoVPCAt<br/>tach - 指定された非 AMS Amazon EC2 Transit Gateway の VPC アタッチメントリクエストの自動承認を無効にします。</p> | <p>事前設定済みのパラメータは許可されません。</p> <p>制約なし</p> |
| <p>Hs4Ma3G235 - ECR プライベートルリポジトリにはタグのイミュータビリティを設定する必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">ECR.2</a></p>                     | <p>AWSManagedServices-TrustedR<br/>emediatorSetImageTagImmutability</p> <p>指定されたりポジトリのイメージタグのミュータビリティ設定を IMMUTABLE に設定します。</p>                       | <p>事前設定済みのパラメータは許可されません。</p> <p>制約なし</p> |

| ID と名前を確認する                                                                                                                     | SSM ドキュメント名と期待される成果                                                                               | サポートされている事前設定済みパラメータと制約                                                                                                               |
|---------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| <p>Hs4Ma3G216 - ECR リポジトリには、少なくとも 1 つのライフサイクルポリシーを設定する必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">ECR.3</a></p> | <p>AWSManagedServices-PutECRRepositoryLifecyclePolicy</p> <p>ECR リポジトリにはライフサイクルポリシーが設定されています。</p> | <p>LifecyclePolicyText: リポジトリに適用する JSON リポジトリポリシーテキスト。</p> <p>自動修復を有効にするには、以下の事前設定済みパラメータを指定する必要があります。</p> <p>LifecyclePolicyText</p> |
| <p>Hs4Ma3G325 - EKS クラスターでは監査ログ記録が有効になっている必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">EKS.8</a></p>             | <p>AWSManagedServices-TrustedRemediatorEnableEKSAuditLog</p> <p>監査ログは EKS クラスターで有効になっています。</p>    | <p>事前設定済みのパラメータは許可されません。</p> <p>制約なし</p>                                                                                              |



| ID と名前を確認する                                                                                                                                            | SSM ドキュメント名と期待される成果                                                                                                                                        | サポートされている事前設定済みパラメータと制約                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Hs4Ma3G183 - Application Load Balancer は HTTP ヘッダーを削除するように設定する必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">ELB.4</a></p>             | <p>AWSConfigRemediation-DropInvalidHeadersForALB</p> <p>Application Load Balancer は、無効なヘッダーフィールドに設定されています。</p>                                             | <p>事前設定済みのパラメータは許可されません。</p> <p>制約なし</p>                                                                                                                                                                                                                                                                                                                                                                                         |
| <p>Hs4Ma3G184 - Application Load Balancer と Classic Load Balancer のログ記録を有効にする必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">ELB.5</a></p> | <p>AWSManagedServices-EnableELBLogging (自動実行モードと手動実行モードの両方のデフォルト SSM ドキュメント)</p> <p>Application Load Balancer と Classic Load Balancer のログ記録が有効になっています。</p> | <ul style="list-style-type: none"><li>• BucketName: バケット名 (ARN ではありません)。バケットポリシーがログ記録用に正しく設定されていることを確認します。</li><li>• S3KeyPrefix: Elastic Load Balancing ログの Amazon S3 バケット内の場所のプレフィックス。</li></ul> <p>自動修復を有効にするには、以下の事前設定済みパラメータを指定する必要があります。</p> <ul style="list-style-type: none"><li>• BucketName</li><li>• S3KeyPrefix</li></ul> <p>Amazon S3 バケットには、バケットにアクセスログを書き込むアクセス許可を Elastic Load Balancing に付与するバケットポリシーが必要です。</p> |

| ID と名前を確認する                                                                                                                                                 | SSM ドキュメント名と期待される成果                                                                                                    | サポートされている事前設定済みパラメータと制約                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Hs4Ma3G18<br/>4 - Application Load Balancer と Classic Load Balancer のログ記録を有効にする必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">ELB.5</a></p> | <p>AWSManagedServices-EnableELBLoggingV2</p> <p>Application Load Balancer と Classic Load Balancer のログ記録が有効になっています。</p> | <ul style="list-style-type: none"><li>• TargetBucketTagKey: ターゲット Amazon S3 バケットを識別するために使用されるタグ名 (大文字と小文字を区別)。これを使用してTargetBucketTagValue、アクセスログ記録の送信先バケットとして機能するバケットにタグを付けます。</li><li>• TargetBucketTagValue: ターゲット Amazon S3 バケットを識別するために使用されるタグ値 (大文字と小文字を区別)。これを使用してTargetBucketTagKey、アクセスログ記録の送信先バケットとして機能するバケットにタグを付けます。</li><li>• S3BucketPrefix: Amazon S3 バケットのプレフィックス (論理階層)。指定するプレフィックスに文字列 AWSLogs を含めることはできません。詳細については、「<a href="#">プレフィックスを使用してオブジェクトを整理する</a>」を参照してください。</li></ul> <p>自動修復を有効にするには、以下の事前設定済みパラメータを指定する必要があります。</p> <ul style="list-style-type: none"><li>• TargetBucketTagKey</li><li>• TargetBucketTagValue</li><li>• S3BucketPrefix</li></ul> |

| ID と名前を確認する                                                                                                               | SSM ドキュメント名と期待される成果                                                                                                                     | サポートされている事前設定済みパラメータと制約                                                             |
|---------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
|                                                                                                                           |                                                                                                                                         | Amazon S3 バケットには、バケットにアクセスログを書き込むアクセス許可を Elastic Load Balancing に付与するバケットポリシーが必要です。 |
| <p>Hs4Ma3G326 - Amazon EMR パブリックアクセスブロック設定を有効にする必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">EMR.2</a></p> | <p>AWSManagedServices-TrustedR<br/>emediatorEnableEMRBlockPubl<br/>icAccess</p> <p>Amazon EMR ブロックのパブリックアクセス設定は、アカウントに対して有効になっています。</p> | <p>事前設定済みのパラメータは許可されません。</p> <p>制約なし</p>                                            |
| <p>Hs4Ma3G135 - AWS KMS キーを意図せずに削除しないでください</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">KMS.3</a></p>              | <p>AWSManagedServices-CancelKe<br/>yDeletion</p> <p>AWS KMS キーの削除はキャンセルされます。</p>                                                        | <p>事前設定済みのパラメータは許可されません。</p> <p>制約なし</p>                                            |

| ID と名前を確認する                                                                                                                               | SSM ドキュメント名と期待される成果                                                                                                               | サポートされている事前設定済みパラメータと制約                  |
|-------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| <p>Hs4Ma3G299 - Amazon DocumentDB 手動クラスターアップショットは公開しないでください</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">Neptune.4</a></p>         | <p>AWSManagedServices-TrustedR<br/>emediatorEnableNeptuneDBClusterDeletionProtection</p> <p>Amazon Neptune クラスターの削除保護を有効にします。</p> | <p>事前設定済みのパラメータは許可されません。</p> <p>制約なし</p> |
| <p>Hs4Ma3G319 - Network Firewall ファイアウォールで削除保護を有効にする必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">NetworkFirewall.9</a></p> | <p>AWSManagedServices-TrustedR<br/>emediatorEnableNetworkFirewallDeletionProtection - AWS Network Firewall の削除保護を有効にします。</p>      | <p>事前設定済みのパラメータは許可されません。</p> <p>制約なし</p> |

| ID と名前を確認する                                                                                                                                      | SSM ドキュメント名と期待される成果                                                                                | サポートされている事前設定済みパラメータと制約                                                                                                                                                                                                                                                           |
|--------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Hs4Ma3G223 - OpenSearch ドメインはノード間で送信されるデータを暗号化する必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">OpenSearch.3</a></p>              | <p>AWSManagedServices-EnableOpenSearchNodeToNodeEncryption</p> <p>ノード間の暗号化は、ドメインに対して有効になっています。</p> | <p>事前設定済みのパラメータは許可されません。</p> <p>node-to-node暗号化を有効にすると、設定を無効にすることはできません。代わりに、暗号化されたドメインの手動スナップショットを作成し、別のドメインを作成し、データを移行してから、古いドメインを削除します。</p>                                                                                                                                    |
| <p>Hs4Ma3G222 - CloudWatch Logs への OpenSearch ドメインエラーのログ記録を有効にする必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">Opensearch.4</a></p> | <p>AWSManagedServices-EnableOpenSearchLogging</p> <p>OpenSearch ドメインでエラーログ記録が有効になっています。</p>        | <p>CloudWatchLogGroupArn: anAmazon CloudWatch Logs ロググループの ARN。</p> <p>自動修復を有効にするには、CloudWatchLogGroupArn という事前設定済みのパラメータを指定する必要があります。</p> <p>Amazon CloudWatch リソースポリシーは、アクセス許可で設定する必要があります。詳細については、「Amazon OpenSearch Service ユーザーガイド」の「<a href="#">監査ログの有効化</a>」を参照してください。</p> |

| ID と名前を確認する                                                                                                                             | SSM ドキュメント名と期待される成果                                                                                                                                   | サポートされている事前設定済みパラメータと制約                                                                                                                                                                                                                                                     |
|-----------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Hs4Ma3G221 - OpenSearch ドメインでは監査ログ記録が有効になっている必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">Opensearch.5</a></p>        | <p>AWSManagedServices-EnableOpenSearchLogging</p> <p>OpenSearch ドメインは、監査ログ記録が有効に設定されています。</p>                                                         | <p>CloudWatchLogGroupArn: ログを発行する CloudWatch Logs グループの ARN。</p> <p>自動修復を有効にするには、次の事前設定済みパラメータを指定する必要があります。CloudWatchLogGroupArn</p> <p>Amazon CloudWatch リソースポリシーは、アクセス許可で設定する必要があります。詳細については、「Amazon OpenSearch Service ユーザーガイド」の「<a href="#">監査ログの有効化</a>」を参照してください。</p> |
| <p>Hs4Ma3G220 - OpenSearch ドメインへの接続は TLS 1.2 を使用して暗号化する必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">Opensearch.8</a></p> | <p>AWSManagedServices-EnableOpenSearchEndpointEncryptionTLS1.2</p> <p>TLS ポリシーはPolicy-Min-TLS-1-2-2019-07」に設定され、HTTPS (TLS) 経由の暗号化された接続のみが許可されます。</p> | <p>事前設定済みのパラメータは許可されません。</p> <p>TLS 1.2 を使用するには、OpenSearch ドメインへの接続が必要です。転送中のデータの暗号化は、パフォーマンスに影響する可能性があります。この機能を使用してアプリケーションをテストし、パフォーマンスプロファイルと TLS の影響を理解します。</p>                                                                                                         |

| ID と名前を確認する                                                                                                                                              | SSM ドキュメント名と期待される成果                                                                                                 | サポートされている事前設定済みパラメータと制約                  |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| <p>Hs4Ma3G194 - Amazon RDS スナップショットはプライベートである必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">RDS.1</a></p>                                   | <p>AWSManagedServices-DisablePublicAccessOnRDSSnapshotV2</p> <p>Amazon RDS スナップショットのパブリックアクセスは無効になっています。</p>        | <p>事前設定済みのパラメータは許可されません。</p> <p>制約なし</p> |
| <p>Hs4Ma3G192 - RDS DB インスタンスは、PubliclyAccessible AWS 設定によって決定されるパブリックアクセスを禁止する必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">RDS.2</a></p> | <p>AWSManagedServices-TrustedRemediatorDisablePublicAccessOnRDSInstance</p> <p>RDS DB インスタンスでのパブリックアクセスを無効にします。</p> | <p>事前設定済みのパラメータは許可されません。</p> <p>制約なし</p> |



| ID と名前を確認する                                                                                                                                                  | SSM ドキュメント名と期待される成果                                                                                                         | サポートされている事前設定済みパラメータと制約                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Hs4Ma3G189<br/>- Amazon RDS<br/>DB インスタンス<br/>用に拡張モニタ<br/>リングが設定さ<br/>れています</p> <p>対応する AWS<br/>Security Hub<br/>CSPM チェック:<br/><a href="#">RDS.6</a></p> | <p>AWSManagedServices-TrustedR<br/>emediatorEnableRDSEnhancedM<br/>onitoring</p> <p>Amazon RDS DB インスタンスの拡張モニタリングを有効にする</p> | <ul style="list-style-type: none"><li>MonitoringInterval: DB インスタンスの拡張モニタリングメトリクスが収集されるポイント間の秒単位の間隔。有効な間隔は 0、1、5、10、15、30、60 です。拡張モニタリングメトリクスの収集を無効にするには、0 を指定します。</li><li>MonitoringRoleName: Amazon RDS が拡張モニタリングメトリクスを Amazon CloudWatch Logs に送信することを許可する IAM ロールの名前。ロールが指定されていない場合、デフォルトのロールが存在しない場合は使用 rds-monitoring-role または作成されます。</li></ul> <p>自動化の実行前に拡張モニタリングが有効になっている場合、事前設定されたパラメータで設定された MonitoringInterval 値と MonitoringRoleName 値を使用して、この自動化によって設定が上書きされる可能性があります。</p> |

| ID と名前を確認する                                                                                                                  | SSM ドキュメント名と期待される成果                                                                                                        | サポートされている事前設定済みパラメータと制約                  |
|------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| <p>Hs4Ma3G190 - Amazon RDS クラスターでは削除保護が有効になっている必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">RDS.7</a></p>     | <p>AWSManagedServices-TrustedR<br/>emediatorEnableRDSDeletionP<br/>rotection</p> <p>削除保護は Amazon RDS クラスターで有効になっています。</p>  | <p>事前設定済みのパラメータは許可されません。</p> <p>制約なし</p> |
| <p>Hs4Ma3G198 - Amazon RDS DB インスタンスでは削除保護が有効になっている必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">RDS.8</a></p> | <p>AWSManagedServices-TrustedR<br/>emediatorEnableRDSDeletionP<br/>rotection</p> <p>削除保護は Amazon RDS インスタンスで有効になっています。</p> | <p>事前設定済みのパラメータは許可されません。</p> <p>制約なし</p> |

| ID と名前を確認する                                                                                                                      | SSM ドキュメント名と期待される成果                                                                                                                   | サポートされている事前設定済みパラメータと制約                                                                                                                                                          |
|----------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Hs4Ma3G199 - RDS DB インスタンスは CloudWatch Logs にログを発行する必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">RDS.9</a></p> | <p>AWSManagedServices-TrustedR<br/>emediatorEnableRDSLogExports</p> <p>RDS DB インスタンスまたは RDS DB クラスターで RDS ログのエクスポートが有効になっています。</p>    | <p>事前設定済みのパラメータは許可されません。</p> <p>サービスにリンクされたロール <a href="#">AWSServiceRoleForRDS</a> が必要です。</p>                                                                                   |
| <p>Hs4Ma3G160 - RDS インスタンスに IAM 認証を設定する必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">RDS.10</a></p>                | <p>AWSManagedServices-UpdateRD<br/>SIAMDatabaseAuthentication</p> <p>AWS Identity and Access Management 認証は RDS インスタンスで有効になっています。</p> | <p>ApplyImmediately: このリクエストの変更と保留中の変更ができるだけ早く非同期的に適用されるかどうかを示します。変更をすぐに適用するには、 <code>true</code> を選択します。次のメンテナンスウィンドウの変更をスケジュールするには、 <code>false</code> を選択します。</p> <p>制約なし</p> |
| <p>Hs4Ma3G161 - RDS クラスターに対して IAM 認証を設定する必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">RDS.12</a></p>              | <p>AWSManagedServices-UpdateRD<br/>SIAMDatabaseAuthentication</p> <p>RDS クラスターで IAM 認証が有効になっています。</p>                                 | <p>ApplyImmediately: このリクエストの変更と保留中の変更ができるだけ早く非同期的に適用されるかどうかを示します。変更をすぐに適用するには、 <code>true</code> を選択します。次のメンテナンスウィンドウの変更をスケジュールするには、 <code>false</code> を選択します。</p> <p>制約なし</p> |

| ID と名前を確認する                                                                                                                      | SSM ドキュメント名と期待される成果                                                                                               | サポートされている事前設定済みパラメータと制約                                                                    |
|----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| <p>Hs4Ma3G162 - RDS 自動マイナーバージョンアップグレードを有効にする必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">RDS.13</a></p>           | <p>AWSManagedServices-UpdateRDSInstanceMinorVersionUpgrade</p> <p>Amazon RDS の自動マイナーバージョンアップグレード設定が有効になっています。</p> | <p>事前設定済みのパラメータは許可されません。</p> <p>この修復を実行するには、Amazon RDS インスタンスが available 状態である必要があります。</p> |
| <p>Hs4Ma3G163 - RDS DB クラスターは、スナップショットにタグをコピーするように設定する必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">RDS.16</a></p> | <p>AWSManagedServices-UpdateRDSCopyTagsToSnapshots</p> <p>CopyTagToSnapshot Amazon RDS クラスターの設定が有効になっています。</p>    | <p>事前設定済みのパラメータは許可されません。</p> <p>この修復を実行するには、Amazon RDS インスタンスが使用可能な状態である必要があります。</p>       |

| ID と名前を確認する                                                                                                                        | SSM ドキュメント名と期待される成果                                                                                               | サポートされている事前設定済みパラメータと制約                                                                                                                               |
|------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Hs4Ma3G164 - RDS DB インスタンスは、スナップショットにタグをコピーするように設定する必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">RDS.17</a></p>  | <p>AWSManagedServices-UpdateRDSCopyTagsToSnapshots</p> <p>CopyTagsToSnapshot Amazon RDS の設定が有効になっています。</p>        | <p>事前設定済みのパラメータは許可されません。</p> <p>この修復を実行するには、Amazon RDS インスタンスが使用可能な状態である必要があります。</p>                                                                  |
| <p><a href="#">rSs93HQwa1</a></p> <p>Amazon RDS パブリックスナップショット</p>                                                                  | <p>AWSManagedServices-DisablePublicAccessOnRDSnapshotV2</p> <p>Amazon RDS スナップショットのパブリックアクセスは無効になっています。</p>       | <p>事前設定済みのパラメータは許可されません。</p> <p>制約なし</p>                                                                                                              |
| <p>Hs4Ma3G103 - Amazon Redshift クラスターはパブリックアクセスを禁止する必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">Redshift.1</a></p> | <p>AWSManagedServices-DisablePublicAccessOnRedshiftCluster</p> <p>Amazon Redshift クラスターでのパブリックアクセスは無効になっています。</p> | <p>事前設定済みのパラメータは許可されません。</p> <p>パブリックアクセスを無効にすると、インターネットからのすべてのクライアントがブロックされます。また、Amazon Redshift クラスターは数分間変更状態になり、修復によりクラスターへのパブリックアクセスが無効になります。</p> |

| ID と名前を確認する                                                                                                                                 | SSM ドキュメント名と期待される成果                                                                                                                                                                                                                   | サポートされている事前設定済みパラメータと制約                                                                                                                                                                                                                                                                                    |
|---------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Hs4Ma3G106 - Amazon Redshift クラスターでは監査ログ記録が有効になっている必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">Redshift.4</a></p>        | <p>AWSManagedServices-TrustedRedshiftClusterAuditLogging</p> <p>監査ログ記録は、メンテナンスウィンドウ中に Amazon Redshift クラスターに対して有効になります。</p>                                                                                                           | <p>事前設定済みのパラメータは許可されません。</p> <p>自動修復を有効にするには、以下の事前設定済みパラメータを指定する必要があります。</p> <p>BucketName: バケットは同じにある必要があります AWS リージョン。クラスターには、読み取りバケットと put オブジェクトのアクセス許可が必要です。</p> <p>自動化の実行前に Redshift クラスターのログ記録が有効になっている場合、ログ記録設定は、事前設定されたパラメータで設定された BucketName および S3KeyPrefix 値を使用して、この自動化によって上書きされる可能性があります。</p> |
| <p>Hs4Ma3G105 - Amazon Redshift では、メジャーバージョンへの自動アップグレードを有効にする必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">Redshift.6</a></p> | <p>AWSManagedServices-EnableRedshiftClusterVersionAutoUpgrade - メジャーバージョンアップグレードは、メンテナンスウィンドウ中にクラスターに自動的に適用されます。Amazon Redshift クラスターには即時のダウンタイムはありませんが、メジャーバージョンにアップグレードすると、Amazon Redshift クラスターのメンテナンス期間中にダウンタイムが発生する可能性があります。</p> | <p>事前設定済みのパラメータは許可されません。</p> <p>制約なし</p>                                                                                                                                                                                                                                                                   |

| ID と名前を確認する                                                                                                                            | SSM ドキュメント名と期待される成果                                                                                                        | サポートされている事前設定済みパラメータと制約                                                                                                                                     |
|----------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Hs4Ma3G104 - Amazon Redshift クラスターは拡張 VPC ルーティングを使用する必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">Redshift.7</a></p> | <p>AWSManagedServices-TrustedRedshiftClusterEnhancedVPCRouting</p> <p>Amazon Redshift クラスターでは、拡張 VPC ルーティングが有効になっています。</p> | <p>事前設定済みのパラメータは許可されません。</p> <p>制約なし</p>                                                                                                                    |
| <p>Hs4Ma3G173 - S3 パブリックアクセスブロック設定はバケットレベルで有効にする必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">S3.8</a></p>               | <p>AWSManagedServices-TrustedRedshiftClusterEnhancedVPCRouting</p> <p>バケットレベルのパブリックアクセスブロックが Amazon S3 バケットに適用されます。</p>    | <p>事前設定済みのパラメータは許可されません。</p> <p>この修復は、S3 オブジェクトの可用性に影響する可能性があります。Amazon S3 がアクセスを評価する方法については、<a href="#">Amazon S3 ストレージへのパブリックアクセスのブロック</a>」を参照してください。</p> |



| ID と名前を確認する                                                                                                        | SSM ドキュメント名と期待される成果                                                                                                                 | サポートされている事前設定済みパラメータと制約                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Hs4Ma3G230 - S3 バケットサーバーアクセスのログ記録を有効にする必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">S3.9</a></p> | <p>AWSManagedServices-EnableBucketAccessLogging (自動実行モードと手動実行モードの両方のデフォルト SSM ドキュメント)</p> <p>Amazon S3 サーバーアクセスのログ記録が有効になっています。</p> | <ul style="list-style-type: none"><li>• TargetBucket: サーバーアクセスログを保存する S3 バケットの名前。</li><li>• TargetObjectKeyFormat: ログオブジェクトの Amazon S3 キー形式 (値は大文字と小文字が区別されます)。ログオブジェクトの S3 キーにシンプルな形式を使用するには、<code>SimplePrefix</code> を選択します。ログオブジェクトにパーティション化された S3 キーを使用し、パーティション化されたプレフィックスに <code>EventTime</code> を使用するには、<code>PartitionedPrefixEventTime</code> を選択します。ログオブジェクトにパーティション化された S3 キーを使用し、パーティション化されたプレフィックスに <code>DeliveryTime</code> を使用するには、<code>PartitionedPrefixDeliveryTime</code> を選択します。有効な値は、<code>SimplePrefix</code>、<code>PartitionedPrefixEventTime</code>、<code>PartitionedPrefixDeliveryTime</code> です。</li></ul> <p>自動修復を有効にするには、TargetBucket という事前設定済みのパラメータを指定する必要があります。</p> |

| ID と名前を確認する | SSM ドキュメント名と期待される成果 | サポートされている事前設定済みパラメータと制約                                                                                                                             |
|-------------|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
|             |                     | レプリケート先バケットは、ログ配信の正しいアクセス許可を持つレプリケート元バケット AWS アカウントと同じ AWS リージョン および 必要がある必要があります。詳細については、「 <a href="#">Amazon S3 サーバーアクセスログを有効にします</a> 」を参照してください。 |

| ID と名前を確認する                                                                                                        | SSM ドキュメント名と期待される成果                                                                                      | サポートされている事前設定済みパラメータと制約                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Hs4Ma3G230 – S3 バケットサーバーのアクセスログ記録を有効にする必要があります</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">S3.9</a></p> | <p>AWSManagedServices-TrustedRolemediatorEnableBucketAccessLoggingV2 - Amazon S3 バケットログ記録が有効になっています。</p> | <ul style="list-style-type: none"> <li>• TargetBucketTagKey: ターゲットバケットを識別するタグ名 (大文字と小文字を区別)。これと TargetBucketTagValue を使用して、アクセスログ記録の送信先バケットとして使用するバケットにタグを付けます。</li> <li>• TargetBucketTagValue: ターゲットバケットを識別するタグ値 (大文字と小文字を区別)。これと TargetBucketTagKey を使用して、アクセスログ記録の送信先バケットとして使用するバケットにタグを付けます。</li> <li>• TargetObjectKeyFormat: ログオブジェクトの Amazon S3 キー形式 (値は大文字と小文字が区別されます): ログオブジェクトの S3 キーにシンプルな形式を使用するには、SimplePrefix を選択します。ログオブジェクトにパーティション化された S3 キーを使用し、パーティション化されたプレフィックスに EventTime を使用するには、PartitionedPrefixEventTime を選択します。ログオブジェクトにパーティション化された S3 キーを使用し、パーティション化されたプレフィックスに DeliveryTime を使用するには、PartitionedPrefixDeliveryTime を選択します。デフォルトは PartitionedPrefixEventTime です。</li> </ul> |

| ID と名前を確認する                                               | SSM ドキュメント名と期待される成果                                                                          | サポートされている事前設定済みパラメータと制約                                                                                                                                                                                                                    |
|-----------------------------------------------------------|----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                           |                                                                                              | <p>自動修復を有効にするには、TargetBucketTagKey と TargetBucketTagValue のパラメータを指定する必要があります。</p> <p>レプリケート先バケットは、ログ配信の正しいアクセス許可を持つレプリケート元バケット AWS アカウントと同じ AWS リージョン および 必要がある必要があります。詳細については、「<a href="#">Amazon S3 サーバーアクセスログを有効にします</a>」を参照してください。</p> |
| <p><a href="#">Pfx0RwqBli</a></p> <p>Amazon S3 バケット許可</p> | <p>AWSManagedServices-TrustedRemediatorBlockS3BucketPublicAccess</p> <p>パブリックアクセスをブロックする</p> | <p>事前設定済みのパラメータは許可されません。</p> <p>このチェックは、複数のアラート条件で構成されます。この自動化により、パブリックアクセスの問題が修正されます。で Trusted Advisor フラグが付けられた他の設定の問題の修正はサポートされていません。この修復は、AWS のサービス 作成された S3 バケット (cf-templates-000000000000 など) の修復をサポートします。</p>                      |

| ID と名前を確認する                                                                                                                            | SSM ドキュメント名と期待される成果                                                                                                                                     | サポートされている事前設定済みパラメータと制約                                                                                                                                                                                                                    |
|----------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Hs4Ma3G27<br/>2 - ユーザーは SageMaker ノートブックインスタンスにルートアクセスできません</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">SageMaker.3</a></p> | <p>AWSManagedServices-TrustedR<br/>emediatorDisableSageMakerNo<br/>tebookInstanceRootAccess</p> <p>SageMaker ノートブックインスタンスでは、ユーザーのルートアクセスは無効になっています。</p> | <p>事前設定済みのパラメータは許可されません。</p> <p>この修復により、SageMaker ノートブックインスタンスが InService 状態の場合、停止が発生します。</p>                                                                                                                                              |
| <p>Hs4Ma3G179 - SNS トピックは保管時にを使用して暗号化する必要があります AWS KMS</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">SNS.1</a></p>               | <p>AWSManagedServices-EnableSN<br/>SEncryptionAtRest</p> <p>SNS トピックはサーバー側の暗号化で設定されます。</p>                                                              | <p>KmsKeyId: サーバー側の暗号化 (SSE) に使用される Amazon SNS またはカスタム CMK の AWS マネージドカスタマーマスターキー (CMK) の ID。デフォルトでは alias/aws/sns に設定されています。</p> <p>カスタム AWS KMS キーを使用する場合は、正しいアクセス許可で設定する必要があります。詳細については、<a href="#">Amazon SNSを有効にする</a>」を参照してください。</p> |
| <p>Hs4Ma3G158 - SSM ドキュメントは公開しないでください</p> <p>対応する AWS Security Hub CSPM チェック: <a href="#">SSM.4</a></p>                                | <p>AWSManagedServices-TrustedR<br/>emediatorDisableSSMDocPubli<br/>cSharing - SSM ドキュメントのパブリック共有を無効にします。</p>                                            | <p>事前設定済みのパラメータは許可されません。</p> <p>制約なし</p>                                                                                                                                                                                                   |

| ID と名前を確認する                                                                                                                   | SSM ドキュメント名と期待される成果                                                                   | サポートされている事前設定済みパラメータと制約                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Hs4Ma3G136<br/>- Amazon SQS<br/>キューは保管時に暗号化する必要があります</p> <p>対応する AWS Security Hub CSPM チェック:<br/><a href="#">SQS.1</a></p> | <p>AWSManagedServices-EnableSQSEncryptionAtRest</p> <p>Amazon SQS のメッセージは暗号化されます。</p> | <ul style="list-style-type: none"><li>• SqsManagedSseEnabled: に設定するtrueとAmazon SQS 所有の暗号化キーを使用したサーバー側のキュー暗号化が有効になり、に設定するfalseと、AWS KMS キーを使用したサーバー側のキュー暗号化が有効になります。</li><li>• KMSKeyId: Amazon SQS の AWS マネージドカスタマーマスターキー (CMK) またはキューのサーバー側の暗号化に使用されるカスタム CMK の ID またはエイリアス。指定しない場合、alias/aws/sqs が使用されます。</li><li>• KmsDataKeyReusePeriodSeconds: Amazon SQS がデータキーを再利用して、AWS KMS 再度 を呼び出す前にメッセージを暗号化または復号できる秒単位の時間の長さ。60秒(1分)から86,400秒(24時間)の秒数を表す整数。が に設定されている場合SqsManagedSseEnabled、この設定は無視されますtrue。</li></ul> <p>暗号化されたキューへの匿名 SendMessage および ReceiveMessage リクエストは拒否されます。SSE が有効なキューへのすべてのリクエストでは必ず、HTTPSと署名バージョン4 を使用する必要があります。</p> |

## Trusted Advisor Trusted Remediator でサポートされている耐障害性チェック

| ID と名前を確認する                                                         | SSM ドキュメント名と期待される成果                                                                                 | サポートされている事前設定済みパラメータと制約                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">c18d2gz138</a><br><br>Amazon<br>DynamoDB のポイントインタイムリカバリ | AWSManagedServices-TrustedRemediatorEnableDDBPITR<br><br>DynamoDB テーブルのpoint-in-time リカバリを有効にします。   | 事前設定済みのパラメータは許可されません。<br><br>制約なし                                                                                                                                                                                                                                                                                                                                                                         |
| <a href="#">R365s2Qddf</a><br><br>Amazon S3 バケットバージョニング             | AWSManagedServices-TrustedRemediatorEnableBucketVersioning<br><br>Amazon S3 バケットのバージョニングが有効になっています。 | 事前設定済みのパラメータは許可されません。<br><br>この修復は、AWS のサービス作成された S3 バケット (cf-templates-0000000000000000 など) の修復をサポートしていません。                                                                                                                                                                                                                                                                                              |
| <a href="#">BueAdJ7NrP</a><br><br>Amazon S3 バケットロギング                | AWSManagedServices-EnableBucketAccessLogging<br><br>Amazon S3 バケットのログ記録が有効になっています。                  | <ul style="list-style-type: none"> <li>TargetBucket: サーバーアクセスログを保存する S3 バケットの名前。</li> <li>TargetObjectKeyFormat: ログオブジェクトの Amazon S3 キー形式。ログオブジェクトの S3 キーのシンプルな形式を使用するには、 <code>SimplePrefix</code> を選択します。ログオブジェクトにパーティション化された S3 キーを使用し、パーティション化されたプレフィックスに <code>EventTime</code> を使用するには、 <code>PartitionedPrefixEventTime</code> を選択します。ログオブジェクトにパーティション化された S3 キーを使用し、パーティション化されたプレフィックス</li> </ul> |



| ID と名前を確認する                                              | SSM ドキュメント名と期待される成果                                                                         | サポートされている事前設定済みパラメータと制約                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------------------------|---------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                          |                                                                                             | <p>クスの DeliveryTime を使用するには、 を選択します PartitionedPrefixDeliveryTime 。デフォルトは PartitionedPrefixEventTime です。有効な値は SimplePrefix 、 、および PartitionedPrefixDeliveryTime (大文字 PartitionedPrefixEventTime と小文字が区別されます) です。</p> <p>自動修復を有効にするには、以下の事前設定済みパラメータを指定する必要があります。</p> <ul style="list-style-type: none"> <li>• TargetBucket</li> </ul> <p>レプリケート先バケットは、ログ配信の正しいアクセス許可を持つレプリケート元バケット AWS アカウントと同じ AWS リージョン および 必要がある必要があります。詳細については、「<a href="#">Amazon S3 サーバーアクセスログを有効にします</a>」を参照してください。</p> |
| <a href="#">f2iK5R6Dep</a><br><br>Amazon RDS<br>Multi-AZ | AWSManagedServices-TrustedRemediatorEnableRDSMultiAZ<br><br>マルチアベイラビリティーゾーンのデプロイが有効になっています。 | <p>事前設定済みのパラメータは許可されません。</p> <p>この変更中にパフォーマンスが低下する可能性があります。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                |

| ID と名前を確認する                                           | SSM ドキュメント名と期待される成果                                                                              | サポートされている事前設定済みパラメータと制約                                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------|--------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">H7lgTzjTYb</a><br><br>Amazon EBS スナップショット | <p>AWSManagedServices-TrustedRemediatorCreateEBSSnapshot</p> <p>Amazon EBSsnapshotsが作成されます。</p>  | <p>事前設定済みのパラメータは許可されません。</p> <p>制約なし</p>                                                                                                                                                                                                                                                                               |
| <a href="#">opQPADkZvH</a><br><br>RDS バックアップ          | <p>AWSManagedServices-EnableRDSBackupRetention</p> <p>Amazon RDS バックアップ保持は DB に対して有効になっています。</p> | <ul style="list-style-type: none"><li>BackupRetentionPeriod: 自動バックアップを保持する日数 (1 ~ 35)。</li><li>ApplyImmediately: RDS バックアップ保持の変更と保留中の変更ができるだけ早く非同期的に適用されるかどうかを示します。変更をすぐにtrue適用するか、次のメンテナンスウィンドウに変更をスケジュールfalseするかを選択します。</li></ul> <p>ApplyImmediately パラメータがに設定されている場合true、db の保留中の変更が RDSBackup 保持設定とともに適用されます。</p> |

| ID と名前を確認する                                                                            | SSM ドキュメント名と期待される成果                                                                                                                   | サポートされている事前設定済みパラメータと制約                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><a href="#">c1qf5bt013</a></p> <p>Amazon RDS DB インスタンスのストレージの自動スケーリングが無効になっています</p> | <p>AWSManagedServices-TrustedRemediatorEnableRDSInstanceStorageAutoScaling - Amazon RDS DB インスタンスでストレージの自動スケーリングが有効になっています。</p>       | <ul style="list-style-type: none"> <li>MaxAllocatedStorageIncreasePercentage: AllocatedStorage の増加率。MaxAllocatedStorage デフォルトでは 26 に設定されています。</li> </ul> <p>最大ストレージしきい値は、現在割り当てられているストレージよりも 10% 以上高く設定する必要があります。最大ストレージしきい値を 26% 以上に設定するのがベストプラクティスです。詳細については、「<a href="#">Managing capacity automatically with Amazon Relational Database Service storage autoscaling</a>」を参照してください。</p> <p>制約なし</p> |
| <p><a href="#">7qGXsKIUw</a></p> <p>Classic Load Balancer 接続ドレイン</p>                   | <p>AWSManagedServices-TrustedRemediatorEnableCLBConnectionDraining</p> <p>Classic Load Balancer で Connection Draining が有効になっています。</p> | <p>ConnectionDrainingTimeout: インスタンスの登録を解除する前に既存の接続を開いたままにする最大時間を秒単位で表します。デフォルトは 300 秒に設定されています。</p> <p>制約なし</p>                                                                                                                                                                                                                                                                                       |

| ID と名前を確認する                                                                   | SSM ドキュメント名と期待される成果                                                                                               | サポートされている事前設定済みパラメータと制約                                                                                                                                                |
|-------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">c18d2gz106</a><br><br>Amazon EBS が AWS Backup プランに含まれていない         | AWSManagedServices-TrustedRemediatorAddVolumeToBackupPlan<br><br>Amazon EBS は AWS Backup プランに含まれています。             | 修復では、Amazon EBS ボリュームに次のタグペアがタグ付けされます。タグペアは、タグベースのリソース選択基準と一致する必要があります AWS Backup。 <ul style="list-style-type: none"> <li>• TagKey</li> <li>• TagValue</li> </ul> 制約なし |
| <a href="#">c18d2gz107</a><br><br>AWS Backup プランに含まれていない Amazon DynamoDB テーブル | AWSManagedServices-TrustedRemediatorAddDynamoDBToBackupPlan<br><br>Amazon DynamoDB テーブルは AWS Backup プランに含まれていません。 | 修復では、Amazon DynamoDB に次のタグペアがタグ付けされます。タグペアは、タグベースのリソース選択基準と一致する必要があります AWS Backup。 <ul style="list-style-type: none"> <li>• TagKey</li> <li>• TagValue</li> </ul> 制約なし |
| <a href="#">c18d2gz117</a><br><br>Amazon EFS が AWS Backup プランに含まれていない         | AWSManagedServices-TrustedRemediatorAddEFSToBackupPlan<br><br>Amazon EFS は AWS Backup プランに含まれています。                | 修復では、Amazon EFS に次のタグペアがタグ付けされます。タグペアは、タグベースのリソース選択基準と一致する必要があります AWS Backup。 <ul style="list-style-type: none"> <li>• TagKey</li> <li>• TagValue</li> </ul> 制約なし      |

| ID と名前を確認する                                                                                 | SSM ドキュメント名と期待される成果                                                                                                                          | サポートされている事前設定済みパラメータと制約           |
|---------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
| <a href="#">c18d2gz105</a><br><br>Network Load Balancer のクロスロードバランシング                       | AWSManagedServices-TrustedRemediatorEnableNLBCrossZoneLoadBalancing<br><br>Network Load Balancer ではクロスゾーン負荷分散が有効になっています。                     | 事前設定済みのパラメータは許可されません。<br><br>制約なし |
| <a href="#">c1qf5bt026</a><br><br>Amazon RDS synchronous_commit パラメータがオフになっている              | AWSManagedServices-TrustedRemediatorRemediateRDSPParameterGroupParameter<br><br>Amazon RDS のパラメータsynchronous_commit がオンになっています。              | 事前設定済みのパラメータは許可されません。<br><br>制約なし |
| <a href="#">c1qf5bt030</a><br><br>Amazon RDS innodb_flush_log_at_trx_commit パラメータはではありません 1 | AWSManagedServices-TrustedRemediatorRemediateRDSPParameterGroupParameter<br><br>Amazon RDS 1のパラメータinnodb_flush_log_at_trx_commit はに設定されています。 | 事前設定済みのパラメータは許可されません。<br><br>制約なし |
| <a href="#">c1qf5bt031</a><br><br>Amazon RDS sync_binlog パラメータがオフになっている                     | AWSManagedServices-TrustedRemediatorRemediateRDSPParameterGroupParameter<br><br>Amazon RDS のパラメータsync_binlog がオンになっています。                     | 事前設定済みのパラメータは許可されません。<br><br>制約なし |

| ID と名前を確認する                                                                       | SSM ドキュメント名と期待される成果                                                                                                                         | サポートされている事前設定済みパラメータと制約           |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
| <a href="#">c1qf5bt036</a><br>Amazon RDS innodb_default_row_format パラメータ設定が安全ではない | AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter<br><br>Amazon RDS DYNAMICのパラメータinnodb_default_row_format は に設定されています。 | 事前設定済みのパラメータは許可されません。<br><br>制約なし |
| <a href="#">c18d2gz144</a><br>Amazon EC2 詳細モニタリングが有効化されていません                      | AWSManagedServices-TrustedRemediatorEnableEC2InstanceDetailedMonitoring<br><br>詳細モニタリングは Amazon EC2 で有効になっています。                             | 事前設定済みのパラメータは許可されません。<br><br>制約なし |

## Trusted Advisor Trusted Remediator でサポートされているパフォーマンスチェック

| ID と名前を確認する                                                  | SSM ドキュメント名と期待される成果                                                                                  | サポートされている事前設定済みパラメータと制約                                                                                                                               |
|--------------------------------------------------------------|------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">COr6dfpM06</a><br>AWS Lambda メモリサイズのプロビジョニング不足関数 | AWSManagedServices-ResizeLambdaMemory<br><br>Lambda 関数のメモリサイズは、が提供する推奨メモリサイズに変更されます Trusted Advisor。 | RecommendedMemorySize: Lambda 関数に推奨されるメモリ割り当て。値の範囲は 128 ~ 10240 です。<br><br>自動化の実行前に Lambda 関数のサイズが変更された場合、この自動化は推奨値で設定を上書きする可能性があります Trusted Advisor。 |
| <a href="#">ZRxQIPsb6c</a><br>使用率の高い Amazon EC2 インスタンス       | AWSManagedServices-ResizeInstanceByOneLevel<br><br>Amazon EC2 インスタンスのサイズは、同じインスタンスファミリー              | <ul style="list-style-type: none"> <li>MinimumDaysSinceLastChange: 前回のインスタンスタイプ変更からの最小日数。インスタンスタイプが指定された時間内に変更され</li> </ul>                           |

| ID と名前を確認する | SSM ドキュメント名と期待される成果                                                                                                                   | サポートされている事前設定済みパラメータと制約                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|             | <p>タイプで 1 つのインスタンスタイプごとに変更されます。インスタンスはサイズ変更オペレーション中に停止および開始され、実行の完了後に初期状態に戻ります。この自動化は、Auto Scaling グループ内のインスタンスのサイズ変更をサポートしていません。</p> | <p>た場合、インスタンスタイプは変更されません。を使用して、この検証0をスキップします。デフォルトは 7 です。</p> <ul style="list-style-type: none"><li>• CreateAMIBeforeResize: サイズ変更前にインスタンス AMI をバックアップとして作成するには、 を選択しますtrue。バックアップを作成しない場合は、 を選択しますfalse。デフォルトは false です。有効な値は trueおよび false (大文字と小文字が区別されます) です。</li><li>• ResizelfStopped: インスタンスが停止状態であっても、インスタンスサイズの変更を続行するには、 を選択しますtrue。停止状態でインスタンスのサイズを自動的に変更しない場合は、 を選択しますfalse。有効な値は trueと false (大文字と小文字が区別されます) です。</li></ul> <p>制約なし</p> |



| ID と名前を確認する                                                                              | SSM ドキュメント名と期待される成果                                                                                                                        | サポートされている事前設定済みパラメータと制約           |
|------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
| <a href="#">c1qf5bt021</a><br><br>最適値未満を使用する<br>Amazon RDS innodb_change_buffering パラメータ | AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter<br><br>Amazon RDS NONE の場合、innodb_change_buffering パラメータの値は に設定されます。 | 事前設定済みのパラメータは許可されません。<br><br>制約なし |
| <a href="#">c1qf5bt025</a><br><br>Amazon RDS autovacuum パラメータがオフになっている                   | AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter<br><br>Amazon RDS のパラメータ autovacuum がオンになっています。                      | 事前設定済みのパラメータは許可されません。<br><br>制約なし |
| <a href="#">c1qf5bt028</a><br><br>Amazon RDS enable_indexonlyscan パラメータがオフになっている         | AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter<br><br>Amazon RDS ではパラメータ enable_indexonlyscan がオンになっています。           | 事前設定済みのパラメータは許可されません。<br><br>制約なし |
| <a href="#">c1qf5bt029</a><br><br>Amazon RDS enable_indexscan パラメータがオフになっている             | AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter<br><br>Amazon RDS のパラメータ enable_indexscan がオンになっています。                | 事前設定済みのパラメータは許可されません。<br><br>制約なし |

| ID と名前を確認する                                                                         | SSM ドキュメント名と期待される成果                                                                                                               | サポートされている事前設定済みパラメータと制約           |
|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
| <a href="#">c1qf5bt032</a><br><br>Amazon RDS innodb_stats_persistent パラメータがオフになっている | AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter<br><br>Amazon RDS のパラメータinnodb_stats_persistent がオンになっています。 | 事前設定済みのパラメータは許可されません。<br><br>制約なし |
| <a href="#">c1qf5bt037</a><br><br>Amazon RDS general_logging パラメータがオンになっている         | AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter<br><br>Amazon RDS のパラメータgeneral_logging は無効になっています。         | 事前設定済みのパラメータは許可されません。<br><br>制約なし |

## Trusted Advisor Trusted Remediator でサポートされているサービス制限チェック

| ID と名前を確認する                                               | SSM ドキュメント名と期待される成果                                                                                                | サポートされている事前設定済みパラメータと制約                                                                                          |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| <a href="#">IN7RR0I7J9</a><br><br>EC2-VPC Elastic IP アドレス | AWSManagedServices-UpdateVpcElasticIPQuota<br><br>EC2-VPC Elastic IP アドレスの新しい制限がリクエストされます。デフォルトでは、制限は 3 つ引き上げられます。 | 増分: 現在のクォータを引き上げる数値。デフォルトは 3 です。<br><br>Trusted Advisor チェックが OKステータスで更新される前にこの自動化が複数回実行されると、制限が引き上げられる可能性があります。 |
| <a href="#">kM7QQ0I7J9</a><br><br>VPC インターネットゲートウェイ       | AWSManagedServices-IncreaseServiceQuota - VPC インターネットゲートウェイの新しい制限がリクエ                                              | 増分: 現在のクォータを引き上げる数値。デフォルトは 3 です。<br><br>Trusted Advisor チェックが OKステータスで更新される前にこの自動                                |

| ID と名前を確認する                                                     | SSM ドキュメント名と期待される成果                                                                                                                   | サポートされている事前設定済みパラメータと制約                                                                                                                                         |
|-----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">jL7PP0I7J9</a><br><br>VPC                           | <p>ストされます。デフォルトでは、制限は 3 つ増加します。</p> <p>AWSManagedServices-Increase ServiceQuota</p> <p>VPC の新しい制限がリクエストされます。デフォルトでは、制限は 3 つ増加します。</p> | <p>化が複数回実行されると、制限が引き上げられる可能性があります。</p> <p>増分: 現在のクォータを引き上げる数値。デフォルトは 3 です。</p> <p>Trusted Advisor チェックが OK ステータスで更新される前にこの自動化が複数回実行されると、制限が引き上げられる可能性があります。</p> |
| <a href="#">fW7HH0I7J9</a><br><br>Auto Scaling グループ             | <p>AWSManagedServices-Increase ServiceQuota</p> <p>Auto Scaling グループの新しい制限がリクエストされます。デフォルトでは、制限は 3 つ増加します。</p>                        | <p>増分: 現在のクォータを引き上げる数値。デフォルトは 3 です。</p> <p>Trusted Advisor チェックが OK ステータスで更新される前にこの自動化が複数回実行されると、制限が引き上げられる可能性があります。</p>                                        |
| <a href="#">3Njm0DJQO9</a><br><br>RDS オプショングループ                 | <p>AWSManagedServices-Increase ServiceQuota</p> <p>Amazon RDS オプショングループの新しい制限がリクエストされます。デフォルトでは、制限は 3 つ増加します。</p>                     | <p>増分: 現在のクォータを引き上げる数値。デフォルトは 3 です。</p> <p>Trusted Advisor チェックが OK ステータスで更新される前にこの自動化が複数回実行されると、制限が引き上げられる可能性があります。</p>                                        |
| <a href="#">EM8b3yLRTr</a><br><br>ELB Application Load Balancer | <p>AWSManagedServices-Increase ServiceQuota</p> <p>ELB Application Load Balancer の新しい制限がリクエストされました。デフォルトでは、制限は 3 つ増加します。</p>          | <p>増分: 現在のクォータを引き上げる数値。デフォルトは 3 です。</p> <p>Trusted Advisor チェックが OK ステータスで更新される前にこの自動化が複数回実行されると、制限が引き上げられる可能性があります。</p>                                        |

| ID と名前を確認する                                                 | SSM ドキュメント名と期待される成果                                                                                              | サポートされている事前設定済みパラメータと制約                                                                                           |
|-------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| <a href="#">8wlqYSt25K</a><br><br>ELB Network Load Balancer | AWSManagedServices-Increase ServiceQuota<br><br>ELB Network Load Balancer の新しい制限がリクエストされます。デフォルトでは、制限は 3 つ増加します。 | 増分: 現在のクォータを引き上げる数値。デフォルトは 3 です。<br><br>Trusted Advisor チェックが OK ステータスで更新される前にこの自動化が複数回実行されると、制限が引き上げられる可能性があります。 |

## Trusted Advisor Trusted Remediator でサポートされているオペレーショナルエクセレンスチェック

| ID と名前を確認する                                                                       | SSM ドキュメント名と期待される成果                                                                                      | サポートされている事前設定済みパラメータと制約                                                                                                                                                                         |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">c18d2gz125</a><br><br>Amazon API Gateway が実行ログを記録しない                  | AWSManagedServices-TrustedRemediatorEnableAPIGatewayExecutionLogging<br><br>実行ログ記録は API ステージで有効になっています。  | 事前設定済みのパラメータは許可されません。<br><br>実行ログを有効にするには、アカウントの CloudWatch にログを読み書きするアクセス許可を API Gateway に付与する必要があります。詳細については、「 <a href="#">API Gateway で REST API の CloudWatch ログ記録を設定する APIs</a> 」を参照してください。 |
| <a href="#">c18d2gz168</a><br><br>ロードバランサーの Elastic Load Balancing 削除保護が有効になっていない | AWSManagedServices-TrustedRemediatorEnableELBDeletionProtection - Elastic Load Balancer の削除保護が有効になっています。 | 事前設定済みのパラメータは許可されません。<br><br>制約なし                                                                                                                                                               |

| ID と名前を確認する                                                                  | SSM ドキュメント名と期待される成果                                                                                                       | サポートされている事前設定済みパラメータと制約                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">c1qf5bt012</a><br><br>Amazon RDS Performance Insights は無効になっています | AWSManagedServices-TrustedR<br>emediatorEnableRDSPerformanceInsights<br><br>Amazon RDS で Performance Insights が有効になっています。 | <ul style="list-style-type: none"><li>• PerformanceInsightsRetentionPeriod: Performance Insights データを保持する日数。有効な値: 7または月 * 31。月は 1 ~ 23 の月数です。例: 93 (3 か月 x 31)、341 (11 か月 x 31)、 589 (19 か月 x 31)、または 731。</li><li>• PerformanceInsightsKMSKeyId : Performance Insights データを暗号化するための AWS KMS キー ID。PerformanceInsightsKMSKeyId の値を指定しない場合、Amazon RDS はデフォルトの AWS KMS キーを使用します。</li></ul><br>制約なし |

| ID と名前を確認する                                                 | SSM ドキュメント名と期待される成果                                                                                               | サポートされている事前設定済みパラメータと制約                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">c1fd6b96l4</a><br><br>Amazon S3 アクセスログが有効になっている | AWSManagedServices-TrustedR<br>emediatorEnableBucketAccess<br>LoggingV2<br><br>Amazon S3 バケットアクセスのログ記録が有効になっています。 | <ul style="list-style-type: none"><li>• TargetBucketTagValue: ターゲットバケットを識別するタグ値 (大文字と小文字を区別)。これと TargetBucketTagKey を使用して、アクセスログ記録の送信先バケットとして使用するバケットにタグを付けます。</li><li>• TargetObjectKeyFormat: ログオブジェクトの Amazon S3 キー形式 (値は大文字と小文字が区別されます)。ログオブジェクトの S3 キーにシンプルな形式を使用するには、 を選択しますSimplePrefix。ログオブジェクトにパーティション化された S3 キーを使用し、パーティション化されたプレフィックスに EventTime を使用するには、 を選択しますPartitionedPrefixEventTime。ログオブジェクトにパーティション化された S3 キーを使用し、パーティション化されたプレフィックスに DeliveryTime を使用するには、 を選択しますPartitionedPrefixDeliveryTime。有効な値は、SimplePrefix、PartitionedPrefixEventTime、PartitionedPrefixDeliveryTime です。</li></ul> |

| ID と名前を確認する | SSM ドキュメント名と期待される成果 | サポートされている事前設定済みパラメータと制約                                                                                                                                                                                                                       |
|-------------|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|             |                     | <p>自動修復を有効にするには、TargetBucketTagKey と TargetBucketTagValue の事前設定済みパラメータを指定する必要があります。</p> <p>レプリケート先バケットは、ログ配信の正しいアクセス許可を持つレプリケート元バケットと同じ AWS リージョン および AWS アカウントにある必要があります。詳細については、「<a href="#">Amazon S3 サーバーアクセスログを有効にします</a>」を参照してください。</p> |

## 信頼できる修復者がサポートする Security Hub CSPM の推奨事項

次の表に、サポートされている Security Hub CSPM の推奨事項、SSM オートメーションドキュメント、事前設定されたパラメータ、およびオートメーションドキュメントの期待される結果を示します。SSM オートメーションドキュメントをチェック修復を有効にする前に、期待される結果を確認して、ビジネス要件に基づいて考えられるリスクを理解するのに役立ちます。

アカウントの Security Hub CSPM が有効になっていることを確認します。詳細については、「[Security Hub CSPM の有効化](#)」を参照してください。

| ID と名前を確認する                                                                      | SSM ドキュメント名と期待される成果                                                           | サポートされている事前設定済みパラメータと制約                                                                                 |
|----------------------------------------------------------------------------------|-------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| security-hub-IAM-22<br><br><a href="#">IAM.22: 45 日間使用されていない IAM ユーザー認証情報は削除</a> | AWSManagedServices-TrusteR<br>emediatorDeactivatelamUserU<br>nusedCredentials | <p>DeleteAccessKeys: 未使用のアクセスキーを完全に削除するには true、無効にするには false に設定します (非アクティブでも回復可能にします)。</p> <p>制約なし</p> |



| ID と名前を確認する                                                                                                                        | SSM ドキュメント名と期待される成果                                                                    | サポートされている事前設定済みパラメータと制約                                                                          |
|------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| <a href="#">する必要があります。</a>                                                                                                         |                                                                                        |                                                                                                  |
| security-hub-IAM-3<br><br><a href="#">IAM.3: IAM ユーザーのアクセスキーは 90 日以内にローテーションする必要があります。</a>                                         | AWSManagedServices-TrusteR<br>emediatorRotatelamAccessKey<br>sOlderThan90Days          | 事前設定済みのパラメータは許可されません。<br><br>制約なし                                                                |
| security-hub-IAM-8<br><br><a href="#">IAM.8: 未使用の IAM ユーザー認証情報を削除する必要があります。</a>                                                    | AWSManagedServices-TrusteR<br>emediatorDeactivatelamUserU<br>nusedCredentials          | DeleteAccessKeys: 未使用のアクセスキーを完全に削除するには true、無効にするには false に設定します (非アクティブでも回復可能にします)。<br><br>制約なし |
| security-hub-networkfirewal<br>l-10<br><br><a href="#">NetworkFirewall.10: Network Firewall ファイアウォールでは、サブネット変更保護を有効にする必要があります。</a> | AWSManagedServices-TrusteR<br>emediatorEnableNetworkFirew<br>allSubnetChangeProtection | 事前設定済みのパラメータは許可されません。<br><br>制約なし                                                                |

| ID と名前を確認する                                                                                                  | SSM ドキュメント名と期待される成果                                                    | サポートされている事前設定済みパラメータと制約                                                                                                          |
|--------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| security-hub-networkfirewall-2<br><a href="#">NetworkFirewall.2: Network Firewall のログ記録を有効にする必要があります。</a>    | AWSManagedServices-TrustedRemediatorEnableNetworkFirewallCloudWatchLog | LogGroupName: ログを送信する CloudWatch ロググループの名前。<br><br>LogTypes: 有効にするログのタイプ。有効な値は FLOW、ALERT、TLS です。<br><br>制約なし                    |
| security-hub-stepfunctions-1<br><a href="#">StepFunctions.1: Step Functions ステートマシンでは、ログ記録を有効にする必要があります。</a> | AWSManagedServices-TrustedRemediatorEnableStepFunctionLogging          | LogGroupName: Step Functions ログ記録用の CloudWatch ロググループの名前。<br><br>LoggingLevel: Step Functions のログ記録レベル。有効な値は ALL、ERROR、FATAL です。 |

## Trusted Remediator で Trusted Advisor チェック修復を設定する

設定は、信頼できる修復アプリケーション AWS AppConfig の一部として保存されます。各 Trusted Advisor チェックカテゴリには個別の設定プロファイルがあります。Trusted Advisor カテゴリの詳細については、[「チェックカテゴリの表示」](#)を参照してください。

修復の設定は、リソースベースまたは Trusted Advisor チェックベースでリクエストできます。リソースタグを使用して例外を適用できます。

### Note

Trusted Advisor 検出結果の修復は現在を使用して設定されており AWS AppConfig、この機能は現在完全にサポートされています。AMS は、これが将来変化すると予測しています。この方法は変更される可能性があるため AWS AppConfig、に依存するオートメーションの構築を避けることがベストプラクティスです。互換性を確保するために、将来の現在の AWS

AppConfig 実装を中心に構築されたオートメーションを更新または変更する必要がある場合があります。

Compute Optimizer -> EC2 インスタンス機能フラグには追加のパラメータがあります。

- allow-upscale プロビジョニング不足で最適化されていない EC2 インスタンスのアップスケールを許可します。デフォルト値は『false』です。
- min-savings-opportunity-percentage 自動修復の最小削減率の機会。デフォルト値は 10% です

## デフォルトの修復設定

個々の Trusted Advisor チェックの設定は AWS AppConfig フラグとして保存されます。フラグ名はチェック名と一致します。各チェック設定には、次の属性が含まれます。

- execution-mode: Trusted Remediator がデフォルトの修復を実行する方法を決定します。
  - 自動: Trusted Remediator は、OpsItem を作成し、SSM ドキュメントを実行してから、正常に実行された後に OpsItem を解決することで、リソースを自動的に修復します。
  - 手動: OpsItem が作成されますが、SSM ドキュメントは自動的に実行されません。OpsItem を確認し、自動 RFC を使用して修復を実行します。詳細については、「[Trusted Remediator で修復を操作する](#)」を参照してください。
  - 条件付き: 修復はデフォルトで無効になっています。タグを使用して、特定のリソースに対して有効にできます。詳細については、以下のセクション[リソースタグを使用して修復をカスタマイズする](#)と [リソースオーバーライドタグを使用して修復をカスタマイズする](#)を参照してください。
  - 非アクティブ: 修復は行われず、OpsItem は作成されません。非アクティブに設定されている Trusted Advisor チェックの実行モードを上書きすることはできません。
- preconfigured-parameters: 自動修復に必要な SSM ドキュメントパラメータの値を の形式でカンマ (,) Parameter=Value で区切って入力します。各チェックの関連する SSM ドキュメントでサポートされている事前設定済みパラメータ[Trusted Advisor Trusted Remediator でサポートされている チェック](#)については、「」を参照してください。
- alternative-automation-document: この属性は、既存のオートメーションドキュメントをサポートされている別のドキュメント (特定のチェックで利用可能な場合) で上書きするのに役立ちます。デフォルトでは、この属性は選択されていません。

**Note**

alternative-automation-document 属性はカスタムオートメーションドキュメントをサポートしていません。にリストされている既存のサポートされている Trusted Remediator オートメーションドキュメントを使用できます [Trusted Advisor Trusted Remediator](#) でサポートされている [チェック](#)。

たとえば、チェック には Qch7DwouX1、AWSManagedServices-StopEC2InstanceAWSManagedServices-ResizeInstanceByOneLevel、AWSManagedServices-TerminateInstance の 3 つの関連 SSM ドキュメントがあります。の値は、AWSManagedServices-ResizeInstanceByOneLevel または AWSManagedServices-TerminateInstance (AWSManagedServices-StopEC2Instance は を修復するデフォルトの SSM ドキュメントです Qch7DwouX1) のいずれか alternative-automation-document です。

各属性の値は、その属性の制約と一致する必要があります。

**Tip**

Trusted Advisor チェックにデフォルト設定を適用する前に、以下のセクションで説明する リソースタグ付けとリソースオーバーライド機能の使用を検討することをお勧めします。デフォルト設定はアカウント内のすべてのリソースに適用されますが、必ずしも望ましくない場合があります。

以下は、実行モードを手動に設定し、制約に一致する属性を持つコンソールのスクリーンショットの例です。

## リソースタグを使用して修復をカスタマイズする

チェック設定の自動 automated-for-tagged-only 属性と manual-for-tagged-only 属性を使用すると、個々のチェックを修復する方法のリソースタグを指定できます。同じタグを共有するリソースのグループに一貫した修復動作を適用する必要がある場合は、この方法を使用することをお勧めします。これらのタグの説明を次に示します。

- `automated-for-tagged-only`: デフォルトの実行モードに関係なく、チェックが自動的に修正するリソースタグ (1 つ以上のタグペア、カンマ区切り) を指定します。
- `manual-for-tagged-only`: デフォルトの実行モードに関係なく、手動で実行する必要がある修復のリソースタグ (1 つ以上のタグペア、カンマ区切り) を指定します。

たとえば、すべての非本番稼働用リソースの自動修復を有効にし、本番稼働用リソースに手動修復を適用する場合は、次のように設定します。

```
"execution-mode": "Conditional",  
"automated-for-tagged-only": "Environment=Non-Production",  
"manual-for-tagged-only": "Environment=Production",
```

前述の設定をリソースに設定すると、修復動作は次のようになります。

- 「`Environment=Non-Production`」でタグ付けされたリソースは自動的に修正されます。
- 「`Environment=Production`」でタグ付けされたリソースには、修復のための手動介入が必要です。
- 「環境」タグのないリソースは、デフォルトの実行モード (この場合は「条件付き」) に従います。したがって、残りのリソースに対してアクションは実行されません。

設定の追加サポートについては、Cloud Architect にお問い合わせください。

## リソースオーバーライドタグを使用して修復をカスタマイズする

リソースオーバーライドタグを使用すると、タグに関係なく、個々のリソースの修復動作をカスタマイズできます。リソースに特定のタグを追加することで、そのリソースのデフォルトの実行モードと Trusted Advisor チェックを上書きします。リソースオーバーライドタグは、デフォルト設定とリソースタグ付け設定よりも優先されます。したがって、リソースオーバーライドタグを使用してリソースのデフォルトの実行モードを自動、手動、または条件付きに設定すると、デフォルトの実行モードとリソースのタグ付け設定が上書きされます。

リソースの実行モードを上書きするには、次の手順を実行します。

1. 修復設定を上書きするリソースを特定します。
2. 上書きする Trusted Advisor チェックのチェック ID を決定します。サポートされているチェック IDs は、[にあります Trusted Advisor Trusted Remediator でサポートされている チェック](#)。  
Trusted Advisor

3. タグ | [更新またはタグ](#) | [一括更新](#) の変更タイプを使用して、次のキーと値を持つタグをリソースに追加します。

- タグキー: TR-*Trusted Advisor check ID*-Execution-Mode (大文字と小文字を区別)

前述のタグキーの例では、 を上書きする Trusted Advisor チェックの一意の識別子 Trusted Advisor check ID に置き換えます。

- タグ値: タグ値には次のいずれかの値を使用します。
  - 自動: Trusted Remediator は、この Trusted Advisor チェックのリソースを自動的に修復します。
  - 手動: リソースに対して OpsItem が作成されますが、修復は自動的に実行されません。自動を使用して修復を確認して実行します。詳細については、「[Trusted Remediator で修復を操作する](#)」を参照してください。
  - 非アクティブ: このリソースと指定された Trusted Advisor チェックでは、修復と OpsItem の作成は実行されません。

たとえば、Trusted Advisor チェック ID を使用して Amazon EBS ボリュームを自動的に修復するには、EBS ボリュームにタグ DAvU99Dc4C を追加します。タグキーは TR-DAvU99Dc4C-Execution-Mode で、タグ値は です Automated。

タグセクションを示すコンソールの例を次に示します。

## 実行モード決定ワークフロー

リソースと各 Trusted Advisor チェックの実行モードを設定するには、複数のレベルがあります。次の図は、信頼された修復者が設定に基づいて使用する実行モードを決定する方法を示しています。

## 修復チュートリアルを設定する

次のチュートリアルでは、信頼された修復ツールで一般的な修復を作成する例を示します。

### すべてのリソースを手動で修復する

この例では、Trusted Advisor チェック ID DAvU99Dc4C (使用率の低い Amazon EBS ボリューム) を持つすべての Amazon EBS ボリュームの手動修復を設定します。

## チェック ID DAvU99Dc4C を使用して Amazon EBS ボリュームの手動修復を設定する

1. 修正設定|更新、変更タイプを使用して設定更新をリクエストします。
2. 以下のパラメータを入力します。
  - CheckIds: DAvU99Dc4C
  - ExecutionMode: 手動

### Note

1 つのリクエストで複数のチェックを設定できます。同じ設定を必要とするチェックの場合は、CheckIds パラメータに複数のチェック IDs を含めます。CheckIds 別の設定を必要とするチェックについては、新しい RemediationConfiguration オブジェクトを作成します。

3. RFC を送信します。

## 選択したリソースを除くすべてのリソースを自動的に修復する

この例では、Trusted Advisor チェック ID DAvU99Dc4C (使用率の低い Amazon EBS ボリューム) を持つすべての Amazon EBS ボリュームの自動修復を設定します。ただし、修正されない指定されたボリューム (非アクティブと指定) を除きます。

選択した非アクティブなリソースを除き、チェック ID DAvU99Dc4C を使用して Amazon EBS ボリュームの自動修復を設定する

1. 選択した Amazon EBS ボリュームの自動修復を上書きします。

[タグ | 更新](#)または[タグ | 一括更新](#)の変更タイプを使用して、自動修復から除外するボリュームに次のタグを適用します。

- キー: TR-DAvU99Dc4C-Execution-Mode
  - 値: 非アクティブ
2. 修正設定|更新変更タイプを使用して、設定の更新をリクエストします。
  3. 以下のパラメータを入力します。
    - CheckIds: DAvU99Dc4C



- ExecutionMode: 自動

#### 4. RFC を送信します。

### タグ付きリソースを自動的に修復する

この例では、Trusted Advisor チェック ID DAvU99Dc4C (使用率の低い Amazon EBS ボリューム) を持つタグStage=NonProdを持つすべての Amazon EBS ボリュームの自動修復を設定します。このタグのない他のすべてのリソースは修復されません。

チェック ID DAvU99Dc4C **Stage=NonProd**の タグを使用して Amazon EBS ボリュームの自動修復を設定する

1. [修正設定 | 更新](#)、変更タイプを使用して設定の更新をリクエストします。
2. 以下のパラメータを入力します。

- CheckIds: DAvU99Dc4C
- ExecutionMode: 条件付き
- AutomatedForTaggedOnly: {"Stage"NonProd"}

#### Note

AutomatedForTaggedOnly パラメータに指定された値は、以前に設定された値を上書きします。既存のタグを保持するには、新しい値にタグを含めます。

#### 3. RFC を送信します。

### 設定をデフォルトにリセットする

この例では、チェック Hs4Ma3G104 の既存のautomated-for-tagged-only設定を削除します。以前に適用したタグ設定を削除するには、AutomatedForTaggedOnly パラメータ値を {} に設定します。

Hs4Ma3G104 チェックの設定をデフォルトにリセットする

1. [修復設定 | 更新](#)変更タイプを使用して、設定の更新をリクエストします。
2. 以下のパラメータを入力します。

- CheckIds: Hs4Ma3G104

- ExecutionMode: 現在使用されている値を入力します
- AutomatedForTaggedOnly: {}

3. RFC を送信します。

## Trusted Remediator で修復を操作する

### Trusted Remediator で修復を追跡する

OpsItems の修復を追跡するには、次の手順を実行します。

1. <https://console.aws.amazon.com/systems-manager/> で AWS Systems Manager コンソールを開きます。
2. オペレーション管理、OpsCenter を選択します。
3. (オプション) Source=Trusted Remediator でリストをフィルタリングして、リストに Trusted Remediator OpsItems のみを含めます。

Source=Trusted Remediator でフィルタリングされた OpsCenter 画面の例を次に示します。

#### Note

OpsCenter から OpsItems を表示するだけでなく、AMS S3 バケットで修復ログを表示できます。OpsCenter 詳細については、「[Trusted Remediator の修復ログ](#)」を参照してください。

### 信頼できる修復ツールで手動修復を実行する

Trusted Remediator は、手動修復用に設定されたチェックの OpsItems を作成します。これらのチェックを確認し、修復プロセスを手動で開始する必要があります。

OpsItem を手動で修正するには、次の手順を実行します。

1. <https://console.aws.amazon.com/systems-manager/> で AWS Systems Manager コンソールを開きます。
2. オペレーション管理、OpsCenter を選択します。

3. (オプション) Source=Trusted Remediator でリストをフィルタリングして、リストに Trusted Remediator OpsItems のみを含めます。
4. 確認する OpsItem を選択します。
5. OpsItem の運用データを確認します。運用データには以下の項目が含まれます。
  - trustedAdvisorCheckCategory: Trusted Advisor チェック ID のカテゴリ。例えば、耐障害性
  - trustedAdvisorCheckId: 一意の Trusted Advisor チェック ID。
  - trustedAdvisorCheckMetadata: リソース ID を含むリソースメタデータ。
  - trustedAdvisorCheckName: Trusted Advisor チェックの名前。
  - trustedAdvisorCheckStatus: リソースに対して検出された Trusted Advisor チェックのステータス。
  - trustedAdvisorCheckManualRemediation: 手動修復のリファレンスの詳細を提供するカスタムデータ。
    - ManualExecutionInput: 手動修復を実行するときに値を変更できるパラメータを定義するオブジェクト。
      - DocumentName: ランブック (SSM ドキュメント) の名前。
      - CustomizableParameters: 変更できるパラメータ名。
    - DefaultInput: 手動修復に使用するパラメータ名と値を定義するオブジェクト。値は、事前設定されたパラメータに基づいて入力されます。
6. OpsItem を手動で修正するには、次の手順を実行します。
  - a. [信頼できる修復器を使用する | 検出結果 | 修正 ct-1c7ch8z5phrjp](#) 変更タイプ
  - b. パラメータで以下の値を使用します。
    - DocumentName: である必要がありますAWSManagedServices-RemediateTrustedRemediatorFinding。
    - リージョン: us-east-1 AWS リージョン形式の。
    - パラメータ: 手動修復パラメータを入力します。
      - OpsItemId: Ops 項目の ID。
      - RemediationDocumentName: 使用する SSM オートメーションドキュメントの名前。ドキュメントは Ops 項目に関連付ける必要があります。複数のドキュメントが Ops 項目に関連付けられている場合は、DocumentName を指定する必要があります。
      - RemediationParameters: 自動化実行のパラメータのキー/値のマップ。形式はで

[\"*ParameterValue2*\"]}。Ops Item trustedAdvisorCheckManualRemediation CustomizableParameters に存在するパラメータのみを使用できます。指定しない場合、パラメータと値は Ops 項目から取得されます。

- c. [Run] (実行) を選択します。エラーがない場合、RFC が正常に作成されたページに、送信された RFC の詳細と最初の実行出力が表示されます。
- d. RFC 実行の進行状況をモニタリングします。
- e. 実行が完了すると、OpsItem が解決されます。RFC が失敗した場合は、「」の手順に従ってください [Trusted Remediator での修復のトラブルシューティング](#)。トラブルシューティングのサポートの詳細については、AMS にお問い合わせください。

## Trusted Remediator での修復のトラブルシューティング

手動修復と修復の失敗に関するサポートについては、AMS にお問い合わせください。

修復のステータスと結果を表示するには、次の手順を実行します。

1. <https://console.aws.amazon.com/systems-manager/> で AWS Systems Manager コンソールを開きます。
2. オペレーション管理、OpsCenter を選択します。
3. (オプション) Source=Trusted Remediator でリストをフィルタリングして、リストに Trusted Remediator OpsItems のみを含めます。
4. 確認する OpsItem を選択します。
5. Automation Executions セクションで、ドキュメント名とステータス、および結果を確認します。
6. 以下の一般的な自動化の失敗を確認します。ここに問題が表示されない場合は、CSDM に連絡してサポートを依頼してください。

### 一般的な修復エラー

#### Automation Executions に実行が表示されない

OpsItem に関連付けられた実行は、パラメータ値が正しくないために実行が開始されなかったことを示している可能性があります。

#### トラブルシューティングのステップ

1. 運用データで、trustedAdvisorCheckAutoRemediationプロパティ値を確認します。

2. DocumentName と Parameters の値が正しいことを確認します。正しい値[Trusted Remediator で Trusted Advisor チェック修復を設定する](#)については、「」で SSM パラメータの設定方法の詳細を確認してください。サポートされているチェックパラメータを確認するには、「」を参照してください。[Trusted Advisor Trusted Remediator でサポートされている チェック](#)
3. SSM ドキュメントの値が許可されたパターンと一致することを確認します。ドキュメントコンテンツでパラメータの詳細を表示するには、ランブックセクションでドキュメント名を選択します。
4. パラメータを確認して修正したら、OpsItem を手動で修復します。修復手順については、「」を参照してください[信頼できる修復ツールで手動修復を実行する](#)。
5. このエラーが繰り返し発生するのを防ぐには、設定で正しいパラメータ値を使用して修復を設定してください。詳細については、[Trusted Remediator で Trusted Advisor チェック修復を設定する](#)を参照してください。

## 自動化の実行で失敗した実行

修復ドキュメントには、API によるさまざまなアクション AWS のサービスの実行とやり取りする複数のステップが含まれています。APIs 失敗の特定の原因を特定するには、次の手順を実行します。

## トラブルシューティングのステップ

1. 個々の実行ステップを表示するには、Automation Executions セクションの「実行 ID」、「リンク」を選択します。以下は、選択したオートメーションの実行ステップを示す Systems Manager コンソールの例です。

2. 失敗ステータスのステップを選択します。エラーメッセージの例を次に示します。

- NoSuchBucket - An error occurred (NoSuchBucket) when calling the GetPublicAccessBlock operation: The specified bucket does not exist

このエラーは、修復設定の事前設定済みパラメータで誤ったバケット名が指定されたことを示します。

このエラーを解決するには、[正しいバケット名を使用して自動化を手動で実行](#)します。この問題が繰り返し発生するのを防ぐには、[修復設定を正しいバケット名で更新](#)します。

- DB instance my-db-instance-1 is not in available status for modification.

このエラーは、DB インスタンスが無効な状態にあるため、オートメーションが予想される変更を実行できなかったことを示します。

このエラーを解決するには、[オートメーションを手動で実行します](#)。

## Trusted Remediator の修復ログ

Trusted Remediator は JSON 形式でログを作成し、Amazon Simple Storage Service にアップロードします。ログファイルは AMS によって作成され、という名前の S3 バケットにアップロードされます `ams-trusted-remediator-{your-account-id}-logs`。AMS は、委任管理者アカウントに S3 バケットを作成します。ログファイルを Quick にインポートして、カスタマイズされた修復レポートを生成できます。

### 修復項目ログ

Trusted Remediator は、修復 OpsItem の作成 Remediation item log 時にを作成します。このログには、手動修復 OpsItem と自動修復 OpsItem が含まれています。を使用して Remediation item log、すべての修復の概要を追跡できます。

Compute Optimizer レコメンデーションの修復項目ログの場所

```
s3://ams-trusted-remediator-delegated-administrator-account-id-logs/  
compute_optimizer_remediation_items/remediation creation time in yyyy-mm-dd  
format/10 digits epoch time or unix timestamp-Compute Optimizer check ID-  
Resource ID.json
```

Trusted Advisor チェックの修復項目ログの場所

```
s3://ams-trusted-remediator-delegated-administrator-account-id-logs/  
remediation_items/remediation creation time in yyyy-mm-dd format/10 digits  
epoch time or unix timestamp-Trusted Advisor check ID- Resource ID.json
```

Security Hub CSPM レコメンデーションの修復項目ログの場所

```
s3://ams-trusted-remediator-delegated-administrator-account-id-logs/  
security_hub_remediation_items/remediation creation time in yyyy-mm-dd  
format/10 digits epoch time or unix timestamp-Security Hub CSPM check ID-  
Resource ID.json
```

修復項目ログファイル URL

```
s3:///ams-trusted-remediator-111122223333-logs/
remediation_items/2023-02-06/1675660464-DAvU99Dc4C-
vol-00bd8965660b4c16d.json
```

### Compute Optimizer 修復項目のログ形式

```
{
  "AccountID": "Account_ID",
  "ComputeOptimizerCheckID": "Compute Optimizer check ID",
  "ComputeOptimizerCheckName": "Compute Optimizer check name",
  "ResourceID": "Resource ID",
  "RemediationTime": Remediation creation time,
  "ExecutionMode": "Automated or Manual",
  "OpsItemID": "OpsItem ID"
}
```

### Trusted Advisor 修復項目のログ形式

```
{
  "TrustedAdvisorCheckID": Trusted Advisor check ID,
  "TrustedAdvisorCheckName": Trusted Advisor check name,
  "TrustedAdvisorCheckResultTime": 10 digits epoch time or unix timestamp,
  "ResourceID": Resource ID,
  "RemediationTime": Remediation creation time,
  "ExecutionMode": Automated or Manual,
  "OpsItemID": OpsItem ID
}
```

### Security Hub CSPM 修復項目のログ形式

```
{
  "AccountID": "Account_ID",
  "SecurityHubCheckID": "Security Hub check ID",
  "SecurityHubCheckName": "Security Hub check name",
  "ResourceID": "Resource ID",
  "RemediationTime": Remediation creation time,
  "ExecutionMode": "Automated or Manual",
  "OpsItemID": "OpsItem ID"
}
```

### Compute Optimizer 修復項目ログ形式のサンプルコンテンツ



```
{
  "AccountID": "123456789012",
  "ComputeOptimizerCheckID": "compute-optimizer-ebs",
  "ComputeOptimizerCheckName": "EBS volumes",
  "ResourceID": "vol-1235589366f77aca7",
  "RemediationTime": 1755044783,
  "ExecutionMode": "Manual",
  "OpsItemID": "oi-b8888b38fe78"
}
```

## Trusted Advisor 修復項目ログ形式のサンプルコンテンツ

```
{
  "TrustedAdvisorCheckID": "DAvU99Dc4C",
  "TrustedAdvisorCheckName": "Underutilized Amazon EBS Volumes",
  "TrustedAdvisorCheckResultTime": 1675614749,
  "ResourceID": "vol-00bd8965660b4c16d",
  "RemediationTime": 1675660464,
  "OpsItemID": "oi-cca5df7af718"
}
```

## Security Hub CSPM 修復項目ログ形式のサンプルコンテンツ

```
{
  "AccountID": "012345678901",
  "SecurityHubControlID": "security-hub-lambda-7",
  "SecurityHubControlName": "Lambda functions should have AWS X-Ray active tracing enabled",
  "SecurityHubControlResultTime": 1764580147,
  "ResourceID": "test-lambda-7-xray-disabled",
  "RemediationTime": 1764900171,
  "ExecutionMode": "Manual",
  "OpsItemID": "oi-ea12c3456d7f"
}
```

## 自動修復実行ログ、Compute Optimizer、Security Hub CSPM、および Trusted Advisor

Trusted Remediator は、自動 SSM ドキュメント実行が完了すると Automated remediation execution log を作成します。このログには、自動修復 OpsItem の SSM 実行の詳細のみが含まれます。このログファイルを使用して、自動修復を追跡できます。

## Compute Optimizer 自動修復ログの場所

```
s3://ams-trusted-remediator-delegated-administrator-account-id-logs//  
remediation_executions/remediation creation time in yyyy-mm-dd format/10  
digits epoch time or unix timestamp-Compute Optimizer recommendation  
ID.json
```

## Security Hub CSPM 自動修復ログの場所

```
s3://ams-trusted-remediator-delegated-administrator-account-id-logs//  
remediation_executions/remediation creation time in yyyy-mm-dd format/10  
digits epoch time or unix timestamp-Security Hub CSPM recommendation  
ID.json
```

## Trusted Advisor 自動修復ログの場所

```
s3://ams-trusted-remediator-delegated-administrator-account-id-logs//  
remediation_executions/remediation creation time in yyyy-mm-dd format/10  
digits epoch time or unix timestamp-Trusted Advisor check ID-Resource  
ID.json
```

## Compute Optimizer 自動修復ログの場所の例

```
s3://ams-trusted-remediator-111122223333-logs/  
remediation_executions/2025-06-26/1750908858-123456789012-compute-  
optimizer-ec2-i-1235173471d2cd789.json
```

## Security Hub CSPM 自動修復ログの場所の例

```
s3://ams-trusted-remediator-111122223333-logs/  
remediation_executions/2025-06-26/763247655-066028476520-security-hub-  
rds-8-miz-tr-sh-test-rds-instance-1.json
```

## Trusted Advisor 自動修復ログの場所の例

```
s3://ams-trusted-remediator-111122223333-logs/  
remediation_executions/2023-02-06/1675660573-DAvU99Dc4C-  
vol-00bd8965660b4c16d.json
```

## 自動修復ログ形式のサンプルコンテンツ

```
{
```

```
"OpsItemID": "oi-767c77e05301",  
"SSMExecutionID": "93d091b2-778a-4cbc-b672-006954d76b86",  
"SSMExecutionStatus": "Success"  
}
```

## Trusted Remediator のベストプラクティス

以下は、信頼できる修復の使用に役立つベストプラクティスです。

- 修復結果が不明な場合は、手動実行モードで開始します。最初から修復の自動実行を適用すると、予期しない結果が発生することがあります。
- 修復と OpsItems を毎週レビューして、信頼された修復の結果に関するインサイトを取得します。
- メンバーアカウントは、委任管理者アカウントから設定を継承します。したがって、同じ設定で複数のアカウントを管理するのに役立つようにアカウントを構造化することが重要です。タグを使用して、デフォルト設定からリソースを除外できます。

## 信頼できる修復に関するFAQs

以下は、信頼できる修復業者に関するよくある質問です。

Trusted Remediator とは何ですか？また、どのようにメリットがありますか？

コンプライアンス違反が Compute Optimizer Trusted Advisor または Security Hub CSPM によって特定された場合、またはレコメンデーションが Compute Optimizer または Security Hub CSPM によって発行された場合、Trusted Remediator は、修復の適用、手動修復による承認の取得、または今後の月次ビジネスレビュー (MBR) 中の修復の報告のいずれかにより、指定された設定に従って応答します。修復は、希望する修復時間またはスケジュールで行われます。Trusted Remediator は、Trusted Advisor チェックを個別にまたは一括で設定および修正できる柔軟性を備え、セルフサービスでチェックに対応する機能を提供します。テスト済みの修復ドキュメントのライブラリにより、AMS は安全チェックを適用して AWS ベストプラクティスに従うことで、アカウントを常に引き上げます。設定で指定する場合にのみ通知されます。AMS ユーザーは、追加料金なしで信頼された修復者にオプトインできます。

Trusted Remediator は、他の とどのように関連し、連携しますか AWS のサービス？

既存のエンタープライズサポートプランの一部として、Trusted Advisor チェック、Compute Optimizer の推奨事項、Security Hub CSPM コントロールにアクセスできます。Trusted Remediator は Trusted Advisor、Compute Optimizer、および Security Hub CSPM と統合して、既存の AMS 自動化機能を活用します。具体的には、AMS は自動修復に AWS Systems Manager 自動化ドキュ

メント (ランブック) を使用します。AWS AppConfig は修復ワークフローの設定に使用されます。Systems Manager OpsCenter を使用して、現在および過去のすべての修復を表示できます。修復ログは Amazon S3 バケットに保存されます。ログを使用して、Quick でカスタムレポートダッシュボードをインポートおよび構築できます。

修復を設定するのは誰ですか？

アカウントの設定を所有している。設定の管理はお客様の責任となります。設定の変更、サポート、手動修復、修復失敗のトラブルシューティングについては、AMS に問い合わせることもできます。

SSM オートメシヨンドキュメントをインストールするにはどうすればよいですか？

SSM オートメシヨンドキュメントは、オンボードされた AMS アカウントに自動的に共有されます。

AMS 所有のリソースも修復されますか？

AMS 所有のリソースは、信頼できる修復者によってフラグが付けられません。Trusted Remediator は、リソースのみに焦点を当てています。

Trusted Remediator AWS リージョン とは何ですか？ 誰が使用できますか？

Trusted Remediator は、AMS Advanced のお客様にご利用いただけます。サポートリージョンの現在のリストについては、[AWS のサービス「リージョン別」](#)を参照してください。

Trusted Remediator はリソースドリフトを引き起こしますか？

SSM オートメシヨンドキュメントは AWS API を介してリソースを直接更新するため、リソースドリフトが発生する可能性があります。タグを使用して、既存の CI/CD パッケージを通じて作成されたリソースを分離できます。他のリソースを修復しながら、タグ付けされたリソースを無視するように信頼された修復を設定できます。

信頼できる修復を一時停止または停止するにはどうすればよいですか？

[管理 | 信頼できる修復 | 状態 | 変更タイプを有効または無効に](#)して、信頼できる修復サービスを停止します。同じ変更タイプを使用して、信頼された修復を再度有効にします。

Trusted Remediator でサポートされていないチェックを修正するにはどうすればよいですか？

サポートされていないチェックについては、Operations On Demand (OOD) を通じて AMS に引き続き問い合わせることができます。AMS は、これらのチェックの修正を支援します。詳細については、[「Operations On Demand」](#)を参照してください。

Trusted Remediator はどのリソースをアカウントにデプロイしますか？

Trusted Remediator は、Trusted Remediator の委任された管理者アカウントに次のリソースをデプロイします。

- `ams-trusted-remediator-{your-account-id}-logs` という名前の Amazon S3 バケット。Trusted Remediator は、修復 OpsItem の作成時に Remediation item log JSON 形式で作成し、ログファイルをこのバケットにアップロードします。
- サポートされている Trusted Advisor チェック、Compute Optimizer、Security Hub CSPM レコメンデーションの修正設定を保持する AWS AppConfig アプリケーション。

Trusted Remediator は、Trusted Remediator メンバーアカウントにリソースをデプロイしません。

# ログ管理

## トピック

- [ログ管理とは](#)
- [AMS ログ記録の仕組み](#)
- [ログのアクセス](#)
- [ログ設定のカスタマイズ](#)

AMS ログ管理は、マネージドアカウントからログの保持を収集、集約、制御します。AWS ログ管理は、アカウント内にデプロイされた Amazon EC2 インスタンスと AWS リソースからのログを CloudWatch Logs に集約します。ログが現在集約されているサービスの詳細なリストは、「」で確認できます[AMS 集計サービスログ](#)。

## ログ管理とは

ログ管理は、インスタンス、アプリケーション、AWS のサービスによって生成されたログイベントを処理するプロセスです。この機能は、AMS がマネージド AWS アカウントで生成されたログイベントを処理、保存、ローテーションする方法を定義します。インフラストラクチャログは、インシデント解決中およびシステム監査をサポートするために使用されます。

## AMS ログ記録の仕組み

AMS シングルアカウントランディングゾーン (SALZ) ログ管理は、インスタンスとアプリケーションがオンボードまたはプロビジョニングされたときに実装される、プリインストールされたさまざまなエージェントとツールを使用します。

ログ記録は、アカウントのオンボーディングプロセス中およびスタックの起動時に設定されます。

インスタンスと AWS のサービスによって生成された AMS マルチアカウントランディングゾーン (MALZ) ログは、AMS が管理する各アカウント内の CloudWatch Logs または Amazon Simple Storage Service (Amazon S3) で利用できます。AMS マルチアカウントランディングゾーンは、個々のアプリケーションアカウントによって生成される一部のログの中央集約場所として機能する中央ログアカウントを提供します。

[ログのアクセス](#) サブセクションの表では、個々のアカウントで利用できるログと、中央のログ記録アカウントで利用できるログについて説明します。

# ログのアクセス

ログにアクセスするには、必要な IAM ロールのいずれかがあり、AMS アカウントにあることを確認します。次に、表示されているディレクトリに移動します。

## Multi-Account Landing Zone (MALZ)

5 つのデフォルトの IAM ロールを提供します。各ロールは、アカウント内のすべてのログへのアクセスを許可します (すべての先頭に `が付きますAWSManagedServices`)。

- AdminRole
- CaseRole
- ChangeManagementRole
- ReadOnlyRole
- SecurityOpsRole

これらのロールへのアクセスはフェデレーションを介して設定され、各ロールは Active Directory ドメイン内のグループにマッピングされます。

これらのロールの詳細については、「」を参照してください [AMS の IAM ユーザーロール](#)。

## Single-Account Landing Zone (SALZ)

AMS シングルアカウントランディングゾーン `Customer_ReadOnly_Role` のデフォルトは、アカウント内のすべてのログへのアクセスを許可します。ログへのアクセスは、Active Directory グループにマッピングされた AWS Identity and Access Management (IAM) ロールを使用して制御されます。

# AMS 集計サービスログ

各 AWS サービスは、CloudWatch Logs または Amazon S3 バケット内の特定の場所にログ記録します。

### Note

特に明記されていない限り、すべてのログの場所はログを生成したアカウントにローカルであり、中央のログ記録アカウントに集約されません。



SALZ および MALZ アカウントでデフォルトの AMS CloudTrail 証跡名を検索するには、CloudTrail の AWS コンソールに移動し、証跡ページに移動して AMS を検索します。AMS リソースにはタグがあるため、この方法で証跡を見つけることができます。AMS CloudTrail タグの例：

```
Environment    AMSInfrastructure
```

ログにアクセスするには、必要な IAM ロールのいずれかがあり、AMS アカウントにあることを確認します。次に、表示されているディレクトリに移動します。

Multi-Account Landing Zone

AMS マルチアカウントランディングゾーン集約サービスログ

|   | サービス名                    | ログの詳細            | ログの場所                                                                                                                                                                                                                                                                                                                                                                  |
|---|--------------------------|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Amazon Aurora            | 全般、スロークエリ、エラーログ。 | CloudWatch LogGroup: /aws/rds/cluster/{ <i>database_name</i> }/{ <i>log_name</i> }                                                                                                                                                                                                                                                                                     |
| 2 | AWS CloudFormation (CFN) | API コールのログ記録のみ。  | <div>AWS CloudFormation API コールは CloudTrail を介して文書化されます。CloudTrail はログを CloudWatch LogGroup に送信し、ログを S3 バケットに同期します。ログはデフォルトで CloudWatch LogGroup に 14 日間保持され、S3 バケットに無期限に保持されます。</div> <div>CloudWatch LogGroup: /CloudTrail/Landing-Zone-Logs</div> <div>S3 バケット [中央ログ記録アカウント内]: aws-landing-zone-logs-ams-a{<i>account_ID</i> }-log-management-{<i>region</i>}</div> |

|   | サービス名                                     | ログの詳細                                                                                                                  | ログの場所                                                                                                                                                                                           |
|---|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|   |                                           |                                                                                                                        | パス: /AWSLogs/{ <i>account_ID</i> }/<br>CloudTrail/                                                                                                                                              |
| 3 | Amazon CloudFront (CloudFront)            | ユーザーリクエストのログ記録。CloudFront ログ記録は明示的に有効にする必要があります。詳細については、「 <a href="#">サポートされているサービスのログ記録の有効化</a> 」を参照してください。           | S3 バケット: <i>ams-a{account_ID }-log-management-{region}</i><br><br>パス: AWS/RedShift/{ <i>CloudFront ##### ID</i> }                                                                               |
| 4 | Amazon CloudWatch (CloudWatch)            | API コールのログ記録のみ。                                                                                                        | CloudWatch LogGroup: /CloudTrail/Landing-Zone-Logs<br><br>S3 バケット [中央ログ記録アカウント内]: <i>aws-landing-zone-logs-{account_ID }-{region}</i><br><br>パス: /AWSLogs/{ <i>account_ID</i> }/<br>CloudTrail/ |
| 5 | Amazon Elastic Block Store (Amazon EBS)   | EBS サービスによってログは生成されません。                                                                                                | 該当しない                                                                                                                                                                                           |
| 6 | Amazon Elastic Compute Cloud (Amazon EC2) | システムログとアプリケーションログ。<br><br>詳細については、「 <a href="#">Amazon Elastic Compute Cloud (Amazon EC2) - システムレベルのログ</a> 」を参照してください。 | CloudWatch Logs: /{ <i>##### ID</i> }                                                                                                                                                           |

|   | サービス名                                   | ログの詳細                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | ログの場所                                                                                                                                                                                                                                                                                                                                     |
|---|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 7 | Amazon Elastic File System (Amazon EFS) | API コールのログ記録のみ。                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <p>CloudWatch LogGroup: /CloudTrail/Landing-Zone-Logs</p> <p>S3 バケット [中央ログ記録アカウント内]: aws-landing-zone-logs-<br/>{<i>account_ID</i>}-{<i>region</i>}</p> <p>パス: /AWSLogs/{<i>account_ID</i> }/<br/>CloudTrail/</p>                                                                                                                         |
| 8 | Elastic Load Balancing (ELB)            | <p>アクセスログエントリとエラーログエントリ。</p> <p>Elastic Load Balancer は、バックエンドインスタンスにルーティングされないリクエストを含め、送信されたすべてのリクエストを記録します。たとえば、クライアントが不正な形式のリクエストを送信した場合や、応答する正常なインスタンスがない場合でも、リクエストはログに記録されます。</p> <p>Elastic Load Balancing ログエントリの詳細については、「」を参照してください。</p> <ul style="list-style-type: none"> <li>Classic Load Balancer: <a href="#">ログエントリにアクセスします。</a></li> <li>Application Load Balancer: <a href="#">ログエントリにアクセスします。</a></li> <li>Network Load Balancer: <a href="#">ログエントリにアクセスします。</a></li> </ul> | <p>API コールログ :</p> <p>CloudWatch LogGroup: /CloudTrail/Landing-Zone-Logs</p> <p>S3 バケット [中央ログ記録アカウント内]: aws-landing-zone-logs-<br/>{<i>account_ID</i>}-{<i>region</i>}</p> <p>パス: /AWSLogs/{<i>account_ID</i> }/<br/>CloudTrail/</p> <p>アクセスログ:</p> <p>S3 バケット: mc-a{<i>account_ID</i> }-logs{<i>region</i>}</p> <p>パス: aws/elbaccess</p> |

|    | サービス名                                                      | ログの詳細                                                                                                                                                                             | ログの場所                                                                                                                                                                                                             |
|----|------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9  | Amazon<br>OpenSearch<br>Service<br>(OpenSearch<br>Service) | <p>サービスエラーログ。</p> <p>OpenSearch ログ記録を明示的に有効にする必要があります。詳細については、「<a href="#">サポートされているサービスのログ記録の有効化</a>」を参照してください。</p>                                                              | <p>CloudWatch LogGroup: /CloudTrail/Landing-Zone-Logs</p> <p>S3 バケット [中央ログ記録アカウント内]: aws-landing-zone-logs-<br/>{<i>account_ID</i>}-{<i>region</i>}</p> <p>パス: /AWSLogs/{<i>account_ID</i> }/<br/>CloudTrail/</p> |
| 10 | Amazon<br>ElastiCache                                      | API コールのログ記録のみ。                                                                                                                                                                   | CloudWatch LogGroup: //CloudTrail/Landing-Zone-Logs                                                                                                                                                               |
| 11 | Amazon<br>GuardDuty                                        |                                                                                                                                                                                   | S3 バケット [中央ログ記録アカウント内]: aws-landing-zone-logs-<br>{ <i>account_ID</i> }-{ <i>region</i> }                                                                                                                         |
| 12 | Amazon<br>Inspector                                        |                                                                                                                                                                                   | パス: /AWSLogs/{ <i>account_ID</i> }/<br>CloudTrail/                                                                                                                                                                |
| 13 | Amazon Macie                                               |                                                                                                                                                                                   |                                                                                                                                                                                                                   |
| 14 | Amazon<br>Redshift                                         | <p>接続、ユーザー、アクティビティログ。</p> <p>ログ記録は、Redshift クラスターの作成 CT (ct-1malj7snzxrkr) を呼び出して Redshift クラスターを作成すると、デフォルトで有効になります。</p> <p>詳細については、「<a href="#">データベース監査ログ記録</a>」を参照してください。</p> | <p>S3 バケット: ams-a{<i>account_ID</i> }-log-management-{<i>region</i>}</p> <p>パス: /AWS/RedShift/{<i>CloudFront ##### ID</i> }</p>                                                                                   |

|    | サービス名                                    | ログの詳細                                                                                                                                                                                                                                                                  | ログの場所                                                                                                                                                                                                                                                                          |
|----|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 15 | Amazon Relational Database Service (RDS) | <p>データベースタイプに固有のログ。</p> <p>RDS ログ記録を明示的に有効にする必要があります。詳細については、「<a href="#">サポートされているサービスのログ記録の有効化</a>」を参照してください。</p> <p>MSSQL ログにはストアドプロシージャを介してのみアクセスできます。詳細については、「<a href="#">ログファイルのアーカイブ</a>」を参照してください。</p>                                                         | <p>CloudWatch LogGroup:</p> <p><code>/aws/rds/(#####または#####)/{<i>database_name</i> }/{<i>log_name</i>}</code></p>                                                                                                                                                             |
| 16 | Amazon S3 (S3)                           | <p>バケットアクセスログ。各アクセスログレコードは、リクエスト、バケット名、リクエスト時間、リクエストアクション、レスポンスステータス、エラーコード (存在する場合) など、単一のアクセスリクエストに関する詳細を提供します。アクセスログ情報は、セキュリティとアクセス監査に役立ちます。また、顧客基盤について知り、Amazon S3 の請求を理解することにも役立ちます。</p> <p>S3 アクセスログエントリの詳細については、<a href="#">S3 サーバーアクセスログの形式</a>」を参照してください。</p> | <p>S3 バケット: <code>mc-a{<i>account_ID</i> }-log-management-{<i>region</i>}</code></p> <p>パス: <code>/aws/s3access/{<i>bucket_name</i> }</code></p> <p>S3 バケット [中央ログ記録アカウント内]: <code>aws-landing-zone-s3-access-logs-{<i>account_ID</i> }-{<i>region</i>}</code></p> <p>パス: /</p> |

|    | サービス名                              | ログの詳細                                                       | ログの場所                                                                                                                                                                                                         |
|----|------------------------------------|-------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 17 | Amazon Simple Email Service (SES)  | SES API サービスコール。                                            | CloudWatch LogGroup: /CloudTrail/Landing-Zone-Logs<br><br>S3 バケット [中央ログ記録アカウント内]: aws-landing-zone-logs-<br>{ <i>account_ID</i> }-{ <i>region</i> }<br><br>パス: /AWSLogs/{ <i>account_ID</i> }/<br>CloudTrail/ |
| 18 | Amazon Virtual Private Cloud (VPC) | VPC フローデータ (VPC のネットワークインターフェイスとの間で送受信される IP トラフィックに関する情報)。 | CloudWatch LogGroup:<br><br>/aws/vpcflow/{ <i>VPC_ID</i> }                                                                                                                                                    |
| 19 | Auto Scaling                       | API コールのログ記録のみ。                                             | CloudWatch LogGroup: /CloudTrail/Landing-Zone-Logs                                                                                                                                                            |
| 20 | AWS Certificate Manager            |                                                             | S3 バケット [中央ログ記録アカウント内]: aws-landing-zone-logs-<br>{ <i>account_ID</i> }-{ <i>region</i> }<br><br>パス: /AWSLogs/{ <i>account_ID</i> }/<br>CloudTrail/                                                           |
| 21 | AWS CodeDeploy                     | インスタンス固有のデプロイログ。                                            | インスタンス上                                                                                                                                                                                                       |
| 22 | AWS Config                         | AWS Config API サービスコール。                                     | CloudWatch LogGroup: /CloudTrail/Landing-Zone-Logs<br><br>S3 バケット [中央ログ記録アカウント内]: aws-landing-zone-logs-<br>{ <i>account_ID</i> }-{ <i>region</i> }<br><br>パス: /AWSLogs/{ <i>account_ID</i> }/<br>CloudTrail/ |

|    | サービス名                                 | ログの詳細                                                                                           | ログの場所                                                                                                                                           |
|----|---------------------------------------|-------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
|    |                                       | AWS Config によって追跡されるリソース設定の変更。                                                                  | S3 バケット [中央ログ記録アカウント内]: aws-landing-zone-logs-<br>{ <i>account_ID</i> }-{ <i>region</i> }<br><br>パス: /AWSLogs/{ <i>account_ID</i> }/<br>Config/ |
| 23 | AWS Database Migration Service        | データベース移行ログ。<br><br>詳細については、 <a href="#">AWS Database Migration Service でのログ管理の紹介</a> を参照してください。 | データベース移行コンソール                                                                                                                                   |
| 24 | AWS Direct Connect (DX)               | API コールのログ記録のみ。                                                                                 | CloudWatch LogGroup: /CloudTrail/Landing-Zone-Logs                                                                                              |
| 25 | AWS Glacier                           |                                                                                                 | S3 バケット [中央ログ記録アカウント内]: aws-landing-zone-logs-<br>{ <i>account_ID</i> }-{ <i>region</i> }                                                       |
| 26 | AWS IAM (IAM)                         |                                                                                                 |                                                                                                                                                 |
| 27 | AWS Key Management Service            |                                                                                                 | パス: /AWSLogs/{ <i>account_ID</i> }/<br>CloudTrail/                                                                                              |
| 28 | AWS マネジメントコンソール (コンソールまたは AWS コンソール)  |                                                                                                 |                                                                                                                                                 |
| 29 | AWS Simple Notification Service (SNS) |                                                                                                 |                                                                                                                                                 |
| 30 | AWS Simple Queueing Service (SQS)     |                                                                                                 |                                                                                                                                                 |



## Single-Account Landing Zone

## AMS シングルアカウントランディングゾーン集約サービスログ

|   | サービス名                                          | ログの詳細                                                                                                                | ログの場所                                                                                                                                                                                                                        |
|---|------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Amazon Aurora                                  | 全般、スロークエリ、エラーログ。                                                                                                     | CloudWatch LogGroup: /aws/rds/cluster/{ <i>database_name</i> }/{ <i>log_name</i> }                                                                                                                                           |
| 2 | Amazon CloudFormation (CloudFormation または CFN) | API コールのログ記録のみ。                                                                                                      | CloudFormation API コールは CloudTrail を介して文書化されます。CloudTrail はログを CloudWatch LogGroup に送信し、ログを S3 バケットに同期します。<br><br>CloudWatch LogGroup: /aws/ams/cloudtrail<br><br>S3 バケット: <i>ams-a{account_ID }-log-management-{region}</i> |
| 3 | Amazon CloudFront (CloudFront)                 | ユーザーリクエストのログ記録。<br><br>CloudFront ログ記録を明示的に有効にする必要があります。詳細については、「 <a href="#">サポートされているサービスのログ記録の有効化</a> 」を参照してください。 | S3 バケット: <i>ams-a{account_ID }-log-management-{region}</i><br><br>パス: AWS/RedShift/{ <i>CloudFront_distribution_ID</i> }                                                                                                     |
| 4 | Amazon CloudWatch (CloudWatch)                 | API コールのログ記録のみ。                                                                                                      | CloudWatch LogGroup: /aws/ams/cloudtrail                                                                                                                                                                                     |
| 5 | Amazon Elastic Block Store (EBS)               | EBS サービスによってログは生成されません。                                                                                              | 該当しない                                                                                                                                                                                                                        |

|   | サービス名                                   | ログの詳細                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | ログの場所                                                                                                                                                                        |
|---|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6 | Amazon Elastic Compute Cloud (EC2)      | <p>システムログとアプリケーションログ。</p> <p>詳細については、「<a href="#">Amazon Elastic Compute Cloud (Amazon EC2) - システムレベルのログ</a>」を参照してください。</p>                                                                                                                                                                                                                                                                                                                                                                    | CloudWatch Logs: <code>/instance_<i>ID</i></code>                                                                                                                            |
| 7 | Amazon Elastic File System (Amazon EFS) | API コールのログ記録のみ。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | CloudWatch LogGroup: <code>/aws/ams/cloudtrail</code>                                                                                                                        |
| 8 | Elastic Load Balancing (ELB)            | <p>アクセスログエントリとエラーログエントリ。</p> <p>Elastic Load Balancer は、バックエンドインスタンスにルーティングされないリクエストを含め、送信されたすべてのリクエストを記録します。たとえば、クライアントが不正な形式のリクエストを送信した場合や、応答する正常なインスタンスがない場合でも、リクエストはログに記録されます。</p> <p>Elastic Load Balancer ログエントリの詳細については、「」を参照してください。</p> <ul style="list-style-type: none"><li>• Classic Load Balancer: <a href="#">ログエントリにアクセスします</a>。</li><li>• Application Load Balancer: <a href="#">ログエントリにアクセスします</a>。</li><li>• Network Load Balancer: <a href="#">ログエントリにアクセスします</a>。</li></ul> | <p>CloudWatch LogGroup: <code>/aws/ams/cloudtrail</code></p> <p>S3 バケット: <code>mc-a{<i>account_ID</i>}-logs-{<i>region</i>}</code></p> <p>パス: <code>aws/elbaccess</code></p> |

|    | サービス名                                                      | ログの詳細                                                                                                                                                                        | ログの場所                                                                                                                                                   |
|----|------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9  | Amazon<br>OpenSearch<br>Service<br>(OpenSearch<br>Service) | サービスエラーログ。<br><br>OpenSearch ログ記録を明示的に有効にする必要があります。詳細については、「 <a href="#">サポートされているサービスのログ記録の有効化</a> 」を参照してください。                                                              | CloudWatch LogGroup: /aws/ams/cloudtrail                                                                                                                |
| 10 | Amazon<br>ElastiCache                                      | API コールのログ記録のみ。                                                                                                                                                              | CloudWatch LogGroup: /aws/ams/cloudtrail                                                                                                                |
| 11 | Amazon<br>GuardDuty                                        |                                                                                                                                                                              |                                                                                                                                                         |
| 12 | Amazon<br>Inspector                                        |                                                                                                                                                                              |                                                                                                                                                         |
| 13 | Amazon Macie                                               |                                                                                                                                                                              |                                                                                                                                                         |
| 14 | Amazon<br>Redshift                                         | 接続、ユーザー、アクティビティログ。<br><br>ログ記録は、Redshift クラスターの作成 CT (ct-1malj7snzxrkr) を呼び出して Redshift クラスターを作成すると、デフォルトで有効になります。<br><br>詳細については、「 <a href="#">データベース監査ログ記録</a> 」を参照してください。 | S3 バケット: <code>ams-a{<i>account_ID</i>}-log-management-{<i>region</i>}</code><br><br>パス: <code>/AWS/RedShift/{<i>CloudFront_Distribution_ID</i>}</code> |

|    | サービス名                                    | ログの詳細                                                                                                                                                                                                                                                                   | ログの場所                                                                                                                |
|----|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| 15 | Amazon Relational Database Service (RDS) | <p>データベースタイプに固有のログ。</p> <p>RDS ログ記録は明示的に有効にする必要があります。詳細については、「<a href="#">サポートされているサービスのログ記録の有効化</a>」を参照してください。</p> <p>MSSQL ログにはストアドプロシージャを介してのみアクセスできます。詳細については、「<a href="#">ログファイルのアーカイブ</a>」を参照してください。</p>                                                          | CloudWatch LogGroup: /aws/rds/(インスタンス クラスター){データベース名}/{ログ名}                                                          |
| 16 | Amazon S3 (S3)                           | <p>バケットアクセスログ。各アクセスログレコードは、リクエスト、バケット名、リクエスト時間、リクエストアクション、レスポンスステータス、エラーコード (存在する場合) など、単一のアクセスリクエストに関する詳細を提供します。アクセスログ情報は、セキュリティおよびアクセス監査に役立ちます。また、顧客ベースについて学び、Amazon S3 請求書を理解するのに役立ちます。</p> <p>S3 アクセスログエントリの詳細については、<a href="#">S3 サーバーアクセスログの形式</a>」を参照してください。</p> | <p>S3 バケット: mc-a{<i>account_ID</i>}-log-management-{<i>region</i>}</p> <p>パス: /aws/s3access/{<i>bucket_name</i>}</p> |

|    | サービス名                              | ログの詳細                                                                                           | ログの場所                                                                                                                                                                                                                       |
|----|------------------------------------|-------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 17 | Amazon Simple Email Service (SES)  | SES API サービスコール。                                                                                | CloudWatch LogGroup: /aws/ams/cloudtrail<br><br>S3 バケット: <code>ams-a{<i>account_ID</i>}-log-management-{<i>region</i>}</code><br><br>パス: <code>AWS/CloudTrail/AWSLogs/{<i>account_ID</i>}/CloudTrail/{<i>region</i>}</code> |
| 18 | Amazon Virtual Private Cloud (VPC) | VPC フローデータ (VPC のネットワークインターフェイスとの間で送受信される IP トラフィックに関する情報)。                                     | CloudWatch LogGroup: /aws/vpcflow/{vpc_id}                                                                                                                                                                                  |
| 19 | Auto Scaling                       | API コールのログ記録のみ。                                                                                 | CloudWatch LogGroup: /aws/ams/cloudtrail                                                                                                                                                                                    |
| 20 | AWS Certificate Manager            |                                                                                                 |                                                                                                                                                                                                                             |
| 21 | AWS CodeDeploy                     | インスタンス固有のデプロイログ。                                                                                | インスタンス上                                                                                                                                                                                                                     |
| 22 | AWS Config                         | AWS Config API サービスコール。                                                                         | CloudWatch LogGroup: /aws/ams/cloudtrail<br><br>S3 バケット: <code>ams-a{<i>account_ID</i>}-log-management-{<i>region</i>}</code><br><br>パス: <code>AWS/CloudTrail/AWSLogs/{<i>account_ID</i>}/CloudTrail/{<i>region</i>}</code> |
| 23 | AWS Database Migration Service     | データベース移行ログ。<br><br>詳細については、 <a href="#">AWS Database Migration Service でのログ管理の紹介</a> を参照してください。 | データベース移行コンソール                                                                                                                                                                                                               |

|    | サービス名                                 | ログの詳細           | ログの場所                                    |
|----|---------------------------------------|-----------------|------------------------------------------|
| 24 | AWS Direct Connect (DX)               | API コールのログ記録のみ。 | CloudWatch LogGroup: /aws/ams/cloudtrail |
| 25 | AWS Glacier                           |                 |                                          |
| 26 | AWS IAM (IAM)                         |                 |                                          |
| 27 | AWS Key Management Service            |                 |                                          |
| 28 | AWS マネジメントコンソール (コンソールまたは AWS コンソール)  |                 |                                          |
| 29 | AWS Simple Notification Service (SNS) |                 |                                          |
| 30 | AWS Simple Queueing Service (SQS)     |                 |                                          |

## AMS 共有サービスログ

次の表は、アカウントの AMS 共有サービスのログとログの場所を示しています。

ログにアクセスするには、必要な IAM ロールのいずれかがあり、AMS アカウントにあることを確認します。次に、表示されているディレクトリに移動します。

## AMS シングルアカウントランディングゾーン共有サービスログ記録

|   | 共有サービス名       | ログの詳細                                                                                                                                                                | ログの場所                                                                                                                                                                                                         |
|---|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | 踏み台ホスト        | 踏み台ホストにアクセスするユーザーに関する情報。                                                                                                                                             | Linux 踏み台 :<br><br>CloudWatch Logs: /{instance id}/var/log/secure<br><br>CloudWatch Logs: /{instance id}/var/log/audit/audit.log<br><br>Windows 踏み台 :<br><br>CloudWatch Logs: /{instance id}/SecurityEventLog |
| 2 | 管理ホスト         | アカウント内の自動アクセス管理アクションを支援するスクリプトの出力。                                                                                                                                   | CloudWatch Logs: /{instance id}/ApplicationEventLog                                                                                                                                                           |
| 4 | EPS ホスト (DSM) | Deep Security Management プラットフォームへのインスタンスの登録に関する情報。                                                                                                                  | CloudWatch Logs: /{instance id}/var/log/DSM.log                                                                                                                                                               |
| 5 | ディレクトリサービス    | アカウントのログイン、アカウント管理、詳細追跡、オブジェクトアクセス、ポリシー変更、アカウントのディレクトリ内での特権の使用に関する情報。<br><br>Directory Services のログ記録を明示的に有効にする必要があります。詳細については、「 <a href="#">サポートされているサービスのログ記録の</a> | CloudWatch Logs: /aws/directoryservice/{directory id}-{directory dns name}                                                                                                                                    |



|   | 共有サービス名 | ログの詳細                                      | ログの場所                                      |
|---|---------|--------------------------------------------|--------------------------------------------|
|   |         | <a href="#">有効化</a> 」を参照してください。            |                                            |
| 6 | lambda  | アカウント内の自動化された運用アクションを支援するさまざまな Lambda の出力。 | CloudWatch Logs: /aws/lambda/{lambda name} |

## AMS マルチアカウントランディングゾーン共有サービスログ記録

|   | 共有サービス名       | ログの詳細                                                                                                           | ログの場所                                                                                                                                                                 |
|---|---------------|-----------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | 踏み台           | インスタンスのログインと認証の失敗の出力。                                                                                           | Linux Bastions CloudWatch Logs: /<br>{ <i>instance_ID</i> } /var/log/secure.log<br><br>Windows Bastions CloudWatch<br>Logs: /{ <i>instance_ID</i> } /SecurityEventLog |
| 2 | 管理ホスト         | アカウント内の自動アクセス管理アクションを支援する scriptsy の出力。                                                                         | CloudWatch Logs: /{ <i>instance_ID</i> } /ApplicationEventLog                                                                                                         |
| 3 | EPS ホスト (DSM) | Deep Security Management プラットフォームへのインスタンスの登録に関する情報。                                                             | CloudWatch Logs: /{ <i>instance_ID</i> } /var/log/DSM.log                                                                                                             |
| 4 | ディレクトリサービス    | アカウントのログイン、アカウント管理、詳細追跡、オブジェクトアクセス、ポリシー変更、アカウントのディレクトリ内での特権の使用に関する情報。<br><br>Directory Services のログ記録を明示的に有効にする | CloudWatch Logs: /aws/directoryservice/{ <i>directory_ID</i> }-{ <i>directory_DNS_name</i> }                                                                          |

|   | 共有サービス名 | ログの詳細                                                                | ログの場所                                                   |
|---|---------|----------------------------------------------------------------------|---------------------------------------------------------|
|   |         | 必要があります。詳細については、「 <a href="#">サポートされているサービスのログ記録の有効化</a> 」を参照してください。 |                                                         |
| 5 | lambda  | アカウント内の自動化された運用アクションを支援するさまざまな Lambda の出力。                           | CloudWatch Logs: /aws/lambda/<br>{ <i>Lambda_name</i> } |

## Amazon Elastic Compute Cloud (Amazon EC2) - システムレベルのログ

インスタンスログは、インスタンスで実行されている CloudWatch Logs エージェントによって収集され、インスタンスと同じ名前の CloudWatch Logs グループを介してアクセスできます。たとえば、インスタンス ID が i-0123456789abcdef0 で、ログファイル名が /var/log/messages の場合、ロググループは i-0123456789abcdef0 と Log Streams /var/log/messages になります。

「[AMS 集計サービスログ](#)」も参照してください。

ログにアクセスするには、必要な IAM ロールのいずれかがあり、AMS アカウントにあることを確認します。次に、表示されているディレクトリに移動します。

### Note

デフォルトでは、次のログが収集されます。

Amazon Linux / Red Hat Linux / Centos Linux / Ubuntu / SUSE Linux

### ログファイル/ログストリーム

```
/var/log/amazon/ssm/amazon-ssm-agent.log
/var/log/amazon/ssm/errors.log
/var/log/audit/audit.log
/var/log/cloud-init-output.log
/var/log/cfn-init.log
```

```
/var/log/cfn-init-cmd.log
/var/log/cloud-init.log (Amazon Linux 1 / Amazon Linux 2 only)
/var/log/cron
/var/log/dnf.log
/var/log/maillog
/var/log/messages
/var/log/secure
/var/log/spooler
/var/log/yum.log
/var/log/aws/ams/bootstrap.log
/var/log/aws/ams/build.log
/var/log/syslog
/var/log/dpkg.log
/var/log/auth.log
/var/log/zypper.log
```

#### Note

Amazon Linux 2023 のログにアクセスする方法については、[EC2 Amazon Linux 2023 インスタンスで /var/log ディレクトリにログがないのはなぜですか？](#)を参照してください。

## Windows

### ログファイル/ログストリーム

```
SecurityEventLog
SystemEventLog
AmazonSSMAgentLog
MicrosoftWindowsAppLockerMSIAndScriptEventLog
MicrosoftWindowsAppLockerEXEAndDLLEventLog
AmazonCloudWatchAgentLog
EC2ConfigServiceEventLog (Windows Server 2012 R2 Only)
ApplicationEventLog
AmazonCloudFormationLog
MicrosoftWindowsGroupPolicyOperationalEventLog
AmazonSSMErrorLog
```

## Splunk との統合

AMS は、Splunk などのカスタマーログ分析サービスへの AWS Lambda ベースのプッシュをサポートしています。

AMS は Amazon Web サービス用の Splunk アドオンを活用して、AWS データを Splunk にストリーミングできるようにします。[「ハードウェアとソフトウェアの要件」](#)を参照してください。

この Splunk ブログ記事 [「AWS CloudWatch Logs を Splunk にストリーミングする方法」](#)を参照してください (ヒント: 思ったよりも簡単です)。AMS のお客様は CloudWatch ログストリーミングがデフォルトで有効になっているため、AMS は AWS Lambda 関数を設定しますが、Splunk HTTP Event Collector (HEC) 入力を設定し、追加機能のリクエストを AMS に送信する必要があります。

データ入力設定は次のようになります。

## ログ設定のカスタマイズ

CloudWatch Logs のログデータ保持を変更したり、追加の AWS サービスのログ記録を有効にしたりできます。

### CloudWatch のログ保持期間の変更

CloudWatch Logs のログデータ保持設定を変更できます。デフォルトでは、ログは無制限に保持され、失効しません。ロググループごとに保持ポリシーを調整し、無制限の保持期間を維持するか、1 日間 ~ 10 年間の保持期間を選択することができます。AMS で許可される最小保持期間を確認するには、AWS Artifact から入手できる AMS 技術標準ドキュメントを参照してください。AWS Artifact にアクセスするには、CSDM に連絡して手順を確認するか、[「AWS Artifact の開始方法」](#)を参照してください。

CloudWatch Logs ログ保持機能は、保持ポリシーに基づいてストリーム内のログイベントを削除します。ログストリームやロググループは削除されません。一般的な情報については、[Amazon CloudWatch Logs ユーザーガイド」の Amazon CloudWatch Logs とは」](#)を参照してください。

ログ保持期間のカスタマイズおよび詳細については、[CloudWatch Logs でのログデータ保持の変更」](#)を参照してください。

### サポートされているサービスのログ記録の有効化

一部のサービスでは、デフォルトでログ記録が有効になっていないため、明示的な有効化が必要です。

CloudFront、OpenSearch、Amazon RDS、Route53 のログ記録を有効にするには、[管理 | その他 | その他 | 変更タイプの作成 \(ct-1e1xtak34nx76\)](#) で RFC を送信し、必要に応じて ## を置き換えます。

Subject: Enable logging for *SERVICE\_NAME*

Description: Service ARN: *SERVICE\_ARN*

# セキュリティ管理

AWS Managed Services (AMS) セキュリティ管理は、AMS が組織のアセットを識別し、それらのアセットを保護するためのポリシーと手順を実装するプロセスです。

## Note

AMS に変更タイプ (CT)、デプロイ | 高度なスタックコンポーネント | 追加の SANs を含む ACM 証明書 | AWS Certificate Manager 証明書のリクエストを送信するために使用できる作成 (ct-3l14e139i5p50) が追加されました。詳細については、「[AWS::CertificateManager::Certificate](#)」を参照してください。この CT では、追加のサブジェクト代替名 (SAN) を作成できます。

一般的な AWS セキュリティの詳細については、「[セキュリティ、アイデンティティ、コンプライアンスのベストプラクティス](#)」を参照してください。

AMS は、セキュリティリスクを次のように分類します。

- マルウェア対策プロセスが処理するマルウェア対策によって検出された既知のリスク。
- セキュリティイベント管理プロセスが処理するアクセス違反などのセキュリティイベント。

## トピック

- [AMS でのデータ保護](#)
- [ID とアクセス管理](#)
- [AMS のセキュリティインシデント対応](#)
- [AMS Advanced での変更リクエストのセキュリティレビュー](#)

## AMS でのデータ保護

AMS は、Amazon GuardDuty、Amazon Macie (オプション)、その他の内部専有ツールやプロセスなどのネイティブ AWS サービスを活用して、マネージドアカウントを継続的にモニタリングします。アラームがトリガーされると、AMS は最初のトリガーとアラームへの応答について責任を負います。対応プロセスは NIST 標準に基づいています。AMS は、セキュリティインシデント対応シミュレーションを使用して対応プロセスを定期的にテストし、ワークフローを既存のカスタマーセキュリティ対応プログラムと整合させます。

AMS は、またはセキュリティポリシーの違反 AWS または差し迫った違反の脅威を検出すると、影響を受けるリソースや設定関連の変更などの情報を収集します。AMS は、すべてのマネージドアカウントでモニタリングダッシュボード、インシデントキュー、サービスリクエストを積極的に確認および調査する専任オペレーターによる 24 時間 365 日体制のfollow-the-sunサポートを提供します。AMS は、セキュリティの専門家と調査結果を調査してアクティビティを分析し、アカウントにリストされているセキュリティエスカレーション連絡先を通じて通知します。

調査結果に基づいて、AMS はお客様と積極的に連携します。アクティビティが不正または疑わしいと思われる場合、AMS はお客様と協力して問題を調査、修復、または封じ込めます。GuardDuty によって生成された特定の検出結果タイプでは、AMS がアクションを実行する前に影響を確認する必要があります。例えば、GuardDuty 検出結果タイプ UnauthorizedAccess:IAMUser/ConsoleLogin は、ユーザーの 1 人が異常な場所からログインしたことを示します。AMS から通知され、この動作が正当かどうかを確認するために検出結果を確認するよう求められます。

## Amazon Macie

AWS Managed Services では、Macie を使用して、個人健康情報 (PHI)、個人を特定できる情報 (PII)、財務データなどの機密データの大規模で包括的なリストを検出することをお勧めします。

Macie は、Amazon S3 バケットで定期的に行うように設定でき、バケット内の新規または変更されたオブジェクトの評価が時間の経過とともに自動化されます。セキュリティ検出結果が生成されると、AMS は通知を行い、必要に応じて修正を行います。

詳細については、[Amazon Macie の検出結果の分析](#)」を参照してください。

### Amazon Macie セキュリティ

Macie は、AWS に保存されている機密データを自動的に検出、分類、保護することで、データ損失を防ぐのに役立つ人工知能/AI を活用したセキュリティサービスです。Macie は機械学習を使用して、個人を特定できる情報 (PII) や知的財産などの機密データを認識し、ビジネス価値を割り当て、このデータが保存されている場所と組織内でどのように使用されているかを可視化します。Macie は、データアクセスアクティビティの異常を継続的にモニタリングし、不正アクセスや不注意によるデータ漏洩のリスクを検出するとアラートを送信します。Macie サービスは Amazon S3 と AWS CloudTrail データソースをサポートしています。

AMS は Macie からアラートを継続的にモニタリングし、アラートが発生した場合は、リソースとアカウントを保護するための迅速なアクションを実行します。AMS がサポートするサービスのリストに Macie を追加することで、お客様の指示に従って、すべてのアカウントで Macie を有効にして設定する責任も果たすようになりました。Macie アラートとアクションが展開されたら、AWS コンソールまたはサポートされている統合で表示できます。アカウントのオンボーディング中に、PII の



保存に使用するアカウントを指定できます。PII を使用するすべての新しいアカウントでは、Macie を使用することをお勧めします。PII を持つ既存のアカウントについては、お問い合わせください。アカウントで有効になります。その結果、追加の保護レイヤーが利用可能になり、AMS によって管理される AWS 環境で Macie のすべての利点を享受できます。

## AMS Macie FAQs

- すべての AMS アカウントで Trend Micro と GuardDuty が有効になっている場合に Macie が必要なのはなぜですか？

Macie は、所有するデータ、データがビジネスにもたらす価値、そのデータへのアクセスに関連する動作を分類することで、Amazon S3 のデータを保護するのに役立ちます。Amazon GuardDuty は、脅威アクターの偵察、インスタンスの問題、問題のあるアカウントアクティビティなどの脅威を特定できるようにすることで、AWS アカウント、ワークロード、データの広範な保護を提供します。どちらのサービスにも、ユーザー動作分析、機械学習、異常検出が組み込まれており、それぞれのカテゴリの脅威を検出できます。Trend Micro は、PII とその脅威を特定することに重点を置いていません。

- AMS アカウントで Macie を有効にするにはどうすればよいですか？

アカウントに PII/PHI が保存されている場合、または保存を計画している場合は、CSDM に連絡するか、サービスリクエストを作成して、AMS が管理する新規または既存のアカウントに対して Macie を有効にします。

- AMS アカウントで Macie を有効にすると、コストにどのような影響がありますか？

Macie の料金は、Amazon Elastic Compute Cloud (Amazon EC2) などの他のサービスと同様の AMS で機能します。Amazon Macie の料金は、使用量と SLAs に基づく AMS の引き上げに基づいて発生します。Macie の料金は使用状況に基づきます。[Amazon Macie の料金](#)」を参照してください。AWS CloudTrail イベントと Amazon S3 ストレージに基づいて測定されます。Macie の料金は Amazon S3 バケットに追加された増分データに基づいて課金されるため、有効になってから 2 か月目からフラット化する傾向があることに注意してください。

Macie の詳細については、[Amazon Macie](#)」を参照してください。

## GuardDuty

GuardDuty は、悪意のある IP アドレスやドメインのリストなどの脅威インテリジェンスフィードを使用する継続的なセキュリティモニタリングサービスであり、機械学習を使用して、AWS 環境内の予期しない、潜在的に不正なアクティビティや悪意のあるアクティビティを特定します。このアク

ティビティには、権限のエスカレートや、公開されている認証情報の使用、悪意のある IP アドレスでの通信も含まれます。また、GuardDuty は、使用したことの無いリージョンにデプロイされたインスタンスなどの不正なインフラストラクチャのデプロイや、パスワード強度を低下させるためのパスワードポリシーの変更などの異常な API コールなど、Amazon Web Services アカウントのアクセス動作をモニタリングします。詳細については、[GuardDuty ユーザーガイド](#)を参照してください。

GuardDuty の検出結果を表示および分析するには、次の手順を使用します。

1. [GuardDuty コンソール](#)を開きます。
2. 検出結果を選択し、特定の検出結果を選択して詳細を表示します。各検出結果の詳細は、検出結果のタイプ、関連するリソース、アクティビティの性質によって異なります。

使用可能な検出結果フィールドの詳細については、[GuardDuty の検出結果の詳細](#)を参照してください。

## GuardDuty セキュリティ

Amazon GuardDuty は、AWS アカウントとワークロードを継続的にモニタリングして保護できる脅威検出を提供します。Amazon GuardDuty は、アカウントから生成されたメタデータの継続的なストリームと、イベント、Amazon VPC フローログ、ドメインネームシステム (DNS) ログにある AWS CloudTrail ネットワークアクティビティを分析します。また、既知の悪意のある IP アドレス、異常検出、機械学習などの統合された脅威インテリジェンスを使用して、脅威をより正確に特定します。GuardDuty はモニタリング対象の AMS サービスです。Amazon GuardDuty のモニタリングの詳細については、「」を参照してください[GuardDuty のモニタリング](#)。GuardDuty の詳細については、[Amazon GuardDuty](#)を参照してください。

すべての新しい AMS アカウントでは、GuardDuty がデフォルトで有効になっています。AMS は、アカウントのオンボーディング中に GuardDuty を設定します。変更リクエストを送信して、いつでも設定を変更できます。GuardDuty の料金は、Amazon Elastic Compute Cloud (Amazon EC2) などの他のサービスと同様に AMS で機能します。GuardDuty の料金は、使用量と SLAs に基づく AMS の引き上げに基づいて発生します。GuardDuty 料金は、Amazon VPC フローログの AWS CloudTrail イベントとボリュームに基づいて測定される使用量 ([Amazon GuardDuty 料金](#)) に基づいています。

AMS の GuardDuty では、次のプライマリ検出カテゴリが有効になっています。

- 偵察 -- 異常な API アクティビティ、VPC 内ポートスキャン、失敗したログインリクエストの異常なパターン、既知の不正な IP からのブロックされていないポート探索など、脅威アクターによる偵察を提案するアクティビティ。

- インスタンスの問題 -- 暗号通貨マイニング、ドメイン生成アルゴリズム (DGA) を使用したマルウェア、アウトバウンドサービス拒否アクティビティ、異常に大量のネットワークトラフィック、異常なネットワークプロトコル、既知の悪意のある IP とのアウトバウンドインスタンス通信、外部 IP アドレスで利用される一時的な Amazon EC2 認証情報、DNS を使用したデータ流出などの問題のあるインスタンスアクティビティ。
- アカウントアクティビティ -- アカウントアクティビティを示す一般的なパターンには、異常な位置情報または匿名化プロキシからの API コール、ログ記録の無効化 AWS CloudTrail の試み、異常なインスタンスまたはインフラストラクチャの起動、異常な AWS リージョンでのインフラストラクチャのデプロイ、既知の悪意のある IP アドレスからの API コールなどがあります。

AMS は、マネージドアカウントで GuardDuty を使用して GuardDuty からの検出結果とアラートを継続的にモニタリングし、アラートが発生した場合は、AMS オペレーションがリソースとアカウントを保護するためにプロアクティブアクションを実行します。GuardDuty の検出結果とアクションは、AWS コンソールまたはサポートされている統合で展開されたときに表示できます。

GuardDuty は、アカウントの Trend Micro Deep Security Manager と連携します。Trend Micro Deep Security Manager は、ホストベースの侵入検知/侵入防止サービスを提供します。Trend Micro Web Reputation サービスは、ホストが脅威として知られているホストまたはウェブサービスと通信しようとしているタイミングを検出する機能で、GuardDuty とある程度重複しています。ただし、GuardDuty は追加の脅威検出カテゴリを提供し、Trend Micro のホストベースの検出を補完する方法であるネットワークトラフィックをモニタリングすることでこれを実現します。ネットワークベースの脅威検出では、ホストが問題のある動作をしている場合にコントロールが失敗しないようにすることで、セキュリティを強化できます。AMS では、すべての AMS アカウントで GuardDuty を使用することをお勧めします。

Trend Micro の詳細については、[「Trend Micro Deep Security Help Center」](#)を参照してください。Amazon 以外のリンクは予告なしに変更される可能性があります。

## GuardDuty のモニタリング

GuardDuty は、AMS がキャプチャしてアラートできる[セキュリティ検出結果](#)を生成することで、AWS 環境のステータスを通知します。

Amazon GuardDuty は、VPC フローログ、AWS CloudTrail イベントログ、ドメインネームシステムログを分析して処理することで、AWS 環境のセキュリティをモニタリングします。GuardDuty を設定して、独自のカスタム IP リスト、信頼できる IP リスト、脅威リストを使用できるようにすることで、このモニタリング範囲を拡張できます。

- 信頼できる IP リストは、AWS インフラストラクチャおよびアプリケーションとの安全な通信を許可した IP アドレスで構成されます。GuardDuty は信頼できる IP リストの IP アドレスの結果は生成しません。どの時点でも、信頼されている IP リストのアップロード数は各リージョンの AWS アカウントにつき 1 つに限られます。
- 脅威リストは、悪意のある既知の IP アドレスで構成されます。GuardDuty では、脅威リストに基づいて検出結果を生成します。どの時点でも、脅威リストのアップロード数は各リージョンの AWS アカウントにつき最大 6 つに限られます。

GuardDuty を実装するには、AMS CT デプロイ | モニタリングと通知 | GuardDuty IP セット | 作成 (ct-08avsj2e9mc7g) を使用して、承認された IP アドレスのセットを作成します。AMS CT デプロイ | モニタリングと通知 | GuardDuty 脅威情報セット | 作成 (ct-25v6r7t8gvkq5) を使用して、拒否された IP アドレスのセットを作成することもできます。

AMS がモニタリングするサービスのリストについては、「」を参照してください[AMS モニタリングシステムは何をモニタリングしますか？](#)。

## Amazon Route 53 Resolver DNS ファイアウォール

Amazon Route 53 Resolver は、パブリックレコード、Amazon VPC 固有の DNS 名、Amazon Route 53 プライベートホストゾーンの AWS リソースからの DNS クエリに再帰的に応答し、すべての VPCs でデフォルトで使用できます。Route 53 Resolver DNS Firewall を使用すると、仮想プライベートクラウド (VPC) のアウトバウンド DNS トラフィックをフィルタリングおよび規制できます。これを行うには、DNS Firewall のルールグループで再利用可能なフィルタリングルールのコレクションを作成し、そのルールグループを VPC に関連付けて、DNS Firewall のログとメトリクスのアクティビティを監視します。アクティビティに基づいて、DNS Firewall の動作を適宜調整できます。詳細については、「[DNS ファイアウォールを使用してアウトバウンド DNS トラフィックをフィルタリングする](#)」を参照してください。

Route 53 Resolver DNS Firewall 設定を表示および管理するには、次の手順を使用します。

1. にサインイン AWS マネジメントコンソール し、<https://console.aws.amazon.com/vpc/> で Amazon VPC コンソールを開きます。
2. DNS Firewall で、ルールグループを選択します。
3. 既存の設定を確認、編集、または削除するか、新しいルールグループを作成します。詳細については、「[Route 53 Resolver DNS Firewall の仕組み](#)」を参照してください。

## Amazon Route 53 Resolver DNS Firewall のモニタリングとセキュリティ

Amazon Route 53 DNS Firewall は、ルールの関連付け、ルールアクション、ルール評価優先度の概念を使用します。ドメインリストは、ルールグループ内の DNS Firewall ルールで使用する、再利用可能なドメイン仕様のセットです。ルールグループを VPC に関連付けると、DNS Firewall はルールで使用されているドメインリストと DNS クエリを比較します。DNS Firewall が一致を検出した場合、DNS クエリは一致するルールのアクションに従って処理されます。ルールグループとルールの詳細については、[「DNS Firewall ルールグループとルール」](#)を参照してください。

ドメインリストは、次の 2 つの主要なカテゴリに分類できます。

- がユーザーに代わって AWS 作成および管理するマネージドドメインリスト。
- 作成および管理する独自のドメインリスト。

ルールグループは、関連付け優先度インデックスに基づいて評価されます。

デフォルトでは、AMS は次のルールとルールグループで構成されるベースライン設定をデプロイします。

- という名前の 1 つのルールグループ DefaultSecurityMonitoringRule。ルールグループには、有効な各の既存の VPC ごとに作成時に使用できる最も優先度の高い関連付けがあります AWS リージョン。
- アクション ALERT DefaultSecurityMonitoringRule で AWSManagedDomainsAggregateThreatList Managed Domain リストを使用して、ルールグループ内で優先度 1 の という名前の 1 つの DefaultSecurityMonitoringRule ルール。

既存の設定がある場合、ベースライン設定は既存の設定よりも優先度が低くデプロイされます。既存の設定がデフォルトです。既存の設定でクエリ解決の処理方法に関する優先度の高い指示が提供されていない場合は、AMS ベースライン設定をキャッチオールとして使用します。ベースライン設定を変更または削除するには、次のいずれかを実行します。

- Cloud Service Delivery Manager (CSDM) または Cloud Architect (CA) にお問い合わせください。
- Management [Other | Other | Create CT \(ct-1e1xtak34nx76\)](#) を使用して [変更リクエスト \(RFC\)](#) を作成します。
- サービスリクエストを作成します。



アカウントがデベロッパーモードまたは直接変更モードで運用されている場合は、変更を自分で実行できます。

## AWS Certificate Manager (ACM) 証明書

AMS には、CT、デプロイ | 高度なスタックコンポーネント | 追加の SANs を含む ACM 証明書 | 作成 (ct-3l14e139i5p50) があります。これを使用して、最大 5 つのサブジェクト代替名 (SAN) (example.com、example.net、example.org など) を追加して AWS Certificate Manager 証明書のリクエストを送信できます。詳細については、「[What is AWS Certificate Manager ?](#)」および「[ACM Certificate Characteristic](#)」を参照してください。

### Note

このタイムアウト設定は、実行に関するだけでなく、E メール検証による ACM 証明書の検証に関するものです。検証しないと、RFC は失敗します。

## AMS でのデータの暗号化

AMS は、データ暗号化にいくつかの AWS サービス、特に Amazon Simple Storage Service、AWS Key Management Service ( AWS KMS )、Amazon Elastic Block Store、Amazon Relational Database Service Amazon Redshift、Amazon ElastiCache AWS Lambda、および Amazon OpenSearch Service を使用します。

### Amazon S3

Amazon S3 には、転送中および保管時のデータを保護するために使用できる、複数のオブジェクト暗号化オプションがあります。サーバー側の暗号化では、オブジェクトをデータセンター内のディスクに保存する前に暗号化し、オブジェクトをダウンロードするときに復号します。リクエストが認証され、お客様がアクセス許可を持っていれば、オブジェクトが暗号化されているかどうかに関係なく同じ方法でアクセスできます。詳細については、「[Amazon S3 におけるデータ保護](#)」を参照してください。

### Amazon EBS

Amazon EBS 暗号化を使用すると、独自のキー管理インフラストラクチャを構築、保守、保護する必要はありません。Amazon EBS 暗号化は、暗号化されたボリュームとスナップショットを作成するときに AWS KMS キーを使用します。暗号化オペレーションは、Amazon EC2 インスタンスをホ

ストするサーバーで行われます。これは、インスタンスとそのアタッチされた Amazon EBS ストレージ間の data-at-rest data-in-transit の両方が安全であることを確認するために行われます。1 つのインスタンスに対し、暗号化されたボリュームと暗号化されていないボリュームの両方を、同時にアタッチできます。詳細については、「[Amazon EBS Encryption](#)」を参照してください。

## Amazon RDS

Amazon RDS は、Amazon RDS DB インスタンスを暗号化することができます。保管時に暗号化されるデータには、DB インスタンス、自動バックアップ、リードレプリカ、スナップショットの基盤となるストレージが含まれます。Amazon RDS 暗号化 DB インスタンスは、業界標準の AES-256 暗号化アルゴリズムを使用して、Amazon RDS DB インスタンスをホストするサーバー上のデータを暗号化します。データが暗号化されると、Amazon RDS はパフォーマンスの影響を最小限に抑えながら、データへのアクセスと復号化の認証を透過的に処理します。暗号化を使用するために、データベースのクライアントアプリケーションを変更する必要はありません。詳細については、「[Amazon RDS リソースの暗号化](#)」を参照してください。

## Amazon Simple Queue Service

デフォルトの Amazon SQS マネージドサーバー側の暗号化 (SSE) オプションに加えて、Amazon SQS マネージド SSE (SSE-SQS) では、Amazon SQS マネージド暗号化キーを使用してメッセージキュー経由で送信される機密データを保護するカスタムマネージドサーバー側の暗号化を作成できます。サーバー側の暗号化 (SSE) により、機密データを暗号化されたキューで送信できます。SSE は、Amazon SQS で管理される暗号化キー (SSE-SQS) または AWS KMS (SSE-KMS) で管理されるキーを使用して、キュー内のメッセージの内容を保護します。を使用して SSE を管理する方法については AWS マネジメントコンソール、「[保管時の暗号化](#)」を参照してください。

## 保管時のデータ暗号化

OpenSearch Service ドメインでは、保管中のデータの暗号化という、データへの不正アクセスを防止するのに役立つセキュリティ機能が提供されます。この機能は AWS Key Management Service (AWS KMS) を使用して暗号化キーを保存および管理し、Advanced Encryption Standard アルゴリズムを 256 ビットキー (AES-256) を使用して暗号化を実行します。詳細については、「[Amazon OpenSearch Service の保管中のデータの暗号化](#)」を参照してください。

## キーの管理

AWS KMS は、データの暗号化に使用される暗号化キーであるカスタマーマスターキー (CMKs) の作成と制御を容易にするマネージドサービスです。AWS KMS CMKs は、中国 (北京) および中国 (寧夏) リージョンを除き、FIPS 140-2 暗号化モジュール検証プログラムによって検証されたハード



ウェアセキュリティモジュール (HSMs) によって保護されています。詳細については、「[AWS Key Management Service とは](#)」を参照してください。

## ID とアクセス管理

AWS Identity and Access Management (IAM) は、AWS リソースへのアクセスを安全に制御するのに役立つウェブサービスです。IAM を使用して、誰を認証 (サインイン) し、誰にリソースの使用を認可する (アクセス許可を付与する) かを制御します。AMS オンボーディング中、各マネージドアカウント内にクロスアカウント IAM 管理者ロールを作成する責任があります。

### マルチアカウントランディングゾーン (MALZ) IAM 保護

AMS マルチアカウントランディングゾーン (MALZ) では、各組織 (AMS と顧客の両方) が自分の ID のライフサイクルを管理できるように、AMS アクセス管理の主な設計目標として Active Directory (AD) 信頼が必要です。これにより、相互のディレクトリに認証情報を持つ必要がなくなります。一方向信頼は、内の Managed Active Directory がカスタマー所有またはマネージド AD を AWS アカウント 信頼してユーザーを認証するように設定されます。信頼は 1 つの方法にすぎないため、マネージド AD がカスタマーアクティブディレクトリによって信頼されているわけではありません。

この設定では、ユーザー ID を管理するカスタマーディレクトリはユーザーフォレストと呼ばれ、Amazon EC2 インスタンスがアタッチされている Managed AD はリソースフォレストと呼ばれます。これは Windows 認証用に一般的に活用されている Microsoft 設計パターンです。詳細については、「[フォレスト設計モデル](#)」を参照してください。

このモデルにより、両方の組織がそれぞれのライフサイクルを自動化し、従業員が組織を離れた場合に AMS とユーザーの両方がアクセスを迅速に取り消すことができます。このモデルがないと、両方の組織が共通のディレクトリを使用した場合 (または、互いのディレクトリにユーザー/グループを作成した場合)、両方の組織は、開始および退出する従業員を考慮して、追加のワークフローとユーザー同期を導入する必要があります。これにより、プロセスにレイテンシーがあり、エラーが発生しやすいため、リスクが発生します。

### MALZ アクセスの前提条件

AWS/AMS コンソール、CLI、SDK にアクセスするための MALZ Identity Provider Integration。

AMS アカウントの Amazon EC2 インスタンスに対する一方向の信頼。

## アイデンティティを使用した認証

AMS は、IAM アイデンティティの一種である IAM ロールを使用します。IAM ロールは、アイデンティティができることとできないことを決定するアクセス許可ポリシーを持つアイデンティティであるという点で、ユーザーと非常によく似ています AWS。ただし、ロールには認証情報が関連付けられておらず、1 人のユーザーと一意に関連付けられるのではなく、ロールを必要とするすべてのユーザーがロールを引き受けることが意図されています。IAM ユーザーは、ロールを引き受けることで、一時的に特定のタスクに対して異なるアクセス許可を取得することができます。

アクセスロールは内部グループメンバーシップによって制御され、オペレーション管理によって管理および定期的にレビューされます。

### AMS の IAM ユーザーロール

IAM ロールは、AWS アイデンティティができることとできないことを決定するアクセス許可ポリシーを持つアイデンティティであるという点で、IAM ユーザーと似ています AWS。ただし、ユーザーは 1 人の特定の人に一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。

現在、標準 AMS アカウント `Customer_ReadOnly_Role` には 1 つの AMS デフォルトユーザーロールがあり、マネージド Active Directory を持つ AMS アカウント `customer_managed_ad_user_role` には追加のロールがあります。

ロールポリシーは、CloudWatch および Amazon S3 ログアクション、AMS コンソールアクセス、ほとんどの に対する読み取り専用制限 AWS のサービス、アカウント S3 コンソールへのアクセス制限、AMS 変更タイプアクセスのアクセス許可を設定します。

さらに、`Customer_ReadOnly_Role` には、インスタンスを予約できる可変リザーブドインスタンスのアクセス許可があります。いくつかのコスト削減値があるため、長期間一定数の Amazon EC2 インスタンスが必要になることがわかっている場合は、これらの APIs 呼び出すことができます。詳細については、[Amazon EC2 リザーブドインスタンス](#) を参照してください。

#### Note

IAM ユーザーのカスタム IAM ポリシーを作成するための AMS サービスレベル目標 (SLO) は、既存のポリシーが再利用されない限り、4 営業日です。既存の IAM ユーザーロールを変更する場合、または新しいロールを追加する場合は、[IAM: エンティティの更新](#) または [IAM: エンティティ RFC](#) の作成をそれぞれ送信します。

Amazon IAM ロールに慣れていない場合は、[「IAM ロール」](#)で重要な情報を確認してください。

マルチアカウントランディングゾーン (MALZ): AMS マルチアカウントランディングゾーンのデフォルト、カスタマイズされていないユーザーロールポリシーを確認するには、[MALZ: デフォルトの IAM ユーザーロール](#)次の「」を参照してください。

#### MALZ: デフォルトの IAM ユーザーロール

デフォルトのマルチアカウント AMS マルチアカウントランディングゾーンユーザーロールの JSON ポリシーステートメント。

##### Note

ユーザーロールはカスタマイズ可能で、アカウントごとに異なる場合があります。ロールの検索手順が表示されます。

これらは、デフォルトの MALZ ユーザーロールの例です。必要なポリシーが設定されていることを確認するには、AWS コマンドを実行する[get-role](#)か、AWS Management -> [IAM コンソール](#)にサインインし、ナビゲーションペインでロールを選択します。

#### コア OU アカウントロール

コアアカウントは、MALZ が管理するインフラストラクチャアカウントです。AMS マルチアカウントランディングゾーン Core アカウントには、管理アカウントとネットワークアカウントが含まれます。

#### Core OU アカウント: 一般的なロールとポリシー

| ロール                                                   | ポリシー                                                                                   |
|-------------------------------------------------------|----------------------------------------------------------------------------------------|
| AWSManagedServicesReadOnlyRole                        | <a href="#">ReadOnlyAccess</a> (パブリック AWS 管理ポリシー)。                                     |
| AWSManagedServicesCaseRole                            | <a href="#">ReadOnlyAccess</a><br><a href="#">AWSSupportAccess</a> (パブリック AWS 管理ポリシー)。 |
| AWSManagedServicesChangeManagementRole (コアアカウントバージョン) | <a href="#">ReadOnlyAccess</a>                                                         |

| ロール | ポリシー                                                    |
|-----|---------------------------------------------------------|
|     | <a href="#">AWSSupportAccess</a>                        |
|     | <a href="#">AMSChangeManagementReadOnlyPolicy</a>       |
|     | <a href="#">AMSChangeManagementInfrastructurePolicy</a> |

## Core OU アカウント: 管理アカウントのロールとポリシー

| ロール                                                   | ポリシー                                                                         |
|-------------------------------------------------------|------------------------------------------------------------------------------|
| AWSManagedServicesBillingRole                         | <a href="#">AMSBillingPolicy</a> (AMSBillingPolicy)。                         |
| AWSManagedServicesReadOnlyRole                        | <a href="#">ReadOnlyAccess</a> (パブリック AWS 管理ポリシー)。                           |
| AWSManagedServicesCaseRole                            | <a href="#">ReadOnlyAccess</a>                                               |
|                                                       | <a href="#">AWSSupportAccess</a> (パブリック AWS 管理ポリシー)。                         |
| AWSManagedServicesChangeManagementRole (管理アカウントバージョン) | <a href="#">ReadOnlyAccess</a>                                               |
|                                                       | <a href="#">AWSSupportAccess</a>                                             |
|                                                       | <a href="#">AMSChangeManagementReadOnlyPolicy</a>                            |
|                                                       | <a href="#">AMSChangeManagementInfrastructurePolicy</a>                      |
|                                                       | <a href="#">AMSMasterAccountSpecificChangeManagementInfrastructurePolicy</a> |

## Core OU アカウント: ネットワークアカウントのロールとポリシー

| ロール                                                       | ポリシー                                                                                                                                                                                                                                                                                   |
|-----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AWSManagedServicesReadOnlyRole                            | <a href="#">ReadOnlyAccess</a> (パブリック AWS 管理ポリシー)。                                                                                                                                                                                                                                     |
| AWSManagedServicesCaseRole                                | <a href="#">ReadOnlyAccess</a><br><br><a href="#">AWSSupportAccess</a> (パブリック AWS 管理ポリシー)。                                                                                                                                                                                             |
| AWSManagedServicesChangeManagementRole (ネットワークアカウントバージョン) | <a href="#">ReadOnlyAccess</a><br><br><a href="#">AWSSupportAccess</a><br><br><a href="#">AMSChangeManagementReadOnlyPolicy</a><br><br><a href="#">AMSChangeManagementInfrastructurePolicy</a><br><br><a href="#">AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy</a> |

## アプリケーションアカウントロール

アプリケーションアカウントロールは、アプリケーション固有のアカウントに適用されます。

## アプリケーションアカウント: ロールとポリシー

| ロール                            | ポリシー                                                                                                                                        |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| AWSManagedServicesReadOnlyRole | <a href="#">ReadOnlyAccess</a> (パブリック AWS 管理ポリシー)。                                                                                          |
| AWSManagedServicesCaseRole     | <a href="#">ReadOnlyAccess</a><br><br><a href="#">AWSSupportAccess</a> (パブリック AWS 管理ポリシー)。<br><br>このポリシーは、すべてのサポートオペレーションとリソースへのアクセスを提供します。 |

| ロール                                                         | ポリシー                                                                                                |
|-------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| AWSManagedServicesSecurityOpsRole                           | 詳細については、「 <a href="#">AWS サポートの開始方法</a> 」を参照してください。                                                 |
|                                                             | <a href="#">ReadOnlyAccess</a>                                                                      |
|                                                             | AWSsupportAccess <a href="#">の例</a>                                                                 |
|                                                             | このポリシーは、すべてのサポートオペレーションとリソースへのアクセスを提供します。                                                           |
| AWSManagedServicesChangeManagementRole (アプリケーションアカウントバージョン) | <a href="#">AWSCertificateManagerFullAccess</a> information、(パブリック AWS 管理ポリシー)                      |
|                                                             | <a href="#">AWSWAFFullAccess</a> information、(パブリック AWS 管理ポリシー)。このポリシーは、AWS WAF リソースへのフルアクセスを許可します。 |
|                                                             | <a href="#">AMSSecretsManagerSharedPolicy</a>                                                       |
|                                                             | <a href="#">ReadOnlyAccess</a>                                                                      |
| AWSManagedServicesAdminRole                                 | <a href="#">AWSsupportAccess</a> (パブリック AWS 管理ポリシー)。                                                |
|                                                             | このポリシーは、すべてのサポートオペレーションとリソースへのアクセスを提供します。詳細については、「 <a href="#">AWS サポートの開始方法</a> 」を参照してください。        |
|                                                             | <a href="#">AMSSecretsManagerSharedPolicy</a>                                                       |
|                                                             | <a href="#">AMSChangeManagementPolicy</a>                                                           |
|                                                             | <a href="#">AMSReservedInstancesPolicy</a>                                                          |
|                                                             | <a href="#">AMSS3Policy</a>                                                                         |
|                                                             | <a href="#">ReadOnlyAccess</a>                                                                      |

| ロール | ポリシー                                                   |
|-----|--------------------------------------------------------|
|     | <a href="#">AWSSupportAccess</a>                       |
|     | <a href="#">AMSCheckManagementInfrastructurePolicy</a> |
|     | <a href="#">AWSMarketplaceManageSubscriptions</a>      |
|     | <a href="#">AMSSecretsManagerSharedPolicy</a>          |
|     | <a href="#">AMSCheckManagementPolicy</a>               |
|     | <a href="#">AWSCertificateManagerFullAccess</a>        |
|     | <a href="#">AWSWAFFullAccess</a>                       |
|     | <a href="#">AMSS3Policy</a>                            |
|     | <a href="#">AMSReservedInstancesPolicy</a>             |

## ポリシーの例

使用するほとんどのポリシーの例を示します。ReadOnlyAccess ポリシー (すべての AWS サービスへの読み取り専用アクセスを提供するページ) を表示するには、アクティブな AWS アカウント: [ReadOnlyAccess](#) がある場合、このリンクを使用できます。また、要約バージョンがここに含まれています。

### AMSBillingPolicy

#### AMSBillingPolicy

新しい請求ロールは、経理部門が管理アカウントの請求情報またはアカウント設定を表示および変更するために使用できます。代替連絡先などの情報にアクセスしたり、アカウントリソースの使用状況を表示したり、請求のタブを保持したり、支払い方法を変更したりするには、このロールを使用します。この新しいロールは、[AWS Billing IAM アクションのウェブページ](#)に記載されているすべてのアクセス許可で構成されます。

## JSON

```
{
```



```
"Version": "2012-10-17",
"Statement": [
  {
    "Action": [
      "aws-portal:ViewBilling",
      "aws-portal:ModifyBilling"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "AllowAccessToBilling"
  },
  {
    "Action": [
      "aws-portal:ViewAccount",
      "aws-portal:ModifyAccount"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "AllowAccessToAccountSettings"
  },
  {
    "Action": [
      "budgets:ViewBudget",
      "budgets:ModifyBudget"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "AllowAccessToAccountBudget"
  },
  {
    "Action": [
      "aws-portal:ViewPaymentMethods",
      "aws-portal:ModifyPaymentMethods"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "AllowAccessToPaymentMethods"
  },
  {
    "Action": [
      "aws-portal:ViewUsage"
    ],
    "Resource": "*",
    "Effect": "Allow",
```

```
        "Sid": "AllowAccessToUsage"
    },
    {
        "Action": [
            "cur:DescribeReportDefinitions",
            "cur:PutReportDefinition",
            "cur>DeleteReportDefinition",
            "cur:ModifyReportDefinition"
        ],
        "Resource": "*",
        "Effect": "Allow",
        "Sid": "AllowAccessToCostAndUsageReport"
    },
    {
        "Action": [
            "pricing:DescribeServices",
            "pricing:GetAttributeValues",
            "pricing:GetProducts"
        ],
        "Resource": "*",
        "Effect": "Allow",
        "Sid": "AllowAccessToPricing"
    },
    {
        "Action": [
            "ce:*",
            "compute-optimizer:*"
        ],
        "Resource": "*",
        "Effect": "Allow",
        "Sid": "AllowAccessToCostExplorerComputeOptimizer"
    },
    {
        "Action": [
            "purchase-orders:ViewPurchaseOrders",
            "purchase-orders:ModifyPurchaseOrders"
        ],
        "Resource": "*",
        "Effect": "Allow",
        "Sid": "AllowAccessToPurchaseOrders"
    },
    {
        "Action": [
            "redshift:AcceptReservedNodeExchange",
```

```
        "redshift:PurchaseReservedNodeOffering"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "AllowAccessToRedshiftAction"
    },
    {
      "Action": "savingsplans:*",
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "AWSSavingsPlansFullAccess"
    }
  ]
}
```

AMSChangeManagementReadOnlyPolicy

AMSChangeManagementReadOnlyPolicy

すべての AMS 変更タイプと、リクエストされた変更タイプの履歴を表示するアクセス許可。

AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

デプロイをリクエストするアクセス許可 | マネージドランディングゾーン | 管理アカウント | アプリケーションアカウントの作成 (VPC を使用) 変更タイプ。

AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

デプロイをリクエストするアクセス許可 | マネージドランディングゾーン | ネットワークアカウント | アプリケーションルートテーブルの変更タイプを作成します。

AMSChangeManagementInfrastructurePolicy

AMSChangeManagementInfrastructurePolicy (管理用 | その他 | その他 CTs)

管理をリクエストするアクセス許可 | その他 | その他 | 作成、管理 | その他 | その他 | 変更タイプを更新する。

## AMSSecretsManagerSharedPolicy

### AMSSecretsManagerSharedPolicy

を通じて AMS によって共有されているシークレットパスワード/ハッシュを表示するアクセス許可  
AWS Secrets Manager (監査用のインフラストラクチャへのパスワードなど)。

AMS と共有するためのシークレットパスワード/ハッシュを作成するアクセス許可 (デプロイする必要がある製品のライセンスキーなど)。

### JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AllowAccessToSharedNameSpaces",
    "Effect": "Allow",
    "Action": "secretsmanager:*",
    "Resource": [
      "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
      "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
    ]
  },
  {
    "Sid": "DenyGetSecretOnCustomerNamespace",
    "Effect": "Deny",
    "Action": "secretsmanager:GetSecretValue",
    "Resource": "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
  },
  {
    "Sid": "AllowReadAccessToAMSNameSpace",
    "Effect": "Deny",
    "NotAction": [
      "secretsmanager:Describe*",
      "secretsmanager:Get*",
      "secretsmanager:List*"
    ],
    "Resource": "arn:aws:secretsmanager:*:*:secret:ams-shared/*"
  }
]
```

## AMSCheckManagementPolicy

### AMSCheckManagementPolicy

すべての AMS 変更タイプをリクエストおよび表示するアクセス許可、およびリクエストされた変更タイプの履歴。

## AMSPurchaseReservedInstancesPolicy

### AMSPurchaseReservedInstancesPolicy

Amazon EC2 リザーブドインスタンスを管理するアクセス許可。料金情報については、[Amazon EC2 リザーブドインスタンス](#)」を参照してください。

## JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AllowReservedInstancesManagement",
    "Effect": "Allow",
    "Action": [
      "ec2:ModifyReservedInstances",
      "ec2:PurchaseReservedInstancesOffering"
    ],
    "Resource": [
      "*"
    ]
  }]
}
```

## AMSS3Policy

### AMSS3Policy

既存の Amazon S3 バケットからファイルを作成および削除するアクセス許可。

#### Note

これらのアクセス許可は、デプロイ | 高度なスタックコンポーネント | S3 ストレージ | 変更タイプの作成で実行する必要がある S3 バケットを作成する機能を付与しません。

## JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:PutObject"
      ],
      "Resource": "*"
    }
  ]
}
```

### AWSSupportAccess

### AWSSupportAccess

へのフルアクセス サポート。詳細については、[「 の開始方法 サポート 」](#)を参照してください。プレミアムサポートの詳細については、「」を参照してください[サポート](#)。

## JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "support:*"
    ],
    "Resource": "*"
  }]
}
```

## AWSMarketplaceManageSubscriptions

### AWSMarketplaceManageSubscriptions (パブリック AWS 管理ポリシー)

AWS Marketplace サブスクリプションをサブスクライブ、サブスクライブ解除、表示するアクセス許可。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "aws-marketplace:ViewSubscriptions",
      "aws-marketplace:Subscribe",
      "aws-marketplace:Unsubscribe"
    ],
    "Effect": "Allow",
    "Resource": "*"
  }]
}
```

## AWSCertificateManagerFullAccess

### AWSCertificateManagerFullAccess

へのフルアクセス AWS Certificate Manager。詳細については、「[AWS Certificate Manager](#)」を参照してください。

[AWSCertificateManagerFullAccess](#) information、(パブリック AWS 管理ポリシー)。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "acm:*"
    ],
  },
```



```
"Resource": "*"
}]
}
```

AWSWAFFullAccess

AWSWAFFullAccess

へのフルアクセス AWS WAF。詳細については、「[AWS WAF - Web Application Firewall](#)」を参照してください。

[AWSWAFFullAccess](#) information、(パブリック AWS 管理ポリシー)。このポリシーは、AWS WAF リソースへのフルアクセスを許可します。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "waf:*",
      "waf-regional:*",
      "elasticloadbalancing:SetWebACL"
    ],
    "Effect": "Allow",
    "Resource": "*"
  }]
}
```

ReadOnlyAccess

ReadOnlyAccess

AWS コンソール上のすべての AWS サービスとリソースへの読み取り専用アクセス。が新しいサービス AWS を起動すると、AMS は ReadOnlyAccess ポリシーを更新して、新しいサービスの読み取り専用アクセス許可を追加します。更新されたアクセス権限は、ポリシーがアタッチされているすべてのプリンシパルエンティティに適用されます。

これにより、EC2 ホストまたはデータベースホストにログインすることはできません。

アクティブな [がある場合は AWS アカウント](#)、このリンク [ReadOnlyAccess](#) を使用して ReadOnlyAccess ポリシー全体を表示できます。ReadOnlyAccess ポリシー全体は、すべてへの読み取り専用アクセスを提供する限り非常に長くなります AWS のサービス。以下は、ReadOnlyAccess ポリシーの一部の抜粋です。

単一アカウントランディングゾーン (SALZ): AMS シングルアカウントランディングゾーンのデフォルト、カスタマイズされていないユーザーロールポリシーを確認するには、[SALZ: デフォルトの IAM ユーザーロール](#) 次の「」を参照してください。

SALZ: デフォルトの IAM ユーザーロール

デフォルトの AMS シングルアカウントランディングゾーンユーザーロールの JSON ポリシーステートメント。

 Note

SALZ のデフォルトのユーザーロールはカスタマイズ可能で、アカウントごとに異なる場合があります。ロールの検索手順が表示されます。

デフォルトの SALZ ユーザーロールの例を次に示します。ポリシーが設定されていることを確認するには、[get-role](#) コマンドを実行します。または、<https://console.aws.amazon.com/iam/> で AWS Identity and Access Management コンソールにサインインし、ロールを選択します。

顧客の読み取り専用ロールは、複数のポリシーの組み合わせです。ロール (JSON) の内訳は次のとおりです。

マネージドサービス監査ポリシー:

マネージドサービス IAM ReadOnly ポリシー

マネージドサービスユーザーポリシー

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCustomerToListTheLogBucketLogs",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket"
```

```
    ],
    "Resource": [
        "arn:aws:s3:::mc-a*-logs-*"
    ],
    "Condition": {
        "StringLike": {
            "s3:prefix": [
                "aws/*",
                "app/*",
                "encrypted",
                "encrypted/",
                "encrypted/app/*"
            ]
        }
    }
},
{
    "Sid": "BasicAccessRequiredByS3Console",
    "Effect": "Allow",
    "Action": [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
    ],
    "Resource": [
        "arn:aws:s3:::*"
    ]
},
{
    "Sid": "AllowCustomerToGetLogs",
    "Effect": "Allow",
    "Action": [
        "s3:GetObject*"
    ],
    "Resource": [
        "arn:aws:s3:::mc-a*-logs-*/aws/*",
        "arn:aws:s3:::mc-a*-logs-*/encrypted/app/*"
    ]
},
{
    "Sid": "AllowAccessToOtherObjects",
    "Effect": "Allow",
    "Action": [
        "s3:DeleteObject*",
        "s3:Get*",
```

```
        "s3:List*",
        "s3:PutObject*"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "AllowCustomerToListTheLogBucketRoot",
    "Effect": "Allow",
    "Action": [
        "s3:ListBucket"
    ],
    "Resource": [
        "arn:aws:s3:::mc-a*-logs-*"
    ],
    "Condition": {
        "StringEquals": {
            "s3:prefix": [
                "",
                "/"
            ]
        }
    }
},
{
    "Sid": "AllowCustomerCWLConsole",
    "Effect": "Allow",
    "Action": [
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups"
    ],
    "Resource": [
        "arn:aws:logs:*:*:log-group:*"
    ]
},
{
    "Sid": "AllowCustomerCWLAccessLogs",
    "Effect": "Allow",
    "Action": [
        "logs:FilterLogEvents",
        "logs:GetLogEvents"
    ],
    "Resource": [
```

```
    "arn:aws:logs:*:*:log-group:/aws/*",
    "arn:aws:logs:*:*:log-group:/infra/*",
    "arn:aws:logs:*:*:log-group:/app/*",
    "arn:aws:logs:*:*:log-group:RDSOSMetrics:*:*"
  ],
},
{
  "Sid": "AWSManagedServicesFullAccess",
  "Effect": "Allow",
  "Action": [
    "amscm:*",
    "amsskms:*"
  ],
  "Resource": [
    "*"
  ]
},
{
  "Sid": "ModifyAWSBillingPortal",
  "Effect": "Allow",
  "Action": [
    "aws-portal:Modify*"
  ],
  "Resource": [
    "*"
  ]
},
{
  "Sid": "DenyDeleteCWL",
  "Effect": "Deny",
  "Action": [
    "logs:DeleteLogGroup",
    "logs:DeleteLogStream"
  ],
  "Resource": [
    "arn:aws:logs:*:*:log-group:*"
  ]
},
{
  "Sid": "DenyMCCWL",
  "Effect": "Deny",
  "Action": [
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
```

```
        "logs:DescribeLogStreams",
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:PutLogEvents"
    ],
    "Resource": [
        "arn:aws:logs:*:*:log-group:/mc/*"
    ]
},
{
    "Sid": "DenyS3MCNamespace",
    "Effect": "Deny",
    "Action": [
        "s3:*"
    ],
    "Resource": [
        "arn:aws:s3:::mc-a*-logs-*/encrypted/mc/*",
        "arn:aws:s3:::mc-a*-logs-*/mc/*",
        "arn:aws:s3:::mc-a*-logs-*/audit/*",
        "arn:aws:s3:::mc-a*-internal-*/*",
        "arn:aws:s3:::mc-a*-internal-*"
    ]
},
{
    "Sid": "ExplicitDenyS3CfnBucket",
    "Effect": "Deny",
    "Action": [
        "s3:*"
    ],
    "Resource": [
        "arn:aws:s3:::cf-templates-*"
    ]
},
{
    "Sid": "DenyListBucketS3LogsMC",
    "Action": [
        "s3:ListBucket"
    ],
    "Effect": "Deny",
    "Resource": [
        "arn:aws:s3:::mc-a*-logs-*"
    ],
    "Condition": {
        "StringLike": {
```

```
        "s3:prefix": [
            "auditlog/*",
            "encrypted/mc/*",
            "mc/*"
        ]
    },
    {
        "Sid": "DenyS3LogsDelete",
        "Effect": "Deny",
        "Action": [
            "s3:Delete*",
            "s3:Put*"
        ],
        "Resource": [
            "arn:aws:s3:::mc-a*-logs-*/*"
        ]
    },
    {
        "Sid": "DenyAccessToKmsKeysStartingWithMC",
        "Effect": "Deny",
        "Action": [
            "kms:*"
        ],
        "Resource": [
            "arn:aws:kms::*:key/mc-*",
            "arn:aws:kms::*:alias/mc-*"
        ]
    },
    {
        "Sid": "DenyListingOfStacksStartingWithMC",
        "Effect": "Deny",
        "Action": [
            "cloudformation:*"
        ],
        "Resource": [
            "arn:aws:cloudformation::*:stack/mc-*"
        ]
    },
    {
        "Sid": "AllowCreateCWMetricsAndManageDashboards",
        "Effect": "Allow",
        "Action": [
```



```

        "cloudwatch:PutMetricData"
    ],
    "Resource": [
        "*"
    ]
  },
  {
    "Sid": "AllowCreateandDeleteCWDashboards",
    "Effect": "Allow",
    "Action": [
        "cloudwatch:DeleteDashboards",
        "cloudwatch:PutDashboard"
    ],
    "Resource": [
        "*"
    ]
  }
]
}

```

## Customer Secrets Manager 共有ポリシー

### JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSecretsManagerListSecrets",
      "Effect": "Allow",
      "Action": "secretsmanager:listSecrets",
      "Resource": "*"
    },
    {
      "Sid": "AllowCustomerAdminAccessToSharedNameSpaces",
      "Effect": "Allow",
      "Action": "secretsmanager:*",
      "Resource": [
        "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
        "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
      ]
    }
  ]
}

```

```
    "Sid": "DenyCustomerGetSecretCustomerNamespace",
    "Effect": "Deny",
    "Action": "secretsmanager:GetSecretValue",
    "Resource": "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
  },
  {
    "Sid": "AllowCustomerReadOnlyAccessToAMSNameSpace",
    "Effect": "Deny",
    "NotAction": [
      "secretsmanager:Describe*",
      "secretsmanager:Get*",
      "secretsmanager:List*"
    ],
    "Resource": "arn:aws:secretsmanager:*:*:secret:ams-shared/*"
  }
]
```

## Customer Marketplace サブスクリプションポリシー

### JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowMarketPlaceSubscriptions",
      "Effect": "Allow",
      "Action": [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Subscribe"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

## セキュリティイベントのロギングとモニタリング

AMS は、マネージド環境のセキュリティ脅威を継続的にモニタリングします。セキュリティイベントは、AMS またはユーザーによって検出される場合があります。AMS は、米国国立標準技術研究所 (NIST) のコンピュータセキュリティインシデント処理ガイドに基づいてオートメーションプロセスを定期的に更新し、セキュリティの脅威をより適切に検出します。

### エンドポイントセキュリティ (EPS)

AMS Advanced 環境でプロビジョニングするリソースには、エンドポイントセキュリティ (EPS) モニタリングクライアントのインストールが自動的に含まれます。このプロセスにより、AMS Advanced が管理するリソースが 24 時間 365 日モニタリングおよびサポートされます。さらに、AMS Advanced はすべてのエージェントアクティビティをモニタリングし、セキュリティイベントが検出されるとインシデントが作成されます。

#### Note

セキュリティインシデントはインシデントとして処理されます。詳細については、[「インシデント対応」](#)を参照してください。

エンドポイントセキュリティはマルウェア対策保護を提供します。具体的には、以下のアクションがサポートされています。

- EC2 インスタンスが EPS に登録される
- EC2 インスタンスが EPS から登録解除する
- EC2 インスタンスのマルウェア対策のリアルタイム保護
- EPS エージェントが開始したハートビート
- 隔離されたファイルの EPS 復元
- EPS イベント通知
- EPS レポート

AMS Advanced は、エンドポイントセキュリティ (EPS) に Trend Micro を使用します。これらはデフォルトの EPS 設定です。Trend Micro の詳細については、[Trend Micro Deep Security ヘルプセンター](#)を参照してください。Amazon 以外のリンクは予告なしに変更される可能性があります。

AMS Advanced Multi-Account Landing Zone (MALZ) のデフォルト設定については、以下のセクションで説明します。デフォルト以外の AMS Multi-Account Landing Zone の EPS 設定については、[「AMS Advanced Multi-Account Landing Zone の EPS のデフォルト以外の設定」](#)を参照してください。

 Note

独自の EPS を持ち込むことができます。[「AMS bring your own EPS」](#)を参照してください。

## 一般的な EPS 設定

エンドポイントセキュリティの一般的なネットワーク設定。

### EPS のデフォルト

| 設定                              | デフォルト                                                                                                                                                                                                                                  |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ファイアウォールポート (インスタンスのセキュリティグループ) | EPS Deep Security Manager エージェント (DSMs) では、エージェント/リレーからマネージャーへの通信用にポート 4120 を開き、マネージャーコンソール用にポート 4119 を開く必要があります。EPS リレーでは、マネージャー/エージェントが通信を中継するためにポート 4122 を開く必要があります。エージェントがすべてのリクエストを開始するため、カスタマーインスタンスのインバウンド通信に特定のポートを開くことはできません。 |
| 通信方向                            | エージェント/アプライアンスが開始されました                                                                                                                                                                                                                 |
| ハートビート間隔                        | 10 分                                                                                                                                                                                                                                   |
| アラートまでに見逃されたハートビートの数            | 2                                                                                                                                                                                                                                      |
| サーバー時間間の最大許容ドリフト (差分)           | 無制限                                                                                                                                                                                                                                    |

| 設定                                            | デフォルト                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 非アクティブ (登録済みだがオンラインではない) 仮想マシンのオフラインエラーを発生させる | なし                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| デフォルトポリシー                                     | 基本ポリシー (次に説明 )                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 同じホスト名の複数のコンピュータのアクティベーション                    | 許可されます                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 保留中の更新のアラートが生成されます                            | 7 日後                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| スケジュールの更新                                     | <p>AMS は、Trend Micro Deep Security Manager (DSM) / Deep Security Agent (DSA) ソフトウェア更新の毎月のリリースサイクルを対象としています。ただし、AMS は更新の SLA を維持しません。更新は、デプロイ中に AMS 開発者チームによってフリート全体で実行されます。</p> <p>DSA/DSA 更新は、AMS がデフォルトで 13 週間ローカルに保持する Trend Micro DSM システムイベントに記録されます。ベンダーのドキュメントについては、Trend Micro Deep Security ヘルプセンターの「<a href="#">システムイベント</a>」を参照してください。ログは、Amazon CloudWatch のロググループ <code>/aws/ams/eps/var/log/DSM.log</code> にもエクスポートされます。</p> |
| ソースの更新                                        | Trend Micro Update Server ( <a href="https://ipv6-iaus.trendmicro.com/iau_server.dll/">https://ipv6-iaus.trendmicro.com/iau_server.dll/</a> )                                                                                                                                                                                                                                                                                              |
| イベントまたはログデータの削除                               | イベントとログは、7 日後に DSM データベースから削除されます。                                                                                                                                                                                                                                                                                                                                                                                                         |
| エージェントソフトウェアバージョンが保持されている                     | 最大 5 つ                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 最新のルール更新が保持されます                               | 最大 10 個                                                                                                                                                                                                                                                                                                                                                                                                                                    |

| 設定      | デフォルト                                                                                        |
|---------|----------------------------------------------------------------------------------------------|
| ログストレージ | デフォルトでは、ログファイルは Amazon S3 に安全に保存されますが、監査およびコンプライアンス要件を満たすために Amazon Glacier にアーカイブすることもできます。 |

## 基本ポリシー

エンドポイントセキュリティの基本ポリシーのデフォルト設定。

### EPS ベースポリシー

| 設定       | デフォルト          |
|----------|----------------|
| 有効なモジュール | マルウェア対策        |
| 無効なモジュール | ウェブ評価          |
|          | ファイアウォール       |
|          | 侵入保護           |
|          | 整合性モニタリング      |
|          | ログ検査           |
|          | アプリケーションコントロール |

## マルウェア対策

エンドポイントセキュリティのマルウェア対策設定。

### EPS マルウェア対策のデフォルト

| 設定         | デフォルト         | 注意                                     |
|------------|---------------|----------------------------------------|
| リアルタイムスキャン | すべてをスキャンする    | 疑わしいウイルスをすべて隔離します。<br>IntelliTrap とスパイ |
|            | 毎日/毎日 (24 時間) |                                        |

| 設定                   | デフォルト                                   | 注意                                    |
|----------------------|-----------------------------------------|---------------------------------------|
|                      |                                         | ウェア/グレーウェアの保護を有効にします。                 |
|                      |                                         | スパイウェアとグレーウェアはマルウェア対策をトリガーし、項目を隔離します。 |
| 手動スキャン               | すべてをスキャンする                              | リクエストする必要がある、デフォルトのリアルタイムスキャン設定に従います。 |
| スケジュールされたスキャン        | すべてをスキャンする                              | 毎月最終日曜日の午前 6 時に を設定します。               |
| スマート保護               | 無効                                      | 該当なし                                  |
| 隔離されたファイル            | Trend Micro Deep Security Manager (DSM) | 隔離用に予約された約 1GB のディスク。                 |
| スキャンの制限              | Trend Micro DSM                         | すべてのサイズのファイルをスキャンします。                 |
| 許可されたスパイウェアまたはグレーウェア | なし                                      | 該当なし                                  |
| ローカルイベント通知           | あり                                      | 該当なし                                  |



## マルウェアの軽減プロセス

AMS は、Trend Micro の Deep Security Platform (マルウェア対策システム) を使用して、AMS マネージドインスタンスのマルウェアを検出して対応します。デフォルトでは、Trend Micro 検出エージェントは、Windows オペレーティングシステムと Linux オペレーティングシステムの両方で、共有サービスおよびプライベートサブネット内のインスタンスを含むすべての Amazon EC2 インスタンスで実行されます。マルウェア対策システムは AMS モニタリングに接続されているため、マルウェアが検出されるたびにイベントが生成されます。顧客への影響がある場合、イベントはインシデント管理プロセスにエスカレーションされます (詳細については、「」を参照してください[AMS インシデント対応](#))。AMS が影響を評価する間、通知を受け取り、影響を軽減しようとします。

Trend Micro が更新を発行すると、Trend Micro のマルウェア対策定義が自動的に更新されます。

アプリケーションのオンボーディング中に、インスタンスでマルウェアが見つかったときに AMS が実行するアクションを指定します。

- 隔離されたファイルが許可リストに含まれていることを確認し、隔離から削除してファイルシステムにリリースします。
- 隔離されたファイルを削除し、インスタンスから削除します。
- インスタンスを停止して置き換えます。その後、中断されたインスタンスは、フォレンジック調査のためにマウントできます。

アプリケーションのオンボーディング後：

- マルウェア対策システムがインスタンスでマルウェアを検出すると、AMS は自動的にマルウェアを隔離します。これにより、イベントとフォローアップ調査がトリガーされます。
- AMS は、サービス通知を通じてイベントを通知し、選択したデフォルトの緩和アクションに従って開始します。
- デフォルトのアクションを選択していない場合、AMS は実行するアクションを尋ねます。指示を受け取ると、AMS は選択したアクションを実行し、通知します。AMS は、該当する場合、フォレンジック分析に必要な詳細など、アクションの完了後に再度通知します。

### Trend Micro Deep Security で IDS と IPS を有効にする

アカウントのデフォルト以外の機能である Trend Micro Intrusion Detection System (IDS) と Intrusion Protection Systems (IPS) を有効にするように AMS にリクエストできます。

これを行うには、更新リクエスト (管理 | その他 | その他 | 更新) を送信し、IDS および IPS 通知を受信する E メールアドレスのリストを含めます。これらのアドレスは、AMS が作成するアカウントの SNS トピックに追加されます。

#### Note

AMS は、他の AMS サービスを提供する能力を妨げる可能性のある Trend Micro サービスを追加することはできません。

## システム全体のマルウェアスキャン

Payment Card Industry Data Security Standard (PCI DSS) では、AMS マネージド VPC でデフォルトで有効になっている完全なシステムマルウェアスキャンが必要です。フルシステムスキャンは、大量の CPU を使用するため、2AM 時 (サーバーで設定されたタイムゾーン) に行われます。フルシステムスキャンは、多くの CPU を使用しない通常のマルウェアスキャンに加えて行われます。

新しい管理変更タイプ (CT) であるマルウェアスキャンを無効にします。これにより、システム全体のマルウェアスキャンを無効にできます。CT は、Management | Host security | Full system scan | Disable classification, change ID ct-1pybwg08h8qsz にあります。スキャンを再度有効にするには、管理 | その他 | その他 | CT の更新を使用します。フルシステムスキャンを無効にしても、通常のマルウェアスキャンは無効になりません。

## Amazon Inspector のセキュリティ

Amazon Inspector サービスは、AMS マネージドスタックのセキュリティをモニタリングします。Amazon Inspector は、デプロイされたインフラストラクチャのセキュリティとコンプライアンスのギャップを特定するのに役立つ自動セキュリティ評価サービスです。AWS。Amazon Inspector セキュリティ評価では、Amazon EC2 インスタンスの意図しないネットワークアクセシビリティと脆弱性をチェックすることで、スタックの露出、脆弱性、ベストプラクティスからの逸脱を自動的に評価できます。評価を実行した後、Amazon Inspector は、重要度のレベルごとに優先順位が付けられたセキュリティ結果の詳細なリストを作成します。Amazon Inspector の評価は、一般的なセキュリティのベストプラクティスと定義にマッピングされた事前定義されたルールパッケージとして提供されます。これらのルールは、AWS セキュリティ研究者によって定期的に更新されます。Amazon Inspector の詳細については、[Amazon Inspector](#) を参照してください。

### AMS Amazon Inspector FAQs

- Amazon Inspector はデフォルトで AMS アカウントにインストールされていますか？

いいえ。Amazon Inspector はデフォルトの AMI ビルドまたはワークロード取り込みの一部ではありません。

- Amazon Inspector にアクセスしてインストールするにはどうすればよいですか？

RFC (管理 | その他 | その他 | 作成) を送信して、アカウントアクセスとインストールを Inspector にリクエストします。AMS オペレーションチームは Customer\_ReadOnly\_Role を変更して、Amazon Inspector コンソールアクセス (SSM アクセスなし) を提供します。

- Amazon Inspector エージェントは、評価するすべての Amazon EC2 インスタンスにインストールする必要がありますか？

いいえ。ネットワーク到達可能性ルールパッケージを使用した Amazon Inspector 評価は、Amazon EC2 インスタンスのエージェントなしで実行できます。エージェントはホスト評価ルールパッケージに必要です。エージェントのインストールの詳細については、[Amazon Inspector エージェントのインストール](#)」を参照してください。

- このサービスには追加料金がかかりますか？

はい。Amazon Inspector の料金は、[Amazon Inspector の料金](#)サイトで確認できます。

- Amazon Inspector の検出結果とは

検出結果は、選択した評価ターゲットの Amazon Inspector 評価中に検出された潜在的なセキュリティ問題です。結果は Amazon Inspector コンソールまたは API に表示され、セキュリティの問題の詳細な説明とそれらを解決するための推奨事項の両方が含まれます。

- Amazon Inspector 評価のレポートは利用できますか？

はい。評価レポートは評価の実行で行われたテストの詳細と、評価の結果を記述したドキュメントです。評価の結果はスタンダードレポート形式です。このレポートはチーム内で結果を共有できるように生成し、コンプライアンスの監査データの強化または今後の参照情報として保存することができます。Amazon Inspector 評価レポートは、評価が正常に完了すると、評価の実行用に生成できます。

- タグを使用して、Amazon Inspector レポートを実行するスタックを識別できますか？

はい。

- AMS オペレーションチームは Amazon Inspector の評価結果にアクセスできますか？

はい。AWS で Amazon Inspector コンソールにアクセスできるユーザーは、結果と評価レポートを表示できます。

- AMS オペレーションチームは、Amazon Inspector レポートの結果に基づいて推奨またはアクションを実行しますか？

いいえ。Amazon Inspector レポートの結果に基づいて変更を行う場合は、RFC (管理 | その他 | その他 | 更新) を通じて変更をリクエストする必要があります。

- Amazon Inspector レポートを実行すると、AMS に通知されますか？

Amazon Inspector アクセスをリクエストすると、RFC を実行している AMS オペレーターがリクエストを CSDM に通知します。

詳細については、[Amazon Inspector のFAQs](#)」を参照してください。

## AMS インシデント対応

AMS は、従来の IT サービス管理 (ITSM) インシデント管理のベストプラクティスを使用して、必要に応じてできるだけ早くサービスを復元します。

専任のオペレーターがダッシュボードとインシデントキューを積極的にモニタリングし、世界中の複数のオペレーションセンターを通じて 24 時間 365 日 follow-the-sun サポートを提供しています。

オペレーションエンジニアは、内部インシデント追跡ツールを使用して、インシデントを特定、ログ記録、分類、優先順位付け、診断、解決、クローズし、AMS コンソールまたは サポート API を通じてこれらのすべてのアクティビティの更新を提供します。オペレーターの多くは、さまざまなテクノロジープロファイルとロールで AWS プレミアムサポートに時間を費やしており、さまざまな内部 サポート ツールを活用してこれらのアクティビティをすべて支援しています。これらのオペレーターは、AMS がサポートするインフラストラクチャに深く精通しており、特定されたすべてのサポート問題に対処するためのエキスパートレベルの技術スキルを持っています。オペレーターがサポートを必要とするまれなケースでは、プレミアムサポートチームと AWS サービスチームが必要に応じてサポートできます。

優先度の高いインシデントが重要なワークロードに影響を与えている場合、AMS はインフラストラクチャの復元を推奨します。多くの場合、問題のトラブルシューティングと既知の正常なバックアップからの復元の間にはトレードオフがあり、サービスのダウンタイムによる顧客のリスクと影響が決定要因です。問題のトラブルシューティングに専念する時間がある場合は、AMS がお手伝いしますが、復元の緊急性が高い場合は、すぐに復元を開始できます。

**Note**

スタックテンプレートの一部ではないエフェメラルデータやデータ復元は失われます。AMS は、AWS サービス提供が利用できない間にインフラストラクチャの復元を実行するために合理的な努力を払います。AWS サービスが利用可能になると、インフラストラクチャの復元が完了します。

AMS の推奨に従ってインフラストラクチャの復元を許可しない場合、インシデント解決時間に対する AMS サービスコミットメントのサービスクレジットは付与されません。

## コンプライアンス検証

AMS は、AWS Config ルールと修復アクションのライブラリをデプロイおよび管理し、アカウントのセキュリティと運用の整合性を低下させる可能性のある設定ミスから保護します。

例えば、Amazon S3 バケットが作成されると、は Amazon S3 バケットがパブリック読み取りアクセスを拒否する必要があるルールに対して Amazon S3 バケットを評価 AWS Config できます。Amazon S3 バケットポリシーまたはバケットアクセスコントロールリスト (ACL) がパブリック読み取りアクセスを許可している場合、はバケットとルールの両方を非準拠として AWS Config フラグ付けします。これらは、評価の結果に基づいて、リソースを準拠、非準拠、または該当なしとして AWS Config ルール マークします。AWS Config サービスの詳細については、「[AWS Config デベロッパーガイド](#)」を参照してください。

AWS Config コンソール、AWS CLI、または AWS Config API を使用して、アカウントにデプロイされたルールと、ルールとリソースのコンプライアンス状態を表示できます。詳細については、「AWS Config ドキュメント: [設定コンプライアンスの表示](#)」を参照してください。

**Note**

このトピックに関する追加情報は、AWS Artifact レポートにアクセスして入手できます。詳細については、「[AWS Artifact のレポートのダウンロード](#)」をご参照ください。AWS Artifact にアクセスするには、CSDM に連絡して手順を確認するか、「[AWS Artifact の開始方法](#)」を参照してください。このユーザーガイドには機密性の高いセキュリティコンテンツが含まれているため、この情報は含まれていません。

# のコンプライアンスステータスを表示するマルチアカウントランディングゾーン AWS Config ルール

AMS マルチアカウントランディングゾーンは AWS Config 、アグリゲータサービスを利用して、すべてのアカウントのコンプライアンスを一元的に表示します。つまり、セキュリティアカウントのアグリゲータで、AMS マルチアカウントランディングゾーン環境 AWS Config ルール 全体のすべての AWS Config のコンプライアンスステータスを確認できます。

以下は、アカウント AWS Config ルール 間で AWS Config の中央コンプライアンスステータスを示すアグリゲータのサンプルです。

詳細については、[Config Aggregator](#) の AWS ドキュメントを参照してください。

- AMS は AWS Config ルールをどのように使用しますか？

AMS は を作成して AWS Config ルール 、ルールで指定された条件に対する AWS リソースの設定を可視化します。ルールが準拠していない場合は、変更をリクエストできます。AMS Ops チームがお客様と協力して是正措置を取ります。

- この場合、AMS アカウントに次の変更が表示されます。
  - AWS Config ルール AWS Config > ルールの下
  - Lambda 関数を含むカスタム Config ルールがアカウントに存在する
  - セキュリティアカウントの Config Aggregator とすべてのアカウントの Config 認可 (マルチアカウントランディングゾーンのみ)

以下は のサンプル AWS Config ルール であり、そのコンプライアンス評価結果を以下に示します。

AWS Config の詳細については、以下を参照してください。

- AWS Config: [Config とは](#)
- AWS Config ルール: [ルールを使用したリソースの評価](#)
- AWS Config ルール: [動的コンプライアンスチェック: AWS Config ルール – クラウドリソースの動的コンプライアンスチェック](#)
- AWS Config Aggregator: [マルチアカウントマルチリージョンデータ集約](#)



# AMS マルチアカウントランディングゾーンサービスコントロールポリシーの制限

このセクションは、機密性の高い AMS セキュリティ関連情報が含まれているため、編集されています。この情報は、AMS コンソールのドキュメントから入手できます。AWS Artifact にアクセスするには、CSDM に連絡して手順を確認するか、[「AWS Artifact の開始方法」](#)を参照してください。

## 耐障害性

AWS グローバルインフラストラクチャは、AWS リージョン およびアベイラビリティゾーンを中心に構築されています。は、低レイテンシー、高スループット、高度に冗長なネットワークで接続された、物理的に分離および分離された複数のアベイラビリティゾーン AWS リージョン を提供します。アベイラビリティゾーンでは、ゾーン間で中断することなく自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性が高く、フォールトトレラントで、スケーラブルです。

AWS リージョンとアベイラビリティゾーンの詳細については、[AWS 「グローバルインフラストラクチャ」](#)を参照してください。

## インフラストラクチャセキュリティ

### Note

このトピックに関する追加情報は、AWS Artifact レポートにアクセスして入手できます。詳細については、「[AWS Artifact のレポートのダウンロード](#)」をご参照ください。AWS Artifact にアクセスするには、CSDM に連絡して手順を確認するか、[「AWS Artifact の開始方法」](#)を参照してください。このユーザーガイドには機密性の高いセキュリティコンテンツが含まれているため、この情報は含まれていません。

## end-of-supportオペレーティングシステムのセキュリティコントロール

オペレーティングシステム製造元のend-of-support」または EOS の一般的なサポート期間外であり、セキュリティ更新プログラムを受け取らないオペレーティングシステムでは、セキュリティリスクが高くなります。



AWS には、オペレーションシステムのend-of-supportの処理に役立つサービスがいくつか用意されています。Windows end-of-supportの詳細については、[「Windows Server End-of-Support移行プログラム」](#)を参照してください。

#### Note

このトピックに関する追加情報は、AWS Artifact レポートにアクセスして入手できます。詳細については、「[<shared id="AWS"/> Artifact のレポートのダウンロード](#)」をご参照ください。AWS Artifact にアクセスするには、CSDM に連絡して手順を確認するか、[「AWS Artifact の開始方法」](#)を参照してください。このユーザーガイドには機密性の高いセキュリティコンテンツが含まれているため、この情報は含まれていません。

## セキュリティグループの使用

セキュリティグループは、1 つ以上のインスタンスのトラフィックを制御する仮想ファイアウォールとして機能します。AMS セキュリティグループを使用すると、インバウンドトラフィックルールとアウトバウンドトラフィックルールをインスタンスレベルで設定できます。セキュリティグループを作成し、AMS アカウント、Amazon EC2 インスタンス、Amazon RDS DB インスタンス、ロードバランサー、Deep Security Manager (DSM) レプリケーションインスタンス、EFS マウントターゲット、ElastiCache クラスターでリソースを指定して、セキュリティグループに関連付けることができます。関連付けられると、それらのインスタンスとの間のトラフィックは、セキュリティグループで設定されたルールによって制約されます。

一般的な AWS セキュリティの詳細については、「[Best Practices for Security, Identity, & Compliance](#)」および[Amazon EC2 Security Groups for Linux Instances](#)」を参照してください。

AMS に、セキュリティグループを作成および管理するための一連の変更タイプが追加されました。

- デプロイ | 高度なスタックコンポーネント | セキュリティグループ | 作成 (ct-10xx2g2d7hc90)
- 管理 | 高度なスタックコンポーネント | セキュリティグループ | 削除 (ct-3cp96z7r065e4)
- 管理 | 高度なスタックコンポーネント | セキュリティグループ | 更新 (ct-3memthlcmvc1b)

例については、「[セキュリティグループ](#)」を参照してください。

## セキュリティグループ

AWS VPCs では、AWS セキュリティグループは仮想ファイアウォールとして機能し、1 つ以上のスタック (インスタンスまたは一連のインスタンス) のトラフィックを制御します。スタックを起動

すると、スタックは 1 つ以上のセキュリティグループに関連付けられ、スタックに到達できるトラフィックが決まります。

- パブリックサブネットのスタックの場合、デフォルトのセキュリティグループはすべての場所 (インターネット) からの HTTP (80) および HTTPS (443) からのトラフィックを受け入れます。スタックは、企業ネットワークからの内部 SSH および RDP トラフィック、および AWS 踏み台も受け入れます。これらのスタックは、任意のポートを介してインターネットに出力できます。また、プライベートサブネットやパブリックサブネット内の他のスタックに出力することもできます。
- プライベートサブネット内のスタックは、プライベートサブネット内の他のスタックに出力でき、スタック内のインスタンスは、任意のプロトコルを介して相互に完全に通信できます。

#### Important

プライベートサブネット上のスタックのデフォルトのセキュリティグループでは、プライベートサブネット内のすべてのスタックが、そのプライベートサブネット内の他のスタックと通信できます。プライベートサブネット内のスタック間の通信を制限する場合は、制限を記述する新しいセキュリティグループを作成する必要があります。たとえば、そのプライベートサブネット内のスタックが特定のポート経由で特定のアプリケーションサーバーからのみ通信できるようにデータベースサーバーとの通信を制限する場合は、特別なセキュリティグループをリクエストします。これを行う方法については、このセクションで説明します。

## デフォルトのセキュリティグループ

### MALZ

次の表に、スタックのデフォルトのインバウンドセキュリティグループ (SG) 設定を示します。SG は SentinelDefaultSecurityGroupPrivateOnly-vpc-ID」という名前で、**ID** は AMS マルチアカウントランディングゾーンアカウントの VPC ID です。すべてのトラフィックは、このセキュリティグループ経由で mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnly」へのアウトバウンドが許可されます (スタックサブネット内のすべてのローカルトラフィックが許可されます)。

すべてのトラフィックは、2 番目のセキュリティグループ SentinelDefaultSecurityGroupPrivateOnly」によって 0.0.0.0/0 へのアウトバウンドが許可されます。

**i** Tip

EC2 create や OpenSearch create ドメインなどの AMS 変更タイプのセキュリティグループを選択する場合は、ここで説明するデフォルトのセキュリティグループのいずれか、または作成したセキュリティグループを使用します。VPC ごとのセキュリティグループのリストは、AWS EC2 コンソールまたは VPC コンソールで確認できます。

内部 AMS 目的で使用される追加のデフォルトのセキュリティグループがあります。

## AMS デフォルトセキュリティグループ (インバウンドトラフィック)

| タイプ             | プロトコル | ポート範囲                           | ソース                                                                           |
|-----------------|-------|---------------------------------|-------------------------------------------------------------------------------|
| すべてのトラフィック      | すべて   | すべて                             | SentinelDefaultSecurityGroupPrivateOnly (同じセキュリティグループのメンバーへのアウトバウンドトラフィックを制限) |
| すべてのトラフィック      | すべて   | すべて                             | SentinelDefaultSecurityGroupPrivateOnlyEgressAll (アウトバウンドトラフィックを制限しません)       |
| HTTP、HTTPS、SSH、 | TCP   | 80 / 443 (ソース 0.0.0.0/0)        | SentinelDefaultSecurityGroupPublic (アウトバウンドトラフィックを制限しません)                     |
|                 |       | 踏み台からの SSH および RDP アクセスが許可されている |                                                                               |
| MALZ 踏み台:       |       |                                 |                                                                               |
| SSH             | TCP   | 22                              | SharedServices VPC CIDR と DMZ VPC CIDR、およびお客様が用意したオンプレミス CIDRs                |
| SSH             | TCP   | 22                              |                                                                               |
| RDP             | TCP   | 3389                            |                                                                               |

| タイプ | プロトコル | ポート範囲 | ソース |
|-----|-------|-------|-----|
| RDP | TCP   | 3389  |     |

SALZ 踏み台:

|     |     |      |                                       |
|-----|-----|------|---------------------------------------|
| SSH | TCP | 22   | mc-initial-garden-LinuxBastionSG      |
| SSH | TCP | 22   | mc-initial-garden-LinuxBastionDMZSG   |
| RDP | TCP | 3389 | mc-initial-garden-WindowsBastionSG    |
| RDP | TCP | 3389 | mc-initial-garden-WindowsBastionDMZSG |

## SALZ

次の表に、スタックのデフォルトのインバウンドセキュリティグループ (SG) 設定を示します。SG の名前は `mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnly-ID` で、**ID** は一意の識別子です。すべてのトラフィックは、このセキュリティグループ経由で `mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnly` へのアウトバウンドが許可されます (スタックサブネット内のすべてのローカルトラフィックが許可されます)。

すべてのトラフィックは、2 番目のセキュリティグループ `mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnlyEgressAll-0` へのアウトバウンドが許可されます。

### Tip

EC2 create や OpenSearch create ドメインなどの AMS 変更タイプのセキュリティグループを選択する場合は、ここで説明するデフォルトのセキュリティグループのいずれか、または作成したセキュリティグループを使用します。VPC ごとのセキュリティグループのリストは、AWS EC2 コンソールまたは VPC コンソールで確認できます。

内部 AMS 目的で使用される追加のデフォルトのセキュリティグループがあります。

## AMS デフォルトセキュリティグループ (インバウンドトラフィック)

| タイプ             | プロトコル | ポート範囲                                                           | ソース                                                                           |
|-----------------|-------|-----------------------------------------------------------------|-------------------------------------------------------------------------------|
| すべてのトラフィック      | すべて   | すべて                                                             | SentinelDefaultSecurityGroupPrivateOnly (同じセキュリティグループのメンバーへのアウトバウンドトラフィックを制限) |
| すべてのトラフィック      | すべて   | すべて                                                             | SentinelDefaultSecurityGroupPrivateOnlyEgressAll (アウトバウンドトラフィックを制限しません)       |
| HTTP、HTTPS、SSH、 | TCP   | 80 / 443 (ソース 0.0.0.0/0)<br><br>踏み台からの SSH および RDP アクセスが許可されている | SentinelDefaultSecurityGroupPublic (アウトバウンドトラフィックを制限しません)                     |
| MALZ 踏み台:       |       |                                                                 |                                                                               |
| SSH             | TCP   | 22                                                              | SharedServices VPC CIDR と DMZ VPC CIDR、およびお客様が用意したオンプレミス CIDRs                |
| SSH             | TCP   | 22                                                              |                                                                               |
| RDP             | TCP   | 3389                                                            |                                                                               |
| RDP             | TCP   | 3389                                                            |                                                                               |
| SALZ 踏み台:       |       |                                                                 |                                                                               |
| SSH             | TCP   | 22                                                              | mc-initial-garden-LinuxBastionSG                                              |
| SSH             | TCP   | 22                                                              | mc-initial-garden-LinuxBastionDMZSG                                           |
| RDP             | TCP   | 3389                                                            | mc-initial-garden-WindowsBastionSG                                            |

| タイプ | プロトコル | ポート範囲 | ソース                                   |
|-----|-------|-------|---------------------------------------|
| RDP | TCP   | 3389  | mc-initial-garden-WindowsBastionDMZSG |

## セキュリティグループの作成、変更、または削除

カスタムセキュリティグループをリクエストできます。デフォルトのセキュリティグループがアプリケーションまたは組織のニーズを満たさない場合は、新しいセキュリティグループを変更または作成できます。このようなリクエストは承認が必要と見なされ、AMS オペレーションチームによってレビューされます。

スタックと VPCs の外部でセキュリティグループを作成するには、Deployment | Advanced stack components | Security group | Create (managed automation) 変更タイプ (ct-10xx2g2d7hc90) を使用して RFC を送信します。

Active Directory (AD) セキュリティグループの変更には、次の変更タイプを使用します。

- ユーザーを追加するには: Management | Directory Service | ユーザーとグループ | ユーザーをグループに追加する [ct-24pi85mjtza8k] を使用して RFC を送信する
- ユーザーを削除するには: Management | Directory Service | Users and groups | Remove user from group [ct-2019s9y3nfm14] を使用して RFC を送信します。

### Note

手動 CTs を使用する場合、AMS では ASAP スケジューリングオプション (コンソールで ASAP を選択し、API/CLI で開始時刻と終了時刻を空白のままにする) を使用することをお勧めします。これらの CTs では、AMS オペレータが RFC を調べ、承認して実行する前にお客様と通信する必要があるためです。これらの RFCs スケジュールする場合は、少なくとも 24 時間かかります。スケジュールされた開始時刻より前に承認が行われない場合、RFC は自動的に拒否されます。

## セキュリティグループの検索

スタックまたはインスタンスにアタッチされているセキュリティグループを見つけるには、EC2 コンソールを使用します。スタックまたはインスタンスを見つけたら、そのスタックまたはインスタンスにアタッチされているすべてのセキュリティグループを確認できます。

コマンドラインでセキュリティグループを検索し、出力をフィルタリングする方法については、「」を参照してください[describe-security-groups](#)。

## AMS 予防的コントロールと検出的コントロールライブラリ

AWS Managed Services (AMS) は、実証済みのサービスコントロールポリシー (SCPs) と ConfigRules の厳選されたライブラリ/カタログを提供します。これらは、セキュリティ体制を改善し、AMS アカウントのコンプライアンスギャップを軽減するために活用できます。

### トピック

- [厳選された SCPs と Config ルール](#)
- [Config ルールのカスタム通知](#)

### 厳選された SCPs と Config ルール

AMS Advanced の厳選された SCPs と Config ルール。

- サービスコントロールポリシー (SCPs): 提供される SCPsは、デフォルトの AMS ポリシーに追加されます。

これらのライブラリコントロールをデフォルトのコントロールと組み合わせて使用して、特定のセキュリティ要件を満たすことができます。

- Config ルール: ベースラインメジャーとして、AMS では、デフォルトの AMS 設定ルール (デフォルトのルールについては AMS アーティファクトを参照) に加えて、コンフォーマンスパック (AWS Config ガイドの「[コンフォーマンスパック](#)」を参照) を適用することをお勧めします。コンフォーマンスパックはコンプライアンス要件の大部分をカバーし、AWS は定期的に更新します。

ここに記載されているルールは、コンフォーマンスパックでカバーされていないユースケース固有のギャップをカバーするために使用できます。

#### Note

AMS のデフォルトのルールとコンフォーマンスパックが時間の経過とともに更新されると、これらのルールが重複することがあります。

AMS では、一般的に重複する Config ルールを定期的にクリーンアップすることをお勧めします。



AMS Advanced の場合、out-of-band変更を避けるため、Config ルールは自動修正 ([「AWS Config ルールによる非準拠 AWS リソースの修正」を参照](#)) を使用しないでください。

### SCP-AMS-001: EBS の作成を制限する

暗号化が有効になっていない場合は、EBS ボリュームの作成を防止します。

```
{
  "Condition": {
    "Bool": {
      "ec2:Encrypted": "false"
    }
  },
  "Action": "ec2:CreateVolume",
  "Resource": "*",
  "Effect": "Deny"
}
```

### SCP-AMS-002: EC2 起動を制限する

EBS ボリュームが暗号化されていない場合、EC2 インスタンスの起動を防止します。これには、暗号化されていない AMLs からの EC2 起動の拒否も含まれます。この SCP はルートボリュームにも適用されるためです。

```
{
  "Condition": {
    "Bool": {
      "ec2:Encrypted": "false"
    }
  },
  "Action": "ec2:RunInstances",
  "Resource": "arn:aws:ec2:*:*:volume/*",
  "Effect": "Deny"
}
```

### SCP-ADV-001: RFC 送信を制限する

デフォルトの AMS ロールが、VPC の作成や VPC の削除など、特定の自動 RFCs を送信しないように制限します。これは、フェデレーティッドロールにより詳細なアクセス許可を適用する場合に便利です。

例えば、VPC の作成と削除、追加のサブネットの作成、アプリケーションアカウントのオフボーディング、SAML ID プロバイダーの更新または削除を許可するものを除き、使用可能な RFCs のほとんどをデフォルトで送信AWSManagedServicesChangeManagement Roleできます。

### SCP-AMS-003: AMS での EC2 または RDS の作成を制限する

特定のタグを持たない Amazon EC2 および RDS インスタンスの作成を防止し、AMS デフォルトAMS Backup IAMロールに許可します。これはディザスタリカバリまたは DR が必要です。

```
{
  "Sid": "DenyRunInstanceWithNoOrganizationTag",
  "Effect": "Deny",
  "Action": [
    "ec2:RunInstances",
    "rds:CreateDBInstance"
  ],
  "Resource": [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:rds:*:*:db:*"
  ],
  "Condition": {
    "Null": {
      "aws:RequestTag/organization": "true"
    },
    "StringNotLike": {
      "aws:PrincipalArn": [
        "arn:aws:iam::<Account_Number>:role/ams-backup-iam-role"
      ]
    }
  }
}
```

### SCP-AMS-004: S3 アップロードを制限する

暗号化されていない S3 オブジェクトのアップロードを防止します。

```
{
  "Sid": "DenyUnencryptedS3Uploads",
  "Effect": "Deny",
  "Action": "s3:PutObject",
  "Resource": "*",
  "Condition": {
```

```
        "StringNotLike": {
            "s3:x-amz-server-side-encryption": ["aws:kms", "AES256"]
        },
        "Null": {
            "s3:x-amz-server-side-encryption": "false"
        }
    }
}
]
```

#### SCP-AMS-005: API とコンソールへのアクセスを制限する

顧客の InfoSec が判断した既知の不正な IP アドレスからのリクエストに対する AWS コンソールと API アクセスを防止します。

#### SCP-AMS-006: IAM エンティティが組織からメンバーアカウントを削除できないようにする

AWS Identity and Access Management エンティティが組織からメンバーアカウントを削除しないようにします。

```
{
  "Effect": "Deny",
  "Action": ["organizations:LeaveOrganization"],
  "Resource": ["*"]
}
```

#### SCP-AMS-007: 組織外のアカウントへのリソースの共有を禁止する

##### AWS 組織外の外部アカウントとのリソースの共有を禁止する

```
{
  "Effect": "Deny",
  "Action": [
    "ram:*"
  ],
  "Resource": [
    "*"
  ],
  "Condition": {
    "Bool": {
```

```

        "ram:AllowsExternalPrincipals": "true"
    }
}
},
{
    "Effect": "Deny",
    "Action": [
        "ram:CreateResourceShare",
        "ram:UpdateResourceShare"
    ],
    "Resource": "*",
    "Condition": {
        "Bool": {
            "ram:RequestedAllowsExternalPrincipals": "true"
        }
    }
}
}

```

#### SCP-AMS-008: 組織または組織単位 (OUsとの共有を禁止する

組織内のアカウントや OU とリソースを共有しないようにします。

```

{
    "Effect": "Deny",
    "Action": [
        "ram:CreateResourceShare",
        "ram:AssociateResourceShare"
    ],
    "Resource": "*",
    "Condition": {
        "ForAnyValue:StringLike": {
            "ram:Principal": [
                "arn:aws:organizations::*:account/o-${OrganizationId}/${AccountId}",
                "arn:aws:organizations::*:ou/o-${OrganizationId}/ou-${OrganizationalUnitId}"
            ]
        }
    }
}
}

```

#### SCP-AMS-009: ユーザーがリソース共有の招待を受け入れないようにする

メンバーアカウントが からの招待を受け入れ AWS RAM でリソース共有に参加できないようにします。この API は条件をサポートしておらず、外部アカウントからの共有のみを防ぎます。

```
{
  "Effect": "Deny",
  "Action": ["ram:AcceptResourceShareInvitation"],
  "Resource": ["*"]
}
```

#### SCP-AMS-010: アカウントリージョンのアクションの有効化と無効化を禁止する

AWS アカウントの新しい AWS リージョンを有効または無効にしないようにします。

```
{
  "Effect": "Deny",
  "Action": [
    "account:EnableRegion",
    "account:DisableRegion"
  ],
  "Resource": "*"
}
```

#### SCP-AMS-011: 請求変更アクションの防止

請求および支払い設定の変更を防止します。

```
{
  "Effect": "Deny",
  "Action": [
    "aws-portal:ModifyBilling",
    "aws-portal:ModifyAccount",
    "aws-portal:ModifyPaymentMethods"
  ],
  "Resource": "*"
}
```

#### SCP-AMS-012: 特定の CloudTrails の削除または変更を防止する

特定の AWS CloudTrail 証跡への変更を防止します。

```
{
  "Effect": "Deny",
  "Action": [
    "cloudtrail:DeleteEventDataStore",
    "cloudtrail:DeleteTrail",

```

```
"cloudtrail:PutEventSelectors",
"cloudtrail:PutInsightSelectors",
"cloudtrail:UpdateEventDataStore",
"cloudtrail:UpdateTrail",
"cloudtrail:StopLogging"
],
"Resource": [
  "arn:${Partition}:cloudtrail:${Region}:${Account}:trail/${TrailName}"
]
}
```

### SCP-AMS-013: デフォルトの EBS 暗号化の無効化を禁止する

デフォルトの Amazon EBS 暗号化の無効化を防止します。

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:DisableEbsEncryptionByDefault"
  ],
  "Resource": "*"
}
```

### SCP-AMS-014: デフォルトの VPC とサブネットの作成を禁止する

デフォルトの Amazon VPC とサブネットの作成を防止します。

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:CreateDefaultSubnet",
    "ec2:CreateDefaultVpc"
  ],
  "Resource": "*"
}
```

### SCP-AMS-015: GuardDuty の無効化と変更を禁止する

Amazon GuardDuty が変更または無効化されないようにします。

```
{
  "Effect": "Deny",
  "Action": [
```

```

    "guardduty:AcceptInvitation",
    "guardduty:ArchiveFindings",
    "guardduty:CreateDetector",
    "guardduty:CreateFilter",
    "guardduty:CreateIPSet",
    "guardduty:CreateMembers",
    "guardduty:CreatePublishingDestination",
    "guardduty:CreateSampleFindings",
    "guardduty:CreateThreatIntelSet",
    "guardduty:DeclineInvitations",
    "guardduty>DeleteDetector",
    "guardduty>DeleteFilter",
    "guardduty>DeleteInvitations",
    "guardduty>DeleteIPSet",
    "guardduty>DeleteMembers",
    "guardduty>DeletePublishingDestination",
    "guardduty>DeleteThreatIntelSet",
    "guardduty:DisableOrganizationAdminAccount",
    "guardduty:DisassociateFromMasterAccount",
    "guardduty:DisassociateMembers",
    "guardduty:InviteMembers",
    "guardduty:StartMonitoringMembers",
    "guardduty:StopMonitoringMembers",
    "guardduty:TagResource",
    "guardduty:UnarchiveFindings",
    "guardduty:UntagResource",
    "guardduty:UpdateDetector",
    "guardduty:UpdateFilter",
    "guardduty:UpdateFindingsFeedback",
    "guardduty:UpdateIPSet",
    "guardduty:UpdateMalwareScanSettings",
    "guardduty:UpdateMemberDetectors",
    "guardduty:UpdateOrganizationConfiguration",
    "guardduty:UpdatePublishingDestination",
    "guardduty:UpdateThreatIntelSet"
  ],
  "Resource": "*"
}
```

## SCP-AMS-016: ルートユーザーアクティビティの防止

ルートユーザーがアクションを実行できないようにします。

```
{
```



```
"Action": "*",
"Resource": "*",
"Effect": "Deny",
"Condition": {
  "StringLike": {
    "aws:PrincipalArn": [
      "arn:aws:iam::*:root"
    ]
  }
}
```

### SCP-AMS-017: ルートユーザーのアクセスキーの作成を禁止する

ルートユーザーのアクセスキーの作成を防止します。

```
{
  "Effect": "Deny",
  "Action": "iam:CreateAccessKey",
  "Resource": "arn:aws:iam::*:root"
}
```

### SCP-AMS-018: S3 アカウントのパブリックアクセスブロックの無効化を禁止する

Amazon S3 アカウントのパブリックアクセスブロックを無効にしないようにします。これにより、アカウントのバケットがパブリックになるのを防ぐことができます。

```
{
  "Effect": "Deny",
  "Action": "s3:PutAccountPublicAccessBlock",
  "Resource": "*"
}
```

### SCP-AMS-019: AWS Config の無効化または Config ルールの変更を禁止する

AWS Config ルールの無効化または変更を防止します。

```
{
  "Effect": "Deny",
  "Action": [
    "config:DeleteConfigRule",
    "config:DeleteConfigurationRecorder",

```

```
"config:DeleteDeliveryChannel",
"config:DeleteEvaluationResults",
"config:StopConfigurationRecorder"
],
"Resource": "*"
}
```

## SCP-AMS-020: すべての IAM アクションを禁止する

すべての IAM アクションを防止します。

```
{
  "Effect": "Deny",
  "Action": [
    "iam:*"
  ],
  "Resource": "*"
}
```

## SCP-AMS-021: CloudWatch Logs グループとストリームの削除を禁止する

Amazon CloudWatch Logs グループとストリームの削除を防止します。

```
{
  "Effect": "Deny",
  "Action": [
    "logs:DeleteLogGroup",
    "logs:DeleteLogStream"
  ],
  "Resource": "*"
}
```

## SCP-AMS-022: Glacier 削除の防止

Amazon Glacier の削除を防止します。

```
{
  "Effect": "Deny",
  "Action": [
    "glacier:DeleteArchive",
    "glacier:DeleteVault"
  ],
  "Resource": "*"
}
```

```
}
```

## SCP-AMS-023: IAM Access Analyzer の削除を禁止する

IAM Access Analyzer の削除を防止します。

```
{
  "Action": [
    "access-analyzer:DeleteAnalyzer"
  ],
  "Resource": "*",
  "Effect": "Deny"
}
```

## SCP-AMS-024: Security Hub CSPM への変更の防止

削除を防止します AWS Security Hub CSPM。

```
{
  "Action": [
    "securityhub:DeleteInvitations",
    "securityhub:DisableSecurityHub",
    "securityhub:DisassociateFromMasterAccount",
    "securityhub:DeleteMembers",
    "securityhub:DisassociateMembers"
  ],
  "Resource": "*",
  "Effect": "Deny"
}
```

## SCP-AMS-025: Directory Service での削除の防止

のリソースの削除を防止します Directory Service。

```
{
  "Action": [
    "ds:DeleteDirectory",
    "ds:DeleteLogSubscription",
    "ds:DeleteSnapshot",
    "ds:DeleteTrust",
    "ds:DeregisterCertificate",
    "ds:DeregisterEventTopic",
    "ds:DisableLDAPS",

```

```
"ds:DisableRadius",
"ds:DisableSso",
"ds:UnshareDirectory"
],
"Resource": "*",
"Effect": "Deny"
}
```

## SCP-AMS-026: 拒否リストに登録されたサービスの使用を禁止する

拒否リストに登録されたサービスの使用を防止します。

### Note

*service1* と *service2* をサービス名に置き換えます。*access-analyzer* または *IAM* の例。

```
{
  "Effect": "Deny",
  "Resource": "*",
  "Action": ["service1:", "service2:"]
}
```

## SCP-AMS-027: 特定のリージョンでの拒否リストに登録されたサービスの使用を禁止する

特定の AWS リージョンで拒否リストに登録されているサービスの使用を防止します。

### Note

*service1* と *service2* をサービス名に置き換えます。*access-analyzer* または *IAM* の例。

*region1* と *region2* をサービス名に置き換えます。*us-west-2* または *us-east-1* の例。

```
{
  "Effect": "Deny",
  "Resource": "*",
  "Action": ["service1:", "service2:"],
  "Condition": {
```

```
"StringEquals": {
  "aws:RequestedRegion": [
    "region1",
    "region2"
  ]
}
```

## SCP-AMS-028: 承認されたプリンシパル以外によるタグの変更を防止する

承認されたプリンシパル以外のユーザーによるタグの変更を防止します。認可タグを使用してプリンシパルを認可します。認可タグは、リソースとプリンシパルに関連付ける必要があります。ユーザー/ロールは、リソースとプリンシパルの両方のタグが一致する場合にのみ、承認されたと見なされます。詳細については、以下のリソースを参照してください。

- [のサービスコントロールポリシーを使用した認可に使用されるリソースタグの保護 AWS Organizations](#)
- [承認されたプリンシパル以外によるタグの変更を防ぐ](#)

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:CreateTags",
    "ec2:DeleteTags"
  ],
  "Resource": [
    "*"
  ],
  "Condition": {
    "StringNotEquals": {
      "ec2:ResourceTag/access-project": "${aws:PrincipalTag/access-project}",
      "aws:PrincipalArn": "arn:aws:iam::${ACCOUNT_ID}:${RESOURCE_TYPE}/${RESOURCE_NAME}"
    },
    "Null": {
      "ec2:ResourceTag/access-project": false
    }
  }
},
{
  "Effect": "Deny",
```

```

"Action": [
  "ec2:CreateTags",
  "ec2>DeleteTags"
],
"Resource": [
  "*"
],
"Condition": {
  "StringNotEquals": {
    "aws:RequestTag/access-project": "${aws:PrincipalTag/access-project}",
    "aws:PrincipalArn": "arn:aws:iam::${ACCOUNT_ID}:${RESOURCE_TYPE}/${RESOURCE_NAME}"
  },
  "ForAnyValue:StringEquals": {
    "aws:TagKeys": [
      "access-project"
    ]
  }
}
},
{
  "Effect": "Deny",
  "Action": [
    "ec2:CreateTags",
    "ec2>DeleteTags"
  ],
  "Resource": [
    "*"
  ],
  "Condition": {
    "StringNotEquals": {
      "aws:PrincipalArn": "arn:aws:iam::${ACCOUNT_ID}:${RESOURCE_TYPE}/${RESOURCE_NAME}"
    },
    "Null": {
      "aws:PrincipalTag/access-project": true
    }
  }
}
}

```

SCP-AMS-029: ユーザーが Amazon VPC フローログを削除できないようにする

Amazon VPC フローログの削除を防止します。

```

{
  "Action": [

```

```
"ec2:DeleteFlowLogs",
"logs:DeleteLogGroup",
"logs:DeleteLogStream",
"s3:DeleteBucket",
"s3:DeleteObject",
"s3:DeleteObjectVersion",
"s3:PutLifecycleConfiguration",
"firehose:DeleteDeliveryStream"
],
"Resource": "*",
"Effect": "Deny"
}
```

SCP-AMS-030: ネットワークアカウント以外のアカウントとの VPC サブネットの共有を禁止する  
Amazon VPC サブネットをネットワークアカウント以外のアカウントと共有しないようにします。

 Note

***NETWORK\_ACCOUNT\_ID*** をネットワークアカウント ID に置き換えます。

```
{
  "Effect": "Deny",
  "Action": [
    "ram:AssociateResourceShare",
    "ram:CreateResourceShare"
  ],
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "ram:Principal": "NETWORK_ACCOUNT_ID"
    },
    "StringEquals": {
      "ram:RequestedResourceType": "ec2:Subnet"
    }
  }
}
```

SCP-AMS-031: 禁止されているインスタンスタイプのインスタンスの起動を禁止する  
禁止された Amazon EC2 インスタンスタイプの遅延を防止します。



**Note**

*instance\_type1* と *instance\_type2* を、*t2.micro* や *\*.nano* #####  
#####。

```
{
  "Effect": "Deny",
  "Action": "ec2:RunInstances",
  "Resource": [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition": {
    "ForAnyValue:StringLike": {
      "ec2:InstanceType": [
        "instance_type1",
        "instance_type2"
      ]
    }
  }
}
```

## SCP-AMS-032: IMDSv2 を使用しないインスタンスの起動を禁止する

IMDSv2 を使用しない Amazon EC2 インスタンスを防止します。IMDSv2

```
[
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "StringNotEquals": {
        "ec2:MetadataHttpTokens": "required"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
```

```

    "NumericGreaterThan": {
      "ec2:MetadataHttpPutResponseHopLimit": "3"
    }
  },
  {
    "Effect": "Deny",
    "Action": "*",
    "Resource": "*",
    "Condition": {
      "NumericLessThan": {
        "ec2:RoleDelivery": "2.0"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:ModifyInstanceMetadataOptions",
    "Resource": "*"
  }
]

```

### SCP-AMS-033: 特定の IAM ロールへの変更を禁止する

指定された IAM ロールへの変更を防止します。

```

{
  "Action": [
    "iam:AttachRolePolicy",
    "iam>DeleteRole",
    "iam>DeleteRolePermissionsBoundary",
    "iam>DeleteRolePolicy",
    "iam:DetachRolePolicy",
    "iam:PutRolePermissionsBoundary",
    "iam:PutRolePolicy",
    "iam:TagRole",
    "iam:UntagRole",
    "iam:UpdateAssumeRolePolicy",
    "iam:UpdateRole",
    "iam:UpdateRoleDescription"
  ],
  "Resource": [
    "arn:aws:iam::{ACCOUNT_ID}:role/{RESOURCE_NAME}"
  ],
}

```

```
"Effect": "Deny"
}
```

### SCP-AMS-034: 特定の IAM ロールで AssumeRolePolicy の変更を禁止する

指定された IAM ロールの AssumeRolePolicy への変更を防止します。

```
{
  "Action": [
    "iam:UpdateAssumeRolePolicy"
  ],
  "Resource": [
    "arn:aws:iam::{ACCOUNT_ID}:role/{RESOURCE_NAME}"
  ],
  "Effect": "Deny"
}
```

### ConfigRule: 必須タグ

EC2 インスタンスに必要なカスタムタグがあるかどうかを確認します。InfoSec に加えて、これはコスト管理にも役立ちます。

```
ConfigRuleName: required-tags
Description: >-
  A Config rule that checks whether EC2 instances have the required tags.
Scope:
  ComplianceResourceTypes:
    - 'AWS::EC2::Instance'
InputParameters:
  tag1Key: COST_CENTER
  tag2Key: APP_ID
Source:
  Owner: AWS
  SourceIdentifier: REQUIRED_TAGS
```

### ConfigRule: アクセスキーがローテーションされました

アクセスキーが指定された期間内にローテーションされていることを確認します。これは通常、一般的なコンプライアンス要件に従って 90 日に設定されます。

```
ConfigRuleName: access-keys-rotated
```

Description: >-

A config rule that checks whether the active access keys are rotated within the number of days specified in maxAccessKeyAge. The rule is NON\_COMPLIANT if the access keys have not been rotated for more than maxAccessKeyAge number of days.

InputParameters:

maxAccessKeyAge: '90'

Source:

Owner: AWS

SourceIdentifier: ACCESS\_KEYS\_ROTATED

MaximumExecutionFrequency: TwentyFour\_Hours

## ConfigRule: AMS の IAM ルートアクセスキー

ルートアクセスキーがアカウントに存在していないことを確認します。AMS Advanced アカウントの場合、これはout-of-the-box準拠することが期待されます。

ConfigRuleName: iam-root-access-key-check

Description: >-

A config rule that checks whether the root user access key is available. The rule is COMPLIANT if the user access key does not exist.

Source:

Owner: AWS

SourceIdentifier: IAM\_ROOT\_ACCESS\_KEY\_CHECK

MaximumExecutionFrequency: TwentyFour\_Hours

## ConfigRule: SSM マネージド EC2

EC2sが SSM Systems Manager によって管理されていることを確認します。

ConfigRuleName: ec2-instance-managed-by-systems-manager

Description: >-

A Config rule that checks whether the EC2 instances in the account are managed by AWS Systems Manager.

Scope:

ComplianceResourceTypes:

- 'AWS::EC2::Instance'
- 'AWS::SSM::ManagedInstanceInventory'

Source:

Owner: AWS

SourceIdentifier: EC2\_INSTANCE\_MANAGED\_BY\_SSM

## ConfigRule: AMS で未使用の IAM ユーザー

指定された期間使用されていない IAM ユーザー認証情報を確認します。キーローテーションチェックと同様に、これは通常、一般的なコンプライアンス要件に従ってデフォルトで 90 日に設定されます。

```
ConfigRuleName: iam-user-unused-credentials-check
Description: >-
  A config rule that checks whether IAM users have passwords
  or active access keys that have not been used within the
  specified number of days provided.
InputParameters:
  maxCredentialUsageAge: '90'
Source:
  Owner: AWS
SourceIdentifier: IAM_USER_UNUSED_CREDENTIALS_CHECK
MaximumExecutionFrequency: TwentyFour_Hours
```

## ConfigRule: S3 バケットのログ記録

アカウントの S3 バケットでログ記録が有効になっていることを確認します。

```
ConfigRuleName: s3-bucket-logging-enabled
Description: >-
  A Config rule that checks whether logging is enabled for S3 buckets.
Scope:
  ComplianceResourceTypes:
    - 'AWS::S3::Bucket'
Source:
  Owner: AWS
SourceIdentifier: S3_BUCKET_LOGGING_ENABLED
```

## ConfigRule: S3 バケットのバージョニング

すべての S3 バケットでバージョニングと MFA 削除 (オプション) が有効になっていることを確認します。

```
ConfigRuleName: s3-bucket-versioning-enabled
Description: >-
  A Config rule that checks whether versioning is enabled for S3
  buckets. Optionally, the rule checks if MFA delete is enabled for S3 buckets.
Scope:
```

```
ComplianceResourceTypes:
  - 'AWS::S3::Bucket'
Source:
  Owner: AWS
SourceIdentifier: S3_BUCKET_VERSIONING_ENABLED
```

## ConfigRule: S3 パブリックアクセス

パブリックアクセス設定 (パブリック ACL、パブリックポリシー、パブリックバケット) がアカウント全体で制限されていることを確認します。

```
ConfigRuleName: s3-account-level-public-access-blocks
Description: >-
  A Config rule that checks whether the required public access block
  settings are configured from account level. The rule is only
  NON_COMPLIANT when the fields set below do not match the corresponding
  fields in the configuration item.
Scope:
  ComplianceResourceTypes:
    - 'AWS::S3::AccountPublicAccessBlock'
InputParameters:
  IgnorePublicAcls: 'True'
  BlockPublicPolicy: 'True'
  BlockPublicAcls: 'True'
  RestrictPublicBuckets: 'True'
Source:
  Owner: AWS
SourceIdentifier: S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS
```

## ConfigRule: アーカイブされていない GuardDuty の検出結果

アーカイブされていない GuardDuty の検出結果が、指定された期間より古いかどうかを確認します。デフォルトの期間は、低レベルの場合は 30 日間、中レベルの場合は 7 日間、高レベル検出の場合は 1 日間です。

```
ConfigRuleName: guardduty-non-archived-findings
Description: >-
  A Config rule that checks whether the Amazon GuardDuty has findings that
  are non archived. The rule is NON_COMPLIANT if GuardDuty has non
  archived low/medium/high severity findings older than the specified number.
InputParameters:
  daysLowSev: '30'
  daysMediumSev: '7'
```

```
daysHighSev: '1'
Source:
  Owner: AWS
  SourceIdentifier: GUARDDUTY_NON_ARCHIVED_FINDINGS
MaximumExecutionFrequency: TwentyFour_Hours
```

### ConfigRule: CMK 削除

削除がスケジュールされている (または保留中) AWS Key Management Service カスタムマスターキー (CMKs) がないか確認します。CMK 削除に関する認識がないと、データが回復不能になる可能性があるため、これは重要です。

```
ConfigRuleName: kms-cmk-not-scheduled-for-deletion
Description: >-
  A config rule that checks whether customer master keys (CMKs) are not
  scheduled for deletion in AWS Key Management Service (AWS KMS). The rule is
  NON_COMPLIANT if CMKs are scheduled for deletion.
Source:
  Owner: AWS
SourceIdentifier: KMS_CMK_NOT_SCHEDULED_FOR_DELETION
MaximumExecutionFrequency: TwentyFour_Hours
```

### ConfigRule: CMK ローターション

アカウント内のすべての CMK で自動ローテーションが有効になっていることを確認する

```
ConfigRuleName: cmk-backing-key-rotation-enabled
Description: >-
  A config rule that checks that key rotation is enabled for each customer
  master key (CMK). The rule is COMPLIANT, if the key rotation is enabled
  for specific key object. The rule is not applicable to CMKs that have
  imported key material.
Source:
  Owner: AWS
SourceIdentifier: CMK_BACKING_KEY_ROTATION_ENABLED
MaximumExecutionFrequency: TwentyFour_Hours
```

### Config ルールのカスタム通知

重大な非準拠の Config ルールが発生し、InfoSec チームとリーダーシップチームに直接エスカレーションされた認識を高める必要がある場合があります。このようなシナリオでは、AMS はコンプライアンス違反のイベント駆動型カスタム通知を設定することをお勧めします。



例 :

```
ConfigRuleName: required-tags
  Description: >-
    A Config rule that checks whether EC2 instances have the mandated tags.
  Scope:
    ComplianceResourceTypes:
      - 'AWS::EC2::Instance'
  InputParameters:
    tag1Key: COST_CENTER
    tag2Key: APP_ID
  Source:
    Owner: AWS
SourceIdentifier: REQUIRED_TAGS
NotificationEventRule:
  Type: 'AWS::Events::Rule'
  Properties:
    Name: CWEventForrequired-tags
    Description: >-
      SNS Notification for Non-Compliant Events of Config Rule:
      required-tags
    State: ENABLED
    EventPattern:
      detail-type:
        - Config Rules Compliance Change
      source:
        - aws.config
      detail:
        newEvaluationResult:
          complianceType:
            - NON_COMPLIANT
        configRuleARN:
          - 'Fn::GetAtt':
              - RequiredEC2Tags
              - Arn
    Targets:
      - Id: RemediationNotification
        Arn:
          Ref: SnsTopic
        InputTransformer:
          InputTemplate: >-
            "EC2 Instance <Instance_ID> is non-compliant. Please add required tags:
            COST_CENTER, APP_ID, Name, and Backup."
          InputPathsMap:
```

```
        instance_id: $.detail.resourceId
SnsTopic:
  Type: 'AWS::SNS::Topic'
  Properties:
    Subscription:
      - Endpoint: Cloud_Ops_Leaders@customer.com
        Protocol: email
    TopicName: noncompliant-instance-notification
SnsTopicPolicy:
  Type: 'AWS::SNS::TopicPolicy'
  Properties:
    PolicyDocument:
      Statement:
        - Sid: __default_statement_ID
          Effect: Allow
          Principal:
            AWS: '*'
          Action:
            - 'SNS:GetTopicAttributes'
            - 'SNS:SetTopicAttributes'
            - 'SNS:AddPermission'
            - 'SNS:RemovePermission'
            - 'SNS>DeleteTopic'
            - 'SNS:Subscribe'
            - 'SNS:ListSubscriptionsByTopic'
            - 'SNS:Publish'
            - 'SNS:Receive'
          Resource:
            Ref: SnsTopic
          Condition:
            StringEquals:
              'AWS:SourceOwner':
                Ref: 'AWS::AccountId'
        - Sid: TrustCWEToPublishEventsToMyTopic
          Effect: Allow
          Principal:
            Service: events.amazonaws.com
          Action: 'sns:Publish'
          Resource:
            Ref: SnsTopic
  Topics:
    - Ref: SnsTopic
```

## AMS Advanced の Amazon EventBridge ルールサービスにリンクされたロール

AMS Advanced は、`AWSServiceRoleForManagedServices_Events` という名前のサービスリンクロール (SLR) を使用します。このロールは AWS、マネージドサービスサービスプリンシパル (`events.managedservices.amazonaws.com`) の 1 つを信頼してロールを引き受けます。サービスは、ロールを使用して EventBridge マネージドルールを作成します。このルールは、AWS アカウントから AWS マネージドサービスにアラーム状態変更情報を配信するために必要なインフラストラクチャです。

### EventBridge SLR for AMS Advanced のアクセス許可

`AWSServiceRoleForManagedServices_Events` サービスにリンクされたロールは、次のサービスを信頼してロールを引き受けます。

- `events.managedservices.amazonaws.com`

このロールには、`AWSManagedServices_EventsServiceRolePolicy` AWS 管理ポリシーがアタッチされています (「[AWS 管理ポリシー: `AWSManagedServices\_EventsServiceRolePolicy`](#)」を参照)。サービスはロールを使用して、アカウントから マネージドサービスに AWS アラーム状態変更情報を配信します。サービスリンク役割の作成、編集、削除を IAM エンティティ (ユーザー、グループ、役割など) に許可するにはアクセス許可を設定する必要があります。詳細については、AWS Identity and Access Management [ユーザーガイドの「サービスにリンクされたロールのアクセス許可」](#)を参照してください。

JSON `AWSManagedServices_EventsServiceRolePolicy` は、次の ZIP: [EventsServiceRolePolicy.zip](#) でダウンロードできます。

### AMS Advanced 用の EventBridge SLR の作成

サービスリンクロールを手動で作成する必要はありません。AWS マネジメントコンソール、AWS CLI または AWS API で AMS にオンボードすると、AMS Advanced によってサービスにリンクされたロールが作成されます。

#### Important

このサービスにリンクされたロールは、2023 年 2 月 7 日より前に AMS Advanced サービスを使用していた場合、サービスにリンクされたロールのサポートが開始されると、AMS Accelerate によってアカウントに `AWSServiceRoleForManagedServices_Events` ロールが作

成されました。詳細については、「[IAM アカウントに新しいロールが表示される](#)」を参照してください。

このサービスリンクロールを削除した後で再度作成する必要がある場合は、同じ手順でアカウントにロールを再作成できます。AMS にオンボードすると、AMS Advanced によってサービスにリンクされたロールが再度作成されます。

## AMS Advanced の EventBridge SLR の編集

AMS Advanced では、AWSServiceRoleForManagedServices\_Events サービスにリンクされたロールを編集することはできません。サービスリンクロールの作成後は、さまざまなエンティティがロールを参照する可能性があるため、ロール名を変更することはできません。ただし、IAM を使用してロールの説明を編集することはできます。詳細については、「IAM ユーザーガイド」の「[サービスリンクロールの編集](#)」を参照してください。

## AMS Advanced の EventBridge SLR の削除

AWSServiceRoleForManagedServices\_Events ロールを手動で削除する必要はありません。AWS マネジメントコンソール、AWS CLI または AWS API で AMS からオフボードすると、AMS Advanced はリソースをクリーンアップし、サービスにリンクされたロールを削除します。

IAM コンソール、AWS CLI または AWS API を使用して、サービスにリンクされたロールを手動で削除することもできます。そのためにはまず、サービスリンクロールのリソースをクリーンアップする必要があります。その後で、手動で削除できます。

### Note

リソースを削除しようとしたときに AMS Advanced サービスがロールを使用している場合、削除が失敗する可能性があります。失敗した場合は数分待ってから操作を再試行してください。

AWSServiceRoleForManagedServices\_Events サービスにリンクされたロールで使用する AMS Advanced リソースを削除するには

サービスリンクロールを IAM で手動削除するには

IAM コンソール、AWS CLI、または AWS API を使用して、AWSServiceRoleForManagedServices\_Events サービスにリンクされたロールを削除します。

詳細については、「IAM ユーザーガイド」の「[サービスにリンクされたロールの削除](#)」を参照してください。

## セキュリティのベストプラクティス

このセクションは、機密性の高い AMS セキュリティ関連情報が含まれているため、編集されています。この情報は、AMS コンソールのドキュメントから入手できます。AWS Artifact にアクセスするには、CSDM に連絡して手順を確認するか、[「AWS Artifact の開始方法」](#)を参照してください。

## AMS マルチアカウントランディングゾーン EPS のデフォルト以外の設定

このセクションは、機密性の高い AMS セキュリティ関連情報が含まれているため、編集されています。この情報は、AMS コンソールのドキュメントから入手できます。AWS Artifact にアクセスするには、CSDM に連絡して手順を確認するか、[「AWS Artifact の開始方法」](#)を参照してください。

## AMS ガードレール

ガードレールは、AMS 環境全体に継続的なガバナンスを提供する高レベルのルールです。

このセクションは、機密性の高い AMS セキュリティ関連情報が含まれているため、編集されています。この情報は、AMS コンソールのドキュメントから入手できます。AWS Artifact にアクセスするには、CSDM に連絡して手順を確認するか、[「AWS Artifact の開始方法」](#)を参照してください。

## MALZ サービスコントロールポリシー

このセクションは、機密性の高い AMS セキュリティ関連情報が含まれているため、編集されています。この情報は、AMS コンソールのドキュメントから入手できます。AWS Artifact にアクセスするには、CSDM に連絡して手順を確認するか、[「AWS Artifact の開始方法」](#)を参照してください。

## AMS のセキュリティインシデント対応

セキュリティは AWS Managed Services (AMS) の最優先事項です。AMS は、リソースとコントロールをアカウントにデプロイして管理します。AWS には責任共有モデルがあります。はクラウドのセキュリティ AWS を管理し、お客様はクラウドのセキュリティを担当します。AMS はデータとアセットを保護し、セキュリティの問題に対するセキュリティコントロールとアクティブなモニタリングを使用して AWS インフラストラクチャの安全性を維持するのに役立ちます。これらの機能は、AWS クラウドで実行されているアプリケーションのセキュリティベースラインを確立するのに役立

ちます。AMS は、セキュリティインシデント対応を通じてお客様と協力して効果を評価し、ベストプラクティスの推奨事項に基づいて封じ込めと修復を実行します。

設定ミスや外部要因の変化など、ベースラインからの逸脱が発生した場合は、対応して調査する必要があります。これを成功させるには、AMS 環境内のセキュリティインシデント対応の基本概念を理解する必要があります。また、セキュリティ上の問題が発生する前にクラウドチームを準備、教育、トレーニングするための要件も理解する必要があります。使用できるコントロールと機能を把握し、ユーザーアカウントの侵害や特権アカウントの悪用などの一般的なセキュリティ問題の対応計画を立て、自動化を使用して対応速度と一貫性を向上させる修復方法を特定することが重要です。さらに、これらの要件を満たすためのセキュリティインシデント対応プログラムの構築に関連するコンプライアンス要件と規制要件を理解する必要があります。

セキュリティインシデント対応は複雑な場合がありますが、反復的なアプローチを実装することで、プロセスを簡素化し、インシデント対応チームが早期かつ継続的な検出と対応を提供することで、アセットステークホルダーの満足度を維持できます。このガイドでは、AMS がインシデント対応に使用する方法、AMS 責任マトリックス (RACI)、セキュリティイベントに備える方法、セキュリティインシデント中に AMS をエンゲージする方法、AMS が使用するインシデント対応ランブックの一部について説明します。

## AMS セキュリティインシデント対応の仕組み

AWS Managed Services は、NIST 800-61 [Computer Security Incident Handling Guide](#) for Security Incident Response に準拠しています。この業界標準に準拠することで、セキュリティイベント管理に一貫したアプローチを提供し、クラウド内のセキュリティインシデントの保護と対応に関するベストプラクティスに従います。

### インシデント対応のライフサイクル

検出がセキュリティアラートを特定して生成する場合、またはセキュリティ支援をリクエストする場合、AWS Managed Services オペレーションチームは、タイムリーな調査を行い、データ収集の実行、優先順位付けと分析のための自動化を実行し、分析の通知を行い、調査と封じ込めアクティビティを実行し、イベント分析を投稿します。

インシデント対応中に実行されるデータ収集、トリアージ、分析、および封じ込めのアクティビティは、調査対象のセキュリティイベントのタイプによって異なります。一部のシナリオのセキュリティインシデント対応ワークフローの例は、このドキュメントの最後にあります。

インシデント中、AMS は正しい一連のアクションを動的に判断します。これにより、文書化されたステップが必要に応じて順序変更またはバイパスされ、適切な結果が得られる可能性があります。

## 準備

脅威の状況が進化するにつれて、AMS は引き続き検出および対応機能を拡張します。新しい検出が追加されると、AMS はこれらの新しい検出からのアラートを検出および応答プラットフォームに組み込みます。AMS セキュリティレスポnderは、セキュリティインシデント対応のライフサイクルを通じて調査し、パートナーとなるようにトレーニングされます。

このパートナーシップアプローチにより、セキュリティチームとアプリケーションチームが AMS と連携して、これらのイベントが発生したときにセキュリティイベントを処理する準備を整えることが重要です。このドキュメントでは、セキュリティイベント中に予想されることについて説明し、セキュリティインシデントが発生したときの迅速な対応に備えるのに役立ちます。

このドキュメントでは、NIST 800-61 定義のイベントをシステムまたはネットワークでの観測可能な出現として使用し、インシデントをポリシー、許容可能な使用ポリシー、または標準セキュリティプラクティスの違反または差し迫った脅威として使用します。

### 準備チェックリスト

AMS クラウドソリューションデリバリーマネージャー (CSDM) および AMS クラウドアーキテクト (CA) と以下のチェックリストを確認してください。

- どのアカウントでどのワークロードが実行されているかを理解します。
- さまざまなワークロードを担当する内部チームを理解し、ワークロードで適切にタグ付けします。
- セキュリティイベントの調査中や封じ込めの決定時に必要となる可能性がある他のチームの連絡先の詳細を内部で維持します。
- セキュリティ連絡先が最新であり、すべてのマネージド AWS アカウントに追加されていることを確認します。問い合わせはアカウントごとに管理されます。
- AMS にセキュリティインシデントを発生させる方法を理解し、重大度と予想される応答時間を理解します。
- セキュリティ通知を受信すると、ページャーやセキュリティオペレーションセンターなどの適切なユーザーとシステムにルーティングされます。
- 使用可能なログソース、アカウントに保存されているログソース、およびログソースにアクセスできるユーザーについて説明します。
- CloudWatch Insights を使用して調査中にログをクエリする方法を理解します。
- リソース (EC2、IAM、S3、および on prem) で利用できる封じ込めオプションと、封じ込め時のワークロードの可用性への影響を理解します。



## 検出

AWS アカountの管理中、AMS はAmazon CloudWatch、Amazon GuardDuty、VPC フローログ、Amazon Macie、Amazon 内部脅威インテリジェンスフィードなど、検出ソースとコントロールから収集されたデータを使用して、ユーザー動作、アカウントアクティビティ、AWS Config 潜在的なセキュリティイベントの異常をモニタリングします。

AMS は、ネイティブ AWS サービスとその他の検出テクノロジーの両方を使用して、以下によって作成されたセキュリティイベントに対応します。

- Config 準拠の検出結果タイプ
- GuardDuty 検出結果タイプ
- Macie 検出結果タイプ
- Amazon Route 53 Resolver DNS ファイアウォールイベント
- AMS セキュリティイベント (クラウド監視アラーム)

サービス、製品、脅威エコシステムが進化するにつれて、追加の検出結果が追加されます。

### セキュリティイベントを AMS に報告する

AMS サポートポータルまたは サポート センターを通じてインシデントを提起し、セキュリティインシデントを AMS に通知するか、調査をリクエストします。

## 分析

セキュリティイベントを特定して報告した後、次のステップは、報告されたイベントが誤検出か実際のインシデントかを分析することです。AMS は、自動化と手動調査の手法を使用してセキュリティイベントを処理します。分析には、ネットワークトラフィックログ、ホストログ、CloudTrail イベント、AWS サービスログなど、さまざまな検出ソースからのログの調査が含まれます。この分析では、相関によって異常な動作を示すパターンも検索します。

パートナーシップは、アカウント環境に固有のコンテキストを理解し、アカウントとワークロードの正常性を確立するために必要です。これにより、AMS は異常をより迅速に特定し、インシデント対応を加速できます。



## セキュリティイベントに関する AMS からの通信を処理する

AMS は、インシデントチケットを通じてセキュリティ連絡先を関与させることで、調査中に情報を提供します。AMS クラウドサービスデリバリーマネージャー (CSDM) と AMS クラウドアーキテクト (CA) は、アクティブなセキュリティ調査中の通信のために連絡すべき連絡先です。

通信には、セキュリティアラートの生成時の自動通知、イベント分析後の通信、通話ブリッジの確立、ログファイルなどのアーティファクトの継続的な配信、感染したリソースのスナップショット、セキュリティイベント中の調査結果の取得が含まれます。

AMS セキュリティアラート通知に含まれる標準フィールドを以下に示します。これらのフィールドには、修復のために組織内の適切なチームにイベントをルーティングするための情報が表示されます。

- 検出結果タイプ
- 検出結果識別子 (該当する場合)
- 検出結果の重要度
- 検出結果の説明
- 作成された日付と時刻の検索
- AWS アカウント ID
- リージョン (該当する場合)
- AWS リソース (IAM user/role/policy、EC2、S3、EKS)

検出結果タイプに応じて追加のフィールドが提供されます。例えば、EKS 検出結果には Pod、コンテナ、クラスターの詳細が含まれます。

## 封じ込め

AMS の封じ込めアプローチは、お客様とのパートナーシップです。ネットワーク分離、IAM ユーザーまたはロールのプロビジョニング解除、インスタンスの再構築など、封じ込めアクティビティによって発生する可能性のあるビジネスとワークロードへの影響を理解している。

封じ込めの重要な部分は意思決定です。たとえば、システムをシャットダウンしたり、ネットワークからリソースを分離したり、アクセスをオフにしたり、セッションを終了したりできます。これらの決定は、インシデントを封じ込めるための事前定義された戦略と手順がある場合に簡単に行うことができます。AMS は、封じ込め戦略を提供し、封じ込めアクションの実装に伴うリスクを考慮した後にソリューションを実装します。

分析対象のリソースに応じて、さまざまな封じ込めオプションがあります。AMS では、インシデント調査中に複数のタイプの封じ込めが同時にデプロイされることを想定しています。これらの例には、次のようなものがあります。

- 保護ルールを適用して不正なトラフィックをブロックする (セキュリティグループ、NACL、WAF ルール、SCP ルール、拒否リスト、署名アクションを隔離またはブロックに設定する )
- リソースの分離
- ネットワークの隔離
- IAM ユーザー、ロール、ポリシーの無効化
- IAM ユーザー、ロール権限の変更/拒否
- コンピューティングリソースの終了/停止/削除
- 影響を受けるリソースからのパブリックアクセスの制限
- アクセスキー、API キー、パスワードの更新
- 公開された認証情報と機密情報をスクラブする

AMS では、リスク選好度の範囲内にある主要なインシデントタイプごとに、封じ込め戦略のタイプを検討することをお勧めします。インシデント発生時の意思決定に役立つ基準が明確に文書化されています。適切な戦略を決定するための基準は次のとおりです。

- リソースへの潜在的な損害
- 証拠の保存
- サービスの利用不能状態 (ネットワーク接続、外部関係者に提供されるサービスなど)
- 戦略の実装に必要な時間とリソース
- 戦略の有効性 (部分的封じ込め、完全封じ込めなど )
- ソリューションの永続性 (一方向ドアと双方向ドアの決定など )
- ソリューションの期間 (例えば、緊急回避策を 4 時間で削除する、一時的な回避策を 2 週間で削除する、永続的なソリューション )。
- 有効にできるセキュリティコントロールを適用してリスクを軽減し、より効果的な封じ込めを定義して実装する時間を確保します。

封じ込めの速度は重要です。AMS は、短期的および長期的なアプローチを戦略化することで、効率的かつ効果的な封じ込めを実現するための段階的なアプローチを推奨します。

このガイドでは、リソースタイプに基づいてさまざまな手法を含む封じ込め戦略を検討します。

## • 封じ込め戦略

- AMS はセキュリティインシデントの範囲を特定できますか？
  - できる場合は、すべてのリソース (ユーザー、システム、リソース) を特定します。
  - できない場合は、特定されたリソースに対する次のステップの実行と並行して調査します。
- リソースは分離できますか？
  - できる場合は、影響を受けるリソースの分離に進みます。
  - できない場合は、システム所有者とマネージャーと協力して、問題を封じ込めるために必要な追加のアクションを決定します。
- 影響を受けるすべてのリソースは、影響を受けないリソースから分離されていますか？
  - されている場合は、次のステップに進みます。
  - いいえの場合、インシデントがさらにエスカレートしないように、短期的な封じ込めが達成されるまで、影響を受けるリソースを分離し続けます。
- システムバックアップ
  - 影響を受けたシステムのバックアップコピーは、さらなる分析のために作成されましたか？
  - フォレンジックコピーは暗号化され、安全な場所に保存されていますか？
    - されている場合は、次のステップに進みます。
    - されていない場合は、フォレンジックイメージを暗号化し、誤って使用、損傷、改ざんされないように安全な場所に保存します。

## 根絶

インシデントが含まれていると、次の復旧段階に進む前に、システムを保護するために脅威の原因を完全に排除するために根絶が必要になる場合があります。排除ステップには、マルウェアの削除、侵害されたユーザーアカウントの削除、悪用されたすべての脆弱性の特定と軽減が含まれる場合があります。根絶時には、環境内の影響を受けるすべてのアカウント、リソース、インスタンスを特定して、修復できるようにすることが重要です。

修復ステップが優先されるように、根絶と復旧は段階的なアプローチで行うのがベストプラクティスです。大規模なインシデントの場合、復旧に数か月かかることがあります。初期フェーズの目的は、将来のインシデントを防ぐために、比較的迅速に (数日から数週間) 価値の高い変更を行うことで、全体的なセキュリティを向上させることです。後のフェーズでは、エンタープライズを可能な限り安全に維持するために、長期的な変更 (インフラストラクチャの変更など) と継続的な作業に焦点を当てる必要があります。

一部のインシデントでは、根絶は不要であるか、復旧中に実行されます。

以下の点を考慮してください。

- 攻撃のリスクを防止または軽減するために、システムを再イメージし、パッチやその他の対策で強化できますか？
- 攻撃者が残したマルウェアやその他のアーティファクトはすべて削除され、影響を受けるシステムはさらなる攻撃に対して強化されていますか？

## 復旧

AMS はお客様と連携して、システムを通常のオペレーションに復元し、システムが正常に機能していることを確認し、(該当する場合) 脆弱性を修正して同様のインシデントを防止します。

以下の点を考慮してください。

- 影響を受けたシステム (複数可) にパッチが適用され、最近の攻撃や将来の攻撃に対して強化されていますか？
- 影響を受けるシステムを本番環境に復元できる日時を教えてください。
- 本番環境に復元するシステムが最初の攻撃手法に対して脆弱でないことをテスト、モニタリング、検証するには、どのようなツールを使用しますか？

## インシデント後レポート

イベント後、AMS はすべてのセキュリティインシデントの調査レビュープロセスを実行します。また、AMS はエラー修正 (COE) プロセスを開始し、システムや、改善の余地があると思われる手続きミスによって引き起こされたセキュリティインシデントに対処します。AMS はお客様と連携して、セキュリティ調査エクスペリエンスを継続的に改善します。COE プロセスは、AMS が顧客に影響を与えるイベントの寄与要因を特定し、それらの原因を、同様のイベントが再発するのを防ぐことができる次のアクション項目に接続したり、影響の期間やレベルを軽減したりするのに役立ちます。

セキュリティインシデントの調査レビュープロセスでは、改善の機会を特定するために、以下の項目に対処します。

- インシデントの開始からインシデント検出、初期影響評価、インシデント処理プロセスの各段階 (封じ込め、復旧など) までの経過時間はどれくらいですか？
- インシデントの最初のレポートにインシデント対応チームが応答するまでにどのくらい時間がかかりましたか？

- 初期影響分析にはどのくらいの時間がかかりましたか？
- これは予防可能でしたか？ これを防ぐ可能性のあるツールやプロセスはありますか？
- これをより早く、どのように検出できたでしょうか。
- 調査を高速化できたことは何ですか？
- 文書化されたインシデント対応手順に従ったか？ それらは適切ですか？
- 他の利害関係者との情報共有はタイムリーに行われましたか？ どのように改善できますか？
- 他のチーム (AWS セキュリティ、アカウントチーム、AWS 開発チーム、カスタマーセキュリティチームの) とのコラボレーションは効果的ですか？ そうでない場合、改善できる点は何ですか？
- どのような準備手順が不足していて、エスカレーションマトリックス、RACI の、責任共有モデルなどが役に立ちましたか？ ランブックを更新する必要がありますか？
- 初期影響評価と最終影響評価の違いは何ですか？ インシデント対応の早い段階で評価の精度を向上させるために何ができますか？
- 学習した教訓から得られるアクション項目は何ですか？

## AMS のセキュリティインシデント対応ランブック

このセクションには、次の 2 つのランブックが含まれています。

- [ルートユーザーアクティビティへのレスポンス](#)
- [マルウェアイベントへの対応](#)

### ルートユーザーアクティビティへのレスポンス

[ルートユーザー](#)は、AWS アカウント内のスーパーユーザーです。AMS はルート使用状況をモニタリングすることに注意してください。ルートユーザーは、アカウント設定の変更、請求とコスト管理への AWS Identity and Access Management (IAM) アクセスのアクティブ化、ルートパスワードの変更、多要素認証 (MFA) の有効化など、必要ないいくつかのタスクにのみ使用することをお勧めします。詳細については、[「ルートユーザーの認証情報を必要とするタスク」](#)を参照してください。

計画されたルート使用状況を AMS に通知する方法の詳細については、[「AMS でルートアカウントを使用するタイミングと方法」](#)を参照してください。

ルートユーザーアクティビティが検出されると、ログインが成功した後にブルートフォース攻撃またはアカウント内のアクティビティを示すログインの試行に失敗すると、イベントが生成され、定義されたセキュリティ連絡先にインシデントが送信されます。

AWS Managed Services オペレーションは、計画外のルートユーザーアクティビティを調査し、データ収集、トリアージ、分析を実行し、お客様の指示に従って封じ込めアクティビティを実行し、イベント後分析を行います。

AMS Advanced 運用モデルを使用している場合は、AMS CSDM エンジニアと AMS Ops エンジニアから追加の通信を受け取り、ルートユーザーの認証情報を保護する AMS の責任により、計画外のルートユーザーのアクティビティを確認します。AMS は、パスフォワードを確認するまでルートユーザーのアクティビティを調査します。

## 準備

不要なインシデント対応アクティビティを防ぐために、計画されたイベントのデータと時刻を含む AMS サービスリクエストを送信することで、ルートユーザーの計画された使用について AMS に通知します。

AMS で GameDays を定期的の実施して、AMS の顧客インシデント対応プロセスを検証し、人員とシステムが最新であることを検証し、責任のある個人と連携し、インシデント対応を高速化します。

## フェーズ A: 検出

AMS は、GuardDuty や AMS モニタリングなどの検出ソースを通じて、アカウントのルートアクティビティをモニタリングします。

AMS Accelerate がある場合、運用モデルはインシデントに応答し、予期しないルートユーザーアクティビティの調査を要求します。これが発生すると、AMS オペレーションは侵害されたアカウントのランブックを開始します。

AMS Advanced を使用している場合、運用モデルはインシデントに応答するか、計画されたルートユーザーアクティビティを CSDM に通知し、アクティブなアカウント侵害調査を終了します。

## フェーズ B: 分析

AMS は、アクティビティが承認されていないと判断された場合、ルートユーザーイベントを徹底的に調査します。オートメーションと AMS セキュリティレスポンスチームの両方を使用して、ログとイベントがルートユーザーの異常と予期しない動作について分析されます。ログは、アクティビティが不明であるか、承認されたルートユーザーイベントであるか、さらに調査する必要があるかどうかを判断するのに役立ちます。

内部チェックをサポートするために調査中に提供される情報の例としては、次のようなものがあります。



- アカウント情報: ルートアカウントはどのアカウントで使用されましたか？
- ルートユーザーの E メールアドレス: 各ルートユーザーは、組織の E メールアドレスに関連付けられます。
- 認証の詳細: ルートユーザーが環境にアクセスした場所と時間
- アクティビティレコード: ルートとしてログインしたときに、ユーザーは何をしましたか？ これらのレコードは CloudWatch イベントの形式です。これらのログの読み方を理解することは、調査に役立ちます。

分析情報を受け取る準備を整え、組織内のアカウントの承認された連絡先に到達する方法を計画しておくことがベストプラクティスです。ルートユーザーの名前は個人ではないため、組織内のアカウントに使用されるルート E メールアドレスにアクセスできるユーザーを特定すると、質問を内部ですばやくルーティングできます。

## フェーズ C: 封じ込めと根絶

AMS はセキュリティチームと連携して、承認されたカスタマーセキュリティ担当者の指示に従って封じ込めを実行します。封じ込めオプションには以下が含まれます。

- 適切な認証情報とキーの更新。
- アカウントとリソースへのアクティブなセッションの終了。
- 作成されたリソースを消去します。

封じ込めアクティビティ中、AMS はセキュリティチームと緊密に連携して、ワークロードの中断を最小限に抑え、ルート認証情報が適切に保護されるようにします。

封じ込め計画が完了したら、AMS オペレーションチームと協力して、必要に応じて復旧アクションを行います。

## インシデント後レポート

必要に応じて、AMS は調査レビュープロセスを開始し、学んだ教訓を特定します。COE の完了の一環として、AMS は影響を受ける顧客に関連する検出結果を伝え、インシデント対応プロセスの改善を支援します。

AMS は調査のすべての最終詳細を文書化し、適切なメトリクスを収集し、割り当てられた CSDM や CA など、情報を必要とする AMS 内部チームにインシデントを報告します。

## マルウェアイベントへの対応

Amazon EC2 インスタンスは、組織内のアプリケーションチームがデプロイしたサードパーティソフトウェアやカスタム開発ソフトウェアなど、さまざまなワークロードをホストするために使用されます。AMS は、AMS によって継続的にパッチ適用および保守されているイメージにワークロードをデプロイすることを提供し、奨励します。

インスタンスのオペレーション中、AMS は Amazon GuardDuty、Endpoint Protection、ネットワークトラフィック、Amazon 内部脅威インテリジェンスフィードなど、さまざまなセキュリティ検出コントロールを通じて動作またはアクティビティの異常をモニタリングします。

AMS Advanced 運用モデルを使用する AMS のお客様は、プロビジョニングされたリソースにエンドポイントセキュリティ (EPS) モニタリングクライアントが自動的にインストールされます。これにより、イベントが検出されたときのセキュリティインシデントの作成など、リソースが 24 時間 365 日モニタリングおよびサポートされます。

AMS は GuardDuty Malware の検出結果もモニタリングします。これらは、有効になっている場合、AMS Advanced と AMS Accelerate の両方で使用できます。詳細については、[Amazon GuardDuty の Malware Protection](#)」を参照してください。

### Note

Bring [Your Own EPS](#) を選択した場合、インシデント対応のプロセスはこのページで説明されているプロセスとは異なります。詳細については、参照先のドキュメントを参照してください。

マルウェアが検出されると、インシデントが作成され、イベントが通知されます。この通知の後には、発生した修復アクティビティが続きます。AMS オペレーションは、調査、データ収集、トリアージ、分析を行い、その後、お客様の指示に従って封じ込めアクティビティを実行し、イベント後分析を行います。

### フェーズ A: 検出

AMS は、GuardDuty とエンドポイントセキュリティソリューションのモニタリングを使用して、インスタンスのイベントをモニタリングします。AMS は、検出結果またはアラートタイプに基づいて封じ込めまたはリスクの受け入れを決定するのに役立つ適切なエンリッチメントおよびトリアージアクティビティを決定します。



データ収集は、検出結果タイプに基づいて実行されます。データ収集では、影響を受けたアカウントの内部と外部の両方に複数のデータソースをクエリして、観察されたアクティビティや関心のある設定の全体像を構築します。

AMS は、影響を受けたアカウントまたは AMS 脅威インテリジェンスプラットフォームからの他のアラームやアラート、テレメトリと結果の相関を実行します。

## フェーズ B: 分析

データが収集されると、そのデータが分析され、懸念されるアクティビティや指標が特定されます。調査のこの段階で、AMS はユーザーと協力して、インスタンスとワークロードに関するビジネスとドメインの知識を統合し、何が期待され、何が通常と異なるかを理解するのに役立ちます。

内部チェックをサポートするために調査中に提供される情報の例としては、次のようなものがあります。

- アカウント情報: マルウェアアクティビティはどのアカウントで観察されましたか？
- インスタンスの詳細: マルウェアイベントに関連するインスタンス (複数可)
- イベントタイムスタンプ: アラートはいつトリガーされましたか？
- ワークロード情報: インスタンスで実行されているものは何ですか？
- 該当する場合はマルウェアの詳細: マルウェアのファミリーとマルウェアに関するオープンソース情報。
- ユーザーまたはロールの詳細: アクティビティの影響を受けるユーザーまたはロール
- アクティビティレコード: インスタンスにはどのようなアクティビティが記録されますか？ これらは CloudWatch イベント、およびインスタンスからのシステムイベントの形式です。これらのログの読み方を理解すると、調査に役立ちます。
- ネットワークアクティビティ: インスタンスに接続しているエンドポイント、インスタンスに接続しているエンドポイント、トラフィック分析とは

調査情報を受け取る準備を整え、組織内のアカウント、インスタンス、ワークロードの適切な連絡先に連絡する方法について計画を立てるのがベストプラクティスです。ネットワークトポロジと予想される接続を理解することで、影響分析を高速化できます。環境で計画されたペネトレーションテストと、アプリケーション所有者が最近実行したデプロイに関する知識があれば、調査を高速化することもできます。

アクティビティが計画および承認されていると判断した場合、インシデントが更新され、調査は終了します。侵害が確認された場合は、お客様と AMS が適切な封じ込め計画を決定します。

## フェーズ C: 封じ込めと根絶

AMS はお客様と協力して、収集されたデータと既知の情報に基づいて、適切な封じ込めアクティビティを決定します。封じ込めオプションには以下が含まれますが、これらに限定されません。

- スナップショットによるデータの保存
- インスタンスに出入りするトラフィックを制限するようにネットワークルールを変更する
- SCP、IAM ユーザー、ロールポリシーを変更してアクセスを制限する
- インスタンスの終了、停止、または無効化
- 永続接続の終了
- 適切な認証情報/キーの更新

インスタンスに対して根絶アクティビティを実行することを選択した場合、AMS はこれを達成するためにサポートします。オプションには以下が含まれますが、これらに限定されません。

- 不要なソフトウェアの削除
- 完全にパッチが適用されたクリーンなイメージからインスタンスを再構築し、アプリケーションと設定を再デプロイする
- 以前のバックアップからインスタンスを復元する
- ワークロードのホストに適したアプリケーションとサービスを アカウント内の別のインスタンスにデプロイします。

サービスが復元される前に、マルウェアがインスタンスでどのように配信および実行されたかを判断し、インスタンスでのマルウェアの再発を防ぐために追加のコントロールが適用されていることを確認することが重要です。AMS は、フォレンジックをサポートするために必要に応じてフォレンジックパートナーまたはチームに追加のインサイトや情報を提供します。

この時点で、復旧アクティビティのために AMS オペレーションを使用します。AMS はお客様と密接に連携して、ワークロードの中断を最小限に抑え、インスタンスを保護します。

## インシデント後レポート

必要に応じて、AMS は調査レビュープロセスを開始し、学んだ教訓を特定します。COE の完了の一環として、AMS はインシデント対応プロセスの改善に役立つ関連する検出結果を伝えます。

AMS は、調査の最終詳細を文書化し、適切なメトリクスを収集し、割り当てられた CSDM や CA などの情報を必要とする AMS 内部チームにインシデントを報告します。

# AMS Advanced での変更リクエストのセキュリティレビュー

AWS Managed Services 変更リクエストのレビュープロセスにより、AMS は、リクエストされた変更がアカウントでユーザーに代わって実装される際に、セキュリティレビューを実行します。

[AMS Advanced 技術標準](#) は、アカウントのベースラインセキュリティを確立するための最小限のセキュリティ基準、設定、プロセスを定義します。AMS がリクエストされた変更を実装するときは、これらの標準に従います。

AMS は、すべての変更リクエストを AMS 技術標準に照らして評価します。技術標準から逸脱することでアカウントのセキュリティ体制を低下させる可能性のある変更は、セキュリティレビュープロセスを通じて行われます。このプロセスでは、関連するリスクが AMS によって強調表示され、セキュリティとビジネスのニーズのバランスを取るために、承認されたリスク承認者によってレビューおよび承認されます。

## カスタマーセキュリティリスク管理プロセス

AMS Advanced Customer Security Risk Management (CSRM) プロセスは、リスクを明確に特定し、適切な所有者に伝えるのに役立ちます。このプロセスにより、環境内のセキュリティリスクが最小限に抑えられ、特定されたリスクに対する継続的な運用オーバーヘッドが軽減されます。

デフォルトでは、組織の誰かが AMS にマネージド環境への変更の実装をリクエストすると、AMS は変更を確認して、リクエストが技術標準に違反していないかどうかを判断します。これにより、アカウントのセキュリティ体制が変わる可能性があります。セキュリティリスクが高い、または非常に高い場合は、承認されたセキュリティ担当者が変更レビューを承認または拒否します。リクエストされた変更は、AMS のアカウント運用能力に悪影響がないかも評価されます。レビューで潜在的な悪影響が見つかった場合は、AMS 内で追加のレビューと承認が必要です。

## リスク許容の有効性とレビュー

リスク承認は、承認日から 1 年間有効です。以前に受け入れられたリスクシナリオが 1 年後に再び発生する場合は、適用する前にリスクの受け入れを確認して再承認する必要があります。この年次レビューにより、リスクに関する意思決定が、現在の技術標準、規制要件、組織の進化するリスクプロファイルと整合性が保たれます。

## オプトアウト

CSRM プロセスの承認ベースのワークフローからオプトアウトして、高リスクまたは非常に高いリスクを回避できます。特定のアカウントの CSRM オプションを標準 CSRM から通知のみに

変更するには、Cloud Service Delivery Managers と協力して 1 回限りのリスク承諾を作成します。Notification Only オプションに進むことを選択した場合、AMS はリスクカテゴリに関係なく、リスクエラストされた変更を実装します。また、AMS は、変更の実装前に承認を求める代わりに、承認されたリスク承認者にリスク通知を送信します。

AMS CSRM プロセス、新しい AMS アカウントのオンボーディング時にデフォルトの CSRM オプションを変更する方法、または既存のアカウントを更新する方法の詳細については、Cloud Architects または Cloud Service Delivery Managers にお問い合わせください。

#### Note

AMS では、すべてのアカウントで標準 CSRM のデフォルトオプションを使用することを強くお勧めします。

## AMS Advanced 技術標準

AMS Advanced 技術標準カテゴリは次のとおりです。

| ID          | カテゴリ                               |
|-------------|------------------------------------|
| AMS-STD-001 | タグ付け設定                             |
| AMS-STD-002 | AWS Identity and Access Management |
| AMS-STD-003 | ネットワークセキュリティ                       |
| AMS-STD-004 | 侵入テスト                              |
| AMS-STD-005 | Amazon GuardDuty                   |
| AMS-STD-006 | ホストセキュリティ                          |
| AMS-STD-007 | ログ記録                               |
| AMS-STD-008 | AMS-MAD                            |
| AMS-STD-009 | 雑則                                 |

# AMS Advanced の標準コントロール

AMS の標準コントロールは次のとおりです。

## AMS-STD-001 - タグ付け設定

以下は、001 - タグ付け設定の標準コントロールです。

1. 運用および管理の目的で AMS チームが必要とするすべての AWS リソースには、次のキーと値のペアが必要です。
  - AppId= AMSInfrastructure
  - 環境 = AMSInfrastructure
  - AppName = AMSInfrastructure
  - AMSResource=True
2. 前述のもの以外の AMS チームが必要とするすべてのタグには、AMS プレフィックスのリストに記載されているプレフィックスが必要です (「注」を参照)。
3. AMS チームに必要なタグ値 (AppId、Environment、AppName) は、変更リクエストに基づいてユーザーが作成した任意のリソースで変更できます。
4. AMS に必要なスタックのタグは、変更リクエストに基づいて削除しないでください。
5. ポイント 2 で説明したように、インフラストラクチャに AMS タグ命名規則を使用することはできません。
6. AMS に必要なリソースにカスタムタグを作成できます (通常は請求とコストレポートのユースケース用)。リソースがテンプレートの更新ではなくスタックの更新によって更新された場合、カスタムタグは保持されます。

### Note

#### AMS プレフィックスのリスト

1. ams-\*
2. AWSManagedServices\*
3. /ams/\*
4. ams\*
5. AMS\*
6. Ams\*

7. mc\*
8. MC\*
9. Mc\*
- 10.センチネル\*
- 11.センチネル\*
- 12.Managed\_Services\*
- 13.NewAMS\*
- 14.AWS\_\*
- 15.aws\*
- 16.VPC\_\*
- 17.CloudTrail\*
- 18.Cloudtrail\*
- 19/aws\_reserved/
- 20取り込み\*
- 21EPSDB\*
- 22MMS\*
- 23.TemplateId\*
- 24.StackSet-ams\*
- 25.StackSet-AWS-Landing-Zone
- 26JAMPolicy\*
- 27.customer-mc-\*
- 28ルート\*
- 29LandingZone\*
- 30.StateMachine\*
- 31.codedeploy\_service\_role
- 32.managementhost
- 33.sentinel.int。
- 34.eps
- 35.UnhealthyInServiceBastion
- 36.ms-

## AMS-STD-002 - AWS Identity and Access Management (IAM)

| ID  | 技術標準                                                                                                                                                                                                                                                                                                                              |
|-----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.0 | タイムアウト期間                                                                                                                                                                                                                                                                                                                          |
| 1.1 | フェデレーティッドユーザーのデフォルトのタイムアウトセッションは 1 時間で、最大 4 時間まで増やすことができます。                                                                                                                                                                                                                                                                       |
| 1.2 | デフォルトのスタックアクセス時間は 12 時間です。                                                                                                                                                                                                                                                                                                        |
| 2.0 | AWS ルートアカウントの使用状況                                                                                                                                                                                                                                                                                                                 |
| 2.1 | 何らかの理由でルートアカウントの使用状況がある場合、Amazon GuardDuty は関連する検出結果を生成するように設定する必要があります。                                                                                                                                                                                                                                                          |
| 2.2 | シングルアカウントランディングゾーン (SALZ) アカウントとマルチアカウントランディングゾーン (MALZ) 管理アカウント (以前はマスター/請求アカウントと呼ばれていました) では、ルートユーザーアカウントで仮想 MFA が有効になっている必要があります、アカウントのオンボーディング中に MFA ソフトトークンが破棄されるため、AMS も顧客もルートとしてログインできません。標準の AWS ルートパスワードの紛失プロセスは、AMS Cloud Service Delivery Manager (CSDM) と組み合わせて実行する必要があります。この設定は、AMS マネージドアカウントのライフサイクル中も維持する必要があります。 |
| 2.3 | ルートアカウントのアクセスキーを作成しないでください。                                                                                                                                                                                                                                                                                                       |



| ID    | 技術標準                                                                                                                                                                                                     |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3.0   | ユーザーの作成と変更                                                                                                                                                                                               |
| 3.1   | プログラムによるアクセスと読み取り専用アクセス許可を持つ IAM ユーザー/ロールは、時間制限付きポリシーなしで作成できます。ただし、アカウント内のすべての Amazon Simple Storage Service バケット内のオブジェクト (S3:GetObject など) の読み取りを許可するアクセス許可は許可されません。                                    |
| 3.1.1 | コンソールアクセスおよび読み取り専用アクセス許可を持つ IAM ヒューマンユーザーは、時間制限ポリシー (最大 180 日) を使用して作成できますが、時間制限ポリシーremoval/renewal/extensionすると、リスク通知が発生します。ただし、アカウント内のすべての S3 バケット内のオブジェクト (S3:GetObject など) の読み取りを許可するアクセス許可は許可されません。 |
| 3.2   | コンソールの IAM ユーザーとロール、およびお客様のアカウントのインフラストラクチャ変更アクセス許可 (書き込みとアクセス許可の管理) を持つプログラムによるアクセスは、リスクの承諾なしに作成しないでください。S3 オブジェクトレベルの書き込みアクセス許可には例外があり、特定のバケットが AMS 関連以外のタグのスコープおよびタグ付けオペレーションにある限り、リスクを受け入れずに許可されます。  |

| ID  | 技術標準                                                                                                                                                                                                                                                                                                                      |
|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3.3 | SALZ または MALZ アプリケーションアカウントcustomer_servicenow_user および *コアアカウント* での ServiceNow 統合customer_servicenow_logging_user に必要な という名前のプログラムによるアクセス権を持つ IAM ユーザーは、時間制限付きポリシーなしで作成できます。                                                                                                                                             |
| 3.4 | SALZ アカウントcustomer_cloud_endure_policy と MALZ アカウントでの CloudEndure 統合に必要な と customer_cloud_endure_deny_policy (読み取り専用アクセス) を使用する、プログラムによるアクセス権を持つ IAM ユーザーを作成できますが、計画された移行期間中は制限されたポリシーが必要です。時間制限は、RA なしで最大 180 日間にすることができます。また、SCP は MALZ アカウントの変更を許可され、これらのポリシーを必要な期間にわたって機能させることができます。必要に応じて適切な移行ウィンドウを定義し、必要に応じて調整します。 |
| 4.0 | ポリシー、アクション、APIs                                                                                                                                                                                                                                                                                                           |
| 4.1 | SALZ アカウントのすべての IAM ユーザーとロールには、AMS インフラストラクチャを偶発的または意図的な損傷から保護するために、デフォルトのカスタマー拒否ポリシー (CDP) がアタッチされている必要があります。                                                                                                                                                                                                            |
| 4.2 | AMS SCPs は、MALZ のすべての AMS マネージドアカウントで有効にする必要があります。                                                                                                                                                                                                                                                                        |

| ID  | 技術標準                                                                                                         |
|-----|--------------------------------------------------------------------------------------------------------------|
| 4.3 | PutKeyPolicy 、 、 などの KMS キーに対して管理アクションを実行できる ID はScheduleKeyDeletion 、 AMS 演算子とオートメーションプリンシパルのみに制限する必要があります。 |
| 4.4 | ポリシーは、リスクを受け入れずに、管理者アクセスに「Effect」：「Allow」と「Action」：「*」を「Resource」：「*」にしたステートメントを提供してはいけません。                  |
| 4.5 | IAM ポリシーには、リスクを受け入れずにバケットに S3:*** を許可するアクションを含むアクションを含めることはできません。                                            |
| 4.6 | カスタマー IAM ポリシーの AMS インフラストラクチャキーの KMS キーポリシーに対する API コールは許可しないでください。                                         |
| 4.7 | インスタンスの起動または停止、S3 バケットまたは RDS インスタンスの作成など、変更管理プロセス (RFC) をバイパスするアクションは許可しないでください。                            |
| 4.8 | Amazon Route 53 の AMS インフラストラクチャ DNS レコードを変更するアクションは許可されません。                                                 |
| 4.9 | 適切なプロセスに従って作成されたコンソールアクセスを持つ IAM ヒューマンユーザーは、信頼ポリシー、継承ロール、時間制限ポリシーを除き、直接アタッチされたポリシーを持つことはできません。               |

| ID     | 技術標準                                                                                                                                                                   |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4.10   | 同じアカウント AWS Secrets Manager 内の特定のシークレットまたは名前空間への読み取りアクセス権を持つ Amazon EC2 インスタンスプロファイルを作成できます。                                                                           |
| 4.11   | AWS Managed Services Change Management (AMSCM) または AWS Managed Services Service Knowledge Management System (AMSSKMS) のアクセス許可は、任意のロール (SR/Incident/RFC を開く機能) に追加できます。 |
| 4.12   | IAM ポリシーには、AMS Amazon CloudWatch ロググループで log:DeleteLogGroup および logs:DeleteLogStream を許可するアクションを含むアクションを含めることはできません。                                                   |
| 4.13   | マルチリージョンキーを作成するアクセス許可は許可しないでください。                                                                                                                                      |
| 4.14   | アカウントでまだ作成されていない S3 バケット ARNs へのアクセスを提供するには、サービス固有の S3 条件キーを使用してアカウント番号s3:ResourceAccount を指定します。                                                                      |
| 4.15   | カスタムダッシュボードへのアクセスを表示、作成、一覧表示、削除できますが、Amazon CloudWatch ダッシュボードへのアクセスのみを表示および一覧表示できます。                                                                                  |
| 4.15.1 | S3 ストレージレンズのカスタムダッシュボードを表示、作成、一覧表示、削除できます。                                                                                                                             |
| 4.16   | SQL Workbench 関連の完全なアクセス許可は、Amazon Redshift データベースを操作するロール/ユーザーに付与できます。                                                                                                |

| ID   | 技術標準                                                                                                                                                                                                                                                                    |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4.17 | CLI の代わりに、お客様のロールにアクセス<br>AWS CloudShell 許可を付与できます。                                                                                                                                                                                                                     |
| 4.18 | を信頼されたプリンシパル AWS のサービス と<br>する IAM ロールも、IAM 技術標準に準拠して<br>いる必要があります。                                                                                                                                                                                                     |
| 4.19 | サービスにリンクされたロール (SLRs)<br>は、IAM サービスチームによって構築および管<br>理されるため、AMS IAM 技術標準の対象では<br>ありません。                                                                                                                                                                                  |
| 4.20 | <p>IAM ポリシーでは、アカウント内のすべての<br/>バケットで Amazon S3 バケットオブジェクト<br/>(Amazon S3:GetObject など) への無制限の読み<br/>取りアクセスを許可することはできません。</p> <ul style="list-style-type: none"><li>• デベロッパーモードのアカウント: 違反によ<br/>りリスク通知が発生する</li><li>• デベロッパーモード以外のアカウントの場<br/>合: 違反にはリスク許容が必要です</li></ul> |
| 4.21 | リソースタイプ「savingsplan」のすべての<br>IAM アクセス許可を顧客に付与できます。                                                                                                                                                                                                                      |
| 4.22 | AMS エンジニアは、Amazon S3、Amazon S3<br>オブジェクト、データベース) を手動でコピー<br>または移動することはできません。 Amazon<br>Relational Database Service DynamoDB                                                                                                                                             |
| 4.23 | SCP ポリシーを変更して、どの AMS マネージ<br>ドアカウントでも追加のアクセスを許可しない<br>でください。                                                                                                                                                                                                            |

| ID   | 技術標準                                                                                                                                                                                       |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4.24 | AMS インフラストラクチャまたは管理機能を損なう可能性のある SCP ポリシーの変更は許可しないでください。(注: AMS リソースには タグAppId= AMSInfrastructure があり、AMS 保護された名前空間に従います)。                                                                  |
| 4.25 | AMS 自動 IAM プロビジョニング機能は、オプトイン機能としてアカウントで有効にする必要があります。                                                                                                                                       |
| 4.26 | AMS の人間が引き受けるロールまたはユーザーは、S3、RDS、DynamoDB、Redshift、Elasticache、EFS、FSx の顧客コンテンツにアクセスすることはできません。また、お客様のコンテンツへのアクセスを許可する他のによってリリース AWS のサービスされた既知の新しい APIs へのアクセスは、オペレーターロールで明示的に拒否する必要があります。 |
| 5.0  | フェデレーション                                                                                                                                                                                   |
| 5.1  | 認証は、AMS マネージドアカウントのフェデレーションを使用して設定する必要があります。                                                                                                                                               |
| 5.2  | AMS AD からアクティブディレクトリへの一方向の送信信頼のみが必要です (AMS AD はオンプレミス AD を信頼します)。                                                                                                                          |
| 5.3  | AMS への認証に使用される ID ストアは、AMS マネージドアプリケーションアカウントに存在してはいけません。                                                                                                                                  |
| 6.0  | クロスアカウントポリシー                                                                                                                                                                               |

| ID    | 技術標準                                                                                                                                                        |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6.1   | IAM ロールは、顧客レコードに従って、同じ顧客に属する AMS アカウント間で信頼ポリシーを設定できます。                                                                                                      |
| 6.2   | AMS アカウントと AMS 以外のアカウント間の IAM ロールの信頼ポリシーは、AMS 以外のアカウントが同じ AMS 顧客によって所有されている場合にのみ設定する必要があります (同じ AWS Organizations アカウントにあることを確認するか、E メールドメインを顧客の会社名と照合します)。 |
| 6.3   | AMS アカウントとサードパーティーアカウント間の IAM ロールの信頼ポリシーは、リスクの承諾なしに設定しないでください。                                                                                              |
| 6.4   | 同じ顧客の AMS アカウント間でカスタマー管理の CMKs にアクセスするためのクロスアカウントポリシーを設定できます。                                                                                               |
| 6.5   | AMS アカウントによって非 AMS アカウント内の任意の KMS キーにアクセスするためのクロスアカウントポリシーを設定できます。                                                                                          |
| 6.6   | サードパーティーアカウントが AMS アカウント内の KMS キーにアクセスするためのクロスアカウントポリシーは、リスクの承諾なしに許可してはいけません。                                                                               |
| 6.6.1 | 非 AMS アカウントが AMS アカウント内の任意の KMS キーにアクセスするためのクロスアカウントポリシーは、非 AMS アカウントが同じ AMS 顧客によって所有されている場合にのみ設定できます。                                                      |



| ID   | 技術標準                                                                                                                                                                                                                                                                      |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6.7  | 同じ顧客の AMS アカウント間でデータを保存できる S3 バケットデータまたはリソース (Amazon RDS、Amazon DynamoDB、Amazon Redshift など) にアクセスするためのクロスアカウントポリシーを設定できます。                                                                                                                                               |
| 6.8  | 読み取り専用アクセス権を持つ AMS アカウントから、非 AMS アカウントにデータを保存できる S3 バケットデータまたはリソース (Amazon RDS、Amazon DynamoDB、Amazon Redshift など) にアクセスするためのクロスアカウントポリシーを設定できます。                                                                                                                         |
| 6.9  | AMS から非 AMS アカウント (または非 AMS から AMS アカウント) への書き込み権限を持つデータを保存できる S3 バケットデータまたはリソース (Amazon RDS、Amazon DynamoDB、Amazon Redshift など) にアクセスするためのクロスアカウントポリシーは、非 AMS アカウントが同じ AMS 顧客によって所有されている (同じ AWS Organizations アカウントにあることを確認するか、E メールドメインを顧客の会社名と照合する) 場合にのみ設定する必要があります。 |
| 6.10 | 読み取り専用アクセス権を持つ AMS アカウントからサードパーティーアカウント (Amazon RDS、Amazon DynamoDB、Amazon Redshift など) にデータを保存できる S3 バケットデータまたはリソースにアクセスするためのクロスアカウントポリシーを設定できます。                                                                                                                        |

| ID   | 技術標準                                                                                                                                                          |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6.11 | 書き込みアクセスを持つ AMS アカウントからサードパーティーアカウント (Amazon RDS、Amazon DynamoDB、Amazon Redshift など) にデータを保存できる S3 バケットデータまたはリソースにアクセスするためのクロスアカウントポリシーは、リスクの承諾なしに設定しないでください。 |
| 6.12 | AMS カスタマー S3 バケットまたはデータを保存できるリソース (asAmazon RDS、Amazon DynamoDB、Amazon Redshift など) にアクセスするためのサードパーティーアカウントのクロスアカウントポリシーは、リスクの承諾なしに設定しないでください。                |
| 7.0  | ユーザーグループ                                                                                                                                                      |
| 7.1  | 読み取り専用アクセス許可と非変更アクセス許可を持つ IAM グループは許可されます。                                                                                                                    |
| 8.0  | リソースベースのポリシー                                                                                                                                                  |
| 8.1  | AMS インフラストラクチャリソースは、リソースベースのポリシーをアタッチすることで、不正な ID による管理から保護する必要があります。                                                                                         |
| 8.2  | 別のポリシーを明示的に指定しない限り、リソースは最小特権のリソースベースのポリシーで設定する必要があります。                                                                                                        |
| 9.0  | セルフサービスプロビジョニングサービス (SSPS)                                                                                                                                    |

| ID  | 技術標準                                                                                                                                                                                         |
|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 9.1 | AMS のデフォルトの IAM ロールまたはポリシー (インスタンスプロファイル、SSPS、パターンを含む) は、リスク承諾の有無にかかわらず変更しないでください。信頼ポリシーの例外は許可されます (リスク承諾なし)。ロール、ポリシー、またはユーザーの変更のタグ付けは、デフォルトの SSP ロールでも許可されます。                               |
| 9.3 | Systems Manager Automation コンソールロールの SSPS ポリシーを、デフォルトロール以外のカスタムロールにアタッチすることはできません。他の SSPS ポリシーをカスタム IAM ロールにアタッチするには、カスタムロールへのポリシーのアタッチが、デフォルトの SSPS サービスの意図した設計外の追加のアクセス許可を提供していないことを確認します。 |
| 9.6 | プログラムによるアクセス (アクセスキーを使用) と、お客様のアカウントのインフラストラクチャ変更アクセス許可 (書き込み、アクセス許可管理、またはタグ付け) を持つ IAM ユーザーを必要とする SSPS は、リスクを受け入れることなくプロビジョニングすることはできません。                                                   |
| 9.7 | SSPS サービス用に作成されたポリシーは、リスクの承諾なしに IAM ユーザーにアタッチしないでください。                                                                                                                                       |

## AMS-STD-003 - ネットワークセキュリティ

以下は、003 - Network Security の標準コントロールです。

| ID  | 技術標準                                                                                                                                                                                                          |
|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     | ネットワーク                                                                                                                                                                                                        |
| 1.0 | すべての EC2 インスタンスには、踏み台ホスト、踏み台ホスト VPC CIDR 範囲、または同じインスタンス VPC CIDR 範囲を介してのみ、SSH または RDP 経由でアクセスする必要があります。                                                                                                       |
| 2.0 | EC2 インスタンスの Elastic IP が許可されます                                                                                                                                                                                |
| 3.0 | AMS コントロールプレーンとデータプレーン TLS 1.2 以降の拡張を使用する必要があります。                                                                                                                                                             |
| 4.0 | すべての出力トラフィックは、アカウント IGW または TGW を使用して渡す必要があります。                                                                                                                                                               |
| 5.0 | 9.0 に従ってロードバランサーにアタッチされていない場合、セキュリティグループはインバウンドルールでソースを 0.0.0.0/0 にすることはできません                                                                                                                                 |
| 6.0 | S3 バケットまたはオブジェクトは、リスクを受け入れることなく公開してはいけません。                                                                                                                                                                    |
| 7.0 | ポート SSH/22 または SSH/2222 (SFTP/2222 以外)、TELNET/23、RDP/3389、WinRM/5985-5986、VPC/5900-5901 TS/CITRIX/1494 または 1604、LDAP/389 または 636、および RPC/135、NETBIOS/137-139 でのサーバー管理アクセスは、セキュリティグループを介して VPC 外部から許可してはいけません。 |
| 8.0 | ポート (MySQL/3306、PostgreSQL/5432、Oracle/1521、MSSQL/1433) またはカスタムポートでのデータベース管理アクセスは、セ                                                                                                                           |

| ID   | 技術標準                                                                                                                                               |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------|
|      | セキュリティグループを介して DX、VPC ピア、または VPN 経由で VPC にルーティングされないパブリック IPs から許可してはいけません。                                                                        |
| 8.1  | 顧客データを保存できるリソースは、パブリックインターネットに直接公開しないでください。                                                                                                        |
| 9.0  | インターネットからのポート HTTP/80、HTTPS/8443、HTTPS/443 経由の直接アプリケーションアクセスは、ロードバランサーにのみ許可されますが、EC2 インスタンス、ECS/EKS/Fargate コンテナなどのコンピューティングリソースに直接アクセスすることはできません。 |
| 10.0 | 顧客のプライベート IP 範囲からのポート HTTP/80 および HTTPS/443 を介したアプリケーションアクセスを許可できます。                                                                               |
| 11.0 | AMS インフラストラクチャへのアクセスを制御するセキュリティグループへの変更は、リスクを受け入れることなく許可してはなりません。                                                                                  |
| 12.0 | AMS Security とは、セキュリティグループがインスタンスにアタッチされるたびに標準を指します。                                                                                               |
| 13.0 | ポート 3389 および 22 のカスタマー踏み台アクセスは、DX、VPC ピア、または VPN を介して VPC にルーティングされるプライベート IP 範囲からのみ許可する必要があります。                                                   |

| ID   | 技術標準                                                                                                                                                                                                      |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 14.0 | AMS から非 AMS アカウント (または非 AMS から AMS アカウント) への VPCs とのプライベートホストゾーンのクロスアカウント関連付けは、非 AMS アカウントが同じ AMS 顧客によって所有されている (同じ AWS Organization アカウントにあることを確認するか、E メールドメインを顧客の会社名と照合する) 場合にのみ、内部ツールを使用して設定する必要があります。 |
| 15.0 | 同じ顧客に属するアカウント間の VPC ピアリング接続を許可できます。                                                                                                                                                                       |
| 16.0 | AMS ベース AMIs は、両方のアカウントが同じ顧客によって所有されている (同じ AWS Organizations アカウントにあることを確認するか、E メールドメインを顧客の会社名と照合する) 限り、AMS 以外のアカウントと共有できません。                                                                            |
| 17.0 | FTP ポート 21 は、リスクを受け入れることなく、どのセキュリティグループでも設定しないでください。                                                                                                                                                      |
| 18.0 | トランジットゲートウェイを介したクロスアカウントネットワーク接続は、すべてのアカウントが顧客によって所有されている限り許可されます。                                                                                                                                        |
| 19.0 | プライベートサブネットをパブリックにすることは許可されていません                                                                                                                                                                          |
| 20.0 | サードパーティーアカウント (お客様が所有していないアカウント) との VPC ピアリング接続は許可しないでください。                                                                                                                                               |

| ID   | 技術標準                                                                                              |
|------|---------------------------------------------------------------------------------------------------|
| 21.0 | サードパーティーアカウント (お客様が所有していないアカウント) との Transit Gateway アタッチメントは許可しないでください。                           |
| 22.0 | AMS がお客様にサービスを提供するために必要なネットワークトラフィックは、お客様のネットワーク送信ポイントでブロックしないでください。                              |
| 23.0 | 同じ顧客 AWS アカウント が所有する とのリゾルバールールの共有は、リスク通知で許可されます                                                  |
| 19.0 | ICMP                                                                                              |
| 19.1 | 顧客インフラストラクチャからの Amazon EC2 へのインバウンド ICMP リクエストには、リスク通知が必要です。                                      |
| 19.2 | DX、VPC ピア、またはセキュリティグループ経由の VPN を介して Amazon VPC にルーティングされたパブリック IPs からのインバウンド リクエストが許可されます。        |
| 19.3 | セキュリティグループ経由で DX、VPC ピア、または VPN 経由で Amazon VPC にルーティングされないパブリック IPs からのインバウンド リクエストには、リスク承諾が必要です。 |
| 19.4 | Amazon EC2 から任意の宛先へのアウトバウンド ICMP リクエストが許可されます。                                                    |
| 20.0 | セキュリティグループ共有                                                                                      |

| ID   | 技術標準                                                                                                                                         |
|------|----------------------------------------------------------------------------------------------------------------------------------------------|
| 20.1 | セキュリティグループがこのセキュリティ標準を満たしている場合、同じアカウントの VPCs 間、および同じ組織内のアカウント間で共有できます。                                                                       |
| 20.2 | セキュリティグループがこの標準を満たさず、このセキュリティグループに以前リスク承諾が必要だった場合、同じアカウントの VPCs 間、または同じ組織内のアカウント間でセキュリティグループ共有機能を使用することは、その新しい VPC またはアカウントのリスク承諾なしに許可されません。 |

## AMS-STD-004 - 侵入テスト

004 - 侵入テストの標準コントロールを次に示します。

1. AMS はペンテストインフラストラクチャをサポートしていません。お客様の責任となります。例えば、Kali は Linux の AMS でサポートされているディストリビューションではありません。
2. お客様は、[侵入テスト](#)に従う必要があります。
3. AMS は、顧客がアカウント内でインフラストラクチャ侵入テストを実行する場合に備えて、24 時間前に事前に通知する必要があります。
4. AMS は、顧客による変更リクエストまたはサービスリクエストに明示的に記載されている顧客要件ごとに、顧客のペンテストインフラストラクチャをプロビジョニングします。
5. お客様のペンテストインフラストラクチャの ID 管理はお客様の責任です。

## AMS-STD-005 - GuardDuty

005 の標準コントロール - GuardDuty を次に示します。

1. GuardDuty は、すべてのカスタマーアカウントで常に有効にする必要があります。
2. MALZ のカスターマネージドアプリケーションアカウント (CMA) からの GuardDuty の検出結果では、運用チームのアラームは発生しません。



3. GuardDuty アラートは、同じアカウント、または同じ組織内の他のマネージドアカウントに保存する必要があります。
4. GuardDuty の信頼できる IP リスト機能を使用しないでください。代わりに、自動アーカイブを代替として使用できます。これは監査目的に役立ちます。
5. 委任管理者は、リスクを受け入れることなく他のアカウントで GuardDuty を無効にするなど、高特権アクションを実行できるため、GuardDuty 管理者の委任を MALZ で有効にすることはできません。
6. GuardDuty 自動アーカイブフィルターは、最大リターンの最小スコープを使用する必要があります。たとえば、AMS が異なる CIDR ブロックに複数の予測不可能な IPs を表示し、適切な企業 ASN がある場合は、ASN を使用します。ただし、特定の範囲または /32 アドレスにスコープダウンできる場合は、それらの範囲にスコープダウンします。

## AMS-STD-006 - ホストセキュリティ

006 - ホストセキュリティの標準コントロールを次に示します。

- ウイルス対策エージェントは常にすべての EC2 インスタンスで実行されている必要があります (Trend Micro DSM など)。
- マルウェア対策モジュールを有効にする必要があります。
- EPS エージェントには、スキャンするすべてのディレクトリとファイルが含まれている必要があります。
- ウイルス対策ソリューションによって隔離されたファイルは、オンデマンドでと共有できます。
- サードパーティーのエンドポイントセキュリティソリューションをインストールしないでください。
- ウイルス対策署名の更新頻度は、少なくとも 1 日に 1 回に設定する必要があります。
- スケジュールされたスキャン頻度は、少なくとも 1 か月に 1 回に設定する必要があります。
- リアルタイム (オンアクセス) スキャンは常に有効にして実行する必要があります。
- AMS は、AMS によって所有または作成されていないカスタムスクリプトをインスタンスで実行しないでください。(注: これを行うには、スタック管理者アクセス CT を介してスタック管理者アクセスを使用するか、[AWS Systems Manager オートメーション \(AMS SSPS\)](#) を使用します。
- Windows ホストでネットワークレベル認証 (NLA) を無効にすることはできません。
- ホストオペレーティングシステムは、設定されたパッチサイクルに従って最新のセキュリティパッチで最新である必要があります。

- AMS マネージドアカウントには、アカウントにアンマネージドインスタンスがあってはなりません。
- AMS によるインスタンスでのローカル管理者アカウントの作成は許可されません。
- EC2 のキーペアを作成しないでください。
- End of Life (EOL) として宣言されたオペレーティングシステムを使用してはならず、ベンダーまたはサードパーティーによって提供される追加のセキュリティサポートはありません。

## AMS-STD-007 - ログ記録

以下は、007 の標準コントロール - ログ記録です。

| ID  | 技術標準                                                                                                                 |
|-----|----------------------------------------------------------------------------------------------------------------------|
| 1.0 | ログタイプ                                                                                                                |
| 1.1 | OS ログ: すべてのホストは、少なくともホスト認証イベント、昇格された権限のすべての使用のためのアクセスイベント、および成功と失敗の両方を含むアクセスと権限設定に対するすべての変更のためのアクセスイベントを記録する必要があります。 |
| 1.2 | AWS CloudTrail: CloudTrail 管理イベントのログ記録を有効にし、S3 バケットにログを配信するように設定する必要があります。                                           |
| 1.3 | VPC フローログ: すべてのネットワークトラフィックログは VPC フローログを介して記録する必要があります。                                                             |
| 1.4 | Amazon S3 Server Access Logging: ログを保存する AMS が義務付ける S3 バケットでは、サーバーアクセスのログ記録が有効になっている必要があります。                         |
| 1.5 | AWS Config スナップショット: すべてのリージョンでサポートされているすべてのリソースの設定変更を記録し、設定スナップショット                                                 |

| ID   | 技術標準                                                                                                                                          |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------|
|      | ファイルを少なくとも 1 日に 1 回 S3 バケットに配信 AWS Config する必要があります。                                                                                          |
| 1.6  | Endpoint Protection System (EPS) ログ: EPS ソリューションのログ記録を有効にし、CloudWatch Logs ロググループにログを配信するように設定する必要があります。                                      |
| 1.7  | アプリケーションログ: お客様は、アプリケーションへのログ記録を有効にし、CloudWatch Logs ロググループまたは S3 バケットに保存できます。                                                                |
| 1.8  | S3 オブジェクトレベルのログ記録: お客様は S3 バケットでオブジェクトレベルのログ記録を有効にすることができます。                                                                                  |
| 1.9  | サービスログ記録: お客様は、コアサービスと同様に SSPS サービスのログを有効にして転送できます。                                                                                           |
| 1.10 | Elastic Load Balancing (Classic/Application Load Balancer/Network Load Balancer) ログ: アクセスログエントリとエラーログエントリは、AMS 2.0 マネージド S3 バケットに保存する必要があります。 |
| 2.0  | アクセスコントロール                                                                                                                                    |
| 2.1  | ログと CloudWatch Logs; ロググループを保存する AMS に必要な S3 バケットへの書き込みまたは削除アクセスがあってはなりません。                                                                   |
| 2.2  | アカウントのすべてのログへの読み取り専用アクセスが必要です。                                                                                                                |

| ID  | 技術標準                                                                     |
|-----|--------------------------------------------------------------------------|
| 2.3 | ログを保存する AMS が義務付ける S3 バケットは、バケットポリシーの原則としてサードパーティーアカウントのユーザーを許可してはいけません。 |
| 2.4 | CloudWatch Logs ロググループからのログは、承認されたセキュリティ連絡先からの明示的な承認なしに削除しないでください。       |
| 3.0 | ログの保持                                                                    |
| 3.1 | AMS が義務付ける CloudWatch Logs ロググループのログの最小保持期間は 90 日間である必要があります。            |
| 3.2 | ログを保存する AMS が義務付ける S3 バケットには、ログに 18 か月の最小保持期間が必要です。                      |
| 3.3 | AWS Backup スナップショットは、サポートされているリソースで 31 日以上保持できる必要があります。                  |
| 4.0 | 暗号化                                                                      |
| 4.1 | 暗号化は、ログを保存する AMS Teams に必要なすべての S3 バケットで有効にする必要があります。                    |
| 4.2 | 顧客アカウントから他のアカウントへのログ転送は暗号化する必要があります。                                     |
| 5.0 | 整合性                                                                      |

| ID  | 技術標準                                                                                 |
|-----|--------------------------------------------------------------------------------------|
| 5.1 | ログファイルの整合性メカニズムを有効にする必要があります。「ログファイルの検証」は、AMS チームに必要な AWS CloudTrail 証跡で設定する必要があります。 |
| 6.0 | ログ転送                                                                                 |
| 6.1 | すべてのログは、ある AMS アカウントから同じ顧客の別の AMS アカウントに転送できます。                                      |
| 6.2 | 非 AMS アカウントが同じ AMS 顧客によって所有されている場合にのみ、すべてのログを AMS から非 AMS アカウントに転送できます。              |
| 6.3 | 顧客アカウントからのログは、サードパーティーアカウント (顧客が所有していないアカウント) に転送しないでください。                           |

## AMS-STD-008 - AMS-MAD

以下は、008 - AMS-MAD の標準コントロールです。

| ID  | 技術標準                                                                                    |
|-----|-----------------------------------------------------------------------------------------|
| 1.0 | アクセス管理                                                                                  |
| 1.1 | カスタマーアカウントでマネージド AD を管理するために管理ホストにログインできるのは、インタラクティブログインとオートメーションタスクを持つ AMS 特権ユーザーのみです。 |
| 1.2 | AD 管理者には、委任管理者権限 (AMS 委任管理者グループ) のみが必要です。                                               |

| ID  | 技術標準                                                                                                                               |
|-----|------------------------------------------------------------------------------------------------------------------------------------|
| 1.3 | お客様の AD 環境 (管理ホストまたはインスタンス) にログインするエンジニアには、期限付きアクセスが必要です。                                                                          |
| 1.4 | お客様は、EC2 インスタンスで Remote Server Administrator Tools を使用して AD オブジェクトへの読み取り専用アクセスが可能です。                                               |
| 1.5 | Active Directory ユーザーまたはグループに対する管理権限は許可しないでください。                                                                                   |
| 1.6 | AWS と同じ顧客 AWS アカウント が所有するとのディレクトリ共有は、リスク通知で許可されます。                                                                                 |
| 2.0 | サービスアカウント                                                                                                                          |
| 2.1 | グループマネージドサービスアカウント (gMSA) は、標準サービスアカウントではなく、アプリケーションでサポートされている場所を使用する必要があります。                                                      |
| 2.2 | 他のすべてのサービスアカウントは、リスク承諾プロセスの後に作成する必要があります。                                                                                          |
| 2.3 | AD セキュリティグループは、お客様が明示的に要求しない限り、再利用しないでください。新しい AD グループを作成する必要があります。サービスアカウントへのアクセスをリクエストするコンピュータオブジェクトは、新しいセキュリティグループに追加する必要があります。 |
| 2.4 | gMSA サービスアカウント (複数可) は、「マネージドサービスアカウント」組織単位 (OU) の下に追加する必要があります。                                                                   |

| ID  | 技術標準                                                                                                                                          |
|-----|-----------------------------------------------------------------------------------------------------------------------------------------------|
| 2.5 | gMSA 以外のサービスアカウント (複数可) は、「Users→Service Accounts」OU の下に追加する必要があります。                                                                          |
| 3.0 | グループポリシーオブジェクト (GPO)                                                                                                                          |
| 3.1 | 「Windows 設定 > セキュリティ設定」 GPO の設定は、アカウントのセキュリティ体制を現在の状態から何らかの方法で低下させる場合は変更しないでください。                                                             |
| 3.2 | MALZ では、GPO の作成をリクエストするアプリケーションアカウントから送信された RFCs は、GPO をアプリケーションアカウントに対応する OU にリンクする必要があります。すべてのアカウントに影響する GPOs は、共有サービスアカウントからのものである必要があります。 |
| 3.3 | デフォルトの RDP アイドルセッションタイムアウトは、アクティブディレクトリドメイン内のすべてのサーバーで 15 分に設定する必要があります。                                                                      |
| 4.0 | Active Directory の信頼                                                                                                                          |
| 4.1 | 条件付きフォワーダーの IPs が DX、VPC ピア、または VPN 経由で VPC にルーティングされている場合、一方向アウトバウンド信頼 (AMS がホストするディレクトリからカスタマーディレクトリへ) が許可されます。                             |
| 5.0 | その他                                                                                                                                           |

| ID  | 技術標準                                                                                 |
|-----|--------------------------------------------------------------------------------------|
| 5.1 | ログファイルの整合性メカニズムを有効にする必要があります。「ログファイルの検証」は、AMS チームに必要な AWS CloudTrail 証跡で設定する必要があります。 |
| 6.0 | ログ転送                                                                                 |
| 6.1 | 顧客ユーザー、グループ、コンピュータオブジェクト、OU、またはその他のエンティティは、AMS 命名規則に従って AMS 命名規則を使用してはなりません。         |
| 6.2 | すべての OUs は AMS によって管理される必要があります。                                                     |

## AMS-STD-009 - その他

以下は、009 - Miscellaneous の標準コントロールです。

- リソース、オブジェクト、データベース、またはファイルシステムで暗号化が有効になっている場合は、無効にしないでください。

## 環境に高い、または非常に高いセキュリティリスクをもたらす変更

以下の変更により、環境のセキュリティリスクが高くなるか、非常に高くなります。

### AWS Identity and Access Management

- High\_Risk-IAM-001: ルートアカウントのアクセスキーを作成する
- High\_Risk-IAM-002: 追加アクセスを許可する SCP ポリシーの変更
- High\_Risk-IAM-003: AMS インフラストラクチャを破損する可能性のある SCP ポリシーの変更
- High\_Risk-IAM-004: 顧客アカウントのインフラストラクチャ変更アクセス許可 (書き込み、アクセス許可管理、またはタグ付け) を持つロール/ユーザーの作成
- High\_Risk-IAM-005: AMS アカウントとサードパーティーアカウント (顧客が所有していない) 間の IAM ロール信頼ポリシー



- High\_Risk-IAM-006: サードパーティーアカウントによって AMS アカウントから任意の KMS キーにアクセスするためのクロスアカウントポリシー )
- High\_Risk-IAM-007: データを保存できる AMS カスタマー S3 バケットまたはリソース (Amazon RDS、Amazon DynamoDB、Amazon Redshift など) にアクセスするためのサードパーティーアカウントのクロスアカウントポリシー
- High\_Risk-IAM-008: ユーザーアカウントのインフラストラクチャ変更アクセス許可を持つ IAM アクセス許可を割り当てる
- High\_Risk-IAM-009: アカウント内のすべての S3 バケットの一覧表示と読み取りを許可する
- High\_Risk-IAM-010: 読み取り/書き込みアクセス許可を持つ自動 IAM プロビジョニング

## ネットワークセキュリティ

- High\_Risk-NET-001: インターネットからの Open OS 管理ポート SSH/22 または SSH/2222 (SFTP/2222 ではない )、TELNET/23、RDP/3389、WinRM/5985-5986、VNC/5900-5901 TS/CITRIX/1494 または 1604、LDAP/389 または 636、NETBIOS/137-139
- High\_Risk-NET-002: データベース管理ポート  
MySQL/3306、PostgreSQL/5432、Oracle/1521、MSSQL/1433、またはインターネットからの管理カスタマーポートを開く
- High\_Risk-NET-003: 任意のコンピューティングリソースでアプリケーションポート  
HTTP/80、HTTPS/8443、HTTPS/443 を直接開きます。例えば、インターネットからの EC2 インスタンス、ECS/EKS/Fargate コンテナなど
- High\_Risk-NET-004: AMS インフラストラクチャへのアクセスを制御するセキュリティグループへの変更
- High\_Risk-NET-006: サードパーティーアカウントとの VPC ピアリング (顧客が所有していない )
- High\_Risk-NET-007: カスタマーファイアウォールをすべての AMS トラフィックの出力ポイントとして追加する
- High\_Risk-NET-008: サードパーティーアカウントとの Transit Gateway アタッチメントは許可されていません
- High\_Risk-S3-001: S3 バケットでパブリックアクセスをプロビジョニングまたは有効にする

## ログ記録

- High\_Risk-LOG-001: CloudTrail を無効にします。 (Ops Site Manager の承認が必要 )
- High\_Risk-LOG-002: VPC フローログを無効にします。 (Ops Site Manager の承認が必要 )

- High\_Risk-LOG-003: AMS マネージドアカウントからサードパーティーアカウント (お客様が所有していない) への任意の方法 (S3 イベント通知、SIEM エージェントプル、SIEM エージェントプッシュなど) によるログ転送
- High\_Risk-LOG-004: CloudTrail に非 AMS 証跡を使用する

## ホストセキュリティ

- High\_Risk-HOST-001: 何らかの理由でアカウントのエンドポイントセキュリティを無効にします。( Ops Site Manager の承認が必要 )
- High\_Risk-HOST-002: リソースまたはアカウントレベルでパッチ適用を無効にします。
- High\_Risk-HOST-003: アカウントにアンマネージド EC2 インスタンスをデプロイします。
- High\_Risk-HOST-004: 顧客が提供するカスタムスクリプトを実行する。
- High\_Risk-HOST-005: インスタンスでのローカル管理者アカウントの作成。
- High\_Risk-HOST-006: Trend Micro EPS ファイルタイプ/拡張スキャンの除外、またはエンドポイントでのマルウェア保護の無効化。

### Note

リスクの承諾は、侵入テスト、脆弱性スキャン、またはプロアクティブアクションを必要とするイベント/既知のパフォーマンス問題に影響を与えるサービスに関連する EPS マルウェア対策の除外または GuardDuty 抑制ルールには必要ありません。このような状況では、リスク通知で十分です。

- High\_Risk-HOST-007: EC2 の KeyPair を作成する
- High\_Risk-HOST-008: EC2 でエンドポイントセキュリティを無効にする
- High\_Risk-HOST-009: End of Life (EOL) OS を使用するアカウント

## Miscellaneous

- High\_Risk-ENC-001: 有効な場合、任意のリソースで暗号化を無効にする

## マネージド Active Directory

- High\_Risk-AD-001: アクティブなディレクターユーザーまたはグループに管理者権限を付与する
- High\_Risk-AD-002: アカウントのセキュリティ体制を軽減できる GPO ポリシー

# AMS Advanced での継続的な管理

継続性管理の一環として、AWS Managed Services (AMS) は AWS Backup を使用したネイティブサービスへの自動アクセスを提供します AWS。これにより、Amazon EBS、Amazon EC2、Amazon RDS、Amazon EFS などをサポートするサービスへのアクセスが容易になります。

詳細については、[AWS Backup 「: 仕組み」](#) を参照してください。

## トピック

- [継続性管理とは](#)
- [継続性管理の仕組み](#)
- [ディザスタリカバリレスポンス](#)
- [ディザスタリカバリ計画](#)

## 継続性管理とは

継続性管理は、AMS がアカウントのバックアップとスナップショットを提供するために使用するプロセスです。

AMS は、バックアップジョブとプランの作成と管理に使用する変更タイプ AWS Backup を通じてへのアクセスを提供します。

## 継続性管理の仕組み

AMS は継続性管理 [AWS Backup](#) に を使用します。

AMS AWS Backup で の使用を開始する場合：

1. オンデマンドバックアップを実行する
2. バックアッププランを作成する (オプション、AMS はデフォルトのバックアッププランを提供します )
3. デフォルトの AMS バックアップポールドを使用する (オプション )
4. バックアッププランと復旧ポイントの管理 (実行、絞り込み、削除など )

# AMS バックアッププラン

バックアッププランは、RDS データベース、EBS ボリューム、DynamoDB テーブル、EFS ファイルシステムなど、サポートされている AWS リソースをバックアップするタイミングと方法を定義するポリシー式です。スケジューリングポリシーと保持ポリシーは、カスタムバックアッププランによって管理されます。カスタムバックアッププランは、AMS Advanced で変更タイプ (CT) を使用するか、AMS Accelerate AWS Backup でを使用して作成できます。タグを使用してバックアッププランにリソースを割り当て、定義されたバックアッププランに従って、割り当てられたリソースのバックアップ AWS Backup を自動的にバックアップして保持します。さまざまなバックアップ要件を持つワークロードがある場合は、複数のバックアッププランを作成できます。

バックアッププランには、スケジュールと保持期間などの詳細を定義する最大 6 つのバックアップルールを含めることができます。バックアップスケジュールは、バックアップジョブ AWS Backup を開始するタイミングとバックアップを作成する頻度を決定します。時間単位、日単位、週単位、または月単位の頻度を選択できます。削除日数の設定により、スナップショットが自動的に削除されるまでの保存日数が決まります。

## Note

AMS Advanced: レガシー AMS バックアップシステムから移行する場合、AMS は下位互換性のためのデフォルトのバックアッププランを作成します。このシナリオのキーと値のペアは Backup:True です。下位互換性をサポートするために、ここでの値は大文字と小文字を区別しないため、Backup:True または Backup:TRUE はすべて有効なタグです。他のすべてのキーと値のペアでは、大文字と小文字が区別されます。

AWS Backup は EBS ボリュームレベルまたは Amazon EC2 インスタンスレベルで動作できますが、バックアップが競合する競合状態につながる可能性があるため、両方を同時に実行することはできません。

## デフォルトのバックアッププラン、マルチアカウントランディングゾーン

新しいアカウント作成 RFC 中、AMS は、ワークロードを保護するために、アカウントレベルで包括的なデフォルトバックアッププランがあることを確認します。次のセクションに示すように、必須フィールドの値はデフォルトで設定されます。

### デフォルトの AMS バックアッププラン

default-backup-plan

## タグキー: Backup

タグ値: True

```
RuleForDailyBackups schedule expression: cron(30 23 ? * *) (a daily backup for 23:30
UTC time)
RuleForDailyBackups delete after days: 31 days
RuleForWeeklyBackups schedule expression: cron(30 23 ? * 7 *) (a weekly backup for
23:30 UTC time only on Saturday)
RuleForWeeklyBackups delete after weeks: 6 weeks
RuleForMonthlyBackups schedule expression: cron(30 23 * ? *) (a monthly backup for
23:30 UTC time on day 1 of the month)
RuleForMonthlyBackups delete after weeks: 26 weeks
RuleForYearlyBackups schedule expression: cron(30 23 1 1 ? *) (a yearly backup for
23:30 UTC time on day 1 of the month, only in January)
RuleForYearlyBackups delete after years: 2 years
```

| デフォルトの AMS バックアッププラン | 開始時刻                                        | Retention |
|----------------------|---------------------------------------------|-----------|
| hourly backup        | N/A                                         | N/A       |
| daily backup         | daily 11:30PM UTC                           | 7 days    |
| weekly backup        | weekly 11:30PM UTC, only on Saturday        | 4 weeks   |
| monthly backup       | monthly 11:30 PM UTC, on day 1 of the month | 26 weeks  |
| yearly backup        | 11:30 PM UTC, on day 1 of the month         | 2 years   |

### 拡張デフォルト AMS バックアッププラン

このプランは、ランサムウェア攻撃から保護するための AWS Backup ベストプラクティスの設計図です。毎日、毎週、毎月、毎年 of のバックアップ戦略を実装します。AWS Backup [継続的なバックアップ](#)は、[サポートされているリソース](#)の最大保持期間 (31 日間) で有効になります。

ams-enhanced-default-backup-plan

タグキー: backup-orchestrator-enhanced

タグ値: true

```
RuleForDailyBackups schedule expression: cron(0 0 4 ? * * ) (a daily backup for 04:00
  UTC time)
RuleForDailyBackups delete after days: 31 days
RuleForDailyBackups continuous backup: true
RuleForWeeklyBackups schedule expression: cron(0 0 2 ? * 7) (a weekly backup for 02:00
  UTC time only on Saturday)
RuleForWeeklyBackups delete after weeks: 6 weeks
RuleForMonthlyBackups schedule expression: cron(0 2 1 * ? *) (a monthly backup for
  02:00 UTC time on day 1 of the month)
RuleForMonthlyBackups delete after weeks: 26 weeks
RuleForYearlyBackups schedule expression: cron(0 2 1 1 ? *) (a yearly backup for 02:00
  UTC time on day 1 of the month, only in January)
RuleForYearlyBackups delete after years: 2 years
```

| 拡張 AMS バックアッププラン | 開始時刻                       | Retention |
|------------------|----------------------------|-----------|
| hourly backup    | N/A                        | N/A       |
| daily backup     | daily 4:00 UTC             | 31 days   |
| weekly backup    | Saturday, 2:00 UTC         | 6 weeks   |
| monthly backup   | 1st of the month, 2:00 UTC | 26 weeks  |
| yearly backup    | Jan 1st, 2:00 UTC          | 2 years   |

## 機密性の高い AMS バックアッププラン

このプランは、データ機密性の高いアプリケーションのランサムウェア攻撃から保護するための AWS Backup のベストプラクティスの設計図です。時間単位、日単位、週単位、月単位、年単位のバックアップ戦略を実装します。AWS Backup [の継続的バックアップ](#)は、[サポートされているリソース](#)の最大保持期間 (31 日) で有効になります。

ams-data-sensitive-backup-plan

タグキー: backup-orchestrator-data-sensitive

タグ値: true

```
RuleForHourlyBackups schedule expression: cron(0 * ? * * *) (an hourly backup at the
hour mark)
RuleForHourlyBackups delete after days: 7 days
RuleForDailyBackups schedule expression: cron(0 0 4 ? * * ) (a daily backup for 04:00
UTC time)
RuleForDailyBackups delete after days: 31 days
RuleForWeeklyBackups schedule expression: cron(0 0 2 ? * 7) (a weekly backup for 02:00
UTC time only on Saturday)
RuleForWeeklyBackups delete after weeks: 6 weeks
RuleForMonthlyBackups schedule expression: cron(0 2 1 * ? *) (a monthly backup for
02:00 UTC time on day 1 of the month)
RuleForMonthlyBackups delete after weeks: 26 weeks
RuleForYearlyBackups schedule expression: cron(0 2 1 1 ? *) (a yearly backup for 02:00
UTC time on day 1 of the month, only in January)
RuleForYearlyBackups delete after years: 2 years
```

| データ機密性の高い AMS<br>バックアッププラン | 開始時刻                       | Retention |
|----------------------------|----------------------------|-----------|
| hourly backup              | at the hour mark           | 7 days    |
| daily backup               | daily 4:00 UTC             | 31 days   |
| weekly backup              | Saturday, 2:00 UTC         | 6 weeks   |
| monthly backup             | 1st of the month, 2:00 UTC | 26 weeks  |
| yearly backup              | Jan 1st, 2:00 UTC          | 2 years   |

## AMS バックアップポールド

AWS Backup は、スナップショットをポールドと呼ばれる論理ストレージユニットに整理します。

タグを使用して、バックアップポールド通知を個々のポールドレベルで制御できます。タグを追加AMSNotificationOptOutし、特定のポールドTrueの値を に設定することで、特定のポールドの通知をオプトアウトできます。ポールドからの通知の取得を再開するには、 タグを削除します。

AMS バックアップのリストを表示するには、 [AWS Backup コンソール](#)を開きます。ナビゲーションペインで、バックアップポールドを選択し、次の表から AMS バックアップポールドのいずれかを選

択します。Backups セクションで、バックアップポールのすべてのバックアップのリストを表示します。編集、削除、または復元するバックアップを選択します。

## AMS バックアッププランのプール

| AMS ポール名                             | 説明                                                                                                                                                                                                                                               |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ams-automated-backups                | This vault receives all recovery points taken by the AMS Advanced default AWS Backup plan default-backup-plan.                                                                                                                                   |
| ams-automated-enhanced-backups       | This vault receives all recovery points taken by AMS Advanced enhanced default AWS Backup plan ams-enhanced-default-backup-plan.                                                                                                                 |
| ams-automated-data-sensitive-backups | This vault receives all recovery points taken by AMS Advanced AWS Backup plan ams-data-sensitive-backup-plan.                                                                                                                                    |
| ams-manual-backups                   | This is the default location for all backups from Start Backup Job RFC (ct-2hhud2lx01tq7) backup plans, if no vault name is defined.                                                                                                             |
| ams-custom-backups                   | This is the default location for the snapshots AMS takes prior to patching an instance using Patch Orchestrator or the monthly patch activities. These are automatically removed according to the AMS patch lifecycle default policy of 60 days. |

## AMS バックアップ変更タイプ

AMS には、バックアッププランを作成および使用するための複数の CTs が用意されています。

### Important

変更が失われる可能性があるため、AMS のデフォルトのバックアッププランを編集しないでください。代わりに、カスタム設定の新しいプランを作成します。



- [バックアッププラン: 作成](#)
- [バックアップジョブ: 開始](#)
- [バックアップジョブ: 停止](#)
- [復旧ポイント: 削除](#)
- [DynamoDB | バックアップから作成](#)
- [EBS ボリューム: バックアップから作成](#)
- [Amazon Elastic File System \(EFS\): バックアップから作成](#)

## AMS バックアップのモニタリングとレポート

### Important

AMS バックアップのモニタリングとレポートは、AMS がサポートされているリージョンでのみ使用できます。これらは、米国東部 (バージニア)、米国西部 (北カリフォルニア)、米国西部 (オレゴン)、米国東部 (オハイオ)、カナダ (中部)、南米 (サンパウロ)、欧州 (アイルランド)、欧州 (フランクフルト)、欧州 (ロンドン)、欧州 (パリ)、アジアパシフィック (ムンバイ)、アジアパシフィック (ソウル)、アジアパシフィック (シンガポール)、アジアパシフィック (シドニー)、アジアパシフィック (東京) です。

AMS は、リソースカバレッジとバックアップジョブのステータスに関する日次セルフサービスレポートと月次レポートを生成します。月次レポートは、月次ビジネスレビュー (MBRs)。日次バックアップレポートの詳細については、[日次バックアップレポート](#)」を参照してください。

AMS エキスパートは、を使用して設定されているすべてのバックアップタスクをモニタリングします AWS Backup。バックアップに障害が発生した場合、AMS は障害を調査し、根本原因と可能な場合は修復オプションを通知します。アラートノイズを回避するため、アカウントで多数のバックアップ障害が発生するイベント中、AMS は個々の障害について通知するのではなく、CSDM を通じてまとめて推奨事項を作成します。

AMS は、AWS サービスのスタンドアロンバックアップ機能を使用して設定されたバックアップをモニタリングしないことに注意してください。

# ディザスタリカバリレスポンス

以下のセクションで説明するオプションに加えて、AMS でディザスタリカバリ (DR) を開始するためにどのような手順を実行するかを知っておくことをお勧めします。

災害が発生し、復旧を開始する必要がある場合は、次の一般的なガイドラインに従ってください。

1. 可用性カテゴリで高優先度インシデントを開きます。AMS は会議ブリッジを開き、チームを招待します。
2. 復旧に必要なリソースのリストを把握します。
3. 復旧する必要があるターゲットランディングゾーン (LZ) (同じアカウント、異なる AZ、異なるアカウント、異なるリージョンなど) を把握します。
4. ターゲットランディングゾーン内の各リソースの復旧リクエストを送信します。既存の DR プランに従うか、次のセクションのオプション (、など[AMS での Elastic Disaster Recovery による EC2 のディザスタ保護](#)) [AMS での EBS スナップショットを使用した EC2 のディザスタ保護](#)を参照してください。
5. アプリケーションの機能を復元し、AMS サポートを使用してインフラストラクチャ関連の問題のトラブルシューティングを行います。

AMS は、このイベントの準備や、組織がこれらの質問に対応するための DR プランの作成に役立ちます。詳細については、クラウドサービスデリバリーマネージャー (CSDM) またはクラウドアーキテクト (CA) にお問い合わせください。

## ディザスタリカバリ計画

ディザスタリカバリ (DR) は、企業のビジネス継続性とコンプライアンスにとって重要なサービスです。AMS は、AMS での DR 戦略の計画、実装、維持を支援するためにお客様と提携します。

AMS ランディングゾーン (LZ) は、マルチアカウントおよびシングルアカウントであり、ほとんどの災害対策シナリオを満たす AMS インフラストラクチャコンポーネントにネイティブ、マルチ AZ、高可用性を提供します。ただし、ビジネスの地理的カバレッジによっては、リージョンの保護が必要になる場合があります。クロスリージョンの可用性と DR の場合、別のリージョンに別の AMS アカウントが必要です (これは、マルチアカウントランディングゾーンとシングルアカウントランディングゾーンの両方に必要です)。

AMS は、このブログ「[Rapidly recover mission-critical systems in a disaster](#)」で説明されている AWS DR ガイダンスに準拠しており、次の 4 つのオプションをサポートしています。

- マルチサイト (または高可用性)
- ウォームスタンバイ
- パイロットライト
- バックアップと復元

これらのオプションと AMS サポートについては、以下のセクションで説明します。

## マルチサイトまたは高可用性 (HA)

HA ソリューションは通常、クラスタリングや同期レプリケーションなど、アプリケーションの組み込み機能によって提供されます。ユーザーは Prod ノードと HA/DR ノードの両方に移動します。DNS はノードを直接、または Elastic Load Balancer (ELB) を介してポイントします。

AMS クラウドアーキテクト (CA) は、Well-Architected-Review および DR 計画の一環として連携します。

HA DR AWSは、次の図に示すように、アプリケーションおよびネイティブのサービスと機能を使用します。

DR サイトは、同じでも異なる でもかまいません AWS リージョン。

### Note

異なるリージョン (クロスリージョン) には、異なる Active Directory 環境があります。

DR (フェイルオーバー) ステップ: 自動フェイルオーバー。手動ステップは必要ありません。プライマリ LZ で障害が発生した場合、ユーザーは自動的に DR/HA ノードに再ルーティングされます。これは、DNS とアプリケーション設定の両方で実現されます。

HA DR メトリクス:

- 目標復旧時点 (RPO): <5 分
- 目標復旧時間と (RTO): <5 分
- メンテナンス: 高 (アプリケーション設定、パッチ適用、SG または ALB、証明書など、両方の環境で同期変更が必要です)。

- コスト: 高

## ウォームスタンバイ

「ウォームスタンバイ」という用語は、スケールダウンされたバージョンの環境がクラウドで実行されているディザスタリカバリ (DR) シナリオを説明するために使用されます。

データレプリケーションはアプリケーションレイヤーによって通常非同期的にオンラインインスタンスに処理されますが、残りのインスタンス (アプリケーション層やウェブ層など) はコストを節約するためにオフになる場合があります。ユーザーは本番稼働用サイトにのみ誘導されます。Elastic Load Balancer (ELB) などの他の AWS リソースも DR サイトで事前プロビジョニングされる場合があります。

AMS クラウドアーキテクト (CA) は、Well-Architected-Review および DR 計画の一環として連携します。

ウォームスタンバイ DR AWSは、次の図に示すように、アプリケーションおよびネイティブのサービスと機能を使用します。

DR サイトは、同じでも異なる でもかまいません AWS リージョン。

### Note

異なるリージョン (クロスリージョン) には、異なる Active Directory 環境があります。

DR (フェイルオーバー) ステップ:

1. データレプリケーションを中断し、DR サイトのデータインスタンスをマスターにする
2. 必要に応じてアプリケーション設定を更新する (新しい IP、サーバー名など)
3. DNS を DR サイト (ELB) にリダイレクトする
4. 必要に応じて AD の依存関係 (サービスアカウント、SPNs、GPOs など)

HA DR メトリクス:

- 目標復旧時点 (RPO): <1hr

- 目標復旧時間と (RTO): <1 時間 (インスタンス数とオーケストレーションによって異なります)
- メンテナンス: 高 (アプリケーション設定、パッチ適用、セキュリティグループ (SG) またはアプリケーションロードバランサー (ALB)、証明書など、両方の環境で同期変更が必要です)。
- コスト: 中

## パイロットライト

このディザスタリカバリ (DR) アプローチでは、限られたコアサービスのセットに対して Prod 環境の一部をレプリケートします。インフラストラクチャのごく一部は常に実行され、同時に変更可能なデータ (データベースやドキュメントなど) を同期します。一方、インフラストラクチャの他の部分はオフになり、テスト中のみ使用されます。バックアップとリカバリのアプローチとは異なり、最も重要なコア要素が DR ランディングゾーン (パイロットライト) ですでに設定され、実行されていることを確認する必要があります。

AMS クラウドアーキテクトは、Well-Architected-Review および DR 計画の一環としてお客様と協力して作業します。

パイロットライト DR は、次の図に示すように、アプリケーションおよび AWS ネイティブのサービスと機能を使用します。

DR サイトは、同じでも異なるでもかまいません AWS リージョン。

### Note

異なるリージョン (クロスリージョン) には、異なる Active Directory 環境があります。

DR (フェイルオーバー) ステップ:

1. データレプリケーションを中断し、DR サイトのデータインスタンスをマスターにする
2. オフになっているインスタンスとインフラストラクチャを起動する
3. 必要に応じてアプリケーション設定を更新する (新しい IP、サーバー名など)
4. 必要に応じてインスタンスを ELB に追加する
5. DNS を DR サイト (ELB) にリダイレクトする
6. 必要に応じて AD の依存関係 (サービスアカウント、SPNs、GPOs など)

## パイロットライト DR メトリクス:

- 目標復旧時点 (RPO): <1hr
- 目標復旧時間と (RTO): ~1 時間 (インスタンス数とオーケストレーションによって異なります)
- メンテナンス: 中
- コスト: 中

## バックアップと復元

このシンプルで低コストのディザスタリカバリ (DR) アプローチは、災害からの復旧時に使用するために、データとアプリケーションをどこからでも DR ランディングゾーンにバックアップします。

AMS Cloud Architect は、バックアップと DR の計画の一環としてユーザーと連携します。

バックアップと復元 DR は、次の図に示すように、AMS 自動ツールとプロセスを使用します。

次の 2 つのバックアップ方法とレプリケーション方法を使用できます。

- EBS スナップショット (目標復旧時点 (RPO) > 1hr)、 「EBS」と呼ばれる
- AWS Elastic Disaster Recovery (目標復旧時点 (RPO) ~ 0.25 時間 ) 、 「DRS」と呼ばれる

DR サイトは、同じ または別の にあることができます AWS リージョン。

### Note

別のリージョン (クロスリージョン) には、別の Active Directory 環境があります。

## DR (フェイルオーバー) ステップ:

1. スナップショットからインスタンスを復元する (プレースホルダーインスタンスを最初に使用して 2 ステップのプロセス)
2. アプリケーション設定を更新する (新しい IP、サーバー名など)
3. 必要に応じて他のインフラストラクチャを設定する (SG、ELB など)
4. DNS を DR サイト (ELB) にリダイレクトする

5. 必要に応じて AD の依存関係を更新または復元する (サービスアカウント、サービスプリンシパル名 (SPNs)、グループポリシーオブジェクト (GPOs) など)

DR メトリクスのバックアップと復元:

- 目標復旧時点 (RPO): >1 時間または ~0.25 時間 (選択したソリューションによって異なります - EBS または DRE)
- 目標復旧時間と (RTO): ~1 時間 (インスタンス数とオーケストレーションによって異なります)
- メンテナンス: 高 (アプリケーション設定、パッチ適用、セキュリティグループまたはアプリケーションロードバランサー、証明書など、両方の環境で同期変更が必要です。)
- コスト: 中

## AMS での EBS スナップショットを使用した EC2 のディザスタ保護

前提条件:

- AMS Prod Landing Zone (ソース)
- AMS DR ランディングゾーン (DR ターゲット)
- EC2 インスタンスで EBS スナップショットが有効になっている (AWS Backup)

スナップショットレプリケーションソリューション:

- クロス AZ: 該当なし - EBS スナップショットは、リージョン内で設計上高可用性です
- クロスリージョン: AWS Backup

次の図は、AMS 上の EBS スナップショットからの EC2 復元プロセスを示しています。

AMS での EC2 DR ステップ:

1. RFC をレイズして、EBS スナップショットをターゲットアカウントと共有します (クロスリージョン DR に必要)。

: 管理、アドバンスドスタックコンポーネント、EBS スナップショット、共有

2. 送信先サブネット (DR サイトサブネット) にプレースホルダー EC2 AMS スタックを作成します。お客様がセキュリティグループと他の (ELB へのインスタンスの追加など) を割り当てるス

テップを同じスタックに組み合わせることができるため、CFN 取り込みを使用してスタックを作成することをお勧めします。

変更タイプ: CloudFormation テンプレートからのデプロイ、取り込み、スタック、作成

### 3. RFC をレイズして EC2 スタックボリュームの復元を実行します。

変更タイプ: 管理、アドバンスドスタックコンポーネント、EC2 インスタンススタック、ボリュームの復元。

CT は、ステップ 1 で共有されたスナップショットからボリュームを復元し、ステップ 2 で作成されたプレースホルダーインスタンスにアタッチします。

ボリューム復元 CT 機能:

- プレースホルダーインスタンスをシャットダウンする
- スナップショットからボリュームを復元する
- ボリュームをスワップアウトする
- インスタンスを起動する
- 古いドメインを残す
- ホスト名の変更
- 再起動します。AMS ブートストラップスクリプトは、起動時にインスタンスをターゲット (DR) ドメインに結合します。

ボリューム復元 CT 入力:

- InstanceId (プレースホルダーインスタンス ID)
- RootDeviceSnapshotId、復元されたルートボリュームの EBS スナップショット
- EC2 インスタンスで復元されたすべてのボリュームを暗号化するための KMSKeyId、KMS キー識別子、または ARN
- DeviceNames、最大 25 (オプション)
- SnapshotIds、最大 25 (オプション)。復元するボリュームのスナップショットのリスト

## AMS での Elastic Disaster Recovery による EC2 のディザスタ保護

前提条件:



- AMS Prod Landing Zone (ソース)
- AMS DR ランディングゾーン (DR ターゲット)
- まず、使用する予定のすべての の Elastic Disaster Recovery AWS リージョン サービスを初期化する必要があります。

Elastic Disaster Recovery コンソールにアクセスするための IAM ロールを DR ランディングゾーン (LZ) に作成します。

- 重要: SSM ドキュメントは DRS 内で起動後アクションとして作成されます。このアクションは、PostLaunch 設定のすべてのサーバーで有効にする必要があります。
- 送信先 (プレースホルダー) インスタンスには、タグキー「AWS:DRS」  
値:「AllowLaunchingIntoThisInstance」が必要です。プレースホルダーインスタンスは停止状態である必要があります。それ以外の場合、AMS は起動設定でプレースホルダーインスタンスを選択できず、Elastic Disaster Recovery はプレースホルダーインスタンスの上に復元できません。

AMS での EC2 の Elastic Disaster Recovery のセットアップと復元プロセスの図については、[AWS Elastic Disaster Recovery \(AWS DRS\) の一般的なアーキテクチャ](#)を参照してください。

AMS での Elastic Disaster Recovery を使用した EC2 DR ステップ:

1. 適切なタグを使用して、送信先サブネット (DR サイトサブネット) にプレースホルダー EC2 AMS スタックを作成します。詳細については、前のセクションを参照してください。セキュリティグループの割り当てと、同じスタック内のインスタンス、EBS ボリューム、およびその他の (ELB へのインスタンスの追加など) タグ付けのステップを組み合わせることができるため、CFN 取り込みを使用してスタックを作成することをお勧めします。

変更タイプ: CloudFormation テンプレートからのデプロイ、取り込み、スタック、作成

2. プレースホルダーインスタンスを停止します。

変更タイプ: 管理、高度なスタックコンポーネント、EC2 インスタンス、停止

3. ステップ 1 で完了していない場合は、プレースホルダーインスタンスとその EBS ボリュームにキー「AWS:DRS」、値:「AllowLaunchingIntoThisInstance」をタグ付けします。

変更タイプ: 管理、高度なスタックコンポーネント、タグ、更新。

4. ステップ 1 のプレースホルダーインスタンスを、インスタンス ID への起動、ソースサーバーの DRS 起動設定のターゲットとして使用します。ソースサーバーの Elastic Disaster Recovery コンソールからインスタンス復旧ドリルを開始します。

 Note

プレースホルダーインスタンスボリュームはアカウントに保持されます。これらのボリュームを削除するには、ディザスタリカバリオペレーションの最後に Management | Advanced stack components | EBS Volume | Delete change type (ct-3e3h8u0sp5z80) を送信します。

## Elastic Disaster Recovery の復元ワークフロー:

- ターゲット (プレースホルダー) インスタンスは停止状態である必要があります
- ボリュームをスワップアウトし、ソース (プレースホルダー) ルートボリュームを削除する
- インスタンスを起動する
- 起動後アクションを実行して、次の項目を完了します。
  - SSM エージェントをアクティブ化します。
  - ボリュームをスワップアウトし、ソース (プレースホルダー) ルートボリュームを削除します。
  - インスタンスを起動する
- PostLaunchScript SSM ドキュメントを実行します。このドキュメントでは以下を実行します。
  1. 古いドメインを離れます。
  2. ホスト名を変更します。
  3. 再起動します。AMS ブートストラップスクリプトは、起動時にインスタンスをターゲット (DR) ドメインに結合します。

# AMS でのパッチ管理

## トピック

- [AMS パッチオーケストレーター: タグベースのパッチ適用モデル](#)
- [パッチオーケストレーターの使用](#)
- [オンデマンドパッチ適用](#)
- [AMS 標準パッチ適用](#)
- [サービスコミットメントのパッチ適用](#)

AMS では、パッチ管理は、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスで OS ベンダーの更新を維持するのに役立つサービスです。Amazon EC2 インスタンスにパッチを適用する頻度とプロセスをカスタマイズできます。

オンボーディング中にパッチ管理を設定し、RFC プロセスを使用して更新できます。変更管理システムとパッチ互換テンプレート (Amazon EC2、Auto Scaling グループ、HA 1 層または 2 層スタックの場合) を使用して作成されたスタックは、パッチ管理に自動的にサブスクライブされます。

AMS には、パッチオーケストレーター - タグベースのパッチ適用機能が用意されており、パッチ適用を設定できます。

パッチ適用用語の定義については、「」を参照してください[AMS の主要な用語](#)。

### Important

- スタックの作成元の AMS テンプレートがパッチ管理と互換性がある場合、スタックまたはスタックの構成要素インスタンスがパッチ管理をオプトアウトすることはできません。現在、パッチ適用は次のスタックテンプレートと互換性があります。
  - Amazon EC2 スタック | 作成、および Amazon EC2 スタック | 作成 (追加のボリュームを含む)
  - 取り込みで起動された Amazon EC2 CloudFormation インスタンス
  - Auto Scaling グループ | 作成 (グループ内の Amazon EC2 インスタンスにパッチが適用されます)
  - 高可用性 1 層スタック | 作成、および高可用性 2 層スタック | 作成
- スタックに影響する進行中のインシデントがある場合、AMS オペレーターはスケジュールされたパッチ適用を再スケジュールまたはキャンセルできます。

- デフォルトでは、特定のパッチ互換スタック内のすべてのインスタンスにインプレースでパッチが適用されます。最新パッチが適用された AMS AMI を使用して、Amazon マシンイメージ (AMI) 置換で Auto Scaling グループにパッチを適用するには、サービスリクエストを送信します。更新された AMIs は毎月アカウントと共有されます。

#### Important

マネージドノードの代替パッチリポジトリを指定できます。AMS がリクエストされたパッチ設定を実装している間は、選択したリポジトリのセキュリティを選択して検証する責任があります。また、サプライチェーンのリスクなど、これらのリポジトリを使用することによるリスクを受け入れる必要があります。

以下は、パッチ管理プロセスのセキュリティに関するベストプラクティスです。

- 信頼できる検証済みのリポジトリソースのみを使用する
- 可能であれば、デフォルトで標準 OS ベンダーリポジトリに設定されます。
- カスタムリポジトリ設定を定期的に監査する

#### Tip

AMS では、貴重なアプリケーションまたはサービスがあるインスタンスのバックアップを有効にすることをお勧めします。バックアップの有効化については、「[バックアップの管理](#)」を参照してください。

## AMS パッチオーケストレーター: タグベースのパッチ適用モデル

新しい AMS Patch Orchestrator タグベースのパッチ適用モデルにオンボーディングしている場合は、タグを使用して、1 つのインスタンスからすべてのインスタンスまで、パッチグループと呼ばれる正確なリソースセットにパッチ設定を適用できます。AMS タグの詳細については、「[タグの使用](#)」を参照してください。パッチオーケストレータータグの設定手順は、次のセクションで説明します。

パッチは、[SSM パッチウィンドウ | 作成で定義したパッチウィンドウ](#)中にインストールされます。各パッチウィンドウは、選択したスケジュールで実行され、期間が設定され、1 つのパッチグループに適用される AWS Systems Manager メンテナンスウィンドウです。明示的なパッチウィンドウの

一部ではないインスタンスには、パッチオーケストレーターにオンボードするときに定義するデフォルトのメンテナンスウィンドウ中にパッチが適用されます。

#### Important

複数のパッチメンテナンスウィンドウを同時に実行するようにスケジュールされている場合、一度に処理されるインスタンスは 1001 未満である必要があります。これは AWS Systems Manager の制限です。AMS では、50 インスタンスごとに少なくとも 1 時間を推奨しています。

デフォルトでは、ベンダーが提供するすべてのオペレーティングシステム (OS) パッチは、メンテナンスウィンドウまたはオンデマンドパッチ中にインストールされます。これはデフォルトのパッチベースラインと呼ばれます。インストールするパッチを制限する場合は、パッチベースライン作成 CTs (OSes) を参照してください。 <https://docs.aws.amazon.com/managedservices/latest/userguide/edeployment-patching-section.html> たとえば、カスタムパッチベースラインを使用して、1 つ以上のパッチグループに重要かつ重要なセキュリティ更新プログラムのみをインストールできます。

インスタンスにパッチをインストールすると、インスタンスは再起動されます。パッチ通知はパッチ適用の前後に送信され、スケジュールされた開始前 96 時間以内に追加のリマインダーが送信されます。さらに、AMS は、選択したメンテナンスウィンドウ中にインフラストラクチャ管理ツール (AWS SSM エージェントなど) に更新を適用します。

#### Important

AMS は、パッチが欠落しているインスタンスの毎月のパッチコンプライアンスレポートを廃止し、毎月のレポートを送信しません。この変更は、24 時間ごとに更新され、オンデマンドで利用でき、最新かつ詳細なデータを提供する、最近リリースされたセルフサービスの運用レポートを考慮して行われました。レポートの詳細については、「セルフサービスレポート」を参照してください。レポートの詳細については、「」を参照してください [セルフサービスレポート](#)。

通知の詳細については、「」を参照してください [パッチ通知](#)。

# パッチオーケストレーターの使用

以下の詳細を含むサービスリクエストを送信して、アカウントの AMS パッチオーケストレーターを有効にします。

- カテゴリ: その他
- 件名: パッチオーケストレーターにオンボードする
- CC E メール: このオンボーディング RFC のステータスが変更されたときに CC E メールアドレスに通知を受け取る
- 詳細: 次の情報を E メールに貼り付け、値を指定します。ThirdTagKey はオプションであることに注意してください。推奨事項と例については、次の表を参照してください。

```
Default maintenance window Schedule:  
Default Maintenance Window Schedule TimeZone:  
Default Maintenance Window Duration:  
Default Maintenance Window Cutoff:  
Default Patch Backup Retention In Days:  
Default Maintenance Window Notification Emails:  
First Tag Key:  
Second Tag Key:  
Third Tag Key:
```

次の表に、指定した値の形式と推奨事項を示します。

## パッチオーケストレーターのタグベースのパッチ設定

| パラメータの名前                 | 情報                                                                                                                                                                                                             | 推奨事項または例                                    |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------|
| デフォルトのメンテナンスウィンドウのスケジュール | <p>cron 式または rate 式形式のデフォルトのメンテナンスウィンドウのスケジュール。例えば、次のようになります。</p> <ul style="list-style-type: none"><li>• <code>cron(0 3 ? * 6L *)</code>: 毎月最終金曜日の午前 3 時</li><li>• <code>rate(7 days)</code>: 7 日ごと</li></ul> | ウィンドウを少なくとも 1 か月に 1 回、一貫した平日に実行することをお勧めします。 |

| パラメータの名前                       | 情報                                                                                                         | 推奨事項または例                                                                                               |
|--------------------------------|------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
|                                | cron 式の作成、および cron および rate 式のリソースへのリンクの詳細については、 <a href="#">「メンテナンスウィンドウの Cron および rate 式」</a> を参照してください。 |                                                                                                        |
| デフォルトのメンテナンスウィンドウのスケジュールタイムゾーン | デフォルトのメンテナンスウィンドウが実行されるタイムゾーンは、Internet Assigned Numbers Authority (IANA) 形式に基づいています。                      | 例えば、次のようになります。 <ul style="list-style-type: none"><li>• America/Los_Angeles</li><li>• その他/UTC</li></ul> |
| デフォルトのメンテナンスウィンドウの期間           | デフォルトのメンテナンスウィンドウの時間単位の期間。                                                                                 | 50 インスタンスごとに少なくとも 1 時間、カットオフには 2 時間。                                                                   |
| デフォルトのメンテナンスウィンドウのカットオフ        | 新しいパッチ適用コマンドが開始されない、デフォルトのメンテナンスウィンドウが終了する前の時間数。この間隔は、ウィンドウが終了する前にパッチ適用を完了するのに十分な時間を確保するために存在します。          | 少なくとも 2 時間。                                                                                            |
| デフォルトのパッチバックアップ保持日数 (オプション)    | インスタンスにパッチを適用する前に作成された EBS 復元ポイントを保持するデフォルトの日数。                                                            | デフォルトは 60 のままにすることをお勧めします。                                                                             |

| パラメータの名前                  | 情報                                                                            | 推奨事項または例                                                         |
|---------------------------|-------------------------------------------------------------------------------|------------------------------------------------------------------|
| デフォルトのメンテナンスウィンドウ通知 E メール | デフォルトのメンテナンスウィンドウのパッチ適用ステータスに関する通知を受け取るための 1~5 つの E メールアドレスまたはディストリビューションリスト。 | 個々の E メールではなく、グループディストリビューションリストを使用することをお勧めします。                  |
| 最初のタグキー                   | パッチグループのタグ値の作成に使用する最初のタグキー。                                                   | 例えば、AppId などです。パッチグループタグを使用して独自のパッチグループを既に定義している場合は、null を指定します。 |
| 2 番目のタグキー                 | パッチグループのタグ値の作成に使用する 2 番目のタグキー。                                                | 例えば、環境などです。パッチグループタグを使用して独自のパッチグループを既に定義している場合は、null を指定します。     |
| 3 番目のタグキー (オプション)         | パッチグループのタグ値の作成に使用するオプションの 3 番目のタグキー。                                          | 例えば、Group などです。                                                  |

新しいパッチオーケストレーターパッチ適用サービスモデルにオンボーディングすると、アカウント内で適切にタグ付けされたすべてのインスタンスは、パッチグループタグを持つパッチグループに属します。パッチオーケストレーターは、既存のパッチグループタグ、またはパッチオーケストレーターのオンボーディング中に指定した 2 つまたは 3 つの連結タグ値で構成される AMS 作成タグを使用します。たとえば、{*Tag Value 1*}-{*Tag Value 2*}-{*Tag Value 3*} です。AMS は、これらの AMS 適用パッチグループタグを 12 時間ごとに更新します。必要に応じて、タグ [更新 \(マネージドオートメーション\)](#) またはタグ [更新 \(マネージドオートメーション\)](#) の変更タイプを使用してパッチグループのタグ値を更新できます。

例えば、Amazon EC2 インスタンスに次のタグキーと値のペアがある場合です。

- AppId:MyApplication



- Environment:Production
- Group:1

オンボーディング中に、次のタグキーを指定しました。

- First Tag Key = AppId
- Second Tag Key = Environment
- Third Tag Key = Group

AMS は、次のパッチグループタグを作成し、インスタンスに適用します: Patch Group:MyApplication-Production-1。

 Note

サポートされていないオペレーティングシステムを持つインスタンス、またはメンテナンスウィンドウ中に停止されたインスタンスでは、パッチ失敗アラートは作成されません。

## パッチオーケストレーターの前提条件

パッチオーケストレーターワークフローは、System Manager Automation Document: AWSManagedServices-PatchInstanceFromMaintenanceWindow の最新バージョンによってパッチが適用された Amazon EC2 インスタンスを対象としています。

ドキュメントワークフローの一部として、実行コマンドドキュメント「AWS-RunPatchBaseline」は、パッチグループメンバーから各 Amazon EC2 インスタンスに対して実行されます。詳細については、[「AWS-RunPatchBaseline SSM ドキュメントについて」](#)を参照してください。

要件:

- AMS が提供する Amazon マシンイメージ (AMI) からデプロイされた Amazon EC2 インスタンス、または「移行パートナー移行インスタンスからのスタック」CT (ct-257p9zjk14ija) を介して AMI にデプロイされた Amazon EC2 インスタンス。
- Egress インターネット接続が有効になりました。ファイアウォール/プロキシソリューションの場合、Windows 更新エンドポイントや Linux リポジトリミラーエンドポイント、AWS システムマネージャプロキシ設定、メタデータプロキシ設定を許可する必要があります。詳細について

は、[「プロキシを使用するように SSM エージェントを設定する」](#) および [「HTTP プロキシを使用する」](#) を参照してください。

- IAM ロールの SSM サービスの最小アクセス許可に一致する IAM customer-mc-ec2-instance-profile ロール。
- 10 GB の使用可能なルートパーティションスペースをお勧めします。Linux OS の場合、/varパーティションで少なくとも 2 GB を使用できます。
- 更新のダウンロードのための有効な認証機関の使用。
- Windows Server Update Services (WSUS) -  
DisableWindowsUpdateAccess、NoWindowsUpdate、自動更新によって Windows Update プロセスのオペレーションが損なわれることはありません。

#### 検証:

- yum パッケージマネージャーを使用する Linux OS インスタンスの場合、 を実行して更新の可用性を検証できます。 #yum check-update
- Linux OS RedHat 5.7 以降、6.1 以降、および 7.0 以降では、Amazon EC2 インスタンスは「移行パートナー移行インスタンスからのスタック」CT (ct-257p9zjk14ija) を介して AMS アカウントに移行され、更新パフォーマンスについてサブスクリプションマネージャーのステータスを検証する必要があります。
- Windows OS で、Windows Server Update Services (WSUS) を有効にします。更新をスキャンまたはインストールする WSUS 機能をブロックするローカルポリシーはありません。管理者としてログインしたら、Windows Update Service コンソールから利用可能な更新のスキャンを実行して検証できます。2012R2、2016、2019 を含む Windows Server OS リリースには、ダウンロードしてインストールするためのデフォルトの Windows Update 設定があります。スキャン前に必要な設定を行うことができます。OS のそれ以降のリリースでは、このオペレーションによってインストールがトリガーされます。必要な動作を事前に設定してください。
- AWSManagedServices-CheckPatchingPrerequisites Automation document to run against Amazon EC2 instance for assessment of patch readiness」というサービスリクエストを送信して、AMS Operations チームから検証をリクエストします。

#### Note

サポートされていないオペレーティングシステムを持つインスタンス、またはメンテナンスウィンドウ中に停止されたインスタンスでは、パッチ失敗アラートは作成されません。

# パッチウィンドウ

特定のパッチグループのインスタンスには、1 つ以上のパッチウィンドウ中にパッチが適用されます。パッチウィンドウは、cron 式または rate 式として定義されたスケジュールで実行され、選択した時間間隔内にパッチ適用関連の中断を維持することを目的とした設定可能な期間があります。AMS では、組織固有のパッチ適用ルーチンに合わせて、すべてのインスタンスをまとめてカバーする複数のパッチウィンドウを作成し、デフォルトのメンテナンスウィンドウをフォールバックとして使用することをお勧めします。パッチウィンドウは、RFC 変更タイプのデプロイ | パッチ適用 | SSM パッチウィンドウ | 作成 (ct-0el2j07llrxs7) で作成されます。パッチウィンドウに含まれていないすべてのインスタンスには、オンボーディング中に作成されたデフォルトのメンテナンスウィンドウ中にパッチが適用されます。

通常、パッチウィンドウを更新して新しいインスタンスを含める必要はありません。通常、これはインスタンスタグを変更することによって行われます。たとえば、次の一連のイベントを考えてみましょう。

1. 2 つのインスタンスには、AppId:MyApplication、Environment:Production というタグが付けられます Group:1。

これにより、最初のタグキー = AppId、2 番目のタグキー = 環境、3 番目のタグキー = グループ、MyApplication-Production-1 パッチグループのパッチウィンドウが作成されると、これらのインスタンスにタグが生成されます。

2. さらに 3 つのインスタンスが作成され、AppId:MyApplication、Environment:Production、でタグ付けされます Group:1。

これにより、パッチグループ:MyApplication-Production-1 のタグが生成されます。

次のスケジュールされた実行時に 5 つのインスタンスをすべて取得するため、パッチウィンドウを変更する必要はありません。

この変更タイプの使用に関する詳細な説明とチュートリアルについては、[「SSM パッチウィンドウ | 作成」](#)を参照してください。

## パッチ通知

### Important

2025 年 2 月 1 日以降、AMS のお客様はマネージドアカウントで空のパッチメンテナンスウィンドウの通知を受信しなくなります。

サブスクライブした E メールアドレス (最大 5 つ) は、パッチメンテナンスウィンドウが開始する直前に次のような E メールを受信します。

```
Dear Customer,
The AMS Patch Maintenance Window THE_MAINTENANCE_WINDOW_NAME was started at:
  2020-02-21T12:02:18.196Z.
Details:
  Maintenance Window AccountId: YOUR_ACCOUNT_ID
  Maintenance Window Region:    YOUR_ACCOUNT_REGION
  Maintenance Window Id:        THE_MAINTENANCE_WINDOW_ID
  Maintenance Window Name:      THE_MAINTENANCE_WINDOW_NAME
  Maintenance Window Description: MaintenanceWindow for patching patch
  Group PATCH_GROUP_NAME
  Maintenance Window Patch Group: PATCH_GROUP_NAME
  Maintenance Window ExecutionId: THE_EXECUTION_ID
Targets:
  InstanceId      InstanceName      StackId
  -----
  THE_INSTANCE_ID  THE_INSTANCE_NAME  THE_STACK_NAME

A follow-up message with a detailed report is sent as soon as the maintenance window is
over.

Please raise a service request if you have any inquires about AMS Patch Orchestrator by
following this URL:
https://console.aws.amazon.com/managedservices/servicerequest/new

Kind Regards,

Amazon Web Services
Amazon Managed Services
Patch Team
```

パッチアクティビティの最後に、サブスクライブした E メールアドレスに次のような E メールが送信されます。

```

Dear Customer,
The AMS Patch Maintenance Window THE_MAINTENANCE_WINDOW_NAME ended at:
  2020-02-21T12:03:20.058Z, with status: SUCCESS.
Details:
  Maintenance Window AccountId: YOUR_ACCOUNT_ID
  Maintenance Window Region:   YOUR_ACCOUNT_REGION
  Maintenance Window Id:       THE_MAINTENANCE_WINDOW_ID
  Maintenance Window Name:     THE_MAINTENANCE_WINDOW_NAME
  Maintenance Window Description: MaintenanceWindow for patching patch
  Group PATCH_GROUP_NAME
  Maintenance Window Patch Group: PATCH_GROUP_NAME
  Maintenance Window ExecutionId: THE_EXECUTION_ID
Targets:
  RfcId                InstanceId                InstanceName                StackId
  Status
  -----
  THE_RFC_ID          THE_INSTANCE_ID          THE_INSTANCE_NAME THE_STACK_NAME
STATUS

You can view the current Patch Compliance of your Amazon EC2 Instances by following
this URL:
https://console.aws.amazon.com/systems-manager/compliance?region=YOUR\_ACCOUNT\_REGION

Please raise an Incident if an issue is impacting one of your production applications
by following this URL:
https://console.aws.amazon.com/managedservices/incident/new

Kind Regards,

Amazon Web Services
Amazon Managed Services
Patch Team

```

96 時間ごとに AMS パッチ適用システムは、その 96 時間以内に予定されているすべてのパッチマネージドメンテナンスウィンドウを識別し、その 96 時間以内のすべてのサブスクライブされた E メールアドレスにリマインダー通知を送信します。これは、ウィンドウの 1 時間前、または 96 時間全体になる可能性があります。例：

Dear Customer,

The AMS Patch Maintenance Window *THE\_MAINTENANCE\_WINDOW\_NAME* will start at:  
2020-05-06T16:35:36.523Z.

Details:

Maintenance Window AccountId: *YOUR\_ACCOUNT\_ID*  
 Maintenance Window Region: *YOUR\_ACCOUNT\_REGION*  
 Maintenance Window Id: *THE\_MAINTENANCE\_WINDOW\_ID*  
 Maintenance Window Name: *THE\_MAINTENANCE\_WINDOW\_NAME*  
 Maintenance Window Description: MaintenanceWindow for patching patch

Group *PATCH\_GROUP\_NAME*

Maintenance Window Patch Group: *PATCH\_GROUP\_NAME*  
 Maintenance Window Next Start Time: 2020-05-06T16:35:36.523Z  
 Maintenance Window Schedule: rate(24 hours)  
 Maintenance Window Timezone: *THE\_TIMEZONE*

At this time, these are the instances in the "*PATCH\_GROUP\_NAME*" Patch Group:

| InstanceId | InstanceName | StackId | InstanceState |
|------------|--------------|---------|---------------|
|------------|--------------|---------|---------------|

---

|                        |                          |                       |                 |
|------------------------|--------------------------|-----------------------|-----------------|
| <i>THE_INSTANCE_ID</i> | <i>THE_INSTANCE_NAME</i> | <i>THE_STACK_NAME</i> | running/stopped |
| <i>THE_INSTANCE_ID</i> | <i>THE_INSTANCE_NAME</i> | <i>THE_STACK_NAME</i> | running/stopped |
| <i>THE_INSTANCE_ID</i> | <i>THE_INSTANCE_NAME</i> | <i>THE_STACK_NAME</i> | running/stopped |

A notification message is sent as soon as the maintenance window starts.

You can view the current Patch Compliance of your Amazon EC2 Instances by following this URL:

[https://console.aws.amazon.com/systems-manager/compliance?region=YOUR\\_ACCOUNT\\_REGION](https://console.aws.amazon.com/systems-manager/compliance?region=YOUR_ACCOUNT_REGION)

If you would like to disable this maintenance window or you have inquires about the AMS Patch Orchestrator click on the following URL:

<https://console.aws.amazon.com/managedservices/servicerequest/new>

If you would like to delete this maintenance window, you can run the CT with id "ct-0q0bic0ywqk6c" against the stack id "stack-rctyznutkyj4tkkzq".

Kind Regards,

Amazon Web Services  
 Amazon Managed Services  
 Patch Team

## パッチベースライン

デフォルトでは、すべてのオペレーティングシステム (OS) ベンダー提供のパッチは、AMS デフォルトパッチベースラインを使用してインストールされます。インストールするパッチを制限する場合は、オプションで RFC 変更タイプデプロイ | パッチ適用 | SSM パッチベースライン | **OS** の作成 (CT ID はオペレーティングシステムによって異なります) を使用してパッチベースラインを作成できます。

これらの変更タイプの使用については、[「パッチ適用サブカテゴリ」](#)を参照してください。

## パッチオーケストレーターの予約済みタグ

パッチオーケストレーターは、変更できない次のタグも生成します。

- **AMSPatchGroup** – このタグはパッチグループのタグ値の生成に使用されます。AMSPatchGroup を変更しないでください。カスタムの「Patch Group」値を使用する場合は、「Patch Group」タグを変更できます。パッチオーケストレーターは、オンボーディング中に提供されたタグキーに基づいて AMSPatchGroup の値を生成し続けますが、カスタム値に設定されている場合、「パッチグループ」タグ値は変更されません。カスタム「パッチグループ」値の使用を停止するには、「パッチグループ」の値を AMSPatchGroup タグ値と一致するように設定できます。
- **AMSDefaultPatchGroup** – このタグは、インスタンスがデフォルトのメンテナンスウィンドウの一部であるかどうかを示し、値は True または False のいずれかです。インスタンスのパッチグループがメンテナンスウィンドウに割り当てられていない場合、この値は True に設定されます。

## オンデマンドパッチ適用

AMS には、パッチベースラインで動作する変更タイプがあり、オンデマンドでインスタンスでパッチを実行できます。これは、オンボーディング時に設定したデフォルトのベースラインか、Patch Baseline 変更タイプで設定した Patch Orchestrator Systems Manager パッチベースライン (CT ID はオペレーティングシステムによって異なります) のいずれかです。

パッチオーケストレーターの有無にかかわらず、オンデマンドパッチ適用変更タイプを使用できます。

この変更タイプの使用については、[「オンデマンドパッチ | 実行」](#)を参照してください。

**Note**

オンデマンドパッチ適用変更タイプで Auto Scaling グループの一部であるインスタンスを使用することはできません。

## AMS 標準パッチ適用

AMS は AMS 標準パッチ適用モデルを使用して既存の顧客をサポートしていますが、このモデルは新しい顧客には利用できず、AMS パッチオーケストレーターを優先して廃止されます。

AMS 標準パッチの一般的なパッチコンテンツには、サポートされているオペレーティングシステムと、サポートされているオペレーティングシステム (IIS や Apache Server など) がプリインストールされたソフトウェアのベンダー更新が含まれます。

AMS オンボーディング中に、パッチ適用の要件、ポリシー、頻度、優先パッチウィンドウを指定します。これらの設定により、インフラストラクチャのパッチ適用のためにアプリケーションを一度にすべてオフラインにする必要がなくなるため、どのインフラストラクチャにパッチを適用するかを制御できます。

**Note**

このトピックで説明するパッチ適用プロセスは、スタックにのみ適用されます。AMS インフラストラクチャには、別のプロセス中にパッチが適用されます。AWS Managed Services メンテナンスウィンドウ (またはメンテナンスウィンドウ) は、AWS Managed Services (AMS) のメンテナンスアクティビティを実行し、毎月第 2 木曜日の太平洋標準時の午後 3 時から午後 4 時まで繰り返します。AMS は、48 時間前に通知することでメンテナンスウィンドウを変更する場合があります。オンボーディング時に AMS パッチウィンドウを設定するか、毎月のパッチサービス通知を承認または拒否します。

AMS は、マネージド Amazon EC2 インスタンスを定期的にスキャンして、オペレーティングシステムの更新機能を通じて利用可能な更新を確認します。また、環境でサポートされている AMS ベースの Amazon マシンイメージ (AMIs) を定期的に更新しています。

検証後、AMS AMI リリースはすべての AMS アカウントと共有されます。[DescribeImages](#) Amazon EC2 API コールまたは Amazon EC2 EC2 コンソールを使用して、使用可能な AWS AMI リリースを表示できます。使用可能な AMS AMIs 「」を参照してください[AMI IDs、AMS の検索](#)。



AMS は、ユーザーからリクエストされた場合にのみアドホックパッチ適用スケジュールを実行します。以前は、AMS は通知を送信します。現在、通知は送信されません。

#### Note

デフォルトでは、AMS は Systems Manager を使用してパッチを適用し、パッケージマネージャー (Linux) または System Update サービス (Windows) がデフォルトのリポジトリをクエリして、利用可能な新しいパッケージを確認します。day-to-dayオペレーション中に、デフォルトのパッケージマネージャーを使用して Linux ホストにパッケージをインストールした場合、そのパッケージマネージャーは、そのソフトウェアの新しいパッケージが利用可能になったときにそのパッケージも受け取ります。このような場合は、パッチ適用アクションを実行して (このセクションで説明)、そのインスタンスをオプトアウトできます。

## サポートされるオペレーティングシステム

サポートされているオペレーティングシステム (x86-64)

- Amazon Linux 2023
- Amazon Linux 2 (AMS サポート終了日は 2026 年 6 月 30 日と想定)
- Oracle Linux 9.x、8.x
- Red Hat Enterprise Linux (RHEL) 9.x、8.x
- SUSE Linux Enterprise Server 15 SP6
- SUSE Linux Enterprise Server for SAP 15 SP3 以降
- Microsoft Windows Server 2025、2022、2019、2016
- Ubuntu 20.04、22.04、24.04

サポートされているオペレーティングシステム (ARM64)

- Amazon Linux 2023
- Amazon Linux 2 (AMS サポート終了日は 2026 年 6 月 30 日と想定)

## サポートされているパッチ

AWS Managed Services は、主にオペレーティングシステムレベルでのパッチ適用をサポートしています。インストールされるパッチは、オペレーティングシステムによって異なる場合があります。

**⚠ Important**

すべての更新は、インスタンスで設定された Systems Manager パッチベースラインサービスのリモートリポジトリからダウンロードされ、このトピックで後述します。パッチ適用を実行するには、インスタンスがリポジトリに接続できる必要があります。

自分で管理するパッケージを配信するリポジトリのパッチベースラインサービスをオプトアウトするには、次のコマンドを実行してリポジトリを無効にします。

```
yum-config-manager DASHDASHdisable REPOSITORY_NAME
```

次のコマンドを使用して、現在設定されているリポジトリのリストを取得します。

```
yum repolist
```

- Amazon Linux 事前設定済みリポジトリ (通常は 4 つ):

| リポジトリ ID         | リポジトリ名                               |
|------------------|--------------------------------------|
| amzn-main/latest | amzn-main-Base                       |
| amzn-updates/最新  | amzn-updates-Base                    |
| epel/x86_64      | Enterprise Linux 6 の追加パッケージ - x86_64 |
| pbis             | PBIS パッケージの更新                        |

- Red Hat Enterprise Linux の事前設定済みリポジトリ (Red Hat Enterprise Linux 7 の場合は 5 つ、Red Hat Enterprise Linux 6 の場合は 5 つ)。

| リポジトリ ID                                        | リポジトリ名                                                     |
|-------------------------------------------------|------------------------------------------------------------|
| rhui-REGION-client-config-server-7/x86_64       | Red Hat Update Infrastructure 2.0 Client Configuration Ser |
| rhui-REGION-rhel-server-releases/7Server/x86_64 | Red Hat Enterprise Linux Server 7                          |

| リポジトリ ID                                        | リポジトリ名                                             |
|-------------------------------------------------|----------------------------------------------------|
| rhui-REGION-rhel-server-releases/7Server/x86_64 | Red Hat Enterprise Linux Server 7 RH Common (RPMs) |
| epel/x86_64                                     | Enterprise Linux 7 の追加パッケージ - x86_64               |
| pbis                                            | PBIS パッケージの更新                                      |

| リポジトリ ID                           | リポジトリ名                                             |
|------------------------------------|----------------------------------------------------|
| rhui-REGION-client-config-server-6 | Red Hat 更新インフラストラクチャ 2.0                           |
| rhui-REGION-rhel-server-releases   | Red Hat Enterprise Linux Server 6 (RPMs)           |
| rhui-REGION-rhel-server-rh-common  | Red Hat Enterprise Linux Server 6 RH Common (RPMs) |
| Epel                               | Enterprise Linux 6 の追加パッケージ - x86_64               |
| pbis                               | PBIS パッケージの更新                                      |

- CentOS 7 事前設定済みリポジトリ (通常は 5 つ):

| リポジトリ ID         | リポジトリ名                               |
|------------------|--------------------------------------|
| base/7/x86_64    | CentOS-7 - ベース                       |
| updates/7/x86_64 | CentOS-7 - 更新                        |
| extras/7/x86_64  | CentOS-7 - 追加                        |
| epel/x86_64      | Enterprise Linux 7 の追加パッケージ - x86_64 |
| pbis             | PBIS パッケージの更新                        |

- Microsoft Windows Server の場合、すべての更新は、Windows Update カタログを使用するように設定された Windows Update エージェントを使用して検出およびインストールされます (Microsoft Update からの更新は含まれません)。

Microsoft Windows オペレーティングシステムでは、Patch Manager は利用可能なオペレーティングシステムのセキュリティ更新のソースとして Microsoft の cab ファイル wsusscn2.cab を使用します。このファイルには、Microsoft が発行するセキュリティ関連の更新に関する情報が含まれています。Patch Manager は、このファイルを Microsoft から定期的にダウンロードし、それを使用して Windows インスタンスで使用できるパッチのセットを更新します。このファイルに含まれている更新は、セキュリティに関連していると Microsoft が判断したもののみです。Patch Manager は、ファイル内の情報の処理に伴って、最新の更新で置き換えた前の更新を削除します。したがって、最新の更新のみが表示され、インストール可能になります。たとえば、KB4012214 が KB3135456 を置き換える場合、KB4012214 のみが Patch Manager の更新として利用可能になります。

wsusscn2.cab ファイルの詳細については、Microsoft の記事「Using [WUA to Scan for Updates Offline](#)」を参照してください。

## パッチ適用とインフラストラクチャ設計

AMS は、インフラストラクチャの設計に応じて、変更可能またはイミュータブルなさまざまなパッチ適用方法を採用しています (詳細な定義については、「」を参照してください[AMS の主要な用語](#))。

変更可能なインフラストラクチャでは、パッチ適用は、AMS オペレーションエンジニアが Amazon EC2 インスタンスに個別に更新を直接インストールする従来のインプレース方法を使用して行われます。このパッチ適用方法は、Auto Scaling グループではなく、1 つの Amazon EC2 インスタンスまたはいくつかのインスタンスを含むスタックに使用されます。このシナリオでは、インスタンスまたはスタックが基づいていた AMI を置き換えると、最初にデプロイされてからそのシステムに加えられたすべての変更が破棄されるため、は行われません。更新は実行中のシステムに適用され、アプリケーションまたはシステムの再起動により、システムのダウンタイム (スタック設定によって異なります) が発生する可能性があります。これは、ブルー/グリーン更新戦略で軽減できます。詳細については、[AWS CodeDeploy 「ブルー/グリーンデプロイの導入」](#)を参照してください。

イミュータブルインフラストラクチャでは、パッチ適用方法は AMI の置き換えです。イミュータブルインスタンスは、Auto Scaling グループ設定で指定された AMI を置き換える更新された AMI を使用して均一に更新されます。AMS リリースは、毎月、通常はパッチ火曜日の週に AMIs を更新 (つまり、パッチを適用) します。次のセクションでは、この仕組みについて説明します。

## AMS 標準パッチの仕組み

AMS は、Systems Manager Run Command サービスを使用して、インフラストラクチャのデプロイ戦略 (変更可能かイミュータブルか) に応じて、インプレースと AMI 置換の 2 つのプリンシパルパッチ適用方法を使用して、毎月定期的にスケジュールされ、必要に応じて重要なパッチを適用します。このセクションでは、AMS パッチ適用サービス、タイプ、メソッド、プロセスについて説明します。

AMS は、スケジュールが異なる 2 つのパッチタイプを定義します。

- 重要なパッチ適用: 更新は、通知の承諾後、できるだけ早く適用されます。
- 標準パッチ適用: OS ベンダーの定期的な更新と毎月の適用。

パッチは、インプレースパッチまたは AMI 置換 (リクエスト時) を通じて適用されます。

### スキヤンの更新

AMS は [Amazon EC2 Run Command Service](#) を使用して Amazon EC2 スタックに連絡し、必要なスキヤンおよびパッチ適用スクリプトをデプロイします。AMS は、サポートされているオペレーティングシステムに既にインストールされているネイティブパッケージ管理コンポーネントを使用して、Amazon EC2 スタックで必要なすべてのスキヤンおよびパッチ適用動作を実行します。Red Hat と Amazon Linux の場合、サービスは yum を使用します。Windows の場合、サービスは Windows Update エージェントを使用します。

スキヤンは、[SSM メンテナンスウィンドウ](#) と AMS のデフォルトの AWS-RunPatchBaseline ドキュメントを使用して毎日実行されます。Linux および Windows の更新リポジトリを使用して、到達可能なすべての Amazon EC2 スタックがスキヤンされます。AMS パッチ適用プロセスは、到達可能なすべての Amazon EC2 スタックを検出し、バッチプロセスでスキヤンを実行します。これにより、スキヤンの実行中に障害が発生した場合でも、スタックは常に正常な状態を維持します。その後、スキヤン結果は Amazon EC2 スタックごとに保存されます。

スタックまたはインスタンスのスキヤン結果を表示するには、スタック ID またはインスタンス ID を使用してサービスリクエストを送信します。

デフォルトの AMS パッチ適用プロセスでは、パッチの分類や重要度 (重要か標準かなど) に関係なく、使用可能なすべてのパッチをインストールします。この例外は、スタックに対して明示的に除外したパッチです (AMS で必須として定義されているパッチは除外しないでください)。

提案されたメンテナンスウィンドウの 14 日前にパッチ適用サービス通知が送信されます。これにより、提案されたパッチをテストし、承認または拒否する時間を確保できます。パッチ適用サービス

通知に返信しない場合、インスタンスにはパッチが適用されません。パッチをインストールするとき、AMS はスタックごとに変更リクエスト (RFC) を作成し、その RFC がアカウントの RFC リストに表示されます。

## AMS で設定されたメンテナンスウィンドウと通知

AMS が設定されたパッチ適用では、各アカウントには毎月のメンテナンスウィンドウがあり、アカウントのオンボーディング時に定義します。AWS Managed Servicesメンテナンスウィンドウ (またはメンテナンスウィンドウ) は、AWS Managed Services (AMS) のメンテナンスアクティビティを実行し、毎月第 2 木曜日の太平洋標準時の午後 3 時から午後 4 時まで繰り返します。AMS は、48 時間前に通知することでメンテナンスウィンドウを変更する場合があります。

パッチ適用ウィンドウは異なります。パッチ適用アウトバウンドサービスリクエスト (サービス通知とも呼ばれます) には、推奨されるパッチウィンドウが含まれています。

### Note

パッチ適用サービス通知への返信については、「」を参照してください[AMS 標準パッチ適用で実行できるアクション](#)。

パッチ適用サービス通知は、アカウントの登録されている連絡先 E メールアドレスに E メールで送信されます。通知には、応答できる AWS サポートコンソールへのリンクが含まれています。AMS サービスリクエストページを使用して通知に応答することもできます。サービス通知には以下が含まれます。

- スタックに適用される更新 IDs (CSUs、IUs、OUs) のリスト、およびリクエストした更新は、パッチ適用から除外されます (存在する場合)。
- 影響を受けるインスタンスの IDs。
- 更新が適用されるときに提案されたパッチ適用ウィンドウ。別のパッチ適用ウィンドウをリクエストできます。
- 提案されたパッチ適用を受け入れるか、追加情報を求めるリクエスト。AMS を使用すると、更新の影響をテストし、パッチ適用を承認または拒否したり、特定の更新を除外するように求める時間を確保できます。テストにさらに時間が必要で、テスト後に更新を適用する場合は、サービス通知に応答して目的を記述するか、以前の RFC の詳細に基づいて新しいパッチ RFC のサービスリクエストを送信します。サービス通知にまったく応答しない場合、パッチ適用アクションは実行されず、RFC はキャンセルされます。

サービス通知を承認すると、AMS はパッチ RFC を実行し、サービスコミットメントに従って、合意されたパッチウィンドウ内に更新を適用します。

パッチ適用が完了すると、AMS はサービスリクエストで、パッチ適用アクティビティの結果 (成功または失敗) の概要を含む通信を送信します。

## インプレースパッチ適用

インプレースパッチとは、AMS が各スタックインスタンスにログインし、パッチを適用する方法を指します。

インプレースパッチは、サポートされているオペレーティングシステムを実行している Amazon EC2 インスタンスを使用して、変更可能なインフラストラクチャで発生します。パッチ適用は、その時点までに利用可能な除外されていないすべての更新を適用します。重要なパッチがリリースされると、重要なパッチ適用プロセスが追加されます。

### 標準パッチ適用: インプレース

標準パッチ適用は、パッチサービス通知で提案されている合意済みのパッチスケジュールで行われ、重要と見なされない定期的なパッチ更新が含まれます。

提案されたパッチ適用ウィンドウの前に、通知に対する肯定的な応答により、パッチ RFC が作成され、RFC ダッシュボードに表示されます。

### 重要なパッチ適用: インプレース

OS ベンダーが重要なセキュリティ更新プログラムをリリースすると、AMS サービスコミットメントに従って、スタックごとに (アカウントの連絡先 E メールに) サービス通知を送信することで、AMS はパッチ RFC を通知します。サービス通知には、更新ごとに以下が含まれます。

- リリース日の更新
- 重要度を更新する
- 更新の詳細 (KB リファレンスなど)
- 影響を受けるスタックの IDs

通知に記載されている更新をテストし、サービス通知に返信してパッチを承認または拒否できます。通知を承認する場合は、更新をインストールするためにスタックごとに特定のパッチウィンドウを指定する必要があります。



**Note**

サービス通知への返信から 24 時間以内のパッチウィンドウは、使用可能な容量に基づいて再スケジュールされる場合があります。

10 日以内に返信しない場合、または提案されたパッチ適用を拒否した場合、パッチ適用はキャンセルされます。

許可された期間 (通知で指定) 後に更新を適用する場合は、前の通知の詳細に基づいて、新しいパッチスケジュールのサービスリクエストを送信します。

サービス通知を承認すると、AMS はサービスコミットメントに従って、指定されたパッチウィンドウ内に更新を適用します。

複数の更新の場合、サービス通知へのレスポンスで除外する更新を指定することで、パッチ適用から特定の更新を除外できます。

AMS は、各更新の結果 (成功または失敗) について、各スタックのサービス通知を送信します。

AMI によるパッチ適用の更新 (Auto Scaling グループのパッチ適用された AMIs を使用)

AMI 置き換えパッチ適用は、Auto Scaling グループに新しい Amazon EC2 インスタンスをデプロイするように設定された AMI ID を更新することにより、イミュータブルインフラストラクチャで行われます。

Amazon マシンイメージ (AMIs) は、サポートされているオペレーティングシステム用に定期的にリリースされます。オペレーティングシステムベンダーは、定期的に新しいパッチをリリースします。AMS は Amazon が提供する AMI を取得し、最新のパッチで更新してから、適切なコンポーネントを追加して AMS 環境で動作できるようにします。次に、AMI をアカウントと共有することで、すべての AMS 顧客が新しい AMS AMI を使用できるようになります。Auto Scaling グループスタックは、新しくリリースされた AMS AMIs を使用して毎月更新できます。次の図は、AMS 環境で AMIs がどのように使用されるかを示しています。

Auto Scaling グループは、Auto Scaling グループの設定された AMI に基づいてインスタンスを作成します。AMS が更新された AMIs を共有する場合、AMI 更新の管理方法に応じて、次のオプションがあります。



- インスタンスの作成後にインスタンスを自動的にカスタマイズするアプリケーションデプロイツール (UserData、CodeDeploy など) を使用している場合は、以下を実行できます。
- 最新の AMS AMI のパッチ適用サービス通知に返信するか、サービスリクエストを送信して、現在の Auto Scaling グループの設定 AMI を置き換えます。Auto Scaling グループの設定の AMI ID が置き換えられると、AMS はインスタンスのローリング更新を開始し、Auto Scaling グループインスタンスの設定 (アプリケーションのインストール、起動スクリプトなど) が新しい AMS AMI で作成された新しいインスタンスに自動的に適用されます。
- Auto Scaling グループの設定でカスタム/ゴールデン AMI を使用している場合は、次のことができます。
- 新しい AMS AMI を使用してインスタンスを作成し、インスタンスをカスタマイズして新しいゴールデン AMI を作成します。Amazon EC2 コンソールを使用して新しいゴールデン AMI を AMS と共有し、サービスリクエストを AMS に送信して、新しいカスタム AMI を使用するように Auto Scaling グループの設定を更新します。
- Amazon EC2 コンソールを使用して既存の golden AMI を AMS と共有し、AMS が golden AMI を更新するためのサービスリクエストを送信します。そのために、AMS はゴールデン AMI からインスタンスを作成し、そのインスタンスにパッチを適用して新しいゴールデン AMI を作成し、新しい AMI を使用するように Auto Scaling グループの設定を更新します。ここでの欠点は、AMS が新しいカスタム AMI が目的どおりに動作することをテストできないことです。代わりに、新しいゴールデン AMI を作成して共有し、AMS に Auto Scaling グループの更新をリクエストする前に、新しい AMI で作成されたインスタンスをテストし、すべてが正しく機能することを確認する必要があります。AMS はこのオプションを推奨しません。

## 標準パッチ適用: AMI 更新

AMS は毎月、サービスの改善と AMIs に適用される新しいパッチを含む新しい Amazon マシンイメージ (AMIs)。

### Note

新しい AMS AMIs は、更新された AWS AMI からパッチ火曜日の後に生成 AMIs。次に、AMS はそれらを利用可能にする前にテストします。新しい AMIs 合格すると、AMS は更新された AMIs を管理アカウントと共有します。

## 重要なパッチ適用: AMI の更新

必要に応じて、AMS は、前回の毎月の AMIs リリース以降にリリースされた重要なセキュリティパッチで更新された AMI を提供します。

イミュータブルインフラストラクチャへの重要なセキュリティ更新のプロセスは、イミュータブルインフラストラクチャの毎月の AMI プロセスと同じですが、新しい重要な更新のリリースに基づいて、新しい AMS AMI が通常のスケジュール (パッチ火曜日) 外で作成される点が異なります。AMS は、アカウントに定義されているサービスレベルアグリーメント (SLAs) に従って、重要なセキュリティパッチを含む新しい AMI を利用できるようにします。リクエストのみによる Auto Scaling グループの AMS 更新。サービスリクエストを使用して AMI 置換リクエストを送信します。

## AMS 標準パッチ適用の失敗

更新が失敗した場合、AMS は分析を実行して失敗の原因を理解し、分析の結果を通知します。障害が AMS に起因する場合、メンテナンスウィンドウ内にある場合は更新を再試行します。それ以外の場合、AMS は失敗したインスタンスの更新に関するサービス通知を作成し、指示を待ちます。

システムに起因する障害については、新しいパッチ RFC を使用してサービスリクエストを送信して、インスタンスを更新できます。

## AMS 標準パッチ適用で実行できるアクション

新しい AMIs テストに加えて、インフラストラクチャのパッチ適用を管理するために実行できるアクションがいくつかあります。

- パッチウィンドウが許容するよりも更新のテストに時間がかかった場合は、サービスリクエストを送信して、準備が整ったときにキャンセルされた更新を AMS に適用するようにリクエストできます (元のサービス通知の詳細をベースとして使用します)。
- 更新のリスト、該当するインスタンス、および必要に応じてその他の詳細を提供するサービスリクエストを送信することで、次の自動更新ウィンドウの前に重要な更新 (IU) またはその他の更新 (OU) を適用するようにリクエストできます。この CT は自動化されていないため、スケジュールと実行に時間がかかります。適切な時間、サービスレベル目標 (SLOs) を確認します。詳細については、「[AMS サービスレベル目標 \(SLOs\)](#)」を参照してください。

さらに、既存のパッチが適用された AMS AMIs を使用してカスタム AMIs を作成できます。詳細については、「[AMI | Create](#)」を参照してください。

**Note**

AMS AMI リリースプロセスはすべての AMS のお客様のために一定の頻度で実行されるため、次のメンテナンスウィンドウの前に重要な更新やその他の更新に基づいて新しい AMS AMI をリクエストすることはできません。

## パッチ適用対象の変更/オプトアウト

AMS が設定されたパッチ適用では、パッチ適用サービス通知への応答またはサービスリクエストで、パッチ適用されるリソースを変更できます。以下の操作を行うことができます。

- スタックごと、およびオペレーティングシステムごとに、修復から除外する必要があるパッチのリストを定義します。
- 特定のパッチまたはすべてのパッチから除外する必要があるリソースのリストを定義します。
- すべてのパッチ適用から常に除外する必要があるリソースのリストを定義します。
- 特定の日と特定の時間にパッチを適用する必要があるリソースのリストを定義します (メンテナンスウィンドウを定義していない場合は適切)。

1 つ以上のパッチを除外するには、サービスリクエストを送信するか、次に示すテンプレートを使用してパッチ適用サービス通知に応答します。RFC を送信しないでください。除外するパッチ名とその理由をリクエストに含めます。次のように、この情報をサービスリクエストに含めます。

- 名前: パッチの名前。Windows パッチの場合、これは などの KB 名です KB3145384。Linux パッチの場合、これは などのパッケージ名です openssh-6.6.1p1-25.61.amzn1.x86\_64。
- 理由: パッチを除外する理由を示すコメント。
- 有効期限: 除外の有効期限が切れる日時。

除外されたパッチが既にインストールされている場合は、削除されます。

リクエストは、これらのパッチを除外するとセキュリティ上の重大なリスクが生じる場合に、オペレーターが説明します。除外されたパッチの有効期限もネゴシエートされます。合意された有効期限が切れると、除外は期限切れになり、パッチはそれ以降のパッチ適用にインストールされます。

除外リストのパッチは、必要に応じてスキャン結果で返されます。

**Note**

Windows とは異なり、Linux パッチはバージョン固有です。除外されたパッチの新しいバージョンは自動的に除外されないため、この区別は重要です。その場合、Linux パッチの新しいバージョンを除外するように AMS に通知するのはお客様の責任です。

## パッチサービス通知返信テンプレート

インスタンスでパッチを適用するには、指定された形式を使用してパッチ適用サービス通知に返信する必要があります。AMS でメンテナンスウィンドウをまだ設定していない場合は、これを行う必要があります。

サービス通知に返信するときは、指定された形式を使用します。

メンテナンスウィンドウが設定されていない場合は、次のようにパッチを適用するタイミングをお知らせください。

| UTC        | StartTime | StackId            | InstanceId (Optional) |
|------------|-----------|--------------------|-----------------------|
| 2019-04-01 | 15:00     | stack-123456789012 | i-1234566789          |
| 2019-04-01 | 15:00     | stack-123456789013 | i-1234566784          |
| 2019-04-01 | 15:00     | stack-123456789014 | i-1234566783          |
| 2019-04-01 | 15:00     | stack-123456789015 | i-1234566782          |

メンテナンスウィンドウが設定されていて、特定のリソースを特定のパッチから除外する場合は、次の形式を使用します。

| StackId            | InstanceId (Optional) | Exclude Patches |
|--------------------|-----------------------|-----------------|
| stack-123456789012 | i-1234566789          | <i>PATCH</i>    |
| stack-123456789013 | i-1234566784          | <i>PATCH</i>    |
| stack-123456789014 | i-1234566783          | <i>PATCH</i>    |
| stack-123456789015 | i-1234566782          | <i>PATCH</i>    |

メンテナンスウィンドウが設定されていて、特定のリソースを常にすべてのパッチ適用から除外する場合は、次の形式を使用します。

| StackId            | InstanceId (Optional) | Exclude Patches |
|--------------------|-----------------------|-----------------|
| stack-123456789012 | i-1234566789          | ALL             |
| stack-123456789015 | i-1234566782          | ALL             |

## パッチ適用の準備

自動パッチ適用のために環境を準備するには、以下をお勧めします。

- パッチを適用するすべてのインスタンスの完全なインベントリがあることを確認してください。
- Continuity of Business 戦略の一環として、リソースが定期的にバックアップされていることを確認します。追加のバックアップはパッチシーケンスの一部として作成され、設定されたパッチオーケストレーターの保持ポリシーに従って自動的に削除されます (デフォルトは 60 日)。
- 関連するすべてのライセンスが最新であることを確認します。
- スタックメンテナンスウィンドウを変更してパッチをずらし、テストスタックが本稼働スタックの前にパッチされるようにします。これにより、パッチ適用によるエラーはテストスタックで検出され、本稼働スタックにパッチを適用する前に特定できます。

## パッチ設定の表示

現在のパッチ適用設定を確認するには、以下を実行します。

- クエリを使用して AMS にサービスリクエストを送信します。
- パッチサービス通知を待ちます。パッチ適用通知では、適用するすべてのパッチとパッチ適用するインスタンスが通知され、パッチウィンドウも提案されます。

サービスリクエストを送信して、以下を変更できます。

- スキャン間隔: このスタックのインスタンスで実行されるコンプライアンススキャン間の分単位の時間。

デフォルトは 240 (4 時間) です。

- NotificationWindow: スケジュールされた変更 (パッチ) のどれだけ前 (分単位) に通知を送信するか。

デフォルトは 10080 (7 日間) です。

## AMS 標準パッチ適用FAQs

このセクションでは、よくある質問への回答を提供します。

- Q: グローバルにパッチ適用をオプトアウトするにはどうすればよいですか？

A: パッチ適用をグローバルにオプトアウトするには、サービスリクエストを提出します。AMS 必須パッチをオプトアウトすることはできません。脆弱性をレポートできるように、すべてのスタックは引き続きスキャンされます。

- Q: 特定のスタックをパッチから除外するにはどうすればよいですか？

A: 特定のスタックをパッチ適用から完全に除外するには、サービスリクエストを送信します。特定のパッチサイクルから特定のスタックを除外するには、除外するスタックのリストを使用して、次のパッチ適用通知に応答します。詳細については、「[パッチ適用対象の変更/オプトアウト](#)」を参照してください。必須パッチはオプトアウトできないことに注意してください。

- Q: パッチ適用サービス通知を承認しない場合どうなりますか？

A: 標準のパッチ適用サービスリクエストを承認するには 14 日間、重要なパッチ適用通知を承認するには 10 日間かかります。期間内にサービスリクエストを承認しない場合、サービスコミットメントは無効になり、パッチは適用されません。必須のパッチ適用の場合、サービスリクエストへの応答に関係なくパッチが適用されます。

- Q: 特定のパッチとパッケージをインストールから除外するにはどうすればよいですか？

A: 特定のパッチまたはパッケージを完全に除外するには、サービスリクエストを送信します。特定のパッチまたはパッケージを特定のパッチサイクルから除外するには、除外するパッチまたはパッケージのリストを含む次のパッチ適用通知に応答します。詳細については、「[パッチ適用対象の変更/オプトアウト](#)」を参照してください。必須パッチはオプトアウトできないことに注意してください。

- Q: パッチ適用の結果としてシステムに障害が発生した場合はどうなりますか？

A: AMS は各システムをモニタリングします。AMS は、スタックとインスタンスごとに各更新の結果 (成功または失敗) に関するサービス通知を送信します。障害が検出されると、AMS は調査を行い、インスタンスの復元に取り組み、AMS オペレーションエンジニアは手動でパッチを適用しようとします。詳細については、「[AMS 標準パッチ適用の失敗](#)」を参照してください。

- Q: AMS によって管理される更新は何ですか？

A: AMS は、ベンダーから AMS に通知されるオペレーティングシステムレベルの更新を管理します。詳細については、「[サポートされているパッチ](#)」を参照してください。

- Q: AMS で管理されていない更新は何ですか？

A: アプリケーションレベルの更新は AMS によって管理されません。

- Q: Auto Scaling グループはどのように更新されますか？

A: Auto Scaling グループは、Auto Scaling グループ設定の AMI 置換で更新され、ローリング更新がプリフォームされます。ローリング更新では、パッチ適用設定の HealthyHostThreshold 設定が観察されます。これにより、パッチ適用中にスタック内でアクティブに維持する必要がある Amazon EC2 インスタンスの数が決まります。詳細については、「[AMI によるパッチ適用の更新 \(Auto Scaling グループのパッチ適用された AMIs を使用\)](#)」を参照してください。

- Q: 通常のサイクル外で更新をインストールするにはどうすればよいですか？

A: 通常のパッチ適用スケジュール外でインストールする OS レベルの更新については、受信したパッチ適用通知を使用してサービスリクエストを送信します。これは、提案されたパッチのテストに 21 日 (標準パッチの場合) または 14 日 (重要なパッチの場合) 以上かかった場合に発生する可能性があります。Out-of-band パッチ適用は、スタンドアロン Amazon EC2 インスタンスに対してインプレースで実行できます。

- Q: 新しくデプロイされたスタックまたはインスタンスにパッチを適用する方法を教えてください。

A: 新しい Amazon EC2 スタックインスタンスまたは Auto Scaling グループを作成するときは、常に最新の AMS AMI を指定する必要があります。この AMS AMI にはすでに最新のパッチが付けられています。変更可能なインフラストラクチャの場合、インラインパッチ適用はスタックがデプロイされるとすぐに実行する必要があります。



## サービスコミットメントのパッチ適用

インフラストラクチャのデプロイのタイプと更新の重要性に基づいて、変更可能およびイミュータブルインフラストラクチャの重要なセキュリティ更新と、変更可能およびイミュータブルインフラストラクチャの重要な更新に関するサービスコミットメントを提供します。

### 標準パッチ適用

これらは、標準パッチ適用の AMS サービスコミットメントです。

標準パッチ適用、変更可能なインフラストラクチャ (インプレースパッチ適用)

| イベント/アクション                                                                                                                                                                                                                                                          | サービスコミットメントの測定                                             |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|
| 重要な更新は 1 か月でリリースされます。                                                                                                                                                                                                                                               | クロック開始                                                     |
| 標準パッチ通知が作成されてから 14 日後、AMS はサービス通知と各スタックの E メールを通じて、予定されているパッチ適用を通知します。サービス通知には以下が含まれます。 <ul style="list-style-type: none"><li>• スタックに適用される (必要かつ適用されない) 更新 IDs (CSUs と IUs)、およびパッチ適用から除外される更新のリスト</li><li>• 影響を受けるスタックの IDs</li><li>• 更新が適用されるメンテナンスウィンドウ</li></ul> | サービス通知が送信されると、クロックは停止します。                                  |
| 更新の影響をテストし、RFC を承認または拒否します。14 日以内に返信しない場合、またはサービス通知への応答でパッチ適用を拒否した場合、アクションは実行されません。                                                                                                                                                                                 | 14 日以内に承認または返信しない場合、保留中の変更はキャンセルされ、更新のサービスコミットメントは適用されません。 |
| テストに 14 日以上かかり、14 日後に更新を適用する場合は、以前の RFC の詳細に基づいて新しいパッチ RFC のサービスリクエストを送信します。                                                                                                                                                                                        |                                                            |



| イベント/アクション                                                                                                                                                                                                                                                                                                                                                           | サービスコミットメントの測定                                                                        |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| <p>14 日以内にサービス通知を承認すると、AMS は更新を適用します。</p> <p>サービス通知へのレスポンスで除外する更新を指定することで、RFC から特定の更新を除外することを選択できます。</p> <p>AMS は、試行された各更新の結果に関するサービス通知を送信します。サービス通知には、次の詳細が含まれます。</p> <ul style="list-style-type: none"><li>• Amazon EC2 インスタンス ID</li><li>• 更新 1 の成功/失敗: ARN a1、ARN a2...</li><li>• 更新 2 の成功/失敗: ARN b1、ARN b2...</li><li>• 更新 N 成功/失敗: ARN c1、ARN c2...</li></ul> | <p>受信から 14 日以内にサービス通知を承認すると、クロックが開始されます。更新のインストールが試行されると、クロックは停止します。</p> <p>該当なし。</p> |
| <p>更新に失敗した場合、AMS は分析を実行して失敗の原因を理解し、分析の結果を通知します。障害が AMS に起因する場合、AMS はメンテナンスウィンドウ内であれば更新を再試行します。そうしないと、AMS は失敗したインスタンス更新の組み合わせに関するサービス通知を作成し、メンテナンスウィンドウの指示を待ちます。</p>                                                                                                                                                                                                  | <p>該当なし。</p>                                                                          |
| <p>お客様に起因する障害については、新しいパッチ RFC のサービスリクエストを送信してインスタンスを更新します。</p>                                                                                                                                                                                                                                                                                                       | <p>該当なし。</p>                                                                          |

## 重要なパッチ適用

これらは、重要なセキュリティ更新のための AMS サービスコミットメントです。

## 重要なセキュリティ更新プログラム、変更可能なインフラストラクチャ

| イベント/アクション                                                                                                                                                                                                                                                                                                                   | サービスコミットメントの測定                                                                                     |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| <p>CSU がリリースされました。</p>                                                                                                                                                                                                                                                                                                       | <p>クロック開始</p>                                                                                      |
| <p>AMS は、各スタックのサービス通知 (E メールも送信) を通じてパッチ RFC を通知します。サービス通知には以下が含まれます。</p> <ul style="list-style-type: none"><li>• リリース日の更新</li><li>• 重要度を更新する</li><li>• 更新の詳細: KB リファレンスなど</li><li>• 影響を受けるスタックの IDs</li></ul>                                                                                                               | <p>サービス通知が送信されると、クロックは停止します。</p>                                                                   |
| <p>RFC にリストされている更新をテストし、サービス通知に返信して 10 日以内に RFC を承認または拒否します。</p> <p>更新をインストールするための特定のメンテナンスウィンドウ (スタックごと) を指定します。サービス通知への応答から 24 時間以内に指定されたメンテナンスウィンドウは、使用可能な容量に基づいて再スケジュールされる場合があります。</p> <p>10 日以内に返信しない場合、またはパッチ RFC を拒否した場合、保留中のアクションはキャンセルされます。</p> <p>14 日後に更新を適用する場合は、前の RFC の詳細に基づいて新しいパッチ RFC のサービスリクエストを送信します。</p> | <p>14 日以内に承認または返信しない場合、保留中の変更はキャンセルされ、更新のサービスコミットメントは適用されません。</p>                                  |
| <p>サービス通知を承認すると、AMS は更新を適用します。</p>                                                                                                                                                                                                                                                                                           | <p>目的のメンテナンスウィンドウがサービスコミットメント期間内にない場合、RFC が目的のメンテナンスウィンドウ内に実行されていない場合にのみ、更新のサービスコミットメントは失われます。</p> |

| イベント/アクション                                                                                                                                                                                      | サービスコミットメントの測定 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| 複数の更新の場合、サービス通知へのレスポンスで除外する更新を指定することで、変更から特定の更新を除外できます。                                                                                                                                         |                |
| AMS は、適用された各更新の結果に関するサービス通知を送信します。サービス通知には、次の詳細が含まれます。 <ul style="list-style-type: none"><li>Amazon EC2 インスタンス ID</li><li>更新の成功: ARN a1、ARN a2...</li><li>更新に失敗しました: ARN c1、ARN c2...</li></ul> | 該当なし。          |
| 更新に失敗した場合、AMS は分析を実行して失敗の原因を理解し、分析の結果を通知します。障害が AMS に起因する場合、AMS はメンテナンスウィンドウ内であれば更新を再試行します。そうでない場合、AMS は失敗したインスタンス更新の組み合わせに関するサービス通知を作成し、新しいメンテナンスウィンドウで指示を待ちます。                                | 該当なし。          |
| お客様に起因する障害については、新しいパッチ RFC のサービスリクエストを送信してインスタンスを更新します。                                                                                                                                         | 該当なし。          |

## 重要なセキュリティ更新プログラム、イミュータブルインフラストラクチャ

| イベント/アクション                                                                                          | サービスコミットメントの測定   |
|-----------------------------------------------------------------------------------------------------|------------------|
| CSU がリリースされました。                                                                                     | クロック開始           |
| AMS は、サービス通知を介して以下を通知します。 <ul style="list-style-type: none"><li>リリース日の更新</li><li>重要度を更新する</li></ul> | クロックは引き続き実行されます。 |

| イベント/アクション                                                                                                                                                                                                                       | サービスコミットメントの測定     |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| <ul style="list-style-type: none"><li>• 更新の詳細 (KB リファレンスなど )</li><li>• 影響を受ける AMS Amazon マシンイメージ (AMI)</li><li>• 新しく更新された AMIs の予想されるリリース日時</li></ul>                                                                            |                    |
| <p>AMS は、マネージドアカウントで更新された AMIs をリリースします。</p>                                                                                                                                                                                     | <p>クロックが停止します。</p> |
| <p>サービス通知を承認すると、AMS は更新を適用します。</p> <p>AMS は、 アカウントで共有AMIs を、サービス通知と E メールで通知します。</p>                                                                                                                                             | <p>該当なし。</p>       |
| <p>新しい AMIs のテストに、割り当てられた時間 (1 週間) より時間がかかる場合は、サービスリクエストを AMS に送信してAuto Scaling グループを新しい AMS AMI (そのまま) で更新できます。設定で新しい AMS AMI を変更する場合は、管理   その他   その他   CT の更新 (ct-0xdawir96cy7k) で RFC を使用してAuto Scaling グループの更新をリクエストします。</p> | <p>該当なし。</p>       |

# レポートとオプション

AWS Managed Services (AMS) は、さまざまなネイティブ AWS サービスからのデータを照合して、主要な AMS サービスに関する付加価値レポートを提供します。

AMS には、次の 2 種類の詳細レポートがあります。

- リクエストレポートの場合: Cloud Service Delivery Manager (CSDM) を使用して、特定のレポートをアドホックにリクエストできます。オンボーディングまたは重要なイベント中に複数回リクエストする必要がある可能性があるため、これらのレポートには制限はありません。ただし、これらのレポートは、週次レポートなどのスケジュールで提供されるように設計されていないことに注意してください。ニーズをよりよく理解するため、またはセルフサービスレポートの使用の詳細については、CSDM にお問い合わせください。
- セルフサービスレポート: AMS セルフサービスレポートを使用すると、必要な頻度でデータを直接クエリおよび分析できます。セルフサービスレポートを使用して AMS コンソールからレポートにアクセスし、S3 バケット (アカウントごとに 1 つのバケット) を介してデータセットをレポートします。これにより、データをお気に入りのビジネスインテリジェンス (BI) ツールに統合して、要件に合わせてレポートをカスタマイズできます。

## トピック

- [リクエスト時レポート](#)
- [セルフサービスレポート](#)

## リクエスト時レポート

### トピック

- [AMS パッチレポート](#)
- [AMS Backup レポート](#)
- [Incidents Prevented and Monitoring Top Talkers レポート](#)
- [請求料金の詳細レポート](#)
- [信頼できる修復レポート](#)

AMS は、さまざまなネイティブ AWS サービスからのデータを照合して、主要な AMS サービスに関する付加価値レポートを提供します。これらのレポートのコピーについては、Cloud Service Delivery Manager (CSDM) にリクエストしてください。

## AMS パッチレポート

### 使用可能なレポート

- [パッチインスタンスの詳細の概要レポート](#)
- [パッチ詳細レポート](#)
- [欠落したパッチがレポートするインスタンス](#)
- [SSM カバレッジレポートのパッチ適用](#)

### パッチインスタンスの詳細の概要レポート

パッチインスタンスの詳細概要レポートには、レポートにオンボードされているインスタンスについて収集されたインスタンスの詳細が表示されます。これは、オンボーディングされたすべてのインスタンス、アカウントステータス、インスタンスの詳細、メンテナンスウィンドウのカバレッジ、メンテナンスウィンドウの実行時間、スタックの詳細、プラットフォームタイプを識別するのに役立つ情報レポートです。このレポートには、以下が表示されます。

1. アカウントの本番稼働用インスタンスと非本番稼働用インスタンスのデータ。注: 本番稼働用ステージと非本番稼働用ステージは、インスタンスタグからではなく、アカウント名から派生します。
2. プラットフォームタイプ別のインスタンスの分散に関するデータ。注: 「N/A」プラットフォームタイプは、が AWS Systems Manager プラットフォーム情報を取得できない場合です。
3. インスタンスの状態の分布、および実行中、停止、または終了中のインスタンスの数に関するデータ。

| フィールド名   | 定義                          |
|----------|-----------------------------|
| レポート日時   | レポートが生成された日時。               |
| アカウント ID | インスタンス ID が属する AWS アカウント ID |
| アカウント名   | AWS アカウント名                  |

| フィールド名               | 定義                                                                                                             |
|----------------------|----------------------------------------------------------------------------------------------------------------|
| 本番稼働用アカウント           | アカウント名に値「PROD」、「NONPROD」が含まれているかどうかに応じて、AMS prod および non-prod アカウントの識別子。例: PROD、NONPROD、使用不可                   |
| アカウントステータス           | AMS アカウントのステータス。例: ACTIVE、INACTIVE                                                                             |
| AMS アカウントサービスコミットメント | PREMIUM、"                                                                                                      |
| ランディングゾーン            | アカウントランディングゾーンタイプのフラグ。例: MALZ、NON-MALZ                                                                         |
| アクセス制限               | アクセスが制限されているリージョン。例: US SOIL                                                                                   |
| インスタンス ID            | EC2 インスタンスの ID                                                                                                 |
| インスタンス名              | EC2 インスタンスの名前                                                                                                  |
| インスタンスプラットフォームタイプ    | オペレーティングシステム (OS) タイプ。例: Windows、Linux など                                                                      |
| インスタンスプラットフォーム名      | オペレーティングシステム (OS) 名。例: MicrosoftWindowsServer2012R2Standard、RedHatEnterpriseLinuxServer                        |
| スタックの名前              | インスタンスを含むスタックの名前                                                                                               |
| スタックタイプ              | AMS スタック (カスタマーアカウント内の AMS インフラストラクチャ) またはカスタマースタック (カスタマーアプリケーションをサポートする AMS マネージドインフラストラクチャ)。例: AMS、CUSTOMER |
| Auto Scaling グループ名   | インスタンスを含む Auto Scaling グループ (ASG) の名前                                                                          |

| フィールド名           | 定義                                                                                                                                                                                             |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| インスタンスパッチグループ    | インスタンスをグループ化し、同じメンテナンスウィンドウを適用するために使用されるパッチグループ名。パッチグループが未割り当ての場合、値は「未割り当て」になります。                                                                                                              |
| インスタンスパッチグループタイプ | <p>パッチグループタイプ。</p> <p>DEFAULT: インスタンスの AMSDefaultPatchGroup:True タグによって決定される、デフォルトのメンテナンスウィンドウを持つデフォルトのパッチグループ。</p> <p>CUSTOMER: お客様が作成したパッチグループ。</p> <p>NOT_ASSIGNED: パッチグループが割り当てられていません</p> |
| インスタンスの状態        | <p>EC2 インスタンスライフサイクル内の状態。<br/>例: TERMINATED、RUNNING、STOPPING、STOPPED、SHUTTING-DOWN、PENDING。</p> <p>詳細については、<a href="#">「インスタンスのライフサイクル」</a>を参照してください。</p>                                      |
| メンテナンスウィンドウカバレッジ | このインスタンスに将来のメンテナンスウィンドウがある場合。例: COVERED または NOT_COVERED                                                                                                                                        |
| メンテナンスウィンドウの実行日時 | 次回はメンテナンスウィンドウの実行が想定されます。NULL の場合、単一ウィンドウ実行、つまり繰り返しではない                                                                                                                                        |



## パッチ詳細レポート

AWS Managed Services (AMS) パッチの詳細レポートには、次のようなさまざまなインスタンスのパッチの詳細とメンテナンスウィンドウのカバレッジが表示されます。

1. パッチグループとそのタイプのデータ。
2. メンテナンスウィンドウ、期間、カットオフ、メンテナンスウィンドウの実行の将来の日付 (スケジュール)、および各ウィンドウで影響を受けるインスタンスのデータ。
3. アカウント内のすべてのオペレーティングシステムのデータと、オペレーティングシステムがインストールされているインスタンスの数。

| フィールド名            | 定義                                                                                                  |
|-------------------|-----------------------------------------------------------------------------------------------------|
| レポート日時            | レポートが生成された日時。                                                                                       |
| アカウント ID          | インスタンス ID が属する AWS アカウント ID                                                                         |
| アカウント名            | AWS アカウント名                                                                                          |
| インスタンス ID         | EC2 インスタンスの ID                                                                                      |
| 本番稼働用アカウント        | アカウント名に値「PROD」、「NONPROD」が含まれているかどうかに応じて、AMS prod および non-prod アカウントの識別子。データが使用できない場合、値は「使用不可」になります。 |
| アカウントステータス        | AMS アカウントのステータス。例: ACTIVE、INACTIVE                                                                  |
| インスタンスプラットフォームタイプ | オペレーティングシステム (OS) タイプ。例: Windows、Linux                                                              |
| インスタンスプラットフォーム名   | オペレーティングシステム (OS) 名。例: MicrosoftWindowsServer2012R2Standard、RedHatEnterpriseLinuxServer             |
| スタックタイプ           | AMS スタック (カスタマーアカウント内の AMS インフラストラクチャ) またはカスタマー                                                     |

| フィールド名           | 定義                                                                                                                                                                                        |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | スタック (カスタマーアプリケーションをサポートする AMS マネージドインフラストラクチャ)。例: AMS、CUSTOMER                                                                                                                           |
| インスタンスパッチグループ    | インスタンスをグループ化し、同じメンテナンスウィンドウを適用するために使用されるパッチグループ名。パッチグループが未割り当ての場合、値は「未割り当て」になります。                                                                                                         |
| インスタンスパッチグループタイプ | <p>パッチグループタイプ。</p> <p>DEFAULT: インスタンスのAMSDefaultPatchGroup:True タグによって決定される、デフォルトのメンテナンスウィンドウを含むデフォルトのパッチグループ</p> <p>CUSTOMER: お客様が作成したパッチグループ</p> <p>UNASSIGNED: パッチグループが割り当てられていません</p> |
| インスタンスの状態        | <p>EC2 インスタンスのライフサイクル内の状態。例: TERMINATED、RUNNING、STOPPING、STOPPED、SHUTTING-DOWN、PENDING</p> <p>詳細については、<a href="#">「インスタンスのライフサイクル」</a>を参照してください。</p>                                      |
| メンテナンスウィンドウ ID   | メンテナンスウィンドウ識別子                                                                                                                                                                            |
| メンテナンスウィンドウの状態   | 指定できる値は、ENABLED または DISABLED です。                                                                                                                                                          |
| メンテナンスウィンドウのタイプ  | メンテナンスウィンドウタイプ                                                                                                                                                                            |

| フィールド名               | 定義                                                                                                   |
|----------------------|------------------------------------------------------------------------------------------------------|
| メンテナンスウィンドウの次の実行日時   | 次回はメンテナンスウィンドウの実行が想定されます。NULL の場合、単一ウィンドウ実行、つまり繰り返しではない                                              |
| 最終実行メンテナンスウィンドウ      | メンテナンスウィンドウが最後に実行された時刻                                                                               |
| メンテナンスウィンドウの期間 (時間 ) | メンテナンスウィンドウの時間単位の期間                                                                                  |
| メンテナンスウィンドウカバレッジ     | メンテナンスウィンドウのカバレッジ                                                                                    |
| パッチベースライン ID         | 現在インスタンスにアタッチされているパッチベースライン                                                                          |
| パッチステータス             | パッチの全体的なコンプライアンスステータス。例: COMPLIANT、NON_COMPLIANT。パッチが少なくとも 1 つ欠落している場合、インスタンスは非準拠、それ以外の場合は準拠と見なされます。 |
| 準拠 - 合計              | 準拠パッチの数 (すべての重要度 )                                                                                   |
| 非準拠 - 合計             | 非準拠パッチの数 (すべての重要度 )                                                                                  |
| 準拠 - 重要              | 重大度が「重大」の準拠パッチの数                                                                                     |
| 準拠 - 高               | 「重要度が高い」準拠パッチの数                                                                                      |
| 準拠 - 中               | 重要度が「中」の準拠パッチの数                                                                                      |
| 準拠 - 低               | 「重要度が低い」準拠パッチの数                                                                                      |
| 準拠 - 情報              | 「情報」重要度の準拠パッチの数                                                                                      |
| 準拠 - 未指定             | 重要度が「未指定」の準拠パッチの数                                                                                    |
| 非準拠 - 重大             | 重要度が「重大」の非準拠パッチの数                                                                                    |
| 非準拠 - 高              | 「重要度が高い」非準拠パッチの数                                                                                     |

| フィールド名    | 定義                 |
|-----------|--------------------|
| 非準拠 - 中   | 「中」重要度の非準拠パッチの数    |
| 非準拠 - 低   | 「重要度が低い」非準拠パッチの数   |
| 非準拠 - 情報  | 「情報」重要度の非準拠パッチの数   |
| 非準拠 - 未指定 | 重要度が「未指定」の非準拠パッチの数 |

## 欠落したパッチがレポートするインスタンス

パッチを見逃した AWS Managed Services (AMS) インスタンスレポートには、前回のメンテナンスウィンドウの実行中にパッチを見逃したインスタンスの詳細が表示されます。

1. パッチ ID レベルで欠落しているパッチのデータ。
2. パッチの重要度、パッチ適用されていない日数、範囲、リリース日などの属性とともに、少なくとも 1 つのパッチが欠落しているすべてのインスタンスのデータ。

| フィールド名          | 定義                                                                   |
|-----------------|----------------------------------------------------------------------|
| レポート日時          | レポートが生成された日時。                                                        |
| アカウント ID        | インスタンス ID が属する AWS アカウント ID                                          |
| アカウント名          | AWS アカウント名                                                           |
| 本番稼働用アカウント      | アカウント名に値「PROD」、「NONPROD」が含まれているかどうかに応じて、AMS prod、non-prod アカウントの識別子。 |
| アカウントステータス      | AMS アカウントのステータス。例: ACTIVE または INACTIVE                               |
| AMS アカウントサービス階層 | PREMIUM または"                                                         |
| [インスタンス ID]     | EC2 インスタンスの ID                                                       |

| フィールド名            | 定義                                                                                                                                             |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| インスタンスプラットフォームタイプ | オペレーティングシステム (OS) タイプ。例: Windows                                                                                                               |
| インスタンスの状態         | EC2 インスタンスのライフサイクルの状態。<br>例: TERMINATED、RUNNING、STOPPING、STOPPED、SHUTTING-DOWN、PENDING<br>詳細については、 <a href="#">「インスタンスのライフサイクル」</a> を参照してください。 |
| パッチ ID            | リリースされたパッチの ID。例: KB3172729                                                                                                                    |
| パッチの重要度           | パブリッシャーあたりのパッチの重要度。<br>例: CRITICAL、IMPORTANT、MODERATE、LOW、UNSPECIFIED                                                                          |
| パッチ分類             | パブリッシャーあたりのパッチの分類。<br>例: CRITICALUPDATES、SECURITYUPDATES、UPDATEROLLUPS、UPDATES、FEATUREPACKS                                                    |
| パッチリリース日時 (UTC)   | パブリッシャーあたりのパッチのリリース日                                                                                                                           |
| パッチのインストール状態      | SSM ごとにインスタンスにパッチの状態をインストールします。例: INSTALLED、MISSING、NOT APPLICABLE                                                                             |
| パッチが適用されていない日数    | 前回の SSM スキャン以降にインスタンスがパッチ適用されていない日数                                                                                                            |
| パッチが適用されていない日数の範囲 | パッチが適用されていない日数のバケット化。<br>例: <30 日、30～60 日、60～90 日、90 日以上                                                                                       |

## SSM カバレッジレポートのパッチ適用

AMS パッチ適用 SSM カバレッジレポートは、アカウントの EC2 インスタンスに SSM エージェントがインストールされているかどうかを通知します。

| フィールド名       | 定義                                                              |
|--------------|-----------------------------------------------------------------|
| 顧客名          | 複数のサブ顧客が存在する状況の顧客名                                              |
| リソースリージョン    | AWS リソースが配置されているリージョン                                           |
| アカウント名       | アカウントの名前                                                        |
| AWS アカウント ID | AWS アカウントの ID                                                   |
| リソース ID      | EC2 インスタンスの ID                                                  |
| リソース名        | EC2 インスタンスの名前                                                   |
| 準拠フラグ        | リソースに SSM エージェントがインストールされているかどうか (「準拠」) を示します (「NON_COMPLIANT」) |

## AMS Backup レポート

### 使用可能なレポート

- [バックアップジョブの成功/失敗レポート](#)
- [バックアップ概要レポート](#)
- [バックアップの概要/カバレッジレポート](#)

### バックアップジョブの成功/失敗レポート

Backup Job Success/Failure レポートには、過去数週間に実行されたバックアップに関する情報が表示されます。レポートをカスタマイズするには、データを取得する週数を指定します。デフォルトの週数は 12 です。次の表に、レポートに含まれるデータを示します。

| フィールド名       | 定義                    |
|--------------|-----------------------|
| AWS アカウント ID | リソースが属する AWS アカウント ID |
| アカウント名       | AWS アカウント名            |

| フィールド名        | 定義                                                              |
|---------------|-----------------------------------------------------------------|
| バックアップジョブ ID  | Backup ジョブの ID                                                  |
| リソース ID       | バックアップされたリソースの ID                                               |
| リソースタイプ       | バックアップされるリソースのタイプ                                               |
| リソースリージョン     | バックアップされたリソースの AWS リージョン                                        |
| バックアップ状態      | バックアップの状態。詳細については、 <a href="#">「バックアップジョブのステータス」</a> を参照してください。 |
| 復旧ポイント ID     | 復旧ポイントの一意的識別子                                                   |
| ステータスメッセージ    | バックアップジョブ中に発生したエラーまたは警告の説明                                      |
| バックアップサイズ     | GB 単位のバックアップのサイズ                                                |
| 復旧ポイント ARN    | 作成されたバックアップの ARN                                                |
| 日数単位の復旧時点経過時間 | 復旧ポイントが作成されてから経過した日数                                            |
| 30 日未満        | 30 日未満のバックアップのインジケータ                                            |

## バックアップ概要レポート

| フィールド名  | 定義                |
|---------|-------------------|
| 顧客名     | 複数のサブ顧客がいる状況の顧客名  |
| バックアップ月 | バックアップ月           |
| バックアップ年 | バックアップの年          |
| リソースタイプ | バックアップされるリソースのタイプ |

| フィールド名        | 定義               |
|---------------|------------------|
| リソースの数        | バックアップされたリソースの数  |
| 復旧ポイントの数      | 個別のスナップショットの数    |
| 30 日未満のバックアップ | 30 日未満のバックアップの数  |
| 最大復旧時間        | 日数での最も古い復旧時点経過時間 |
| 最小復旧ポイント経過時間  | 最新の復旧時点経過日数      |

## バックアップの概要/カバレッジレポート

Backup Summary/Coverage レポートには、どの AWS Backup プランでも現在保護されていないリソースの数が表示されます。可能な場合はカバレッジを増やし、データ損失のリスクを減らすための適切な計画を CDSM と話し合います。

| フィールド名       | 定義                                                                                         |
|--------------|--------------------------------------------------------------------------------------------|
| 顧客名          | 複数のサブ顧客がいる状況の顧客名                                                                           |
| リージョン        | AWS リソースが配置されているリージョン                                                                      |
| アカウント名       | アカウントの名前                                                                                   |
| AWS アカウント ID | AWS アカウントの ID                                                                              |
| リソースタイプ      | リソースのタイプ。リソースは AWS Backup (Aurora、DocumentDB、DynamoDB、EBS、EC2、EFS、FSx、RDS、S3) でサポートされています。 |
| リソースARN      | リソースの ARN                                                                                  |
| リソース ID      | リソースの ID                                                                                   |



| フィールド名        | 定義                                                 |
|---------------|----------------------------------------------------|
| カバレッジ         | リソースがカバーされているかどうかを示します (「COVERED」または「NOT_COVERED」) |
| リソースの数        | アカウントでサポートされているリソースの数                              |
| perc_coverage | 過去 30 日間に実行されたバックアップでサポートされているリソースの割合。             |

## Incidents Prevented and Monitoring Top Talkers レポート

使用可能なレポート

- [防止されたインシデントレポート](#)
- [トップトーカーレポートのモニタリング](#)

### 防止されたインシデントレポート

Incidents Prevented レポートには、自動的に修復された Amazon CloudWatch アラームが一覧表示され、インシデントの可能性が防止されます。詳細については、[「自動修復」](#)を参照してください。次の表に、このレポートに含まれる情報を示します。

| フィールド名                   | 定義                             |
|--------------------------|--------------------------------|
| execution_start_time_utc | オートメーションが実行された日付               |
| customer_name            | アカウントの顧客名                      |
| account_name             | アカウントの名称                       |
| AwsAccountId             | AWS アカウントの ID                  |
| document_name            | 実行された SSM ドキュメントまたはオートメーションの名称 |
| duration_in_minutes      | オートメーションの分単位の長さ                |

| フィールド名                      | 定義                    |
|-----------------------------|-----------------------|
| リージョン                       | AWS リソースが配置されているリージョン |
| Automation_execution_id     | 実行の ID                |
| Automation_execution_status | 実行のステータス              |

## トップトーカーレポートのモニタリング

Monitoring Top Talkers レポートには、特定の期間中に生成された Amazon CloudWatch アラートの数が表示され、アラートの最大数を生成するリソースが可視化されます。このレポートは、アラートを最も多く生成するリソースを特定するのに役立ちます。これらのリソースは、根本原因分析を実行して問題を修正したり、実際の問題がない場合に不要なトリガーを防ぐためにアラームのしきい値を変更したりする候補となる場合があります。次の表に、このレポートに含まれる情報を示します。

| フィールド名      | 定義                           |
|-------------|------------------------------|
| 顧客名         | 顧客の名前                        |
| AccountId   | AWS アカウントの ID                |
| アラートカテゴリ    | トリガーされたアラートのタイプ              |
| 説明          | アラートの説明                      |
| リソース ID     | アラートをトリガーしたリソースの ID          |
| リソース名       | アラートをトリガーしたリソースの名前           |
| リージョン       | AWSリソースが配置されているリージョン         |
| インシデントステータス | アラームによって生成されたインシデントの最新のステータス |
| 最初の出現       | アラートが初めてトリガーされたとき            |
| 最近の出現       | アラートがトリガーされた最新の時刻            |

| フィールド名 | 定義                     |
|--------|------------------------|
| アラート数  | 初回と最近の発生の上に生成されたアラートの数 |

## 請求料金の詳細レポート

AWS Managed Services (AMS) 請求料金詳細レポートには、リンクされたアカウントとそれぞれの AWS サービスでの AMS 請求料金の詳細が表示されます。

- AMS サービスレベルの料金、引き上げ率、アカウントレベルの AMS サービス階層、AMS 料金。
- リンクされたアカウントと AWS 使用料

| フィールド名         | 定義                                                    |
|----------------|-------------------------------------------------------|
| 請求月            | 請求されたサービスの月と年                                         |
| 支払者アカウント ID    | AMS 料金の支払いを担当するアカウントを識別する 12 桁の ID                    |
| リンクされたアカウント ID | 経費を生成するサービスを消費する AMS アカウントを識別する 12 桁の ID              |
| AWS サービス名      | 使用された AWS サービス                                        |
| AWS 料金         | AWS サービス名に記載されている AWS サービス名の AWS 料金                   |
| 料金プラン          | リンクされたアカウントに関連付けられた料金プランの名前                           |
| アップリフト比率       | pricing_plan、SLA、AWS サービスに基づく引き上げ率 (10 進 V.WXYZ として ) |
| 調整済み AWS 料金    | AWS AMS 用に調整された使用量                                    |

| フィールド名                | 定義                                                                                                                             |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------|
| AWS 料金の引き上げ           | AMS に対して請求される AWS 料金の割合;<br>$\text{adjusted\_aws\_charges} * \text{uplift\_percent}$                                           |
| インスタンス EC2 RDS の使用    | EC2 インスタンスと RDS インスタンスの使用                                                                                                      |
| AMS 料金                | 製品の AMS 料金の合計、 $\text{uplifted\_aws\_charges} + \text{instance\_ec2\_rds\_spend} + \text{uplifted\_ris} + \text{uplifted\_sp}$ |
| 按分された最低料金             | 契約上の最小値を満たすために請求される金額                                                                                                          |
| 最小料金                  | AMS 最小料金 (該当する場合 )                                                                                                             |
| リンクされたアカウントの合計 AMS 料金 | $\text{linked\_account}$ のすべての料金の合計                                                                                            |
| 支払者アカウントの合計 AMS 料金    | 支払者アカウントのすべての料金の合計                                                                                                             |

## 信頼できる修復レポート

### 使用可能なレポート

- [信頼できる修復の概要レポート](#)
- [信頼できる修復者設定の概要レポート](#)
- [Trusted Advisor 概要レポートを確認する](#)

## 信頼できる修復の概要レポート

信頼できる修復者修復ステータスレポートは、以前の修復サイクル中に発生した修復に関する情報を提供します。デフォルトの週数は 1 です。レポートをカスタマイズするには、修復スケジュールに基づいて週数を指定します。

| フィールド名   | 定義                    |
|----------|-----------------------|
| 日付       | データが収集された日付。          |
| アカウント ID | リソースが属する AWS アカウント ID |

| フィールド名        | 定義                                               |
|---------------|--------------------------------------------------|
| アカウント名        | AWS アカウント名                                       |
| チェックカテゴリ      | AWS Trusted Advisor チェックカテゴリ                     |
| チェック名         | 修正された Trusted Advisor チェックの名前                    |
| チェック ID       | 修正された Trusted Advisor チェックの ID                   |
| 実行モード         | 特定の Trusted Advisor チェック用に設定された実行モード             |
| OpsItem ID    | 修復 Trusted Advisor のために によって作成された OpsItem の ID   |
| OpsItem ステータス | レポート Trusted Advisor 時に によって作成された OpsItem のステータス |
| リソース ID       | 修復用に作成されたリソースの ARN                               |

## 信頼できる修復者設定の概要レポート

Trusted Remediator Configuration Summary レポートには、各 Trusted Advisor チェックの現在の Trusted Remediator Remediation 設定に関する情報が表示されます。

| フィールド名   | 定義                                    |
|----------|---------------------------------------|
| 日付       | データが収集された日付。                          |
| アカウント ID | 設定が適用される AWS アカウント ID                 |
| アカウント名   | AWS アカウント名                            |
| チェックカテゴリ | AWS Trusted Advisor チェックカテゴリ          |
| チェック名    | 設定が適用される修復された Trusted Advisor チェックの名前 |

| フィールド名      | 定義                                   |
|-------------|--------------------------------------|
| チェック ID     | 設定が適用される修復 Trusted Advisor チェックの ID  |
| 実行モード       | 特定の Trusted Advisor チェック用に設定された実行モード |
| 自動へのオーバーライド | 実行モードを自動に上書きするように設定されている場合のタグパターン    |
| 手動へのオーバーライド | 実行モードを手動に上書きするように設定されている場合のタグパターン    |

## Trusted Advisor 概要レポートを確認する

Trusted Advisor チェック概要レポートには、現在の Trusted Advisor チェックに関する情報が表示されます。このレポートは、毎週の修復スケジュールの後にデータを収集します。デフォルトの週数は 1 です。レポートをカスタマイズするには、修復サイクルに基づいて週数を指定します。

| フィールド名   | 定義                                                                     |
|----------|------------------------------------------------------------------------|
| 日付       | データが収集された日付。                                                           |
| アカウント ID | 設定が適用される AWS アカウント ID                                                  |
| 顧客名      | AWS アカウント名                                                             |
| チェックカテゴリ | AWS Trusted Advisor チェックカテゴリ                                           |
| チェック名    | 設定が適用される修復された Trusted Advisor チェックの名前                                  |
| チェック ID  | 設定が適用される修復 Trusted Advisor チェックの ID                                    |
| ステータス    | チェックのアラートステータス。使用可能なステータスは、OK (緑)、警告 (黄)、エラー (赤)、または not_available です。 |

| フィールド名        | 定義                                                     |
|---------------|--------------------------------------------------------|
| フラグが付けられたリソース | Trusted Advisor チェックによってフラグ付け (一覧表示) された AWS リソースの数。   |
| 無視されるリソース     | 抑制済みとしてマークした Trusted Advisor ために によって無視された AWS リソースの数。 |
| クリティカル状態のリソース | クリティカル状態のリソースの数                                        |
| 警告状態のリソース     | 警告状態にあるリソースの数                                          |

## セルフサービスレポート

AWS Managed Services (AMS) セルフサービスレポート (SSR) は、さまざまなネイティブ AWS サービスからデータを収集し、主要な AMS サービスに関するレポートへのアクセスを提供する機能です。SSR は、オペレーション、設定管理、アセット管理、セキュリティ管理、コンプライアンスをサポートするために使用できる情報を提供します。

SSR を使用して AMS コンソールからレポートにアクセスし、Amazon S3 バケット (アカウントごとに 1 つのバケット) を介してデータセットをレポートします。データをお気に入りのビジネスインテリジェンス (BI) ツールに接続して、独自のニーズに基づいてレポートをカスタマイズできます。AMS はこの S3 バケット (S3 バケット名: (ams-reporting-data-a<Account\_ID>)) をプライマリ AWS リージョンに作成し、データは us-east-1 リージョンでホストされている AMS コントロールプレーンから共有されます。

### Important

この機能にアクセスするには、次のいずれかのロールが必要です。

- マルチアカウントランディングゾーン: AWSManagedServicesReadOnlyRole
- 単一アカウントランディングゾーン: Customer\_ReadOnly\_Role

### Important

でのカスタムキーの使用 AWS Glue

AWS Glue メタデータをカスターマネージド KMS キーで暗号化するには、以下の追加ステップを実行して、AMS がアカウントからデータを集約できるようにする必要があります。

1. <https://console.aws.amazon.com/kms> で AWS Key Management Service コンソールを開き、カスターマネージドキーを選択します。
2. AWS Glue メタデータの暗号化に使用する予定のキー ID を選択します。
3. エイリアスタブを選択し、エイリアスの作成を選択します。
4. テキストボックスに AmsReportingFlywheelCustomKey と入力し、エイリアスの作成を選択します。

## トピック

- [内部 API オペレーション](#)
- [パッチレポート \(毎日\)](#)
- [バックアップレポート \(毎日\)](#)
- [インシデントレポート \(毎週\)](#)
- [請求レポート \(毎月\)](#)
- [集計レポート](#)
- [AMS セルフサービスレポートダッシュボード](#)
- [データ保持ポリシー](#)
- [SSR からのオフボード](#)

## 内部 API オペレーション

API オペレーションをモニタリングすると、次の内部専用オペレーションの呼び出しが表示される場合があります。

- GetDashboardUrl
- ListReportsV2

### 内部 API オペレーション: GetDashboardUrl

このオペレーションは、AMS コンソールによって呼び出されるとシステムログに表示されます。他にユースケースはありません。直接使用することはできません。



対応するレポートの埋め込みダッシュボード URL を返します。このオペレーションは、`dashboardName` 返された を受け入れます `ListReports`。

## リクエストの構文

```
HTTP/1.1 200
Content-type: application/json
{
  "dashboardName": "string"
}
```

## リクエスト要素

**dashboardName:** URL がリクエストされているクイックダッシュボードの名前。ダッシュボード名は `ListReportsV2` で返されます。

タイプ: 文字列

## レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json
{
  "url": "string"
}
```

## レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。サービスから以下のデータが JSON 形式で返されます。

**url:** リクエストされた のクイック URL を返します `dashboardName`。

タイプ: 文字列

## エラー

すべてのアクションに共通するエラーについては、[「一般的なエラー」](#)を参照してください。

### **BadRequestException:**

送信されたリクエストは無効です。たとえば、入力が不完全または正しくない場合などです。詳細については、添付のエラーメッセージを参照してください。

HTTP ステータスコード: 400

**NotFoundException:**

リクエストされたリソースが見つかりません。リクエスト URI が正しいことを確認します。

HTTP ステータスコード: 404

**TooManyRequestsException:**

リクエストがスロットリング制限に達しました。指定された期間の後に再試行します。

HTTP ステータスコード: 429

**UnauthorizedException:**

発信者のアクセス許可が不十分なため、リクエストは拒否されます。

HTTP ステータスコード: 401

## 内部 API オペレーション: ListReportsV2

この API は、AMS コンソールによって呼び出されるとシステムログに表示されます。他にユースケースはありません。直接使用することはできません。

指定されたアカウントで利用できる運用レポートのリストを返します。

### リクエストの構文

リクエストにリクエスト本文がありません。

### レスポンスの構文

```
HTTP/1.1 200
Content-type: application/json
{
  "reportsList": [
    {
      "dashboard": "string",
      "lastUpdatedTime": "string",
    }
  ],
  "reportsType": "string"
}
```

## レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。サービスから以下のデータが JSON 形式で返されます。

**reportsList:** 使用可能な運用レポートのリスト。

タイプ: Dashboard オブジェクトの配列

**reportsType:** レポートが複数のアカウントで集計されるかどうかを示します。

タイプ: 文字列

## エラー

すべてのアクションに共通するエラーについては、[「一般的なエラー」](#)を参照してください。

### BadRequestException:

送信されたリクエストは無効です。たとえば、入力が不完全または正しくないとします。詳細については、添付のエラーメッセージを参照してください。

HTTP ステータスコード: 400

### NotFoundException:

リクエストされたリソースが見つかりません。リクエスト URI が正しいことを確認します。

HTTP ステータスコード: 404

### TooManyRequestsException:

リクエストがスロットリング制限に達しました。指定された期間の後に再試行します。

HTTP ステータスコード: 429

### UnauthorizedException:

発信者のアクセス許可が不十分なため、リクエストは拒否されます。

HTTP ステータスコード: 401

## パッチレポート (毎日 )

使用可能なレポート

-

- [パッチの詳細](#)
- [パッチを見逃したインスタンス](#)

これは、パッチオーケストレーター (PO)、アカウントステータス、インスタンスの詳細、メンテナンスウィンドウのカバレッジ、メンテナンスウィンドウの実行時間、スタックの詳細、プラットフォームタイプにオンボードされているすべてのインスタンスを識別するのに役立つ情報レポートです。

このデータセットは以下を提供します。

- アカウントの本番稼働用インスタンスと非本番稼働用インスタンスのデータ。本番稼働用ステージと非本番稼働用ステージは、インスタンスタグからではなく、アカウント名から派生します。
- プラットフォームタイプ別のインスタンスの分散に関するデータ。「N/A」プラットフォームタイプは、AWS Systems Manager (SSM) がプラットフォーム情報を取得できない場合に発生します。
- インスタンスの状態の分布、実行中、停止、または終了中のインスタンスの数に関するデータ。

| コンソールフィールド名 | データセットフィールド名         | 定義                                      |
|-------------|----------------------|-----------------------------------------|
| アクセス制限      | access_restrictions  | アクセスが制限されているリージョン                       |
| アカウント ID    | aws_account_id       | AWS インスタンス ID が属するアカウント ID              |
| 管理者アカウント ID | aws_admin_account_id | 信頼された AWS Organizations アカウントが有効になりました。 |
| アカウント名      | account_name         | AWS アカウント名                              |
| アカウントステータス  | account_status       | AMS アカウントのステータス                         |
|             | account_sla          | AMS アカウントサービスコミットメント                    |
| アカウントの種類    | malz_role            | MALZ ロール                                |

| コンソールフィールド名        | データセットフィールド名              | 定義                                               |
|--------------------|---------------------------|--------------------------------------------------|
| Auto Scaling グループ名 | instance_asg_name         | インスタンスを含む Auto Scaling グループ (ASG) の名前            |
| インスタンス ID          | instance_id               | EC2 インスタンスの ID                                   |
| インスタンス名            | instance_name             | EC2 インスタンスの名前                                    |
| インスタンスパッチグループ      | instance_patch_group      | インスタンスをグループ化し、同じメンテナンスウィンドウを適用するために使用されるパッチグループ名 |
| インスタンスパッチグループタイプ   | instance_patch_group_type | パッチグループタイプ                                       |
| インスタンスプラットフォームタイプ  | instance_platform_type    | オペレーティングシステム (OS) タイプ                            |
| インスタンスプラットフォーム名    | instance_platform_name    | オペレーティングシステム (OS) 名                              |
| インスタンスの状態          | instance_state            | EC2 インスタンスライフサイクル内の状態                            |
| インスタンスタグ           | ec2_tags                  | Amazon EC2 インスタンス ID に関連付けられたタグ                  |
| ランディングゾーン          | malz_flag                 | MALZ 関連アカウントのフラグ                                 |

| コンソールフィールド名      | データセットフィールド名                   | 定義                                                                                             |
|------------------|--------------------------------|------------------------------------------------------------------------------------------------|
| メンテナンスウィンドウカバレッジ | mw_covered_flag                | インスタンスで、将来の実行日を持つメンテナンスウィンドウが少なくとも 1 つ有効になっている場合、そのインスタンスは対象と見なされ、それ以外の場合は対象外と見なされます。          |
| メンテナンスウィンドウの実行日時 | earliest_window_execution_time | 次回メンテナンスウィンドウの実行が予想される場合                                                                       |
| メンテナンスウィンドウの実行日時 | earliest_window_execution_time | 次回メンテナンスウィンドウの実行が予想される場合                                                                       |
| 本番稼働用アカウント       | prod_account                   | アカウント名に値「PROD」、「NONPROD」が含まれているかどうかに応じて、AMS prod および non-prod アカウントの識別子。                       |
| レポート日時           | dataset_datetime               | レポートが生成された日時。                                                                                  |
| スタックの名前          | instance_stack_name            | インスタンスを含むスタックの名前                                                                               |
| スタックタイプ          | instance_stack_type            | AMS スタック (カスタマーアカウント内の AMS インフラストラクチャ) またはカスタマースタック (カスタマーアプリケーションをサポートする AMS マネージドインフラストラクチャ) |

## パッチの詳細

このレポートには、さまざまなインスタンスのパッチの詳細とメンテナンスウィンドウのカバレッジが表示されます。

このレポートは以下を提供します。

- パッチグループとそのタイプのデータ。
- メンテナンスウィンドウ、期間、カットオフ、メンテナンスウィンドウの実行の将来の日付 (スケジュール)、および各ウィンドウで影響を受けるインスタンスのデータ。
- アカウント内のすべてのオペレーティングシステムのデータと、オペレーティングシステムがインストールされているインスタンスの数。

| フィールド名     | データセットフィールド名            | 定義                         |
|------------|-------------------------|----------------------------|
| レポート日時     | dataset_datetime        | レポートが生成された日時。              |
| アカウント ID   | aws_account_id          | AWS インスタンス ID が属するアカウント ID |
| アカウント名     | account_name            | AWS アカウント名                 |
| アカウントステータス | account_status          | AMS アカウントのステータス            |
| 準拠 - 重要    | compliant_critical      | 重要度が「重大」の準拠パッチの数           |
| 準拠 - 高     | compliant_high          | 「重要度が高い」準拠パッチの数            |
| 準拠 - 中     | compliant_medium        | 重要度が「中」の準拠パッチの数            |
| 準拠 - 低     | compliant_low           | 「重要度が低い」準拠パッチの数            |
| 準拠 - 情報    | compliant_informational | 「情報」重要度の準拠パッチの数            |

| フィールド名            | データセットフィールド名              | 定義                                                                                                                                                                 |
|-------------------|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 準拠 - 未指定          | compliant_unspecified     | 重要度が「未指定」の準拠パッチの数                                                                                                                                                  |
| 準拠 - 合計           | compliant_total           | 準拠パッチの数 (すべての重要度)                                                                                                                                                  |
| インスタンス ID         | instance_id               | EC2 インスタンスの ID                                                                                                                                                     |
| インスタンス名           | instance_name             | EC2 インスタンスの名前                                                                                                                                                      |
|                   | account_sla               | AMS アカウントサービス階層                                                                                                                                                    |
| インスタンスプラットフォームタイプ | instance_platform_type    | オペレーティングシステム (OS) タイプ                                                                                                                                              |
| インスタンスプラットフォーム名   | instance_platform_name    | オペレーティングシステム (OS) 名                                                                                                                                                |
| インスタンスパッチグループタイプ  | instance_patch_group_type | DEFAULT: インスタンスの AMSDefaultPatchGroup:True タグによって決定される、デフォルトのメンテナンスウィンドウを含むデフォルトのパッチグループ<br><br>CUSTOMER: お客様が作成したパッチグループ<br><br>NOT_ASSIGNED: パッチグループが割り当てられていません |
| インスタンスパッチグループ     | instance_patch_group      | インスタンスをグループ化し、同じメンテナンスウィンドウを適用するために使用されるパッチグループ名                                                                                                                   |



| フィールド名               | データセットフィールド名                  | 定義                                                                                |
|----------------------|-------------------------------|-----------------------------------------------------------------------------------|
| インスタンスの状態            | instance_state                | EC2 インスタンスのライフサイクル内の状態                                                            |
| インスタスタグ              | ec2_tags                      | Amazon EC2 インスタンス ID に関連付けられたタグ                                                   |
| 最終実行メンテナンスウィンドウ      | last_execution_window         | メンテナンスウィンドウが最後に実行された時刻                                                            |
| メンテナンスウィンドウ ID       | window_id                     | メンテナンスウィンドウ ID                                                                    |
| メンテナンスウィンドウの状態       | window_state                  | メンテナンスウィンドウの状態                                                                    |
| メンテナンスウィンドウのタイプ      | window_type                   | メンテナンスウィンドウタイプ                                                                    |
| メンテナンスウィンドウの次の実行日時   | window_next<br>execution_time | 次回メンテナンスウィンドウの実行が予想される場合                                                          |
| メンテナンスウィンドウの期間 (時間 ) | window_duration               | メンテナンスウィンドウの時間単位の期間                                                               |
| メンテナンスウィンドウカバレッジ     | mw_covered_flag               | インスタンスに将来の実行日を持つ有効なメンテナンスウィンドウが少なくとも 1 つある場合、そのインスタンスは対象と見なされ、それ以外の場合は対象外と見なされます。 |
| 非準拠 - 重大             | noncompliant_critical         | 重要度が「重大」の非準拠パッチの数                                                                 |
| 非準拠 - 高              | noncompliant_high             | 「重要度が高い」非準拠パッチの数                                                                  |

| フィールド名       | データセットフィールド名        | 定義                                                                        |
|--------------|---------------------|---------------------------------------------------------------------------|
| 非準拠 - 中      | noncompliant_medium | 重要度が「中」の非準拠パッチの数                                                          |
| 非準拠 - 低      | noncompliant_low    | 「重要度が低い」非準拠パッチの数                                                          |
| 非準拠 - 情報     | 非準拠<br>情報           | 「情報」重要度の非準拠パッチの数                                                          |
| 非準拠 - 未指定    | 非準拠<br>_指定なし        | 重要度が「未指定」の非準拠パッチの数                                                        |
| 非準拠 - 合計     | noncompliant_total  | 非準拠パッチの数 (すべての重要度 )                                                       |
| パッチベースライン ID | patch_baseline_id   | 現在インスタンスにアタッチされているパッチベースライン                                               |
| パッチステータス     | patch_status        | パッチの全体的なコンプライアンスステータス。パッチが少なくとも 1 つ欠落している場合、インスタンスは非準拠、それ以外の場合は準拠と見なされます。 |
| 本番稼働用アカウント   | prod_account        | アカウント名に値「PROD」、「NONPROD」が含まれているかどうかに応じて、AMS prod、non-prod アカウントの識別子。      |

| フィールド名  | データセットフィールド名          | 定義                                                                                             |
|---------|-----------------------|------------------------------------------------------------------------------------------------|
| スタックタイプ | instance_stack_type   | AMS スタック (カスタマーアカウント内の AMS インフラストラクチャ) またはカスタマースタック (カスタマーアプリケーションをサポートする AMS マネージドインフラストラクチャ) |
|         | window_next_exec_yyyy | window_next_execution_time の年単位                                                                |
|         | window_next_exec_mm   | window_next_execution_time の月部分                                                                |
|         | window_next_exec_D    | window_next_execution_time のデイパート                                                              |
|         | window_next_exec_HHMM | 時間: window_next_execution_time の分単位                                                            |

## パッチを見逃したインスタンス

このレポートには、前回のメンテナンスウィンドウの実行中にパッチを見逃したインスタンスの詳細が表示されます。

このレポートには、以下が表示されます。

- パッチ ID レベルで欠落しているパッチのデータ。
- パッチの重要度、パッチ適用されていない日数、範囲、リリース日など、パッチと属性が少なくとも 1 つ欠落しているすべてのインスタンスのデータ。

| フィールド名 | データセットフィールド名     | 定義           |
|--------|------------------|--------------|
| レポート日時 | dataset_datetime | レポートが生成された日時 |

| フィールド名            | データセットフィールド名           | 定義                                                                              |
|-------------------|------------------------|---------------------------------------------------------------------------------|
| アカウント ID          | aws_account_id         | AWS インスタンス ID が属するアカウント ID                                                      |
| アカウント名            | account_name           | AWS アカウント名                                                                      |
| 顧客名の親             | customer_name_parent   |                                                                                 |
| 顧客名               | customer_name          |                                                                                 |
| 本番稼働用アカウント        | prod_account           | アカウント名に値「PROD」または「NONPROD」が含まれているかどうかに応じて、AMS prod アカウントまたは non-prod アカウントの識別子。 |
| アカウントステータス        | account_status         | AMS アカウントのステータス                                                                 |
| アカウントの種類          | account_type           |                                                                                 |
|                   | account_sla            | AMS アカウントサービス階層                                                                 |
| インスタンス ID         | instance_id            | EC2 インスタンスの ID                                                                  |
| インスタンス名           | instance_name          | EC2 インスタンスの名前                                                                   |
| インスタンスプラットフォームタイプ | instance_platform_type | オペレーティングシステム (OS) タイプ                                                           |
| インスタンスの状態         | instance_state         | EC2 インスタンスのライフサイクル内の状態                                                          |
| インスタスタグ           | ec2_tags               | Amazon EC2 インスタンス ID に関連付けられたタグ                                                 |
| パッチ ID            | patch_id               | リリースされたパッチの ID                                                                  |

| フィールド名            | データセットフィールド名          | 定義                                  |
|-------------------|-----------------------|-------------------------------------|
| パッチの重要度           | patch_sev             | パブリッシャーあたりのパッチの重要度                  |
| パッチ分類             | patch_class           | パッチパブリッシャーあたりのパッチの分類                |
| パッチリリース日時 (UTC)   | release_dt_utc        | パブリッシャーあたりのパッチのリリース日                |
| パッチのインストール状態      | install_state         | SSM ごとのインスタンスへのパッチのインストール状態         |
| パッチが適用されていない日数    | days_unpatched        | 前回の SSM スキャン以降にインスタンスがパッチ適用されていない日数 |
| パッチが適用されていない日数の範囲 | days_unpatched_bucket | パッチが適用されていない日数のバケット化                |

## バックアップレポート (毎日 )

バックアップレポートは、プライマリリージョンとセカンダリリージョン (該当する場合) を対象としています。バックアップ (成功/失敗) のステータスと、作成されたスナップショットのデータについて説明します。

このレポートには、以下が表示されます。

- バックアップステータス
- 作成されたスナップショットの数
- 復旧ポイント
- バックアッププランとボールド情報

| フィールド名 | データセットフィールド名     | 定義            |
|--------|------------------|---------------|
| レポート日時 | dataset_datetime | レポートが生成された日時。 |

| フィールド名                       | データセットフィールド名         | 定義                                      |
|------------------------------|----------------------|-----------------------------------------|
| アカウント ID                     | aws_account_id       | インスタンス ID が属する AWS アカウント ID             |
| 管理者アカウント ID                  | aws_admin_account_id | 信頼された AWS Organizations アカウントが有効になりました。 |
| アカウント名                       | account_name         | AWS アカウント名                              |
| アカウント SLA                    | account_sla          | AMS アカウントサービスコミットメント                    |
|                              | malz_flag            | MALZ 関連アカウントのフラグ                        |
|                              | malz_role            | MALZ ロール                                |
|                              | access_restrictions  | アクセスが制限されているリージョン                       |
| バックアップスナップショットのスケジュールされた開始日時 | start_by_dt_utc      | スナップショットの開始がスケジュールされているタイムスタンプ          |
| バックアップスナップショットの実際の開始日時       | creation_dt_utc      | スナップショットが実際に開始されるタイムスタンプ                |
| バックアップスナップショットの完了日時          | completion_dt_utc    | スナップショットが完了したときのタイムスタンプ                 |
| バックアップスナップショットの有効期限日時        | expiration_dt_utc    | スナップショットの有効期限が切れるタイムスタンプ                |
| バックアップジョブのステータス              | backup_job_status    | スナップショットの状態                             |
| バックアップタイプ                    | backup_type          | バックアップのタイプ                              |

| フィールド名          | データセットフィールド名         | 定義                                  |
|-----------------|----------------------|-------------------------------------|
| バックアップジョブ ID    | backup_job_id        | バックアップジョブの一意の識別子                    |
| バイト単位のバックアップサイズ | backup_size_in_bytes | バイト単位のバックアップサイズ                     |
| バックアッププラン ARN   | backup_plan_arn      | バックアッププラン ARN                       |
| バックアッププラン ID    | backup_plan_id       | バックアッププランの一意の識別子                    |
| バックアッププラン名      | backup_plan_name     | バックアッププラン名                          |
| バックアッププランのバージョン | backup_plan_version  | バックアッププランのバージョン                     |
| バックアップルール ID    | backup_rule_id       | バックアップルール ID                        |
| バックアップボールド ARN  | backup_vault_arn     | バックアップボールド ARN                      |
| バックアップボールド名     | backup_vault_name    | バックアップボールド名                         |
| IAM ロール ARN     | iam_role_arn         | IAM ロール の ARN                       |
| インスタンス ID       | instance_id          | 一意のインスタンス ID                        |
| インスタンスの状態       | instance_state       | インスタンスの状態                           |
| インスタスタグ         | ec2_tags             | EC2 インスタンス ID に関連付けられたタグ            |
| リソースARN         | resource_arn         | Amazon リソース名                        |
| リソース ID         | resource_id          | 一意のリソース識別子                          |
| リソースリージョン       | resource_region      | リソースのプライマリ (および該当する場合はセカンダリ) リージョン。 |

| フィールド名                    | データセットフィールド名                                   | 定義                                     |
|---------------------------|------------------------------------------------|----------------------------------------|
| リソースタイプ                   | resource_type                                  | リソースのタイプ                               |
| 復旧ポイント ARN                | recovery_point_arn                             | 復旧ポイントの ARN                            |
| 復旧ポイント ID                 | recovery_point_id                              | 復旧ポイントの一意的識別子                          |
| 復旧ポイントのステータス              | recovery_point_status                          | 復旧ポイントのステータス                           |
| 日経過後の復旧ポイントの削除            | recovery_point_delete_after_days               | 日数経過後の復旧ポイントの削除                        |
| 復旧ポイントが数日後にコールドストレージに移動する | recovery_point_move_to_cold_storage_after_days | バックアップスナップショットがコールドストレージに移動された完了日からの日数 |
| 復旧ポイントの暗号化ステータス           | recovery_point_is_encrypted                    | 復旧ポイントの暗号化ステータス                        |
| 復旧ポイント暗号化キー ARN           | recovery_point_encryption_key_arn              | 復旧ポイント暗号化キー ARN                        |
| スタック ID                   | stack_id                                       | Cloudformation スタックの一意的識別子             |
| スタックの名前                   | stack_name                                     | スタックの名前                                |
| タグ: AMS デフォルトパッチグループ      | tag_ams_default_patch_group                    | タグ値: AMS デフォルトパッチグループ                  |
| タグ: アプリ ID                | tag_app_id                                     | タグ値: アプリ ID                            |
| タグ: アプリ名                  | tag_app_name                                   | タグ値: アプリケーション名                         |
| タグ: Backup                | tag_backup                                     | タグ値: Backup                            |
| タグ: Compliance Framework  | tag_compliance_framework                       | タグ値: Compliance Framework              |
| タグ: Cost Center           | tag_cost_center                                | タグ値: コストセンター                           |



| フィールド名                 | データセットフィールド名            | 定義                 |
|------------------------|-------------------------|--------------------|
| タグ: Customer           | tag_customer            | タグ値: Customer      |
| タグ: データ分類              | tag_data_classification | タグ値: データ分類         |
| タグ: 環境タイプ              | tag_environment_type    | タグ値: 環境タイプ         |
| タグ: Hours of Operation | tag_hours_of_operation  | タグ値: オペレーション時間     |
| タグ: Owner Team         | tag_owner_team          | タグ値: 所有者チーム        |
| タグ: 所有者チームの E メール      | tag_owner_team_email    | タグ値: 所有者チームの E メール |
| タグ: Patch Group        | tag_patch_group         | タグ値: パッチグループ       |
| タグ: Support Priority   | tag_support_priority    | タグ値: サポート優先度       |
| ボリュームの状態               | volume_state            | ボリュームの状態           |

## インシデントレポート (毎週)

このレポートには、インシデントの集計リストと、優先度、重要度、最新のステータスが表示されます。

- マネージドアカウントのインシデントに分類されるサポートケースのデータ
- マネージドアカウントのインシデントメトリクスを視覚化するために必要なインシデント情報
- すべてのインシデントのインシデントカテゴリと修復ステータスに関するデータ

週次インシデントレポートでは、視覚化とデータの両方を使用できます。

- 視覚化には、レポートのページからアカウントの AMS コンソールからアクセスできます。
- 次のスキーマを持つデータセットには、 マネージドアカウントの S3 バケットからアクセスできます。
- 指定された日付フィールドを使用して、インシデントが作成または解決された月、四半期、週、日に基づいてインシデントをフィルタリングします。

| フィールド名      | データセットフィールド名         | 定義                                                                                                                                     |
|-------------|----------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| レポート日時      | dataset_datetime     | レポートが生成された日時。                                                                                                                          |
| アカウント ID    | aws_account_id       | AWS インシデントが属するアカウント ID。                                                                                                                |
| 管理者アカウント ID | aws_admin_account_id | 信頼された AWS Organizations アカウントが有効になりました。                                                                                                |
| アカウント名      | account_name         | AWS アカウント名。                                                                                                                            |
| ケース ID      | case_id              | インシデントの ID。                                                                                                                            |
| 作成された月      | created_month        | インシデントが作成された月。                                                                                                                         |
| 優先度         | priority             | インシデントの優先度。                                                                                                                            |
| 緊急度         | severity             | インシデントの重要度。                                                                                                                            |
| ステータス       | ステータス                | インシデントのステータス。                                                                                                                          |
| カテゴリ        | yuma_category        | インシデントのカテゴリ。                                                                                                                           |
| 作成日         | created_day          | インシデントが YYYY-MM-DD 形式で作成された日。                                                                                                          |
| 作成された週      | created_wk           | インシデントが YYYY-WW 形式で作成された週。日曜日から土曜日は、1 週間の最初と最後にカウントされます。週は 01~52 です。01 週は、常に年の最初の日を含む週です。例えば、2023-12-31 と 2024-01-01 は 2024 年 1 月の週です。 |

| フィールド名        | データセットフィールド名  | 定義                                                                                                                                              |
|---------------|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| 作成された四半期      | created_qtr   | インシデントが YYYY-Q 形式で作成された四半期。01/01 ~ 03/31 は Q1 として定義されます。                                                                                        |
| 解決日           | resolved_day  | インシデントが YYYY-MM-DD 形式で解決された日。                                                                                                                   |
| 解決された週        | resolved_wk   | インシデントが YYYY-WW 形式で解決された週。日曜日から土曜日は、1 週間の最初と最後にカウントされます。週は 01 ~ 52 です。01 週は、常に年の最初の日を含む週です。例を挙げると、2023-12-31 と 2024-01-01 は 2024 年 1 月 1 日の週です。 |
| 解決月           | 解決済み_月        | インシデントが YYYY-MM 形式で解決された月。                                                                                                                      |
| 解決された四半期      | resolved_qtr  | インシデントが YYYY-Q 形式で解決された四半期。01/01 ~ 03/31 は Q1 として定義されます。                                                                                        |
| 作成されたグループ化ルール | grouping_rule | インシデントに適用されるグループ化ルール。「no_grouping」または「instance_grouping」のいずれか。                                                                                  |
| インスタンス ID     | instance_ids  | インシデントに関連付けられたインスタンス。                                                                                                                           |

| フィールド名    | データセットフィールド名     | 定義                                                                                       |
|-----------|------------------|------------------------------------------------------------------------------------------|
| アラートの数    | number_of_alerts | そのインシデントに関連付けられたアラートの数。グループ化を有効にしている場合、この数は 1 より大きい場合があります。グループ化が有効になっていない場合、常に 1 になります。 |
| 作成日       | created_at       | インシデントが作成されたタイムスタンプ。                                                                     |
| アラーム ARNs | alarm_arns       | インシデントに関連付けられたアラームの Amazon リソースネーム (「arn」)。                                              |
| 関連するアラーム  | related_alarms   | インシデントに関連付けられたすべてのアラームの人間が読み取れる名前。                                                       |

## 請求レポート (毎月)

### 請求料金の詳細

このレポートには、リンクされたアカウントとそれぞれの AWS サービスでの AMS 請求料金の詳細が表示されます。

このレポートには、以下が表示されます。

- AMS サービスレベルの料金、引き上げ率、アカウントレベルの AMS サービス階層、AMS 料金に関するデータ。
- リンクされたアカウントと AWS 使用料に関するデータ。

**⚠ Important**

月別請求レポートは、Management Payer Account (MPA) または定義された Charge Account でのみ使用できます。これらは、AMS 月額請求書が送信されるアカウントです。これらのアカウントが見つからない場合は、Cloud Service Delivery Manager (CSDM) にお問い合わせください。

| フィールド名         | データセットフィールド名          | 定義                                                       |
|----------------|-----------------------|----------------------------------------------------------|
| 請求日            | date                  | 請求されるサービスの月と年                                            |
| 支払者アカウント ID    | payer_account_id      | AMS 料金の支払いを担当するアカウントを識別する 12 桁の ID                       |
| リンクされたアカウント ID | linked_account_id     | 拡張を生成するサービスを消費する AMS アカウントを識別する 12 桁の ID                 |
| AWS サービス名      | product_name          | 使用された AWS サービス                                           |
| AWS 料金         | aws_charges           | AWS サービス名での AWS サービス名の AWS 料金                            |
| 料金プラン          | pricing_plan          | リンクされたアカウントに関連付けられた料金プラン                                 |
| AMS サービスグループ   | tier_uplifting_groups | 引き上げ率を決定する AMS サービスグループコード                               |
| アップリフト比率       | uplift_percent        | pricing_plan、SLA、および AWS サービスに基づく引き上げ率 (10 進 V.WXYZ として) |
| 調整済み AWS 料金    | 調整済み_aws_usage        | AWS AMS 用に調整された使用量                                       |

| フィールド名                | データセットフィールド名                        | 定義                                                                                                                               |
|-----------------------|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| 引き上げられた AWS 料金        | uplifted_aws_charges                | AMS に対して請求される AWS 料金の割合、 $\text{adjusted\_aws\_charges} * \text{uplift\_percent}$                                                |
| インスタンス EC2 RDS の使用    | instances_ec2_rds_spend             | EC2 インスタンスと RDS インスタンスの使用                                                                                                        |
| リザーブドインスタンス料金         | ris_charges                         | リザーブドインスタンスの料金                                                                                                                   |
| 引き上げられたリザーブドインスタンス料金  | uplifted_ris                        | AMS に対して請求されるリザーブドインスタンス料金の割合、 $\text{ris\_charges} * \text{uplift\_percent}$                                                    |
| Savings Plan sの料金     | sp_charges                          | SavingsPlan の使用料金                                                                                                                |
| Savings Planの引き上げ料金   | uplifted_sp                         | AMS に対して請求される Savings Plans 料金の割合、 $\text{sp\_charges} * \text{uplift\_percent}$                                                 |
| AMS 料金                | ams_charges                         | 製品に対する合計 ams 料金、 $\text{uplifted\_aws\_charges} + \text{instance\_ec2\_rds\_spend} + \text{uplifted\_ris} + \text{uplifted\_sp}$ |
| 按分された最低料金             | 按分_最小                               | 契約上の最小値を満たすために請求される金額                                                                                                            |
| リンクされたアカウントの合計 AMS 料金 | linked_account_total<br>ams_charges | linked_account のすべての料金の合計                                                                                                        |
| 支払者アカウントの合計 AMS 料金    | payer_account_total<br>ams_charges  | 支払者アカウントのすべての料金の合計                                                                                                               |

| フィールド名                        | データセットフィールド名      | 定義                                 |
|-------------------------------|-------------------|------------------------------------|
| 最小料金                          | 最小料金              | AMS 最小料金 (該当する場合)                  |
| リザーブドインスタンスと Savings Plan の割引 | adj_ri_sp_charges | RI/SP 料金に適用される RI/SP 割引 (特定の状況で適用) |

## 集計レポート

集約型セルフサービスレポート (SSR) では、組織レベルで集約された既存のセルフサービスレポートをクロスアカウントで表示できます。これにより、内の AMS 管理下にあるすべてのアカウントで、パッチコンプライアンス、バックアップカバレッジ、インシデントなどの主要な運用メトリクスを可視化できます AWS Organizations。

集約 SSR は、AWS Managed Services AWS リージョン が利用可能なすべての商用 で利用できます。使用可能なリージョンの完全なリストについては、[リージョン表](#)を参照してください。

### 集計レポートを有効にする

AWS Organizations [管理アカウント](#)から集約された SSR を管理する必要があります。管理アカウントは、組織の作成に使用した AWS アカウントです。

AMS にオンボードされている AWS Organizations 管理アカウントの集約 SSR を有効にするには、AMS コンソールにアクセスしてレポートに移動します。top-right-hand隅にある Organization Access を選択して、[AWS Managed Services Console: Organization View](#) ペインを開きます。このペインから、集約 SSR 機能を管理できます。

AWS Organizations AMS にオンボーディングされていない 管理アカウントは、AMS コンソールにアクセスできません。AMS にオンボーディングされていない AWS Organizations 管理アカウントの集約 SSR を有効にするには、まず を認証し AWS アカウント、[AWS コンソール](#)に移動してマネージドサービスを検索します。これにより、AMS Marketing ページが開きます。このページで、ナビゲーションバーの Organization Access リンクを選択して、AWS Managed Services コンソール「Organization View」を開き、集約 SSR 機能を管理できます。

[AWS Managed Services Console: Organization View](#) に初めてアクセスする場合は、次の手順を実行します。

1. まだセットアップしていない場合は AWS Organizations、コンソールから有効化 AWS Organizations を選択します。セットアップの詳細については AWS Organizations、[AWS Organizations 「ユーザーガイド」](#) を参照してください。すでに を使用している場合は、このステップをスキップできます AWS Organizations。
2. 集約セルフサービスレポートサービスを有効にするには、コンソールで信頼されたアクセスを有効にするを選択します。
3. ( オプション) 委任管理者を登録して、組織ビューの読み取りアクセス権を付与します。

## 集約レポートを委任管理者として表示する

委任管理者は、集計レポートへの読み取りアクセス権を持つことを選択したアカウントです。委任管理者は、AMS にオンボーディングされたアカウントであり、集計レポートへの読み取りアクセス権を持つ唯一のアカウントである必要があります。

委任された管理者を選択するには、AWS Managed Servicesコンソール: Organization View のステップ 3 でアカウント ID を入力します。一度に登録できる委任管理者アカウントは 1 つだけです。委任管理者アカウントは AMS 管理アカウントである必要があります。

委任管理者アカウントを更新するには、[AWS Managed Servicesコンソール: Organization View](#) に移動し、委任管理者の削除を選択します。コンソールでは、委任管理者として登録する新しいアカウント ID を挿入するように求められます。

## 集計レポートの読み取り

委任管理者を登録せず、AWS Organizations 管理アカウントが AMS にオンボーディングされている場合、AWS Organizations 管理アカウントはデフォルトで集約レポートへの読み取りアクセスを取得します。AWS Organizations 管理アカウントが AMS によって管理されていない場合は、集約レポートへの読み取りアクセス権を持つ委任管理者アカウントを選択する必要があります。

AMS にオンボードされた 1 つのアカウントのみが、AWS Organizations 管理アカウントまたは登録された委任管理者のいずれかの集約レポートへの読み取りアクセス権を持ちます。組織内の (および AMS にオンボーディングされた) 他のすべてのメンバーアカウントは、個々のアカウントの単一アカウントレポートにのみアクセスできます。

集約 SSR を有効にしたら、[レポート](#) に移動します。既存のセルフサービスレポートはすべてこのセクションに表示され、青いタグは集計されたことを示します。集計レポートへの読み取りアクセスを選択したアカウントから AMS コンソールにアクセスする必要があることに注意してください。これは AWS Organizations 管理アカウントまたは委任管理者アカウントです。



集約 SSR を有効にすると、集約レポートは次のレポートサイクル以降から使用できます。

## 集計レポートを無効にする

集約 SSR を無効にするには、[AWS Managed Servicesコンソール: Organization View](#) を開きます。信頼されたアクセスを無効にするを選択します。集約 SSR の信頼されたアクセスを無効にすると、AMS セルフサービスレポートは、アカウント間で組織レベルで集約されなくなります。また、非アクティブ化は、次のレポートサイクル以降も有効になることに注意してください。

集約 SSR を無効にすると、AMS コンソールのレポートがシングルアカウントレポートとして表示されるまで待機します。この遅延は、機能の非アクティブ化が次のレポートサイクル以降有効になるために発生します。

## AMS セルフサービスレポートダッシュボード

AMS セルフサービスレポートには、[リソースタグ付けダッシュボード](#)と [セキュリティ設定ルールダッシュボード](#) の 2 つのダッシュボードがあります。

### リソースタグ付けダッシュボード

AMS Resource Tagger Dashboard には、Resource Tagger でサポートされているリソースに関する詳細情報と、Resource Tagger がそれらのリソースに適用するように設定されたタグの現在のステータスが表示されます。

#### リソースタイプ別のリソースタグ付けカバレッジ

このデータセットは、Resource Tagger によって管理されるタグを持つリソースのリストで構成されます。

リソースタイプ別のリソースカバレッジは、次のメトリクスを記述する 4 つの折れ線グラフとして視覚化されます。

- リソース数: リソースタイプ別の、リージョン内のリソースの合計数。
- マネージドタグがないリソース: マネージドタグを必要とするが Resource Tagger によってタグ付けされていない、リソースタイプ別のリージョン内のリソースの合計数。
- アンマネージドリソース: Resource Tagger によってマネージドタグが適用されていない、リソースタイプ別のリージョン内のリソースの合計数。これは通常、これらのリソースが Resource Tagger 設定と一致しないか、設定から明示的に除外されることを意味します。

- マネージドリソース: アンマネージドリソースメトリクス (リソース数 - アンマネージドリソース) に対応します。

次の表に、このレポートによって提供されるデータを示します。

| フィールド名                      | データセットフィールド名                        | 定義                                                                                  |
|-----------------------------|-------------------------------------|-------------------------------------------------------------------------------------|
| レポート日時                      | dataset_datetime                    | レポートが生成された日時 (UTC 時間)                                                               |
| AWS アカウント ID                | aws_account_id                      | AWS アカウント ID                                                                        |
| 管理者アカウント ID                 | aws_admin_account_id                | 信頼された AWS Organizations アカウントが有効になりました。                                             |
| リージョン                       | region                              | AWS リージョン                                                                           |
| リソースタイプ                     | resource_type                       | このフィールドはリソースのタイプを識別します。Resource Tagger でサポートされているリソースタイプのみが含まれます。                   |
| リソース数                       | resource_count                      | このリージョンにデプロイされた (指定されたリソースタイプの) リソースの数。                                             |
| ResourcesMissingManagedTags | resource_missing_managed_tags_count | 設定プロファイルに従ってマネージドタグを必要とするが、Resource Tagger によってまだタグ付けされていないリソース (指定されたリソースタイプの) の数。 |
| UnmanagedResources          | unmanaged_resource_count            | Resource Tagger によって管理タグが適用されていないリソースの数 (指定されたリソース                                  |

| フィールド名 | データセットフィールド名 | 定義                                                                   |
|--------|--------------|----------------------------------------------------------------------|
|        |              | スタンプ)。通常、これらのリソースは Resource Tagger 設定ブロックと一致しないか、設定ブロックから明示的に除外されます。 |

## Resource Tagger 設定ルールのコンプライアンス

このデータセットは AWS リージョン、リソースタイプ別の 内のリソースのリストで構成され、特定の設定プロファイルが適用されます。これは折れ線グラフとして視覚化されます。

次の表に、このレポートによって提供されるデータを示します。

| フィールド名       | データセットフィールド名             | 定義                                                                |
|--------------|--------------------------|-------------------------------------------------------------------|
| レポート日時       | dataset_datetime         | レポートが生成された日時 (UTC 時間)                                             |
| AWS アカウント ID | aws_account_id           | AWS アカウント ID                                                      |
| 管理者アカウント ID  | aws_admin_account_id     | 信頼された AWS Organizations アカウントが有効になりました。                           |
| リージョン        | region                   | AWS リージョン                                                         |
| リソースタイプ      | resource_type            | このフィールドはリソースのタイプを識別します。Resource Tagger でサポートされているリソースタイプのみが含まれます。 |
| 設定プロファイル ID  | configuration_profile_id | Resource Tagger 設定プロファイルの ID。設定プロファイルは、リソースのタグ付けに使用されるポリシーとルー     |

| フィールド名                | データセットフィールド名   | 定義                                                                                                                       |
|-----------------------|----------------|--------------------------------------------------------------------------------------------------------------------------|
|                       |                | ルを定義するために使用されます。                                                                                                         |
| MatchingResourceCount | resource_count | Resource Tagger 設定プロファイル ID に一致するリソース (指定されたリソースタイプのもの) の数。リソースが設定プロファイルと一致するには、プロファイルを有効にし、リソースがプロファイルのルールと一致する必要があります。 |

## Resource Tagger 非準拠のリソース

このデータセットは、単一の Resource Tagger 設定に準拠していないリソースのリストで構成されます。このデータは、リソースコンプライアンスの日次スナップショットであり、これらのレポートが顧客アカウントに配信された時点の顧客リソースの状態を示します (履歴ビューはありません)。これは、特定の設定に対して苦情ではないリソースで構成されるピボットテーブルとして視覚化されます。

次の表に、このレポートによって提供されるデータを示します。

| フィールド名       | データセットフィールド名         | 定義                                      |
|--------------|----------------------|-----------------------------------------|
| レポート日時       | dataset_datetime     | レポートが生成された日時 (UTC 時間)                   |
| AWS アカウント ID | aws_account_id       | AWS アカウント ID                            |
| 管理者アカウント ID  | aws_admin_account_id | 信頼された AWS Organizations アカウントが有効になりました。 |
| リージョン        | region               | AWS リージョン                               |

| フィールド名                | データセットフィールド名             | 定義                                                                            |
|-----------------------|--------------------------|-------------------------------------------------------------------------------|
| リソースタイプ               | resource_type            | このフィールドはリソースのタイプを識別します。Resource Tagger でサポートされているリソースタイプのみが含まれます。             |
| Resource ID (リソース ID) | resource_id              | Resource Tagger でサポートされているリソースの一意的識別子。                                        |
| カバレッジ状態               | coverage_state           | このフィールドは、リソースが Resource Tagger 設定 ID で設定されたとおりにタグ付けされているかどうかを示します。            |
| 設定プロファイル ID           | configuration_profile_id | Resource Tagger 設定プロファイルの ID。設定プロファイルは、リソースのタグ付けに使用されるポリシーとルールを定義するために使用されます。 |

## セキュリティ設定ルールダッシュボード

Security Config Rules Dashboard では、AMS アカウントのリソースと AWS Config ルールのコンプライアンスについて詳しく説明します。ルールの重要度でレポートをフィルタリングして、最も重要な結果に優先順位を付けることができます。次の表に、このレポートによって提供されるデータを示します。

| フィールド名       | データセットフィールド名 | 定義                        |
|--------------|--------------|---------------------------|
| AWS アカウント ID | AWS アカウント ID | 関連するリソースに関連付けられたアカウント ID。 |

| フィールド名                  | データセットフィールド名          | 定義                                                                                                      |
|-------------------------|-----------------------|---------------------------------------------------------------------------------------------------------|
| 管理者アカウント ID             | aws_admin_account_id  | 信頼された AWS Organizations アカウントが有効になりました。                                                                 |
| レポート日時                  | レポートの日付               | レポートが生成された日時。                                                                                           |
| customer_name           | 顧客名                   | 顧客名。                                                                                                    |
| account_name            | アカウント名                | アカウント ID に関連付けられた名前                                                                                     |
| resource_id             | Resource ID (リソース ID) | リソースの識別子。                                                                                               |
| resource_region         | リソースリージョン             | リソース AWS リージョン が配置されている。                                                                                |
| resource_type           | リソースタイプ               | AWS のサービス または リソースタイプ。                                                                                  |
| resource_name           | リソース名                 | リソースの名前。                                                                                                |
| resource_ams_flag       | リソース AMS フラグ          | リソースが AMS 所有の場合、このフラグは TRUE に設定されます。リソースが顧客所有の場合、このフラグは FALSE に設定されます。所有権が不明な場合、このフラグは UNKNOWN に設定されます。 |
| config_rule             | Config ルール            | 設定ルールのカスタマイズ不可能な名前。                                                                                     |
| config_rule_description | Config ルールの説明         | 設定ルールの説明。                                                                                               |

| フィールド名                  | データセットフィールド名 | 定義                                                                                                     |
|-------------------------|--------------|--------------------------------------------------------------------------------------------------------|
| source_identifier       | ソース識別子       | マネージド設定ルールの一意の識別子で、カスタム設定ルールの識別子はありません。                                                                |
| Compliance_flag         | コンプライアンスフラグ  | リソースが設定ルールに準拠しているかどうかを示します。                                                                            |
| rule_type               | ルールタイプ       | ルールが事前定義かカスタムビルドかを示します。                                                                                |
| exception_flag          | 例外フラグ        | リソース例外フラグは、非準拠リソースに対するリスク承諾を示します。リソース例外フラグがリソースに対して TRUE の場合、リソースは除外されます。例外フラグが NULL の場合、リソースは除外されません。 |
| cal_dt                  | 日付           | ルールの評価日。                                                                                               |
| remediation_description | 修復の説明        | ルールコンプライアンスを修復する方法の説明。                                                                                 |
| severity                | 緊急度          | Config ルールの重要度は、コンプライアンス違反の影響を示します。                                                                    |
| customer_action         | カスタマーアクション   | ルールを修正するために必要なアクション。                                                                                   |
| 推奨事項                    | 推奨事項         | 設定ルールがチェックする内容の説明。                                                                                     |

| フィールド名 | データセットフィールド名 | 定義                                     |
|--------|--------------|----------------------------------------|
| 修復カテゴリ | 修復カテゴリ       | このルールが非準拠になったときに AMS が実行するデフォルトのアクション。 |

## データ保持ポリシー

AMS SSR には、報告された期間後にレポートごとにデータ保持ポリシーがあり、データは消去され、使用できなくなります。

| レポート名                          | データ保持 SSR コンソール | データ保持 SSR S3 バケット |
|--------------------------------|-----------------|-------------------|
| インスタンスの詳細の概要<br>(パッチオーケストレーター) | 2 か月            | 2 年               |
| パッチの詳細                         | 2 か月            | 2 年               |
| メンテナンスウィンドウの実行中にパッチを見逃したインスタンス | 2 か月            | 2 年               |
| AMS 請求料金の詳細                    | 2 年             | 2 年               |
| 日次バックアップレポート                   | 1 か月            | 2 年               |
| 週次インシデントレポート                   | 2 か月            | 2 年               |
| セキュリティ設定ルールダッシュボード             | 3 か月            | 2 年               |
| Resource Tagger ダッシュボード        | 1 年             | 2 年               |



## SSR からのオフボード

SSR サービスからオフボードするには、AMS コンソールを使用してサービスリクエスト (SR) を作成します。SR を送信すると、AMS オペレーションエンジニアが SSR からのオフボードを支援します。SR で、オフボードする理由を入力します。

アカウントをオフボードしてリソースのクリーンアップを実行するには、AMS コンソールを使用して SR を作成します。SR を送信すると、AMS オペレーションエンジニアが SSR Amazon S3 バケットの削除を支援します。

AMS からオフボードすると、AMS SSR コンソールから自動的にオフボードされます。AMS は、アカウントへのデータの送信を自動的に停止します。AMS は、オフボーディングプロセスの一環として SSR S3 バケットを削除します。

# AMS でのインシデントレポート、サービスリクエスト、請求に関する質問

## トピック

- [インシデント管理](#)
- [サービスリクエスト管理](#)
- [請求に関する質問](#)

AWS Managed Services (AMS) では、AMS コンソールを使用して、運用上の問題やリクエストに関するヘルプをいつでもリクエストできます。AMS オペレーションエンジニアは、選択したアカウントサービス階層 (プラス、プレミアム) に応じて、レスポンスタイムのサービスレベルアグリーメント (SLAs) とサービスレベル目標 (SLOs) を使用して、インシデントとサービスリクエストに 24 時間 365 日対応できます。AMS オペレーションエンジニアは、同じメカニズムを使用して重要なアラートや質問を事前に通知します。

## インシデント管理

### トピック

- [インシデント管理とは？](#)
- [インシデント管理サービスのコミットメント](#)
- [インシデント管理の例](#)

インシデントは、AWS Managed Services (AMS) またはユーザーによって決定される、マネージド環境に影響を与える AWS のサービス パフォーマンスの問題です。AMS チームによって識別されたインシデントは、最初に「イベント」として受信されます。これは、モニタリングによってキャプチャされたシステム状態の変化です。設定されたしきい値を超えると、イベントはアラートとも呼ばれるアラームをトリガーします。AMS オペレーションチームは、イベントが影響を受けていないか、インシデント (サービスの中断または低下)、または問題 (1 つ以上の解決されたインシデントの根本的な根本原因) であるかを判断します。

AMS チームは、サポート センターを通じて、または [AWS サポート API](#) とサービスコードを使用してプログラムで特定されたインシデントも受け取ります `sentinel-report-incident`。

インシデントが AMS オペレーションチームによって受信されると、インシデントがサービスリクエストとして適切に分類されないようにレビューされます。サービスリクエストとして分類する必要がある場合は、すぐに再分類され、AMS サービスリクエストチームが引き継ぎ、お客様に通知されます。受信側オペレーターがインシデントを解決できる場合、インシデントを解決するためのステップがすぐに実行されます。AMS オペレーターは、解決策について社内ドキュメントを参照し、必要に応じて、インシデントが解決されるまでインシデントを他のサポートリソースにエスカレーションします。インシデント解決プロセスの各ステップで通知を受けるには、CC Emails オプションを必ず入力し、フェデレーションで接続する場合は、AMS が送信する E メールリンクに従う前にログインします。解決後、AMS オペレーションチームはインシデントと解決を今後の使用のために文書化します。

インシデント解決にインフラストラクチャの変更が必要な場合は、セキュリティレビューが必要になる場合があります。セキュリティレビューが必要なインフラストラクチャの変更には、IAM、リソースベースのポリシー、またはリスク承認に関連する変更が含まれます。これらのタイプのインシデントでは、変更を行う前に AMS オペレーションエンジニアが RFC を作成する必要があり、その RFC に対する承認が必要です。例えば、インシデント解決で IAM ポリシーの更新が必要な場合、AMS セキュリティレビューが行われ、AMS オペレーションエンジニアが Management | Advanced スタックコンポーネント | Identity and Access Management (IAM) | Update entity or policy change type (ct-27tuth19k52b4) を使用して RFC を作成し、RFC の承認を待ってから次に進みます。

#### Note

AMS では、RFC 承認の追加ステップなしでインフラストラクチャの変更が必要なインシデント解決が可能になりました。インシデントの解決に必要な変更がセキュリティレビューを必要としない場合 (変更は IAM、リソースベースのポリシー、またはリスク承認に関連しない)、AMS は、RFC で別途承認することなく、インシデントで受け取った承認に基づいて変更を行うことができます。

インシデント管理用語の定義については、[「AMS の主要な用語」](#)を参照してください。

インシデントのエスカレーションパスを理解するには、[「Getting help」](#)を参照してください。

インシデントに対する AMS レスポンスの説明については、[「AMS インシデント対応」](#)を参照してください。

## インシデント管理とは？

インシデント管理は、AMS がアクティブなインシデントの記録、対応、進捗状況の伝達、通知を行うために使用するプロセスです。

インシデント管理プロセスの目的は、マネージドサービスの通常の運用をできるだけ早く復元し、ビジネスへの影響を最小限に抑え、すべての関係者に最新情報を確実に提供することです。

インシデントの例としては、ネットワーク接続の損失や低下、応答しないプロセスや API、スケジュールされたタスクが実行されていない (バックアップの失敗など) などがあります (ただし、これらに限定されません)。

次の図は、AMS に報告されたインシデントのワークフローを示しています。

この図は、AMS によって報告されるインシデントのワークフローを示しています。

### インシデントの優先度

AWS サポートセンター、コンソール、またはサポート API (SAPI) で作成されたインシデントの分類は、AMS コンソールで作成されたインシデントとは異なります。

- 低: AWS または AMS リソースに関連するビジネスサービスまたはアプリケーションの重要ではない機能が影響を受けます。
- 中: AWS および/または AMS リソースに関連するビジネスサービスまたはアプリケーションが中程度の影響を受け、機能が低下しています。
- 高: ビジネスに大きな影響を与えます。AWS や AMS リソースに関連するアプリケーションの重要な機能は利用できません。本番稼働システムに影響を与える最も重要な停止用に予約されています。

#### Note

AWS サポートコンソールには、3 つの AMS レベルに変換する 5 つのレベルのインシデント優先度が用意されています。

## 問題とインシデント

AMS は、インシデントによってより大きな欠陥や設定ミスが明らかになり、再発する可能性がある  
と判断した場合、単なるインシデントではなく問題と見なされます。このような場合、AMS は問題  
の分析を行い、問題を解決するための提案を提供します。

## インシデント管理サービスのコミットメント

### インシデント管理サービスのコミットメント

| イベントまたはアクション                                                                                                                                                   | サービスコミットメントの測定                                                                                                                                                                                                                                                                                    |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>ケース 1: 既知の影響があるイベントが生成されます。AMS はインシデントを開き、通知します。</p> <p>ケース 2: AMS から連絡があり、イベントの影響を確認します。イベントがインシデントであることを確認します。</p> <p>ケース 3: 問題に気づき、インシデントレポートを送信します。</p> | <p>インシデント対応とインシデント解決のクロックは、次の場合に開始されます。</p> <p>ケース 1: AMS はインシデントを作成します。</p> <p>ケース 2: アラートがインシデントであることを確認します。</p> <p>ケース 3: インシデントを送信します。</p> <p>サービスコミットメントは、作成されたインシデントの優先度によって異なります。</p>                                                                                                      |
| <p>インシデントを送信すると、AMS は確認応答を送信します。</p> <p>AMS がユーザーに代わってインシデントを作成する場合、別のインシデント対応は送信されません。</p>                                                                    | <p>インシデント解決のクロックはティックを継続します。</p> <p>AMS がインシデント確認を送信すると、インシデント対応時間のクロックが停止します。</p> <div><p> <b>Note</b></p><p>入力の待機にかかった時間は、インシデント解決時間の計算から除外されます。AMS が作成するインシデントの場合、最初の応答時間は、最初のインシデント通知が作成された時刻です。</p></div> |

| イベントまたはアクション                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | サービスコミットメントの測定                                                                                                                         |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <p>問題のリソース/サービスについて、AMS はヘルスをチェックして以下を確認します。</p> <ul style="list-style-type: none"><li>AMS が検出したイベントまたはお客様が送信したインシデントがインシデントに該当する、および</li><li>インシデントの優先順位が正しく設定されている</li></ul> <p>送信したインシデントの優先順位が正しくない場合、AMS はそのインシデントの優先順位を再設定します。AMS がインシデントの優先度を変更すると、優先度の変更の根拠とともに通知が送信されます。場合によっては、送信した問題が、原因によってはインシデントとして認定されないことがあります。このような場合、AMS はインシデントを終了し、その理由を説明する通知を送信します。イベントの分類に関係なく、AMS は必要に応じてサポートします。</p> <p>インシデント分類のルールについては、「」を参照してください<a href="#">インシデントの優先度</a>。</p> | <p>インシデントの優先度に変更された場合、新しい優先度のサービスコミットメントが適用されます。クロックはティックを継続します。インシデントの定義を満たさないためにインシデントがクローズされた場合、サービスコミットメントは適用されません。クロックは停止します。</p> |

| イベントまたはアクション                                                                                                                                                                                                                                                                                                                                                                                                         | サービスコミットメントの測定                                                                                                                                                     |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>AMS はインシデントに取り組み、サービスコミットメント内で解決します。場合によっては、利用できないスタック (複数可) またはリソース (複数可) をタイムリーに解決できないと AMS が判断した場合、AMS は解決のオプションとしてインフラストラクチャの復元を提供します。インフラストラクチャの復元では、影響を受けるスタックのテンプレート (複数可) に基づいて既存のスタック (複数可) を再デプロイし、ユーザーが特に指定しない限り、最後の既知の復元ポイント (EBS/RDS スナップショット) に基づいてデータ復元を開始します。個々の EC2 インスタンスのエフェメラルデータは失われます。AWS の推奨に従ってインフラストラクチャの復元を許可しない場合、関連する Incident Resolution Time Service コミットメントのサービスクレジットは付与されません。</p> | <p>クロックは、次の場合に停止します。</p> <ul style="list-style-type: none"><li>AMS が、そのインシデントに関連するすべての使用できないサービスまたはリソースを利用可能な状態に復元した場合、または</li><li>インフラストラクチャの復元が開始されます。</li></ul> |
| <p>AMS では、事前に定義され、承認されたアクションがない限り、インシデント解決作業を進めるための明確化やアクティビティが必要になることがあります。その結果、インシデントを解決するために AMS とユーザーの間で通信が行われます。</p>                                                                                                                                                                                                                                                                                            | <p>クロックは、AMS がユーザーからの応答またはアクションを待っているときに停止します。</p> <p>クロックは、AMS がユーザーからレスポンスを受け取るか、AMS が必要とするアクションが完了したときに再起動します。</p>                                              |

**Note**

サービスコミットメントの完全なリストについては、[AMS サービスレベルアグリーメント](#)をダウンロードしてください。

## インシデント管理の例

インシデント管理の例。

トピック

- [インシデントテスト](#)
- [インシデントの報告](#)
- [インシデントのモニタリングと更新](#)
- [AWS サポート API を使用したインシデントの管理](#)
- [AMS で生成されたインシデントへの対応](#)

次の例では、AMS コンソールを使用してインシデントを送信する方法について説明します。送信後、AMS チームはお客様と協力して、サービスレベルアグリーメント (SLA) に従ってインシデントを解決します。

### インシデントテスト

AMS インシデントの送信をテストするときは、件名テキストに AMSTestNoOpsActionRequired を含める必要があります。このフラグは、インシデントの送信がテスト専用であることを AMS に知らせます。AMS オペレーションエンジニアはそのフラグを確認すると、インシデント送信に応答しません。

### インシデントの報告

AMS コンソールを使用してインシデントを報告します。新しい問題や質問ごとに新しいインシデントを作成することが重要です。古い問い合わせに関連するケースを開くときは、以前のやり取りを参照できるように、関連するケース番号を含めると便利です。

#### Note

ケースコレスポンスが元の問題から逸脱した場合、AMS オペレーターから新しいインシデントの報告を求められることがあります。

AMS コンソールを使用してインシデントを報告するには:

1. 左側のナビゲーションから、Incidents を選択します。



インシデントリストが開きます。

インシデントリストが空の場合、フィルターをクリアオプションはフィルターを Any ステータスにリセットします。

電話またはチャットを使用する場合は、サポートセンターでインシデントの作成をクリックして、サポートセンターコンソールでインシデントの作成ページを開き、AMS サービスタイプが自動的に入力されます。

 Important

- 応答を改善するために、 で開始された通話 サポート が記録されます。通話が切断された場合は、サポートセンターのケースを通じてコールバックする必要があります。コールバックするメカニズム AWS はありません。
- 電話とチャットのサポートは、RFC やセキュリティの問題ではなく、サポートケース、インシデント、サービスリクエストを支援するように設計されています。
- RFC の問題については、関連する RFC の詳細ページでコレスポンスオプションを使用し、AMS エンジニアに連絡してください。
- セキュリティ上の問題については、優先度の高い (P1 または P2) サポートケースを作成します。ライブチャット機能は、セキュリティイベント用ではありません。

2. 既存のインシデントを検索する場合は、ドロップダウンリストからインシデントステータスフィルターを選択します。

- まだ解決されていないすべてのインシデント。
- まだ割り当てられていない新しいインシデント。
- 割り当てられたインシデント。
- 再開したインシデント。
- 割り当てられた複雑なインシデント。

- 次のステップの前にフィードバックが必要なインシデント。
- 最近情報を送信したインシデント。
- が終了したインシデント。
- アカウント内のすべてのインシデント。

### 3. [作成] を選択します。

インシデントの作成ページが開きます。

### 4. 優先度を選択します。

- 低: AWS/AMS リソースに関連するビジネスサービスまたはアプリケーションの重要ではない機能が影響を受けます。
- 中: AWS/AMS リソースに関連するビジネスサービスまたはアプリケーションが中程度の影響を受け、機能が低下しています。
- 高: ビジネスに大きな影響があります。AWS/AMS リソースに関連するアプリケーションの重要な機能は利用できません。本番稼働システムに影響を与える最も重要な停止用に予約されています。

### 5. カテゴリを選択します。

#### Note

インシデント機能をテストする場合は、インシデントタイトルにアクションなしフラグ (AMSTestNoOpsActionRequired) を追加します。

### 6. 次の情報を入力します。

- 件名: インシデントレポートのわかりやすいタイトル。
- CC E メール: インシデントレポートと解決について通知するユーザーの E メールアドレスのリスト。
- 詳細: インシデントの包括的な説明、影響を受けるシステム、および解決の期待される結果。事前設定された質問に回答するか、それらを削除して関連情報を入力します。

添付ファイルを追加するには、添付ファイルの追加を選択し、必要な添付ファイルを参照し、開くをクリックします。添付ファイルを削除するには、削除アイコン をクリックします。

#### 7. [Submit] を選択してください。

詳細ページが開き、タイプ、件名、作成済み、ID、ステータスなどのインシデントに関する情報と、作成したリクエストの説明を含む通信エリアが表示されます。

返信をクリックしてコレスポンスエリアを開き、ステータスの追加の詳細または更新を提供します。

インシデントが解決されたら「Close Case」をクリックします。

1 ページに収まるよりも多くのコレスポンスがある場合は、「ロードする」をクリックします。

コミュニケーションを評価することを忘れないでください。

インシデントがインシデントリストページに表示されます。

YouTube Video: [AWS Managed Services コンソールからインシデントを発生させるにはどうすればよいですか？](#)

## インシデントのモニタリングと更新

インシデントレポートとサービスリクエストは、AMS コンソールを使用するか、サポート API を使用してプログラムで更新、モニタリング、確認することができます。サポート API の使用の詳細については、「[DescribeCases](#)オペレーション」を参照してください。

AMS コンソールを使用してケース、インシデント、またはサービスリクエストをモニタリングするには、次の手順に従います。

1. AMS コンソールのインシデントレポートまたはサービスリクエストダッシュボードで、ケースを参照し、件名を選択して、現在のステータスと対応の詳細ページを開きます。

報告されたインシデントまたはサービスリクエストケースが AMS オペレーションチームによって更新されると、AMS コンソールでインシデントへのリンクと E メールが届きます。E メールに返信してインシデントのやり取りに応答することはできません。

**⚠ Important**

サービスリクエストまたはインシデントケースの状態変更の通知を受け取るには、E メールアドレスを入力する必要があります。通知は、ケースの作成時に追加された E メールアドレスにのみ送信されます。

AMS フェデレーティッドネットワークで E メールサーバーを使用しない限り、通知 Eメールのリンクは機能しません。ただし、AMS コンソールに移動し、ケースの詳細ページを使用して対応できます。

2. リストに多くのケースがある場合は、フィルターオプションを使用できます。

- All open (デフォルト): このフィルターを使用して、解決されていないすべてのケースを表示します。
- 未割り当て: ケースを送信したばかりで、ケースの状態が変更されたという通知を受け取っていない場合に使用します。インシデントとサービスリクエストのケースは、送信された優先度 (インシデント) またはサービスレベルアグリーメント (サービスリクエスト) に応じて、異なるプロンプトで対処されることに注意してください。
- オープン: ケースが「Amazon 保留中」アクションであるという通知を受け取った場合に使用します。これは、ケースが割り当てられたが、まだ作業が開始されていないことを意味します。
- Reopened: 解決後にケースが再開されたという通知を受け取った場合に使用します。
- 進行中の作業: オペレーターがケースの処理を開始したという通知を受け取った場合は、 を使用します。
- 保留中のカスタマーアクション: オペレーターからアクションのリクエストを受け取った場合は、 を使用します。
- カスタマーアクションの完了: ケースに対するアクションが処理されたという通知を受け取った場合は、 を使用します。
- 解決済み: 解決済みのケースを表示するために使用します。解決されたケースは 12 か月間履歴に保持されます。
- 任意のステータス: このフィルターを使用して、ステータスに関係なくすべてのケースを表示します。

3. 最新のステータスを確認するには、ページを更新します。
4. コレスポnden スが多すぎてすべてのコレスポnden スがページに表示されない場合は、「Load More」を選択します。
5. ケースのステータスを更新するには、返信を選択し、新しいコレスポnden スを入力し、送信を選択します。
6. 満足のいくように解決された後にケースを終了するには、ケースを閉じるを選択します。

1～5 星の評価でサービスを評価し、AMS に現状を知らせてください。

## AWS サポート API を使用したインシデントの管理

[AWS サポート API](#) を使用すると、問題の調査や AWS サポートスタッフとのやり取りを通じて、インシデントを作成し、対応を追加できます。AWS サポート API は、[AWS サポートセンター](#)の動作の多くをモデル化します。この AWS サポートサービスの使用方法の詳細については、「[AWS サポートケースのプログラミング](#)」を参照してください。

### Note

AMS Advanced インシデントに AWS サポート API または SAPI を使用する場合は、次のサービスコードを使用します: `sentinel-report-incident`。

## AMS で生成されたインシデントへの対応

AMS はリソースをプロアクティブにモニタリングします。詳細については、「[モニタリングとイベント管理](#)」を参照してください。AMS はインシデントケースを特定して作成する場合があります。ほとんどの場合、インシデントについて通知します。インシデントを解決するためにユーザー側でアクションが必要な場合、AMS はアカウントに提供した連絡先情報に通知を送信します。このインシデントには、他のインシデントと同じ方法で対応します。通常、インシデントには AMS コンソールから対応します。場合によっては、E メールまたは電話による連絡が必要です。

### Note

AMS は、AWS アカウントのプライマリ E メールアドレスに通信を送信します。インシデント管理プロセスを容易にするために、代替のオペレーション連絡先 E メールエイリアスを追加することをお勧めします。これは、AMS オンボーディングプロセスおよび関連するオンボーディングドキュメントで説明されています。オンボーディング中に (CSDM に通知し

た) リソースベースの問い合わせを AMS に提供した場合、それらの問い合わせが使用されます。たとえば、セキュリティ関連のインシデントや通知に使用する SecurityContactsCSDMs/CAs に提供できます。CSDM にタグ情報の使用に同意している場合、インスタンス/リソースの問い合わせタグは AMS が生成するインシデントに使用されます。この通知サービスの詳細については、[「通知」](#)を参照してください。

## サービスリクエスト管理

### トピック

- [サービスリクエストを使用するタイミング](#)
- [サービスリクエスト管理の仕組み](#)
- [AMS でのサービスリクエストのテスト](#)
- [AMS でのサービスリクエストの作成](#)
- [AMS でのサービスリクエストのモニタリングと更新](#)
- [AMS で生成されたサービスリクエストへの応答](#)

サービスリクエストは、情報またはアドバイスを求めるためにユーザーが作成した AMS への通信です。標準サービスリクエストの例として、Alarm Manager、パッチオーケストレーターなどの AMS サービスの設定に関するガイダンスやヘルプがあります。AMS からサービスリクエストを受信することもできます。これらはアウトバウンドサービスリクエストまたはサービス通知と呼ばれます。AMS から送信されたサービスリクエストとアウトバウンドサービスリクエスト (サービス通知) のリストを確認するには、AMS コンソールのサービスリクエストページを参照してください。

アウトバウンドサービスリクエストの詳細については、「」を参照してください [AMS で生成されたサービスリクエストへの応答](#)。

AWS Managed Services (AMS) サービスリクエストを作成するには、AMS コンソールを使用するか、プログラムで サポート API を使用します。API の使用の詳細については、[サポート「API」](#)を参照してください。AMS の場合は、sentinel-service-request サービスコードを選択します。

AMS オペレーションチームがサービスリクエストを受信すると、サービスレベルアグリーメントに従って優先順位が付けられます。サービスリクエスト解決プロセスの各ステップで通知を受けるには、CC Emails オプションを必ず入力し、フェデレーションで接続する場合は、E メール AMS が送信するリンクに従う前にログインします。

AMS コンソールのサービスリクエストの作成ページを使用して、次のタスクを実行します。

- サービスリクエストの作成と更新
- 現在のすべてのサービスリクエストのリストと詳細情報を取得する
- 解決されたリクエストを含む、日付とインシデント識別子でサービスリクエストの検索を絞り込む
- コミュニケーションと添付ファイルをリクエストに追加し、ケースコレスポンス用の E メール受信者を追加する
- サービスリクエストの解決
- サービスリクエスト通信のレート

## サービスリクエストを使用するタイミング

次の例では、サービスリクエストについて説明します。

- AMS または AWS 一般的なガイダンス
- MW 関連の質問にパッチを適用する
- バックアップスケジュール関連の質問
- AWS サービスの機能に関する質問

以下は、サービスリクエストで発生すべきではない内容の例です。

- アクセスの問題
- パッチの失敗
- バックアップの失敗
- ビジネスの中断を引き起こす RFC 障害または RFC (ビジネスの中断にインシデントを使用する )
- RFC 質問、RFC スコープの追加入力または変更 (RFC 双方向通信を使用 )

## サービスリクエスト管理の仕組み

サービスリクエストは、オンコール AMS オペレーションチームによって処理されます。

AMS オペレーションチームがサービスリクエストを受信すると、リクエストがインシデントとしてより適切に分類されていないかが確認されます。インシデントとして分類する必要がある場合は、すぐに再分類され、AMS インシデント管理チームが引き継ぎ、通知されます。

RFC の送信でサービスリクエストを解決できる場合、レビューオペレーターから適切な RFC の送信を求める E メールが送信されます (詳細は記載されています)。

AMS オペレーターがサービスリクエストを解決できる場合、その手順はすぐに実行されます。たとえば、サービスリクエストがアーキテクチャのアドバイスやその他の情報に関するものである場合、オペレーターは適切なリソースを参照するか、質問に直接回答します。

サービスリクエストの分析でバグまたは機能リクエストが特定された場合、AMS はサービスリクエストを通じて通知を送信します。機能リクエストやバグ修正のための ETA がないため、元のサービスリクエストは閉じられます。元のサービスリクエストに関連するフォローアップの質問については、CSDM にお問い合わせください。

サービスリクエストが AMS オペレーションの範囲外である場合、オペレーターはリクエストをクラウドサービス配信マネージャーに送信して、ユーザーと通信できるようにするか、適切な AWS オペレーションチームに E メールとともに、どのような手順が実行されているかを知らせます。

サービスリクエストは、結果に満足していることを示すまで解決されません。

#### Note

コミュニケーションを容易にするために、すべてのケースで連絡先の E メール、名前、電話番号を提供することをお勧めします。

## AMS でのサービスリクエストのテスト

AMS サービスリクエストをテストするときは、サブジェクトテキストに次のフラグを含める必要があります: AMSTestNoOpsActionRequired。AMS オペレーションエンジニアがそのフラグを確認すると、サービスリクエストには応答しません。

## AMS でのサービスリクエストの作成

AWS Managed Services (AMS) コンソールを使用してサービスリクエストを作成するには:

1. 左側のナビゲーションから、サービスリクエストを選択します。

サービスリクエストリストが開きます。

サービスリクエストリストが空の場合、フィルターをクリアオプションはフィルターを Any ステータスにリセットします。



電話またはチャットを使用する場合は、サポートセンターでサービスリクエストの作成をクリックして、サポートセンターコンソールでサービスリクエストの作成ページを開き、AMS サービスタイプが自動的に入力されます。

 Note

応答を改善するために、サポートセンターで開始された通話が記録されます。通話が切断された場合は、サポートセンターのケースを通じてコールバックする必要があります。コールバックするメカニズム AWS はありません。

 Important

電話とチャットのサポートは、サポートケース、インシデント、サービスリクエストに役立つように設計されています。RFC の問題については、関連する RFC の詳細ページでレスポンスオプションを使用し、AMS エンジニアに連絡してください。

2. 既存のサービスリクエストを検索する場合は、ドロップダウンリストからサービスリクエストのステータスフィルターを選択します。

- まだ解決されていないすべてのサービスリクエスト。
- まだ割り当てられていない新しいサービスリクエスト。
- 割り当てられたサービスリクエスト。
- 再開したサービスリクエスト。
- 割り当てられた複雑なサービスリクエスト。
- 次のステップの前にフィードバックを必要とするサービスリクエスト。
- 最近情報を送信したサービスリクエスト。
- が終了したサービスリクエスト。
- アカウント内のすべてのサービスリクエスト。

### 3. [作成] を選択します。

サービスリクエストの作成ページが開きます。

### 4. カテゴリを選択します。

#### Note

サービスリクエスト機能をテストする場合は、サービスリクエストのタイトルにアクションなしフラグ `AMSTestNoOpsActionRequired` を追加します。

### 5. 次の情報を入力します。

- 件名: これにより、リストページのサービスリクエストの詳細へのリンクが作成されます。
- CC E メール: これらの E メールは、デフォルトの E メール連絡先に加えて通信を受信します。
- 詳細: できるだけ多くの情報をここに入力します。

添付ファイルを追加するには、添付ファイルの追加を選択し、必要な添付ファイルを参照し、開くをクリックします。添付ファイルを削除するには、削除アイコン をクリックします。

### 6. [Submit] を選択してください。

詳細ページが開き、タイプ、件名、作成済み、ID、ステータスなどのサービスリクエストに関する情報と、作成したリクエストの説明を含む通信エリアが表示されます。

さらに、サービスリクエストがサービスリクエストリストページに表示されます。これは、アラートがあるが、AMS からまだ聞こえていない場合に使用します。

返信をクリックしてコレスポンスエリアを開き、追加の詳細またはステータスの更新を指定します。

サービスリクエストが解決されたら、ケースの解決をクリックします。

Load More をクリックして、最初のページに収まらない追加のコレスポンスを表示します。

コミュニケーションを評価することを忘れないでください。

請求関連のクエリの場合は、サポートセンターコンソールからサービスリクエストケースを作成します。

YouTube 動画: [AWS コンソールからサービスリクエストを作成する方法とタイミング、およびサービスレベル目標は何ですか？](#)

## AMS でのサービスリクエストのモニタリングと更新

インシデントレポートとサービスリクエストは、AMS コンソールを使用するか、サポート API を使用してプログラムで更新、モニタリング、確認することができます。サポート API の使用の詳細については、「[DescribeCases](#)オペレーション」を参照してください。

AMS コンソールを使用してケース、インシデント、またはサービスリクエストをモニタリングするには、次の手順に従います。

1. AMS コンソールのインシデントレポートまたはサービスリクエストダッシュボードで、ケースを参照し、件名を選択して、現在のステータスと対応の詳細ページを開きます。

報告されたインシデントまたはサービスリクエストケースが AMS オペレーションチームによって更新されると、AMS コンソールでインシデントへのリンクと E メールが届きます。E メールに返信してインシデントのやり取りに応答することはできません。

### Important

サービスリクエストまたはインシデントケースの状態変更の通知を受け取るには、E メールアドレスを入力する必要があります。通知は、ケースの作成時に追加された E メールアドレスにのみ送信されます。

AMS フェデレーティッドネットワークで E メールサーバーを使用しない限り、通知 Eメールのリンクは機能しません。ただし、AMS コンソールに移動し、ケースの詳細ページを使用して対応できます。

2. リストに多くのケースがある場合は、フィルターオプションを使用できます。

- All open (デフォルト): このフィルターを使用して、解決されていないすべてのケースを表示します。
  - 未割り当て: ケースを送信したばかりで、ケースの状態が変更されたという通知を受け取っていない場合に使用します。インシデントとサービスリクエストのケースは、送信された優先度 (インシデント) またはサービスレベルアグリーメント (サービスリクエスト) に応じて、異なるプロンプトで対処されることに注意してください。
  - オープン: ケースが「Amazon 保留中」アクションであるという通知を受け取った場合に使用します。これは、ケースが割り当てられたが、まだ作業が開始されていないことを意味します。
  - Reopened: 解決後にケースが再開されたという通知を受け取った場合に使用します。
  - 進行中の作業: オペレーターがケースの処理を開始したという通知を受け取った場合は、 を使用します。
  - 保留中のカスタマーアクション: オペレーターからアクションのリクエストを受け取った場合は、 を使用します。
  - カスタマーアクションの完了: ケースに対するアクションが処理されたという通知を受け取った場合は、 を使用します。
  - 解決済み: 解決済みのケースを表示するために使用します。解決されたケースは 12 か月間履歴に保持されます。
  - 任意のステータス: このフィルターを使用して、ステータスに関係なくすべてのケースを表示します。
3. 最新のステータスを確認するには、ページを更新します。
  4. コレスポネンスが多すぎてすべてのコレスポネンスがページに表示されない場合は、「Load More」を選択します。
  5. ケースのステータスを更新するには、返信を選択し、新しいコレスポネンスを入力し、送信を選択します。
  6. 満足のいくように解決された後にケースを終了するには、ケースを閉じるを選択します。
- 1~5 星の評価でサービスを評価し、AMS に現状を知らせてください。

## AMS で生成されたサービスリクエストへの応答

AMS パッチ管理は、設定されたメンテナンスウィンドウの前にサービスリクエスト (サービス通知) を送信します。詳細については、[「AMS メンテナンスウィンドウ」](#)を参照してください。AMS は、サービスによってインフラストラクチャが影響を受ける可能性がある場合、またはアカウント

の EC2 インスタンスを再起動する必要がある場合にも AWS、サービス通知を送信します。詳細については、[「サービス通知」](#)を参照してください。

 Note

AMS は、指定した AWS アカウントのプライマリ E メールアドレスに通信を送信します。サービスリクエストまたはサービス通知管理プロセスを容易にするために、代替のオペレーション連絡先 E メールエイリアスを追加することをお勧めします。これらの E メール追加は、AMS オンボーディングプロセスおよび関連するオンボーディングドキュメントで説明されています。

## 請求に関する質問

請求関連の質問を送信するには、次の手順を実行します。

1. <https://console.aws.amazon.com/support/home#/> で [AWS サポート センター](#)を開きます。
2. アカウントと請求を選択します。
3. [ケースを作成] を選択します。
4. アカウントと請求を選択し、プロンプトに従ってケースを送信します。

# オペレーションオンデマンド

Operations on Demand (OOD) は、AMS オペレーションプランまたは によって現在ネイティブに提供されていないオペレーションサービスを提供することで、AMS オペレーションプランの標準範囲を拡張する AWS Managed Services (AMS) 機能です AWS。 <https://aws.amazon.com/managed-services/features/> 選択すると、カタログの提供は自動化と高度なスキルを持つ AMS リソースの組み合わせによって提供されます。長期契約や追加の契約がないため、必要に応じて既存の AMS と AWS 運用および機能を拡張できます。1 ブロックあたり 20 時間 (OOD ブロック) を毎月購入することに同意します。

標準化されたサービスのカタログから選択し、サービスリクエストを通じて新しい OOD エンゲージメントを開始できます。OOD サービスの例としては、Amazon EKS のメンテナンス、 の運用 AWS Control Tower、SAP クラスターの管理の支援などがあります。新しいカタログサービスは、需要と最も頻繁に見られる運用上のユースケースに基づいて定期的に追加されます。

OOD は、AMS Advanced オペレーションプランと AMS Accelerate オペレーションプランの両方で使用でき、AMS が利用可能なすべての [AWS リージョン](#) で使用できます。

AMS は、リクエストされた変更を実装しながら、カスタマーセキュリティリスク管理 (CSRM) を実行します。CSRM プロセスの詳細については、「[変更リクエストのセキュリティレビュー](#)」を参照してください。

## Operations on Demand サービスのカタログ

Operations on Demand (OOD) は、次の表で説明するサービスを提供します。

### Note

主要用語の定義については、AWS Managed Services ドキュメント [の主要用語](#) を参照してください。

| オペレーション<br>プラン                      | タイトル                    | 説明                                                                   | 期待される成果                          |
|-------------------------------------|-------------------------|----------------------------------------------------------------------|----------------------------------|
| AMS Advanced<br>と AMS<br>Accelerate | Amazon EKS クラスターのメンテナンス | AMS は、Amazon Elastic Kubernetes Service (Amazon EKS) デプロイの継続的なメンテナンス | カスタマーチームは、Amazon EKS クラスターの更新の基盤 |

|                |            |                                                                                                                                                                                                                                                                                                                                                                 |                                                       |
|----------------|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|
|                |            | <p>を処理することで、コンテナ開発者を解放します。AMS は、コントロールプレーン、アドオン、ノードのコンポーネントに対応するクラスターを更新するために必要なend-to-endの手順を実行します。AMS は、マネージド型ノードタイプへの更新と、Amazon EKS および Kubernetes アドオンの厳選されたセットを実行します。</p>                                                                                                                                                                                  | <p>となる運用作業を支援しました。</p>                                |
| AMS Accelerate | AMI の構築と販売 | <p>AMS は、AMI の構築と販売を継続的に管理します。</p> <p>当社のエンジニアは、サブスクライブされた AMIs の毎月のリリース、緊急パッチ適用アクティビティ用のオンデマンド AMIs のリリース、ランブックを使用した変更の管理、CloudWatch Monitoring を使用した AMI ビルドのモニタリングを行います。また、指定されたアカウントで使用されるすべての AMIs のトラブルシューティング支援と詳細なレポートも提供します。このサービスでは、EC2 Image Builder を介して AMI ビルドパイプラインをデプロイする必要があります。AMS は、EC2 Image Builder とやり取りする他のオートメーションやサービスをサポートしていません。</p> | <p>お客様のセキュリティ体制が改善され、AMI の構築と販売に費やすお客様の時間が短縮AMIs。</p> |

|                |                              |                                                                                                                                                                                                                                                     |                                                                                                                                                                                |
|----------------|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AMS Accelerate | 厳選された変更の実行                   | 当社の熟練した運用エンジニアと協力して、ビジネス要件を、お客様の AWS 環境内で安全に実行できる検証済みの変更リクエストに変換します。自動化への独自のアプローチと運用上のベストプラクティス (影響評価、ロールバック、2 人称ルールなど) に関する知識を活用します。これは、大規模な単純な変更でも、ダウンストリームへの影響を伴う複雑なアクションでもかまいません。                                                               | お客様は、カスタム変更リクエストの定義、作成、実行を支援しました。変更には、手動または自動 (CloudFormation、SSM) を使用できます。必要に応じて、設定ガイド サポート に関するとの相談が含まれます。アプリケーションコード、アプリケーションのインストール/デプロイ、データ移行、または OS 設定の変更を意図したものではありません。 |
| AMS Accelerate | AWS Network Firewall オペレーション | AMS はお客様と協力してファイアウォールをオンボードし、継続的なファイアウォールオペレーションのポリシーとルールを実装および管理します。エンジニアは、運用上のベストプラクティスと自動化を活用して標準化されたポリシーとルールを設定し、モニタリングを有効にして自動化プロセス以外で行われた変更を検出することでこれを行います。AMS は、不要な変更を迅速に通知し、必要に応じてそれらを含めるか、システムの全体的な安定性を確保するためにアカウントを以前の設定に復元するオプションを提供します。 | お客様のチームは、意図しないネットワークファイアウォールの変更をすばやく検出することで、管理オーバーヘッドの削減を支援しました。これにより、インシデントの解決が改善され、予期される問題と予期しない問題の両方の根本原因分析時間が短縮されます。                                                       |



|                |                                     |                                                                                                                                                                                                                                                                                                                                             |                                                                                              |
|----------------|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| AMS Accelerate | AWS Control Tower オペレーション           | Transit Gateway や AWS を含むラン AWS Control Tower デイングゾーンの継続的な運用と管理<br>AWS Organizations は、包括的なランディングゾーンソリューションを提供します。カスタムコントロールとガードレールのライブラリを使用して、アカウント供給、SCP と OU の管理、ドリフト修復、SSO ユーザー管理、AWS Control Tower アップグレードを処理します。                                                                                                                      | カスタマーチームは、管理、AWS Transit Gateway AWS Control Tower、およびの基本的な運用作業の一部を支援しました AWS Organizations。 |
| AMS Accelerate | AWS ランディングゾーン<br>Accelerate オペレーション | AMS は、AWS ランディングゾーンアクセラレーター (LZA) を通じてデプロイされた AWS ランディングゾーンの継続的なオペレーションを提供します。<br><br>当社のエンジニアは、設定ファイルの変更、AWS Control Tower (CT) 環境管理 (アカウント供給、OU 作成、CT ガードレール)、サービスコントロールポリシー (SCP) 管理、CT ドリフトの検出と修復、ネットワーク設定管理、CT と LZA フレームワークの更新を処理します。AWS LZA は、運用上のベストプラクティスやなどのサービスを使用して、安全なマルチアカウント AWS 環境をセットアップおよび管理する手段を提供します AWS Control Tower。 | カスタマーチームは、AWS Landing Zone Accelerator ソリューションの継続的な運用と管理を支援しました。                             |

|                 |                      |                                                                                                                                     |                                                                                                          |
|-----------------|----------------------|-------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| AMS Accelerate  | SAP クラスター<br>アシスト    | SAP クラスターの専用のアラーム、モニタリング、クラスターパッチ適用、バックアップ、インシデント修復。このカタログ項目を使用すると、SAP 運用チームから進行中の運用作業の一部をオフロードできるため、チームは容量管理とパフォーマンス調整に集中できます。     | 顧客またはパートナーの SAP チームは、基盤となる運用作業の一部を支援しました。引き続き、キャパシティ管理、パフォーマンス調整、DBA、SAP ベースの管理など、他の SAP 機能を提供する必要があります。 |
| AMS アドバンス<br>スト | Priority RFC の<br>実行 | 指定された AMS オペレーションエンジニアのキャパシティーは、変更リクエスト (RFC) の実行を優先します。すべての送信はより高いレベルのレスポンスを受け取り、Amazon Chime 会議室を通じてエンジニアと直接やり取りすることで優先順位を調整できます。 | RFCs。                                                                                                    |

|                                              |                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                          |
|----------------------------------------------|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>AMS Advanced<br/>と AMS<br/>Accelerate</p> | <p>レガシー OS の<br/>アップグレード</p> | <p>インスタンスをサポートされているオペレーティングシステムのバージョンにアップグレードすることで、インスタンスの移行を回避できます。オートメーションとソフトウェアベンダーのアップグレード機能 (Microsoft Windows 2008 R2 から Microsoft Windows 2012 R2 など) を活用して、選択したインスタンスでインプレースアップグレードを実行できます。このアプローチは、新しいインスタンスに簡単に再インストールできず、古い OS バージョンで既知および軽減されていないセキュリティ脅威からさらに保護するレガシーアプリケーションに最適です。</p> <p>インプレースアップグレードでは、次のオペレーティングシステムがサポートされています。</p> <ul style="list-style-type: none"><li>• Microsoft Windows 2012 R2 から Microsoft Windows 2016 以降</li><li>• Microsoft Windows 2016 から Microsoft Windows 2022 以降</li><li>• Red Hat Enterprise Linux 7 から Red Hat Enterprise Linux 8</li><li>• Red Hat Enterprise Linux 8 から Red Hat Enterprise Linux 9 へ</li><li>• Oracle Linux 7 から Oracle Linux 8</li></ul> | <p>このソリューションは、新しいインスタンスに再インストールできなくなったアプリケーション (ソースコードの紛失、ISV のビジネス停止など) 向けに提供されています。失敗したアップグレードを元の状態にロールバックできます。運用上の観点からは、ロールバックが推奨されます。これは、インスタンスが最新のセキュリティパッチでよりサポート可能な状態になるためです。</p> |
|----------------------------------------------|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## トピック

- [オンデマンドでの AMS オペレーションのリクエスト](#)
- [Operations on Demand サービスに変更を加える](#)

## オンデマンドでの AMS オペレーションのリクエスト

AWS Managed Services (AMS) Operations on Demand (OOD) は、AMS にオンボードされているすべての AWS アカウント で使用できます。Operations on Demand を利用するには、クラウドサービスデリバリーマネージャー (CSDM)、ソリューションアーキテクト (SA)、アカウントマネージャー、またはクラウドアーキテクト (CA) に追加情報をリクエストします。利用可能な OOD オファリングは、前述の[オファリングの Operations on Demand カタログ](#)表に記載されています。エンゲージメントスコープが完了したら、AMS Operations にサービスリクエストを送信して OOD のエンゲージメントを開始します。

各 OOD サービスリクエストには、エンゲージメントに関する以下の詳細情報が含まれている必要があります。

- リクエストされた特定の OOD サービス、および特定の OOD サービスごとに:
  - 特定の OOD オファリングに割り当てるブロックの数 (1 つのブロックは、特定の暦月における運用リソース時間の 20 時間に等しく、該当する Operations on Demand オファリング AWS のその時点の標準レートで課金されます)。
  - 特定の OOD 提供がリクエストされている各 AWS Managed Services アカウントのアカウント ID。

OOD サービスリクエストは、次のいずれかを通じて送信する必要があります。

- 該当する Operations on Demand サービスを受け取る AWS Managed Services アカウント、または
- AWS Managed Services アカウントであるメンバーアカウントに代わって、すべての機能モードで AWS Organizations 管理アカウントである AWS Managed Services アカウント。

OOD サービスリクエストを受信すると、AMS Operations はアカウントを確認して、承認、部分承認、または拒否で更新します。

OOD 提供サービスリクエストが承認されたら、AMS とユーザーが調整してエンゲージメントを開始します。OOD の提供は、サービスリクエストが承認され、エンゲージメント開始日が合意されるまで開始されません。

AMS は、OOD ブロックの毎月のサブスクリプション割り当てを使用します。承認されたブロック数は、エンゲージメント開始日から新しいサービスリクエストのオプトアウトをリクエストするまで毎月割り当てられます。OOD ブロックは暦月に有効です。未使用のブロックまたはブロック部分は、今後数か月にロールオーバーまたは引き継がれません。

実際に使用された時間数に関係なく、毎月最低 1 つの OOD ブロックが請求されます。時間が使用されていない追加の割り当て済み OOD ブロックは請求されません。

## Operations on Demand サービスに変更を加える

Operations on Demand (OOD) サービスの継続的なエンゲージメントの変更をリクエストするには、次の情報を含むサービスリクエストを送信します。

- リクエストされている変更 (複数可) 、および
- 変更が有効になるようにリクエストされた日付。

OOD サービスリクエストを受け取った後、AMS Operations はリクエストを確認し、承認して更新するか、割り当てられた CSDM がユーザーと協力して変更の範囲と影響を判断するようにリクエストします。CSDM でスコープ作業が必要であると判断された場合は、スコープ演習の完了後に変更されたエンゲージメントを開始するために、2 番目の OOD サービスリクエストを送信する必要があります。

承認されると、最後に変更されたブロック割り当ては になり、引き続きアクティブになり、以前のブロック割り当てよりも優先されます。ただし、AWS とユーザーによる別段の合意がある場合は除きます。

## ドキュメント履歴

次の表に、AMS Advanced ユーザーガイドの各リリースにおける重要な変更点を示します。このドキュメントの更新に関する通知を受け取るには、RSS フィードにサブスクライブできます。

- API バージョン: 2019-05-21
- 新規または更新された CTs とチュートリアル: [AMS Advanced Change Type Reference Document History](#)。
- 新しい AMS AMIs: [AMS Amazon マシンイメージ \(AMIs\)](#)。

| 変更                                                       | 説明                                                                            | 日付              |
|----------------------------------------------------------|-------------------------------------------------------------------------------|-----------------|
| <a href="#">Managed Firewall Palo Alto サービスドキュメントを削除</a> | サービスの廃止により、Managed Firewall Palo Alto (MFPA) サービスドキュメントを削除しました。               | 2026 年 3 月 31 日 |
| <a href="#">DB インスタンスまたはクラスター変更タイプのパラメータグループの更新の例を追加</a> | DB インスタンスまたはクラスター変更タイプのパラメータグループの更新の例を追加しました。                                 | 2026 年 3 月 30 日 |
| <a href="#">Site-to-Site VPN トンネル変更タイプの置き換えの例を追加</a>     | Site-to-Site VPN トンネル変更タイプの例を追加しました。                                          | 2026 年 3 月 30 日 |
| <a href="#">DNS スカベンジング問題変更タイプの修正の例を追加</a>               | Remediate DNS scavenging issue change type の例を追加しました。                         | 2026 年 3 月 30 日 |
| <a href="#">VPC ルート変更タイプの削除の例を追加</a>                     | VPC ルート変更タイプの例を追加しました。                                                        | 2026 年 3 月 30 日 |
| <a href="#">サポート終了オペレーティングシステムを更新</a>                    | サポートされているサポート終了 (EOS) オペレーティングシステムリストから Red Hat Enterprise Linux (RHEL) 7.x お | 2026 年 3 月 27 日 |

よび Oracle Linux 7.5-7.9 を削除しました。

### [更新された AMS AMIs](#)

サポートされている AMI リストから Red Hat Enterprise 7 (最新のマイナーリリース)、Ubuntu Linux 18.04、Amazon Linux AMI (HVM / 64 ビット) AMIs。サポートされている AMI として Windows Server 2025 を追加しました。PBIS/Beyond Trust AD Bridge を PBIS Enterprise/Beyond Trust AD Bridge に更新し、BeyondTrust が 2022 年 6 月の時点で PBIS Open のサポートを提供しなくなったことに注意してください。

2026 年 3 月 27 日

### [Compute Optimizer レコメンデーションのブール値を更新](#)

標準規則との整合性を保つために、すべてのブールパラメータ値を大文字 (True/False) から小文字 (true/false) に更新しました。

2026 年 3 月 24 日

### [クロスアカウントポリシーの AMS-STD-002 ポイント 6.11 を更新](#)

サードパーティーアカウントへの書き込みアクセス権を持つクロスアカウントポリシーを、リスク承諾で設定できることを明確にしました。

2026 年 3 月 24 日

### [AWS Health モニタリングノートを更新](#)

AMS オペレーションによるアクションが必要な AWS Health イベントに対してのみ通知が送信されることを明確にしました。

2026 年 3 月 24 日

### [ONTAP ボリューム容量の自動修復を追加](#)

AMSFSXONTAPVolumeCapacityUtilization アラートを自動修復テーブルに追加し、ONTAP ボリューム容量修復オートメーションを説明する新しいセクションを追加しました。

2026 年 3 月 24 日

### [CloudWatch アラームの変更手順を更新](#)

管理 | その他 | その他 | 管理への作成 | その他 | その他 | 更新から CloudWatch アラームを変更または削除するための変更タイプリファレンスを更新しました。

2026 年 3 月 13 日

### [AWS Lake Formation ブループリント作成手順の更新](#)

でブループリントを作成するための変更タイプリファレンスを Management | Other | Other to Management | AWS サービス | Self-provisioned service | Add (マネージドオートメーション) AWS Lake Formation から更新しました。

2026 年 3 月 13 日

### [AWS Certificate Manager よくある質問セクションを更新しました](#)

管理 | その他 | その他 | 管理の更新 | 高度なスタックコンポーネント | ACM | 証明書の削除から ACM 証明書を削除または変更するための変更タイプリファレンスを更新しました。

2026 年 3 月 3 日



|                                                                                                                  |                                                                                                                                                      |                  |
|------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| <a href="#">「カスタマーセキュリティリスク管理プロセス」セクションを更新しました。</a>                                                              | 「カスタマーセキュリティリスク管理プロセス」セクションを更新し、リスク許容の有効性、レビュー、オプトアウト情報を追加しました。                                                                                      | 2026 年 1 月 15 日  |
| <a href="#">Operations On Demand セクションの表を更新しました</a>                                                              | Operations On Demand セクションの表を更新し、内容を更新しました。                                                                                                          | 2026 年 1 月 7 日   |
| <a href="#">「AMS での RFC エラーのトラブルシューティング」セクションの更新された内容</a>                                                        | AMS セクションの RFC エラーのトラブルシューティングを更新し、内容を更新しました。                                                                                                        | 2026 年 1 月 6 日   |
| <a href="#">Security Hub CSPM に関する情報を使用して、AMS の Trusted Remediator セクションを更新し、新しいコンテンツを追加しました。</a>                | AMS の Trusted Remediator セクションを更新し、Security Hub CSPM に関する情報を追加しました。新しいページ「Security Hub CSPM recommendations supported by Trusted Remediator」を追加しました。 | 2025 年 12 月 11 日 |
| <a href="#">AMS Advanced セクションの標準コントロールを AMS-STD-002 -(IAM) の 2 つの技術標準で更新 AWS Identity and Access Management</a> | AMS-STD-002 - AWS Identity and Access Management (IAM) の表を更新し、9.6 と 9.7 の 2 つの技術標準を追加しました。                                                           | 2025 年 10 月 23 日 |
| <a href="#">RFCsおよび AMS 実行モードに関する情報を更新しました</a>                                                                   | RFC が通過する 2 つのケースと、リクエストを処理するための 3 つの AMS 実行モードの新しいコンテンツを提供するようにページを更新しました。                                                                          | 2025 年 10 月 22 日 |

[AMS Advanced セクションの標準コントロールの AWS Identity and Access Management \(IAM\) の表を更新しました。](#)

IAM ポリシーと Amazon S3 バケットへのアクセスに関する表の情報を更新しました。

2025 年 9 月 25 日

[請求関連のクエリのステップを更新しました](#)

「AMS でのサービスリクエストの作成」セクションの「請求関連のクエリのサービスリクエストを作成する」ステップを更新しました。

2025 年 9 月 25 日

[変更タイプの E メール通知に関する情報を更新しました](#)

RFC E メール通知の設定 (コンソール) セクションの変更タイプの E メール通知を追加するための情報と例を更新しました。

2025 年 9 月 25 日

[更新された変更タイプ](#)

AMS インフラストラクチャの自動タグ付けセクションを更新し、AMS が作成したリソースにタグ付けするための変更タイプを追加しました。

2025 年 9 月 25 日

[AWS Managed Services の「VM Import/Export」に関するよくある質問を更新](#)

ツールがインスタンスからコマンドを実行できるように、インスタンスプロファイルのリクエストに使用される RFC を更新しました。

2025 年 9 月 24 日

[SAP Applications 15 SP6 インスタンス用の SUSE Linux Enterprise Server を起動するための変更リクエスト \(RFC\) を更新しました](#)

正しい RFC を使用して新しい SUSE Linux Enterprise Server for SAP Applications 15 SP6 インスタンスを起動する方法のステップ 2 を更新しました。

2025 年 9 月 22 日

|                                                                                     |                                                                                                                                                                                                                                                                                             |                 |
|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <a href="#">変更リクエスト (RFC) の更新</a>                                                   | AWS Managed Services のよくある質問セクション AWS Elastic Disaster Recovery を正しい RFC で更新し、アカウント内で必要な IAM ロールを作成しました。                                                                                                                                                                                    | 2025 年 9 月 22 日 |
| <a href="#">Trusted Remediator でサポートされている 4 つの新しい Trusted Advisor コスト最適化チェックを追加</a> | 次のコスト最適化チェックを追加しました。 <ul style="list-style-type: none"><li>• c1z7kmr00n - インスタンスの Amazon EC2 コスト最適化に関する推奨事項</li><li>• c1z7kmr02n - ボリュームの Amazon EBS コスト最適化に関する推奨事項</li><li>• c1z7kmr03n - DB インスタンスの Amazon RDS コスト最適化の推奨事項</li><li>• c1z7kmr05n - 関数の AWS Lambda コスト最適化に関する推奨事項</li></ul> | 2025 年 9 月 22 日 |
| <a href="#">アベイラビリティーゾーン (AZs) のメモを更新しました</a>                                       | AMS のセキュリティグループに関する情報を更新しました。                                                                                                                                                                                                                                                               | 2025 年 9 月 5 日  |
| <a href="#">更新された変更タイプ</a>                                                          | Managed AD をアプリケーションアカウントと共有するために、AWS Managed Services の Amazon FSx に関するよくある質問セクションを変更タイプで更新しました。                                                                                                                                                                                           | 2025 年 9 月 5 日  |

|                            |                                                                                                                                          |                |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| <a href="#">更新された変更タイプ</a> | AWS Managed Services の Amazon DocumentDB に関するよくある質問セクションを更新し、削除 APIs。                                                                    | 2025 年 9 月 5 日 |
| <a href="#">更新された変更タイプ</a> | AWS Managed Services での Alexa for Business に関するよくある質問」セクションを更新し、Alexa for Business ゲートウェイをインストールして運用するためのアクセスが制限された IAM ユーザー 2 名に変更しました。 | 2025 年 9 月 5 日 |
| <a href="#">更新された変更タイプ</a> | AWS Managed Services の WorkSpaces アプリケーションに関するよくある質問セクションを更新し、すべてのフリートストリーミングインスタンスで利用できる IAM ロールを作成および選択する変更タイプを追加しました。                 | 2025 年 9 月 5 日 |
| <a href="#">更新された変更タイプ</a> | AWS Managed Services FAQ セクションの EventBridge を更新し、EventBridge を使用して他の AWS リソースをトリガーする前に EventBridge サービスロールをリクエストする変更タイプを追加しました。          | 2025 年 9 月 5 日 |

|                                                                                            |                                                                                                                                |                 |
|--------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <a href="#">Trusted Remediator による Trusted Advisor セキュリティチェックのサポートを更新</a>                  | Hs4Ma3G108 チェックでサポートされている事前設定済みパラメータと制約を更新<br>- CloudTrail 証跡は Amazon CloudWatch Logs と統合する必要があります                             | 2025 年 9 月 5 日  |
| <a href="#">Trusted Remediator による Trusted Advisor セキュリティチェックのサポートを更新</a>                  | Trusted Advisor セキュリティチェックを更新して Hs4Ma3G184 のバージョン 2 を追加 - Application Load Balancer と Classic Load Balancer のログ記録を有効にする必要があります | 2025 年 9 月 5 日  |
| <a href="#">Trusted Remediator セクションでサポートされている Trusted Advisor 運用上の優秀性チェックを更新</a>          | Trusted Remediator セクションでサポートされている Trusted Advisor 運用上の優秀性チェックを更新し、サポートされている新しいチェック c1fd6b96l4 Amazon S3 アクセスログが有効になりました。      | 2025 年 8 月 28 日 |
| <a href="#">更新された変更タイプ</a>                                                                 | カスタム IAM ロールの変更タイプ。                                                                                                            | 2025/08/25      |
| <a href="#">AMS セクションで CloudWatch Application Insights for .Net and SQL Server を使用して更新</a> | CloudWatch Application Insights を使用するように変更タイプを改訂しました。                                                                          | 2025/08/25      |
| <a href="#">変更リクエスト (RFC) の更新</a>                                                          | Amazon S3 バケットにタグを追加する変更のリクエスト (RFC)。                                                                                          | 2025/08/25      |

|                                                                   |                                                                                                                                                |                 |
|-------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <a href="#">変更リクエスト (RFC) の更新</a>                                 | 管理目的で AMS によって作成されたすべてのリソースにタグを付けるための変更リクエスト (RFC)。                                                                                            | 2025/08/25      |
| <a href="#">AWS Managed Servicesに関するよくある質問セクションの Lambda を更新</a>   | イベントソースを作成するために、他の AWS サービスにアクセスするための変更タイプを改訂しました。                                                                                             | 2025/08/25      |
| <a href="#">AWS Managed Servicesに関するよくある質問セクションの Lambda を更新</a>   | Lambda 関数をプロビジョニングするように変更タイプを改訂しました。                                                                                                           | 2025/08/25      |
| <a href="#">セキュリティグループの作成、変更、または削除セクションを更新</a>                    | 変更タイプを改訂して、スタックと VPCs。                                                                                                                         | 2025/08/25      |
| <a href="#">Compute Optimizer の新しいコンテンツを含めるように信頼された修復セクションを更新</a> | 信頼できる修復者セクションを更新し、サポートされている AWS Compute Optimizer レコメンデーションの新しいコンテンツを追加しました。                                                                   | 2025 年 8 月 18 日 |
| <a href="#">TOC 用語集リンクを削除しました</a>                                 | <a href="#">AWS 用語集</a> 。                                                                                                                      | 2025 年 8 月 8 日  |
| <a href="#">正確な変更タイプのレコメンデーション</a>                                | カスタマーメトリクスをアプリケーションモニタリングシステムに統合するには、デプロイ   モニタリングと通知   SNS   CT の作成 (ct-3dfng lm4ombbs) で RFC を送信して、メトリクスの Amazon SNS トピックの作成を AMS にリクエストします。 | 2025 年 8 月 8 日  |

## [正確な変更タイプのレコメン デーション](#)

プレースホルダーインスタンスボリュームを削除するには、管理 | 高度なストックコンポーネント | EBS ボリューム | 変更タイプの削除 (ct-3e3h8u0sp5z80) を送信します。

2025 年 8 月 8 日

## [新しいモニタリングアラート: SecureChannelFailure と壊れ た Secure Channel](#)

[AMS AMS のアラートの自動  
修復におけるベースラインモ  
ニタリングからのアラート。](#)

2025 年 8 月 8 日

|                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                 |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <a href="#">新しい信頼された修復者の<br/>チェック</a>      | <a href="#">Trusted Advisor Trusted<br/>Remediator Hs4Ma3G12<br/>0-AWSManagedServic<br/>es-TerminateEC2Ins<br/>tanceStoppedForPer<br/>iodOfTime、Hs4Ma3G2<br/>30-AWSManagedServices-<br/>TrustedRemediatorEnable<br/>BucketAccessLoggingV2、お<br/>よび c18d2gz150-AWSMana<br/>gedServices-TerminateEC2Ins<br/>tanceStoppedForPer<br/>iodOfTime でサポートされ<br/>ている Trusted Remediator<br/>セキュリティチェックでサ<br/>ポートされているコスト最適<br/>化</a> <a href="#">チェック。</a> <a href="#">Trusted Advisor<br/>Hs4Ma3G120 AWSManage<br/>dServices-TerminateEC2Insta<br/>nceStoppedForPeriodOfTime<br/>Hs4Ma3G230AWSManag<br/>edServices-TrustedRemediato<br/>rEnableBucketAcces<br/>sLoggingV2 AWSManage<br/>dServices-TerminateEC2Insta<br/>nceStoppedForPeriodOfTime</a> | 2025 年 8 月 8 日  |
| <a href="#">ポイント 3.2 での IAM 標準の<br/>更新</a> | 言語を明確にし、タグ付けに<br>関する言及を削除しました。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 2025 年 7 月 25 日 |
| <a href="#">アラートオプトアウトオブ<br/>ションの更新</a>    | タグを追加すると、追加の 2<br>つのアラートをオプトアウト<br>できます。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 2025 年 7 月 25 日 |



|                                                                  |                                                                                     |                 |
|------------------------------------------------------------------|-------------------------------------------------------------------------------------|-----------------|
| <a href="#">セルフサービスプロビジョニングサービスの廃止</a>                           | CloudEndure セルフサービスプロビジョニングサービスは廃止されました AWS Application Migration Service。          | 2025 年 7 月 25 日 |
| <a href="#">バックアップの新機能</a>                                       | 新しいタグを使用して、バックアップポールの通知をカスタマイズします。                                                  | 2025 年 7 月 25 日 |
| <a href="#">更新されたコントロールテーブル</a>                                  | AMS-STD-002 - AWS Identity and Access Management (IAM) テーブルセクションで重複するコントロールを削除しました。 | 2025 年 6 月 26 日 |
| <a href="#">更新された SSP サービスの AWS Transfer Family 前提条件</a>         | 前提条件セクションに情報を追加しました。                                                                | 2025 年 6 月 26 日 |
| <a href="#">更新された IAM ポリシーの例</a>                                 | IAM ポリシーの例を更新し、推奨される制限を追加しました。                                                      | 2025 年 6 月 26 日 |
| <a href="#">AMI でサポートされている OSesの更新</a>                           | Ubuntu Linux 22.04 に Ubuntu Linux 24.04 を追加し、すべての参照を SP5 から SP6 に変更しました。            | 2025 年 6 月 26 日 |
| <a href="#">セルフサービスプロビジョニングサービス、MediaStore は廃止されました</a>          | の廃止に関する注意事項を追加しました AWS Elemental MediaStore。                                        | 2025 年 6 月 26 日 |
| <a href="#">セルフサービスプロビジョニングサービス、Amazon Inspector Classic の廃止</a> | Amazon Inspector Classic の廃止に関する注意事項を追加しました。                                        | 2025 年 6 月 26 日 |

|                                                             |                                                                                    |                 |
|-------------------------------------------------------------|------------------------------------------------------------------------------------|-----------------|
| <a href="#">セルフサービスプロビジョニングサービス、Amazon Connect は廃止されました</a> | Amazon Connect の廃止に関する注意事項を追加しました。                                                 | 2025 年 6 月 26 日 |
| <a href="#">AMS でサポートされている設定のセクションを更新しました</a>               | AMS でサポートされているオペレーティングシステムとサポートされているサポート終了 (EOS) オペレーティングシステムのサポート設定を更新しました。       | 2025 年 6 月 25 日 |
| <a href="#">セルフサービスプロビジョニングサービス、WorkDocs 廃止</a>             | ページと廃止された WorkDocs への参照を削除しました。                                                    | 2025 年 6 月 19 日 |
| <a href="#">代替パッチリポジトリのパッチ管理に関する重要なセキュリティノート</a>            | AMS で代替パッチリポジトリを使用するための重要なセキュリティ上の注意事項とベストプラクティス。                                  | 2025 年 6 月 10 日 |
| <a href="#">サポートされているオペレーティングシステムの更新</a>                    | AMS Advanced でサポートされているオペレーティングシステムが更新され、一部が追加され、一部が削除されます。                        | 2025 年 5 月 22 日 |
| <a href="#">内部専用 APIs</a>                                   | 一部の CloudWatch ログに表示される内部専用 APIs。                                                  | 2025 年 5 月 22 日 |
| <a href="#">AMS Trusted Remediator の更新</a>                  | 新しいパラメータを使用してpreconfigured-parameters、信頼できる修復ツールで Trusted Advisor チェックをカスタマイズする方法。 | 2025 年 5 月 22 日 |

|                                                                                               |                                                                                                                                                                                                    |                 |
|-----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <a href="#">SSP Amazon Elastic Container Registry の更新</a>                                     | Amazon ECR サービスをオンボードすると、より多くのロールが自動的にプロビジョニングされます。                                                                                                                                                | 2025 年 5 月 8 日  |
| <a href="#">AMS Advanced Trusted Remediator のよくある質問と更新。</a>                                   | サポートされている Trusted Advisor チェックのいくつかの更新、Trusted Remediator FAQ (「Trusted Remediator がアカウントにデプロイするリソースは何ですか？」を追加) など。 <a href="#">Trusted Advisor 「Trusted Remediator でサポートされているチェック」</a> も参照してください。 | 2025 年 5 月 8 日  |
| <a href="#">AMS Advanced Standard セキュリティコントロールの更新。</a>                                        | 「セキュリティグループ共有」コントロールを追加しました。                                                                                                                                                                       | 2025 年 5 月 8 日  |
| <a href="#">AMS Advanced で保護された名前空間。</a>                                                      | AMS で保護された名前空間 EPSMarketplaceSubscriptionRole と EPS を追加しました。                                                                                                                                       | 2025 年 4 月 24 日 |
| <a href="#">AMS Advanced ログの場所。</a>                                                           | ログの場所が追加されました。                                                                                                                                                                                     | 2025 年 4 月 24 日 |
| <a href="#">WorkSpaces アプリケーションの AMS Advanced Self-Service Provisioning モードの前提条件が更新されました。</a> | WorkSpaces アプリケーションの前提条件が追加されました。サービスのプロビジョニング RFC を送信するときは、Amazon S3 バケット名を含める必要があります。                                                                                                            | 2025 年 4 月 24 日 |

|                                                                                            |                                                                                                  |                 |
|--------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|-----------------|
| <a href="#">AMS Advanced New Amazon RDS 自動修復アラート。</a>                                      | アラート ID:- 0224、リクエストされた割り当てられたストレージが設定された最大ストレージしきい値以上になるとトリガーされます。                              | 2025 年 3 月 27 日 |
| <a href="#">AMS Advanced AWS は、2024 年 7 月 25 日に Amazon CloudSearch への新しい顧客アクセスを閉鎖しました。</a> | 既存のお客様は引き続き サービスを使用できますが、新機能はありません。                                                              | 2025 年 3 月 27 日 |
| <a href="#">AMS Advanced AWS は AWS CodeCommit、2024 年 7 月 25 日に への新しい顧客アクセスを閉鎖しました。</a>     | 既存のお客様は引き続き サービスを使用できますが、新機能はありません。                                                              | 2025 年 3 月 27 日 |
| <a href="#">Trusted Remediator が利用可能になりました。</a>                                            | AWS Trusted Advisor チェックの修復を自動化する AWS Managed Servicesソリューションである Trusted Remediator が利用可能になりました。 | 2025 年 3 月 19 日 |
| <a href="#">AMS Advanced 新しい自動修正 RDS アラート。</a>                                             | RDS-EVENT-0224 を追加しました。                                                                          | 2025 年 3 月 17 日 |
| <a href="#">AMS Advanced 新機能: インシデント通知。</a>                                                | AppRegistry を使用してアプリケーションを作成し、それらのアプリケーションのインシデント通知をカスタマイズできます。                                  | 2025 年 3 月 13 日 |
| <a href="#">AMS RDS アラームモニタリングしきい値の更新。</a>                                                 | RDS 平均 CPU 使用率アラームのしきい値が 75% から 90% に変更されました。                                                    | 2025 年 2 月 20 日 |

### [集計レポート表示用の新しいデータオプションでセルフサービスレポートを更新](#)

次のセルフサービスレポートに、新しいフィールド名: Admin Account ID、データセットフィールド名: aws\_admin\_account\_id、定義: を含めるデータオプションを追加 Trusted AWS Organization account enabled by the customer しました。

2025 年 1 月 28 日

- パッチレポート (毎日)
- バックアップレポート (毎日)
- インシデントレポート (毎週)

### [SSP AWS Batch の更新](#)

次の RFC を使用して AMS アカウント AWS Batch でプロビジョニングできます: 管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (ct-1w8z66n899dct)。

2025 年 1 月 28 日

### [新しい AMS 機能: 集約セルフサービスレポート](#)

集約型セルフサービスレポート (SSR) では、組織レベルで集約された既存のセルフサービスレポートをクロスアカウントで表示できます。

2025 年 1 月 21 日

### [Forecast SSP セクションの更新](#)

注: AWS は、2024 年 7 月 29 日に Amazon Forecast への新しい顧客アクセスを閉鎖しました。Amazon Forecast の既存のお客様は、通常どおりサービスを引き続き使用できます。

2025 年 1 月 10 日

[AMS で保護された名前空間セクションの更新](#)

AMS で保護された名前空間のリストに、欠落している保護された名前空間 (\*mc、\*MC、\*Mc) を追加しました。

2025 年 1 月 9 日

[「モニタリングの仕組み」セクションの更新](#)

インシデントごとではなく、リソースまたはインスタンス ID ごとにアラート通知を設定する新機能に関する情報を追加しました。

2025 年 1 月 8 日

[更新: タグベースの更新コンテンツ](#)

keyname の誤字を修正し、不正な設定ファイルパスを修正しました。

2025 年 1 月 6 日

[更新: AMS AMI ノート](#)

Zip ファイルには、最新の AMS Amazon マシンイメージ (AMIs) と最新の AMIs。

2024 年 11 月 21 日

[Operations On Demand オペレーティングテーブルを更新](#)

インプレースアップグレードでは、次のオペレーティングシステムがサポートされています。

2024 年 11 月 11 日

- Microsoft Windows 2016 から Microsoft Windows 2022 以降

## [Operations On Demand オ ファリングテーブルを更新](#)

インプレースアップグレード  
では、次のオペレーティング  
システムがサポートされてい  
ます。

2024 年 11 月 1 日

- Microsoft Windows 2012  
R2 から Microsoft Windows  
2016 以降
- Red Hat Enterprise Linux  
7 から Red Hat Enterprise  
Linux 8
- Red Hat Enterprise Linux  
8 から Red Hat Enterprise  
Linux 9 へ
- Oracle Linux 7 から Oracle  
Linux 8

## [サポートされている設定の更 新](#)

サポートされている Oracle  
Linux オペレーティングシステ  
ムを 9.0~9.3、8.0~8.9、7.5  
~7.9 に更新しました。

2024 年 10 月 24 日

## [AMS Amazon マシンイメージ \(AMIs\)の更新](#)

Windows ベースの AMIs  
し、Windows 2012 および  
2012 R2 を削除しました。L  
inux ベースの AMIsして、サ  
ポートされなくなった複数の  
AMI を削除し、以下を追加し  
ました。

2024 年 10 月 24 日

- Amazon Linux 2 (ARM64)
- RHEL 9
- SUSE Linux Enterprise  
Server 15 SP5

|                                                                    |                                                                                                                                                                                                                                                                                       |                 |
|--------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <a href="#"><u>タグベースのアラートに複数の E メールアドレスを含めることができるようになりました。</u></a> | タグベースのアラートで複数の E メールアドレスがサポートされるようになりました。                                                                                                                                                                                                                                             | 2024 年 9 月 20 日 |
| <a href="#"><u>変更リクエストのセキュリティレビューセクションを追加しました。</u></a>             | 変更リクエストのセキュリティレビュープロセスの詳細を提供する新しいセクションが追加されました。                                                                                                                                                                                                                                       | 2024 年 9 月 17 日 |
| <a href="#"><u>新しいセクションが追加されました。</u></a>                           | AMS Advanced で変更リクエストのセキュリティレビューがどのように行われるかを説明する新しいセクションが利用可能になりました。                                                                                                                                                                                                                  | 2024 年 9 月 12 日 |
| <a href="#"><u>AMS Advanced でサポートされている新しいサービス。</u></a>             | AWS Resilience Hub が AMS Advanced でサポートされるようになりました。                                                                                                                                                                                                                                   | 2024 年 8 月 30 日 |
| <a href="#"><u>AMS Advanced でサポートされている新しいサービス。</u></a>             | AMS Advanced で 5 つの新しいサービスがサポートされるようになりました。 <ul style="list-style-type: none"><li>• Amazon Bedrock</li><li>• Amazon Kendra</li><li>• Amazon Quantum Ledger Database (Amazon QLDB)</li><li>• AWS Service Catalog AppRegistry</li><li>• Amazon Managed Service for Prometheus</li></ul> | 2024 年 8 月 21 日 |
| <a href="#"><u>新しいエンドポイントセキュリティネットワークのデフォルト設定が利用可能になりました。</u></a>  | 更新ソースが EPS のデフォルトのネットワーク設定に含まれるようになりました。                                                                                                                                                                                                                                              | 2024 年 8 月 21 日 |



|                                                                                |                                                                                  |                 |
|--------------------------------------------------------------------------------|----------------------------------------------------------------------------------|-----------------|
| <a href="#">更新: AMS AMI ノート</a>                                                | Zip ファイルには、最新の AMS Amazon マシンイメージ (AMIs) と最新の AMIs。                              | 2024 年 7 月 30 日 |
| <a href="#">AMS が Amazon Route 53 Resolver DNS Firewall をサポートするようになりました。</a>   | AMS が Amazon Route 53 Resolver DNS Firewall をサポートするようになりました。                     | 2024 年 7 月 30 日 |
| <a href="#">AWS DataSync SSPS 更新</a>                                           | AWS DataSync Amazon S3 バケット名に「datasync-」プレフィックスが不要になりました。                        | 2024 年 7 月 30 日 |
| <a href="#">セキュリティ設定ルールダッシュボード</a>                                             | セキュリティ設定ルールダッシュボードがセルフサービスレポートで使えるようになりました。                                      | 2024 年 7 月 24 日 |
| <a href="#">AMS は、Oracle Linux 8.9、RHEL 8.10、および RHEL 9.4 をサポートするようになりました。</a> | AMS は、Oracle Linux 8.9、RHEL 8.10、および RHEL 9.4 をサポートするようになりました。                   | 2024 年 7 月 5 日  |
| <a href="#">Amazon Bedrock がセルフサービスプロビジョニングモードで利用可能に</a>                       | AMS SSP モードで Amazon Bedrock をリクエストできるようになりました。                                   | 2024 年 6 月 27 日 |
| <a href="#">セキュリティインシデント対応の Amazon Route 53 Resolver DNS ファイアウォールイベント</a>      | AMS がセキュリティインシデント対応で Amazon Route 53 Resolver DNS ファイアウォールイベントをモニタリングするようになりました。 | 2024 年 6 月 21 日 |
| <a href="#">AMS Bring Your Own EPS (BYOEPS) 機能を有効にする方法に関する追加情報を追加しました。</a>     | AMS Bring Your Own EPS (BYOEPS) 機能を有効にする方法に関する追加情報を追加しました。                       | 2024 年 6 月 5 日  |

|                                                                               |                                                                                           |                 |
|-------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|-----------------|
| <a href="#">更新: AMS AMI ノート</a>                                               | Zip ファイルには、最新の AMS Amazon マシンイメージ (AMIs) と最新の AMIs。                                       | 2024 年 5 月 23 日 |
| <a href="#">セルフサービスプロビジョニングモード (MALZ 環境のみ) AWS Amplify でのカスタムロールの使用に関する詳細</a> | MALZ 環境がセルフサービスプロビジョニングモードで AWS Amplify でカスタムロールを使用する方法に関する手順を追加しました。                     | 2024 年 5 月 23 日 |
| <a href="#">Amazon Kendra がセルフサービスプロビジョニングモードで利用可能になりました。</a>                 | Amazon Kendra がセルフサービスプロビジョニングモードで利用可能になりました。                                             | 2024 年 5 月 23 日 |
| <a href="#">AMS Advanced は追加のオペレーティングシステムをサポートしています。</a>                      | AMS Advanced は、Red Hat Enterprise Linux (RHEL) 9.x および Ubuntu 20.04 および 22.04 をサポートしています。 | 2024 年 4 月 25 日 |
| <a href="#">AMS Advanced は、Amazon Linux 2 の ARM64 アーキテクチャをサポートしています。</a>      | AMS Advanced は、Amazon Linux 2 の ARM64 アーキテクチャをサポートしています。                                  | 2024 年 4 月 25 日 |
| <a href="#">マルチアカウントランディングゾーン (MALZ) ランディングゾーンアカウントセクションからオフボードを更新しました。</a>   | マルチアカウントランディングゾーンからアプリケーションアカウントとコアアカウントをオフボードする方法に関する詳細情報を追加しました。                        | 2024 年 4 月 11 日 |
| <a href="#">更新: サービスリクエスト管理の説明。</a>                                           | 「サービスの説明」トピックの「サービスリクエスト管理の説明」を更新しました。                                                    | 2024 年 3 月 21 日 |
| <a href="#">更新: インシデント管理サービスのコミットメントセクション。</a>                                | AMS サービスレベルアグリーメントへのリンクを追加しました。                                                           | 2024 年 3 月 21 日 |

|                                           |                                                    |                 |
|-------------------------------------------|----------------------------------------------------|-----------------|
| <a href="#">更新: サービスリクエスト管理の仕組みセクション。</a> | AMS が機能リクエストまたはバグを含むサービスリクエストを処理する方法に関する説明を追加しました。 | 2024 年 3 月 21 日 |
| <a href="#">更新: サポートセクションの取得。</a>         | サポートの取得セクションを更新し、新しい請求に関する質問セクションを追加しました。          | 2024 年 3 月 21 日 |
| <a href="#">更新: AMS 自動 IAM プロビジョニング</a>   | カスタム拒否リスト情報で AMS 自動 IAM プロビジョニングを更新                | 2024 年 3 月 21 日 |

## 以前の更新

次の表は、2024 年 3 月以前の AMS Advanced ガイドのドキュメントに対する重要な変更点を示しています。

| 変更                                          | 説明                                                                      | Link                                                               |
|---------------------------------------------|-------------------------------------------------------------------------|--------------------------------------------------------------------|
| 2024 年 2 月                                  |                                                                         |                                                                    |
| サポートされているオペレーティングシステムの更新                    | SUSE Linux Enterprise Server 15 SP5 を含むようにサポートされているオペレーティングシステムを更新しました。 | <a href="#">「サポートされている設定」</a> を参照してください。                           |
| AMS のベースラインモニタリングからのアラートにメモを追加しました。         | EC2 非ルートボリューム使用状況のアラームがデフォルトで無効になっていることを示す注記を追加しました。                    | <a href="#">「AMS でのベースラインモニタリングからのアラート」</a> を参照してください。             |
| モニタリングとイベント管理に新しいセクション AMS イベントルーターを追加しました。 | AMS Advanced Event Router について説明する新しいセクションを追加しました。                      | <a href="#">「AMS での Amazon EventBridge マネージドルールの使用」</a> を参照してください。 |

| 変更                                                               | 説明                                                                                       | Link                                                                                 |
|------------------------------------------------------------------|------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| 更新: AMS AMI ノート                                                  | Zip ファイルには、最新の AMS Amazon マシンイメージ (AMIs) と最新の AMIs。                                      | 「 <a href="#">AMIs.csv-and-notes.02.2024</a> 」を参照してください。                             |
| 2024 年 2 月                                                       |                                                                                          |                                                                                      |
| AMS Advanced の Amazon EventBridge ルールサービス リンクロールの新しいセクションを追加しました | インフラストラクチャセキュリティセクションに、AMS Advanced の Amazon EventBridge ルールサービス リンクロールの新しいセクションを追加しました。 | <a href="#">AMS Advanced の「Amazon EventBridge ルールサービスにリンクされたロール」</a> を参照してください。      |
| 「セルフサービスプロビジョニングモード」セクションを更新しました                                 | セルフサービスプロビジョニングモードで新しい Amazon Inspector の新しいセクションを追加しました。                                | <a href="#">Amazon Inspector Classic (AMS SSPS)</a> 」を参照してください。                      |
| 2024 年 1 月                                                       |                                                                                          |                                                                                      |
| 計画イベント管理 (PEM) セクションを更新しました                                      | 計画イベント管理 (PEM) に詳細と FAW を追加しました。                                                         | 「 <a href="#">AWS Managed Services で計画されたイベント管理</a> 」を参照してください。                      |
| SSM Agent 自動インストールの新しいセクションを追加しました                               | 自動 EC2 インスタンス設定に SSM Agent 自動インストールの新しいセクションを追加しました。                                     | 「 <a href="#">SSM エージェントの自動インストール</a> 」を参照してください。                                    |
| 追加 AWS Resilience Hub (AMS SSPS)                                 | 新しい SSPS サービスを追加しました。                                                                    | 「 <a href="#">AMS SSP を使用して AMS アカウント AWS Resilience Hub でプロビジョニングする</a> 」を参照してください。 |
| 更新: AMS AMI ノート                                                  | Zip ファイルには、最新の AMS Amazon マシンイメージ (AMIs) と最新の AMIs。                                      | 「 <a href="#">AMIs.csv-and-notes.01.2024</a> 」を参照してください。                             |

| 変更                                                   | 説明                                                                     | Link                                                                                                     |
|------------------------------------------------------|------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| 2023 年 12 月                                          |                                                                        |                                                                                                          |
| AMS での直接変更モードの更新                                     | 新しいサブセクション、Direct Change Mode のユースケースを AMS の Direct Change モードに追加しました。 | 「 <a href="#">AMS の直接変更モード</a> 」を参照してください。                                                               |
| 更新 AWS Amplify (AMS SSPS)                            | 「よくある質問」を更新し、Amplify をリクエストするためにリスク承諾が必要であることを明確にしました。                 | 「 <a href="#">AMS SSP を使用して AMS アカウント AWS Amplify でプロビジョニングする</a> 」を参照してください。                            |
| 新規 AWS Elastic Disaster Recovery (AMS SSPS)          | 新しい SSPS サービスを追加しました                                                   | 「 <a href="#">AMS SSP を使用して AMS アカウント AWS Elastic Disaster Recovery でプロビジョニングする</a> 」を参照してください。          |
| 新しい Amazon Managed Service for Prometheus (AMS SSPS) | 新しい SSPS サービスを追加しました                                                   | 「 <a href="#">AMS SSP を使用して AMS アカウントで Amazon Managed Service for Prometheus をプロビジョニングする</a> 」を参照してください。 |
| 「継続性管理の仕組み」セクションを更新しました。                             | 新しいサブセクション「AMS バックアップのモニタリングとレポート」を追加しました。                             | 「 <a href="#">継続性管理の仕組み</a> 」を参照してください。                                                                  |
| 新しい Amazon DevOps Guru (AMS SSPS)                    | 新しい SSPS サービスを追加しました                                                   | 「 <a href="#">AMS SSP を使用して AMS アカウントに Amazon DocumentDB (MongoDB 互換) をプロビジョニングする</a> 」を参照してください。        |

| 変更                                           | 説明                                                                | Link                                                                                              |
|----------------------------------------------|-------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| 更新: AMS AMI ノート                              | Zip ファイルには、最新の AMS Amazon マシンイメージ (AMIs) と最新の AMIs。               | 「 <a href="#">AMIs.csv-and-notes .12.2023</a> 」を参照してください。                                         |
| 2023 年 11 月                                  |                                                                   |                                                                                                   |
| Amazon CloudWatch Synthetics の更新 (AMS SSPS)  | 正しいロール名を使用するようにFAQs。                                              | 「 <a href="#">AMS SSP を使用して AMS アカウントで Amazon CloudWatch Synthetics をプロビジョニングする</a> 」を参照してください。   |
| Amazon API Gateway セルフサービスプロビジョニングモードを更新しました | API Gateway セクションcustomer_apigateway_cloudwatch_role にロールを追加しました。 | 「 <a href="#">AMS SSP を使用して AMS アカウントに Amazon API Gateway をプロビジョニングする</a> 」を参照してください。             |
| セルフサービスプロビジョニングモードに新しいサービスを追加しました            | セルフサービスプロビジョニングモードセクション AWS Service Catalog AppRegistry に追加されました  | 「 <a href="#">AMS SSP を使用して AMS アカウント AWS Service Catalog AppRegistry でプロビジョニングする</a> 」を参照してください。 |
| 更新: AMS AMI ノート                              | Zip ファイルには、最新の AMS Amazon マシンイメージ (AMIs) と最新の AMIs。               | 「 <a href="#">AMIs.csv-and-notes .11.2023</a> 」を参照してください。                                         |

2023 年 9 月

| 変更                         | 説明                                                                                                                                  | Link                                                     |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|
| パッチオーケストレーターの使用にメモを追加      | <p>パッチオーケストレーターの使用セクションに次の注意事項を追加しました。</p> <p>「サポートされていないオペレーティングシステムを持つインスタンス、またはメンテナンスウィンドウ中に停止されたインスタンスでは、パッチ失敗アラートは作成されません」</p> | 「 <a href="#">AMS でのパッチ管理</a> 」を参照してください。                |
| 追加のサービスによるデータ暗号化の更新        | AMS のデータ暗号化にサービスを追加しました。                                                                                                            | 「 <a href="#">AMS でのデータ保護</a> 」を参照してください。                |
| RFC エラーメッセージに新しい段落を追加しました。 | サービスリクエストの作成リンクを追加するための新しい段落を追加しました。                                                                                                | 「 <a href="#">AMS での RFC エラーのトラブルシューティング</a> 」を参照してください。 |
| IAM ロール名を修正しました。           | IAM ロール名 customer_emr_cluster_autoscaling_role を修正しました。                                                                             | 「 <a href="#">AMS でのセルフサービスプロビジョニングモード</a> 」を参照してください。   |
| ベースラインモニタリング情報の更新          | 2 つの非推奨アラーム RDSReadLatencyAlarm と RDSWriteLatencyAlarm への参照を削除しました。                                                                 | 「 <a href="#">AMS でのベースラインモニタリングからのアラート</a> 」を参照してください。  |
| 2023 年 8 月                 |                                                                                                                                     |                                                          |
| 追加: AMS セキュリティインシデント対応     | AMS セキュリティインシデント対応の使用に関するドキュメントを追加しました。                                                                                             | 「 <a href="#">AMS のセキュリティインシデント対応</a> 」を参照してください。        |
| 2023 年 7 月                 |                                                                                                                                     |                                                          |

| 変更                          | 説明                                                                                                                           | Link                                                      |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|
| 追加: 自動 IAM プロビジョニング         | 自動 IAM プロビジョニングの使用に関するドキュメントを追加しました。                                                                                         | 「 <a href="#">自動 IAM プロビジョニング AMS</a> 」を参照してください。         |
| 更新: アクセスロールテーブル             | AMS Access に欠落しているロールを追加しました。                                                                                                | 「 <a href="#">AMS カスタマーアカウント アクセス IAM ロール</a> 」を参照してください。 |
| 2023 年 6 月                  |                                                                                                                              |                                                           |
| 更新: モニタリング対象の RDS アラートのリスト。 | AMS ベースラインモニタリングの RDS アラートのリストを更新しました。9 つの新しい RDS アラートタイプが追加され、3 つの既存の RDS アラートタイプが削除されました。                                  | 「 <a href="#">AMS でのベースラインモニタリングからのアラート</a> 」を参照してください。   |
| 更新: アクセスロールテーブル             | AMS セキュリティの新しいロール。                                                                                                           | 「 <a href="#">AMS カスタマーアカウント アクセス IAM ロール</a> 」を参照してください。 |
| 2023 年 5 月                  |                                                                                                                              |                                                           |
| 更新: サービス請求開始日ポリシー。          | 請求開始日の定義を更新しました。                                                                                                             | 「 <a href="#">AMS の主要な用語</a> 」を参照してください。                  |
| 2023 年 4 月                  |                                                                                                                              |                                                           |
| 更新: 月次請求セルフサービスレポート。        | 注: 月別請求レポートは Management Payer アカウント (AMS Advanced マルチアカウントランディングゾーン) でのみ使用できますが、リンクされたすべての AMS Accelerate マネージドアカウントで使用できます。 | 「 <a href="#">請求レポート (毎月)</a> 」を参照してください。                 |



| 変更                                 | 説明                                                  | Link                                                                    |
|------------------------------------|-----------------------------------------------------|-------------------------------------------------------------------------|
| 更新: 「標準パッチ」コンテンツを削除                | AMS はパッチオーケストレーターを使用します。                            | <a href="#">AMS でのパッチ管理</a>                                             |
| 更新: AMS とは                         | 以前に「AMS とは」のトピックをいくつか移動しました。は AMS サービスの説明の一部になります。  | <a href="#">サービスの説明</a>                                                 |
| 更新: マルチアカウントランディングゾーンのオフボーディング     | さまざまな明確化を行いました。                                     | <a href="#">AMS マルチアカウントランディングゾーンアカウントからのオフボード</a>                      |
| 更新: AWS Transfer Family (AMS SSPS) | 転送セットアップチュートリアルへのリンクを追加しました。                        | <a href="#">AMS SSP を使用して AMS アカウント AWS Transfer Family でプロビジョニングする</a> |
| 更新されたコンテンツ: セルフサービスプロビジョニング        | AWS legal に従ってCodeSuiteを「Code services」に置き換えました。    | <a href="#">AMS SSP を使用して AMS アカウントで AMS Code サービスをプロビジョニングする</a>       |
| 更新されたコンテンツ: CloudWatch メトリクスとアラーム  | <a href="#">例: 用語の出現数をカウントするへのリンクを追加しました。</a>       | <a href="#">AMS でのカスタム CloudWatch メトリクスとアラームの作成</a>                     |
| 更新: AMS AMI ノート                    | Zip ファイルには、最新の AMS Amazon マシンイメージ (AMIs) と最新の AMIs。 | <a href="#">AMIs.csv-and-notes.04.2023</a>                              |
| 2023 年 3 月                         |                                                     |                                                                         |
| 更新されたコンテンツ: AMS からのオフボーディング        | マルチアカウントランディングゾーンアカウントをオフボードするときに削除するリソースを明確にしました   | <a href="#">AMS マルチアカウントランディングゾーンアカウントからのオフボード</a>                      |

| 変更                          | 説明                                                                   | Link                                       |
|-----------------------------|----------------------------------------------------------------------|--------------------------------------------|
| 更新: AMS AMIs                | Doc History セクションに、毎月の AMI ZIP ファイルへのリンクを追加しました。                     | <a href="#">ドキュメント履歴</a>                   |
| 更新: 自動修復                    | EC2 ボリュームオートメーションの LVM サポートを削除しました。                                  | <a href="#">アラートの AMS 自動修復</a>             |
| 更新: パッチ RACI                | パッチ適用のための RACI のいくつかの更新と明確化。                                         | <a href="#">AMS 責任マトリックス (RACI)</a>        |
| 更新されたコンテンツ: セルフサービスプロビジョニング | よくある質問の箇条書きを追加しました。新しい AWS Datasync エージェントを起動するには、WIGS 取り込みは必要ありません。 | <a href="#">AMS でのセルフサービスプロビジョニングモード</a>   |
| 更新されたコンテンツ: セルフサービスプロビジョニング | よくある質問の箇条書きを追加しました。新しい AWS Datasync エージェントを起動するには、WIGS 取り込みは必要ありません。 | <a href="#">AMS でのセルフサービスプロビジョニングモード</a>   |
| 更新: AMS AMI ノート             | Zip ファイルには、最新の AMS Amazon マシンイメージ (AMIs) と最新の AMIs。                  | <a href="#">AMIs.csv-and-notes.03.2023</a> |
| 2023 年 2 月                  |                                                                      |                                            |
| 更新されたコンテンツ: AMS からのオフボーディング | マルチアカウントランディングゾーン環境、VPCs、およびアプリケーションアカウントをオフボードする方法を明確にしました          | <a href="#">AMS アカウントのオフボード</a>            |

| 変更                          | 説明                                                                                                                                                                                                                                                                                                                                                                                                           | Link                                              |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|
| 更新されたコンテンツ: ARNs の検索        | DynamoDB describe-table テーブル ARN を検索するための DynamoDB CLI を追加                                                                                                                                                                                                                                                                                                                                                   | <a href="#">AMS で Amazon リソースネーム (ARNs) を検索する</a> |
| 更新されたコンテンツ: セルフサービスプロビジョニング | 実際の SSPS ではないため、AMS "CodeSuite" オプションを削除しました。Management   AWS service   Self-provisioned service   Add (マネージドオートメーション) (ct-3qe6io8t6jtny) 変更タイプを使用し、CodeBuild、CodeDeploy、CodePipeline の 3 つのサービスをリクエストできます。その後、AMS は、customer_codebuild_service_role 、customer_codedeploy_service_role および の IAM ロールをアカウントにプロビジョニングしますaws_code_pipeline_service_role 。アカウントでプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。 | <a href="#">AMS でのセルフサービスプロビジョニングモード</a>          |

| 変更                                    | 説明                                                                  | Link                                                              |
|---------------------------------------|---------------------------------------------------------------------|-------------------------------------------------------------------|
| 更新されたコンテンツ: Secrets Manager の更新       | マルチアカウントランディングゾーン (MALZ) とシングルアカウントランディングゾーン (SALZ) に必要なロールを修正しました。 | <a href="#">Secrets Manager を使用したキーの共有に関するよくある質問</a>              |
| 更新されたコンテンツ: アラートの AMS 自動修復            | Logical Volume Manager (LVM) ボリュームのサポートが追加されました。                    | <a href="#">EC2 ボリューム使用量修復の自動化</a>                                |
| 更新されたコンテンツ: AMS Amazon マシンイメージ (AMIs) | アカウントから AMIs を削除するためのサンプルコードを使用して AMS AMIs オフボードするセクションを追加しました。     | <a href="#">AMS Amazon マシンイメージ (AMIs)</a>                         |
| 更新されたコンテンツ: IAM ユーザーロール               | IAM ポリシー AMSBillingPolicy を更新しました。                                  | <a href="#">AMS の IAM ユーザーロール</a>                                 |
| 新しいコンテンツ: サポートされていない OSes             | AMS がサポート対象外のオペレーティングシステム (OSes)。                                   | <a href="#">AMS でサポートされていないオペレーティングシステムの機能</a>                    |
| 更新されたコンテンツ: オンデマンドレポート                | 特定のオンデマンドレポートは AMS Advanced で使用できず、利用可能と誤って表示されました。                 | <a href="#">リクエスト時レポート</a>                                        |
| 更新されたコンテンツ: AMS アカウントのオフボーディング        | MALZ アプリケーションアカウントをオフボーディングする手順を明確にしました。                            | <a href="#">AMS アプリケーションアカウントのオフボード</a>                           |
| 更新されたコンテンツ: Secrets Manager           | Secrets Manager の使用に必要な IAM ロールの名前を修正しました。                          | <a href="#">AWS Managed Services の Secrets Manager に関するよくある質問</a> |

| 変更                                   | 説明                                                              | Link                                                                           |
|--------------------------------------|-----------------------------------------------------------------|--------------------------------------------------------------------------------|
| 更新: AMS AMI ノート                      | Zip ファイルには、最新の AMS Amazon マシンイメージ (AMIs) と最新の AMIs。             | <a href="#">AMIs.csv-and-notes.02.2023</a>                                     |
| 2023 年 1 月                           |                                                                 |                                                                                |
| 新しいコンテンツ: AWS Device Farm (AMS SSPS) | 新しい SSPS サービス: AWS Device Farm を追加しました。                         | <a href="#">AMS SSP を使用して AMS アカウント AWS Device Farm でプロビジョニングする</a>            |
| 更新: サポートされている Windows バージョン          | Windows Server 2022 のサポートが追加されました。                              | <a href="#">AMS Amazon マシンイメージ (AMIs)、サポートされている設定、および SNS を使用した AMS AMI 通知</a> |
| 更新: 継続性管理                            | デフォルトの AMS バックアッププランのルールを更新しました。                                | <a href="#">デフォルトのバックアッププラン、マルチアカウントランディングゾーン</a>                              |
| 更新: AMS AMI ノート                      | Zip ファイルには、最新の AMS Amazon マシンイメージ (AMIs) と最新の AMIs。             | <a href="#">AMIs.csv-and-notes.01.2023</a>                                     |
| 2022 年 12 月                          |                                                                 |                                                                                |
| 更新: 踏み台の使用                           | 不正なリンクを修正しました。                                                  | <a href="#">踏み台を使用したインスタンスへのアクセス</a>                                           |
| 更新: Resource Scheduler               | いくつかの改善を行い、より多くのコンテキストのために AWS Instance Scheduler へのリンクを追加しました。 | <a href="#">AWS Managed Services リソーススケジューラ</a>                                |

| 変更                                                 | 説明                                                                                                                                                                                                                                                                                                           | Link                                                                  |
|----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| 更新: Windows AMIsとサポートされている設定 (新しい Windows AMIsの場合) | EC2Launch (Windows Server 2016 以降) から EC2Launch (Windows Server 2016 および Windows Server 2019) に追加された AMS AMI コンテンツを更新し、EC2LaunchV2 (Windows Server 2022 以降) を追加しました。Microsoft Windows Server (2012、2012 R2、2016、2019) から Microsoft Windows Server (2012、2012 R2、2016、2019、2022) に Windows ベースの AMIs を更新しました。 | <a href="#">AMS Amazon マシンイメージ (AMIs)</a> および <a href="#">サービスの説明</a> |
| 更新: Resourced Scheduler セクション                      | AMS Resource Scheduler のデプロイとカスタマイズの方法を改善しました。                                                                                                                                                                                                                                                               | <a href="#">AWS Managed Services リソーススケジューラ</a>                       |
| 更新: AMS の設定: プライベートおよびパブリック DNS                    | DNS アーキテクチャ図を更新しました。                                                                                                                                                                                                                                                                                         | <a href="#">プライベート DNS とパブリック DNS のセットアップ</a>                         |
| 更新: MALZ ネットワークアーキテクチャ                             | Accelerate アプリケーションアカウントの図を更新し、ガイダンスを追加しました。                                                                                                                                                                                                                                                                 | <a href="#">MALZ ネットワークアーキテクチャ</a>                                    |
| 更新: セットアップ: タグの使用                                  | 新しい注意: カスタムタグ付けは、コアアカウントではなく MALZ アプリケーションアカウントでのみサポートされています。                                                                                                                                                                                                                                                | <a href="#">AMS インフラストラクチャの自動タグ付け</a>                                 |
| 更新: アクセス管理: 踏み台の使用                                 | RDP 踏み台の導入を更新しました。                                                                                                                                                                                                                                                                                           | <a href="#">単一アカウントランディングゾーン (SALZ) 踏み台でのコスト削減</a>                    |

| 変更                                   | 説明                                                                  | Link                                                                                       |
|--------------------------------------|---------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| 更新: AMS デフォルト設定: アラート                | EC2 インスタンス: 非ルートボリューム使用状況をアラートのテーブルに追加しました。                         | <a href="#">AMS でのベースラインモニタリングからのアラート</a>                                                  |
| 更新: 継続性管理                            | 継続的バックアップに関するガイダンスを追加しました。                                          | <a href="#">継続性管理の仕組み</a>                                                                  |
| 更新: EC2 インスタンスの自動設定                  | PowerBroker Identity Service (PBIS) とインスタンスコード (OIC) のサポートが追加されました。 | <a href="#">Linux インスタンスで PBIS を自動的に更新する</a> および <a href="#">Linux インスタンスでコードを自動的に更新する</a> |
| 更新: Secrets Manager のセルフサービスプロビジョニング | Secrets Manager をアカウントに追加するための CT を更新FAQsの下 )。                      | <a href="#">AMS SSP を使用して AMS アカウント AWS Secrets Manager でプロビジョニングする</a>                    |
| 更新: ログ管理                             | EC2 システムレベルのログのリストを更新しました。                                          | <a href="#">Amazon Elastic Compute Cloud (Amazon EC2) - システムレベルのログ</a>                     |
| 更新: AMS AMI ノート                      | Zip ファイルには、最新の AMS Amazon マシンイメージ (AMIs) と最新の AMIs。                 | AMIs.csv-and-notes.12.2022                                                                 |
| 2022 年 11 月                          |                                                                     |                                                                                            |
| 更新: AMS Amazon マシンイメージ (AMIs)        | サポートされている SUSE Linux バージョンを更新しました。                                  | <a href="#">AMS Amazon マシンイメージ (AMIs)</a>                                                  |
| 更新: MALZ アカウント                       | カスターマネージドアプリケーションアカウントを削除するガイダンスを追加しました。                            | <a href="#">カスターマネージドアプリケーションアカウント</a>                                                     |

| 変更                            | 説明                                                                       | Link                                               |
|-------------------------------|--------------------------------------------------------------------------|----------------------------------------------------|
| 更新: AMS のセットアップ               | customer-ams-amazon2-security-enhanced が追加されました。                         | <a href="#">SNS を使用した AMS AMI 通知</a>               |
| 更新: モニタリングの仕組み                | サービス通知とインシデントレポートの説明を更新しました。                                             | <a href="#">モニタリングの仕組み</a>                         |
| 更新: MALZ アプリケーションアカウントタイプ     | アカウントタイプの説明を改善しました。                                                      | <a href="#">アプリケーションアカウントタイプ</a>                   |
| 更新: デベロッパーモード                 | デベロッパーモードに関する警告を追加しました。                                                  | <a href="#">AMS デベロッパーモードを開始する前に</a>               |
| 更新: 計画されたイベント管理               | 「PEM のタイプ」セクションを追加しました。                                                  | <a href="#">AWS Managed Services での計画されたイベント管理</a> |
| 更新: Amazon マシンイメージ (AMIs)     | サポートされている SUSE Linux バージョンを更新しました                                        | <a href="#">AMS Amazon マシンイメージ (AMIs)</a>          |
| 更新: AMS AMI ノート               | Zip ファイルには、最新の AMS Amazon マシンイメージ (AMIs) と最新の AMIs。                      | <a href="#">AMIs.csv-and-notes.11.2022</a>         |
| 2022 年 10 月                   |                                                                          |                                                    |
| 新規: 自動インスタンス設定                | 新しいセクションでは、自動インスタンス設定プロセスについて説明します。                                      | <a href="#">AMS Advanced の自動インスタンス設定</a>           |
| 新規: 手動 CT のみが一部の SSPS で許容されます | SSPS を追加するための自動 CT ではなく、手動 CT を使用するように 50 を超えるセルフサービスプロビジョニングサービスの FAQs。 | <a href="#">AMS でのセルフサービスプロビジョニングモード</a>           |



| 変更                         | 説明                                                                                                | Link                                          |
|----------------------------|---------------------------------------------------------------------------------------------------|-----------------------------------------------|
| 更新: AMS のセットアップ            | MALZ の Amazon EC2 IAM インスタンスプロファイルに 2 つのポリシーを追加しました。                                              | <a href="#">EC2 IAM インスタンスプロファイル</a>          |
| 新規: カスタム検出ルールと予防ルールのライブラリ。 | 複数の顧客からの学習に基づいて、一連のサービスコントロールポリシー (SCPs) の例と予防的 Config ルールコントロールを追加しました。                          | <a href="#">厳選された SCPs と Config ルール</a>       |
| 更新: AWS Backup 警告          | 「変更が失われる可能性があるため、AMS バックアッププランを編集しないでください。代わりに、カスタム設定に ct-2hyozbpa0sx0m を使用して新しいバックアッププランを作成します。」 | <a href="#">継続性管理の仕組み</a>                     |
| 更新: AWS Backup 注意          | フェデレーションへの新しい IAM ロールの追加に関するメモを追加しました。                                                            | <a href="#">AMS Advanced での IAM リソースのデプロイ</a> |
| 更新: 管理のモニタリング              | アラートはサービスリクエストではなくインシデントレポートを生成します。                                                               | <a href="#">モニタリングの仕組み</a>                    |
| 更新: 独自の EPS を使用する          | SALZ と MALZ に適用されます。                                                                              | <a href="#">AMS が独自の EPS を導入する</a>            |
| 更新: アプリケーションアカウントの高速化      | Accelerate アカウントがアプリケーションアカウントであることを明確にしました。                                                      | <a href="#">アプリケーションアカウントタイプ</a>              |

| 変更                          | 説明                                                                       | Link                                          |
|-----------------------------|--------------------------------------------------------------------------|-----------------------------------------------|
| 更新: AMS AMI ノート             | Zip ファイルには、最新の AMS Amazon マシンイメージ (AMIs) と最新の AMIs。                      | <a href="#">AMIs.csv-and-notes.10.2022</a>    |
| 2022 年 9 月                  |                                                                          |                                               |
| 更新: リソースを検索するための CLI コマンドの例 | 新しい例を追加し、 -- region オプションが必要になる可能性があることを追加しました。                          | <a href="#">必要なデータ (SKMS)、AMS の検索</a>         |
| 更新: IAM ロールのプロビジョニング        | IAM ロールを で作成および管理できるようになりましたAWSManagedServices CloudFormationAdminRole 。 | <a href="#">Direct Change モードを使用したスタックの作成</a> |
| 更新: AMS 技術標準                | AMS-STD-007 ログ記録: (#20) 転送要件を明確にしました。                                    | <a href="#">セキュリティとコンプライアンス</a>               |
| 更新: 継続性管理の仕組み               | バックアップジョブの開始の文言を「既存」ではなく「オンデマンド」に改訂しました。                                 | <a href="#">継続性管理の仕組み</a>                     |
| 更新: セキュリティとコンプライアンス         | 標準 AMS-STD-007 番号 20: アカウント間のログ転送の説明とガイダンスを更新しました。                       | <a href="#">セキュリティとコンプライアンス</a>               |
| 更新: 変更管理のユースケース             | レガシー変更管理ユーザーガイドへの壊れたリンクを削除しました。                                          | <a href="#">変更管理のユースケース</a>                   |

| 変更              | 説明                                                  | Link                                       |
|-----------------|-----------------------------------------------------|--------------------------------------------|
| 更新: AMS AMI ノート | Zip ファイルには、最新の AMS Amazon マシンイメージ (AMIs) と最新の AMIs。 | <a href="#">AMIs.csv-and-notes.09.2022</a> |
| 2022 年 8 月 11 日 |                                                     |                                            |

| 変更                                                   | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Link                                    |
|------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|
| 更新: 一貫性と読みやすさのための章見出し、いくつかのトピックサブセクションをより適切なセクションに移動 | <p>「MALZ ネットワークアーキテクチャ」と「SALZ ネットワークアーキテクチャ」は、最上位の「ネットワークアーキテクチャ」セクションのサブセクション、以前は「AMS ネットワークアーキテクチャ」セクションになりました。</p> <p>「変更管理の変更」は「変更管理」の新しい見出しです。</p> <p>「デフォルト設定」は「AMS の設定」のサブセクションになりました</p> <p>「AD FS クレームルールと SAML 設定」(以前のActiveDirectory フェデレーションサービス (ADFS) クレームルールと SAML 設定) が「AMS の設定」のサブセクションになりました。</p> <p>「アクセス管理」は「AMS でのアクセス」の新しい見出しであり、TOC で移動されます。</p> <p>「必要なデータを見つける」が「サービスナレッジ管理」の新しい見出しです。</p> <p>「レポートとオプション」は「AMS Reporting」の新しい</p> | <a href="#">AWS Managed Services とは</a> |

| 変更                                 | 説明                                                                      | Link                                                                                               |
|------------------------------------|-------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
|                                    | 見出しであり、TOC では下位にあります。<br><br>「Operations on Demand」が TOC の最後のトピックになりました |                                                                                                    |
| 更新: 検出結果と ARN、新規: ARN を使用したリソースの検索 | どちらの手順も、役に立つように完全に書き換えられています。                                           | 「 <a href="#">AMS で Amazon リソースネーム (ARNs) を検索する</a> 」および「 <a href="#">AMS で ARN 別にリソースを検索する</a> 」。 |
| 更新: CMA と Transit Gateway の接続      | 自動化は、コアルートドメインへのルートの追加、および更新が必要な手順をサポートしていません。                          | <a href="#">CMA と Transit Gateway の接続</a>                                                          |
| 更新: MALZ 基本コンポーネントの料金              | すべての料金は米ドルで、ドル記号で表示されます。                                                | <a href="#">AMS 環境の基本コンポーネント</a>                                                                   |
| 更新: AMS AMI ノート                    | Zip ファイルには、最新の AMS Amazon マシンイメージ (AMIs) と最新の AMIs。                     | <a href="#">AMIs.csv-and-notes.08.2022</a>                                                         |
| 2022 年 7 月 14 日                    |                                                                         |                                                                                                    |
| 更新: セルフサービスレポート                    | KMS キーを使用して AWS Glue メタデータを暗号化する手順を追加しました。                              | <a href="#">セルフサービスレポート</a>                                                                        |
| 更新: AMS ベースラインモニタリング               | DeleteRecoveryPoint バックアップアラートを追加しました。                                  | <a href="#">AMS でのベースラインモニタリングからのアラート</a>                                                          |
| 更新: サポートされているオペレーティングシステム          | Amazon Linux 2 のサポート終了日を追加しました。                                         | <a href="#">サポートされている設定</a>                                                                        |

| 変更                  | 説明                                                                                      | Link                                                                    |
|---------------------|-----------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| 更新: セルフサービスプロビジョニング | AWS Transfer SSPS の前提条件を追加しました。                                                         | <a href="#">AMS SSP を使用して AMS アカウント AWS Transfer Family でプロビジョニングする</a> |
| 更新: AMS レポート        | オプトインリージョンに関する注意事項を追加しました。                                                              | <a href="#">レポートとオプション</a>                                              |
| 更新: RFC の対応と添付ファイル  | 許可されたテキストファイルタイプを明確にしました。特に、YAML ファイルは .yaml (.yml ではなく) で終わる必要があります。                   | <a href="#">RFC コレスポネンスとアタッチメントを追加する (コンソール)</a>                        |
| 2022 年 6 月 21 日     |                                                                                         |                                                                         |
| 更新された内容             | 以前は「変更管理モード」または「標準 CM モード」と呼ばれていた AMS モードは、「RFC モード」と呼ばれるようになりました。モードセクションが展開されました。     | <a href="#">モードの概要</a>                                                  |
| 新しいアラーム             | AWS Backup アラームを追加しました。                                                                 | <a href="#">AMS でのベースラインモニタリングからのアラート</a>                               |
| 2022 年 6 月 16 日     |                                                                                         |                                                                         |
| 新しいコンテンツ            | インシデント管理。セキュリティリスクではないインシデントは、インシデントレポートでの承認により AMS で解決できるようになりました。個別の RFC と承認は必要ありません。 | <a href="#">インシデント管理</a>                                                |

| 変更      | 説明                                                                                                                                                                                                                                                                                                                                                              | Link                                                                     |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| 更新された内容 | MALZ: ネットワークアーキテクチャ図を更新しました。更新: マスターアカウント VPC から共有サービス vpc への VPC ピアリングは、存在しないため削除する必要があります。                                                                                                                                                                                                                                                                    | <a href="#">ネットワークアカウントアーキテクチャ</a>                                       |
|         | Sagemaker セルフサービス プロビジョニングサービス (SSPS)。Sagemaker 用にオンボーディング時に追加された新しい IAM ロールで更新されました。                                                                                                                                                                                                                                                                           | <a href="#">AMS SSP を使用して AMS アカウントに Amazon SageMaker AI をプロビジョニングする</a> |
|         | SNS 通知でサポートされている AMIs のリスト: customer-ams-sles12、customer-ams-sles15、customer-ams-amazon1-security-enhanced、customer-ams-rhel8、customer-ams-rhel8-security-enhanced、customer-ams-ubuntu18、customer-ams-windows2012、customer-ams-windows2019、customer-ams-windows2019-security-enhanced を追加しました。customer-ams-rhel6 および customer-ams-rhel6-security-enhanced AMIs。 | <a href="#">SNS を使用した AMS AMI 通知</a>                                     |
|         | エスカレーション E メールを削除しました。                                                                                                                                                                                                                                                                                                                                          | <a href="#">AWS Managed Services でのヘルプの取得</a>                            |

| 変更                                                                   | 説明                                                                                                                                                   | Link                                          |
|----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
|                                                                      | トピックリストを開いた段落の下に移動しました。                                                                                                                              | <a href="#">AWS Managed Services とは</a>       |
|                                                                      | サービスログを更新し、ロードバランシングログのリンクも改善しました。                                                                                                                   | <a href="#">AMS 集計サービスログ</a>                  |
| EKS セルフサービスプロビジョニングサービス (SSPS)。クラスターでエンベロープシークレット暗号化を有効にする情報を追加しました。 | <a href="#">AMS SSP を使用して AMS アカウントの AWS Fargate で Amazon EKS をプロビジョニングする</a>                                                                        |                                               |
| 2022 年 6 月 9 日                                                       |                                                                                                                                                      |                                               |
| 更新されたコンテンツ、ヘルプの取得                                                    | エスカレーションパス E メールを削除しました。AMS は、インシデントレポート、サービスリクエスト、RFCsを通じて通信方法を提供します。                                                                               | <a href="#">AWS Managed Services でのヘルプの取得</a> |
| 2022 年 5 月 12 日                                                      |                                                                                                                                                      |                                               |
| 新しいコンテンツ、Operations on Demand (OOD) サブスクリプションモデル                     | AMS は、Operations on Demand オンボーディングを現在のサインアップおよび更新モデルからサブスクリプション割り当ておよびデフォルトのオプトインモデルに変更しました。AMS アカウントをオンボーディングすると、Operations on Demand に自動的に登録されます。 | <a href="#">オペレーションオンデマンド</a>                 |
| 2022 年 4 月 14 日                                                      |                                                                                                                                                      |                                               |



| 変更                                           | 説明                                                                                  | Link                                                                         |
|----------------------------------------------|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| 新しいコンテンツ、コスト最適化                              | AMS は、コスト最適化に関する推奨事項を提供します。                                                         | <a href="#">AWS Managed Servicesコスト最適化</a>                                   |
| 更新されたコンテンツ、MALZ の Accelerate アカウント           | 誤ったロール名 (Customer DefaultAdminRole) が正しいロール名 (AccelerateDefaultAdminRole) に更新されました。 | <a href="#">AMS Accelerate アカウント</a><br>「Accelerate アカウントへのアクセス」セクション。       |
| 更新されたコンテンツ、AMS アクセス IAM ロール                  | アカウントへのアクセスに使用される他の AMS IAM ロールを追加しました。                                             | <a href="#">AMS がアカウントにアクセスする理由とタイミング</a> 「AMS カスタマーアカウントアクセス IAM ロール」セクション。 |
| 更新されたコンテンツ、AMS バックアッププラン                     | AMS マネージドバックアッププランを追加しました。                                                          | <a href="#">AMS バックアッププラン</a> および <a href="#">AMS バックアップポータル</a>             |
| 更新されたコンテンツ、AWS Secrets Manager               | よくある質問を更新しました。                                                                      | <a href="#">AMS SSP を使用して AMS アカウント AWS Secrets Manager でプロビジョニングする</a>      |
| 更新されたコンテンツ、Direct Change Mode (DCM) オンボーディング | AMS は、Service Catalog のお客様の DCM へのオンボーディングをサポートしていません。                              | <a href="#">直接変更モードの開始方法</a>                                                 |

| 変更                             | 説明                                                                                                                                                                                                                                                                                                                   | Link                                    |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|
| 更新されたコンテンツ、サービスの説明             | <p>サポートされているサービスのセクションを明確にしました。</p> <ul style="list-style-type: none"><li>• AWS Fargate での Amazon EKS -&gt; Fargate での Amazon Elastic Kubernetes Service</li><li>• Amazon ECS for Fargate -&gt; AWS Fargate での Amazon Elastic Container Service</li><li>• Amazon Kinesis -&gt; Amazon Kinesis Data Streams</li></ul> | <a href="#">サポートされている AWS サービス</a>      |
| 更新されたコンテンツ、MALZ アカウントのオフボーディング | アプリケーションアカウントをオフボーディングするための新しい変更タイプを参照するように更新されました。                                                                                                                                                                                                                                                                  | <a href="#">AMS アプリケーションアカウントのオフボード</a> |
| 更新されたコンテンツ、デベロッパーモードのインシデント管理  | インシデント SLA の説明をに更新しました。AMS SLA は、AMS 変更管理の外部で作成または更新されたリソース (デベロッパーモードを含む) には適用されません。したがって、デベロッパーモードで更新または作成されたリソースは自動的に P3 に低下し、サポートがベストエフォートです。                                                                                                                                                                    | <a href="#">AMS デベロッパーモードでのインシデント管理</a> |
| 更新されたコンテンツ、DCM オンボーディング        | 新しい DCM の RFC テンプレートに、SAML プロバイダー ARN の フィールドが含まれるようになりました。                                                                                                                                                                                                                                                          | <a href="#">直接変更モードの開始方法</a>            |

| 変更                                 | 説明                                                                                     | Link                                                                            |
|------------------------------------|----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| 更新されたコンテンツ、DCM for CloudFormation  | CloudFormation スタックを作成および更新する手順に YAML の例が含まれるようになりました。                                 | <a href="#">AMS 変換</a>                                                          |
| 更新されたコンテンツ、MALZ Tools アカウント        | 移行用の新しい IAM ロールがあります: AWSManagedServicesMigration Role 。                               | <a href="#">AWS アプリケーション移行サービス (AWS MGN) および新しい AMS Tools アカウントへのアクセスを有効にする</a> |
| 新しいコンテンツ、マルチアカウントランディングゾーンアカウント    | マルチアカウントランディングゾーン AMS 管理アカウントで Accelerate アカウントを作成できます。                                | <a href="#">AMS Accelerate アカウント</a>                                            |
| 更新されたコンテンツ、API/ CLI SDK のインストール    | インストール手順に、Mac/ Linux インストールのファイル名が正しくないか、コマンドが正しくありません。この問題は修正されました。                   | <a href="#">AMS API と CLI の使用</a>                                               |
| 更新されたコンテンツ、MALZ の Accelerate アカウント | 誤ったルール名 (Customer DefaultAdminRole) があり、正しいルール名 (AccelerateDefaultAdminRole) に更新されました。 | <a href="#">AMS Accelerate アカウント</a> 、「Accelerate アカウントへのアクセス」セクション             |
| 更新されたコンテンツ、モニタリング                  | ルート使用状況モニタリングが 85% から 95% に改訂されました。                                                    | <a href="#">AMS でのベースラインモニタリングからのアラート</a>                                       |
| 更新されたコンテンツ、AMI 通知                  | 新しい AMS AMIs にはさまざまなタイプの SNS 通知を作成できます。さまざまなタイプの作成に関する情報を追加しました。                       | <a href="#">SNS を使用した AMS AMI 通知</a>                                            |

| 変更                                             | 説明                                                                                                             | Link                                                                  |
|------------------------------------------------|----------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| 更新されたコンテンツ、AMS のデフォルト設定                        | Macie Classic への参照を削除し、Macie に置き換えました。                                                                         | <a href="#">AMS でのベースラインモニタリングからのアラート</a>                             |
| 更新されたコンテンツ、AMS 予約プレフィックス                       | リザーブドプレフィックスのリストをアルファベット化しました。                                                                                 | <a href="#">AMS 予約プレフィックス</a>                                         |
| 更新されたコンテンツ、サービスの説明                             | 変更管理とセルフサービスプロビジョニングの機能セクションが AMS モードの詳細で更新されました。                                                              | <a href="#">AWS Managed Services (AMS) AMS Advanced オペレーションプランの機能</a> |
|                                                |                                                                                                                |                                                                       |
| 更新されたコンテンツ、AWS Secrets Manager                 | Secrets Manager を使用したキーの共有。                                                                                    | 2022 年 2 月 10 日                                                       |
| 新しいコンテンツ、セルフサービスプロビジョニング、Amazon Connect        | 発信通話または着信通話の国のリストの追加をリクエストする方法に関するよくある質問を追加しました。                                                               | 2022 年 2 月 10 日                                                       |
| 新しいコンテンツ、セルフサービスプロビジョニング、Fargate での Amazon EKS | AWS Cloud Development Kit (CDK) または CloudFormation Ingest を介した EKS クラスターのデプロイが AMS でサポートされないという FAQ 制限を追加しました。 | 2022 年 2 月 10 日                                                       |
| 変更されたコンテンツ、デベロッパーモード                           | 修正。RFC またはサービスリクエストを使用してフェデレーションソリューションにユーザーを割り当ててではなく、ソリューションに応じて自分で割り当てます。                                   | 2022 年 2 月 10 日                                                       |

| 変更                           | 説明                                                                           | Link            |
|------------------------------|------------------------------------------------------------------------------|-----------------|
| 変更されたコンテンツ、直接<br>変更モード (DCM) | IAM は DCM ではサポートされていないことに注意してください。                                           | 2022 年 2 月 10 日 |
|                              | DCM、検証を書き留めます。                                                               | 2022 年 2 月 10 日 |
|                              | DCM、さまざまなロールの制限を明確にします。                                                      | 2022 年 2 月 10 日 |
| コンテンツの変更、ベースラインアラートのモニタリング   | Redshift クラスターリソースアラートが変更されました。                                              | 2022 年 2 月 10 日 |
| コンテンツの変更、セルフサービスレポート         | お客様がレポートを取得するために使用する正確な s3 バケット名 (ams-reporting-data-a<Account_ID>) を追加しました。 | 2022 年 2 月 10 日 |

| 変更                                                   | 説明                                                                                                                                                                                                                                                                           | Link            |
|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| 手動管理ではなく自動変更タイプを参照するようにコンテンツを変更、更新   その他   その他 (MOO) | <p>自動変更タイプ (3 つ、<br/>「TGW アタッチメントをルートテーブルに関連付ける」、<br/>「この VPC に接続する TGW ルートテーブルにルートを作成する」、<br/>「AMS マルチアカウントランディングゾーントランジットゲートウェイを指すように VPC ルートテーブルを設定する」) を参照するように、マルチアカウントランディングゾーン (MALZ) アプリケーションアカウントのコンテンツを更新しました。</p> <p>AMS によって生成されたアラートの受信</p> <p>タグベースのアラート通知</p> | 2022 年 2 月 10 日 |
| 変更内容: AMS AMIs。                                      | <p>セキュリティ強化 AMIs に関する新しい情報を追加しました。<a href="#">サポートされている設定</a>、<a href="#">AMS Amazon マシンイメージ (AMIs)</a>、および <a href="#">セキュリティ強化 AMIs</a> を参照してください。</p>                                                                                                                     | 2022 年 1 月 27 日 |
| 新しいコンテンツ: セルフサービスプロビジョニング。                           | <p>Amazon Fsx for OpenZFS を追加しました。「<a href="#">AMS SSP を使用して AMS アカウントで Amazon FSx for OpenZFS をプロビジョニングする</a>」を参照してください。</p>                                                                                                                                                | 2022 年 1 月 27 日 |

| 変更                                             | 説明                                                                                                                                                              | Link            |
|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| 変更内容: Code-Deploy セルフサービスプロビジョニング サービス (SSPS)。 | 追加のロール名と追加の制限に関する注意事項。「」を参照してください <a href="#">AMS SSP を使用して AMS アカウント AWS CodeDeploy でプロビジョニングする</a> 。                                                          | 2022 年 1 月 27 日 |
| 変更内容: リンクを更新しました。                              | 壊れたリンクを修正しました: AMS-AMIs、設定の検索、スタック ID の検索、VPC ID の検索、ListVpcSummaries、ListStackSummaries、GetStack APIs 例については、「 <a href="#">AMS でスタック IDs を検索する</a> 」を参照してください。 | 2022 年 1 月 13 日 |
| 変更内容: Fargate の EKS サポート                       | FAQs: EKS を使用した EC2 ノードグループの作成または管理はサポートされていません。「 <a href="#">AMS SSP を使用して AMS アカウントの AWS Fargate で Amazon EKS をプロビジョニングする</a> 」を参照してください。                     | 2022 年 1 月 13 日 |
| 変更内容: CloudFormation、直接変更モード (DCM)             | AmsStackTransform を使用して CF スタックを作成または更新する手順を追加しました。「 <a href="#">Direct Change モードを使用したスタックの作成</a> 」を参照してください。                                                  | 2022 年 1 月 13 日 |

| 変更                                                      | 説明                                                                                                                                                                                    | Link            |
|---------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| 変更内容: AWS サービス名の統一性                                     | への AMS リファレンスは、公式の AWS タイトルまたはメタデータと AWS のサービス完全に一致します。以前は、パターンマッチングが複雑な小さなバリエーションがありました。例については、「 <a href="#">AMS SSP を使用して AMS アカウントで Alexa for Business をプロビジョニングする</a> 」を参照してください。 | 2022 年 1 月 13 日 |
| 変更内容: Elastic Container Registry (ECR) のセルフサービスプロビジョニング | ECR を使用してユーザーアクセス許可を管理するためのよくある質問項目を追加しました。「 <a href="#">AMS SSP を使用して AMS アカウントに Amazon Elastic Container Registry をプロビジョニングする</a> 」を参照してください。                                       | 2022 年 1 月 13 日 |



翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。