AMS Accelerate の概念と手順

# AMS Accelerate ユーザーガイド

Version October 3, 2025

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

# AMS Accelerate ユーザーガイド: AMS Accelerate の概念と手順

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 のものではない製品またはサービスと関連付けてはならず、また、お客様に混乱を招くような形や Amazon の信用を傷つけたり失わせたりする形で使用することはできません。Amazon が所有しない商標はすべてそれぞれの所有者に所属します。所有者は必ずしも Amazon と提携していたり、関連しているわけではありません。また、Amazon 後援を受けているとはかぎりません。

# Table of Contents

AMS Accelerate とは ..... 1
運用計画 ..... 1
運用計画の迅速化 ..... 2
高度な運用計画 ..... 2
仕組み ..... 2
重要な用語 ..... 3
サービスの説明 ..... 9
AWS Managed Services (AMS) AMS Accelerate オペレーションプランの機能 ..... 9
サポートされている設定 ..... 13
サポートされる サービス ..... 15
役割と責任 ..... 18
AMS Accelerate によって実行される変更の範囲 ..... 33
サポートされていないオペレーティングシステム ..... 34
問い合わせとエスカレーション ..... 35
対応時間 ..... 36
営業時間 ..... 36
エスカレーションパス ..... 37
リソースインベントリ ..... 37
はじめに ..... 39
オンボーディング ..... 39
オンボーディングの前提条件 ..... 39
ステップ 1. アカウント検出 ..... 42
ステップ 2. 管理リソースのオンボーディング ..... 44
ステップ 3. デフォルトポリシーを使用したオンボーディング機能 ..... 54
ステップ 4. 機能のカスタマイズ ..... 64
AMS コンソールの使用 ..... 66
AMS パターン ..... 68
AMS パターンの仕組み ..... 68
AMS パターン ..... 69
自動インスタンス設定 ..... 72
仕組み ..... 72
SSM エージェントの自動インストール ..... 74
インスタンス設定の自動変更 ..... 76
AMS Accelerate からのオフボード ..... 80

オフボーディング効果 ..... 81
依存関係を使用したオフボーディング ..... 83
オフボーディングのサポートを受ける ..... 83
通知の設定 ..... 84
Tagging ..... 85
タグ ..... 86
タグとは ..... 87
タグ付けの仕組み ..... 87
カスタマーマネージドタグ ..... 87
高速マネージドタグ ..... 91
お客様が用意したタグ ..... 92
タグ管理ツール ..... 92
リソースタグ付け ..... 93
CloudFormation ..... 112
Terraform ..... 116
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 ..... 118
インシデント管理 ..... 118
インシデント管理とは ..... 119
インシデント対応と解決の仕組み ..... 120
インシデントの使用 ..... 121
サービスリクエスト管理 ..... 124
サービスリクエストを使用するタイミング ..... 125
サービスリクエスト管理の仕組み ..... 126
サービスリクエストの作成 ..... 126
サービスリクエストのモニタリングと更新 ..... 128
サポート API を使用したサービスリクエストの管理 ..... 129
AMS Accelerate が生成したサービスリクエストへの応答 ..... 129
インシデントレポートとサービスリクエストのテスト ..... 130
請求に関する質問 ..... 130
計画されたイベント管理 ..... 131
AMS PEM 基準 ..... 131
PEM のタイプ ..... 131
AMS PEM プロセス ..... 132
PEM FAQs ..... 132
オンデマンドオペレーション ..... 134
オンデマンドでの AMS オペレーションのリクエスト ..... 142

Operations on Demand サービスの変更 ... 143
レポートとオプション ... 144
リクエスト時レポート ... 144
AMS ホスト管理レポート ... 145
AMS Backup レポート ... 145
AWS Config コントロールコンプライアンスレポート ... 148
AMS Config Rules Response Configuration レポート ... 149
Incidents Prevented and Monitoring Top Talkers レポート ... 151
請求料金の詳細レポート ... 153
信頼できる修復レポート ... 154
セルフサービスレポート ... 157
内部 API オペレーション ... 158
パッチレポート (毎日 ) ... 162
バックアップレポート (毎日 ) ... 171
インシデントレポート (毎週 ) ... 175
請求レポート (毎月 ) ... 178
集計レポート ... 181
AMS セルフサービスレポートダッシュボード ... 183
データ保持ポリシー ... 190
SSR からのオフボード ... 191
アクセス管理 ... 192
コンソールにアクセスする ... 192
機能を使用するためのアクセス許可 ... 192
アカウントにアクセスする理由とタイミング ... 207
アクセストリガー ... 207
IAM ロールにアクセスする ... 208
アカウントへのアクセス方法 ... 210
root を使用する方法とタイミング ... 211
セキュリティ管理 ... 212
Log4j SSM ドキュメントを使用して発生を検出する ... 213
インフラストラクチャセキュリティモニタリング ... 214
サービスにリンクされたロールの使用 ... 216
AWS マネージドポリシー ... 230
データ保護 ... 238
Amazon Macie でモニタリングする ... 239
GuardDuty によるモニタリング ... 239

Amazon Route 53 Resolver DNS Firewall によるモニタリング ..... 241
データの暗号化 ..... 242
AWS Identity and Access Management ..... 242
AMS Accelerate での ID による認証 ..... 243
ポリシーを使用したアクセスの管理 ..... 251
セキュリティインシデント対応 ..... 251
仕組み ..... 252
準備 ..... 253
検出 ..... 254
分析 ..... 254
封じ込め ..... 255
根絶 ..... 257
復旧 ..... 258
インシデント後レポート ..... 258
セキュリティインシデント対応ランブック ..... 259
セキュリティイベントのロギングとモニタリング ..... 265
設定コンプライアンス ..... 265
AMS Config ルールライブラリ ..... 266
違反への対応 ..... 293
ルール例外の作成 ..... 295
AWS Config コストの削減 ..... 296
カスタマイズされた検出結果のレスポンス ..... 296
インシデントへの対応 ..... 298
インシデント対応とオンボーディング ..... 298
耐障害性 ..... 299
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 ..... 299
セキュリティのベストプラクティス ..... 300
変更リクエストのセキュリティレビュー ..... 300
カスタマーセキュリティリスク管理プロセス ..... 300
AMS Accelerate の技術標準 ..... 301
AMS Accelerate の標準コントロール ..... 301
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 ..... 316
セキュリティに関するよくある質問 ..... 317
AMS オペレーションエンジニアはいつ環境にアクセスしますか？ ..... 317
AMS オペレーションエンジニアは、アカウントにアクセスするときにどのようなロールを引き受けますか？ ..... 318

AMS オペレーションエンジニアが自分のアカウントにアクセスする方法 ..... 318
AMS マネージド AWS アカウントで AMS によって行われた変更を追跡するにはどうすればよいですか？ ..... 319
AMS オペレーションエンジニアが自分のアカウントにアクセスするためのプロセスコントロールは何ですか？ ..... 320
特権アクセスはどのように管理されますか？ ..... 320
AMS オペレーションエンジニアは MFA を使用していますか？ ..... 320
AMS 従業員が組織を離れたり、職務を変更したりした場合、アクセスはどうなりますか？ ..... 320
アカウントへの AMS オペレーションエンジニアのアクセスを管理するアクセスコントロールは何ですか？ ..... 320
AMS はルートユーザーアクセスをどのようにモニタリングしますか？ ..... 321
AMS はセキュリティインシデントにどのように対応しますか？ ..... 321
AMS はどのような業界標準の認定とフレームワークに準拠していますか？ ..... 321
セキュリティ証明書、フレームワーク、コンプライアンスに関する最新のレポートにアクセスするにはどうすればよいですか AWS？ ..... 322
AMS は、AMS 機能のさまざまな側面のリファレンスアーキテクチャ図を共有していますか？ ..... 323
AMS は、アカウントにアクセスするユーザーと、アクセスのためのビジネスニーズをどのように追跡しますか？ ..... 323
AMS エンジニアは、Amazon S3、Amazon RDS、DynamoDB、Amazon Redshift などの AWS データストレージサービスに保存されているデータにアクセスできますか？ ..... 324
AMS エンジニアは、Amazon EBS、Amazon EFS、Amazon FSx に保存されている顧客データにアクセスできますか？ ..... 324
環境に対する高い権限を持つオートメーションロールのアクセスは、どのように制限または制御されますか？ ..... 324
AMS は、自動化ロールの AWS Well-Architected フレームワークで提唱されている最小特権の原則をどのように実装していますか？ ..... 324
オートメーションロールに関連する不正アクセスの試みや疑わしいアクティビティを検出するために、どのようなログ記録およびモニタリングシステムが使用されますか？ ..... 325
オートメーションインフラストラクチャに関するセキュリティインシデントや違反はどのように処理され、どのようなプロトコルが迅速な対応と緩和に役立ちますか？ ..... 325
オートメーションインフラストラクチャでは、定期的なセキュリティ評価、脆弱性スキャン、侵入テストを実施していますか？ ..... 325
オートメーションインフラストラクチャへのアクセスは、承認された担当者のみに制限されるのですか？ ..... 326

セキュリティ標準を維持し、オートメーションパイプラインでの不正アクセスやデータ侵害を防ぐために、どのような対策が実装されていますか？ ... 326
特権のエスカレーションやアクセスの誤用を検出して AMS チームにプロアクティブに警告するために、アクセスログ記録または監査ログ記録に対して異常検出またはモニタリングが有効になっていますか？ ... 326
AMS マネージドアカウントから抽出される顧客データの種類と、その使用および保存方法 ... 327
モニタリングとイベント管理 ... 328
モニタリングとは ... 328
モニタリングの仕組み ... 329
EC2 インスタンスグループ化通知 ... 331
タグベースのアラート通知 ... 332
AMS でのベースラインモニタリングからのアラート ... 333
AMS でのアプリケーション対応インシデント通知 ... 356
AppRegistry にオンボードしてアプリケーションを作成する ... 357
タグを作成してケースエンリッチメントを有効にする ... 358
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 ... 358
必要なアクセス許可を確認する ... 359
アラームマネージャー ... 360
Alarm Manager の仕組み ... 360
Alarm Manager の開始方法 ... 361
Alarm Manager タグ ... 362
Alarm Manager 設定プロファイル ... 367
追加の CloudWatch アラームの作成 ... 385
Alarm Manager によってモニタリングされるリソースの数の表示 ... 385
アラートの AMS 自動修復 ... 387
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 ... 391
EC2 ボリューム使用量修復の自動化 ... 392
Amazon RDS の低ストレージイベント修復の自動化 ... 393
AMS イベントルーター ... 393
AMS によってデプロイされた Amazon EventBridge マネージドルール ... 394
AMS のマネージドルールの作成 ... 396
AMS のマネージドルールの編集 ... 397
AMS のマネージドルールの削除 ... 397
信頼できる修復 ... 397
主な利点 ... 397

Trusted Remediator の仕組み ... 398
重要な用語 ... 398
Trusted Remediator の使用を開始する ... 400
サポートされている Compute Optimizer の推奨事項 ... 402
サポートされている Trusted Advisor チェック ... 407
チェック修復を設定する ... 462
実行モードの決定ワークフロー ... 466
修復チュートリアルを設定する ... 466
修復の操作 ... 469
修復ログ ... 473
QuickSight との統合 ... 478
ベストプラクティス ... 480
よくある質問 ... 480
EKS のモニタリングとインシデント管理 ... 484
Amazon EKS のモニタリングとインシデント管理とは ... 484
Amazon EKS のモニタリングとインシデント管理の仕組み ... 485
AMS 責任マトリックス (RACI) ... 486
ベースラインアラート ... 488
アラートとアクション ... 488
要件 ... 495
オンボード ... 497
オフボード ... 498
継続性管理 ... 500
継続性管理の仕組み ... 500
AMS バックアッププランを選択する ... 501
デフォルトの AMS バックアッププラン ... 501
拡張バックアッププラン ... 502
データ機密性の高いバックアッププラン ... 503
AMS Accelerate オンボーディングバックアッププラン ... 503
バックアップ用にリソースにタグを付ける ... 504
AMS ボールトでバックアップを表示する ... 505
バックアップのモニタリングとレポート ... 507
パッチ管理 ... 508
パッチ適用に関する推奨事項 ... 509
パッチ責任に関する推奨事項 ... 510
アプリケーションチーム向けガイダンス ... 510

セキュリティ運用チーム向けのガイダンス ..... 511
ガバナンスチームとコンプライアンスチームのガイダンス ..... 511
高可用性 Windows アプリケーションの設計例 ..... 512
パッチレコメンデーションFAQs ..... 512
パッチウィンドウの作成 ..... 513
パッチメンテナンスウィンドウの制限 ..... 513
パッチ火曜日のパッチウィンドウの作成: AMS コンソール ..... 515
パッチウィンドウの作成： CloudFormation ..... 516
パッチウィンドウの作成: Systems Manager コンソール ..... 517
パッチウィンドウの作成: Systems Manager CLI ..... 519
フックを使用したパッチ ..... 520
AMS パッチフック RACI ..... 521
パッチフックの SSM ドキュメントを作成する ..... 522
SSM コマンドドキュメントを AMS パッチフックとして使用するように AMS パッチメンテナンスウィンドウを設定する ..... 522
AMS Accelerate パッチベースライン ..... 524
デフォルトのパッチベースライン ..... 524
カスタムパッチベースライン ..... 525
オンデマンドパッチ適用のアクセス許可 ..... 525
パッチ通知とパッチ障害を理解する ..... 526
パッチサービスリクエストと E メール通知 ..... 527
CloudWatch Events を介したパッチ通知 ..... 527
パッチ障害の調査 ..... 531
AMS Resource Scheduler によるコスト最適化 ..... 533
Resource Scheduler でのリソースの使用 ..... 534
Resource Scheduler のオンボーディング ..... 535
Resource Scheduler のカスタマイズ ..... 536
Resource Scheduler の使用 ..... 537
期間とスケジュールの操作 ..... 540
リソースのタグ付け ..... 546
コスト見積りツール ..... 546
アラームサプレッサー ..... 547
ログ管理 ..... 549
ログ管理 — AWS CloudTrail ..... 549
CloudTrail ログへのアクセスと監査 ..... 551
CloudTrail ログの保護と保持 ..... 551

Amazon EC2 ログへのアクセス ..... 551
Amazon EC2 ログの保持 ..... 552
ログ管理 — Amazon EC2 ..... 552
ログ管理 — Amazon VPC フローログ ..... 553
変更の追跡 ..... 555
変更レコードの表示 ..... 556
デフォルトクエリ ..... 557
クエリでの日時フィルターの変更 ..... 565
デフォルトのクエリ例 ..... 566
レコードのアクセス許可を変更する ..... 577
AWS Systems Manager Accelerate の ..... 579
利用可能な AMS Accelerate SSM ドキュメント ..... 579
AMS Accelerate SSM ドキュメントバージョン ..... 579
Systems Manager の料金 ..... 580
ドキュメント履歴 ..... 581
以前の更新 ..... 602
..... dcxxx

# AMS Accelerate とは

AMS Accelerate for Amazon Web Services () へようこそAWS。AMS Accelerate は、運用上の優秀性の実現に役立つさまざまな運用サービスを提供します AWS。クラウドで始めたばかりの場合でも、現在のチームを強化したい場合でも、長期的な運用ソリューションが必要な場合でも、Accelerate はクラウドでの運用目標を達成するのに役立ちます。 AWS のサービス とオートメーション、設定、ランブックのライブラリを活用して、新規および既存の AWS 環境の両方にend-to-endの運用ソリューションを提供します。

Accelerate サービスは、一連のネイティブ AWS のサービス および 機能を活用して、包括的なインフラストラクチャ管理機能を提供します。これらの中で AWS のサービス、Accelerate は、インフラストラクチャを準拠した安全な方法で運用するために、厳選されたモニタリングコントロール、検出ガードレール、オートメーション、ランブックを作成および維持します。

トピック


- AMS オペレーションプラン
- AMS Accelerate オペレーションプランの使用
- AMS の主要な用語
- サービスの説明
- Accelerate 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
- 問い合わせとエスカレーション
- Accelerate のリソースインベントリ


## 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。オペレーションプランには、特定の一連の機能が用意されており、サービス、技術的機能、要件、料金、制限のレベルが異なります。運用プランでは、 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とって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、および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」および「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 によって安全とサポートの両方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 Accelerate オペレーションプランの使用

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。ワークロードが既に AWS アカウントにある場合も、新しいアカウントへの移行を計画している場合も、新しい移行を経験したり、ダウンタイムが発生したり、AWS の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 AMS Accelerate 運用サービスを利用できます。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、既存のアクセスおよび変更メカニズムを引き続き使用できます。

AMS Accelerate は運用を簡素化できますが、アプリケーションの開発、デプロイ、テストとチューニング、管理は引き続きお客様の責任となります。AMS Accelerate は、インシデント、アラーム、修復、および一部のサービスリクエストの結果としてのみアカウントを変更します。AMS Accelerate は、ユーザーに代わってアカウントにリソースをプロビジョニングしません。AMS Accelerate 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 Accelerate は、ユーザーの知識と承認なしにアプリケーション設定にアクセスまたは検証しません。AMS Accelerate のサービスと変更は AWS コンソールと APIs で直接提供されるため、 AWS および利用可能な AWS Marketplace ソリューションで既存のアカウントを引き続き活用できます。AMS Accelerate はinfrastructure-as-codeを変更しませんが、運用およびセキュリティのベストプラクティスに従うために変更が必要なチームをガイドできます。CloudFormation

## 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 アドバンストアカウント: AMS アドバンスト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 アカウントおよび/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 メールとは、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: サービスリクエストを通じて AWS 少なくとも 30 日間の通知を提供することで、すべての AWS Managed ServicesAWS Managed Servicesアカウント、または指定された AWS Managed Servicesサービスを終了できます。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お客様に引き渡します。
  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 Managed Servicesアカウントに対して AWS 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、インシデントはインシデントリストに作成されます。
- 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AWS 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: インシデントが AMS によって、またはユーザーによって低、中、高のいずれかとして優先順位付けされる方法。
  - 低: AMS サービスの重大ではない問題。

- 中: マネージド環境内の AWS サービスを利用できますが、意図したとおりに動作しません (該当するサービスの説明を参照 ) 。
- 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 が使用できない場合、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ず、使用不能によりアプリケーションが関数を実行できなくなる場合。

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顧客アカウント。
- 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): 予想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 の除外から直接または間接的に生じる利用不能は、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。

パッチ適用条件：

- 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」と評価される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ときに発表され、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：
  - CSU (Critical Security Update): 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「Critical」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、所有者に通知したり、リソースをプロアクティブに変更または終了したりして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 がサービスリクエストリストページに投稿した通知。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) からも通知されます。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アドバンストコンソール、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ンデンスに関するケースコレスポンデンス評価、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 データやその他のデータを集約し 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) を操作するときに、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 Accelerate 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。

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

AMS Accelerate には次の機能があります。

- インシデント管理：

  インシデント管理は、AMS サービスが報告されたインシデントに対応するために使用するプロセスです。

  AMS Accelerate は、インシデントをプロアクティブに検出して対応し、チームの問題解決を支援します。 AWS サポートセンターを使用して、AMS Accelerate オペレーションエンジニアに 24 時

間 365 日連絡できます。応答時間の SLAs、アカウントで選択した応答レベルによって異なります。

- モニタリング:

  モニタリングは、AMS サービスがリソースを追跡するために使用するプロセスです。

  AMS Accelerate に登録されているアカウントは、ノイズを減らし、今後のインシデントの可能性を特定するために最適化された Amazon CloudWatch イベントとアラームのベースラインデプロイで設定されます。アラートを受け取った後、AMS チームは自動修復、人員、プロセスを使用してリソースを正常な状態に戻し、必要に応じてチームと協力して、動作とその防止方法に関する学習に関するインサイトを提供します。修復に失敗すると、AMS はインシデント管理プロセスを開始します。デフォルトの設定ファイルを更新することで、ベースラインを変更できます。

- のセキュリティ

  セキュリティ管理は、AMS サービスがリソースを保護するために使用するプロセスです。AWS Managed Services、 AWS Config ルールや Amazon GuardDuty などの複数のコントロールを使用して、情報アセットを保護し、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。

  AMS Accelerate は、 AWS Config ルール および 修復アクションのライブラリを維持し、すべてのアカウントがセキュリティと運用の整合性に関する業界標準に準拠していることを確認します。は、記録されたリソース間の設定変更 AWS Config ルール を継続的に追跡します。変更がルール条件に違反すると、AMS は調査結果を報告し、違反の重大度に応じて、違反を自動またはリクエストで修正できるようにします。 は、Center for Internet Security (CIS)、米国国立標準技術研究所 (NIST) クラウドセキュリティフレームワーク (CSF)、医療保険の相互運用性と説明責任に関する法律 (HIPAA)、および Payment Card Industry (PCI) Data Security Standard (DSS) によって設定された標準への準拠 AWS Config ルール を促進します。

  さらに、AMS Accelerate は Amazon GuardDuty を活用して、AWS 環境で不正または悪意のある可能性のあるアクティビティを特定します。GuardDuty の検出結果は、AMS によって 24 時間 365 日モニタリングされます。AMS はお客様と協力して、ベストプラクティスの推奨事項に基づいて検出結果と修復の影響を理解します。AMS は、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を保護するために Amazon Macie もサポートしています。最後に、AMS はマネージドアカウントで生成されたすべての Amazon Route 53 Resolver ALERT イベントと BLOCK イベントをモニタリングしてトリアージし、ネットワークトラフィックをさらに検査して検出機能を強化します。

- パッチ管理 :

  パッチ管理は、AMS サービスがリソースを更新するために使用するプロセスです。

パッチアドオンを使用する AWS アカウントの場合、AWS Managed Services は、選択したメンテナンスウィンドウ中に、サポートされているオペレーティングシステムの Amazon EC2 インスタンスにベンダーの更新を適用してインストールします。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、パッチのインストールをモニタリングして、結果を通知します。パッチが失敗した場合、AMS は失敗を調査し、問題を修正するための一連のアクションを推奨します。または、AMS はリクエストに応じてインスタンスをロールバックに復元します。AMS は、パッチコンプライアンスカバレッジのレポートを提供し、ビジネスに推奨される一連のアクションについてアドバイスします。

- バックアップ管理：

  AMS はバックアップ管理を使用してリソースのスナップショットを作成します。

  AWS Managed Services は、 でサポートされている AWS サービスのスナップショットを作成、モニタリング、保存します AWS Backup。バックアップスケジュール、頻度、保持期間を定義するには、アカウントとアプリケーションのオンボーディング中に AWS Backup プランを作成します。計画をリソースに関連付けます。AMS はすべてのバックアップジョブを追跡し、バックアップジョブが失敗すると、修復を実行するようにチームに警告します。AMS はスナップショットを活用して、必要に応じてインシデント中に復元アクションを実行します。AMS には、バックアップカバレッジレポートとバックアップステータスレポートが用意されています。

- 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。

- 指定されたエキスパート：

  AMS Accelerate は、Cloud Service Delivery Manager (CSDM) と Cloud Architect (CA) も指定し、組織と連携して運用とセキュリティの優秀性を推進します。CSDM と CA は、AMS Accelerate の設定時とオンボーディング後のガイダンスを提供し、運用メトリクスの月次レポートを提供し、AWS Cost Explorer、コストと使用状況レポート、 などのツールを使用して潜在的なコスト削減を特定します Trusted Advisor。

- オペレーションツール：

  AMS Accelerate は、AWS のワークロードのインフラストラクチャに対して継続的なオペレーションを提供できます。当社のパッチ、バックアップ、モニタリング、インシデント管理サービスは、リソースにタグを付けること、および AWS Systems Manager (SSM) エージェントと CloudWatch

エージェントを SSM および Amazon CloudWatch サービスとやり取りすることを許可する IAM インスタンスプロファイルを使用して Amazon EC2 インスタンスにインストールおよび設定することに依存します。AMS Accelerate には、ルールに基づいてリソースにタグを付けるのに役立つ Resource Tagger や、Amazon 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自動インスタンス設定などのツールが用意されています。イミュータブルなインフラストラクチャプラクティスに従っている場合は、コンソールまたは infrastructure-as-code テンプレートで直接前提条件を完了できます。

- コストの最適化：

  AMS Resource Scheduler は、Amazon Elastic Compute Cloud (Amazon EC2) インスタンス、Amazon Relational Database Service (Amazon RDS) インスタンス、Amazon EC2 Auto Scaling グループの開始と停止を自動化します。AMS Resource Scheduler は、使用されていないリソースを停止し、容量が必要な場合にリソースを再開することで、運用コストを削減するのに役立ちます。

- ログ記録とレポート：

  AWS Managed Services は、CloudWatch CloudTrail 、Amazon VPC フローログのオペレーションの結果として生成されたログを集約して保存します。AMS からのログ記録は、インシデントの迅速な解決とシステム監査に役立ちます。AMS Accelerate 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も提供します。レポートは、指定された 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 Accelerate 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、または追加の AMS サービスをリクエストするためのサービスリクエストを送信できます。

AMS Accelerate のすべてのお客様は、インシデント管理、モニタリング、セキュリティモニタリング、ログ記録、前提条件ツール、バックアップ管理、レポート機能から始めます。AMS パッチ管理アドオンは追加料金で追加できます。

> **Note**
>
> でサポートされていない機能のリストについては AWS GovCloud (US)、「 の AMS Accelerate の違い」を参照してください。 AWS GovCloud (US)

## サポートされている設定

AMS Accelerate は、次の設定をサポートしています。

- 言語: 英語。
- リージョン: リージョンAWS Managed Servicesサービスでサポートされている AWS リージョン AWS 」を参照してください。

> **Note**
>
> 2019 年 3 月 20 日より前に導入された AWS リージョンは「元の」リージョンと見なされ、デフォルトで有効になっています。この日付以降に導入されたリージョンは「オプトイン」リージョンであり、デフォルトでは無効になっています。アカウントが複数のリージョンを使用していて、デフォルトのリージョンとして「オプトイン」リージョンが有効になっているアカウントに AMS Accelerate をオンボードする場合、AMS レポート機能はそのリージョンでのみ使用できます。デフォルトのリージョンを設定しない場合、最後にアクセスしたリージョンがデフォルトのリージョンになります。
> リージョンを有効にするには、「リージョンの有効化」を参照してください。デフォルトのリージョンを設定するには、「リージョンの選択」を参照してください。各リージョンのオプトインステータスのリストについては、「Amazon Elastic Compute Cloud ユーザーガイド」の「利用可能なリージョン」を参照してください。

- オペレーティングシステムアーキテクチャ (x86-64 または ARM64): Systems Manager と CloudWatch の両方でサポートされている 。
- サポートされるオペレーティングシステム
  - AlmaLinux 8.3-8.9、9.x (AlmaLinux は x86 アーキテクチャでのみサポートされています )
  - Amazon Linux 2023
  - Amazon Linux 2 (2026 年 6 月 30 日に予定されている AMS サポート終了日 )
  - 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 2022、2019、2016
- Ubuntu 20.04、22.04、24.04

- 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：

> **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ている場合にのみ、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 OS を使用するインスタンスは、「 Accelerate 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 が必要とする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 OS 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
- SAP 12 SP5 用 SUSE Linux Enterprise Service
- Microsoft Windows Server 2012/2012 R2
- Red Hat Enterprise Linux (RHEL):7.x
- Oracle Linux 7.5 ~ 7.9

- AWS Control Tower を使用してマルチアカウント環境を管理する場合は、 Accelerate との互換性 AWS Control Tower のために の最新バージョンを実行していることを確認してください。2.7 よ

り前の AWS Control Tower バージョン (2021 年 4 月にリリース) を使用する環境はサポートされていません。更新方法については AWS Control Tower、「ランディングゾーンの更新」を参照してください。

## サポートされる サービス

AWS Managed Services 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 の運用管理サポートのレベルは、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。次のリストでサポート対象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して AWS Managed Servicesによるサービスの提供をリクエストした場合、お客様がリクエストした設定で提供される 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。

- インシデント: すべての AWS サービス
- サービスリクエスト: すべての AWS サービス
- パッチ適用: Amazon EC2
- バックアップと復元: で AWS のサービス サポートされているすべて AWS Backup。でサポートされているサービスのリストについては AWS Backup、AWS Backup「サポートされているリソース」を参照してください。
- Resource Scheduler: Amazon Elastic Compute Cloud (Amazon EC2) インスタンス、Amazon Relational Database Service (Amazon RDS)、Amazon EC2 Auto Scaling グループ
- 運用イベントでモニタリングされるサービス: サポートされているチェックと Trusted Advisor、Application Load Balancer、Aurora、Amazon EC2、Elastic Load Balancing、Amazon FSx for NetApp ONTAP、Amazon FSx for Windows File Server、NAT ゲートウェイ (ネットワークアドレス変換 (NAT) サービス ) 、OpenSearch、Amazon Redshift Health Dashboard、Amazon Relational Database Service (Amazon RDS)、Site-to-Site VPN。AMS Accelerate がサービスの一部としてモニタリングしている内容の詳細については、「AMS 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。
- セキュリティ Config Rules: AWS Account によってモニタリングされるサービス GuardDuty、Macie、 Amazon API Gateway、 AWS Certificate Manager AWS Config、 CloudTrail、CloudWatch、 AWS CodeBuild、 AWS Database Migration Service、 Amazon DynamoDB、Amazon EC2、 Amazon ElastiCache、 Amazon Elastic Block Store (Amazon EBS) Amazon Elastic File System (Amazon EFS) Amazon Elastic Kubernetes Service (Amazon EKS) Elastic Load Balancing、 Amazon OpenSearch Service、 Amazon EMR、 AWS Identity and Access Management （ IAM) AWS Key Management Service、、 AWS Lambda、 Amazon Redshift、

Amazon Relational Database Service、 Amazon S3、 Amazon SageMaker AI、 AWS Secrets Manager 、 Amazon Simple Notification Service、 AWS Systems Manager、 Amazon VPC (セキュリティグループ、 ボリューム、 Elastic IP アドレス、 VPN 接続、 インターネットゲートウェイ ) 、 Amazon VPC フローログ。詳細については、「Accelerate の設定コンプライアンス」および「Accelerate でのデータ保護」を参照してください。追加の AMS セキュリティ情報は AWS Artifact、AWS Managed Services のレポートタブからアクセスできるプライベートセキュリティガイドで確認できます。

> **Note**
>
> AMS Accelerate for the Middle East (UAE) リージョンは、次の表に示すように、一連の範囲内の機能をサポートしています。このリージョンの AMS アカウントコンソールとインスタンスへのアクセスは、インバウンドサービスリクエストトリガーによってのみ駆動されます。中東 (UAE) リージョンでの Accelerate の可用性の詳細については、アカウントマネージャーまたは AWS Cloud Service Delivery Manager (CSDM) にお問い合わせください。

| 中東 (UAE) リージョンの AMS Accelerate スコープ内機能 | 機能の説明 |
| --- | --- |
| インシデント管理 | AMS は、チームが問題を解決するのに役立つインシデント対応とサポートを提供します。AMS がインシデント管理を支援するには、サービスリクエストを送信する必要があります。AMS は、このリージョンのインシデントをプロアクティブに検出または対応しません。 |
| モニタリング | サービスリクエストを受け取った後、AMS はリソースの修復を支援できます。AMS は自動修復、人員、プロセスを使用して、リソースを正常な状態に戻します。AMS は、このリージョンのベースライン CloudWatch イベントとアラームを設定しません。既存のモニタリングツールがある場合は、Cloud Architect (CA) と |

| 中東 (UAE) リージョンの AMS Accelerate スコープ内機能 | 機能の説明 |
| --- | --- |
| | CSDM の評価に基づいて、リソースのプロアクティブ追跡が利用できる場合があります。 |
| セキュリティ | サービスリクエストを受け取った後、AMS はセキュリティ問題の修復を支援できます。AMS は、 AWS Config ルール や GuardDuty などのセキュリティコントロールをデプロイしたり、このリージョンのセキュリティ検出結果をモニタリングしたりしません。既存のセキュリティツールがある場合は、CA と CSDM の評価に基づいてプロアクティブセキュリティモニタリングが利用できる場合があります。 |
| パッチ管理 | AMS は、選択したメンテナンスウィンドウ中にサポートされているオペレーティングシステムの Amazon EC2 インスタンスにベンダー更新を適用し、事前パッチスナップショットを作成できます。AMS がパッチ管理を支援するには、サービスリクエストを送信する必要があります。AMS パッチ通知とレポートは、このリージョンでは使用できません。 |
| バックアップ管理 | AMS は、 で AWS のサービス サポートされている のスナップショットを作成および保存し AWS Backup、バックアップ修復を支援できます。AMS がバックアップ管理を支援するには、サービスリクエストを送信する必要があります。AMS はこのリージョンのバックアップジョブを追跡しません。 |
| 指定されたエキスパート | AMS は、Cloud Architect (CA) と Cloud Service Delivery Manager (CSDM) を指定して、お客様の組織と提携し、運用とセキュリティの優秀性を推進します。 |

| 中東 (UAE) リージョンの AMS Accelerate スコープ内機能 | 機能の説明 |
| --- | --- |
| サービスリクエスト管理 | マネージド環境、AMS、または AWS のサービス サービスに関する情報をリクエストするには、AMS Accelerate コンソールからサービスリクエストを送信します。この表で説明するように、 および 機能に関する AWS のサービス「方法」の質問、またはこのリージョンで利用可能な AMS サービスをリクエストするためのサービスリクエストを送信できます。 |

## 役割と責任

AMS Accelerate は、責任、説明責任、相談、情報、または RACI マトリックスに、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。この表では、お客様の責任 (「お客様」) と当社の責任 (「AMS Accelerate」) について説明しています。

このセクションでは、AMS がアカウントに変更を加えることが許可されている特定の状況と、AMS が行うことができないいくつかのタイプの変更をAMS Accelerate によって実行される変更の範囲一覧表示します。

### AMS Accelerate RACI マトリックス

AMS Accelerate は AWS インフラストラクチャを管理します。次の表は、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、お客様と AMS Accelerate の役割と責任の概要を示しています。

- 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「Consulted」の略で、通常は対象分野の専門家として意見を求められ、二国間通信を行う当事者です。
- 「Informed」の略です。多くの場合、タスクの完了時にのみ進行状況が通知されます。

> **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。

| アクティビティ | お客様 | AWS Managed Services (AMS) |
|---|---|---|
| AMS パターン | | |
| 新しいパターンを作成する | I | R |
| パターンのデプロイとカスタマイズ | R | C、I |
| パターンのテストと削除 | R | I |
| 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の要件、分析、設計 | R | I |
| アプリケーションのデプロイ | R | I |
| AWS リソースのデプロイ | R | I |
| 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 |
| 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 | I |
| 問題のトラブルシューティングと解決 | R | I |
| AWS インフラストラクチャでサポートされているモニタリング | C | R |

| アクティビティ | お客様 | AWS Managed Services (AMS) |
|---|---|---|
| AWS ネットワーク問題のインシデント対応 | C | R |
| AWS リソースの問題のインシデント対応 | C | R |
| マネージドアカウントのオンボーディング | | |
| AMS チームおよびツールの AWS マネージドアカウントへのアクセス権を付与する | R | C |
| アカウントまたは環境に変更を実装して、アカウントにツールをデプロイできるようにします。例えば、サービスコントロールポリシー (SCPs の変更 | R | C |
| EC2 インスタンスに SSM エージェントをインストールする | R | C |
| AMS サービスを提供するために必要なツールをインストールして設定します。例えば、CloudWatch エージェント、パッチ適用用のスクリプト、アラーム、ログなど | I | R |
| AMS エンジニアのアクセスとアイデンティティのライフサイクルを管理する | I | R |
| AMS サービスを設定するために必要なすべての入力を収集します。例えば、パッチメンテナンスウィンドウの期間、スケジュール、ターゲットなど | R | I |
| AMS サービスの設定をリクエストし、必要な入力をすべて提供する | R | I |
| お客様からのリクエストに従って AMS サービスを設定します。例えば、パッチメンテナンスウィンドウ、リソースタガー、アラームマネージャーなど | C | R |

| アクティビティ | お客様 | AWS Managed Services (AMS) |
|---|---|---|
| AWS アカウントとインスタンス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ユーザーとそのアクセス許可のライフサイクルを管理する | R | I |
| リザーブドインスタンスの最適化を推奨 | I | R |
| 信頼できる修復者にアカウントをオンボードする (複数可 ) | C、I | R |
| パッチ管理 | | |
| パッチメンテナンスウィンドウ、パッチベースライン、ターゲットを設定するために必要なすべての入力を収集する | R | I |
| パッチメンテナンスウィンドウとベースラインの設定をリクエストし、必要なすべての入力を提供する | R | I |
| お客様からのリクエストに応じて、パッチメンテナンスウィンドウ、パッチベースライン、ターゲットを設定する | C | R |
| EC2 インスタンスでサポートされている OS および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該当する更新をモニタリングする | I | R |
| サポートされている OS とメンテナンスウィンドウのカバレッジに対する更新の欠落に関するレポート | I | R |
| 更新を適用する前にインスタンスのスナップショットを作成する | I | R |
| 顧客設定ごとに EC2 インスタンスに更新を適用する | I | R |
| EC2 インスタンスへの失敗した更新を調査する | C | R |
| Auto Scaling グループ (ASGs) の AMIs とスタックを更新する | R | C |

| アクティビティ | お客様 | AWS Managed Services (AMS) |
|---|---|---|
| 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 | R |
| 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 | I |
| 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 | R |
| 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 |
| バックアップ | | |
| バックアッププランとターゲットリソースを設定するために必要なすべての入力を収集する | R | I |
| Backup プランの設定をリクエストし、必要なすべての入力を提供する | R | I |
| 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 | C | R |
| バックアップスケジュールとターゲットリソースを指定する | R | I |
| プランごとにバックアップを実行する | I | R |
| 失敗したバックアップジョブを調査する | I | R |
| バックアップジョブのステータスとバックアップカバレッジのレポート | I | R |

| アクティビティ | お客様 | AWS Managed Services (AMS) |
|---|---|---|
| バックアップの検証 | R | I |
| インシデント管理の一環として、サポートされている AWS サービスリソースのリソースのバックアップ復元をリクエストする | R | I |
| サポートされている AWS サービス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 | I | R |
| 影響を受けるカスタムアプリケーションまたはサードパーティーアプリケーションを復元する | R | I |
| ネットワーク | | |
| マネージドアカウント VPCs、IGWs、直接接続、およびその他の AWS ネットワークサービスのプロビジョニングと設定 | R | I |
| マネージドアカウント内で AWS セキュリティGroups/NAT/NACL を設定して運用する | R | I |
| 顧客ネットワーク内のネットワーク設定と実装 (DirectConnect など ) | R | I |
| AWS ネットワーク内のネットワーク設定と実装 | R | I |
| セキュリティグループを含むネットワークセキュリティについて AMS で定義されるモニタリング | I | R |
| ネットワークレベルのログ記録の設定と管理 (VPC フローログなど ) | I | R |
| ログ記録 | | |
| すべてのアプリケーション変更ログを記録する | R | I |
| AWS インフラストラクチャ変更ログを記録する | I | R |
| AWS 監査証跡を有効にして集約する | I | R |

| アクティビティ | お客様 | AWS Managed Services (AMS) |
|---|---|---|
| AWS リソースから ログを集約する | I | R |
| モニタリングと修復 | | |
| アラームマネージャー、リソースタガー、アラームしきい値を設定するために必要なすべての入力を収集する | R | I |
| アラームマネージャーの設定をリクエストし、必要な入力をすべて提供する | R | I |
| お客様のリクエストに応じて、アラームマネージャー、リソースタガー、アラームしきい値を設定します。 | C | R |
| 顧客設定ごとに AMS CloudWatch ベースラインメトリクスとアラームをデプロイする | I | R |
| ベースライン CloudWatch メトリクスとアラームを使用してサポートされている AWS リソースをモニタリングする | I | R |
| AWS リソースからのアラートを調査する | C | R |
| 定義された設定に基づいてアラートを修正するか、インシデントを作成します。 | I | R |
| 顧客固有のモニターを定義、モニタリング、調査する | R | I |
| アプリケーションモニタリングからのアラートの調査 | R | C |
| 修復の Trusted Advisor チェックを設定する | R | C |
| サポートされている Trusted Advisor チェックを自動的に修正する | I | R |
| サポートされている Trusted Advisor チェックを手動で修正する | R | C |
| レポート修復ステータス | I | R |

| アクティビティ | お客様 | AWS Managed Services (AMS) |
|---|---|---|
| 修復失敗のトラブルシューティング | R | C |
| セキュリティアーキテクチャ | | |
| セキュリティの問題と潜在的な脅威について AMS リソースとコードを確認する | I | R |
| AMS リソースとコードにセキュリティコントロールを実装してセキュリティリスクを軽減する | I | R |
| アカウントとその AWS リソースのセキュリティ管理のためにサポートされている AWS サービスを有効にする | I | R |
| AMS エンジニアのアカウントと OS アクセスの特権認証情報を管理する | I | R |
| セキュリティリスク管理 | | |
| GuardDuty や Macie など、セキュリティ管理のためにサポートされている AWS サービスをモニタリングする | I | R |
| AMS で定義された Config ルールを定義して作成し、AWS リソースが Center for Internet Security (CIS) と NIST セキュリティのベストプラクティスに準拠しているかどうかを検出します。 | I | R |
| AMS で定義された Config ルールをモニタリングする | I | R |
| Config ルールの適合ステータスを報告する | I | R |
| 必要な Config ルールのリストを定義して修正する | I | R |
| AMS で定義された Config ルールの修正の影響を評価する | R | I |
| AWS アカウントで AMS で定義された Config ルールの修正をリクエストする | R | I |

| アクティビティ | お客様 | AWS Managed Services (AMS) |
|---|---|---|
| AMS で定義された Config ルールから除外されるリソースを追跡する | R | I |
| AWS アカウントでサポートされている AMS 定義 Config ルールを修正する | C | R |
| AWS アカウントでサポートされていない AMS 定義の Config ルールを修正する | R | I |
| 顧客固有の Config ルールを定義、モニタリング、調査する | R | I |
| インシデント管理 | | |
| AWS リソースで AMS によって検出されたインシデントについて通知する | I | R |
| AWS リソース内のインシデントを通知する | R | I |
| モニタリングに基づいて AWS リソースのインシデントを通知する | I | R |
| 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 |
| インシデント対応を提供する | I | R |
| 利用可能なバックアップを使用して、リソースのインシデント解決またはインフラストラクチャの復元を提供する | C | R |
| セキュリティインシデント対応 – 準備 | | |
| 通信 | | |
| 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 AMS の顧客セキュリティ連絡先の詳細を提供および更新する | 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。 | C | 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 | R | R |
| リソース管理 | | |
| アラート、アラート相関、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 |
| 各アセットの価値とビジネスにとっての重要性の詳細を含め、 AWS リソース (Amazon EC2、Amazon S3 など) の包括的なインベントリを維持します。この情報は、効果的な封じ込め戦略を決定するのに役立ちます。 | R | C |
| 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 | C |
| ログの保持とアーカイブを定義および設定する | I | R |
| AWS アカウント、サービス、アクセス管理に関する組織のセキュリティポリシーと設定を定義して適用することで、安全なベースラインを確立する | R | I |
| 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 | I | R |

| アクティビティ | お客様 | AWS Managed Services (AMS) |
|---|---|---|
| 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 | R | I |
| エンドポイントセキュリティ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 | R | I |
| 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 |
| 社内のステークホルダーとのコミュニケーションとリーダーシップの更新を調整して、対応時間を改善する | R | I |
| 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 | C | R |
| AWS インフラストラクチャ変更ログを記録する | R | I |
| ログ記録、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 | R | 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 | I |
| 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 | 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 - 分析 | | |
| 調査と分析 | | |
| 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 | R |
| 利用可能なデータを使用して誤検出/真陽性を評価する | R | R |
| 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 | C |
| 調査に役立つアプリケーションログを収集する | 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 | R | R |
| セキュリティ調査 AWS のサービス に 内の SMEs を関与させる | C | R |
| 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 |
| 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 | | |

| アクティビティ | お客様 | AWS Managed Services (AMS) |
|---|---|---|
| リスクを評価して封じ込め戦略を決定し、潜在的なサービスへの影響を認識する | R | C |
| 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 | I | 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 | C |
| 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 | I | 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 | C | 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 | I | 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 | C | R |
| 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 | I |
| 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 | C | R |
| EC2 インスタンス、ネットワーク、IAM 根絶などの脅威を根絶し、AWS リソースを強化する | R | C |
| 脅威を根絶し、アプリケーションとワークロードを強化する (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を使用 ) | 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 - 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 | I | R |
| 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 | R | I |
| 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 |
| 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 |
| 問題管理 | | |
| インシデントを関連付けて問題を特定する | I | R |
| 問題の根本原因分析 (RCA) を実行する | I | R |
| 問題の修正 | I | R |

| アクティビティ | お客様 | AWS Managed Services (AMS) |
|---|---|---|
| アプリケーションの問題を特定して修正する | R | I |
| サービス管理 | | |
| 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 |
| コスト最適化に関する推奨事項を提供する | I | R |
| 毎月のサービスレポートの準備と配信 | I | R |
| 変更管理 | | |
| マネージド環境でリソースをプロビジョニングおよび更新するための変更管理プロセスとツール | R | I |
| アプリケーション変更カレンダーのメンテナンス | R | I |
| 今後のメンテナンスウィンドウの通知 | R | I |
| AMS オペレーションによって行われた変更を記録する | I | R |
| コスト最適化 | | |
| Resource Scheduler を設定するために必要なすべての入力を収集する | R | I |
| Resource Scheduler のオンボーディング、設定をリクエストし、必要なすべての入力を提供する | R | I |
| 顧客設定ごとに Resource Scheduler をデプロイする | C、I | R |
| カスタマーアカウントで Resource Scheduler を無効化および有効化する | R | C |
| スケジュールの作成、削除、説明、更新 | C | R |

| アクティビティ | お客様 | AWS Managed Services (AMS) |
|---|---|---|
| 期間の作成、削除、説明、更新 | C | R |
| Resource Scheduler の問題の調査とトラブルシューティング | I | R |
| Resource Scheduler のオフボードのリクエスト | R | I |
| Resource Scheduler をアカウントからオフボードする | C、I | R |

## AMS Accelerate によって実行される変更の範囲

AMS Accelerate は、次に説明する特定の目的と状況に対してのみ変更を行います。AMS は、 コンソールまたは APIs。AMS は、アプリケーション、コントロール、またはドメインレイヤーを変更しません。AMS (または他のユーザー) による変更は、一連の構築済みクエリを使用して確認できます。これを行うには、「」を参照してくださいAMS Accelerate アカウントの変更の追跡。

AWS リソース

AMS Accelerate は、以下の状況でのみ AWS リソースをデプロイまたは更新します。

- AMS に必要なツールとリソースをデプロイおよび更新するには。
- AMS モニタリングの一環として、イベントとアラームに応じて。
- の一部としてセキュリティの問題を修正する Accelerate での違反への対応 (非準拠のリソースをセキュリティのベストプラクティスに準拠させる ) 。
- インシデント対応の一環としての修復と復元中。
- 次のような AMS 機能を設定するお客様のリクエストに応答する場合 :
  - アラームマネージャー
  - リソースタガー
  - パッチベースラインとメンテナンスウィンドウ
  - リソーススケジューラ
  - バックアッププラン

AMS Accelerate は、このような状況以外でリソースをデプロイまたは更新しません。他の状況で変更を加えるために AMS からのヘルプが必要な場合は、Operations on Demand の使用を検討してください。

オペレーティングシステムソフトウェア

AMS Accelerate は、当社のサービスレベルアグリーメントで定義されているように、インシデント解決を通じて、利用できない状況でオペレーティングシステムソフトウェアを変更することができます。AMS は、 の一部としてオペレーティングシステムを変更することもできますAMS Accelerate の自動インスタンス設定。

アプリケーションコードと設定

AMS Accelerate はコード (AWS CloudFormation テンプレート、他の infrastructure-as-code テンプレート、Lambda 関数など) を変更しませんが、運用上およびセキュリティ上のベストプラクティスに従うために変更が必要なチームをガイドできます。AMS Accelerate 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 Accelerate はアプリケーション設定にアクセスまたは検証しません。

# Accelerate 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。 |
| 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 |

| 機能 | 注 |
| --- | --- |
| | 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 GuardDuty の検出結果とAWS Config ルール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、AMS にカスタマイズされた AWS Backup プランとボールトを使用して、 Accelerate for EC2 で継続性管理を提供します。 EC2 |

# 問い合わせとエスカレーション

指定されたクラウドサービスデリバリーマネージャー (CSDM) があり、AMS Accelerate 全体でアドバイザリ支援を提供し、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会議を組織し、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 Accelerate 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応答して解決します。
- 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。

# 対応時間

AMS Accelerate には、さまざまな理由でさまざまなタイミングで問い合わせることができます。

| 機能 | AMS Accelerate |
| --- | --- |
| | 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 |
| 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: 8:00 ~ 17:00、現地営業時間 |

# 営業時間

| 機能 | AMS Accelerate |
| --- | --- |
| | 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 (P1) | 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 |

| 機能 | AMS Accelerate |
| --- | --- |
| | プレミアム階層 |
| 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: 9:00 ~ 17:00、現地営業時間 |

## エスカレーションパス

AMS は、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従って、インシデント管理とサービスリクエスト管理で 1 日 24 時間、週 7 日、年 365 日のお客様をサポートします。

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ケースを送信します。詳細については、「Accelerate のインシデントの送信」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、「」を参照してくださいAMS Accelerate でのインシデント管理。

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、「Accelerate での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、「」を参照してくださいAccelerate でのサービスリクエスト管理。

## Accelerate のリソースインベントリ

AMS Accelerate が AWS アカウント または アカウントにデプロイするすべてのリソースは、`resource_inventory.zip`ファイル resource_inventory.xlsx スプレッドシート (圧縮) に一覧表示されます。

> **Note**
>
> リソース名列のプレフィックス CFN: は、リソース名ではなく CloudFormation 論理 ID を示します。これらは、S3 バケットポリシーなど、名前のないリソースに表示されます。

AMS は、「」で説明されているように、一連のサービスをデプロイしますサービスの説明。空のアカウントにデプロイする場合、デプロイのコストは低くなりますが、使用率が増加するにつれてコストが増加します。たとえば、ログが作成され、リソースが変更されると設定ルールが呼び出されます。

設定ルールに複数の変更を加えると、複数の設定コンプライアンス呼び出しがトリガーされ、コストが高くなる可能性があります。インスタンスのモニタリングに使用される Amazon CloudWatch にも同じ可能性が適用されます。モニタリングの詳細度が高いほど、サービスのコストも高くなります。AWS Backup は別の例です。複数のバックアップが保存されている場合、または保持期間が長い場合は、より多くのストレージを使用しているため、コストが高くなります。

これらの数値を予測するのは困難です。クラウドサービスデリバリーマネージャー (CSDM) との毎月のビジネスレビュー中に、変更を追跡し、コスト削減の機会領域を特定してください。

# AMS Accelerate の開始方法

AWS マネージドサービス (AMS) がアカウントをまだ運用していない場合は、まず AWS Managed Servicesサービス - 販売へのお問い合わせページを使用して、アマゾン ウェブ サービス (AWS) 販売担当者にお問い合わせください。

AMS にサインアップすると、AMS Accelerate チームが各 の次のオンボーディングプロセスを案内します AWS アカウント。

AWS Managed Services」で機能セットを確認してください。

> **Note**
>
> AMS Accelerate は GovCloud リージョンをサポートしています。サービスが に存在する場合は AWS GovCloud (US) Region、「 の開始方法 AWS GovCloud (US)」も参照してください。

## Accelerate のアカウントオンボーディングプロセス

AMS Accelerate へのアカウントのオンボーディングには 4 つのステージがあります。

1. ステップ 1. Accelerate でのアカウント検出 は、アカウントの現在の状態を評価し、アカウントをオンボーディングするためのテクニカルブロッカーを特定します。
2. ステップ 2. Accelerate での管理リソースのオンボーディング は、利用規約に同意し、AMS Accelerate クラウドアーキテクト (CAs) のオンボーディングロールを作成します。CA は、セキュリティベースラインの設定と、必要に応じて問題の解決を支援します。
3. ステップ 3. デフォルトポリシーを使用した AMS 機能のオンボーディング for Accelerate のモニタリング、パッチ適用、バックアップなどの機能。
4. ステップ 4. Accelerate の機能をカスタマイズする は、EC2 インスタンスを含むリソースがアプリケーション用に正しく設定されていることを確認します。

### オンボーディングの前提条件を加速する

オンボーディングプロセスを開始する前に、 Accelerate コンポーネントが依存する技術的な依存関係を理解することが重要です。

> **Note**
>
> AMS Accelerate を使用するには、Enterprise On-Ramp または Enterprise の 2 つのサポートされている サポート プランのいずれかを使用している必要があります。デベロッパープランとビジネスプランは、AMS Accelerate の対象にはなりません。さまざまなプランの詳細については、「Compare サポート Plans」を参照してください。

## AMS Accelerate VPC エンドポイント

VPC エンドポイントは、VPC とサポートされている AWS サービス、および を搭載した VPC エンドポイントサービス間のプライベート接続を有効にします AWS。アウトバウンドインターネット接続をフィルタリングする必要がある場合は、次の VPC サービスエンドポイントを設定して、AMS Accelerate がサービスの依存関係と接続できるようにします。

> **Note**
>
> 次のリストでは、*region* は、米国東部 (オハイオ) AWS リージョンなど、 リージョンus-east-2の識別子を表します。

```
com.amazonaws.region.logs
com.amazonaws.region.monitoring
com.amazonaws.region.ec2
com.amazonaws.region.ec2messages
com.amazonaws.region.ssm
com.amazonaws.region.ssmmessages
com.amazonaws.region.s3
com.amazonaws.region.events
```

AWS VPC エンドポイントを設定する方法については、「VPC エンドポイント」を参照してください。

> **Note**
>
> 上記のすべてのサービスについて アカウントに VPC エンドポイントを作成する場合は、このサンプル CloudFormation テンプレートを参照してください。このテンプレートを更新し、ユースケースに従って VPC エンドポイント定義を削除または追加できます。

## Accelerate でのアウトバウンドインターネット接続

1. egressMgmt.zip をダウンロードします。
2. **ams-egress.json** ファイルを開きます。
3. JSON プロパティで URLs を見つけます。
   - `WindowsPatching`
   - `RedHatPatching`
   - `AmazonLinuxPatching`
   - `EPELRepository`
4. これらの URLsへのアクセスを許可します。

## Accelerate でのアウトバウンド接続のテスト

次のいずれかの方法を使用してアウトバウンド接続をテストします。

> **Note**
>
> スクリプト/コマンドを実行する前に、赤い*#####*を などのリージョン識別子に置き換えますus-east-1。

### Windows PowerShell スクリプト

```
$region = 'region'
@('logs','monitoring','ec2','ec2messages','ssm','ssmmessages','s3','events') | `
ForEach-Object { `
Test-NetConnection ("$_" + '.' + "$region" + '.amazonaws.com') -Port 443 } | `
Format-Table ComputerName,RemotePort,RemoteAddress,PingSucceeded,TcpTestSucceeded -
AutoSize
```

### Linux コマンド

```
for endpoint in logs monitoring ec2 ec2messages ssm ssmmessages s3 events; do nc -zv
 $endpoint.region.amazonaws.com 443; done
```

### Accelerate の Amazon EC2 Systems Manager

AWS Systems Manager エージェント (SSM エージェント) は、AMS が管理するすべての EC2 インスタンスにインストールする必要があります。また、SSM エージェントが必要とするバケットのアクセス許可を追加する必要があります。Amazon EC2 の概要については、「」を参照してくださいステップ 3. デフォルトポリシーを使用した AMS 機能のオンボーディング。

### Accelerate の IAM

AMS コンソールへのアクセスやバックアップの設定など、ユーザーが AMS Accelerate 機能を読み取って設定できるようにするには、これらのアクションを実行するための明示的なアクセス許可を AWS Identity and Access Management (IAM) で付与する必要があります。IAM ポリシーの例については、「AMS 機能を使用するアクセス許可」を参照してください。

## ステップ 1. Accelerate でのアカウント検出

AMS は、アカウント検出中にお客様と協力してアカウントの現在の状態を評価し、アカウントのオンボーディングのためのテクニカルブロッカーを特定します。AMS は、アカウント検出段階では運用サービスを提供しません。AMS は、`AWSServiceRoleForSupport`サービスにリンクされたロールを使用してテクニカルブロッカーを特定し、ユーザーと協力してそれらを修復してから、アカウントレベルのオンボーディングステージに移行します。

### Accelerate でのアカウント検出プロセス

アカウントの分析と検出に役立つように、AMS はオペレーションチェックを実行して、読み取り専用 API コールを通じてテクニカルブロッカーを特定します。アカウントが AMS にオンボーディングされると、これらのチェックはアカウントの体制を維持するためにオンデマンドで実行されます。AMS はお客様と協力して、必要に応じてこれらのチェックに関連する検出結果を修復します。AMS は、アカウント検出の一部として以下のオペレーションチェックと読み取り専用 API アクションを使用します。

| 運用チェック | 目的 | AWS 使用される API コール |
| --- | --- | --- |
| AWS Control Tower バージョン評価 | AWS Control Tower バージョンを識別して、 のオンボーディングでサポートされている最小バージョンであること | • `ControlTower:GetLandingZone`<br>• `ControlTower:ListEnabledControls` |

| 運用チェック | 目的 | AWS 使用される API コール |
| --- | --- | --- |
| | を確認します AWS アカウント。 | • ControlTower:ListLandingZones |
| AWS CloudTrail 評価 | CloudTrail AWS CloudTrail 証跡のコストを最小限に抑える AWS アカウント ために、 をオンボーディングするための証跡とその設定を識別します。 | • CloudTrail:GetTrail<br>• CloudTrail:ListTrails<br>• S3:GetBucketOwnershipControls<br>• S3:GetBucketPolicy<br>• KMS:GetKeyPolicy<br>• CloudTrail:GetEventSelectors<br>• S3:GetBucketLogging<br>• S3: GetBucketLifecycleConfiguration<br>• S3: GetBucketEncryption |
| CloudFormation フック評価 | での AMS サービスのデプロイをブロック AWS アカウント するオンボーディングの CloudFormation フックを識別します AWS アカウント。 | • CloudFormation:ListTypes |
| Amazon EC2 インスタンスの評価 | AWS Systems Manager エージェント (SSM エージェント) を実行 AWS アカウント しておらず、AMS でサポートされていない の EC2 インスタンスを識別します。 | • EC2:DescribeInstances<br>• EC2:DescribeImages<br>• SSM:DescribeInstanceInformation |

AMS Accelerate は、業界のベストプラクティスに従ってコンプライアンス資格を満たし、維持します。アカウントへの AMS Accelerate Discovery アクセスは、AWSServiceRoleForSupport サービスにリンクされたロール AWS CloudTrail を介して に記録されます。これは、要件のモニタリングと監査に役立ちます。詳細については AWS CloudTrail、AWS CloudTrail 「 ユーザーガイド」を参照してください。

## ステップ 2. Accelerate での管理リソースのオンボーディング

これは、管理リソースのオンボーディングプロセスの概要です。

条件に同意する

クラウドサービスデリバリーマネージャー (CSDM) が承認プロセスを案内します。利用規約、選択、アドオン、サービスレベルアグリーメント (SLA) AWS リージョンに同意する必要があります。

AMS ロールにアクセス許可を付与する

AMS プロセスと Cloud Architect へのアクセスを許可する必要があります。これを行うには、ロールごとに CloudFormation スタックを作成します。AMS ロールを作成するテンプレート 「」と「」を参照してくださいfor Accelerate CloudFormation aws_managedservices_onboarding_roleでを作成する。詳細については、「AMS Accelerate でのアクセス管理」を参照してください。

AMS が設定を確認する

Cloud Architect (CA) は、サービスコントロールポリシー (SCPs) や、AMS が AMS に必要なツールやリソースをデプロイできない可能性のあるセキュリティ検出結果など、アカウントで発生する可能性のある設定上の問題も探します。CA は、検出結果を修復し、AMS ツールとリソースのデプロイに対するブロッカーを削除するのに役立ちます。

AMS が AWS CloudTrail 証跡設定を確認する

Cloud Architect (CA) は CloudTrail 証跡設定を確認し、AMS でグローバル CloudTrail 証跡をデプロイするか、Accelerate を CloudTrail アカウントまたは Organization 証跡リソースと統合するかを確認します。Accelerate を CloudTrail 証跡と統合することを選択した場合、CA は CloudTrail 証跡リソースの設定に必要な更新をガイドします。

AMS が管理リソースをデプロイする

AMS チームは、AMS Accelerate のさまざまなサービスを提供するツールと AWS リソースをデプロイします。完了すると、AMS は AWS Managed Services アカウントを構築し、アカウントがアクティブであることを AMS から通知されます。

これで、オンボーディング管理リソースステージは終了です。オンボーディングプロセスの次のステップ に直接進むことができますステップ 3. デフォルトポリシーを使用した AMS 機能のオンボーディング。

> **Note**
>
> アカウントがアクティブになったので、次のいずれかのタスクを実行できます。
>
> - サポートセンターコンソールを使用して、 AWS インフラストラクチャのインシデントとサービスリクエストを作成します。「AMS Accelerate 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」を参照してください。
> - AMS、 によってデプロイされた AWS Config ルールのアカウントの適合ステータスを確認しますAccelerate の設定コンプライアンス。
> - GuardDuty および Macie (オプション) の検出結果を見つけて分析します。「GuardDuty によるモニタリング」を参照してください。
> - CloudTrail ログへのアクセスと監査
> - AMS Accelerate アカウントの変更を追跡します。「AMS Accelerate アカウントの変更の追跡」を参照してください。
> - Resource Tagger を使用してタグを作成します。「リソースタガーの高速化」を参照してください。
> - パッチ、バックアップ、 AWS Config レポートをリクエストします。「レポートとオプション」を参照してください。

## 設定を確認して更新し、AMS Accelerate が CloudTrail 証跡を使用できるようにします。

AMS Accelerate は、アカウント内のすべてのリソースの監査とコンプライアンスを管理するために AWS CloudTrail ログ記録に依存しています。オンボーディング中に、 Accelerate がプライマリ AWS リージョンに CloudTrail 証跡をデプロイするか、既存の CloudTrail アカウントまたは Organization 証跡によって生成されたイベントを使用するかを選択します。アカウントに証跡が設定されていない場合、 Accelerate はオンボーディング中にマネージド CloudTrail 証跡をデプロイします。

> **Important**
>
> CloudTrail ログ管理設定は、AMS Accelerate を CloudTrail アカウントまたは Organization 証跡と統合する場合にのみ必要です。

Cloud Architect (CA) を使用して、CloudTrail イベント配信先の CloudTrail 証跡設定、Amazon S3 バケットポリシー、および AWS KMS キーポリシーを確認します。 Amazon S3

Accelerate が CloudTrail 証跡を使用する前に、Cloud Architect (CA) と協力して Accelerate の要件を満たすように設定を確認して更新する必要があります。Accelerate を CloudTrail Organization 証跡と統合することを選択した場合、CA はお客様と協力して CloudTrail イベント配信先の Amazon S3 バケットと AWS KMS キーポリシーを更新し、Accelerate アカウントからのクロスアカウントクエリを有効にします。Amazon S3 バケットは、 Accelerate が管理するアカウント、またはユーザーが管理するアカウントにあることができます。オンボーディング中、 Accelerate は CloudTrail Organization 証跡イベントの配信先に対してクエリを実行できることを検証し、クエリが失敗するとオンボーディングを一時停止します。CA と協力してこれらの設定を修正し、オンボーディングを再開できるようにします。

CloudTrail アカウントまたは組織の証跡設定を確認して更新する

CloudTrail アカウントまたは Organization 証跡リソースの Accelerate CloudTrail ログ管理を統合するには、次の設定が必要です。

- CloudTrail 証跡は、すべての からのイベントをログに記録するように設定されています AWS リージョン。
- CloudTrail 証跡では、グローバルサービスイベントが有効になっています。
- CloudTrail アカウントまたは Organization 証跡は、読み取りおよび書き込みイベントを含むすべての管理イベントをログに記録し、 AWS KMS Amazon RDS Data API イベントログ記録が有効になっています。 https://docs.aws.amazon.com/awscloudtrail/latest/userguide/logging-management-events-with-cloudtrail.html#read-write-events-mgmt
- CloudTrail 証跡では、ログファイルの整合性検証が有効になっています。
- CloudTrail 証跡の Amazon S3 バケットは、SSE-S3 または SSE-KMS 暗号化を使用してイベントを暗号化するためにイベントを配信します。
- CloudTrail 証跡がイベントを配信する Amazon 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ます。

- CloudTrail 証跡がイベントを配信する Amazon S3 バケットには、CloudTrail 証跡データを少なくとも 18 か月間保持するライフサイクル設定があります。
- CloudTrail 証跡がイベントを配信する Amazon S3 バケットには、オブジェクト所有権がバケット所有者に設定されています。
- CloudTrail 証跡がイベントを配信する Amazon S3 バケットは、 Accelerate からアクセスできます。

CloudTrail イベント配信先の Amazon S3 バケットポリシーを確認して更新する

オンボーディング中、Cloud Architect (CA) と協力してAmazon S3 バケットポリシーステートメントを CloudTrail イベント配信先に追加します。ユーザーが Accelerate アカウントから CloudTrail イベント配信先 Amazon S3 バケットの変更をクエリできるようにするには、Accelerate が管理する Organization の各アカウントに統一された名前の IAM ロールをデプロイし、すべての Amazon S3 バケットポリシーステートメント`aws:PrincipalArn`のリストに追加します。この設定では、ユーザーは Athena を使用して Accelerate でアカウントの CloudTrail Organization 証跡イベントをクエリおよび分析できます。Amazon S3 バケットポリシーを更新する方法の詳細については、Amazon Simple Storage Service ユーザーガイドの「Amazon S3コンソールを使用したバケットポリシーの追加」を参照してください。

> **Important**
>
> Amazon S3 バケットポリシーの更新は、Accelerate が一元化された S3 バケットにイベントを配信する CloudTrail 証跡と統合されている場合にのみ必要です。Accelerate は、一元化されたバケットに を配信する CloudTrail 証跡との統合をサポートしていませんが、 AWS 組織の下にアカウントはありません。

> **Note**
>
> Amazon S3 バケットポリシーを更新する前に、*##*フィールドを該当する値に置き換えます。
>
> - *amzn-s3-demo-bucket* アカウントからの証跡イベントを含む Amazon S3 バケットの名前。
> - *your-organization-id* と、アカウントがメンバーである AWS 組織の ID。

- *your-optional-s3-log-delievery-prefix* と CloudTrail 証跡の Amazon S3 バケット配信プレフィックス。例えば、CloudTrail 証跡の作成時に設定した my-bucket-prefixなどです。 CloudTrail

  証跡に Amazon S3 バケット配信プレフィックスを設定していない場合は、次の Amazon S3 バケットポリシーステートメントから*#your-optional-s3-log-delievery-prefix*」とスラッシュ (/) を削除します。

次の 3 つの Amazon S3 バケットポリシーステートメントは、 Accelerate アカウントからイベント配信先 Amazon S3 バケット内の CloudTrail イベントを分析するための の設定を取得して AWS Athena クエリを実行するアクセスを Accelerate に付与します。

```
{
    "Sid": "DONOTDELETE-AMS-ALLOWBUCKETCONFIGAUDIT",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": [
        "s3:GetBucketLogging",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetEncryptionConfiguration"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
    "Condition": {
        "StringEquals": {
            "aws:PrincipalOrgID": "your-organization-id"
        },
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/ams-access-*"
            ]
        }
    }
},
{
    "Sid": "DONOTDELETE-AMS-ALLOWLISTBUCKET",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
```

```
    },
    "Action": "s3:ListBucket",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": "athena.amazonaws.com"
        },
        "StringLike": {
            "s3:prefix": "your-optional-s3-log-delievery-prefix/AWSLogs/*"
        },
        "StringEquals": {
            "aws:PrincipalOrgID": "your-organization-id"
        },
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/ams-access-*"
            ]
        }
    }
},
{
    "Sid": "DONOTDELETE-AMS-ALLOWGETOBJECT",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/your-optional-s3-log-delievery-
prefix/AWSLogs/*",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": "athena.amazonaws.com"
        },
        "StringEquals": {
            "aws:PrincipalOrgID": "your-organization-id"
        },
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/ams-access-*"
            ]
        }
    }
}
```

CloudTrail イベント配信先の AWS KMS キーポリシーを確認して更新する

オンボーディング中、Cloud Architect (CA) と協力して、Amazon S3 バケットに配信される CloudTrail 証跡イベントの暗号化に使用される AWS KMS キーポリシーを更新します。参照 AWS KMS キーポリシーステートメントを既存の AWS KMS キーに追加してください。これにより、 Accelerate が既存の CloudTrail 証跡イベント配信先 Amazon S3 バケットと統合され、イベントが復号化されるように設定されます。ユーザーが Accelerate アカウントから CloudTrail イベント配信先 Amazon S3 バケットの変更をクエリできるようにするには、Accelerate が管理している Organization の各アカウントに統一された名前の IAM ロールをデプロイし、それを「aws:PrincipalArn」リストに追加します。この設定では、ユーザーはイベントをクエリできます。

考慮すべき AWS KMS キーポリシーの更新シナリオはさまざまです。すべてのイベントを暗号化するために CloudTrail 証跡に設定された AWS KMS キーのみがあり、Amazon S3 バケット内のオブジェクトを暗号化する AWS KMS キーがない場合があります。または、CloudTrail によって配信されるイベントを暗号化する AWS KMS キーと、Amazon S3 バケットに保存されているすべてのオブジェクトを暗号化する AWS KMS 別のキーがある場合があります。 AWS KMS キーが 2 つある場合は、各 AWS KMS キーのキーポリシーを更新して、Accelerate に CloudTrail イベントへのアクセスを許可します。ポリシーを更新する前に、参照 AWS KMS キーポリシーステートメントを既存の AWS KMS キーポリシーに修正してください。 AWS KMS キーポリシーを更新する方法の詳細については、「 AWS Key Management Service ユーザーガイド」の「キーポリシーの変更」を参照してください。

**Important**

Accelerate がログファイル SSE-KMS 暗号化が有効になっている CloudTrail 証跡と統合されている場合にのみ、 AWS KMS キーポリシーを更新する必要があります。

**Note**

この AWS KMS キーポリシーステートメントを Amazon S3 バケットに配信される AWS CloudTrail イベントの暗号化に使用される AWS KMS キーに適用する前に、次の##フィールドを該当する値に置き換えます。

- アカウントがメンバーである AWS 組織の ID を持つ *YOUR-ORGANIZATION-ID*。

この AWS KMS キーポリシーステートメントは、Accelerate が CloudTrail イベントのクエリと分析に使用する Athena に制限されたアクセスを持つ、組織内の各アカウントから Amazon S3 バケットに配信される証跡イベントの復号化とクエリへのアクセスを高速化します。 CloudTrail

```
{
    "Sid": "DONOTDELETE-AMS-ALLOWTRAILOBJECTDECRYPTION",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": [
        "kms:Decrypt",
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": "athena.amazonaws.com"
        },
        "StringEquals": {
            "aws:PrincipalOrgID": "YOUR-ORGANIZATION-ID"
        },
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/ams-access-*"
            ]
        }
    }
}
```

## AMS ロールを作成するテンプレート

次の AMS ロールは、AMS クラウドアーキテクト (CA) にアクセス許可を付与します。次の zip ファイルには、IAM ロール、アクセス許可ポリシー、信頼ポリシーの作成を簡素化する Terraform コードと CloudFormation テンプレートが含まれています。詳細については、CA にお問い合わせください。

| ロール名 | で必須 | サンプルテンプレート |
| --- | --- | --- |
| `aws_managedservices_onboarding_role` | AMS personnel during onboarding only | onboarding_role_minimal.zip |

> **Note**
>
> サンプルテンプレート (ロールごとに 1 つずつ) を選択してダウンロードしたら、 の CloudFormation スタックの定義としてアップロードしますfor Accelerate CloudFormation `aws_managedservices_onboarding_role`で を作成する。

## for Accelerate CloudFormation **`aws_managedservices_onboarding_role`**で を作成する

AWS Identity and Access Management ロール は、 CloudFormation から `aws_managedservices_onboarding_role`を使用して作成できます AWS マネジメントコンソール。または、 のコマンドを使用してロールを AWS CloudShell デプロイすることもできます。

を使用する AWS マネジメントコンソール

> **Note**
>
> 開始する前に、各ロールの JSON または YAML ファイルをアップロードする準備をします。詳細については、「AMS ロールを作成するテンプレート」を参照してください。

からロールを作成するには AWS マネジメントコンソール、次の手順を実行します。

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/cloudformation で CloudFormation コンソールを開きます。

2. スタックの作成 > 新しいリソース (標準 ) を選択します。次のページが表示されます。

3. テンプレートファイルのアップロードを選択し、IAM ロールの JSON または YAML ファイルをアップロードしてから、次へを選択します。次のページが表示されます。

4. スタック名フィールドにスタック名**`ams-onboarding-role`**「」を入力します。「YYYY-MM-DDT00:00:00Z」の形式を使用して DateOfExpiry を入力します (現在の日付から 30 日後が推奨されます ) 。このページに到達するまで、下にスクロールして次を選択します。

5. チェックボックスがオンになっていることを確認し、スタックの作成を選択します。
6. スタックが正常に作成されたことを確認します。

からコマンドを使用する AWS CloudShell

IAM aws_managedservices_onboarding_role ロールをデプロイするには、 で次のコマンドを実行しますAWS CloudShell。

AWS CLI

```
curl -s "https://docs.aws.amazon.com/en_us/managedservices/latest/accelerate-guide/
samples/onboarding_role_minimal.zip" -o "onboarding_role_minimal.zip"
unzip -q -o onboarding_role_minimal.zip
aws cloudformation create-stack \
    --stack-name "aws-managedservices-onboarding-role" \
    --capabilities CAPABILITY_NAMED_IAM \
    --template-body file://onboarding_role_minimal.json \
    --parameters ParameterKey=DateOfExpiry,ParameterValue="`date -d '+30 days' -u '+
%Y-%m-%dT%H:%M:%SZ'`"
```

AWS Tools for PowerShell

```
Invoke-WebRequest -Uri 'https://docs.aws.amazon.com/en_us/managedservices/
latest/accelerate-guide/samples/onboarding_role_minimal.zip' -OutFile
 'onboarding_role_minimal.zip'
Expand-Archive -Path 'onboarding_role_minimal.zip' -DestinationPath . -Force
New-CFNStack `
    -StackName 'aws-managedservices-onboarding-role' `
    -Capability CAPABILITY_NAMED_IAM `
    -TemplateBody (Get-Content 'onboarding_role_minimal.json' -Raw) `
    -Parameter @{ParameterKey = "DateOfExpiry"; ParameterValue = (Get-
Date).AddDays(30).ToString('yyyy-MM-ddTHH:mm:ssZ')}
```

ロールを作成したら、Cloud Architect (CA) と協力してステップ 2. Accelerate での管理リソースのオンボーディングプロセスを完了します。AMS がアカウントがアクティブであることを通知したら、インスタンスをオンボードする準備が整います。

# ステップ 3. デフォルトポリシーを使用した AMS 機能のオンボーディング

この段階では、デフォルトのポリシーを使用して AMS 機能をオンボードします。これには、Amazon EC2 インスタンスの追加、モニタリング、バックアップ、 AWS Config 修復、パッチの設定 (該当する場合、AMS パッチオーケストレーターは特にリクエストする必要があるアドオンです) が含まれます。これは自分で行うか、入力に基づいて AMS に機能をオンボードするようにリクエストできます。AMS にヘルプをリクエストするには、サービスリクエストを作成し、タスクを完了するために必要なすべての入力を指定します。サービスリクエストはすぐには解決されないことに注意してください。

> **Note**
>
> アカウントはバックアップ、パッチ、またはモニタリングにデフォルトポリシーを使用する場合がありますが、適切なポリシーを有効にするにはリソースにタグを付ける必要があります。

トピック


- ( オプション) Accelerate のクイックスタートテンプレート
- オンボーディング Accelerate モニタリング
- 高速化のための EC2 インスタンスのオンボーディング
- Accelerate AWS Backup でのオンボーディング
- Accelerate でのオンボーディングパッチ適用
- Accelerate で不適合レポートを確認する


## ( オプション) Accelerate のクイックスタートテンプレート

クイックスタートテンプレートは、Accelerate が有効な AWS アカウントでの AMS Resource Tagger のデプロイと設定を自動化します。このテンプレートは、手動セットアップと比較して時間と労力を節約します。このテンプレートをそのまま使用して、モニタリング、パッチ適用、バックアップの基本を 1 つのアカウントで定義します。または、StackSet として使用して Organizations ユニット間で設定を適用し、複数のアカウントの設定を標準化します。

また、独自のカスタム AMS Resource Tagger プロファイルを構築する開始点として使用し、ドキュメントのスニペットを使用して、タグ付けのより複雑な定義を作成することもできます。

### クイックスタートテンプレートの機能

クイックスタートテンプレートは次のタスクを完了します。

- AMS Resource Tagger の設定バージョンを作成してデプロイします。
- AMS 管理とモニタリングリソースの作成を可能にする Amazon EC2 インスタンスにタグを適用します。
- (オプション) 必要なスケジュールでパッチを適用できるようにするマネージド EC2 インスタンスにタグを適用し、パッチ適用を容易にするためにパッチ適用メンテナンスウィンドウを作成します。

> **Warning**
>
> デフォルトでは、インスタンスは再起動され、停止したインスタンスはパッチインストールのために自動的に開始されます。

- (オプション) マネージド EC2 インスタンスにタグを適用し、デフォルトの AMS Backup Plan で定義されているとおりにバックアップできるようにします。
- (オプション) 拡張バックアッププランに従ってバックアップできるようにするマネージド Amazon Relational Database Service (Amazon RDS) リソースにタグを適用します。バックアッププランは、Amazon RDS のポイントインタイムリカバリ (PITR) も有効にします。Amazon RDS 自動バックアップが有効になっていない場合、データベースは次のバックアップウィンドウの時刻近くに再起動します。

### クイックスタートテンプレートの上書きと除外

このテンプレートを使用してクイックスタートスタックを作成したら、次のステップを使用して、管理/モニタリング、パッチ適用、またはバックアップから特定のインスタンスを除外します。

- 管理とモニタリング： EC2 インスタンスが AMS によって管理およびモニタリングされないようにするには、次のタグをインスタンスに追加します: `ExcludeFromAMSQuickStartMonitoring=true`。
- パッチ適用： Auto Scaling グループ、Amazon Elastic Container Service、または Amazon Elastic Kubernetes Service クラスターのメンバーである EC2 インスタンスは、このクイックスタートテンプレートによってパッチ適用から除外されます。

パッチウィンドウの作成と EC2 インスタンスのパッチ関連のタグ付けを無効にするには、CloudFormation スタックパラメータを に設定しますEnablePatching=false。

で EC2 インスタンスがクイックスタートパッチ適用ウィンドウのターゲットから除外するにはEnablePatching=true、次のタグをインスタンスに追加します: ExcludeFromAMSQuickStartPatching=true。

- バックアップ： Auto Scaling グループ、ECS、または EKS クラスターのメンバーである EC2 インスタンスは、このクイックスタートテンプレートによってバックアップから除外されます。

  EC2 インスタンスをデフォルトの AMS Backup Plan のターゲットから除外するには、 の場合EnableBackup=true、このタグをそのインスタンスに追加します: ExcludeFromAMSQuickStartBackup=true。

> **Tip**
>
> EC2 インスタンスは一括でタグ付けできます。タグエディタを使用して、 の 1 つのステップでリソースを一括選択およびタグ付けします AWS マネジメントコンソール。

クイックスタートテンプレートパラメータ

このクイックスタートテンプレートは、タグを追加するインスタンスを除き、アカウントams:rt:ams-managed=true内のすべての EC2 インスタンスにExcludeFromAMSQuickStartMonitoring=trueタグを追加するように Resource Tagger を設定します。以下のパラメータを使用して、要件に応じてこのスタックのオプション部分を制御します。

| CFN パラメータ | 値 | 効果 |
| --- | --- | --- |
| EnableBackup | 'true' (デフォルト ) | すべての AMS マネージド EC2 インスタンス (ams:rt:ams-managed=true ) には、デフォルトの AMS Backup Plan に従って、UTC 4AM 時にバックアップams:rt:backup-orchestrator=true 用に というタグが付けられます。 |

| CFN パラメータ | 値 | 効果 |
| --- | --- | --- |
| | | すべての RDS インスタンスとクラスターについて、テンプレートは拡張バックアッププランに従って最大保持期間 (31 日 ) でams:rt:backup-orchestrator-enhanced=true 「継続的バックアップ」を適用します。 https://docs.aws.amazon.com/aws-backup/latest/devguide/point-in-time-recovery.html#point-in-time-recovery-rds https://docs.aws.amazon.com/manageservices/latest/accelerate-guide/acc-backup-select-plan.html#acc-backup-plan-enhanced<br><br>これにより PITR の保持期間が変更された場合、たとえば、他の保留中の設定更新がある場合などに、データベースが再起動されることがあります。 |
| | 「false」 | このクイックスタートテンプレートでは、バックアップの対象となるインスタンスはありません。 |
| EnablePatching | 'false' (デフォルト ) | このクイックスタートテンプレートによるパッチ適用の対象となるインスタンスはありません。 |

| CFN パラメータ | 値 | 効果 |
| --- | --- | --- |
| | 「true」 | すべての AMS マネージドインスタンス (`ams:rt:ams-managed=true` ) には というタグが付けられ`ams:rt:Patch Group=AMS QuickStartPatchWindow` 、で定義されたスケジュールに従ってパッチ適用を容易にするために基本的な SSM メンテナンスウィンドウリソースが作成されます`CronExpression` 。<br><br>`ams:rt:Patch Group` タグを EC2 インスタンスに適用するには、そのインスタンスのインスタンスメタデータ内のタグへのアクセスをオフにする必要があります。 |
| CronExpression | - | のデフォルト値は、 `Timezone`パラメータに従って毎月第 2 土曜日の午後 7 時 30 分`cron(0 30 19 ? * SAT#2 *)`に設定します。cron 構文を使用します。 |
| タイムゾーン | - | ターゲットインスタンスには、に従ってパッチが適用されます`CronExpression` 。IANA 形式を使用します。 |

クイックスタートテンプレートをダウンロードする

AMSQuickStart.zip ファイルをダウンロードします。

または、 で次のコマンドを実行して をAWS CloudShellデプロイします`AMSQuickStart.yaml`。

### AWS Command Line Interface

```
curl -s "https://docs.aws.amazon.com/en_us/managedservices/latest/accelerate-guide/
samples/AMSQuickStart.zip" -o "AMSQuickStart.zip"
unzip -q -o AMSQuickStart.zip
for region in region1 region2 ;
do
aws cloudformation create-stack \
    --region $region \
    --stack-name "AMSQuickStart" \
    --template-body file://AMSQuickStart.yaml \
    --parameters \
        ParameterKey=EnableBackup,ParameterValue="true" \
        ParameterKey=EnablePatching,ParameterValue="false" \
        ParameterKey=Timezone,ParameterValue="US/Eastern" \
        ParameterKey=CronExpression,ParameterValue="cron(0 30 19 ? * SAT#2 *)" \
;
done
```

### AWS Tools for PowerShell

```
Invoke-WebRequest -Uri 'https://docs.aws.amazon.com/en_us/managedservices/latest/
accelerate-guide/samples/AMSQuickStart.zip' -OutFile 'AMSQuickStart.zip'
Expand-Archive -Path 'AMSQuickStart.zip' -DestinationPath . -Force
@('region1', 'region2') | `
ForEach-Object { `
New-CFNStack `
    -Region $_ `
    -StackName 'AMSQuickStart' `
    -TemplateBody (Get-Content 'AMSQuickStart.yaml' -Raw) `
    -Parameter @(
        @{ParameterKey = "EnableBackup"; ParameterValue = "true"},
        @{ParameterKey = "EnablePatching"; ParameterValue = "false"},
        @{ParameterKey = "Timezone"; ParameterValue = "US/Eastern"},
        @{ParameterKey = "CronExpression"; ParameterValue = "cron(0 30 19 ? * SAT#2
 *)"}
    )
}
```

各パラメータの説明については、前のセクション「」を参照してくださいクイックスタートテンプレートパラメータ。

# オンボーディング Accelerate モニタリング

モニタリングは、Amazon EC2 インスタンスを除くすべての新しいリソースでデフォルトで有効になっています。インスタンスにタグを付けることで、Amazon EC2 インスタンスのモニタリングを開始できます。

モニタリングをオンボードするには、まず AMS がモニタリングするリソースを 設定でモニタリングし、無視するリソースを無視することを確認します。

次の CloudWatch ダッシュボードを使用して、AMS のモニタリングとタグ付けの対象となるリソースの数と、対象ではないリソースの数を確認できます。アカウントで、CloudWatch ダッシュボードコンソールに移動し、次のいずれかを選択します。

- AMS-Alarm-Manager-Reporting-Dashboard
- AMS-Resource-Tagger-Reporting-Dashboard

ダッシュボードメトリクスの詳細については、以下を参照してください。

- Alarm Manager for Accelerate によってモニタリングされるリソースの数の表示
- Resource Tagger によって管理されるリソースの数の表示

Accelerate でモニタリングするオンボーディングリソース

例えば、non-EC2リソースのデフォルトモニタリングを無効にするなど、デフォルトの動作を上書きするには、カスタム設定プロファイルを使用してそれらのリソースのタグを解除する必要があります。モニタリングのタグ付けの詳細については、「」を参照してくださいAccelerate でのモニタリング。

EC2 インスタンスのモニタリングは、インスタンスをオンボードするまで無効になります。これには、カスタム設定プロファイルを使用したインスタンスのタグ付けが含まれます。次のセクションでは、EC2 インスタンスのオンボーディングについて説明します。

Accelerate でのモニタリング設定プロファイルの作成

- デフォルト設定の使用については、「」を参照してくださいアラームマネージャーの高速化。
- カスタム設定の使用については、「」を参照してくださいAccelerate アラームのデフォルト設定の変更。

## 高速化のための EC2 インスタンスのオンボーディング

EC2 インスタンスは、自動インスタンス設定と呼ばれるプロセスを通じて AMS Accelerate にオンボードされます。これにより、各インスタンスが正しいログを書き込み、AMS がインスタンスを適切に管理するための正しいメトリクスを出力します。AMS が一部を無視するように特に希望しない限り、すべての EC2 インスタンスをオンボードする必要があります。自動インスタンス設定では、AMS がインスタンスを設定できるようにする特定の条件が満たされている必要があります (詳細については、「」を参照してくださいAccelerate の自動インスタンス設定の前提条件 )。最も重要な条件は、AMS が管理する各 Amazon EC2 インスタンスに AWS Systems Manager エージェント (SSM エージェント) をインストールする必要があることです。SSM エージェントの詳細については、「SSM エージェントの使用」を参照してください。

Accelerate 用の標準 AMIs にプリインストールされた SSM

SSM エージェントは、以下のオペレーティングシステム用に既に用意されている AMIs AWSにインストールされています。

- Amazon Linux および Amazon Linux 2
- SUSE Linux Enterprise Server (SLES) 12 および 15
- Microsoft Windows Server 2019、2016、2012 R2、2012
- Ubuntu Linux 18.04 および 20.04

これらの AWS AMI AMIs「」を参照してくださいAccelerate でのインスタンスのタグ付け。

Accelerate での SSM の手動インストール

次のオペレーティングシステムの場合、またはカスタム AMI を使用する場合は、SSM エージェントを手動でインストールできます。または、AMS SSM エージェントの自動インストール機能を使用できます。SSM 自動インストールの詳細については、「」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。手動インストールの手順については、お使いのオペレーティングシステムのリンクを選択してください。

- CentOS SSM のインストール
- Oracle SSM のインストール
- Red Hat SSM のインストール
- SUSE Linux Enterprise Server SSM のインストール
- Windows SSM のインストール

Accelerate でのインスタンスのタグ付け

SSM エージェントをインストールしたら、インスタンスにタグを付ける必要があります。「AMS Accelerate でのタグ付け」を参照してください。

Accelerate の自動インスタンス設定

インスタンスにタグを付けると、AMS は自動インスタンス設定を実行します。これには以下が含まれます。

- オペレーティングシステムのログとメトリクスを記録する
- AMS エンジニアのリモートアクセスを有効にする
- インスタンスでリモートコマンドを実行する

これらのタスクは、AMS のモニタリング、パッチ、ログサービス、および AMS がインシデントに対応するために不可欠です。自動インスタンス設定の設定の詳細については、「」を参照してくださいAMS Accelerate の自動インスタンス設定。

自動インスタンス設定が完了すると、次のことが可能になります。

- サポートセンターコンソールを使用して、Amazon EC2 インスタンスとオペレーティングシステムのインシデントとサービスリクエストを作成します。詳細については、「AMS Accelerate 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」を参照してください。
- Amazon EC2 ログへのアクセスと監査
- パッチレポートを取得する

## Accelerate AWS Backup でのオンボーディング

バックアップを設定するには、バックアッププランと呼ばれるバックアップポリシーを作成する必要があります。バックアッププランは、バックアップする AWS リソース、バックアップする必要がある頻度、バックアップ保持期間を指定します。組織の継続性、セキュリティ、コンプライアンス要件を評価して、必要なバックアッププランを決定することをお勧めします。

オプトイン

- 以下の手順に従って、アカウント、リージョン、リソースタイプごとに AWS Backup が有効になっていることを確認します。

  開始方法 1: サービスオプトイン。

オプションで、開始方法 2: オンデマンドバックアップを作成します。

バックアッププランを選択する

- バックアッププランを選択するには、「」を参照してくださいAMS バックアッププランを選択する。

リソースの追加

デフォルトでは、リソースはバックアッププランに関連付けられません。これらはバックアッププランに追加する必要があります。

- バックアッププランにリソースを追加するには、「」を参照してくださいリソースにタグを付けて AMS バックアッププランを適用する。
- タグを使用してすべてのリソースでバックアップを有効にするには、「」を参照してくださいAccelerate でのバックアップのタグの管理。

## Accelerate でのオンボーディングパッチ適用

パッチ適用を設定して、ソフトウェアがup-to-dateであり、コンプライアンスポリシーを満たしていることを確認する必要があります。

AWS Backup 前提条件: パッチ適用メンテナンスウィンドウ中にルートボリュームスナップショットを作成できるようにするには、「Getting started 1: Service Opt-in」の手順に従って、Amazon EBS リソースタイプのアカウントとリージョンごとに AWS Backup が有効になっていることを確認します。（開始方法 2: オンデマンドバックアップの作成に進む必要はありません）。

パッチ適用のタイミング: パッチ適用はメンテナンスウィンドウ中に行われます。パッチが事前設定された時間にのみ適用されるように、メンテナンスウィンドウをスケジュールできます。

パッチ適用対象: パッチを適用する Amazon EC2 インスタンスをメンテナンスウィンドウに関連付ける必要があります。インスタンスをメンテナンスウィンドウに関連付けるには、Amazon EC2 インスタンスにタグを付け、メンテナンスウィンドウにそれらのタグをターゲットとして含める必要があります。

インストールするパッチ: パッチベースラインを使用して、オペレーティングシステムや重要度の高いパッチなど、特定のタイプのパッチを自動承認するルールを設定します。ルールに例外を指定することもできます。たとえば、常に承認または拒否されるパッチのリストなどです。

Amazon EC2 パッチポリシーのガイダンスパッチ適用に関する推奨事項については、「」を参照してください。

- パッチ管理の設定を開始するには、「」を参照してください。 AMS Accelerate でのパッチ管理を理解する
- カスタムパッチ設定を作成するには、「」を参照してくださいAMS Accelerate を使用したカスタムパッチベースライン。

### Accelerate で不適合レポートを確認する

AMS は、米国国立標準技術研究所 (NIST) クラウドセキュリティフレームワーク (CSF) である Center for Internet Security (CIS) によって設定された標準に対する違反を特定するのに役立つ AWS Config ルールをデプロイします。配信チームとの不適合レポートを確認して、アカウントが準拠状態にベースライン付けされるように修復アクションを優先することをお勧めします。

## ステップ 4. Accelerate の機能をカスタマイズする

この段階では、モニタリング、パッチ適用、バックアップをデフォルトのポリシーでオンボーディング済みです。これで、ニーズに合わせてポリシーをカスタマイズできます。

パッチ、バックアップ、モニタリングにデフォルトのポリシーを使用するか、必要に応じてカスタムポリシーを選択できます。AMS はタグを使用してリソースを運用ポリシーに関連付けます。AMS には、アプリケーションのグループ化やその他のグループ化ロジックに基づいて AWS リソースにタグを適用する方法に関するルールを指定できる Resource Tagger が用意されています。詳細については、「」を参照してくださいリソースタガーの高速化。

お客様が用意したタグ機能を使用すると、AMS リソースにカスタムタグを追加および削除できます。詳細については、「Accelerate のお客様が用意したタグ」を参照してください。

トピック

- Accelerate でモニタリングをカスタマイズする
- Accelerate でバックアップをカスタマイズする
- Accelerate でのパッチ適用のカスタマイズ

### Accelerate でモニタリングをカスタマイズする

アプリケーションのニーズに基づいてクラウドリソースのモニタリングをカスタマイズするには：

1. カスタムモニタリングポリシーを作成します。「Accelerate アラームのデフォルト設定の変更」を参照してください。
2. タグを使用してカスタムポリシーをリソースに適用します。「Accelerate でのモニタリング」を参照してください。
3. リソース所有者にアラートをルーティングします。「タグベースのアラート通知」を参照してください。

次の CloudWatch ダッシュボードを使用して、AMS のモニタリングとタグ付けの対象となるリソースの数と、対象ではないリソースの数を確認できます。アカウントで、CloudWatch ダッシュボードコンソールに移動し、次のいずれかを選択します。

- AMS-Alarm-Manager-Reporting-Dashboard
- AMS-Resource-Tagger-Reporting-Dashboard

ダッシュボードメトリクスの詳細については、以下を参照してください。

- Alarm Manager for Accelerate によってモニタリングされるリソースの数の表示
- Resource Tagger によって管理されるリソースの数の表示

## Accelerate でバックアップをカスタマイズする

AMS のデフォルトのバックアッププランをカスタマイズすることはできません。代わりに、アプリケーションのニーズに基づいて新しいバックアッププランを作成し、タグを使用してカスタムプランにリソースをアタッチします。AMS がバックアップするリソース、頻度、保持期間を選択するのはお客様次第です。組織の継続性、セキュリティ、コンプライアンス要件を評価して、必要なバックアッププランを決定することをお勧めします。

- バックアッププランを作成するには、「バックアッププランの作成」を参照してください。
- バックアッププランにリソースを割り当てるには、「バックアッププランにリソースを割り当てる」を参照してください。

## Accelerate でのパッチ適用のカスタマイズ

パッチ適用により、ソフトウェアがup-to-dateであり、コンプライアンスポリシーを満たしていることが保証されます。

パッチ適用のタイミング: パッチ適用はメンテナンスウィンドウ中に行われます。パッチが事前設定された時間にのみ適用されるように、メンテナンスウィンドウをスケジュールできます。

パッチ適用対象: パッチを適用する Amazon EC2 インスタンスをメンテナンスウィンドウに関連付ける必要があります。インスタンスをメンテナンスウィンドウに関連付けるには、Amazon EC2 インスタンスにタグを付け、メンテナンスウィンドウにそれらのタグをターゲットとして含める必要があります。

インストールするパッチ: パッチベースラインを使用して、オペレーティングシステムや重要度の高いパッチなど、特定のタイプのパッチを自動承認するルールを設定します。ルールに例外を指定することもできます。たとえば、常に承認または拒否されるパッチのリストなどです。

- 一般的なパッチ適用の推奨事項については、「」を参照してくださいパッチ適用に関する推奨事項。
- カスタムメンテナンスウィンドウを作成するには、「」を参照してくださいAMS でパッチメンテナンスウィンドウを作成する。
- カスタムパッチベースラインを作成するには、「」を参照してくださいAMS Accelerate を使用したカスタムパッチベースライン。
- パッチアラートをリソース所有者にルーティングするには、「」を参照してくださいAMS Accelerate のパッチ通知とパッチ障害を理解する。

## 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 Accelerate 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、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。
    - リソースのインシデント: AWS サポートセンターでインシデントケースを開くボタン、および承認待ちで注意が必要なインシデントケースの数とオープンケースの数
    - コンプライアンスステータス: 非準拠または準拠のルールとリソースへのリンク
    - サービスリクエスト: AWS サポートセンターでサービスリクエストケースを開くボタン、および承認待ちで注意が必要な の数とオープンな の数
    - アカウントレベルのセキュリティ: リアルタイム脅威検出 GuardDuty の検出結果とデータセキュリティおよびプライバシー Macie の検出結果の詳細へのリンク
    - クイックアクション: バックアップボールトまたはパッチインスタンスの設定ページを開く
  - 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
  - 設定: リソースが仕様に従って正常に管理されていることを確認します。
    - SSM エージェントのインストール: SSM エージェントが必要です
    - タグ付けルールを設定する: AMS Resource Tagger を開きます
    - アラームの設定: AMS CloudWatch アラーム設定を開きます
    - パッチスケジュールの設定: AWS Systems Manager コンソールを開きます
    - パッチベースラインの設定: AWS Patch Manager コンソールを開きます
    - バックアッププランの設定: AWS Backup コンソールを開きます
- 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
- 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 パターン

AWS Managed Services (AMS) パターンは、AMS マネージド環境での一連のユースケースを解決する一般化されたソリューションです。

AMS プラットフォームで運用する場合、AMS クラウドアーキテクト (CAs) はお客様と協力して、ビジネスおよび運用の要件を満たします。AMS のお客様は独自の方法で運用されていますが、同様のユースケースがあります。このような場合、CAs は一般的なソリューションテンプレート、つまり「パターン」を作成します。これは、最小限の設定とデプロイの労力で複数の顧客環境で使用されます。

AMS パターンは、AMS 顧客に機能を提供するのに役立つように構築されており、通常はそれをリクエストする顧客のアカウント CA によって構築されます。

## AMS パターンの仕組み

パターンをデプロイするために必要なクラウドフォーメーションテンプレートを含む各パターンの詳細をリクエストするには、*##### Pattern_Name* に関する追加の詳細をリクエストする」 (必要なパターンを置き換える) を件名として AMS サービスリクエストを送信し、AMS クラウドアーキテクト (CA) を追加連絡先オプションに追加します。

AMS パターンは 2 つの (2) カテゴリに分類されます。

- 汎用: パターンは、デプロイされ、複数の AMS 顧客が使用しているため、安定していると見なされます。
- プレビューモード: AMS では、検証のために非本番環境にプレビューモードパターンをデプロイし、デプロイ前に Cloud Architect と連携してユースケースについて話し合うことをお勧めします。

> **Important**
>
> AMS パターンは、デフォルトの AMS サービスレベルアグリーメント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) に準拠していません。パターンのサポートと更新はベストエフォートベースで行われます。
> この AWS コンテンツは、お客様と Amazon Web Services, Inc. または Amazon Web Services EMEA SARL (AWS 「欧州」) またはその両方との間のAWS カスタマーアグリーメントまたはその他の書面による契約の条件に従って提供されます。

このソフトウェアに具体化されたマテリアルは、明示、黙示、その他を問わず、いかなる種類の保証もなしに「現状有姿」で提供されます。これには、特定の目的への適合性の保証が含まれますが、これらに限定されません。

## AMS パターン

AMS パターン。

AMS パターン

| 名前 | 概要 | 利点 | カテゴリ |
| --- | --- | --- | --- |
| CloudWatch アラーム通知をカスタマイズする | CloudWatch アラーム通知をカスタマイズして、インスタンス名、アプリケーション ID などのインスタンスタグからの情報を含めます。 | アラーム通知にコンテキスト情報を追加すると、よりわかりやすくなり、実用的な情報が提供されます。 | モニタリング |
| ディスク使用状況レポート | ディスク使用状況レポートパターンは、複数のアプリケーションアカウントにわたるボリュームの消費領域を収集し、Athena テーブルクエリ機能を備えた Amazon S3 の一元的なレポートとして結果を表示します。 | アカウントボリュームの実際の使用状況に関するインサイトを提供し、コスト削減の機会を決定します。 | コスト最適化 |
| Prowler スタック | CloudShell を使用できない Amazon EC2 を使用するアカウントで Prowler チェックを実行します。 | アクセス許可またはタイムアウトの問題により、現在のセキュリティ体制に影響を与えずに CloudShel | セキュリティ |

| 名前 | 概要 | 利点 | カテゴリ |
| --- | --- | --- | --- |
| | | l を使用できない場合は、 Accelerate オンボーディング (Prowler) のブロックを解除してください。 | |
| カスタムオブジェクトキーを使用した AMS Amazon S3 レプリケーション | Amazon S3 オブジェクトのコピーを作成し、すべてのメタデータとオブジェクトキー (フォルダ) を保持します。<br><br>レプリケート元オブジェクトキーの一部をストライピングするか、レプリケーション中にカスタム送信先オブジェクトキーを作成します。 | Amazon S3 レプリケーション中にオブジェクトキー (フォルダ) をカスタマイズします。必要なフォルダにオブジェクトを移動するための追加のスクリプトは必要ありません。 | 信頼性 |
| Amazon EBS スナップショットの削除 | Lambda と CloudWatch Events に基づく自動化により AWS Backup、保持期間に基づいて、の外部で作成された Amazon EBS スナップショットの削除を自動化します。 | AWS Backup オーケストレーターの外部で作成された個々のスナップショットを消去し、時間の経過とともに追加コストを削減できます。 | コスト最適化 |

| 名前 | 概要 | 利点 | カテゴリ |
| --- | --- | --- | --- |
| AMS Amazon RDS シークレットのローテーション | CloudFormation テンプレートを使用して、サポートされている Amazon RDS データベース、Redshift、および DocumentDB のシークレットの更新に必要なすべてのリソース (Lambda 関数、セキュリティグループ、Elastic Network Interface、または ENIs) を自動的にデプロイします。 | データベースシークレットのローテーションを自動化し、ローテーションの失敗時に通知メカニズムを提供します。 | セキュリティ |
| 自動キーローテーション | CloudWatch Events と Lambda に基づいて、IAM ユーザーのアクセスキーとシークレットキーを自動的にローテーションします。 | IAM ユーザーのアクセスキーとシークレットキーを簡単にローテーションできます。 | セキュリティ |

| 名前 | 概要 | 利点 | カテゴリ |
| --- | --- | --- | --- |
| Amazon EBS ボリュームスナップショットのタグ付け | Amazon EC2 インスタンスのタグを使用して、すべての Amazon EBS ボリュームとスナップショットにタグを付けます。 | 意味のある関連ビジネス情報を使用してコストを分類して追跡できるため、どこで費用が費やされているかを簡単に検証し、タグ付けされたボリュームとスナップショットの自動化を使用できます。AWS コスト最適化の柱で強く推奨されるベストプラクティス。 | タグ付け (コスト最適化、セキュリティ、インシデント管理、自動化 ) |

# AMS Accelerate の自動インスタンス設定

AMS Accelerate は、自動インスタンス設定サービスを提供します。このサービスにより、AMS がインスタンスを適切に管理するための正しいログとメトリクスがインスタンスから出力されます。自動インスタンス設定には、このセクションで後述するオンボーディングのための独自の前提条件と手順があります。

トピック

- Accelerate での自動インスタンス設定の仕組み
- SSM エージェントの自動インストール
- インスタンス設定の自動変更

## Accelerate での自動インスタンス設定の仕組み

自動インスタンス設定により、AMS Accelerate は特定のエージェントとタグを追加して指定したインスタンスに対して、特定の設定を毎日実行できます。

## Accelerate の自動インスタンス設定の前提条件

AMS Accelerate がマネージドインスタンスで前述の自動アクションを実行できるようにするには、これらの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ている

AMS Accelerate 自動インスタンス設定では、 AWS Systems Manager SSM エージェントがインストールされている必要があります。

AMS SSM エージェントの自動インストール機能の使用については、「」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。

SSM エージェントを手動でインストールする方法については、以下を参照してください。

- Linux: Linux 用の Amazon 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 用の Amazon 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 エージェントは マネージド状態です

AMS Accelerate 自動インスタンス設定には、運用可能な SSM エージェントが必要です。SSM エージェントをインストールし、Amazon EC2 インスタンスが マネージド状態である必要があります。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。

## インスタンス設定の自動設定

前提条件が満たされていると仮定して、特定の Amazon EC2 インスタンスタグを追加すると、AMS Accelerate 自動インスタンス設定が自動的に開始されます。このタグを追加するには、次のいずれかの方法を使用します。

1. ( 強く推奨) AMS Accelerate Resource Tagger を使用する

   アカウントのタグ付けロジックを設定するには、「」を参照してくださいタグ付けの仕組み。タグ付けが完了すると、タグと自動インスタンス設定が自動的に処理されます。
2. タグを手動で追加する

   Amazon EC2 インスタンスに手動で次のタグを追加します。

Key:ams:rt:ams-managed、Value:true。

> **Note**
>
> インスタンス設定サービスは、ams:rt:ams マネージドタグがインスタンスに適用されると、必要な AMS 設定を適用しようとします。サービスは、インスタンスが起動されるたびに、および AMS の毎日の設定チェックが発生するときに、AMS に必要な設定をアサートします。

## SSM エージェントの自動インストール

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**
>
> - 6/03/2024 以降にアカウントが AMS Accelerate にオンボーディングされている場合、この機能はデフォルトで有効になっています。この機能をオフにするには、CA または CSDM にお問い合わせください。
> - 6/03/2024 より前にオンボーディングされたアカウントでこの機能を有効にするには、CA または CSDM にお問い合わせください。
> - 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。

### 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サービスコントロールポリシーが AWS Organizations レベルに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。

## インスタンス設定の自動変更

AMS Accelerate インスタンス設定の自動化は、アカウントで次の変更を行います。

1. IAM 許可

   AMS Accelerate によってインストールされたエージェントを使用するためのアクセス許可をインスタンスに付与するために必要な IAM 管理ポリシーを追加します。

2. エージェント

   a. 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。インスタンス設定の自動化により、CloudWatch エージェントがインストールされ、AMS Accelerate の最小バージョンが実行されます。

b. AWS Systems Manager 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 AMS Accelerate の最小バージョンを実行していることが保証されます。

3. CloudWatch 設定

a. 必要なメトリクスとログを確実に出力するために、AMS Accelerate は CloudWatch 設定をカスタマイズします。詳細については、次の「CloudWatch 設定変更の詳細」セクションを参照してください。

自動インスタンス設定は、IAM インスタンスプロファイルと CloudWatch 設定を変更または追加します。

## IAM アクセス許可の変更の詳細

各マネージドインスタンスには、次の管理ポリシーを含む AWS Identity and Access Management ロールが必要です。

- arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore
- arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy
- arn:aws:iam::aws:policy/AMSInstanceProfileBasePolicy

最初の 2 つは AWS管理ポリシーです。AMS 管理ポリシーは次のとおりです。

AMSInstanceProfileBasePolicy

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "secretsmanager:CreateSecret",
                "secretsmanager:UpdateSecret"
            ],
            "Resource": [
                "arn:aws:secretsmanager:*:*:secret:/ams/byoa/*"
            ],
            "Effect": "Allow"
```

```
        },
        {
            "Action": [
                "kms:Encrypt"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

インスタンスに既に IAM ロールがアタッチされているが、これらのポリシーのいずれかが欠落している場合、AMS は欠落しているポリシーを IAM ロールに追加します。インスタンスに IAM ロールがない場合、AMS は AMSOSConfigurationCustomerInstanceProfile IAM ロールをアタッチします。AMSOSConfigurationCustomerInstanceProfile IAM ロールには、AMS Accelerate に必要なすべてのポリシーがあります。

> **Note**
>
> デフォルトのインスタンスプロファイル制限である 10 に達すると、AMS は制限を 20 に引き上げて、必要なインスタンスプロファイルをアタッチできるようにします。

## CloudWatch 設定変更の詳細

CloudWatch 設定に関する追加の詳細。

- インスタンス上の CloudWatch 設定ファイルの場所：
  - Windows: %ProgramData%\Amazon\AmazonCloudWatchAgent\amazon-cloudwatch-agent.json
  - Linux: /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/ams-accelerate-config.json
- Amazon S3 の CloudWatch 設定ファイルの場所: Amazon S3
  - Windows: 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

- 収集されるメトリクス：
  - Windows:
    - AWS Systems Manager SSM エージェント (CPU_Usage)
    - CloudWatch エージェント (CPU_Usage)
    - すべてのディスクのディスク容量使用率 (% 空き容量 )
    - メモリ (使用中のコミットバイト数の割合 )
  - Linux:
    - AWS Systems Manager SSM エージェント (CPU_Usage)
    - CloudWatch エージェント (CPU_Usage)
    - CPU (cpu_usage_idle、cpu_usage_iowait、cpu_usage_user、cpu_usage_system)
    - ディスク (used_percent、inodes_used、inodes_total)
    - Diskio (io_time、write_bytes、read_bytes、writes、reads)
    - Mem (mem_used_percent)
    - スワップ (swap_used_percent)
- 収集される口グ：
  - 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 Accelerate からのオフボード

AMS Accelerate は、エンタープライズクラスの運用環境を簡単に運用する方法を提供します。また、AMS Accelerate は、 AWS 移行と使用のためのサポートインフラストラクチャオペレーションモデルを提供します。ただし、AMS Accelerate を使用した後、 AWS インフラストラクチャ運用の責任を他のチームにインソースまたは再割り当てすることを決定できます。これを行うには、AMS サービスからアカウントをオフボードする必要があります。

AMS Accelerate からアカウントをオフボードすると、AMS はサービスの説明で定義されているすべての責任をユーザーに返します。例えば、インシデントやサービスリクエストを AMS にカットすることはできません。同様に、オペレーションエンジニアとオートメーションは Accelerate アカウントにアクセスできなくなり、ヘルス、可用性、セキュリティ、コンプライアンスの検出結果を修復できなくなります。 AWS ワークロードは、AMS が運用していたのと同じアカウントで引き続き実行できます。

今後インフラストラクチャオペレーションサービスを実行するチームを含めて、Accelerate オフボーディング後に使用する人、ツール、プロセスを定義する必要があります。AMS はガードレールやログなどの AMS ツールの一部を残して、「運用環境とモデル」の開発を可能にします。次のドキュメントをよく読んで、引き続き使用できるツールと、アカウントのオフボードをリクエストする方法を理解してください。

# AMS Accelerate オフボーディング効果

Accelerate からオフボードする準備をする際は、以下の考慮事項に留意してください。

- アクセス: `ams-access-management` AWS Identity and Access Management ロールを定義する`ams-access-management` CloudFormation スタックは削除されません。オフボーディング後、これらのリソースは残りますが、残っている他のコンポーネントでは使用されません。スタックとロールは、必要に応じて削除できます。
- AMS リソースの保持: オフボーディング後、一部の AMS リソースはアカウントに残ります。保持されるリソースとその使用方法については、`resource_inventory.zip`スプレッドシート (圧縮) を参照してください。
- 自動化: オフボーディング後、AMS が厳選した AWS SSM 自動化ランブックと AWS Lambda 関数は使用できなくなります。
- バックアップ管理: AMS はバックアップ管理を使用してリソースのスナップショットを作成します。オフボーディング後は、AMS バックアッププラン AWS Backup を除き、 で定義されているバックアップスケジュール、頻度、保持期間を引き続き使用できます。「」を参照してくださいAMS バックアッププランを選択する。AMS Backup Orchestrator によって作成された AWS Identity and Access Management リソースは削除されますが、AMS が作成したバックアップボールトおよび対応する AWS KMS キーは削除されません。Accelerate 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。
- コスト最適化: オフボーディング後、AMS Resource Scheduler は削除されます。AMS Resource Scheduler は、使用されていないリソースを停止し、容量が必要なときにリソースを再開することで、運用コストを削減するのに役立ちます。AMS は、引き続きコスト最適化の推奨事項を提供しません。Resource Scheduler の詳細については、「AMS Resource Scheduler によるコスト最適化」を参照してください。
- 指定されたエキスパート: オフボーディング後、指定された Cloud Service Delivery Manager (CSDM) と Cloud Architect (CA) は、オフボーディングされた Accelerate アカウントの運用上およびセキュリティ上の優秀性に関するガイダンスを提供しなくなりました。
- インシデント管理: インシデント管理は、AMS サービスが報告されたインシデントに対応するために使用するプロセスです。オフボーディング後、Accelerate はインシデントを検出して対応したり、チームの問題解決を支援したりしなくなりました。Accelerate アカウントの Accelerate および Accelerate コンソールアクセスとインシデントおよびサービスリクエストの通信を交換できません。
- ログ記録とレポート: オフボーディング後、CloudWatch、CloudTrail、VPC フローログの結果として保存されたログを保持します。これらのサービスの設定をそのままにしておくと、ログの生成を

継続できますが、AMS はそのような設定をモニタリングしなくなります。Accelerate は、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なくなりました。セルフサービスレポート (SSR) から生成されたデータは保持しますが (「」を参照セルフサービスレポート )、Accelerate は新しいデータを生成しません。

- モニタリング: モニタリングは、AMS サービスがリソースを追跡するために使用するプロセスです。オフボーディング中、AMS は Alarm Manager や Resource Tagger などの AMS 固有のツール、および AMS が AMS モニタリングベースラインの一部としてデプロイした EventBridge イベントルールや CloudWatch アラームを削除します。Accelerate は、オフボーディング後にアラームに応答したり、新しいアラームを設定したりしなくなりました。Alarm Manager と Resource Tagger の詳細については、「Tag-based Alarm Manager and Resource Tagger」を参照してください。
- オペレーションツール: AMS Accelerate は、AWS のワークロードのインフラストラクチャに対して継続的なオペレーションを提供できます。Accelerate アカウントをオフボードすると、ルールに基づいてリソースにタグを付けるのに役立つ Resource Tagger などのツールや、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自動インスタンス設定にアクセスできなくなります。インスタンス上の 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。`AMSOSConfigurationCustomerInstanceRole` IAM プロファイルと `AMSInstanceProfileBasePolicy`はインスタンスからデタッチされ、Accelerate アカウントから削除されます。
- パッチ管理: パッチ管理は、AMS サービスが EC2 インスタンスを更新するために使用するプロセスです。オフボーディング後、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。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 Accelerate によってインストールされなくなります。
- 問題管理: オフボーディング後、Accelerate は問題を特定して調査し、根本原因を特定するための分析を実行しなくなりました。
- セキュリティ: セキュリティ管理は、AMS サービスがリソースを保護するために使用するプロセスです。オフボーディング後は、Amazon GuardDuty ディテクターと検出結果を保持し、 Accelerate によって AWS Config デプロイされた AWS Config ルールはすべて削除されます。Accelerate は、これらのツールの検出結果をモニタリング、修復、またはレポートしなくなりました。
- 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。

## Alarm Manager と Resource Tagger への依存関係による AMS Accelerate からのオフボーディング

Alarm Manager または Resource Tagger に関連する設定を、AMS 提供の Alarm Manager および Resource Tagger 設定スタックとともにデプロイ CloudFormation するカスタマイズされたスタックは、AWS Managed Services からオフボードするときにアカウントに残ります。

オフボーディングプロセス中に AMS 設定スタックを削除するには、オフボーディングプロセスを開始する前に、カスタム CloudFormation テンプレートから Alarm Manager または Resource Tagger の依存関係と参照を削除する必要があります。リファレンスを削除すると、AMS からオフボードするときにスタックがアカウントから適切に削除されるようになります。

> **Important**
>
> オフボーディングプロセスを開始する前に、CloudFormation テンプレートを慎重に確認し、Alarm Manager と Resource Tagger への参照をすべて削除します。そうしないと、AMS からオフボードした後でも、これらのスタックがアカウントに保持される可能性があります。これらのスタックには Alarm Manager と Resource Tagger に固有の設定情報が含まれていますが、その存在によって継続的な料金や料金が発生することはありません。

## Accelerate アカウントのオフボーディング支援を受ける

AMS は、AMS アカウントサービス終了リクエストを通じて少なくとも 30 日間の通知を受け取った後、アカウントをオフボードします。サービス終了日は、30 日間の必要な終了通知期間の終了日の翌月の最終日です。ただし、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。

アカウントのオフボーディングをリクエストするには、以下を行う必要があります。

1. サービスリクエストを使用してアカウントをオフボードするための正式なリクエストを送信します。オフボードするすべてのアカウントを文書化した 1 つのサービスリクエスト (SR)、またはアカウントごとに 1 つの SR。

リクエストで、オフボードするアカウント IDs のリスト、オフボードの理由、その他の考慮事項を指定します。

2. オフボーディングするアカウントを CSDM に通知し、オフボーディングプロセスの実行支援をリクエストします。

## Accelerate の通知設定

ユーザーと AMS 間の通信は、さまざまな理由で発生します。

- アラートをモニタリングして作成されたイベント
- Patch アドオンにオプトインしている場合のサービス通知のパッチ適用
- サービスリクエストとインシデントレポート
- ときどき重要な AWS お知らせ (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 )

すべての通知は、オンボーディング時にパッチ通知用に指定した E メールを使用して送信されます。それ以外の場合、オンボーディング時に AMS に提供したデフォルトの E メールに通知が送信されます。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。

GuardDuty または AWS Config に基づくアラートなど、リソースベース以外の通知には、名前付き連絡先リストを使用できます。たとえば、 という名前のリスト`SecurityContacts`と、 という名前のリストがあるとします`OperationsContacts`。AMS は、これらのリストにアラームと通知を送信します。

詳細については、「AWS Config コントロールコンプライアンスレポート」を参照してください。

# AMS Accelerate でのタグ付け

ほとんどの Accelerate 機能 (パッチ適用、バックアップ、モニタリング) では、タグと設定プロファイルを使用して、管理するリソース、適用するアクション、適用するタイミングを決定します。タグは、 リソースに適用するラベルです。設定プロファイルには、これらのタグに基づくルールが含まれています。

Accelerate の各機能には、独自のタグ付け要件があります。一部の機能では特定のタグを使用する必要がありますが、他の機能では任意のタグを使用できます。

必要なタグの詳細については、「」を参照してくださいAccelerate のカスタマーマネージドタグ。

顧客を定義できるタグの詳細については、「」を参照してください。 Accelerate のお客様が用意したタグ

目次


- AMS Accelerate のタグ
  - タグとは
  - タグ付けの仕組み
  - Accelerate のカスタマーマネージドタグ
    - Accelerate でのモニタリング
    - Accelerate での EC2 インスタンスのタグの設定
    - Accelerate でのバックアップのタグの管理
  - 高速マネージドタグ
  - Accelerate のお客様が用意したタグ
- Accelerate のタグ管理ツール
  - リソースタガーの高速化
    - Resource Tagger とは
    - Resource Tagger の仕組み
    - AMS Accelerate のリソースタグ付け設定プロファイル
      - 構文と構造
    - AMS Accelerate のリソースタグ付けのユースケース
      - Resource Tagger によって適用されるタグの表示
      - Resource Tagger を使用したタグの作成

        - Resource Tagger によるリソースの変更の防止
        - 設定プロファイルの例
        - デフォルト設定のマージ
        - デフォルト設定の無効化
        - Resource Tagger によって適用されるタグの削除
        - Resource Tagger 設定の表示または変更
        - 設定変更のデプロイ
        - Resource Tagger タグを無視するように Terraform を設定する
        - Resource Tagger によって管理されるリソースの数の表示
- CloudFormation を使用して AMS Accelerate のタグを作成する
    - CloudFormation AMS Accelerate のユースケース
        - for Accelerate を使用した EC2 インスタンス CloudFormation のタグ付け
        - CloudFormation for Accelerate を使用した AutoScaling Group (ASG) のタグ付け
        - CloudFormation for Accelerate を使用して設定プロファイルをデプロイする
- Terraform を使用して AMS Accelerate のタグを作成する


# AMS Accelerate のタグ

目次


- タグとは
- タグ付けの仕組み
- Accelerate のカスタマーマネージドタグ
    - Accelerate でのモニタリング
    - Accelerate での EC2 インスタンスのタグの設定
    - Accelerate でのバックアップのタグの管理
- 高速マネージドタグ
- Accelerate のお客様が用意したタグ

# タグとは

タグは、 AWS リソースに割り当てるラベルです。タグはそれぞれ、1 つのキーとオプションの 1 つの値で構成されており、どちらもお客様側が定義します。

タグを使用して、目的、所有者、環境など、さまざまな方法で AWS リソースを分類します。たとえば、アカウントの Amazon EC2 インスタンスの一連のタグを定義して、各インスタンスの所有者とスタックレベルを追跡できます。

タグにはAmazon EC2 に関連する意味はなく、完全に文字列として解釈されます。

詳細については、「 AWS リソースのタグ付け」を参照してください。

# タグ付けの仕組み

リソースにタグを適用する方法は複数あります。リソースの作成時に、各 AWS サービスのコンソールでリソースに直接タグ付けしたり、 AWS タグエディタを使用して複数のリソースのタグを追加、削除、編集したり、リソースタグなどの CloudFormation プロビジョニングツールを使用したりできます。AMS Accelerate には、自動タグライフサイクルマネージャーのルールの定義に使用する AMS Accelerate Resource Tagger も用意されています。AMS Accelerate で Resource Tagger を使用する方法については、「」を参照してくださいリソースタガーの高速化。AMS Accelerate には、AMS リソースにカスタムタグを追加および削除するお客様が用意したタグも用意されています。お客様が用意したタグの詳細については、「」を参照してくださいAccelerate のお客様が用意したタグ。

# Accelerate のカスタマーマネージドタグ

さまざまな AMS Accelerate アクションをトリガーするには、特定のタグが必要です。

目次


- Accelerate でのモニタリング
- Accelerate での EC2 インスタンスのタグの設定
- Accelerate でのバックアップのタグの管理


## Accelerate でのモニタリング

AMS Accelerate は、サポートされているリソースの状態、可用性、信頼性をモニタリングします。このサービスの詳細については、「」を参照してくださいAMS Accelerate でのモニタリングとイベント管理。

AMS Accelerate は、ベースラインモニタリングに追加 AWS のサービス の を定期的にオンボードします。Resource Tagger のデフォルト設定を使用すると、これらの更新は自動的にアカウントにデプロイされ、変更はサポートされているリソースに反映されます。

Amazon EC2 インスタンスを AMS Accelerate で管理するようにオプトインするには、AppConfig のカスタマイズプロファイルを介して次のタグを適用する必要があります。詳細については、「ステップ 3: 設定と設定プロファイルの作成」を参照してください。

リソースに次のタグを適用します。

| キー | 値 |
| --- | --- |
| ams:rt:ams-managed | true |

たとえば、次のようなカスタマイズされた設定ドキュメントを作成して、AMS がサポートするすべての EC2 リソースにタグを適用できます。

```
{
    "AWS::EC2::Instance": {
        "AllEC2": {
            "Enabled": true,
            "Filter": {
                "Platform": "*"
            },
            "Tags": [
                {
                    "Key": "ams:rt:ams-managed",
                    "Value": "true"
                }
            ]
        }
    }
}
```

**Important**

設定の変更を行った後は、必ずデプロイしてください。SSM AppConfig では、作成後に設定の新しいバージョンをデプロイする必要があります。

Amazon EC2 以外のサービスには、デフォルトのベースラインモニタリングがあります。AMS Accelerate によってモニタリングされるリソースをオプトアウトするには、カスタマイズ設定プロファイルを使用して特定のリソースまたは を除外できます AWS のサービス。これにより、ベースラインアラーム定義をデプロイするためにモニタリングタグを持つリソースを制御できます。「AMS Accelerate のリソースタグ付けのユースケース」を参照してください。

リソースタグ付けの使用

アカウントの AMS Accelerate Resource Tagger 設定を使用すると、この 1 つのタグ (ams:rt:ams-managed) を適用すると、次のタグが自動的にデプロイされます。

ベースラインモニタリングのために、サポートされているリソースに次のタグが適用されます。

| キー | 値 | ルール |
| --- | --- | --- |
| ams:rt:ams-monitoring-policy | ams-monitored | AMS でサポートされているすべての EC2 リソースに適用されます |
| ams:rt:ams-monitoring-policy-platform | ams-monitored-linux | Linux OS を実行しているすべての Amazon EC2 インスタンスに適用されます |
| ams:rt:ams-monitoring-policy-platform | ams-monitored-windows | Windows OS を実行しているすべての Amazon EC2 インスタンスに適用されます |

サポートされている他のサービスの場合

指定されたルールに従って、次のタグをリソースに適用します。

| キー | 値 | ルール |
| --- | --- | --- |
| ams:rt:ams-monitoring-policy | ams-monitored | AMS Accelerate モニタリングでサポートされているすべてのリソースに適用されます。 |
| ams:rt:ams-monitoring-with-kms | ams-monitored-with-kms | KMS を使用した OpenSearch ドメイン |

| キー | 値 | ルール |
| --- | --- | --- |
| ams:rt:ams-monitoring-with-master | ams-monitored-with-master | 専用マスターノードを使用した OpenSearch ドメイン |

Resource Tagger を使用していない場合

AMS Resource Tagger を使用する以外の方法を使用して正しいモニタリングタグを適用する方法については、Resource Tagger を使用せずにタグを高速化する「」を参照してください。

## Accelerate での EC2 インスタンスのタグの設定

AMS Accelerate は、SSM エージェントや CloudWatch エージェントなど、Amazon EC2 インスタンス上のエージェントを管理します。このサービスの詳細については、「」を参照してください。AMS Accelerate の自動インスタンス設定

Amazon EC2 インスタンスを AMS Accelerate で管理するようにオプトインするには、Amazon EC2 インスタンスに次のタグを適用する必要があります。

| キー | 値 |
| --- | --- |
| ams:rt:ams-managed | true |

## Accelerate でのバックアップのタグの管理

AMS Accelerate は、サポートされているリソースのバックアップを管理します。このサービスの詳細については、「」を参照してくださいAMS Accelerate での継続的な管理。

AMS Accelerate バックアップ管理では、タグを使用して、自動的にバックアップするリソースを特定します (また、手動バックアップ機能も提供します ) 。任意のタグ key:value の組み合わせを使用して、リソースをバックアッププランに関連付けることができます。ams-default-backup-plan AWS Backup プランを使用して自動バックアップにオプトインするには、サポートされているリソースに次のタグを適用する必要があります。

| キー | 値 |
| --- | --- |
| ams:rt:backup-orchestrator | true |

> **Note**
>
> オンボーディング中、AMS Accelerate はすべてのリソースに ams:rt:backup-orchestrator-onboarding を短い間隔、短い保持スナップショットの値 true でタグ付けします。これは、ams-onboarding-backup-plan バックアッププランによって管理されます。AMS Accelerate マネージド AWS Backup プランの詳細については、「」を参照してくださいAMS バックアッププランを選択する。

## 高速マネージドタグ

AMS Accelerate へのオンボーディング中に、複数の AWS リソースがアカウントにデプロイされます。そのため、これらのリソースには次のタグが付けられます。

| キー | 値 |
| --- | --- |
| ams:resourceOwner | AMS |
| ams:resourceOwnerService | このリソースを提供する AMS Accelerate サービスの説明。例えば、AMS デプロイ、バックアップ、コントロール、モニタリング、パッチなどです。 |
| AppId | AMSInfrastructure |
| AppName | |
| 環境 | |

> **Note**
>
> これらのタグは CloudFormation スタックレベルのタグを使用して適用され、作成されたリソースへのタグの CloudFormation 伝達に依存します。詳細については、「リソースタグ」を参照してください。

# Accelerate のお客様が用意したタグ

お客様が用意したタグとは

お客様が提供するタグは、アカウントでの AMS リソースのタグ付け方法を管理するルールを指定するために使用される AMS Accelerate サービス機能です。お客様が用意したタグを使用すると、アカウントにデプロイされた AMS リソースにユーザー定義のカスタムタグを追加できます。お客様が用意したタグ機能は、自動サービスを使用して Cloud Service Delivery Manager (CSDM) にリクエストすると、リクエストされたアカウントに自動的に追加されます。AMS タグを上書きすることはできません。AMS タグは「ams:」で始まります。

独自のタグ (ラベル) を定義し、すべての AMS Accelerate リソースに対してこれらのタグの機能を指定できます。AMS にオンボードする前にこれらのタグを指定して、オンボーディングプロセス中に AMS タグとカスタムタグを適用できます。または、オンボーディング後にタグを指定することもできます。

お客様が用意したタグを追加するにはどうすればよいですか？

リソースへのこれらのタグの追加をリクエストするには、CSDM にお問い合わせください。これらのタグは、アカウントの AMS リソースに適用されます。

タグの範囲を教えてください。

この機能は現在、Accelerate のお客様および AWS 商用リージョンでのみ使用できます。所有しているすべてのアカウントまたは特定のアカウントリストにタグを追加できます。

> **Note**
>
> これらのタグは AMS リソースにのみ適用され、独自のリソースには影響しません。

# Accelerate のタグ管理ツール

目次


- リソースタガーの高速化
- CloudFormation を使用して AMS Accelerate のタグを作成する
- Terraform を使用して AMS Accelerate のタグを作成する

# リソースタガーの高速化

Resource Tagger を使用すると、アカウントでの AWS リソースのタグ付け方法を管理するルールを指定できます。アカウントのオンボーディング中、AMS Accelerate はタグ付けポリシーをデプロイして、マネージドアカウント内のリソースにタグが付けられていることを確認します。

目次


- Resource Tagger とは
- Resource Tagger の仕組み
- AMS Accelerate のリソースタグ付け設定プロファイル
  - 構文と構造
- AMS Accelerate のリソースタグ付けのユースケース
  - Resource Tagger によって適用されるタグの表示
  - Resource Tagger を使用したタグの作成
  - Resource Tagger によるリソースの変更の防止
  - 設定プロファイルの例
  - デフォルト設定のマージ
  - デフォルト設定の無効化
  - Resource Tagger によって適用されるタグの削除
  - Resource Tagger 設定の表示または変更
  - 設定変更のデプロイ
  - Resource Tagger タグを無視するように Terraform を設定する
  - Resource Tagger によって管理されるリソースの数の表示


## Resource Tagger とは

Resource Tagger は、アカウントでの AWS リソースのタグ付け方法を管理するルールを指定するために使用する AMS Accelerate サービスです。これは、タグがリソースにどのように適用されるかを完全に可視化する AWS ことを目的としています。

Resource Tagger は、設定プロファイルで指定したタグ付けルールに基づいて、サポートされている AWS リソースのタグを自動的に作成、更新、削除します。例えば、Amazon EC2 インスタンスのコレクションにタグを適用するルールを指定して、AMS Accelerate で管理する必要があることを示すと、インスタンスがモニタリングまたはバックアップされます。このようなタグを使用して、 AWS

AppConfig 設定プロファイルで定義されたポリシーに基づいてリソース AWS のコンプライアンスステータスを識別できます。詳細については、「AWS AppConfig」を参照してください。

AMS Accelerate にはデフォルトのマネージドタグ付け設定が用意されているため、AMS Accelerate でリソースをモニタリングできます。AMS Accelerate で管理する必要があるリソースを定義し、マネージドタグ付けルールにより、適切なタグを持つリソースが AMS Accelerate によってモニタリングされるようにします。

Resource Tagger を選択すると、デフォルトの AMS Accelerate マネージドタグを上書きまたは非アクティブ化したり、ポリシーを満たす独自のタグ付けルールを指定したり、Terraform などの他のメカニズムを使用してドリフトを回避したりできます。オペレーションに基づいて、スケーリングする例外を定義できます。たとえば、サポートされているプラットフォーム (Windows や Linux など) を持つすべての Amazon EC2 インスタンスにタグを適用し、特定のインスタンス IDs のタグ付けから除外するポリシーを定義できます。

> **Important**
>
> Resource Tagger は、ams:rt: プレフィックスを持つアカウント内のすべてのタグを制御します。このプレフィックスで始まるタグは、Resource Tagger の設定ルールに存在しない限り削除されます。要約すると、ams:rt: で始まるサポートされているリソースのタグは、Resource Tagger によって所有されていると見なされます。ams:rt: などで手動でタグ付けすると、いずれかの Resource Tagger 設定プロファイルで指定されていない場合、そのタグは自動的に削除されます。

## Resource Tagger の仕組み

アカウントが AMS Accelerate にオンボーディングされると、2 つの JSON 設定ドキュメントが のアカウントにデプロイされます AWS AppConfig。設定プロファイルと呼ばれる 2 つのドキュメントは、デフォルトの設定プロファイルと呼ばれる AMSManagedTags と、カスタマイズ設定プロファイルと呼ばれる CustomerManagedTags です。カスタマイズ設定プロファイルを使用して、アカウントの独自のポリシーとルールを定義します。これらは AMS Accelerate によって上書きされません。

どちらのプロファイルも AMSResourceTagger アプリケーションと AMSInfrastructure 環境にあります。リソースタガーによって適用されるすべてのタグには、キープレフィックス ams:rt: があります。

カスタマイズ設定プロファイル：

カスタマイズ設定プロファイルは、アカウントのオンボーディング時に最初は空です。ただし、プロファイルドキュメントに配置されたルールは、デフォルトの設定プロファイルのルールに加えて適用されます。カスタマイズ設定プロファイルの設定はすべてお客様によって完全に管理され、リクエストによって以外は AMS Accelerate によって上書きされません。

サポートされている AWS リソースのカスタム設定プロファイルに必要なカスタムタグ付けルールを指定できます。また、ここで AMS Accelerate が管理するデフォルト設定の変更を指定することもできます。「」を参照してくださいAMS Accelerate のリソースタグ付けのユースケース。

> **Important**
>
> このプロファイルを更新すると、Resource Tagger は 内のすべての関連リソースで変更を自動的に適用します AWS アカウント。変更は自動的に有効になりますが、有効になるまでに最大 60 分かかる場合があります。

このプロファイルを更新するには、 を使用するか AWS マネジメントコンソール、 AWS CLI/SDK ツールを使用します。カスタマイズ設定プロファイルの更新については、 AWS AppConfig ユーザーガイド「What Is?」を参照してください AWS AppConfig。

デフォルトの設定プロファイル：

デフォルトの設定プロファイルドキュメントは AMS Accelerate の内部にあり、AMS Accelerate が提供するデフォルトのルールが含まれており、完全に変更または削除することはできません。このプロファイルは、AMS Accelerate によっていつでも更新でき、レビューのために利用できるようになります。このプロファイルに加えた変更は、自動的に削除されます。カスタマイズ設定プロファイルを使用するデフォルト設定ルールを変更または無効にする場合は、「」を参照してくださいAMS Accelerate のリソースタグ付けのユースケース。

## AMS Accelerate のリソースタグ付け設定プロファイル

設定プロファイルは、リソースの存続期間中、タグをリソースに均一に適用するのに役立ちます。

### 構文と構造

設定プロファイルは、次の構造を持つ JSON オブジェクトです。

```
{
   "Options": {
```

```
      "ReadOnly": false
   },
   "ResourceType": {
      "ConfigurationID": {
      "Enabled": true,
      "Filter": { ... },
      "Tags": [  ...  ]
      },
      "ConfigurationID": {
      ...
      }
   },
   "ResourceType": {
     ...
   }
}
```

オプション: (オプション) ResourceTagger の動作方法のオプションを指定します。ブロックを省略することは、すべてのオプションをデフォルト値に設定するのと同じです。使用可能なオプション設定については、以下を参照してください。

- ReadOnly: (オプション、デフォルトは false): Resource Tagger の ReadOnly モードを指定します。ReadOnly を true に設定して、AWS リソースでタグを作成または削除する Resource Tagger を無効にします。詳細については、「Resource Tagger によるリソースの変更の防止」を参照してください。

ResourceType: このキーは、次のサポートされている文字列のいずれかでなければならず、指定されたリソースタイプに関連するすべての設定を表します。

- AWS::AutoScaling::AutoScalingGroup
- AWS::DynamoDB::Table
- AWS::EC2::Instance
- AWS::EC2::NatGateway
- AWS::EC2::VPNConnection
- AWS::EFS::FileSystem
- AWS::EKS::Cluster
- AWS::ElasticLoadBalancing::LoadBalancer
- AWS::ElasticLoadBalancingV2::LoadBalancer

- AWS::Elasticsearch::Domain
- AWS::FSx::FileSystem
- AWS::OpenSearch::Domain
- AWS::RDS::DBCluster
- AWS::RDS::DBInstance
- AWS::Redshift::Cluster
- AWS::S3::Bucket
- AWS::Synthetics::Canary

ConfigurationID: このキーはプロファイルドキュメント内で一意である必要があり、次の設定ブロックに一意に名前を付けます。同じ ResourceType ブロック内の 2 つの設定ブロックが同じ ConfigurationID を持つ場合、プロファイルに最後に表示される設定ブロックが有効になります。カスタマイズプロファイルで、デフォルトドキュメントで指定されたものと同じ ConfigurationID を指定すると、カスタマイズプロファイルで定義された設定ブロックが有効になります。

> **Important**
>
> ConfigurationID は AMS Accelerate プロファイルと重複########。たとえば、AMSMonitoringLinux または AMSMonitoringWindows にすることはできません。そうしないと、AMSManagedTags 設定プロファイルの各設定が無効になります。

有効 (オプション、デフォルトは true): 設定ブロックを有効にするかどうかを指定します。設定ブロックを無効にするには、これを false に設定します。無効になっている設定ブロックは効果がありません。

フィルタ: 設定が適用されるリソースを指定します。各フィルターオブジェクトには、次のフィールドのいずれか 1 つ (1 つだけ) を含めることができます。

- AWS::AutoScaling::AutoScalingGroup：
  - AutoScalingGroupName: Autoscaling グループ名。このフィールドはワイルドカードマッチングをサポートします。
- AWS::DynamoDB::Table：
  - TableName: DynamoDB テーブルの名前。このフィールドはワイルドカードマッチングをサポートします。

- AWS::EC2::Instance：
  - AvailabilityZone: フィルターは、指定されたアベイラビリティーゾーンの EC2 インスタンスに一致します。このフィールドはワイルドカードマッチングをサポートしているため、*a は us-east-1a、ap-northeast-1a などと一致します。
  - InstanceId: フィルターは、指定されたインスタンス ID を持つ EC2 インスタンスに一致します。このフィールドはワイルドカードマッチングをサポートしているため、i-00000* は i-00000 で始まるインスタンス ID を持つすべてのインスタンスと一致します。
  - プラットフォーム: フィルターは、EC2 インスタンスと指定されたプラットフォームに一致します。有効な値は、Windows、Linux、またはワイルドカード * (任意のプラットフォームに一致) です。
- AWS::EC2::NatGateway：
  - NatGatewayId: NAT ゲートウェイの ID。このフィールドはワイルドカードマッチングをサポートします。
  - 状態: NAT ゲートウェイの状態 (保留中 | 失敗 | 使用可能 | 削除 | 削除またはワイルドカード「*」 )
  - VpcId: NAT ゲートウェイが存在する VPC の ID。このフィールドはワイルドカードマッチングをサポートします。
  - SubnetId: NAT ゲートウェイが存在するサブネットの ID。このフィールドはワイルドカードマッチングをサポートします
- AWS::EC2::VPNConnection：
  - VpnConnectionId: 接続の ID。このフィールドはワイルドカードマッチングをサポートします。
- AWS::EFS::FileSystem：
  - FileSystemId: EFS ファイルシステムの ID。このフィールドはワイルドカードマッチングをサポートします。
- AWS::EKS::Cluster：
  - ClusterName: クラスターの名前。このフィールドはワイルドカードマッチングをサポートします。
- AWS::ElasticLoadBalancing::LoadBalancer (Classic Load Balancer)：
  - LoadBalancerName: LoadBalancer 名。このフィールドはワイルドカードマッチングをサポートします。
  - スキーム:「インターネット向け」、「内部」、またはワイルドカード「*」のいずれかです。
  - VPCId: ロードバランサーがデプロイされる VPCId は、ワイルドカード「*」にすることができます。

- AWS::ElasticLoadBalancingV2::LoadBalancer (Application Load Balancer (ALB)) :
  - LoadBalancerArn: LoadBalancer Amazon リソースネーム (ARN)。
  - DNSName: LoadBalancer の DNSName。このフィールドはワイルドカードマッチングをサポートします。
  - LoadBalancerName: LoadBalancer 名。このフィールドはワイルドカードマッチングをサポートします。
- AWS::Elasticsearch::Domain :
  - DomainId: ElasticSearch リソースの DomainId。このフィールドはワイルドカードマッチングをサポートします。
  - DomainName: ElasticSearch リソースの DomainName。このフィールドはワイルドカードマッチングをサポートします。
  - HasMasterNode: true または false のブール値。ドメインに専用マスターノードがある場合に一致。
  - HasKmsKey ブール値は true または false です。ドメインに保管時の暗号化用の KMS キーがある場合に一致。
- AWS::FSx::FileSystem :
  - FileSystemId: FSx ファイルシステムの ID。このフィールドはワイルドカードマッチングをサポートします。
- AWS::OpenSearch::Domain :
  - DomainId: OpenSearch リソースの DomainId。このフィールドはワイルドカードマッチングをサポートします。
  - DomainName: OpenSearch リソースの DomainName。このフィールドはワイルドカードマッチングをサポートします。
  - HasMasterNode: ブール値。ドメインに専用マスターノードがある場合、これは true に設定できます。
  - HasKmsKey: ドメインに保管時の暗号化用の KMS キーがある場合、これは true に設定できます。
- AWS::RDS::DBCluster :
  - DBClusterIdentifier: フィルターは、RDS クラスター識別子と指定された識別子に一致します。このフィールドはワイルドカードマッチングをサポートしていないため、クラスター識別子を指定する必要があります。
  - エンジン: RDS インスタンスで使用されているエンジン。このフィールドはワイルドカードマッチングをサポートします。

  - EngineVersion: エンジンのバージョン。このフィールドはワイルドカードマッチングをサポートします。
- AWS::RDS::DBInstance：
  - DBInstanceIdentifier: フィルターは、指定されたインスタンス ID を持つ RDS インスタンスに一致します。このフィールドはワイルドカードマッチングをサポートしていないため、インスタンス識別子を指定する必要があります。
  - エンジン: RDS インスタンスで使用されているエンジン。このフィールドはワイルドカードマッチングをサポートします。
  - EngineVersion: エンジンのバージョン。このフィールドはワイルドカードマッチングをサポートします。
- AWS::Redshift::Cluster：
  - ClusterIdentifier: クラスター識別子。このフィールドはワイルドカードマッチングをサポートします。
- AWS::S3::Bucket：
  - BucketName: S3 バケットの名前。このフィールドはワイルドカードマッチングをサポートします。
- AWS::Synthetics::Canary：
  - CanaryName: Synthetics Canary の名前。

その他のフィルタープロパティ：

- タグ: フィルターは、指定されたタグが既に適用されているすべてのリソースに適用されます。このプロパティの値は、次のフィールドを持つ JSON オブジェクトである必要があります。
  - キー: 正確な文字列でなければならず、リソースにその正確なキーを持つタグが必要であることを指定します。
  - 値: タグに一致する値を指定します。ワイルドカードをサポートしているため、Sample の値は、Sample という文字列で終わる任意の値と一致します。
- Fn::AND: JSON オブジェクトの JSON 配列。各オブジェクトは、フィルター設定ブロックと同じルールに従います。これは、フィルターがすべてのサブフィルターに一致するすべてのリソースと一致することを指定します。
- Fn::OR: JSON オブジェクトの JSON 配列。各オブジェクトは、フィルター設定ブロックと同じルールに従います。これは、フィルターがいずれかのサブフィルターに一致するリソースと一致することを指定します。

- Fn::NOT: Filter 設定ブロックと同じルールに従う JSON オブジェクト。これは、フィルターがサブフィルターに一致するリソースと明示的に一致しないことを指定します。これを使用して、タグ付けルールの除外を指定します。

タグ: 一致するリソースに適用されるタグ。（「タグの命名規則と使用規則」を参照してください）。このフィールドは、キーと値のペアの配列です。

- キー: 適用するタグのキー。
- 値: 適用するタグの値。

> **Note**
>
> Resource Tagger によって適用されるタグには、常に ams:rt: で始まるキーがあります。プロファイルでこのプレフィックスを指定しない場合、Resource Tagger によって挿入されます。これは、Resource Tagger が所有および管理するタグを、他の目的で他のツールが使用するタグと区別する方法です。

## AMS Accelerate のリソースタグ付けのユースケース

このセクションでは、Resource Tagger で一般的に実行されるアクションを一覧表示します。

Resource Tagger によって適用されるタグの表示

Resource Tagger によって適用されるすべてのタグには、キープレフィックス ams:rt: があります。たとえば、次のタグ定義は、key ams:rt:sampleKey と value sampleValue を持つタグになります。このプレフィックスを持つすべてのタグは、Resource Tagger の一部として扱われます。

```
{
 "Key": "sampleKey",
 "Value": "sampleValue"
}
```

> **Important**
>
> ams:rt: プレフィックスを使用して独自のタグを手動で作成した場合、Resource Tagger によって管理されていると見なされます。つまり、リソースが Resource Tagger によって管理されているが、設定プロファイルでタグを適用する必要があることが示されていない場

合、Resource Tagger は手動で追加されたタグを削除します。Resource Tagger によって管理されるリソースに手動でタグ付けする場合は、タグキーに ams:rt: プレフィックスを使用しないでください。

### Resource Tagger を使用したタグの作成

AMS Accelerate Resource Tagger は、AMS Accelerate オンボーディング中にアカウントにデプロイされるコンポーネントです。Resource Tagger には、リソースのタグ付け方法を定義する設定可能なルールのセットがあり、それらのルールを適用し、リソースにタグを自動的に追加および削除して、ルールに準拠できるようにします。

Resource Tagger を使用してリソースにタグを付ける場合は、「」を参照してくださいリソースタガーの高速化。

以下は、すべての Amazon EC2 インスタンスに true の値を持つタグ ams:rt:ams-managed を追加する Resource Tagger 設定スニペットの例です。ams:rt:ams マネージドタグは、AMS Accelerate によるリソースのモニタリングをオプトインします。

```
{
    "AWS::EC2::Instance": {
        "SampleConfigurationBlock": {
            "Enabled": true,
            "Filter": {
                "Platform": "*"
            },
            "Tags": [
                {
                    "Key": "ams:rt:ams-managed",
                    "Value": "true"
                }
            ]
        }
    }
}
```

**Warning**

AMS 管理の設定を誤って同じ名前で上書きする可能性があるため、新しい設定の名前 (SampleConfigurationBlock の例では ) を指定するときは注意してください。

### Resource Tagger によるリソースの変更の防止

Resource Tagger は、リソースにタグを追加または削除できない読み取り専用モードに設定できます。これは、独自のタグ付けメカニズムを提供する場合に便利です。

読み取り専用モードの場合、Resource Tagger は引き続きマネージド設定プロファイルと顧客設定プロファイルで指定されているタグ付けルールを調べ、これらのタグ付けルールを満たさないリソースをスキャンします。非準拠のリソースは で表示されます AWS Config。検索 AWS Config ルール できる には `AMSResourceTagger-`プレフィックスがあります。たとえば、`AMSResourceTagger-EC2Instance` AWS Config ルールは、設定プロファイルに基づいて`AWS::EC2::Instance`リソースに適切なタグが作成されているかどうかを評価します。

Resource Tagger はこの時点で停止し、リソースに変更を加えません (タグを追加または削除しません ) 。

読み取り専用モードを有効にするには、オプションブロックに ReadOnly キーを含めるように顧客設定プロファイルを変更します。たとえば、次の設定プロファイルスニペットは、これがどのように表示されるかを示しています。

```
{
    "Options": {
        "ReadOnly": true
    },
    "AWS::EC2::Instance": {
        [... the rest of your configuration ...]
    }
}
```

Resource Tagger は、デプロイが完了するとすぐにこの新しい設定に反応し、リソースへのタグの追加と削除を停止します。

> **Note**
>
> タグの変更を再度有効にするには、デフォルト値が false であるため、ReadOnly 値を false に変更するか、キーを完全に削除します。

オプション設定の詳細については、次の構文と構造「」を参照してください。

### 設定プロファイルの例

次のプロファイルドキュメントの例では、スタック* CloudFormation スタックの一部であるすべての Windows EC2 インスタンスを AMS Accelerate で管理するように指定していますが、 は ID i-00000000000000001 の特定の EC2 インスタンスを明示的に除外します。

```
{
    "AWS::EC2::Instance": {
        "AMSMonitoringWindows": {
            "Enabled": true,
            "Filter": {
                "Fn::AND": [
                    {
                        "Platform": "Windows"
                    },
                    {
                        "Tag": {
                            "Key": "aws:cloudformation:stack-name",
                            "Value": "stack-*"
                        }
                    },
                    {
                        "Fn::NOT": {
                            "InstanceId": "i-00000000000000001"
                        }
                    }
                ]
            },
            "Tags": [
                {
                    "Key": "ams:rt:ams-managed",
                    "Value": "true"
                }
            ]
        }
    }
}
```

> **Warning**
>
> AMS 管理の設定を誤って同じ名前で上書きする可能性があるため、新しい設定の名前 (SampleConfigurationBlock の例では ) を指定するときは注意してください。

### デフォルト設定のマージ

デフォルトの設定プロファイルは、アカウントのオンボーディング時に AMS Accelerate によって提供されます。このプロファイルは、アカウントにデプロイされるデフォルトのルールを提供します。

デフォルトの設定プロファイルを変更することはできませんが、カスタマイズ設定プロファイルでデフォルトの設定ブロックと同じ ConfigurationID で設定ブロックを指定することで、デフォルトを上書きできます。これを行うと、設定ブロックはデフォルトの設定ブロックを上書きします。

たとえば、次のデフォルト設定ドキュメントを考えてみましょう。

```
{
 "AWS::EC2::Instance": {
  "AMSManagedBlock1": {
   "Enabled": true,
   "Filter": {
    "Platform": "Windows"
   },
   "Tags": [{
    "Key": "my-tag",
    "Value": "SampleValueA"
   }]
  }
 }
}
```

ここで適用されるタグ値を から SampleValueA に変更しSampleValueB、Windows インスタンスだけでなくすべてのインスタンスにタグを適用するには、次のカスタマイズ設定プロファイルを指定します。

```
{
 "AWS::EC2::Instance": {
  "AMSManagedBlock1": {
   "Enabled": true,
   "Filter": {
    "Platform": "*"
   },
   "Tags": [{
    "Key": "my-tag",
    "Value": "SampleValueB"
   }]
  }
```

```
 }
}
```

> **Important**
>
> 設定の変更後は、必ずデプロイしてください。詳細については、「設定変更のデプロイ」を参照してください。SSM AppConfig では、作成後に設定の新しいバージョンをデプロイする必要があります。

デフォルト設定の無効化

デフォルトの設定ルールを無効にするには、カスタマイズ設定プロファイルに同じ ConfigurationID の設定ブロックを追加し、値に false の Enabled フィールドを指定します。

たとえば、デフォルトの設定プロファイルに次の設定がある場合です。

```
{
 "AWS::EC2::Instance": {
  "AMSManagedBlock1": {
   "Enabled": true,
   "Filter": {
    "Platform": "Windows"
   },
   "Tags": [{
    "Key": "my-tag",
    "Value": "SampleValueA"
   }]
  }
 }
}
```

このタグ付けルールを無効にするには、カスタマイズ設定プロファイルに以下を含めます。

```
{
 "AWS::EC2::Instance": {
  "AMSManagedBlock1": {
   "Enabled": false
  }
 }
}
```

> **Important**
>
> 設定の変更は、必ずデプロイしてください。詳細については、「」を参照してください設定変更のデプロイ。SSM AppConfig では、作成後に設定の新しいバージョンをデプロイする必要があります。

Resource Tagger によって適用されるタグの削除

ams:rt というプレフィックスが付いたタグは、タグが設定プロファイルに存在しない場合、または存在する場合はフィルターが一致しない場合、Resource Tagger によって削除されます。つまり、次のいずれかを実行して、Resource Tagger によって適用されるタグを削除できます。

- タグを定義するカスタマイズ設定セクションを変更します。
- 特定のリソースの例外を追加して、フィルターと一致しないようにします。

例: Linux インスタンスに次のタグがある場合：

```
"Tags": [{
    "Key": "ams:rt:MyOwnTag",
    "Value": true
},{
    "Key": "myTag",
    "Value": true
}]
```

また、次の Resource Tagger 設定プロファイルをデプロイします。

```
{
    "AWS::EC2::Instance": {
        "AMSMonitoringWindows": {
            "Enabled": true,
            "Filter": {
                "Platform": "Windows"
            },
            "Tags": [{
                "Key": "ams:rt:ams-managed",
                "Value": "true"
            }]
        }
```

```
    }
}
```

Resource Tagger は新しい設定変更に反応し、インスタンス上の唯一のタグは次のようになります。

```
"Tags": [{
    "Key": "myTag",
    "Value": true
}]
```

> **Warning**
>
> AMS 管理の設定を誤って同じ名前で上書きする可能性があるため、新しい設定の名前 (SampleConfigurationBlock の例では ) を指定するときは注意してください。

> **Important**
>
> 設定の変更は、必ずデプロイしてください。詳細については、「」を参照してください設定変更のデプロイ。SSM AppConfig では、作成後に設定の新しいバージョンをデプロイする必要があります。

Resource Tagger 設定の表示または変更

オンボーディング時に AWS AppConfig のアカウントにデプロイされた AMSManagedTags と CustomerManagedTags の 2 つの JSON 設定プロファイルは、AMSResourceTagger アプリケーションと AMSInfrastructure 環境で、AppConfig の GetConfiguration API を通じて確認できます。

この GetConfiguration 呼び出しの例を次に示します。

```
aws appconfig get-configuration
 --application AMSResourceTagger
 --environment AMSInfrastructure
 --configuration AMSManagedTags
 --client-id ANY_STRING
 outfile.json
```

アプリケーション: 機能を提供する AppConfig 論理ユニット。Resource Tagger の場合、これは AMSResourceTagger です。

- 環境: AMSInfrastructure。
- 設定: AMS Accelerate のデフォルトのタグ定義を表示するには、値は AMSManagedTags で、カスタマータグ定義を表示するには、値は CustomerManagedTags です。
- クライアント ID: 一意のアプリケーションインスタンス識別子。任意の文字列にすることができます。
- タグ定義は、指定された出力ファイル、この場合は outfile.json で表示できます。

その後、アラーム定義は指定された出力ファイル、この場合は outfile.json で表示できます。

AMSInfrastructure 環境で過去のデプロイを表示することで、アカウントにデプロイされている設定のバージョンを確認できます。

タグルールを上書きするには：

既存のタグルールは、 CloudFormation for Accelerate を使用して設定プロファイルをデプロイするまたは CloudFormation でカスタマイズプロファイルを更新するか、AppConfig の CreateHostedConfigurationVersion API を使用して直接更新することで上書きできます。デフォルトの設定タグルールと同じ ConfigurationID を使用すると、デフォルトのルールが上書きされ、代わりにカスタムルールが適用されます。

CustomerManagedTags ドキュメントに加えられた変更をデプロイするには：

カスタマイズ設定プロファイルを変更したら、変更をデプロイする必要があります。新しい変更をデプロイするには、AppConfig の StartDeployment API を AWS AppConfig コンソールまたは CLI を使用して実行する必要があります。

設定変更のデプロイ

カスタマイズが完了したら、StartDeployment API を使用してこれらの変更を AWS AppConfig デプロイする必要があります。次の手順は、 を使用してデプロイする方法を示しています AWS CLI。さらに、 を使用してこれらの変更 AWS マネジメントコンソール を行うことができます。詳細については、「ステップ 5: 設定をデプロイする」を参照してください。

```
aws appconfig start-deployment
--application-id <application_id>
--environment-id <environment_id>
--deployment-strategy-id <deployment_strategy_id>
--configuration-profile-id <configuration_profile_id>
--configuration-version 1
```

- アプリケーション ID: アプリケーション AMSResourceTagger のアプリケーション ID。ListApplications API コールでこれを取得します。
- 環境 ID: 環境 ID。ListEnvironments API コールで取得します。
- デプロイ戦略 ID: デプロイ戦略 ID。これを ListDeploymentStrategies API コールで取得します。
- 設定プロファイル ID: CustomerManagedTags の設定プロファイル ID。ListConfigurationProfiles API コールで取得します。
- 設定バージョン: デプロイする設定プロファイルのバージョン。

> **Important**
>
> Resource Tagger は、設定プロファイルで指定されたタグを適用します。リソースタグに対して ( AWS マネジメントコンソールまたは CloudWatch CLI/SDK を使用して) 手動で行った変更は、自動的に元に戻されるため、変更が Resource Tagger で定義されていることを確認します。Resource Tagger によって作成されるタグを確認するには、 というプレフィックスが付いたタグキーを探しますams:rt:。

StartDeployment および StopDeployment API アクションを使用してデプロイへのアクセスを、ターゲットに新しい設定をデプロイする責任と結果を理解している信頼されたユーザーに制限します。

AWS AppConfig 機能を使用して設定を作成およびデプロイする方法の詳細については、「AWS AppConfig の使用」のドキュメントを参照してください。

Resource Tagger タグを無視するように Terraform を設定する

Terraform を使用してリソースをプロビジョニングし、Resource Tagger を使用してリソースにタグを付ける場合、Resource Tagger タグは Terraform によってドリフトとして識別される場合があります。

ライフサイクル設定ブロックまたは ignore_tags グローバル設定ブロックを使用して、すべての Resource Tagger タグを無視するように Terraform を設定できます。詳細については、「Resource Tagging」の「Resource Tagging」に関する Terraform ドキュメントを参照してください。

次の例は、Resource Tagger タグプレフィックス で始まるすべてのタグを無視するグローバル設定を作成する方法を示していますams:rt:。

```
provider "aws" {
```

```
  # ... potentially other configuration ...

  ignore_tags {
    key_prefixes = ["ams:rt:"]
  }
}
```

Resource Tagger によって管理されるリソースの数の表示

Resource Tagger は、 AMS/ResourceTagger名前空間の Amazon CloudWatch に 1 時間ごとにメトリクスを送信します。メトリクスは、Resource Tagger でサポートされているリソースタイプに対してのみ出力されます。

| メトリクス名 | ディメンション | 説明 |
| --- | --- | --- |
| ResourceCount | コンポーネント、ResourceType | 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。<br><br>単位: カウント |
| ResourcesMissingManagedTags | コンポーネント、ResourceType | 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。<br><br>単位: カウント |
| UnmanagedResources | コンポーネント、ResourceType | 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タイプ ) 。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。<br><br>単位: カウント |
| MatchingResourceCount | コンポーネント、ResourceType、ConfigClauseName | Resource Tagger 設定ブロックに一致する (指定されたリソースタイプの) リソースの数。リソースが設定ブロックと一致するには、ブロックを有効にし、リソースがブロックのフィルターと一致する必要があります。 |

| メトリクス名 | ディメンション | 説明 |
| --- | --- | --- |
| | | 単位: カウント |

これらのメトリクスは、AMS-Resource-Tagger-Reporting-Dashboard でグラフとしても表示できます。ダッシュボードを表示するには、Amazon CloudWatch マネジメントコンソールから AMS-Resource-Tagger-Reporting-Dashboard を選択します。デフォルトでは、このダッシュボードのグラフには過去 12 時間のデータが表示されます。

AMS Accelerate は CloudWatch アラームをアカウントにデプロイして、AMS Resource Tagger によって管理から除外されたリソースなど、アンマネージドリソースの数の大幅な増加を検出します。AMS オペレーションは、同じタイプの 3 つのリソース、または同じタイプのすべてのリソースの 50% を超えるアンマネージドリソースの増加を調査します。変更が意図的なものではないと思われる場合、AMS オペレーションから変更の確認を求められることがあります。

## CloudFormation を使用して AMS Accelerate のタグを作成する

を使用して CloudFormation 、スタックレベル ( CloudFormation ドキュメント、リソースタグを参照) または個々のリソースレベル (Amazon EC2 リソースのタグ付けなど) でタグを適用できます。

> **Important**
>
> 一部の AMS Accelerate サービスコンポーネントには、ams:rt: プレフィックスが付いたタグが必要です。Resource Tagger は、これらのタグを所有していると見なし、Resource Tagger 設定ルールで許可されていない場合は削除します。 CloudFormation または Terraform を使用している場合でも、これらのタグには必ず Resource Tagger 設定プロファイルをデプロイする必要があります。

### CloudFormation AMS Accelerate のユースケース

このセクションでは、 で一般的に実行されるアクションを一覧表示します CloudFormation。

トピック

- for Accelerate を使用した EC2 インスタンス CloudFormation のタグ付け
- CloudFormation for Accelerate を使用した AutoScaling Group (ASG) のタグ付け
- CloudFormation for Accelerate を使用して設定プロファイルをデプロイする

for Accelerate を使用した EC2 インスタンス CloudFormation のタグ付け

以下は、タグ ams:rt:ams-managed を true の値で、 によって管理される Amazon EC2 インスタンスに適用する方法の例です CloudFormation。ams:rt:ams マネージドタグは、リソースを AMS Accelerate でモニタリングすることをオプトインします。

```
 Type: AWS::EC2::Instance

Properties:
  InstanceType: "t3.micro"

  # ...other properties...

  Tags:
    - Key: "ams:rt:ams-managed"
      Value: "true"
```

CloudFormation for Accelerate を使用した AutoScaling Group (ASG) のタグ付け

以下は、タグ ams:rt:ams-managed を によって管理される Auto Scaling グループに true の値で適用する方法の例です CloudFormation。Auto Scaling グループは、作成した Amazon EC2 インスタンスにタグを伝達することに注意してください。ams:rt:ams マネージドタグは、リソースを AMS Accelerate でモニタリングすることをオプトインします。

```
  Type: AWS::AutoScaling::AutoScalingGroup
Properties:
  AutoScalingGroupName: "SampleASG"

  # ...other properties...

  Tags:
    - Key: "ams:rt:ams-managed"
      Value: "true"
```

CloudFormation for Accelerate を使用して設定プロファイルをデプロイする

を使用してCustomerManagedTags設定プロファイルをデプロイする場合は CloudFormation、次の CloudFormation テンプレートを使用できます。目的の JSON 設定を AMSResourceTaggerConfigurationVersion.Contentフィールドに入力します。

テンプレートを CloudFormation スタックまたはスタックセットにデプロイすると、設定に必要な JSON 形式に従わない場合、AMSResourceTaggerDeployment リソースのデプロイは失敗します。予想される形式の詳細については、構文と構造「」を参照してください。

これらのテンプレートを CloudFormation スタックまたはスタックセットとしてデプロイする方法については、以下の関連 AWS CloudFormation ドキュメントを参照してください。

- AWS CloudFormation コンソールでのスタックの作成
- を使用したスタックの作成 AWS CLI
- スタックセットの作成

> **Note**
>
> これらのテンプレートのいずれかを使用して設定バージョンをデプロイし、その後 CloudFormation スタック/スタックセットを削除すると、テンプレート設定バージョンは現在のデプロイバージョンのままになり、追加のデプロイは行われません。デフォルト設定に戻す場合は、スタックを削除するのではなく、手動で空の設定 ( のみ{}) をデプロイするか、スタックを空の設定に更新する必要があります。

JSON

```
{
  "Description": "Custom configuration for the AMS Resource Tagger.",
  "Resources": {
    "AMSResourceTaggerConfigurationVersion": {
      "Type": "AWS::AppConfig::HostedConfigurationVersion",
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-ApplicationId"
        },
        "ConfigurationProfileId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-CustomerManagedTags-
ProfileID"
        },
        "Content": "{\"Options\": {\"ReadOnly\": false}}",
        "ContentType": "application/json"
      }
    },
    "AMSResourceTaggerDeployment": {
```

```
      "Type": "AWS::AppConfig::Deployment",
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-ApplicationId"
        },
        "ConfigurationProfileId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-CustomerManagedTags-
ProfileID"
        },
        "ConfigurationVersion": {
          "Ref": "AMSResourceTaggerConfigurationVersion"
        },
        "DeploymentStrategyId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-Deployment-StrategyID"
        },
        "EnvironmentId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-EnvironmentId"
        }
      }
    }
  }
}
```

YAML

```
Description: Custom configuration for the AMS Resource Tagger.
Resources:
  AMSResourceTaggerConfigurationVersion:
    Type: AWS::AppConfig::HostedConfigurationVersion
    Properties:
      ApplicationId:
        !ImportValue AMS-ResourceTagger-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-ResourceTagger-Configuration-CustomerManagedTags-ProfileID
      Content: |
        {
          "Options": {
            "ReadOnly": false
          }
        }
      ContentType: application/json
  AMSResourceTaggerDeployment:
    Type: AWS::AppConfig::Deployment
```

```
    Properties:
      ApplicationId:
        !ImportValue AMS-ResourceTagger-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-ResourceTagger-Configuration-CustomerManagedTags-ProfileID
      ConfigurationVersion:
        !Ref AMSResourceTaggerConfigurationVersion
      DeploymentStrategyId:
        !ImportValue AMS-ResourceTagger-Configuration-Deployment-StrategyID
      EnvironmentId:
        !ImportValue AMS-ResourceTagger-Configuration-EnvironmentId
```

## Terraform を使用して AMS Accelerate のタグを作成する

AMS Accelerate Resource Tagger を使用しない場合は、Terraform を使用して独自のタグを適用できます。ただし、Terraform 定義からのドリフトのために Resource Tagger を使用しない場合は、Resource Tagger を使用して、それが引き起こすドリフトを無視する方法があります。「」を参照してくださいResource Tagger タグを無視するように Terraform を設定する。

> **Important**
>
> 一部の AMS Accelerate サービスコンポーネントには、ams:rt: プレフィックスが付いたタグが必要です。Resource Tagger は、これらのタグを所有していると見なし、Resource Tagger 設定ルールで許可されていない場合は削除します。 CloudFormation または Terraform を使用している場合でも、これらのタグの Resource Tagger 設定プロファイルをデプロイする必要があります。

以下は、値が true のタグ ams:rt:ams-managed を Terraform によって管理される Amazon EC2 インスタンスに適用する方法の例です。ams:rt:ams マネージドタグは、AMS Accelerate によるリソースのモニタリングをオプトインします。

```
resource "aws_instance" "sample_linux_instance" {
  # ...ami and other properties...

  instance_type = "t3.micro"

  tags = {
      "ams:rt:ams-managed" = "true"
```

```
    }
}
```

以下は、値が true の ams:rt:ams-managed タグを Terraform によって管理される Auto Scaling グループに適用する方法の例です。Auto Scaling グループは、タグを、そのグループによって作成された Amazon EC2 インスタンスに伝達することに注意してください。ams:rt:ams マネージドタグは、リソースを AMS Accelerate でモニタリングすることをオプトインします。

```
  resource "aws_autoscaling_group" "sample_asg" {
    # ...other properties...

    name = "terraform-sample"

    tags = {
        "ams:rt:ams-managed" = "true"
    }
}
```

Terraform が作成したリソースタグを管理する方法については、「」を参照してくださいResource Tagger タグを無視するように Terraform を設定する。

# AMS Accelerate 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

AMS Accelerate を使用すると、 AWS のサポートセンターを通じて、運用上の問題やリクエストに対するサポートをいつでもリクエストできます AWS マネジメントコンソール。AMS Accelerate オペレーションエンジニアは、インシデントやサービスリクエストに round-the-clock対応し、サービスの応答時間サービスレベルアグリーメント (SLAsを利用できます。AMS Accelerate 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。

AMS Accelerate は、運用上の優秀性の実現に役立つさまざまな運用サービスを提供します AWS。24 round-the-clock体制のヘルプデスク、プロアクティブモニタリング、セキュリティ、パッチ適用、ログ記録、バックアップなど、いくつかの主要な運用機能 AWS クラウド を使用して、チームが で全体的な運用上の優秀性を達成するのに AMS がどのように役立つかをすばやく理解するには、「AMS リファレンスアーキテクチャ図」を参照してください。

トピック

- AMS Accelerate でのインシデント管理
- Accelerate でのサービスリクエスト管理
- Accelerate でのインシデントレポートとサービスリクエストのテスト
- AMS Accelerate の請求に関する質問

## AMS Accelerate でのインシデント管理

AMS Accelerate では、 AWS Support Center Console を使用してインシデントレポートをファイルします。インシデントは、AMS Accelerate 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 Accelerate チームによって特定されたインシデントは、最初にイベント (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) として受信されます。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 Accelerate 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。

> **Note**
>
> AMS Accelerate チームは、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作成したインシデントも受け取りますservice-ams-operations-report-incident。

の使用の詳細については サポート、「 の開始方法 サポート」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。本稼働システムに影響す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。

## インシデント対応と解決の仕組み

AMS Accelerate は、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。

世界中のオペレーションセンターを通じて 24 時間 365 follow-the-sunサポートを提供し、専任のオペレーターがモニタリングダッシュボードとインシデントキューを積極的に監視しています。

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、クローズします。これらのすべてのアクティビティの更新は、 AWS サポートセンターと AWS サポート API を通じて提供されます。オペレーターは、さまざまな内部 AWS サポートツールを活用して、これらのすべてのアクティビティを支援します。これらのオペレーターは、AMS Accelerate 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。オペレーターにサポートが必要な場合は、プレミアムサポートチームと AWS サービスチームを利用できます。

AMS Accelerate オペレーションチームがインシデントを受け取った後、明確化が必要な場合は、優先度と分類を検証します。例えば、インシデントレポートがサービスリクエストとしてより適切に分類されている場合、インシデントレポートは再分類され、AMS Accelerate サービスリクエストチームが引き継ぎ、通知を受け取ります。インシデントを受信側オペレーターが解決できる場合、インシデントを迅速に解決するためのステップが実行されます。AMS Accelerate 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。解決後、AMS Accelerate 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。

重大な重大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 Accelerate はインフラストラクチャの復元を推奨することがあります。多くの場合、問題のトラブルシューティングと既知の機能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 Accelerate がサポートし、クラウドサービスデリバリーマネージャー (CSDM) が関与する可能性がありますが、復元の緊急性が高い場合、AMS Accelerate はすぐに復元を開始できます。

# AMS Accelerate でのインシデントの操作

AWS サポートセンターから、次のタスクを実行できます。

- インシデントを報告して更新します。AMS Accelerate インシデントを報告するには、サービスメニューから AMS Operations -- Report Incident を選択します。
- 送信されたすべてのインシデントのリストと詳細情報を取得します。
- インシデントの検索をステータスやその他のフィルターで絞り込みます。
- インシデントに通信とファイルの添付ファイルを追加し、ケースの通信用に E メール受信者を追加します。
- ライブチャットを開始するか、インシデントのコールバックをリクエストします。

> **Note**
>
> 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。セキュリティ問題の場合は、優先度の高い (P1 または P2) サポートケースを作成します。

- インシデントを解決します。
- インシデントコミュニケーションを評価します。

次の例では、 サポートセンター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 Accelerate チームはお客様と協力して、標準の AMS Accelerate SLA に従ってインシデントを解決します。

## Accelerate のインシデントの送信

サポートセンターを使用してインシデントを報告するには、サポートドキュメント「サポートケースの作成」を参照してください。

サポート センターを使用してインシデントを報告するには：

1. ケースの作成 をクリックします。インシデントケースの作成ページが開きます。
2. テクニカルサポートの問題タイプメニューを開き、AMS Operations -- Report Incident を選択します。インシデントに関する情報を入力し、作成を選択します。
3. インシデント解決プロセスの各ステップで E メールで通知を受けるには、CC Emails オプションを必ず入力してください。フェデレーションで接続する場合は、AMS Accelerate がインシデントについて送信する E メールのリンクに従う前にログインしてください。

> **Note**
>
> できるだけ詳しく説明します。関連するリソース情報と、問題を理解するのに役立つその他の情報を含めてください。たとえば、パフォーマンスのトラブルシューティングの場合は、タイムスタンプとログの情報を含めます。機能のリクエストや一般的なガイダンスの質問の場合は、お使いの環境と目的の説明を含めます。いずれの場合も、ケースの送信フォームに表示される説明の指示に従って入力してください。
> できるだけ詳しく説明していただくことで、ケースを迅速に解決できる可能性が高まります。

AWS サポート API をサービスコードとともに使用`service-ams-operations-report-incident`して、インシデントを報告することもできます。

## Accelerate インシデントのモニタリングと更新

サポートセンターを使用するか、 サポート API `DescribeCases`オペレーションを使用してプログラムでインシデントレポートとサービスリクエストを更新、モニタリング、確認できます。

Center 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 サポート 、次の手順に従います。

1. AWS マネジメントコンソールで、 サポートを参照してください。
2. 左側のナビゲーションから、サポートケースを選択し、ケースを参照し、Subjectlink 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。

   この時点で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ケースを開くをクリックして、 サポート センターでケース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。

   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 Accelerate オペレーションチームによって更新されると、サポートセンターに E メールとインシデントへのリンクが届き、対応できるようになります。

   > **Note**
   >
   > E メールに返信してケースコレスポンデンスに応答することはできません。

ダッシュボードに多くのケースがある場合は、Filteroption を使用できます。

- 件名: このフィルターを使用して、ケースの件名のキーワードを検索します。
- 重要度: リストから重要度を選択して、重要度でケースをフィルタリングします。
- ケースタイプ: 特定のケースタイプのすべてのケースを表示するには、これを使用します。Accelerate インシデントとサービスリクエストは、サービス固有のケースとともにテクニカルサポートケースタイプに表示されます。
- ステータス: リストから特定のステータスを選択して、ステータスでケースをフィルタリングします。

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. コレスポンデンスが多すぎて、すべて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、新しいコレスポンデンスを入力し、送信を選択します。
6. 満足のいくように解決し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。

## サポート API を使用した Accelerate インシデントの管理

サポート API を使用してインシデントを作成し、問題の調査中に サポート スタッフとの通信を追加できます。 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 サポートサービスを使用できる方法については、AWS 「サポートケースの有効期間のプログラミング」を参照してください。

> **Note**
>
> AMS Accelerate チームは、サービスコード で を使用してプログラムで作成したインシデントを受け取りますservice-ams-operations-report-incident。

## AMS Accelerate が生成したインシデントへの対応

AMS Accelerate 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、「AMS Accelerate でのモニタリングとイベント管理」を参照してください。AMS Accelerate はインシデン

トを特定して作成する場合があり、ほとんどの場合、イベントを通知するためのものです。インシデントを解決するためにユーザー側のアクションが必要な場合は、AMS Accelerate チームから、アカウントに提供した連絡先情報に通知が送信されます。この通知には、他のインシデントと同じ方法で応答します。通常は サポートセンターを通じて応答しますが、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。

> **Important**
>
> インシデントケースまたはサービスリクエストの状態変更通知を受信するには、アドレスフィールドに E メールアドレスを入力します。

詳細については、Akshay の動画をご覧ください (4:15)

# Accelerate でのサービスリクエスト管理

トピック

- Accelerate のサービスリクエストを使用するタイミング
- Accelerate でのサービスリクエスト管理の仕組み
- Accelerate でのサービスリクエストの作成
- Accelerate のサービスリクエストのモニタリングと更新
- Accelerate のサポート API を使用したサービスリクエストの管理
- AMS Accelerate が生成したサービスリクエストへの応答

AMS Accelerate は、サービスリクエスト管理を使用して、アクティブなサービスリクエストの記録、対応、進捗状況の伝達、通知を行います。

サービスリクエスト管理プロセスの目標は、マネージドサービスが必要なものを確実に提供できるようにすることです。

請求関連のクエリの場合は、サービスリクエストを作成します。

> **Note**
>
> AMS Accelerate チームは、AWS サポート API とサービスコード を使用して、ユーザーが作成したサービスリクエストをプログラムで受け取りますservice-ams-operations-service-request。

AWS サポートセンターを使用して、次のタスクを実行できます。

- サービスリクエストをレポートして更新します。AMS Accelerate サービスリクエストの場合は、サービスメニューから AMS オペレーション -- サービスリクエストを選択します。
- 送信された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します。
- ステータスやその他のフィルターでサービスリクエストの検索を絞り込みます。
- リクエストに通信とファイルの添付ファイルを追加し、ケースの通信用に E メール受信者を追加します。
- サービスリクエストを解決します。
- サービスリクエストの通信をレートします。

## Accelerate の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。サービスリクエストを送信すると、AMS Accelerate チームはお客様と協力して AMS SLA に従ってリクエストを解決します。

- 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

# Accelerate での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 Accelerate オペレーションチームによって処理されます。

サービスリクエストが AMS Accelerate オペレーションチームによって受信されると、サービスリクエストまたはインシデントとして適切に分類されていることを確認するためにレビューされます。インシデントとして再分類された場合、AMS Accelerate インシデント管理プロセスが開始され、通知が送信されます。

AMS Accelerate 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 Accelerate 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 サポートチームに、実行されている手順に関する E メールを送ります。

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。

# Accelerate でのサービスリクエストの作成

サービスリクエストを作成するには、次の手順に従います。

1. AMS Accelerate コンソールから、Dashboard を参照します。
2. Open a service request を選択します。AMS – Service Request が事前に選択されています。
3. カテゴリを選択します。
4. 重要度 (プラス階層またはプレミアム階層のみ) を選択します。
5. 次の情報を入力します。

- 件名: サービスリクエストのわかりやすいタイトル。
- 説明: サービスリクエスト、影響を受けるシステム、解決の期待される結果の包括的な説明。

6. 添付ファイルを追加するには、添付ファイルを選択し、必要な添付ファイルを参照し、開くを選択します。添付ファイルを削除するには、削除アイコンを選択します。
7. お問い合わせ: ウェブ経由のデフォルトの問い合わせ AMS。他のオプションを選択するには：
   - 優先連絡先言語: AMS Accelerate サービスリクエストでサポートされている言語は英語です。
   - ウェブ: サービスリクエストはウェブ経由で送信され、AMS オペレーションチームによって処理されます。
   - チャット: AMS Accelerate オペレーション担当者とオンラインでチャットします。このオプションは、チャットキューに追加します。
   - 電話: AMS オペレーションの担当者が折り返し電話します。該当する場合は、AWS リージョン、電話番号、および拡張機能を入力します。
   - 追加の連絡先: サービスリクエストにコピーする追加の E メールアドレスを入力します。
8. [Submit] を選択してください。

   ケースの詳細ページが開き、Type、Subject、Created、ID、Status などのサービスリクエストに関する情報が表示されます。さらに、作成したリクエストの説明を含む aCorrespondencearea。

   コレスポンデンスエリアを開き、ステータスの追加の詳細または更新を提供するには、返信を選択します。

   サービスリクエストが解決されたら、ケースの解決を選択します。

   コレスポンデンスが多すぎてすべてのコレスポンデンスがページに表示されない場合は、「Load More」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。

> **Note**
>
> サービスリクエスト機能をテストする場合は、 などのサービスリクエストの件名にアクションなしフラグを追加することをお勧めしますAMSTestNoOpsActionRequired。その後、サービスリクエスト解決プロセスを開始せずにテストできます。

AMS Accelerate チームは、AWS サポート API とサービスコード を使用して、ユーザーが作成したサービスリクエストをプログラムで受け取りますservice-ams-operations-service-request。

## Accelerate のサービスリクエストのモニタリングと更新

Center 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 サポート 、次の手順に従います。

1. AWS マネジメントコンソールで、 サポートを参照してください。
2. 左側のナビゲーションから、サポートケースを選択し、ケースを参照し、Subjectlink 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。

   この時点で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ケースを開くをクリックして、 サポート センターでケースの作成ページを開き、AMS サービスタイプを自動入力します。

   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 Accelerate オペレーションチームによって更新されると、サポートセンターに E メールとインシデントへのリンクが届き、対応できるようになります。

   > **Note**
   >
   > E メールに返信してケースコレスポンデンスに応答することはできません。

   ダッシュボードに多くのケースがある場合は、Filteroption を使用できます。

   - 件名: このフィルターを使用して、ケースの件名のキーワードを検索します。
   - 重要度: リストから重要度を選択して、重要度でケースをフィルタリングします。
   - ケースタイプ: 特定のケースタイプのすべてのケースを表示するには、これを使用します。Accelerate インシデントとサービスリクエストは、サービス固有のケースとともにテクニカルサポートケースタイプに表示されます。
   - ステータス: リストから特定のステータスを選択して、ステータスでケースをフィルタリングします。
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. コレスポンデンスが多すぎてすべてのコレスポンデ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、新しいコレスポンデンスを入力し、送信を選択します。
6. 満足のいくように解決し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。

## Accelerate のサポート API を使用したサービスリクエストの管理

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、サービスリクエストを作成し、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。

また、AMS チームは、AWS サポート API とサービスコード service-ams-operations-service-request を使用して、ユーザーが作成したサービスリクエストをプログラムで受け取ります。

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 「サポートケースの有効期間のプログラミング」を参照してください。

## AMS Accelerate が生成したサービスリクエストへの応答

AMS Accelerate 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、「」を参照してくださいAMS Accelerate でのモニタリングとイベント管理。AMS Accelerate は、通常、サービスリクエストを解決するためにユーザー側のアクションが必要な場合に、サービスリクエストまたはサービス通知を作成することがあります。この場合、AMS Accelerate チームは、アカウントに対して指定した連絡先に通知を送信します。このサービスリクエストには、他のケースと同じ方法で応答します。通常は サポートセンターを通じて応答しますが、場合によっては、E メールまたは電話による通信が必要になります。

> **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通知を受信するには、アドレスフィールドに 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。

通知 E メールのリンクは、AMS Accelerate 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ている場合にのみ機能します。それ以外の場合は、AMS Accelerate 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。

> **Note**
>
> AMS Accelerate 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。サービスリクエスト/通知管理プロセスを容易にするために、代替オペレーションの連絡先 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 Accelerate オンボーディングプロセス中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。

## Accelerate でのインシデントレポートとサービスリクエストのテスト

インシデントレポートまたはサービスリクエストをテストするときは、AMSTestNoOpsActionRequired をサブジェクトテキストに含める必要があります。これにより、インシデントまたはリクエスト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、それを見ても応答しません。

## AMS Accelerate の請求に関する質問

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。

# 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アクティビティ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。
- 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、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。特定の要件については、CSDM にお問い合わせください。

# 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 Cases: Service Request (SRs)/Incident を介して AMS を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*。

  該当する場合は、ライブコンタクトオプションを使用できます。
- 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 関連のケースが送信されると、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 の詳細へのリンクは、内部的に AMS エンジニアに提供されます。

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 (サービスリクエスト、インシデント) 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 Accelerate 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」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。

# オンデマンドオペレーション

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、カタログサービス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。

| オペレーションプラン | タイトル | 説明 | 期待される成果 |
| --- | --- | --- | --- |
| AMS 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 |

| | | | |
|---|---|---|---|
| | | 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と、Amazon EKS および Kubernetes アドオンの厳選されたセットの更新を実行します。 | となるオペレーション作業を支援しました。 |
| AMS Accelerate | AMI の構築と販売 | AMS は、AMI の構築と販売を継続的に管理します。<br><br>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。 | 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。 |

| | | | |
|---|---|---|---|
| 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、設定ガイダンス 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。当社のエンジニアは、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の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 ディングゾーンの継続的な運用と管理 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、、 AWS Transit Gateway AWS Control Tower、 の管理の基盤となる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 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、パフォーマンスチューニング、DBA、SAP ベース管理などの他の SAP 機能を提供する必要があります。 |

| | | | |
|---|---|---|---|
| AMS Accelerate | EC2 オペレーションでの SQL Server | AMS はお客様と協力して、EC2 インスタンスにデプロイされた SQL Server データベースの継続的なオペレーションをオンボード、実装、管理します。<br><br>当社のエンジニアは、運用上のベストプラクティスと自動化を活用して、バックアップとパッチ適用などのタスクを実行し、AMS 運用サポートを SQL Server のパッチ適用に拡張して、クラスター対応のローリング更新、ランサムウェア防御戦略に沿ったバックアップと復元サービス、お客様が提供するバックアップとパッチ適用のコントロールへの準拠をモニタリングすることで、データベースチームを解放します。 | SQL Server のお客様は、独自のライセンス (BYOL) を EC2 に持ち込むことでライセンスコストを最適化するだけでなく、ワークロードの耐障害性とセキュリティ体制を向上させるために、パッチ適用とバックアップデータベースオペレーションのオフロードを支援しました。 |
| AMS アドバンスト | 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とヘルスを処理することで、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と、Amazon EKS および Kubernetes アドオンの厳選されたセットの更新を実行します。 | カスタマーチームは、Amazon EKS クラスターの更新の基盤となるオペレーション作業を支援しました。 |

| | | | |
|---|---|---|---|
| AMS アドバンスト | Priority RFC の実行 | 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応答を受け取り、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。 |

| | | | |
|---|---|---|---|
| AMS Advanced と AMS Accelerate | レガシー OS のアップグレード | 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ないレガシーアプリケーションに最適であり、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します。<br><br>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。<br><br>• Microsoft Windows 2012 R2 から Microsoft Windows 2016 以降<br>• Microsoft Windows 2016 から Microsoft Windows 2022 以降<br>• Red Hat Enterprise Linux 7 から Red Hat Enterprise Linux 8 へ<br>• Red Hat Enterprise Linux 8 から Red Hat Enterprise Linux 9<br>• Oracle Linux 7 から Oracle Linux 8 | 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戻すことができます。運用上の観点からは、ロールバックが推奨されます。ロールバックは、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。 |

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 サービスの変更


# 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、ロールオーバーされず、将来の月に引き継がれません。

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 サービスの変更

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、その承認で更新するか、割り当てられた CSDM がお客様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。

# 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。これらのレポートは、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ため、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 ホスト管理レポート
- AMS Backup レポート
- AWS Config コントロールコンプライアンスレポート
- AMS Config Rules Response Configuration 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 ホスト管理レポート

使用可能なレポート

- SSM エージェントカバレッジレポート

### SSM エージェントカバレッジレポート

AMS SSM エージェント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 |
| 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、「バックアップジョブのステータス」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の識別子 |
| 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 |
| 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 |

| フィールド名 | 定義 |
| --- | --- |
| | 、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 |
| 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。 |

## AWS Config コントロールコンプライアンスレポート

AWS Config コントロールコンプライアンスレポートでは、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。レポートを Config ルールの重要度でフィルタリングして、最も重要な検出結果を優先します。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 | 説明 |
| --- | --- |
| 日付 | レポート日 |
| 顧客名 | 顧客名 |
| AWS アカウント ID | 顧客の関連 AWS アカウント ID |
| ソース識別子 | AWS Config ルールの一意のソース識別子 |
| ルールの説明 | AWS Config ルールの説明 |
| ルールタイプ | AWS Config ルールタイプ |

| フィールド | 説明 |
| --- | --- |
| コンプライアンスフラグ | AWS Config ルールのコンプライアンス状態 |
| リソースタイプ | AWS リソースタイプ |
| リソース名 | AWS リソース名 |
| 緊急度 | AWS Config ルールの AMS で定義されるデフォルトの推奨重要度 |
| 修復カテゴリ | AWS Config ルールの関連する修復レスポンスカテゴリ |
| 修復の説明 | AWS Config ルールに準拠するように説明する修復アクション |
| カスタマーアクション | AWS Config ルールを準拠させるために必要な顧客アクション |
| Delta メトリクスレポート | 指定された 2 つの日付の間のルールのコンプライアンスに関する変更 |

## AMS Config Rules Response Configuration レポート

AMS Config Rules Response Configuration レポートでは、非準拠の AMS 設定ルールに応答するように Accelerate が現在どのように設定されているかについて詳しく説明します。AMS 設定ルールのレスポンスを変更する方法の詳細については、「AMS Accelerate Customized findings responses」を参照してください。

このレポートには、変更した設定のみが表示され、AMS Config ルールライブラリにリストされている AMS デフォルト設定は除外されます。このレポートには、以下を含む、AMS アカウントのリソースおよび AMS 設定ルールレスポンス設定に関するデータが表示されます。

- AMS 設定ルールのデフォルトレスポンスを変更した AWS アカウントのリスト。
- AMS 設定ルールのレスポンスを関連付けたタグのリスト。
- 各ルール、アカウント、タグのレスポンス設定のリスト。
- AMS 設定ルールのデフォルトレスポンスを変更したリソースのリスト。

## 最新のレスポンス設定レポート

| フィールド | 説明 |
| --- | --- |
| 日付 | レポートが生成された日付 |
| 顧客名 | 顧客名 |
| AWS アカウント ID | 設定に関連付けられた AWS アカウント ID |
| アカウント名 | AWS アカウントレベルのリソースグループのアカウント名 |
| 検出結果タイプ | 特定された検出結果のタイプ。この場合、AWS Config |
| ソース識別子 | AWS Config ルールの一意のソース識別子 |
| リソースグループ ID | レスポンス設定に関連付けられたリソースグループ ID |
| 設定されたレスポンスアクション | AMS によってトリガーされるアクションタイプ |
| 関連付けられた SSM ランブック | 実行される修復ランブックがある場合 |
| リソースグループタイプ | これはアカウントまたはタグにすることができます |

## Config ルールのカスタムデフォルトレスポンスを持つリソース

| フィールド名 | 定義 |
| --- | --- |
| 顧客名 | 顧客名 |
| 日付 | レポートが生成された日付 |
| AWS アカウント名 | AWS アカウント名 |

| フィールド名 | 定義 |
| --- | --- |
| アカウント ID | 関連付けられた AWS アカウント ID |
| AMS 設定ルール | リソースをターゲットとし、設定で適用する AMS 設定ルール |
| リソース ID | AMS 設定ルールの対象となる顧客アカウントのリソース ID |
| リソースリージョン | 設定が適用される AWS リージョン |
| リソースタイプ | AWS リソースタイプ |
| リソースグループ ID | レスポンス設定に関連付けられたリソースグループ ID |
| リソース AMS フラグ | AWS リソースが AMS によってデプロイされている場合、このフィールドは に設定されます。 `True` |
| トリガータイプ | リソースに設定されたレスポンスのタイプ |
| コンプライアンスフラグ | AMS 設定ルールのコンプライアンス状態 |

## 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 | アカウント顧客名 |
| account_name | アカウントの名前 |
| 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前 |
| duration_in_minutes | オートメーションの分単位の長さ |
| 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 |

| フィールド名 | 定義 |
| --- | --- |
| 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 |
| アラート数 | 初回と最近の発生の間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 |

| フィールド名 | 定義 |
| --- | --- |
| 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 |
| AWS 料金の引き上げ | AMS に対して請求される AWS 料金の割合; adjusted_aws_charges * 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。uplifted_aws_charges + instance_ec2_rds_spend + uplifted_ris + 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 | 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 |
| 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。 |

| フィールド名 | 定義 |
| --- | --- |
| 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 |
| 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 |

| フィールド名 | 定義 |
| --- | --- |
| 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。

ユーザーが AMS コンソールで AMS Accelerate レポートを表示できるようにするには、 AWS Identity and Access Management (IAM) でこれらのアクションを実行するための明示的なアクセス

許可を付与する必要があります。IAM ポリシーの例については、「AMS 機能を使用するアクセス許可」を参照してください。

> **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マーマネージド 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、カスタマ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、 によって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 QuickSight 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 QuickSight 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使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

- AMS パッチ適用のインスタンス詳細の概要
- パッチの詳細
- パッチを見逃したインスタンス

## AMS パッチ適用のインスタンス詳細の概要

これは、AMS パッチ適用にオンボードされている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 |

| 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 |
| 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になります。 |
| 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、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。

このレポートには、以下が表示されます。

- 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に関するデータ。
- 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 | 重大度が「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 |
| 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><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 の日単位 |
| | window_next<br>_exec_HHMI | 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、パッチのリリース日など、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「PROD」または「NONPROD」の値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 |
| 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ト情報

| 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ト ARN | backup_vault_arn | バックアップボールト ARN |
| バックアップボールト名 | backup_vault_name | バックアップボールト名 |
| 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 |
| インスタンスタグ | 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の識別子 |
| 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 |
| 日数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てから完了日までの日数 |
| 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 スタックの一意の識別子 |
| 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: アプリケーション名 | 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 |

| フィールド名 | データセットフィールド名 | 定義 |
| --- | --- | --- |
| タグ: Cost Center | tag_cost_center | タグ値: コストセンター |
| 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: パッチグループ | 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で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、アカウントの AMS コンソールからレポートページ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、週の始めと終わりとしてカウントされます。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 |

| フィールド名 | データセットフィールド名 | 定義 |
| --- | --- | --- |
| | | 2024-01-01 は 2024 年 1 月週です。 |
| 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、週の始めと終わりとしてカウントされます。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 | 請求されたサービスの月と年 |
| 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。 adjusted_aws_charges * 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、ris_charges * 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、sp_charges * uplift_percent |
| AMS 料金 | ams_charges | 製品に対する合計 ams 料金、uplifted_aws_charges + instance_ec2_rds_spend + uplifted_ris + 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><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><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コンソール: Organization View に初めてアクセスするときは、次の手順を実行します。

1. をまだ設定していない場合は AWS Organizations、コンソールから有効化 AWS Organizationsを選択します。設定の詳細については 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、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。組織内の他のすべてのメンバーアカウント (および AMS へのオンボーディング) 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から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、 Resource Tagger ダッシュボードと の 2 つのダッシュボードがありますセキュリティ設定ルールダッシュボード。

### Resource Tagger 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 |

| フィールド名 | データセットフィールド名 | 定義 |
| --- | --- | --- |
| | | スタイプ ) 。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 (指定されたリソースタイプの) リソースの数。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。 |
| 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の識別子。 |
| 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 | 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 | ルールが事前定義済み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の 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。 |
| レコメンデーション | 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 |
| --- | --- | --- |
| AMS パッチ適用のインスタンス詳細の概要 | 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 Accelerate でのアクセス管理

アクセス管理は、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、リソースを保護する方法です。AMS Accelerate では、アクセス管理ソリューション、アクセスポリシー、関連プロセスなど、 とその AWS アカウント 基盤となるリソースへのアクセスを管理する責任があります。アクセスソリューションの管理に役立つように、AMS Accelerate は一般的な IAM の設定ミスを検出し、修復通知を配信する AWS Config ルールをデプロイします。一般的な IAM の設定ミスは、ルートユーザーがアクセスキーを持っていることです。`iam-root-access-key-check` 設定ルールは、ルートユーザーアクセスキーが使用可能で準拠しているかどうか、またはアクセスキーが存在しないかどうかを確認します。AMS によってデプロイされた設定ルールのリストについては、AMS AWS Config ルールライブラリを参照してください。

トピック


- Accelerate コンソールにアクセスする
- AMS 機能を使用するためのアクセス許可
- 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方法
- 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


## Accelerate コンソールにアクセスする

Accelerate にオンボードすると、 Accelerate コンソールに自動的にアクセスできます。コンソールにアクセスするには、AWS マネジメントコンソールでマネージドサービスを検索します。Accelerate コンソールには、 Accelerate の機能の概要が表示されます。このビューには、ダッシュボードと設定ページに表示される個々のコンポーネントが含まれます。

## AMS 機能を使用するためのアクセス許可

AMS コンソールへのアクセスやバックアップの設定など、ユーザーが AMS Accelerate 機能を読み取って設定できるようにするには、それらのアクションを実行するための IAM ロールに明示的なアクセス許可を付与する必要があります。次の CloudFormation テンプレートには、AMS に関連付けられたサービスの読み取りと設定に必要なポリシーが含まれており、IAM ロールに割り当てることができます。これらは、管理者または読み取り専用のアクセス許可が必要な IT 業界の一般的な職務と密接に一致するように設計されています。ただし、ユーザーに異なるアクセス許可を付与する必要

がある場合は、ポリシーを編集して特定のアクセス許可を含めるか除外することができます。独自のカスタムポリシーを作成することもできます。

テンプレートには 2 つのポリシーがあります。このAMSAccelerateAdminAccessポリシーは、AMS Accelerate コンポーネントのセットアップと運用に使用することを目的としています。このポリシーは通常、IT 管理者が引き受け、パッチ適用やバックアップなどの AMS 機能を設定するアクセス許可を付与します。は、AMS Accelerate 関連のリソースを表示するために必要な最小限のアクセス許可AMSAccelerateReadOnlyを付与します。

```
AWSTemplateFormatVersion: 2010-09-09
Description: AMSAccelerateCustomerAccessPolicies

Resources:
  AMSAccelerateAdminAccess:
    Type: 'AWS::IAM::ManagedPolicy'
    Properties:
      ManagedPolicyName: AMSAccelerateAdminAccess
      Path: /
      PolicyDocument:
        Fn::Sub:
        - |
          {
            "Version": "2012-10-17",
            "Statement": [
              {
                 "Sid": "AmsSelfServiceReport",
                 "Effect": "Allow",
                 "Action": "amsssrv:*",
                 "Resource": "*"
              },
              {
                "Sid": "AmsBackupPolicy",
                "Effect": "Allow",
                "Action": "iam:PassRole",
                "Resource": "arn:aws:iam::${AWS::AccountId}:role/ams-backup-iam-role"
              },
              {
                "Sid": "AmsChangeRecordKMSPolicy",
                "Effect": "Allow",
                "Action": [
                  "kms:Encrypt",
                  "kms:Decrypt",
                  "kms:GenerateDataKey"
```

```
                ],
                "Resource": [
                  "arn:aws:kms:${AWS::Region}:${AWS::AccountId}:key/*"
                ],
                "Condition": {
                  "ForAnyValue:StringLike": {
                    "kms:ResourceAliases": "alias/AMSCloudTrailLogManagement"
                  }
                }
              },
              {
                "Sid": "AmsChangeRecordAthenaReadPolicy",
                "Effect": "Allow",
                "Action": [
                  "athena:BatchGetNamedQuery",
                  "athena:Get*",
                  "athena:List*",
                  "athena:StartQueryExecution",
                  "athena:UpdateWorkGroup",
                  "glue:GetDatabase*",
                  "glue:GetTable*",
                  "s3:GetAccountPublicAccessBlock",
                  "s3:ListAccessPoints",
                  "s3:ListAllMyBuckets"
                ],
                "Resource": "*"
              },
              {
                "Sid": "AmsChangeRecordS3ReadPolicy",
                "Effect": "Allow",
                "Action": [
                  "s3:Get*",
                  "s3:List*"
                ],
                "Resource": [
                  "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}",
                  "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}/
*",
                  "arn:aws:s3:::ams-a${AWS::AccountId}-cloudtrail-${AWS::Region}",
                  "arn:aws:s3:::ams-a${AWS::AccountId}-cloudtrail-${AWS::Region}/*"
                ]
              },
              {
                "Sid": "AmsChangeRecordS3WritePolicy",
```

```
                "Effect": "Allow",
                "Action": [
                  "s3:PutObject",
                  "s3:PutObjectLegalHold",
                  "s3:PutObjectRetention"

                ],
                "Resource": [
                  "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}/*"
                ]
              },
              {
                "Sid": "MaciePolicy",
                "Effect": "Allow",
                "Action": [
                  "macie2:GetFindingStatistics"
                ],
                "Resource": "*"
              },
              {
                "Sid": "GuardDutyPolicy",
                "Effect": "Allow",
                "Action": [
                  "guardduty:GetFindingsStatistics",
                  "guardduty:ListDetectors"
                ],
                "Resource": "*"
              },
              {
                "Sid": "SupportPolicy",
                "Effect": "Allow",
                "Action": "support:*",
                "Resource": "*"
              },
              {
                "Sid": "ConfigPolicy",
                "Effect": "Allow",
                "Action": [
                  "config:Get*",
                  "config:Describe*",
                  "config:Deliver*",
                  "config:List*",
                  "config:StartConfigRulesEvaluation"
                ],
```

```
                "Resource": "*"
              },
              {
                "Sid": "AppConfigReadPolicy",
                "Effect": "Allow",
                "Action": [
                  "appconfig:List*",
                  "appconfig:Get*"
                ],
                "Resource": "*"
              },
              {
                "Sid": "AppConfigPolicy",
                "Effect": "Allow",
                "Action": [
                  "appconfig:StartDeployment",
                  "appconfig:StopDeployment",
                  "appconfig:CreateHostedConfigurationVersion",
                  "appconfig:ValidateConfiguration"
                ],
                "Resource": [
                  "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSAlarmManagerConfigurationApplicationId}",
                  "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSAlarmManagerConfigurationApplicationId}/configurationprofile/
${AMSAlarmManagerConfigurationCustomerManagedAlarmsProfileID}",
                  "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSAlarmManagerConfigurationApplicationId}/environment/*",
                  "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSResourceTaggerConfigurationApplicationId}",
                  "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSResourceTaggerConfigurationApplicationId}/configurationprofile/
${AMSResourceTaggerConfigurationCustomerManagedTagsProfileID}",
                  "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSResourceTaggerConfigurationApplicationId}/environment/*",
                  "arn:aws:appconfig:*:${AWS::AccountId}:deploymentstrategy/*"
                ]
              },
              {
                "Sid": "CloudFormationStacksPolicy",
                "Effect": "Allow",
                "Action": [
                  "cloudformation:DescribeStacks"
                ],
```

```
      "Resource": "*"
    },
    {
      "Sid": "EC2Policy",
      "Action": [
        "ec2:DescribeInstances"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Sid": "SSMPolicy",
      "Effect": "Allow",
      "Action": [
        "ssm:AddTagsToResource",
        "ssm:CancelCommand",
        "ssm:CancelMaintenanceWindowExecution",
        "ssm:CreateAssociation",
        "ssm:CreateAssociationBatch",
        "ssm:CreateMaintenanceWindow",
        "ssm:CreateOpsItem",
        "ssm:CreatePatchBaseline",
        "ssm:DeleteAssociation",
        "ssm:DeleteMaintenanceWindow",
        "ssm:DeletePatchBaseline",
        "ssm:DeregisterPatchBaselineForPatchGroup",
        "ssm:DeregisterTargetFromMaintenanceWindow",
        "ssm:DeregisterTaskFromMaintenanceWindow",
        "ssm:Describe*",
        "ssm:Get*",
        "ssm:List*",
        "ssm:PutConfigurePackageResult",
        "ssm:RegisterDefaultPatchBaseline",
        "ssm:RegisterPatchBaselineForPatchGroup",
        "ssm:RegisterTargetWithMaintenanceWindow",
        "ssm:RegisterTaskWithMaintenanceWindow",
        "ssm:RemoveTagsFromResource",
        "ssm:SendCommand",
        "ssm:StartAssociationsOnce",
        "ssm:StartAutomationExecution",
        "ssm:StartSession",
        "ssm:StopAutomationExecution",
        "ssm:TerminateSession",
        "ssm:UpdateAssociation",
```

```
            "ssm:UpdateAssociationStatus",
            "ssm:UpdateMaintenanceWindow",
            "ssm:UpdateMaintenanceWindowTarget",
            "ssm:UpdateMaintenanceWindowTask",
            "ssm:UpdateOpsItem",
            "ssm:UpdatePatchBaseline"
          ],
          "Resource": "*"
        },
        {
          "Sid": "AmsPatchRestrictAMSResources",
          "Effect": "Deny",
          "Action": [
            "ssm:DeletePatchBaseline",
            "ssm:UpdatePatchBaseline"
          ],
          "Resource": [
            "arn:aws:ssm:${AWS::Region}:${AWS::AccountId}:patchbaseline/*"
          ],
          "Condition": {
            "StringLike": {
              "aws:ResourceTag/ams:resourceOwner": "*"
            }
          }
        },
        {
          "Sid": "AmsPatchRestrictAmsTags",
          "Effect": "Deny",
          "Action": [
            "ssm:AddTagsToResource",
            "ssm:RemoveTagsFromResource"
          ],
          "Resource": "*",
          "Condition": {
            "ForAnyValue:StringLike": {
              "aws:TagKeys": [
                "AMS*",
                "Ams*",
                "ams*"
              ]
            }
          }
        },
        {
```

```
                "Sid": "TagReadPolicy",
                "Effect": "Allow",
                "Action": [
                  "tag:GetResources",
                  "tag:GetTagKeys"
                ],
                "Resource": "*"
              },
              {
                "Sid": "CloudtrailReadPolicy",
                "Effect": "Allow",
                "Action": [
                  "cloudtrail:DescribeTrails",
                  "cloudtrail:GetTrailStatus",
                  "cloudtrail:LookupEvents"
                ],
                "Resource": "*"
              },
              {
                "Sid": "EventBridgePolicy",
                "Effect": "Allow",
                "Action": [
                  "events:Describe*",
                  "events:List*",
                  "events:TestEventPattern"
                ],
                "Resource": "*"
              },
              {
                "Sid": "IAMReadOnlyPolicy",
                "Action": [
                    "iam:ListRoles",
                    "iam:GetRole"
                ],
                "Effect": "Allow",
                "Resource": "*"
              },
              {
                "Sid": "AmsResourceSchedulerPassRolePolicy",
                "Effect": "Allow",
                "Action": "iam:PassRole",
                "Resource": "arn:aws:iam::${AWS::AccountId}:role/
ams_resource_scheduler_ssm_automation_role",
                "Condition": {
```

```
                    "StringEquals": {
                        "iam:PassedToService": "ssm.amazonaws.com"
                    }
                }
              }
            ]
          }
        - AMSAlarmManagerConfigurationApplicationId: !ImportValue "AMS-Alarm-Manager-
Configuration-ApplicationId"
          AMSAlarmManagerConfigurationCustomerManagedAlarmsProfileID: !ImportValue
 "AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-ProfileID"
          AMSResourceTaggerConfigurationApplicationId: !ImportValue "AMS-
ResourceTagger-Configuration-ApplicationId"
          AMSResourceTaggerConfigurationCustomerManagedTagsProfileID: !ImportValue
 "AMS-ResourceTagger-Configuration-CustomerManagedTags-ProfileID"

  AMSAccelerateReadOnly:
    Type: 'AWS::IAM::ManagedPolicy'
    Properties:
      ManagedPolicyName: AMSAccelerateReadOnly
      Path: /
      PolicyDocument: !Sub |
        {
          "Version": "2012-10-17",
          "Statement": [
          {
                "Sid": "AmsSelfServiceReport",
                "Effect": "Allow",
                "Action": "amsssrv:*",
                "Resource": "*"
             },
           {
              "Sid": "AmsBackupPolicy",
              "Effect": "Allow",
              "Action": [
                "backup:Describe*",
                "backup:Get*",
                "backup:List*"
              ],
              "Resource": "*"
           },
           {
               "Action": [
                   "rds:DescribeDBSnapshots",
```

```
                "rds:ListTagsForResource",
                "rds:DescribeDBInstances",
                "rds:describeDBSnapshots",
                "rds:describeDBEngineVersions",
                "rds:describeOptionGroups",
                "rds:describeOrderableDBInstanceOptions",
                "rds:describeDBSubnetGroups",
                "rds:DescribeDBClusterSnapshots",
                "rds:DescribeDBClusters",
                "rds:DescribeDBParameterGroups",
                "rds:DescribeDBClusterParameterGroups",
                "rds:DescribeDBInstanceAutomatedBackups"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "dynamodb:ListBackups",
                "dynamodb:ListTables"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "elasticfilesystem:DescribeFilesystems"
            ],
            "Resource": "arn:aws:elasticfilesystem:*:*:file-system/*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "ec2:DescribeSnapshots",
                "ec2:DescribeVolumes",
                "ec2:describeAvailabilityZones",
                "ec2:DescribeVpcs",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeImages",
                "ec2:DescribeSubnets",
                "ec2:DescribePlacementGroups",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes"
```

```
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "tag:GetTagKeys",
                "tag:GetTagValues",
                "tag:GetResources"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:DescribeCachediSCSIVolumes",
                "storagegateway:DescribeStorediSCSIVolumes"
            ],
            "Resource": "arn:aws:storagegateway:*:*:gateway/*/volume/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:ListGateways"
            ],
            "Resource": "arn:aws:storagegateway:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:DescribeGatewayInformation",
                "storagegateway:ListVolumes",
                "storagegateway:ListLocalDisks"
            ],
            "Resource": "arn:aws:storagegateway:*:*:gateway/*"
        },
        {
            "Action": [
                "iam:ListRoles",
                "iam:GetRole"
            ],
            "Effect": "Allow",
            "Resource": "*"
```

```
            },
            {
                "Effect": "Allow",
                "Action": "organizations:DescribeOrganization",
                "Resource": "*"
            },
            {
                "Action": "fsx:DescribeBackups",
                "Effect": "Allow",
                "Resource": "arn:aws:fsx:*:*:backup/*"
            },
            {
                "Action": "fsx:DescribeFileSystems",
                "Effect": "Allow",
                "Resource": "arn:aws:fsx:*:*:file-system/*"
            },
            {
                "Action": "ds:DescribeDirectories",
                "Effect": "Allow",
                "Resource": "*"
            },
            {
              "Sid": "AmsChangeRecordKMSPolicy",
              "Effect": "Allow",
              "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:GenerateDataKey"
              ],
              "Resource": [
                "arn:aws:kms:${AWS::Region}:${AWS::AccountId}:key/*"
              ],
              "Condition": {
                "ForAnyValue:StringLike": {
                  "kms:ResourceAliases": "alias/AMSCloudTrailLogManagement"
                }
              }
            },
            {
              "Sid": "AmsChangeRecordAthenaReadPolicy",
              "Effect": "Allow",
              "Action": [
                "athena:BatchGetNamedQuery",
                "athena:Get*",
```

```
            "athena:List*",
            "athena:StartQueryExecution",
            "athena:UpdateWorkGroup",
            "glue:GetDatabase*",
            "glue:GetTable*",
            "s3:GetAccountPublicAccessBlock",
            "s3:ListAccessPoints",
            "s3:ListAllMyBuckets"
        ],
        "Resource": "*"
    },
    {
        "Sid": "AmsChangeRecordS3ReadPolicy",
        "Effect": "Allow",
        "Action": [
            "s3:Get*",
            "s3:List*"
        ],
        "Resource": [
            "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}",
            "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}/*",
            "arn:aws:s3:::ams-a${AWS::AccountId}-cloudtrail-${AWS::Region}",
            "arn:aws:s3:::ams-a${AWS::AccountId}-cloudtrail-${AWS::Region}/*"
        ]
    },
    {
        "Sid": "AmsChangeRecordS3WritePolicy",
        "Effect": "Allow",
        "Action": [
            "s3:PutObject",
            "s3:PutObjectLegalHold",
            "s3:PutObjectRetention"
        ],
        "Resource": [
            "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}/*"
        ]
    },
    {
        "Sid": "MaciePolicy",
        "Effect": "Allow",
        "Action": [
            "macie2:GetFindingStatistics"
        ],
        "Resource": "*"
```

```
        },
        {
          "Sid": "GuardDutyReadPolicy",
          "Effect": "Allow",
          "Action": [
            "guardduty:GetFindingsStatistics",
            "guardduty:ListDetectors"
          ],
          "Resource": "*"
        },
        {
          "Sid": "SupportReadPolicy",
          "Effect": "Allow",
          "Action": "support:Describe*",
          "Resource": "*"
        },
        {
          "Sid": "ConfigReadPolicy",
          "Effect": "Allow",
          "Action": [
            "config:Get*",
            "config:Describe*",
            "config:List*"
          ],
          "Resource": "*"
        },
        {
          "Sid": "AppConfigReadPolicy",
          "Effect": "Allow",
          "Action": [
            "appconfig:List*",
            "appconfig:Get*"
          ],
          "Resource": "*"
        },
        {
          "Sid": "CloudFormationReadPolicy",
          "Effect": "Allow",
          "Action": [
            "cloudformation:DescribeStacks"
          ],
          "Resource": "*"
        },
        {
```

```
            "Sid": "EC2ReadPolicy",
            "Effect": "Allow",
            "Action": [
              "ec2:DescribeInstances"
            ],
            "Resource": "*"
          },
          {
            "Sid": "SSMReadPolicy",
            "Effect": "Allow",
            "Action": [
              "ssm:Describe*",
              "ssm:Get*",
              "ssm:List*"
            ],
            "Resource": "*"
          },
          {
            "Sid": "TagReadPolicy",
            "Effect": "Allow",
            "Action": [
              "tag:GetResources",
              "tag:GetTagKeys"
            ],
            "Resource": "*"
          },
          {
            "Sid": "CloudtrailReadPolicy",
            "Effect": "Allow",
            "Action": [
              "cloudtrail:DescribeTrails",
              "cloudtrail:GetTrailStatus",
              "cloudtrail:LookupEvents"
            ],
            "Resource": "*"
          },
          {
            "Sid": "EventBridgePolicy",
            "Effect": "Allow",
            "Action": [
              "events:Describe*",
              "events:List*",
              "events:TestEventPattern"
            ],
```

```
            "Resource": "*"
          }
        ]
      }
```

# AMS がアカウントにアクセスする理由とタイミング

AMS Accelerate (Accelerate) 演算子は、特定の状況で、 リソースを管理するためにアカウントコンソールとインスタンスにアクセスできます。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 Accelerate Operations チームおよび AMS Accelerate Automation によってアカウントのアクティビティを確認する方法の詳細については、「」を参照してくださいAMS Accelerate アカウントの変更の追跡。

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コール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 |
| 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) |
| --- | --- | --- |
| インシデントの調査と修復 | お客様 | 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 | お客様 | |

## AMS カスタマーアカウントアクセス IAM ロール

AMS 演算子は、アカウントをサービスするために次のロールを必要とします。

> **Note**
>
> AMS アクセスロールを使用すると、AMS オペレーターはリソースにアクセスして AMS 機能を提供できます (「」を参照サービスの説明 )。これらのロールを変更すると、これらの機能を提供する機能が妨げられる可能性があります。AMS アクセスロールを変更する必要がある場合は、Cloud Architect を参照してください。

カスタマーアカウントへの AMS アクセス用の IAM ロール

| ロール名 | 説明 |
| --- | --- |
| ams-access-admin | このロールには、制限なしでアカウントへの完全な管理アクセス権があります。AMS サービスは、AMS インフラストラクチャをデプロイしてアカウントを運用するためのアクセスを制限する制限付きセッションポリシーでこのロールを使用します。 |
| ams-access-admin-operations | このロールは、アカウントを運用するための管理アクセス許可を AMS オペレーターに付与します。このロールは、Amazon Simple Storage Service、Amazon Relational Database Service、Amazon DynamoDB、Amazon Redshift、Amazon ElastiCache など、データストアとして一般的に使用される AWS サービスの顧客コンテンツに読み取り、書き込み、または削除のアクセス許可を付与しません。このロールを引き受けることができるのは、アクセス管理の知識と経験 |

| ロール名 | 説明 |
| --- | --- |
| | が豊富な認定 AMS オペレーターのみです。これらのオペレーターは、アクセス管理の問題のエスカレーションポイントとして機能し、アカウントにアクセスして AMS オペレーターのアクセスの問題をトラブルシューティングします。 |
| ams-access-management | オンボーディング中に手動でデプロイされます。AMS Access システムでは、 `ams-access-roles` と `ams-access-managed-policies` スタックを管理するためにこのロールが必要です。 |
| ams-access-operations | このロールには、アカウントで管理タスクを実行するアクセス許可があります。このロールには、Amazon Simple Storage Service、Amazon Relational Database Service、Amazon DynamoDB、Amazon Redshift、Amazon ElastiCache など、データストアとして一般的に使用される AWS サービスの顧客コンテンツに対する読み取り、書き込み、または削除のアクセス許可はありません。 AWS Identity and Access Management 書き込みオペレーションを実行するアクセス許可もこのロールから除外されます。AMS Accelerate オペレーションスタッフとクラウドアーキテクト (CAs) がこのロールを引き受けることができます。 |
| ams-access-read-only | このロールには、 アカウントへの読み取り専用アクセス権があります。AMS Accelerate オペレーションスタッフとクラウドアーキテクト (CAs) がこのロールを引き受けることができます。Amazon S3、Amazon RDS、DynamoDB、Amazon Redshift、ElastiCache など、データストアとして一般的に使用される AWS サービスの顧客コンテンツへの読み取りアクセス許可は、このロールには付与されません。 |

| ロール名 | 説明 |
| --- | --- |
| ams-access-security-analyst | この AMS セキュリティロールには、専用のセキュリティアラートモニタリングとセキュリティインシデント処理を実行するアクセス許可が AMS アカウントに付与されています。このロールを引き受けることができる AMS セキュリティ担当者はほとんどいません。 |
| ams-access-security-analyst-read-only | この AMS セキュリティロールは、専用のセキュリティアラートモニタリングとセキュリティインシデント処理を実行するための AMS アカウントの読み取り専用アクセス許可に制限されています。 |

> **Note**
>
> これは、ams-access-management ロールのテンプレートです。これは、クラウドアーキテクト (CAs) がオンボーディング時にアカウント内に手動でデプロイするスタックです: management-role.yaml。
> これは、さまざまなアクセスレベルのさまざまなアクセスロールのテンプレートです。ams-access-read-only、ams-access-operations、ams-access-admin-operations、ams-access-admin: accelerate-roles.yaml。

# AMS がアカウントにアクセスする方法

AMS Accelerate オペレーターは、特定の状況でアカウントコンソールとインスタンスにアクセスできます。

AMS オペレーターは、内部 AMS Accelerate アクセスサービスを使用して、安全で監査済みの方法でアカウントにアクセスします。インスタンスにアクセスするために、AMS オペレーターはブローカーと同じ内部 AMS アクセスサービスを使用し、アクセスが許可された後、AMS Accelerate オペレーターは SSM セッションマネージャーを使用してセッション認証情報を使用してアクセスを取得します。Windows インスタンスの RDP アクセスは、インスタンスへのポート転送を確立し、SSM を使用してローカルユーザーを作成することによって提供されます。ローカルユーザーの認証情報は RDP アクセスに使用され、セッションの終了時に削除されます。

# 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

AMS Accelerate を使用したルート：

AMS は、ルートユーザーアカウントの使用を禁止するものではありません。ただし、AMS Operations and Security は、その使用を調査すべき問題として扱い、使用のたびにセキュリティチームに連絡します。

CSDM と CA に 24 時間前に問い合わせて、実行するルートアクセス作業についてアドバイスすることをお勧めします。

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 Accelerate のセキュリティ管理

AWS Managed Services は、複数のコントロールを使用して情報アセットを保護し、 AWS インフラストラクチャの安全性を維持します。AMS Accelerate は、 AWS Config ルール および 修復アクションのライブラリを維持し、すべてのアカウントがセキュリティと運用の整合性に関する業界標準に準拠していることを確認します。 は、記録されたリソース間の設定変更 AWS Config ルール を継続的に追跡します。変更がルール条件に違反する場合、AMS は調査結果を報告し、違反の重大度に応じて、違反を自動またはリクエストで修正できるようにします。 は、Center for Internet Security (CIS)、米国国立標準技術研究所 (NIST) クラウドセキュリティフレームワーク (CSF)、医療保険の相互運用性と説明責任に関する法律 (HIPAA)、および Payment Card Industry (PCI) Data Security Standard (DSS) によって設定された標準への準拠 AWS Config ルール を促進します。

さらに、AMS は Amazon GuardDuty を活用して、 AWS 環境内の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。AMS は GuardDuty の検出結果を 24 時間 365 日モニタリングします。AMS はお客様と協力して結果の影響を理解し、ベストプラクティスの推奨事項に基づいて修復を特定します。また、AMS は Amazon 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を保護します。

> **Note**
>
> Amazon Macie はオプションサービスであり、デフォルトでは有効になっていません。

AMS Accelerate は、運用上の優秀性の実現に役立つさまざまな運用サービスを提供します AWS。チームが 24 時間 365 日体制のヘルプデスク、プロアクティブモニタリング、セキュリティ、パッチ適用、ログ記録、バックアップなど、AMS の主要な運用機能 AWS クラウド を使用して で全体的な運用上の優秀性を達成するのに役立つ方法の詳細については、「AMS リファレンスアーキテクチャ図」を参照してください。

トピック

- Log4j SSM ドキュメントを使用して Accelerate の出現を検出する
- AMS でのインフラストラクチャセキュリティモニタリング
- Accelerate でのデータ保護
- AWS Identity and Access Management AMS Accelerate での
- AMS のセキュリティインシデント対応
- Accelerate のセキュリティイベントのログ記録とモニタリング

- Accelerate の設定コンプライアンス
- Accelerate でのインシデント対応
- Accelerate の耐障害性
- 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
- Accelerate のセキュリティのベストプラクティス
- 変更リクエストのセキュリティレビュー
- セキュリティに関するよくある質問

# Log4j SSM ドキュメントを使用して Accelerate の出現を検出する

Log4j AWS Systems Manager ドキュメント (SSM ドキュメント) は、取り込まれたワークロード内の Apache Log4j2 ライブラリの検索に役立ちます。自動化ドキュメントは、Log4j2 ライブラリがアクティブになっている Java アプリケーションのプロセス ID のレポートを提供します (複数可 ) 。

レポートには、JndiLookup クラスを含む指定された環境内にある Java アーカイブ (JAR ファイル) に関する情報が含まれています。検出されたライブラリを利用可能な最新バージョンにアップグレードするのがベストプラクティスです。このアップグレードにより、CVE-2021-44228 で識別されるリモートコード実行 (RCE) が軽減されます。Apache から Log4j ライブラリの最新バージョンをダウンロードします。詳細については、「Apache Log4j 2 のダウンロード」を参照してください。

このドキュメントは、 Accelerate にオンボードされているすべてのリージョンと共有されます。ドキュメントにアクセスするには、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. ナビゲーションペインで、[ドキュメント] を選択します。
3. 自分と共有を選択します。
4. 検索ボックスに、AWSManagedServices-GatherLog4jInformation と入力します。
5. レート制御を使用して、ドキュメントを大規模に実行します。

AWSManagedServices-GatherLog4jInformation ドキュメントは、次のパラメータを収集します。

- InstanceId: EC2 インスタンスの (必須) ID。
- S3Bucket: (オプション) 結果をアップロードする S3 署名付き URL または S3 URI (s3://BUCKET_NAME)。

- AutomationAssumeRole: (必須) 自動削除がユーザーに代わってアクションを実行できるようにするロールの ARN。

レート制御を使用してこのドキュメントを実行するのがベストプラクティスです。レート制御パラメータを InstanceId に設定し、インスタンスのリストを割り当てるか、タグキーの組み合わせを適用して、特定のタグを持つすべての EC2 インスタンスをターゲットにすることができます。AWS Managed Services では、SAmazon S3S3) バケットを提供することをお勧めします。S3 で結果を集計する方法の例については、EC2 インスタンススタック | Log4j 情報の収集」を参照してください。

パッケージをアップグレードできない場合は、 AWS 「セキュリティサービスの使用」で説明されているガイドラインに従って、Log4j 脆弱性から保護、検出、対応します。 AWS Log4j JndiLookup クラス機能を削除して脆弱性を軽減するには、Java アプリケーション (複数可) とインラインで Log4j ホットパッチを実行します。ホットパッチの詳細については、「Hotpatch for Apache Log4j」を参照してください。

自動化の出力や追加の緩和策の進め方に関するご質問は、サービスリクエストを送信してください。

# AMS でのインフラストラクチャセキュリティモニタリング

AMS Accelerate にオンボードすると、 は次の AWS Config ベースラインインフラストラクチャと一連のルールを AWS デプロイします。AMS Accelerate はこれらのルールを使用してアカウントをモニタリングします。

- AWS Config サービスにリンクされたロール: AMS Accelerate は、AWSServiceRoleForConfig という名前のサービスにリンクされたロールをデプロイします。このロールは、他の AWS サービスのステータスをクエリ AWS Config するために によって使用されます。AWSServiceRoleForConfig サービスにリンクされたロールは、 AWS Config サービスを信頼してロールを引き受けます。AWSServiceRoleForConfig ロールのアクセス許可ポリシーには、AWS Config リソースに対する読み取り専用および書き込み専用のアクセス許可と、 が AWS Config サポートする他のサービスのリソースに対する読み取り専用アクセス許可が含まれています。 AWS Config Recorder で既にロールを設定している場合、AMS Accelerate は既存のロールに AWS Config マネージドポリシーがアタッチされていることを確認します。そうでない場合、AMS Accelerate はロールをサービスにリンクされたロール AWSServiceRoleForConfig に置き換えます。
- AWS Config レコーダーと配信チャネル: 設定レコーダー AWS Config を使用してリソース設定の変更を検出し、これらの変更を設定項目としてキャプチャします。AMS Accelerate は、設定レコーダーをすべてのサービスにデプロイし AWS リージョン、すべてのリソースを継続的に記録

します。AMS Accelerate は、 AWS リソースで発生した変更を記録するために使用する Amazon S3 バケットである設定配信チャネルも作成します。設定レコーダーは、配信チャネルを介して設定状態を更新します。が機能 AWS Config するには、設定レコーダーと配信チャネルが必要です。AMS Accelerate は、すべての にレコーダーを作成し AWS リージョン、単一の に配信チャネルを作成します AWS リージョン。にレコーダーと配信チャネルがすでにある場合 AWS リージョン、AMS Accelerate は既存の AWS Config リソースを削除しません。代わりに、AMS Accelerate は、正しく設定されていることを検証した後、既存のレコーダーと配信チャネルを使用します。AWS Config コストを削減する方法の詳細については、「」を参照してくださいAccelerate の AWS Config コストを削減する。

- AWS Config ルール: AMS Accelerate は、セキュリティと運用の整合性に関する業界標準に準拠できるように、 AWS Config ルール および 修復アクションのライブラリを維持します。 は、記録されたリソース間の設定変更 AWS Config ルール を継続的に追跡します。変更がルール条件に違反した場合、AMS はその検出結果を報告し、違反の重大度に応じて、違反を自動またはリクエストで修正できます。 は、Center for Internet Security (CIS)、米国国立標準技術研究所 (NIST) クラウドセキュリティフレームワーク (CSF)、医療保険の相互運用性と説明責任に関する法律 (HIPAA)、および Payment Card Industry (PCI) Data Security Standard (DSS) によって設定された基準への準拠 AWS Config ルール を容易にします。
- AWS Config アグリゲータ認可: アグリゲータは、複数のアカウントと複数のリージョンから AWS Config 設定およびコンプライアンスデータを収集する AWS Config リソースタイプです。AMS Accelerate は、アカウントを設定アグリゲータにオンボードします。このアグリゲータから、AMS Accelerate はアカウントのリソース設定情報を集約し、コンプライアンスデータを設定して、コンプライアンスレポートを生成します。AMS 所有アカウントに既存のアグリゲータが設定されている場合、AMS Accelerate は追加のアグリゲータをデプロイし、既存のアグリゲータは変更されません。

> **Note**
>
> Config アグリゲータは アカウントでは設定されず、AMS 所有のアカウントで設定され、アカウントにオンボードされます (複数可 ) 。

詳細については AWS Config、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 アグリゲータ: マルチアカウントマルチリージョンデータ集約

レポートの詳細については、「」を参照してくださいAWS Config コントロールコンプライアンスレポート。

## AMS Accelerate のサービスにリンクされたロールの使用

AMS Accelerate は AWS Identity and Access Management (IAM) サービスにリンクされたロールを使用します。サービスにリンクされたロール (SLR) は、AMS Accelerate に直接リンクされた一意のタイプの IAM ロールです。サービスにリンクされたロールは AMS Accelerate によって事前定義されており、サービスがユーザーに代わって他の AWS サービスを呼び出すために必要なすべてのアクセス許可が含まれています。

サービスにリンクされたロールを使用すると、必要なアクセス許可を手動で追加する必要がなくなるため、AMS Accelerate の設定が簡単になります。AMS Accelerate は、サービスにリンクされたロールのアクセス許可を定義します。特に定義されている場合を除き、AMS Accelerate のみがそのロールを引き受けることができます。定義される許可は信頼ポリシーと許可ポリシーに含まれており、その許可ポリシーを他の IAM エンティティにアタッチすることはできません。

サービスにリンクされたロールをサポートする他のサービスの詳細については、AWS 「IAM と連携するサービス」を参照し、「サービスにリンクされたロール」列で「はい」があるサービスを探します。サービスリンクロールに関するドキュメントをサービスで表示するには、リンクで [はい] を選択します。

### AMS Accelerate のサービスにリンクされたロールのデプロイツールキット

AMS Accelerate は、AWSServiceRoleForAWSManagedServicesDeploymentToolkit 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、AMS Accelerate インフラストラクチャをカスタマーアカウントにデプロイします。

> **Note**
>
> このポリシーは最近更新されました。詳細については、「」を参照してくださいサービスにリンクされたロールの更新を高速化する。

### AMS Accelerate デプロイツールキット SLR

AWSServiceRoleForAWSManagedServicesDeploymentToolkit 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。

- `deploymenttoolkit.managedservices.amazonaws.com`

AWSManagedServicesDeploymentToolkitPolicy という名前のポリシーにより、AMS Accelerate は次のリソースに対してアクションを実行できます。

- `arn:aws*:s3:::ams-cdktoolkit*`
- `arn:aws*:cloudformation:*:*:stack/ams-cdk-toolkit*`
- `arn:aws:ecr:*:*:repository/ams-cdktoolkit*`

この SLR は、CloudFormation テンプレートや Lambda アセットバンドルなどのリソースをコンポーネントデプロイのアカウントにアップロードするために AMS が使用するデプロイバケットを作成および管理するためのアクセス許可を Amazon S3 に付与します。この SLR は、デプロイバケットを定義する CloudFormation スタックをデプロイするアクセス許可を CloudFormation に付与します。詳細については、「AWSManagedServices_DeploymentToolkitPolicy」を参照してください。

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、「IAM ユーザーガイド」の「サービス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。

### AMS Accelerate 用のデプロイツールキット 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 Accelerate 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、サービスにリンクされたロールのサポートを開始した 2022 年 6 月 9 日より前に AMS Accelerate サービスを使用していた場合、アカウントに AWSServiceRoleForAWSManagedServicesDeploymentToolkit ロールを作成しました。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生じた場合は、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 Accelerate 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 Accelerate 用のデプロイツールキット SLR の編集

AMS Accelerate では、AWSServiceRoleForAWSManagedServicesDeploymentToolkit 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 Accelerate 用のデプロイツールキット SLR の削除

AWSServiceRoleForAWSManagedServicesDeploymentToolkit 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、、または AWS API で AMS からオフボードすると、AMS Accelerate はリソースをクリーンアップし AWS CLI、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 Accelerate 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。

AWSServiceRoleForAWSManagedServicesDeploymentToolkit サービスにリンクされたロールによって使用されている AMS Accelerate リソースを削除するには

アカウントが AMS でオンボーディングされたすべてのリージョンから`ams-cdk-toolkit`スタックを削除します (最初に S3 バケットを手動で空にする必要がある場合があります ) 。

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、AWSServiceRoleForAWSManagedServicesDeploymentToolkit 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。

## AMS Accelerate のサービスにリンクされたロールを Detective が制御する

AMS Accelerate は、AWSServiceRoleForManagedServices_DetectiveControlsConfig という名前のサービスリンクロール (SLR) を使用します。AWS Managed Services はこのサービスリンクロールを使用して、config-recorder、config ルール、S3 バケット検出コントロールをデプロイします。

AWSServiceRoleForManagedServices_DetectiveControlsConfig サービスにリンクされたロールにアタッチされた管理ポリシーは、AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy です。このポリシーの更新については、「AWS 管理ポリシーの更新を高速化する」を参照してください

AMS Accelerate の検出コントロール SLR のアクセス許可

AWSServiceRoleForManagedServices_DetectiveControlsConfig 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。

- `detectivecontrols.managedservices.amazonaws.com`

このロールにアタッチされているのは `AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy` AWS マネージドポリシーです (AWS マネージドポリシー: AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy「 サービスは ロールを使用してアカウントに AMS Detective Controls の設定を作成します。これには、s3 バケット、設定ルール、アグリゲータなどのリソースのデプロイが必要です」を参照してください。 IAM エンティティ (ユーザー、グループ、ロールなど) がサービスにリンクされたロールを作成、編集、または削除できるようにする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。

AMS Accelerate の検出コントロール 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 Accelerate 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、サービスにリンクされたロールのサポートが開始された 2022 年 6 月 9 日以前に AMS Accelerate サービスを使用していた場合、アカウントに AWSServiceRoleForManagedServices_DetectiveControlsConfig ロールを作成できます。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生じた場合は、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 Accelerate 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 Accelerate の検出コントロール SLR の編集

AMS Accelerate では、AWSServiceRoleForManagedServices_DetectiveControlsConfig 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「サービスにリンクされたロールの編集」を参照してください。

AMS Accelerate の検出コントロール SLR の削除

AWSServiceRoleForManagedServices_DetectiveControlsConfig 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、、または AWS API で AMS からオフボードすると、AMS Accelerate はリソースをクリーンアップし AWS CLI、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 Accelerate 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_DetectiveControlsConfig サービスにリンクされたロールで使用される AMS Accelerate リソースを削除するには

ams-detective-controls-config-recorderアカウントが AMS でオンボーディングされたすべてのリージョンから ams-detective-controls-config-rules-cdk、 ams-detective-controls-infrastructure-cdkスタックを削除します (最初に S3 バケットを手動で空にする必要がある場合があります )。

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、、または AWS API を使用して AWS CLI、AWSServiceRoleForManagedServices_DetectiveControlsConfig 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。

## AMS Accelerate の Amazon EventBridge ルールサービスにリンクされたロール

AMS Accelerate 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 Managed Services 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 Amazon 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 AWS Managed Services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。

AMS Accelerate 用 EventBridge SLR 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

このロールにアタッチされているのは、 AWSManagedServices_EventsServiceRolePolicy AWS 管理ポリシーです (「」を参照AWS マネージドポリシー: AWSManagedServices_EventsServiceRolePolicy )。サービスは ロールを使用して、アカウントから AMS に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 Accelerate 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 Accelerate 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 Accelerate 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たときに、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生じた場合は、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 Accelerate 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 Accelerate 用の EventBridge SLR の編集

AMS Accelerate 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 Accelerate 用の 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、、または AWS API で AMS からオフボードすると、AMS Accelerate はリソースをクリーンアップし AWS CLI、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 Accelerate 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される AMS Accelerate 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。

## AMS Accelerate のサービスにリンクされたロールに連絡する

AMS Accelerate は、AWSServiceRoleForManagedServices_Contacts 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、サービスが影響を受けるリソースの既存のタグを読み取って、適切な連絡先の設定済み E メールを取得できるようにすることで、インシデントが発生したときの自動通知を容易にします。

これは、このサービスにリンクされたロールを使用する唯一のサービスです。

AWSServiceRoleForManagedServices_Contacts サービスにリンクされたロールにアタッチされた管理ポリシーは、AWSManagedServices_ContactsServiceRolePolicy です。このポリシーの更新については、「AWS 管理ポリシーの更新を高速化する」を参照してください

AMS Accelerate の問い合わせ SLR のアクセス許可

AWSServiceRoleForManagedServices_Contacts 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。

- `contacts-service.managedservices.amazonaws.com`

このロールにアタッチされているのは、AWS `AWSManagedServices_ContactsServiceRolePolicy` 管理ポリシーです (「」を参照AWS マ

ネージドポリシー: AWSManagedServices_ContactsServiceRolePolicy ）。サービスは、 ロールを使用して任意の AWS リソースのタグを読み取り、インシデントが発生したときの適切な連絡先のタグに含まれる E メールを見つけます。このロールは、AMS が影響を受けるリソースでそのタグを読み取って E メールを取得できるようにすることで、インシデントが発生したときの自動通知を容易にします。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。

> **Important**
>
> 個人情報 (PII) などの機密情報や秘匿性の高い情報はタグに格納しないでください。AMS はタグを使用して管理サービスを提供します。タグは、プライベートデータや機密データに使用することを意図していません。

AWSManagedServices_ContactsServiceRolePolicy という名前のロールアクセス許可ポリシーにより、AMS Accelerate は指定されたリソースに対して次のアクションを実行できます。

- アクション: Contacts Service が、AMS が任意の AWS リソースでインシデント通知を送信するための E メールを含むように特別に設定されたタグを読み取ることを許可します。

JSON AWSManagedServices_ContactsServiceRolePolicy は、次の ZIP: ContactsServicePolicy.zip でダウンロードできます。

AMS Accelerate の問い合わせ 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 Accelerate 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 16 日より前に AMS Accelerate 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を開始したときに、AMS Accelerate がアカウントに AWSServiceRoleForManagedServices_Contacts ロールを作成したときに、アカウントに表示されます。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生じた場合は、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 Accelerate 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 Accelerate の問い合わせ SLR の編集

AMS Accelerate では、AWSServiceRoleForManagedServices_Contacts 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 Accelerate の問い合わせ SLR の削除

AWSServiceRoleForManagedServices_Contacts 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、、または AWS API で AMS からオフボードすると、AMS Accelerate はリソースをクリーンアップし AWS CLI、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 Accelerate 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_Contacts サービスにリンクされたロールで使用される AMS Accelerate 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_Contacts 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。

## AMS Accelerate サービスにリンクされたロールでサポートされているリージョン

AMS Accelerate は、サービスが利用可能なすべてのリージョンでサービスにリンクされたロールの使用をサポートしています。詳細については、「AWS リージョンとエンドポイント」を参照してください。

## サービスにリンクされたロールの更新を高速化する

このサービスがこれらの変更の追跡を開始してからの Accelerate サービスにリンクされたロールの更新に関する詳細を表示します。このページの変更に関する自動アラートについては、Accelerate AMS Accelerate ユーザーガイドのドキュメント履歴ページの RSS フィードにサブスクライブしてください。

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| 更新されたポリシー – Deployment Toolkit | • これらの新しいアクセス許可がリソース に追加されましたarn:aws:ecr:*:*:repository/ams-cdktoolkit* 。<br>`ecr:BatchGetRepositoryScanningConfiguration`<br>`ecr:PutImageScanningConfiguration` | 2024 年 4 月 4 日 |
| 更新されたポリシー – Deployment Toolkit | • これらの新しいアクセス許可がリソース に追加されましたarn:aws:cloudformation:*:*:stack/ams-cdk-toolkit* 。<br>`cloudformation:DeleteChangeSet`<br>`cloudformation:DescribeStackEvents`<br>`cloudformation:GetTemplate`<br>`cloudformation:TagResource`<br>`cloudformation:UntagResource`<br>• これらの新しいアクセス許可がリソース に追加されましたarn:aws:ecr:*:*:repository/ams-cdktoolkit* 。<br>`ecr:CreateRepository`<br>`ecr:DeleteLifecyclePolicy` | 2023 年 5 月 9 日 |

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| | ecr:DeleteRepository<br>ecr:DeleteRepositoryPolicy<br>ecr:DescribeRepositories<br>ecr:GetLifecyclePolicy<br>ecr:ListTagsForResource<br>ecr:PutImageTagMutability<br>ecr:PutLifecyclePolicy<br>ecr:SetRepositoryPolicy<br>ecr:TagResource<br>ecr:UntagResource<br>• また、ワイルドカードを持つ既存のアクションの一部は、個々のアクションにスコープダウンされました。<br>- s3:DeleteObject*<br>+ s3:DeleteObject<br>+ s3:DeleteObjectTagging<br>+ s3:DeleteObjectVersion<br>+ s3:DeleteObjectVersionTagging<br><br>- s3:GetObject*<br>+ s3:GetObject<br>+ s3:GetObjectAcl<br>+ s3:GetObjectAttributes<br>+ s3:GetObjectLegalHold<br>+ s3:GetObjectRetention<br>+ s3:GetObjectTagging<br>+ s3:GetObjectVersion<br>+ s3:GetObjectVersionAcl<br>+ s3:GetObjectVersionAttributes<br>+ s3:GetObjectVersionForReplication<br>+ s3:GetObjectVersionTagging<br>+ s3:GetObjectVersionTorrent<br><br>- cloudformation:UpdateTermination*<br>+ cloudformation:UpdateTerminationProtection | |

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| 更新されたポリシー – Detective Controls | • CloudFormation アクションは、セキュリティおよびアクセスチームに確認した後、さらに絞り込まれました。<br>• Lambda アクションはオンボーディング/オフのオンボーディングに影響を与えないため、ポリシーから削除されました | 2023 年 4 月 10 日 |
| 更新されたポリシー – Detective Controls | ポリシーを更新し、アクセス許可の境界ポリシーを追加しました。 | 2023 年 3 月 21 日 |
| 新しいサービスにリンクされたロール – SLR への問い合わせ | Accelerate は、問い合わせサービスの新しいサービスにリンクされたロールを追加しました。<br><br>このロールは、サービスが影響を受けるリソースの既存のタグを読み取って、適切な連絡先の設定済み E メールを取得できるようにすることで、インシデントが発生したときの自動通知を容易にします。 | 2023 年 2 月 16 日 |
| 新しいサービスにリンクされたロール – EventBridge | Accelerate は、Amazon EventBridge ルールに新しいサービスにリンクされたロールを追加しました。<br><br>このロールは、AWS Managed Services 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 Amazon 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 AWS Managed Services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。 | 2023 年 2 月 7 日 |

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| 更新されたサービスにリンクされたロール – Deployment Toolkit | 新しい S3 アクセス許可を使用して、更新された AWSServiceRoleForAWSManagedServicesDeployment Toolkit を高速化します。<br><br>これらの新しいアクセス許可が追加されました。<br><br>`"s3:GetLifecycleConfiguration", "s3:GetBucketLogging", "s3:ListBucket", "s3:GetBucketVersioning", "s3:PutLifecycleConfiguration", "s3:GetBucketLocation", "s3:GetObject*"` | 2023 年 1 月 30 日 |
| Accelerate が変更の追跡を開始 | Accelerate は、サービスにリンクされたロールの変更の追跡を開始しました。 | 2022 年 11 月 30 日 |
| 新しいサービスにリンクされたロール – Detective Controls | Accelerate は、 Accelerate 検出コントロールをデプロイするための新しいサービスにリンクされたロールを追加しました。<br><br>AWS Managed Services はこのサービスにリンクされたロールを使用して、config-recorder、config ルール、S3 バケット検出コントロールをデプロイします。 | 2022 年 10 月 13 日 |
| 新しいサービスにリンクされたロール – Deployment Toolkit | Accelerate は、 Accelerate インフラストラクチャをデプロイするための新しいサービスにリンクされたロールを追加しました。<br><br>このロールは、AMS Accelerate インフラストラクチャをカスタマーアカウントにデプロイします。 | 2022 年 6 月 9 日 |

# AWS AMS Accelerate の マネージドポリシー

AWS 管理ポリシーは、 によって作成および管理されるスタンドアロンポリシーです AWS。 AWS 管理ポリシーは、ユーザー、グループ、ロールにアクセス許可の割り当てを開始できるように、多くの一般的なユースケースにアクセス許可を付与するように設計されています。

AWS 管理ポリシーは、すべての AWS お客様が使用できるため、特定のユースケースに対して最小特権のアクセス許可を付与しない場合があることに注意してください。ユースケースに固有のカスタマー管理ポリシーを定義して、アクセス許可を絞り込むことをお勧めします。

AWS 管理ポリシーで定義されているアクセス許可は変更できません。が AWS マネージドポリシーで定義されたアクセス許可 AWS を更新すると、ポリシーがアタッチされているすべてのプリンシパル ID (ユーザー、グループ、ロール) に影響します。 AWS は、新しい が起動されるか、新しい API オペレーション AWS のサービス が既存のサービスで使用できるようになったときに、 AWS マネージドポリシーを更新する可能性が高くなります。

詳細については「IAM ユーザーガイド」の「AWS マネージドポリシー」を参照してください。

変更の表については、「」を参照してくださいAWS 管理ポリシーの更新を高速化する。

## AWS マネージドポリシー: AWSManagedServices_AlarmManagerPermissionsBoundary

AWS Managed Services (AMS) は `AWSManagedServices_AlarmManagerPermissionsBoundary` AWS マネージドポリシーを使用します。この AWS管理ポリシーは、AWSManagedServices_AlarmManager_ServiceRolePolicy で使用され、AWSServiceRoleForManagedServices_AlarmManager によって作成された IAM ロールのアクセス許可を制限します。

このポリシーは、 の一部として作成された IAM ロールAlarm Manager の仕組み、Config AWS 評価、 AWS Config 読み取りによる Alarm Manager 設定の取得、必要な Amazon CloudWatch アラームの作成などのオペレーションを実行するアクセス許可を付与します。

`AWSManagedServices_AlarmManagerPermissionsBoundary` ポリシーは、`AWSServiceRoleForManagedServices_DetectiveControlsConfig`サービスにリンクされたロールにアタッチされます。このロールの更新については、「」を参照してくださいサービスにリンクされたロールの更新を高速化する。

このポリシーは IAM アイデンティティにアタッチできます。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- AWS Config – 設定ルールを評価し、リソース設定を選択するためのアクセス許可を付与します。
- AWS AppConfig – AlarmManager 設定を取得するアクセス許可を付与します。
- Amazon S3 – AlarmManager バケットとオブジェクトを操作するアクセス許可を付与します。
- Amazon CloudWatch – AlarmManager マネージドアラームとメトリクスを読み取って配置するアクセス許可を付与します。
- AWS Resource Groups and Tags – リソースタグを読み取るアクセス許可を付与します。
- Amazon EC2 – Amazon EC2 リソースを読み取るアクセス許可を付与します。
- Amazon Redshift – Redshift インスタンスとクラスターを読み取るアクセス許可を付与します。
- Amazon FSx – ファイルシステム、ボリューム、リソースタグを記述するアクセス許可を付与します。
- Amazon CloudWatch Synthetics – Synthetics リソースを読み取るアクセス許可を付与します。
- Amazon Elastic Kubernetes Service – Amazon EKS クラスターを記述するアクセス許可を付与します。
- Amazon ElastiCache – リソースを記述するアクセス許可を付与します。

この ZIP: RecommendedPermissionBoundary.zip でポリシーファイルをダウンロードできます。

## AWS マネージドポリシー: AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy

AWS Managed Services (AMS) は AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy AWS マネージドポリシーを使用します。この AWS管理ポリシーは、AWSServiceRoleForManagedServices_DetectiveControlsConfigサービスにリンクされたロールにアタッチされます (「」を参照AMS Accelerate のサービスにリンクされたロールを Detective が制御する )。AWSServiceRoleForManagedServices_DetectiveControlsConfig サービスにリンクされたロールの更新については、「」を参照してくださいサービスにリンクされたロールの更新を高速化する。

このポリシーは、サービスリンクロールがユーザーに代わってアクションを完了することを許可します。

AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy ポリシーを IAM エンティティにアタッチできます。

詳細については、「AMS Accelerate 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。

アクセス許可の詳細

このポリシーには、Detective Controls AWS Managed Services に必要なすべてのリソースをデプロイおよび設定するための以下のアクセス許可があります。

- `CloudFormation` – AMS Detective Controls が s3 バケット、設定ルール、config-recorder などのリソースを使用して CloudFormation スタックをデプロイできるようにします。
- `AWS Config` – AMS Detective Controls が AMS 設定ルールを作成し、アグリゲータを設定し、リソースにタグを付けることを許可します。
- `Amazon S3` – AMS Detective Controls が s3 バケットを管理できるようにします。

JSON ポリシーファイルは、次の ZIP でダウンロードできます: DetectiveControlsConfig_ServiceRolePolicy.zip。

## AWS マネージドポリシー: AWSManagedServicesDeploymentToolkitPolicy

AWS Managed Services (AMS) は `AWSManagedServicesDeploymentToolkitPolicy` AWS マネージドポリシーを使用します。この AWS管理ポリシーは、AWSServiceRoleForAWSManagedServicesDeploymentToolkitサービスにリンクされたロールにアタッチされます (「」を参照AMS Accelerate のサービスにリンクされたロールのデプロイツールキット)。このポリシーは、サービスリンクロールがユーザーに代わってアクションを完了することを許可します。このポリシーを IAM エンティティにアタッチすることはできません。詳細については、「AMS Accelerate 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。

`AWSServiceRoleForManagedServicesDeploymentToolkitPolicy` サービスにリンクされたロールの更新については、「」を参照してくださいサービスにリンクされたロールの更新を高速化する。

アクセス許可の詳細

このポリシーには、Detective Controls AWS Managed Services に必要なすべてのリソースをデプロイおよび設定するための以下のアクセス許可があります。

- `CloudFormation` – AMS Deployment Toolkit が CDK に必要な S3 リソースを使用して CFN スタックをデプロイできるようにします。
- `Amazon S3` – AMS Deployment Toolkit が S3 バケットを管理できるようにします。
- `Elastic Container Registry` – AMS Deployment Toolkit は、AMS CDK アプリケーションに必要なアセットをデプロイするために使用される ECR リポジトリを管理できます。

JSON ポリシーファイルは、次の ZIP でダウンロードできます。AWSManagedServicesDeploymentToolkitPolicy.zip。

## AWS マネージドポリシー: AWSManagedServices_EventsServiceRolePolicy

AWS Managed Services (AMS) は AWS `AWSManagedServices_EventsServiceRolePolicy` 管理ポリシーを使用します。この AWS管理ポリシーは、AWSServiceRoleForManagedServices_Eventsサービスにリンクされたロールにアタッチされます。このポリシーは、サービスリンクロールがユーザーに代わってアクションを完了することを許可します。このポリシーを IAM エンティティにアタッチすることはできません。詳細については、「AMS Accelerate 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。

`AWSServiceRoleForManagedServices_Events` サービスにリンクされたロールの更新については、「」を参照してくださいサービスにリンクされたロールの更新を高速化する。

アクセス許可の詳細

このポリシーには、Amazon EventBridge がアカウントから AWS Managed Servicesにアラーム状態変更情報を配信できるようにする以下のアクセス許可があります。

- `events` – Accelerate が Amazon EventBridge マネージドルールを作成できるようにします。このルールは、 アカウントから にアラーム状態変更情報を配信 AWS アカウント するために必要な インフラストラクチャです AWS Managed Services。

この ZIP: EventsServiceRolePolicy.zip で JSON ポリシーファイルをダウンロードできます。

## AWS マネージドポリシー: AWSManagedServices_ContactsServiceRolePolicy

AWS Managed Services (AMS) は AWS `AWSManagedServices_ContactsServiceRolePolicy` 管理ポリシーを使用します。この AWS管理ポリシー

は、AWSServiceRoleForManagedServices_Contactsサービスにリンクされたロールにアタッチされます (「」を参照AMS Accelerate の問い合わせ SLR の作成 )。このポリシーにより、AMS Contacts SLR は AWS リソースのリソースタグとその値を確認できます。このポリシーを IAM エンティティにアタッチすることはできません。詳細については、「AMS Accelerate 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。

> **Important**
>
> 個人情報 (PII) などの機密情報や秘匿性の高い情報はタグに格納しないでください。AMS はタグを使用して管理サービスを提供します。タグは、プライベートデータや機密データに使用することを意図していません。

AWSServiceRoleForManagedServices_Contacts サービスにリンクされたロールの更新については、「」を参照してくださいサービスにリンクされたロールの更新を高速化する。

アクセス許可の詳細

このポリシーには、Contacts SLR がリソースタグを読み取って、事前に設定したリソース連絡先情報を取得できるようにする次のアクセス許可があります。

- IAM – Contacts サービスが IAM ロールと IAM ユーザーのタグを確認できるようにします。
- Amazon EC2 – Contacts サービスが Amazon EC2 リソースのタグを確認できるようにします。
- Amazon S3 – Contacts Service が Amazon S3 バケットのタグを確認できるようにします。このアクションでは、 条件を使用して、AMS が HTTP 認可ヘッダー、SigV4 署名プロトコル、および TLS 1.2 以降の HTTPS を使用してバケットタグにアクセスするようにします。詳細については、「認証方法」とAmazon S3 署名バージョン 4 認証固有のポリシーキー」を参照してください。
- Tag – Contacts サービスが他の AWS リソースのタグを確認できるようにします。

- 「iam:ListRoleTags」、「iam:ListUserTags」、「tag:GetResources」、「tag:GetTagKeys」、「tag:GetTagValues」、「ec2:DescribeTags」、「s3:GetBucketTagging」

この ZIP: ContactsServicePolicy.zip で JSON ポリシーファイルをダウンロードできます。

## AWS 管理ポリシーの更新を高速化する

このサービスがこれらの変更の追跡を開始してからの Accelerate の AWS マネージドポリシーの更新に関する詳細を表示します。

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| 更新されたポリシー – Deployment Toolkit | • これらの新しいアクセス許可がリソース に追加されましたarn:aws:ecr:*:*:repository/ams-cdktoolkit* 。<br>`ecr:BatchGetRepositoryScanningConfiguration`<br>`ecr:PutImageScanningConfiguration` | 2024 年 4 月 4 日 |
| 更新されたポリシー – Deployment Toolkit | • これらの新しいアクセス許可がリソース に追加されましたarn:aws:cloudformation:*:*:stack/ams-cdk-toolkit* 。<br>`cloudformation:DeleteChangeSet`<br>`cloudformation:DescribeStackEvents`<br>`cloudformation:GetTemplate`<br>`cloudformation:TagResource`<br>`cloudformation:UntagResource`<br>• これらの新しいアクセス許可がリソース に追加されましたarn:aws:ecr:*:*:repository/ams-cdktoolkit* 。<br>`ecr:CreateRepository`<br>`ecr:DeleteLifecyclePolicy`<br>`ecr:DeleteRepository`<br>`ecr:DeleteRepositoryPolicy`<br>`ecr:DescribeRepositories`<br>`ecr:GetLifecyclePolicy`<br>`ecr:ListTagsForResource`<br>`ecr:PutImageTagMutability`<br>`ecr:PutLifecyclePolicy` | 2023 年 5 月 9 日 |

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| | <pre>ecr:SetRepositoryPolicy<br>ecr:TagResource<br>ecr:UntagResource</pre><br>• また、ワイルドカードを持つ既存のアクションの一部は、個々のアクションにスコープダウンされました。<br><pre>- s3:DeleteObject*<br><br>+ s3:DeleteObject<br>+ s3:DeleteObjectTagging<br>+ s3:DeleteObjectVersion<br>+ s3:DeleteObjectVersionTagging<br><br>- s3:GetObject*<br>+ s3:GetObject<br>+ s3:GetObjectAcl<br>+ s3:GetObjectAttributes<br>+ s3:GetObjectLegalHold<br>+ s3:GetObjectRetention<br>+ s3:GetObjectTagging<br>+ s3:GetObjectVersion<br>+ s3:GetObjectVersionAcl<br>+ s3:GetObjectVersionAttributes<br>+ s3:GetObjectVersionForReplication<br>+ s3:GetObjectVersionTagging<br>+ s3:GetObjectVersionTorrent<br><br>- cloudformation:UpdateTermination*<br>+ cloudformation:UpdateTerminationProt<br>ection</pre> | |
| 更新されたポリシー – Detective Controls | • CloudFormation アクションは、セキュリティおよびアクセスチームに確認した後、さらに絞り込まれました。<br>• Lambda アクションはオンボーディング/オフのオンボーディングに影響を与えないため、ポリシーから削除されました | 2023 年 4 月 10 日 |

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| 更新されたポリシー – Detective Controls | `ListAttachedRolePolicies` アクションはポリシーから削除されます。アクションにはリソースがワイルドカード (*) として含まれていました。「list」は非ミューテーションアクションであるため、すべてのリソースへのアクセスが許可され、ワイルドカードは許可されません。 | 2023 年 3 月 28 日 |
| 更新されたポリシー – Detective Controls | ポリシーを更新し、アクセス許可の境界ポリシーを追加しました。 | 2023 年 3 月 21 日 |
| 新しいポリシー – Contacts Service | Accelerate は、リソースタグからアカウントの連絡先情報を確認する新しいポリシーを追加しました。<br><br>Accelerate は、事前に設定したリソース連絡先情報を取得できるように、リソースタグを読み取る新しいポリシーを追加しました。 | 2023 年 2 月 16 日 |
| 新しいポリシー – Events Service | Accelerate は、アカウントから AWS Managed Services にアラーム状態変更情報を配信する新しいポリシーを追加しました。<br><br>必要な Amazon EventBridge マネージドルールを作成するためのAlarm Manager の仕組みアクセス許可の一部として作成された IAM ロールを付与します。 | 2023 年 2 月 7 日 |
| 更新されたポリシー – Deployment Toolkit | Accelerate からの顧客のオフボーディングをサポートする S3 アクセス許可を追加しました。 | 2023 年 1 月 30 日 |
| 新しいポリシー – Detective Controls | サービスにリンクされたロール AMS Accelerate のサービスにリンクされたロールを Detective が制御するが Accelerate 検出コントロールをデプロイするためのアクションを完了できるようにします。 | 2022 年 12 月 19 日 |

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| 新しいポリシー – Alarm Manager | Accelerate は、アラームマネージャータスクを実行するアクセス許可を付与する新しいポリシーを追加しました。<br><br>Config AWS 評価、アラームマネージャー設定を取得するための読み取り AWS 設定、必要な Amazon CloudWatch アラームの作成などのオペレーションを実行するアクセスAlarm Manager の仕組み許可の一部として作成された IAM ロールを付与します。 | 2022 年 11 月 30 日 |
| Accelerate が変更の追跡を開始 | Accelerate は、 AWS マネージドポリシーの変更の追跡を開始しました。 | 2022 年 11 月 30 日 |
| 新しいポリシー – Deployment Toolkit | Accelerate は、デプロイタスクにこのポリシーを追加しました。<br><br>サービスにリンクされたロール AWSServiceRoleForAWSManagedServicesDeploymentToolkit に、デプロイ関連の Amazon S3 バケットと CloudFormation スタックにアクセスして更新するためのアクセス許可を付与します。 | 2022 年 6 月 9 日 |

# Accelerate でのデータ保護

AMS Accelerate は、Amazon GuardDuty、Amazon Macie (オプション ) 、その他の内部独自のツールやプロセス AWS のサービス などのネイティブを活用して、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 Accelerate は最初のトリアージとアラームへの応答について責任を負います。AMS レスポンスプロセスは NIST 標準に基づいています。AMS Accelerate 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 Accelerate 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 Accelerate 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用オペレーターによる 24 時間 365 follow-the-sunサポートを

提供します。Accelerate は、社内のセキュリティエキスパート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。

結果に基づいて、Accelerate はプロアクティブにお客様とやり取りします。アクティビティが不正または疑わしいことが判明した場合、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。Accelerate がアクションを実行する前に、影響を確認する必要がある GuardDuty によって生成された特定の検出結果タイプがあります。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 でモニタリングする

AMS Accelerate は、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ために Amazon Macie をサポートしており、これを使用するのがベストプラクティスです。

Amazon S3 バケットで定期的に を実行するように Macie を設定できます。これにより、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、必要に応じて検出結果を修復します。

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。

## GuardDuty によるモニタリング

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、悪意のあるアクティビティを特定します。これには、権限のエスカレーション、公開された認証情報の使用、悪意のある IP アドレスやドメインとの通信などの問題が含まれる場合があります。GuardDuty は、不正なインフラストラクチャのデプロイ、 にデプロイされたインスタンス、使用したことのない AWS リージョンなど、侵害の兆候がないか AWS アカウント アクセス動作をモニタリングします。GuardDuty は、パスワードの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、異常な API コールも検出します。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、次の手順を実行します。

1. https://console.aws.amazon.com/guardduty/ で 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 抑制ルールを使用して検出結果をフィルタリングする

抑制ルールは、フィルター属性と値を組み合わせた一連の基準です。抑制ルールを使用して、誤検出の検出結果や既知のアクティビティなど、対処する予定のない低値の検出結果をフィルタリングできます。検出結果をフィルタリングすると、環境に最も影響を与える可能性のあるセキュリティ脅威を簡単に認識できます。

結果をフィルタリングするために、サプレッションルールは、指定した条件に一致する新しい検出結果を自動的にアーカイブします。アーカイブされた検出結果は、 AWS Security Hub、Amazon S3、または CloudTrail Events に送信されません。したがって、Security Hub またはサードパーティーの SIEM アラートおよびチケット発行アプリケーションを介して GuardDuty の検出結果を使用すると、サプレッションフィルターは実行不可能なデータを削減します。

AMS には、マネージドアカウントの抑制ルールを識別するための一連の条件が定義されています。マネージドアカウントがこの基準を満たすと、AMS はフィルターを適用し、デプロイされたサプレッションフィルターの詳細を示すサービスリクエスト (SR) を作成します。

SR を介して AMS と通信して、抑制フィルターを変更または元に戻すことができます。

### アーカイブされた結果を表示する

GuardDuty は、検出結果が抑制ルールと一致しても検出結果を生成し続けます。抑制された検出結果はアーカイブ済みとしてマークされます。GuardDuty はアーカイブされた検出結果を 90 日間保存します。GuardDuty コンソールで 90 日間アーカイブされた結果を表示するには、結果テーブルからアーカイブされた を選択します。または、Service.archived の findingCriteria が true に等しい ListFindings API を使用して、GuardDuty API を介してアーカイブされた検出結果を表示します。

### 抑制ルールの一般的なユースケース

次の検出結果タイプには、抑制ルールを適用する一般的ユースケースがあります。

- Recon:EC2/Portscan: サプレッションルールを使用して、承認された脆弱性スキャナーを使用するときに検出結果を自動的にアーカイブします。

- UnauthorizedAccess:EC2/SSHBruteForce: 踏み台インスタンスを対象としている場合、サプレッションルールを使用して検出結果を自動的にアーカイブします。
- Recon:EC2/PortProbeUnprotectedPort: サプレッションルールを使用して、意図的に公開されたインスタンスをターゲットにした場合に、検出結果を自動的にアーカイブします。

## Amazon Route 53 Resolver DNS Firewall によるモニタリング

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 ファイアウォールで、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`の `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。
- サービスリクエストを作成します。

## AMS Accelerate でのデータ暗号化

AMS Accelerate は、データ暗号化 AWS のサービス に複数の を使用します。

Amazon Simple Storage Service には、転送中および保管中のデータを保護するオブジェクト暗号化オプションがいくつか用意されています。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。

# AWS Identity and Access Management AMS Accelerate での

AWS Identity and Access Management 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 により、誰を認証 (サインイン) し、誰にリソースの使用を承認する (ア

クセス権限を持たせる) かを制御します。AMS Accelerate の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。

AMS Accelerate では、アクセス管理ソリューション、アクセスポリシー、関連プロセスなど、 AWS アカウント とその基盤となるリソースへのアクセスを管理する責任があります。つまり、 AWS コンソールまたは AWS APIs にアクセスするためのユーザーライフサイクル、ディレクトリサービスのアクセス許可、およびフェデレーティッド認証システムを管理します。アクセスソリューションの管理に役立つように、AMS Accelerate は一般的な IAM の設定ミスを検出する AWS Config ルールをデプロイし、修復通知を送信します。詳細については、AWS Config 管理ルールを参照してください。

## AMS Accelerate での ID による認証

AMS は、IAM ID 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引き受けることができます。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 は次の IAM ロールを使用します。

> **Note**
>
> AMS アクセスロールを使用すると、AMS オペレーターはリソースにアクセスして AMS 機能を提供できます (「」を参照サービスの説明 )。これらのロールを変更すると、これらの機能を提供する機能が妨げられる可能性があります。AMS アクセスロールを変更する必要がある場合は、Cloud Architect を参照してください。

| ロール名 | 説明 |
| --- | --- |
| 使用ユーザー (エンティティ): AMS Access Service のみ | |
| ams-access-management | オンボーディング中に手動でデプロイされます。アクセスロールをデプロイまたは更新するための AMS アクセスによってのみ引き受けら |

| ロール名 | 説明 |
| --- | --- |
| | れます。アクセスロールの今後の更新のためにオンボーディング後も、 はアカウントに残ります。 |
| 使用ユーザー (エンティティ): AMS オペレーション | |
| ams-access-admin-operations | このロールには、 アカウントで運用するための管理権限がありますが、Amazon Simple Storage Service、Amazon Relational Database Service、Amazon DynamoDB、Amazon Redshift、Amazon ElastiCache など、データストアとして一般的に使用される AWS サービスの顧客コンテンツの読み取り、書き込み、削除を行う権限はありません。このロールを引き受けることができる AMS の個人はごくわずかです。 |
| ams-access-operations | この AMS オペレーションロールには、アカウントで管理タスクを実行するアクセス許可があります。このロールには、Amazon Simple Storage Service、Amazon Relational Database Service、Amazon DynamoDB、Amazon Redshift、Amazon ElastiCache など、データストアとして一般的に使用される AWS サービスの顧客コンテンツに対する読み取り、書き込み、または削除のアクセス許可はありません。 AWS Identity and Access Management 書き込みオペレーションを実行するアクセス許可もこのロールから除外されます。 |

| ロール名 | 説明 |
| --- | --- |
| ams-access-read-only | この AMS 読み取り専用ロールは、AMS アカウントの読み取り専用アクセス許可に制限されます。Amazon S3、Amazon RDS、DynamoDB、Amazon Redshift、ElastiCache など、データストアとして一般的に使用される AWS サービスの顧客コンテンツへの読み取りアクセス許可は、このロールでは付与されません。 |
| 使用ユーザー (エンティティ): AMS オペレーションと AMS サービス | |
| ams_ssm_automation_role | アカウント内で SSM Automation ドキュメントを実行する AWS Systems Manager ために によって引き受けられます。 |
| ams_ssm_automation_role | |
| 使用ユーザー (エンティティ): AMS セキュリティ | |
| ams-access-security-analyst | この AMS セキュリティロールには、専用のセキュリティアラートモニタリングとセキュリティインシデント処理を実行するアクセス許可が AMS アカウントに付与されています。このロールを引き受けることができる AMS セキュリティ担当者はほとんどいません。Amazon S3、Amazon RDS、Amazon DynamoDB、Amazon Redshift、ElastiCache など、データストアとして一般的に使用される AWS サービスの顧客コンテンツへの読み取りアクセス許可は、このロールでは付与されません。 |

| ロール名 | 説明 |
| --- | --- |
| ams-access-security-analyst-read-only | この AMS セキュリティロールは、専用のセキュリティアラートモニタリングとセキュリティインシデント処理を実行するための AMS アカウントの読み取り専用アクセス許可に制限されています。Amazon S3、Amazon RDS、Amazon DynamoDB、Amazon Redshift、ElastiCache など、データストアとして一般的に使用される AWS サービスの顧客コンテンツへの読み取りアクセス許可は、このロールでは付与されません。 |
| 使用ユーザー (エンティティ): AWS サービス | |
| ams-access-admin | この AMS 管理者ロールには、制限なしでアカウントを操作するための完全なアクセス許可があります。管理者ロールを引き受けることができるのは、AMS 内部サービス (スコープダウンセッションポリシーを使用) のみです。 |
| ams-opscenter-eventbridge-role | Amazon EventBridge が AMS 固有の AWS Config ルール 修復ワークフローの一部として AWS Systems Manager OpsItems を作成することを引き受けます。 |
| AMSOSConfigurationCustomerInstanceRole | この IAM ロールは、AMS OS-Configuration サービスが必要な IAM ポリシーがないことを検出すると、Amazon EC2 インスタンスに適用されます。これにより、Amazon EC2 インスタンスは AWS Systems Manager、、Amazon CloudWatch、および Amazon EventBridge サービスとやり取りできます。また、Windows インスタンスへの RDP アクセスを有効にする AMS カスタム管理ポリシーもアタッチされています。 |

| ロール名 | 説明 |
| --- | --- |
| mc-patch-glue-service-role | データ変換を実行し、AMS パッチレポートジェネレーターを準備するために AWS Glue ETL ワークフローによって引き受けられます。 |
| 使用ユーザー (エンティティ): AMS サービス | |
| ams-alarm-manager-AWSManagedServices AlarmManagerDe-<8 桁のハッシュ > | 新しい AWS AppConfig デプロイの評価を実行する AWS Config ルール ために、AMS アカウント内の AMS アラームマネージャーインフラストラクチャによって引き受けられます。 |
| ams-alarm-manager-AWSManagedServices AlarmManagerRe-<8 桁のハッシュ > | AMS アカウント内の AMS アラームマネージャー修復インフラストラクチャによって引き受けられ、修復のためのアラームの作成または削除を許可します。 |
| ams-alarm-manager-AWSManagedServices AlarmManagerSS-<8 桁のハッシュ > | AMS アカウント内で AMS アラームマネージャー修復サービスを呼び出す AWS Systems Manager ために によって引き受けられます。 |
| ams-alarm-manager-AWSManagedServices AlarmManagerTr-<8 桁のハッシュ > | 定期的な AMS AWS Config ルール 評価を行うために AWS 、アカウント内の AMS アラームマネージャーインフラストラクチャによって引き受けられます。 |
| ams-alarm-manager-AWSManagedServices AlarmManagerVa-<8 桁のハッシュ > | 必要なアラームがアカウントに存在することを確認するために、AMS アカウント内の AMS アラームマネージャーインフラストラクチャによって引き受けられます AWS 。 |
| ams-backup-iam-role | このロールは、アカウント AWS Backup 内でを実行するために使用されます。 |

| ロール名 | 説明 |
| --- | --- |
| ams-monitoring-AWSManagedServicesLogGroupLimitLamb-<8 桁のハッシュ > | Amazon CloudWatch Logs グループの制限を評価し、サービスクォータと比較するために、AMS アカウントの AMS ログ記録とモニタリングインフラストラクチャによって引き受けられます。 |
| ams-monitoring-AWSManagedServicesRDSMonitoringRDSE-<8 桁のハッシュ > | Amazon RDS イベントを Amazon CloudWatch Events に転送するために、AMS アカウントの AMS ログ記録とモニタリングインフラストラクチャによって引き受けられます。 |
| ams-monitoring-AWSManagedServicesRedshiftMonitorin-<8 桁のハッシュ > | Amazon Redshift イベント (CreateCluster と DeleteCuster) を Amazon CloudWatch Events に転送するために、AMS アカウントの AMS ログ記録とモニタリングインフラストラクチャによって引き受けられます。 |
| ams-monitoring-infrastruc-AWSManagedServicesMonito-<8 桁のハッシュ > | AMS アカウントの AMS ログ記録とモニタリングインフラストラクチャによって引き受けられ、Amazon Simple Notification Service にメッセージを発行して、アカウントが必要なすべてのデータを報告していることを検証します。 |
| ams-opscenter-role | アカウントのアラートに関連する AWS Systems Manager OpsItems を管理するために、AMS アカウントの AMS 通知管理システムによって引き受けられます。 |
| ams-opsitem-autoexecution-role | アカウントのリソースに関連するアラートをモニタリングするための SSM ドキュメントを使用して自動修復を処理するために、AMS 通知管理システムによって引き受けられます。 |
| ams-patch-infrastructure-amspatchconfigruleroleC1-<8-digit hash> | AMS パッチリソースを評価し、スタック CloudFormation のドリフトを検出 AWS Config するために によって引き受けられます。 |

| ロール名 | 説明 |
| --- | --- |
| ams-patch-infrastructure-amspatchcwruleopsitemams-<8 桁のハッシュ > | パッチ適用の失敗に対して AWS Systems Manager OpsItems を作成するために Amazon EventBridge が引き受けます。 |
| ams-patch-infrastructure-amspatchservicebusamspat-<8 桁のハッシュ > | AWS Systems Manager メンテナンスウィンドウの状態変更通知のために AMS パッチオーケストレーターイベントバスにイベントを送信することを Amazon EventBridge が引き受けます。 |
| ams-patch-reporting-infra-amspatchreportingconfigr-<8 桁のハッシュ > | によって引き受けられ AWS Config 、AMS Patch レポートリソースを評価し、 CloudFormation スタックのドリフトを検出します。 |
| ams-resource-tagger-AWSManagedServicesResourceTagg-<8 桁のハッシュ > | 新しい AWS AppConfig デプロイ時に AWS Config ルール 評価を実行するために、AMS アカウント内の AMS Resource Tagger インフラストラクチャによって引き受けられます。 |
| ams-resource-tagger-AWSManagedServicesResourceTagg-<8 桁のハッシュ > | マネージドリソースに必要な AWS タグが存在することを検証するために、AMS アカウント内の AMS Resource Tagger インフラストラクチャによって引き受けられます。 |
| ams-resource-tagger-AWSManagedServicesResourceTagg-<8 桁のハッシュ > | AMS アカウントで AMS Resource Tagger 修復ワークフローを呼び出す AWS Systems Manager ために が引き受けます。 |
| ams-resource-tagger-AWSManagedServicesResourceTagg-<8 桁のハッシュ > | マネージドリソースの AWS タグを作成または削除するために、AMS アカウント内の AMS Resource Tagger 修復インフラストラクチャによって引き受けられます。 |

| ロール名 | 説明 |
| --- | --- |
| ams-resource-tagger-AWSManagedServicesResourceTagg-<8 桁のハッシュ > | 定期的な AMS Config ルール評価を行うために AWS 、アカウント内の AMS Resource Tagger インフラストラクチャによって引き受けられます。 |
| ams_os_configuration_event_rule_role-<AWS リージョン > | アカウントから正しいリージョンの AMS OS-Configuration サービス EventBus にイベントを転送するために Amazon EventBridge EventBridge が引き受けます。 |
| mc-patch-reporting-service | AMS パッチデータアグリゲータとレポートジェネレーターによって引き受けられます。 |

> **Note**
>
> これは、ams-access-management ロールのテンプレートです。これは、オンボーディング時にクラウドアーキテクト (CAs) がアカウント内に手動でデプロイするスタックです: management-role.yaml。
> これは、さまざまなアクセスロールとアクセスレベルのテンプレートです。ams-access-read-only、ams-access-operations、ams-access-admin-operations、ams-access-admin: accelerate-roles.yaml。

ハッシュを含む AWS Cloud Development Kit (AWS CDK) （ AWS CDK) 識別子の詳細については、UniqueIDs」を参照してください。

AMS Accelerate 機能サービスは、アカウントへのプログラムによるアクセスのために ams-access-admin ロールを引き受けますが、セッションポリシーの範囲はそれぞれの機能サービス (パッチ、バックアップ、モニタリングなど) に限定されます。

AMS Accelerate は、業界のベストプラクティスに従ってコンプライアンス資格を満たし、維持します。AMS Accelerate のアカウントへのアクセスは CloudTrail に記録され、変更の追跡を通じて確認することもできます。この情報を取得するために使用できるクエリについては、「」を参照してくださいAMS Accelerate アカウントの変更の追跡。

# ポリシーを使用したアクセスの管理

Operations Engineers、Cloud Architects、Cloud Service Delivery Manager (CSDMs) など、さまざまな AMS Accelerate サポートチームでは、サービスリクエストやインシデントに対応するためにアカウントへのアクセスが必要になる場合があります。アクセスは、ビジネス上の根拠、サービスリクエスト、オペレーション項目、サポートケースなどのコントロールを強制する内部 AMS アクセスサービスによって管理されます。デフォルトのアクセスは読み取り専用で、すべてのアクセスが追跡および記録されます。「」も参照してくださいAMS Accelerate アカウントの変更の追跡。

## IAM リソースの検証

AMS Accelerate アクセスシステムは、定期的に (少なくとも 24 時間ごとに) アカウントでロールを引き受け、すべての IAM リソースが期待どおりに動作することを検証します。

アカウントを保護するために、AMS Accelerate には、上記の IAM ロールの存在とステータス、およびアタッチされたポリシーをモニタリングおよびアラームする「canary」があります。Canary は定期的に ams-access-read-only ロールを引き受け、アカウントに対して CloudFormation および IAM API コールを開始します。Canary は AMS Accelerate アクセスロールのステータスを評価し、常に変更されておらずup-to-dateであることを確認します。このアクティビティは、アカウントに CloudTrail ログを作成します。

Canary の AWS Security Token Service （ AWS STS) セッション名は、CloudTrail に表示される AMS-Access-Roles-Auditor-{uuid4()} で、次の API コールが発生します。

- Cloud Formation API コール: `describe_stacks()`
- IAM API コール :
  - `get_role()`
  - `list_attached_role_policies()`
  - `list_role_policies()`
  - `get_policy()`
  - `get_policy_version()`
  - `get_role_policy()`

# 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準備し、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、トリアージと分析の実行、分析の通知、調査と封じ込めアクティビティの実行、イベント分析の投稿を行います。

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。一部のシナリオにおける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ンダーは、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、お客様と提携す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。

- どのワークロードがどのアカウントで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調査中や封じ込めの決定時に必要となる可能性の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や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理解します。
- 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 上の son on) 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 アカウントの管理中、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 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工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た後、次の復旧段階に進む前に、脅威の原因を完全に排除してシステムを保護するには、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、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、長期的な変更 (インフラストラクチャの変更など) と、エンタープライズを可能な限り安全に保つための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にパッチが適用され、最近の攻撃や将来の攻撃の可能性に対して強化されていますか (複数可 ) 。
- 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チーム) 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 はルートの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。

ルートの計画使用量を 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。

ルートユーザーの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 および 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して、ルートユーザーの計画された使用について AMS にアドバイスします。

AMS で GameDays を定期的に実施して、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 セキュリティ対応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。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ために、ログが提供されます。

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日時
- アクティビティレコード: root 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 は影響を受けるお客様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によってデプロイされたサードパーティー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、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 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 Operations は、調査、データ収集、トリアージ、分析を行い、次に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 を使用する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承諾の決定を行う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関係を実行します。

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および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が観察されたアカウント
- 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: アラートがトリガーされたのはいつですか？
- 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、インシデントは更新され、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 はお客様と連携して、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。

# Accelerate のセキュリティイベントのログ記録とモニタリング

AMS Accelerate に登録されているアカウントは、ノイズを減らし、真のインシデントの兆候を特定するために最適化された CloudWatch Events and Alarms のベースラインデプロイで設定されます。AMS Accelerate は、アカウントモニタリングに GuardDuty も採用しています。詳細については、「GuardDuty によるモニタリング」を参照してください。

# Accelerate の設定コンプライアンス

AMS Accelerate は、セキュリティと運用の整合性に関する高い基準にリソースを設定し、次の業界標準に準拠するのに役立ちます。

- インターネットセキュリティセンター (CIS)
- 米国国立標準技術研究所 (NIST) クラウドセキュリティフレームワーク (CSF)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry (PCI) データセキュリティ標準 (DSS)

これを行うには、コンプライアンス AWS Config ルールセット全体をアカウントにデプロイします。「」を参照してくださいAMS Config ルールライブラリ。 AWS Config ルールは、リソースに必要な設定を表し、 AWS リソースの設定の変更に対して評価されます。設定を変更すると、コンプライアンスをテストするための多数のルールがトリガーされます。例えば、Amazon S3 バケットを作成し、NIST 標準に違反してパブリックに読み取れるように設定するとします。ams-nist-cis-s3-bucket-public-read-prohibited ルールは違反を検出し、設定レポートで S3 バケットに非準拠のラベルを付けます。このルールは自動インシデント修復カテゴリに属しているため、すぐにインシデントレポートを作成し、問題を警告します。その他のより重大なルール違反では、AMS によって問題が自動的に修正される可能性があります。「Accelerate での違反への対応」を参照してください。

> **Important**
>
> 例えば、AMS で違反を修復する場合は、その修復カテゴリに関係なく、AMS に非準拠リソースの修復を求めるサービスリクエストを送信します。サービスリクエストには、「AMS 設定ルールの修正の一環として、非苦情リソース *RESOURCE_ARNS_OR_IDs*、アカウントの設定ルール *CONFIG_RULE_NAME*」などのコメントを含め、違反を修正するために必要な入力を追加します。

例えば、設計上パブリックアクセスを必要とする特定の S3 バケットに対してアクションを実行しない場合は、例外を作成できます。「」を参照してくださいAccelerate でのルール例外の作成。

## AMS Config ルールライブラリ

Accelerate は、アカウントを保護するために AMS 設定ルールのライブラリをデプロイします。これらの設定ルールは で始まりますams-。アカウント内のルールとそのコンプライアンス状態は、AWS Config コンソール、 AWS CLI、または AWS Config API から表示できます。の使用に関する一般的な情報については AWS Config、ViewingConfiguration Compliance」を参照してください。

> **Note**
>
> オプトイン AWS リージョンおよび Gov クラウドリージョンの場合、リージョンの制限により、設定ルールのサブセットのみをデプロイします。AMS Accelerate 設定ルールテーブルの識別子に関連付けられたリンクをチェックして、リージョンのルールの可用性を確認します。
> デプロイされた AMS Config ルールを削除することはできません。

### ルールの表

ams_config_rules.zip としてダウンロードします。

AMS 設定ルール

| ルール名 | サービス | Trigger トリガー) | アクション | フレームワーク |
|---|---|---|---|---|
| ams-nist-cis-guardduty-enabled-centralized | GuardDuty | 定期的 | 修復 | CIS: CIS.13、CIS.14、NIST-CSF: PR.DS-1、HIPAA: 164.312(a)(2)(iv)、164.312(e)(2)(ii)、PCI: 2.2、3.4、8.2.1、 |

| ルール名 | サービス | Trigger トリガー) | アクション | フレームワーク |
| --- | --- | --- | --- | --- |
| ams-nist-cis-vpc-flow-logs-enabled | VPC | 定期的 | 修復 | CIS: CIS.6; NIST-CSF: DE.AE-1,DE.AE-3,PR.DS-5,PR.PT-1; HIPAA: 164.308(a)(3)(ii)(A)、164.312(b)、PCI: 2.2,10.1,10.3.2,10.3.3,10.3.510.3.4,10.3.6; |
| ams-eks-secrets-encrypted | EKS | 定期的 | インシデント | CIS: NA; NIST-CSF: NA; HIPAA: NA; PCI: NA; |
| ams-eks-endpoint-no-public-access | EKS | 定期的 | インシデント | CIS: NA; NIST-CSF: NA; HIPAA: NA; PCI: NA; |
| ams-nist-cis-vpc-default-security-group-closed | VPC | 設定の変更 | インシデント | CIS: CIS.11、CIS.12、CIS.9、NIST-CSF: DE.AE-1、PR.AC-3、PR.AC-5、PR.PT-4、HIPAA: 164.312(e)(1)、PCI: 1.2、1.3、2.1、2.2、1.2.1、1.3.1、1.3.2、2.2.2 |

| ルール名 | サービス | Trigger トリガー) | アクション | フレームワーク |
| --- | --- | --- | --- | --- |
| ams-nist-cis-iam-password-policy | IAM | 定期的 | インシデント | CIS: NA、NIST-CSF: PR.AC-1,PR.AC-4、HIPAA: 164.308(a)(3)(i)、164.308(a)(3)(ii)(A)、164.308(a)(3)(ii)(B)、164.308(a)(4)(i)、164.308(a)(4)(ii)(A)、164.308(a)(4)(a)(ii)、164.312(a)(1)、PCI: 7.1.2、7.1.3、7.2.1、7.2.2、7.2。 |
| ams-nist-cis-iam-root-access-key-check | IAM | 定期的 | インシデント | CIS: CIS.16,CIS.4; NIST-CSF: PR.AC-1,PR.AC-4,PR.PT-3; HIPAA: 164.308(a)(3)(i)、164.308(a)(3)(ii)(A)、164.308(a)(a)、164.308(a)(i)、164.308(a)(4)(ii)(A)、164.308(a)(4)(ii)(B)、164.308(a)(4)(ii)(C)、164.312(a)(1); PCI: 2.2,7.1.2,7.3.2,7.2.3.3 |

| ルール名 | サービス | Trigger トリガー) | アクション | フレームワーク |
| --- | --- | --- | --- | --- |
| ams-nist-cis-iam-user-mfa-enabled | IAM | 定期的 | インシデント | CIS: CIS.16; NIST-CSF: PR.AC-1,PR.AC-4; HIPAA: 164.308(a)(3)(i)、164.308(a)(3)(ii)(A)、164.308(a)(ii)(B)、164.308(a)(4)(i)、164.308(a)(4)(ii)(A)、164.308(a)(ii)(B)、164.308(a)(4)(ii)(C)、164.312(a)(1)、PCI: 2.2,7.1.2,7.1.3,7.2.2,7.2.2. |
| ams-nist-cis-restricted-ssh | セキュリティグループ | 設定の変更 | インシデント | CIS: CIS.16; NIST-CSF: PR.AC-1,PR.AC-4; HIPAA: 164.308(a)(3)(i)、164.308(a)(4)(ii)(A)、164.308(a)(4)(ii)(B)、164.308(a)(4)(ii)(C)、164.312(a)(1)、PCI: 2.2,7.2.1,8.1.4; |
| ams-nist-cis-restricted-common-ports | セキュリティグループ | 設定の変更 | インシデント | CIS: CIS.11、CIS.12、CIS.9、NIST-CSF: DE.AE-1、PR.AC-3、PR.AC-5、PR.PT-4、HIPAA: 164.308(a)(3)(i)、164.308(a)(3)(ii)(B)、164.308(a)(4)(i)、164.308(a)(4)(ii)(A)、164.308(a)(4)(ii)(ii)(B)、164.308(a)(4)(C)、164.312(e)(1)、PCI: 1.2,1.3.2,2.2 |

| ルール名 | サービス | Trigger トリガー) | アクション | フレームワーク |
| --- | --- | --- | --- | --- |
| ams-nist-cis-s3-account-level-public-access-blocks | S3 | 設定の変更 | インシデント | CIS: CIS.9、CIS .12、CIS.14、NIST-CSF: PR.AC-3、P R.AC-4、PR.AC-5、PR. DS-5、PR.PT-3、PR.PT -4、HIPAA: 164.308(a )(3)(i)、164.308(a)(4) (ii)(A)、164.308(a)(4) (ii)(C)、164.312(a)(1) 、164.312(e)(1)、PCI: 1.2,1.2.1,1.3,1.3.1,1.3.2,2 .2.2; |
| ams-nist-cis-s3-bucket-public-read-prohibited | S3 | 設定の変更 | インシデント | CIS: CIS.12、CI S.14、CIS.9、NIST-CSF: PR.AC-3、P R.AC-4、PR.AC-5、PR. DS-5、PR.PT-3、PR.PT -4、HIPAA: 164.308(a )(3)(i)、164.308(a)(4) (ii)(A)、164.308(a)(4) (ii)(C)、164.312(a)(1) 、164.312(e)(1)、PCI: 1.2,1.3,2.2,1.2.1.2.1.3.1,1 .3.2,1.3.4,1.3.6,2.2.2.2; |

| ルール名 | サービス | Trigger トリガー) | アクション | フレームワーク |
| --- | --- | --- | --- | --- |
| ams-nist-cis-s3-bucket-public-write-prohibited | S3 | 設定の変更 | インシデント | CIS: CIS.12、CIS.14、CIS.9、NIST-CSF: PR.AC-3、PR.AC-4、PR.AC-5、PR.DS-5、PR.PT-3、PR.PT-4、HIPAA: 164.308(a)(3)(i)、164.308(a)(4)(ii)(A)、164.308(a)(4)(ii)(C)、164.312(a)(1)、164.312(e)(1)、PCI: 1.2,1.3,2.2,1.2.1.2.1,1.3.1,1.3.2,1.3.4,1.3.6,2.2.2.2 |
| ams-nist-cis-s3-bucket-server-side-encryption-enabled | S3 | 設定の変更 | インシデント | CIS: CIS.13、CIS.14、NIST-CSF: PR.DS-1、HIPAA: 164.312(a)(2)(iv)、164.312(c)(2)、164.312(e)(2)(ii)、PCI: 2.2、3.4、10.5、8.2.1、 |
| ams-nist-cis-securityhub-enabled | Security Hub | 定期的 | インシデント | CIS: CIS.3、CIS.4、CIS.6、CIS.12、CIS.16、CIS.19、NIST-CSF: PR.DS-5、PR.PT-1、HIPAA: 164.312(b)、PCI: NA、 |
| ams-nist-cis-ec2-instance-managed-by-systems-manager | EC2 | 設定の変更 | レポートを行う | CIS: CIS.2,CIS.5、NIST-CSF: ID.AM-2,PR.IP-1、HIPAA: 164.308(a)(5)(ii)(B)、PCI: 2.4、 |

| ルール名 | サービス | Trigger トリガー) | アクション | フレームワーク |
| --- | --- | --- | --- | --- |
| ams-nist-cis-cloudtrail-enabled | CloudTrail | 定期的 | レポートを行う | CIS: CIS.16,CIS.6; NIST-CSF: DE.AE-1,DE.AE-3,PR.DS-5,PR.MA-2,PR.PT-1; HIPAA: 164.308(a)(3)(ii)(A)、164.308(a)(5)(ii)(C)、164.312(b); PCI: 10.1,10.2.1,10.2.3 10.2.2,10.2.410.2.5,10.2.6,10.2.7,10.3.110.3.2,10.3.3,10.3.4,,10.3.5,,,10.3.6 |
| ams-nist-cis-access-keys-rotated | IAM | 定期的 | レポートを行う | CIS: CIS.16、NIST-CSF: PR.AC-1、HIPAA: 164.308(a)(4)(ii)(B)、PCI: 2.2、 |
| ams-nist-cis-acm-certificate-expiration-check | Certificate Manager | 設定の変更 | レポートを行う | CIS: CIS.13,CIS.14; NIST-CSF: PR.AC-5,PR.PT-4; HIPAA: NA; PCI: 4.1; |
| ams-nist-cis-alb-http-to-https-redirection-check | ALB | 定期的 | レポートを行う | CIS: CIS.13,CIS.14; NIST-CSF: PR.DS-2; HIPAA: 164.312(a)(2)(iv)、164.312(e)(1)、164.312(e)(2)(i)、164.312(e)(2)(ii)、PCI: 2.3,4.1,8.2.1; |

| ルール名 | サービス | Trigger トリガー) | アクション | フレームワーク |
| --- | --- | --- | --- | --- |
| ams-nist-cis-api-gw-cache-enabled-and-encrypted | API Gateway | 設定の変更 | レポートを行う | CIS: CIS.13、CIS.14、NIST-CSF: PR.DS-1、HIPAA: 164.312(a)(2)(iv)、164.312(e)(2)(ii)、PCI: 3.4、 |
| ams-nist-cis-api-gw-execution-logging-enabled | API Gateway | 設定の変更 | レポートを行う | CIS: CIS.6; NIST-CSF: DE.AE-1,DE.AE-3,PR.PT-1; HIPAA: 164.312(b); PCI: 10.1,10.3.1,10.3.2,10.3.3,10.3.4,10.3.510.3.6,10.5.4; |
| ams-nist-autoscaling-group-elb-healthcheck-required | ELB | 設定の変更 | レポートを行う | CIS: NA、NIST-CSF: PR.PT-1、PR.PT-5、HIPAA: 164.312(b)、PCI: 2.2、 |
| ams-nist-cis-cloud-trail-encryption-enabled | CloudTrail | 定期的 | レポートを行う | CIS: CIS.13、CIS.14、NIST-CSF: PR.DS-1、HIPAA: 164.312(a)(2)(iv)、164.312(e)(2)(ii)、PCI: 2.2、3.4、10.5、 |
| ams-nist-cis-cloud-trail-log-file-validation-enabled | CloudTrail | 定期的 | レポートを行う | CIS: CIS.6、NIST-CSF: PR.DS-6、HIPAA: 164.312(c)(1)、164.312(c)(2)、PCI: 2.2,10.5,11.5,10.5.2,10.5.5、 |

| ルール名 | サービス | Trigger トリガー) | アクション | フレームワーク |
| --- | --- | --- | --- | --- |
| ams-nist-cis-cloudtrail-s3-dataevents-enabled | CloudTrail | 定期的 | レポートを行う | CIS: CIS.6; NIST-CSF: DE.AE-1,DE.AE-3,PR.DS-5,PR.PT-1; HIPAA: 164.308(a)(3)(ii)(A)、164.312(b)、PCI: 2.2,10.1,10.2.1,10.2.2,10.2.3,10.2.5,10.3.210.3.1,10.3.3,10.3.4,,10.3.5,,10.3.6; |
| ams-nist-cis-cloudwatch-alarm-action-check | CloudWatch | 設定の変更 | レポートを行う | CIS: CIS.13、CIS.14、NIST-CSF: NA、HIPAA: 164.312(a)(2)(iv)、164.312(e)(2)(ii)、PCI: 3.4、 |
| ams-nist-cis-cloudwatch-log-group-encrypted | CloudWatch | 定期的 | レポートを行う | CIS: CIS.13、CIS.14、NIST-CSF: NA、HIPAA: 164.312(a)(2)(iv)、164.312(e)(2)(ii)、PCI: 3.4、 |
| ams-nist-cis-codebuild-project-envvar-awscred-check | CodeBuild | 設定の変更 | レポートを行う | CIS: CIS.18、NIST-CSF: PR.DS-5、HIPAA: 164.308(a)(3)(i)、164.308(a)(4)(ii)(A)、164.308(a)(4)(ii)(C)、164.312(a)(1)、PCI: 8.2.1、 |

| ルール名 | サービス | Trigger トリガー) | アクション | フレームワーク |
| --- | --- | --- | --- | --- |
| ams-nist-cis-codebuild-project-source-repo-url-check | CodeBuild | 設定の変更 | レポートを行う | CIS: CIS.18、NIST-CSF: PR.DS-5、HIPAA: 164.308(a)(3)(i)、164.308(a)(4)(ii)(A)、164.308(a)(4)(ii)(C)、164.312(a)(1)、PCI: 8.2.1、 |
| ams-nist-cis-db-instance-backup-enabled | RDS | 設定の変更 | レポートを行う | CIS: CIS.10、NIST-CSF: ID.BE-5、PR.DS-4、PR.IP-4、PR.PT-5、RC.RP-1、HIPAA: 164.308(a)(7)(i)、164.308(a)(7)(ii)(A)、164.308(a)(7)(ii)(B)、PCI: NA。 |
| ams-nist-cis-dms-replication-not-public | DMS | 定期的 | レポートを行う | CIS: CIS.12、CIS.14、CIS.9、NIST-CSF: PR.AC-3、PR.AC-4、PR.AC-5、PR.DS-5、PR.PT-3、PR.PT-4、HIPAA: 164.308(a)(3)(i)、164.308(a)(4)(ii)(A)、164.308(a)(4)(ii)(C)、164.312(a)(1)、164.312(e)(1)、PCI: 1.2,1.3,1.2.1,1.3.1,1.3.1,1.3.2,1.3.2; |

| ルール名 | サービス | Trigger トリガー) | アクション | フレームワーク |
| --- | --- | --- | --- | --- |
| ams-nist-dynamodb-autoscaling-enabled | DynamoDB | 定期的 | レポートを行う | CIS: NA、NIST-CSF: ID.BE-5、PR.DS-4、PR.PT-5、RC.RP-1、HIPAA: 164.308(a)(7)(i)、164.308(a)(7)(ii)(C)、PCI: NA、 |
| ams-nist-cis-dynamodb-pitr-enabled | DynamoDB | 定期的 | レポートを行う | CIS: CIS.10、NIST-CSF: ID.BE-5、PR.DS-4、PR.IP-4、PR.PT-5、RC.RP-1、HIPAA: 164.308(a)(7)(i)、164.308(a)(7)(ii)(A)、164.308(a)(7)(ii)(B)、PCI: NA、 |
| ams-nist-dynamodb-throughput-limit-check | DynamoDB | 定期的 | レポートを行う | CIS: NA、NIST-CSF: NA、HIPAA: 164.312(b)、PCI: NA、 |
| ams-nist-ebs-optimized-instance | EBS | 設定の変更 | レポートを行う | CIS: NA、NIST-CSF: NA、HIPAA: 164.308(a)(7)(i)、PCI: NA、 |

| ルール名 | サービス | Trigger トリガー) | アクション | フレームワーク |
| --- | --- | --- | --- | --- |
| ams-nist-cis-ebs-snapshot-public-restorable-check | EBS | 定期的 | レポートを行う | CIS: CIS.12,CIS.14,CIS.9; NIST-CSF: PR.AC-3,PR.AC-4,PR.AC-5,PR.DS-5,PR.PT-3,PR.PT-4; HIPAA: 164.308(a)(3)(i)、164.308(a)(4)(ii)(A)、164.308(a)(4)(ii)(C)、164.312(a)(1)、164.312(e)(1); PCI: 1.2,1.3,1.2.1,1.3.1,1.3.1,1.3.1,1.3.2; |
| ams-nist-ec2-instance-detailed-monitoring-enabled | EC2 | 設定の変更 | レポートを行う | CIS: NA、NIST-CSF: DE.AE-1、PR.PT-1、HIPAA: 164.312(b)、PCI: NA、 |
| ams-nist-cis-ec2-instance-no-public-ip | EC2 | 設定の変更 | レポートを行う | CIS: CIS.12,CIS.14,CIS.9; NIST-CSF: PR.AC-3,PR.AC-4,PR.AC-5,PR.PT-3,PR.PT-4; HIPAA: 164.308(a)(3)(i)、164.308(a)(4)(ii)(A)、164.308(a)(4)(ii)(C)、164.312(a)(1)、164.312(e)(1); PCI: 1.2,1.3,1.2.1,1.3.1,1.3.2,1.3.4,1.3.6,2.2.2.2 |

| ルール名 | サービス | Trigger トリガー) | アクション | フレームワーク |
| --- | --- | --- | --- | --- |
| ams-nist-cis-ec2-managedinstance-association-compliance-status-check | EC2 | 設定の変更 | レポートを行う | CIS: CIS.12,CIS.9; NIST-CSF: PR.AC-3,PR.AC-4,PR.AC-5,PR.PT-3,PR.PT-4; HIPAA: 164.308(a)(3)(i)、164.308(a)(4)(ii)(A)、164.308(a)(4)(ii)(C)、164.312(a)(1)、164.312(e)(1); PCI: 1.2,1.3,1.2.1,1.3.1,1.3.2,1.3.4,1.3.6,2.2.2; |
| ams-nist-cis-ec2-managedinstance-patch-compliance-status-check | EC2 | 設定の変更 | レポートを行う | CIS: CIS.2,CIS.5、NIST-CSF: ID.AM-2,PR.IP-1、HIPAA: 164.308(a)(5)(ii)(B)、PCI: 6.2、 |
| ams-nist-cis-ec2-stopped-instance | EC2 | 定期的 | レポートを行う | CIS: CIS.2; NIST-CSF: ID.AM-2,PR.IP-1; HIPAA: NA; PCI: NA; |
| ams-nist-cis-ec2-volume-inuse-check | EC2 | 設定の変更 | レポートを行う | CIS: CIS.2; NIST-CSF: PR.IP-1; HIPAA: NA; PCI: NA; |
| ams-nist-cis-efs-encrypted-check | EFS | 定期的 | レポートを行う | CIS: CIS.13、CIS.14、NIST-CSF: PR.DS-1、HIPAA: 164.312(a)(2)(iv)、164.312(e)(2)(ii)、PCI: 3.4,8.2.1、 |

| ルール名 | サービス | Trigger トリガー) | アクション | フレームワーク |
| --- | --- | --- | --- | --- |
| ams-nist-cis-eip-attached | EC2 | 設定の変更 | レポートを行う | CIS: CIS.13、CIS.14、NIST-CSF: PR.DS-1、HIPAA: 164.312(a)(2)(iv)、164.312(e)(2)(ii)、PCI: 3.4,8.2.1、 |
| ams-nist-cis-elasticache-redis-cluster-automatic-backup-check | ElastiCache | 定期的 | レポートを行う | CIS: CIS.10、NIST-CSF: ID.BE-5、PR.DS-4、PR.IP-4、PR.PT-5、RC.RP-1、HIPAA: 164.308(a)(7)(i)、164.308(a)(7)(ii)(A)、164.308(a)(7)(ii)(B)、PCI: NA、 |
| ams-nist-cis-opensearch-encrypted-at-rest | OpenSearch | 定期的 | レポートを行う | CIS: CIS.14、CIS.13、NIST-CSF: PR.DS-1、HIPAA: 164.312(a)(2)(iv)、164.312(e)(2)(ii)、PCI: 3.4,8.2.1、 |
| ams-nist-cis-opensearch-in-vpc-only | OpenSearch | 定期的 | レポートを行う | CIS: CIS.13、CIS.14、NIST-CSF: PR.DS-1、HIPAA: 164.312(a)(2)(iv)、164.312(e)(2)(ii)、PCI: 3.4,8.2.1、 |

| ルール名 | サービス | Trigger トリガー) | アクション | フレームワーク |
| --- | --- | --- | --- | --- |
| ams-nist-cis-elb-acm-certificate-required | Certificate Manager | 設定の変更 | レポートを行う | CIS: CIS.12,CIS.9; NIST-CSF: PR.AC-3,PR.AC-4,PR.AC-5,PR.DS-5,PR.PT-3,PR.PT-4; HIPAA: 164.308(a)(3)(i)、164.308(a)(4)(ii)(A)、164.308(a)(4)(ii)(C)、164.312(a)(1)、164.312(e)(1); PCI: 1.2,1.3,1.2.1,1.3.1,1.3.2,1.3.4,1.3.6,2.2.2 |
| ams-nist-elb-deletion-protection-enabled | ELB | 設定の変更 | レポートを行う | CIS: CIS.13、CIS.14、NIST-CSF: PR.DS-2、HIPAA: 164.312(a)(2)(iv)、164.312(e)(1)、164.312(e)(2)(i)、164.312(e)(2)(ii)、PCI: 4.1,8.2.1、 |
| ams-nist-cis-elb-logging-enabled | ELB | 設定の変更 | レポートを行う | CIS: CIS.6; NIST-CSF: DE.AE-1,DE.AE-3,PR.PT-1; HIPAA: 164.312(b); PCI: 10.1,10.3.1,10.3.2,10.3.3,10.3.4,10.3.510.3.6,10.5.4; |
| ams-nist-cis-emr-kerberos-enabled | EMR | 定期的 | レポートを行う | CIS: CIS.6; NIST-CSF: DE.AE-1,DE.AE-3,PR.PT-1; HIPAA: 164.312(b); PCI: 10.1,10.3.1,10.3.2,10.3.3,10.3.4,10.3.510.3.6,10.5.4; |

| ルール名 | サービス | Trigger トリガー) | アクション | フレームワーク |
| --- | --- | --- | --- | --- |
| ams-nist-cis-emr-master-no-public-ip | EMR | 定期的 | レポートを行う | CIS: CIS.14,CIS.16; NIST-CSF: PR.AC-1,PR.AC-4,PR.AC-6; HIPAA: 164.308(a)(3)(i)、164.308(a)(3)(ii)(A)、164.308(a)(a)、164.308(a)(i)、164.308(a)(4)(ii)(A)、164.308(a)(4)(ii)(B)、164.308(a)(4)(ii)(C)、164.312(a)(1); PCI: 7.2.1; |
| ams-nist-cis-encrypted-volumes | EBS | 設定の変更 | レポートを行う | CIS: CIS.12,CIS.9; NIST-CSF: PR.AC-3,PR.AC-4,PR.AC-5,PR.PT-3,PR.PT-4; HIPAA: 164.308(a)(3)(i)、164.308(a)(4)(ii)(A)、164.308(a)(4)(ii)(C)、164.312(a)(1)、164.312(e)(1); PCI: 1.2,1.3,1.2.1,1.3.1,1.3.2,1.3.4,1.3.6,2.2.2; |

| ルール名 | サービス | Trigger トリガー) | アクション | フレームワーク |
| --- | --- | --- | --- | --- |
| ams-nist-cis-guardduty-non-archived-findings | GuardDuty | 定期的 | レポートを行う | CIS: CIS.12,CIS.13,CIS.16,CIS.19,CIS.3,CIS.4,CIS.6,CIS.8; NIST-CSF: DE.AE-2,DE.AE-3,DE.CM-4,DE.DP-5,ID.RA-1,ID.RA-3,PR.DS-5,PR.PT-1; HIPAA: 164.308(a)(5)(ii)(C)、164.308(a)(6)(ii)、164.312(b)、PCI: 6.1,11.4,5.1.2; |
| ams-nist-iam-group-has-users-check | IAM | 設定の変更 | レポートを行う | CIS: NA、NIST-CSF: PR.AC-4、PR.AC-1、HIPAA: 164.308(a)(3)(i)、164.308(a)(3)(ii)(A)、164.308(a)(3)(ii)(B)、164.308(a)(4)(i)、164.308(a)(4)(ii)(A)、164.308(a)(4)(a)(4)(ii)(C)、164.312(a)(1)、PCI: 7.1.2、7.1.3、7.2.1、7.2.2、7.2.2。 |
| ams-nist-cis-iam-policy-no-statements-with-admin-access | IAM | 設定の変更 | レポートを行う | CIS: CIS.16、NIST-CSF: PR.AC-6、PR.AC-7、HIPAA: 164.308(a)(4)(ii)(B)、164.308(a)(5)(ii)(D)、164.312(d)、PCI: 8.2.3、8.2.4、8.2.5、 |

| ルール名 | サービス | Trigger トリガー) | アクション | フレームワーク |
| --- | --- | --- | --- | --- |
| ams-nist-cis-iam-user-group-membership-check | IAM | 設定の変更 | レポートを行う | CIS: CIS.16,CIS.4; NIST-CSF: PR.AC-1,PR.AC-4,PR.PT-3; HIPAA: 164.308(a)(3)(i)、164.308(a)(4)(ii)(A)、164.308(a)(4)(ii)(B)、164.308(a)(4)(ii)(C)、164.312(a)(1)、164.312(a)(2)(i)、PCI: 2.2,7.1.2,7.2.1,8.1.1; |
| ams-nist-cis-iam-user-no-policies-check | IAM | 設定の変更 | レポートを行う | CIS: CIS.16、NIST-CSF: PR.AC-1、PR.AC-7、HIPAA: 164.308(a)(4)(ii)(B)、164.312(d)、PCI: 8.3、 |
| ams-nist-cis-iam-user-unused-credentials-check | IAM | 定期的 | レポートを行う | CIS: CIS.16; NIST-CSF: PR.AC-1,PR.AC-4,PR.PT-3; HIPAA: 164.308(a)(3)(i)、164.308(a)(3)(ii)(A)、164.308(a)(3)(ii)(B)、164.308(a)(4)(i)、164.308(a)(4)(ii)(A)、164.308(a)(ii)(B)、164.308(a)(a)(4)(ii)、C)、164.312(a)(1); PCI: 2.2,7.1.2,7.1.3,7.2 |

| ルール名 | サービス | Trigger トリガー) | アクション | フレームワーク |
| --- | --- | --- | --- | --- |
| VPC 内の ams-nist-cis-ec2-instances instances-in-vpc | EC2 | 設定の変更 | レポートを行う | CIS: CIS.11、CIS.12、CIS.9、NIST-CSF: DE.AE-1、PR.AC-3、PR.AC-5、PR.PT-4、HIPAA: 164.308(a)(3)(i)、164.308(a)(3)(ii)(B)、164.308(a)(4)(i)、164.308(a)(4)(ii)(A)、164.308(a)(ii)(4)(ii)(B)、164.308(a)(4)(C)、164.312(e)(1)、PCI: 1.2,1.3.2,2.2 |
| ams-nist-cis-internet-gateway-authorized-vpc-only | インターネットゲートウェイ | 定期的 | レポートを行う | CIS: CIS.9,CIS.12; NIST-CSF: NA; HIPAA: NA; PCI: NA; |
| ams-nist-cis-kms-cmk-not-scheduled-for-deletion | KMS | 定期的 | レポートを行う | CIS: CIS.13,CIS.14; NIST-CSF: PR.DS-1; HIPAA: NA; PCI: 3.5,3.6; |
| ams-nist-lambda-concurrency-check | Lambda | 設定の変更 | レポートを行う | CIS: NA、NIST-CSF: NA、HIPAA: 164.312(b)、PCI: NA、 |
| ams-nist-lambda-dlq-check | Lambda | 設定の変更 | レポートを行う | CIS: NA、NIST-CSF: NA、HIPAA: 164.312(b)、PCI: NA、 |

| ルール名 | サービス | Trigger トリガー) | アクション | フレームワーク |
| --- | --- | --- | --- | --- |
| ams-nist-cis-lambda-function-public-access-prohibited | Lambda | 設定の変更 | レポートを行う | CIS: CIS.12,CIS.9; NIST-CSF: PR.AC-3,PR.AC-4,PR.AC-5,PR.DS-5,PR.PT-3,PR.PT-4; HIPAA: 164.308(a)(3)(i)、164.308(a)(4)(ii)(A)、164.308(a)(4)(ii)(C)、164.312(a)(1)、164.312(e)(1); PCI: 1.2,1.3,1.2.1,1.3.1,1.3.2,1.3.4,2.2.2; |
| ams-nist-cis-lambda-inside-vpc | Lambda | 設定の変更 | レポートを行う | CIS: CIS.12,CIS.9; NIST-CSF: PR.AC-3,PR.AC-4,PR.AC-5,PR.PT-3,PR.PT-4; HIPAA: 164.308(a)(3)(i)、164.308(a)(4)(ii)(A)、164.308(a)(4)(ii)(C)、164.312(a)(1)、164.312(e)(1); PCI: 1.2,1.3,1.2.1,1.3.2,1.3.4,2.2.2; |
| ams-nist-cis-mfa-enabled-for-iam-console-access | IAM | 定期的 | レポートを行う | CIS: CIS.16、NIST-CSF: PR.AC-7、HIPAA: 164.312(d)、PCI: 2.2,8.3、 |

| ルール名 | サービス | Trigger トリガー) | アクション | フレームワーク |
| --- | --- | --- | --- | --- |
| ams-nist-cis-multi-region-cloudtrail-enabled | CloudTrail | 定期的 | レポートを行う | CIS: CIS.6; NIST-CSF: DE.AE-1,DE.AE-3,PR.DS-5,PR.MA-2,PR.PT-1; HIPAA: 164.308(a)(3)(ii)(A)、164.312(b); PCI: 2.2,10.1,10.2.1,10.2.2,,10.2.3,10.2.510.2.4,10.2.6,10.2.7,10.3.1,10.3.2,,10.3.310.3.4,10.3.5,,,,10.3.6,; |
| ams-nist-rds-enhanced-monitoring-enabled | RDS | 設定の変更 | レポートを行う | CIS: NA、NIST-CSF: PR.PT-1、HIPAA: 164.312(b)、PCI: NA、 |
| ams-nist-cis-rds-instance-public-access-check | RDS | 設定の変更 | レポートを行う | CIS: CIS.12、CIS.14、CIS.9、NIST-CSF: PR.AC-3、PR.AC-4、PR.AC-5、PR.DS-5、PR.PT-3、PR.PT-4、HIPAA: 164.308(a)(3)(i)、164.308(a)(4)(ii)(A)、164.308(a)(4)(ii)(C)、164.312(a)(1)、164.312(e)(1)、PCI: 1.2,1.3,1.2.1,1.3.1,1.3.1,1.3.4,1.3.6,2.2.2.2.2 |
| ams-nist-rds-multi-az-support | RDS | 設定の変更 | レポートを行う | CIS: NA、NIST-CSF: ID.BE-5、PR.DS-4、PR.PT-5、RC.RP-1、HIPAA: 164.308(a)(7)(i)、164.308(a)(7)(ii)(C)、PCI: NA、 |

| ルール名 | サービス | Trigger トリガー) | アクション | フレームワーク |
| --- | --- | --- | --- | --- |
| ams-nist-cis-rds-snapshots-public-prohibited | RDS | 設定の変更 | レポートを行う | CIS: CIS.12,CIS.14,CIS.9; NIST-CSF: PR.AC-3,PR.AC-4,PR.AC-5,PR.DS-5,PR.PT-3,PR.PT-4; HIPAA: 164.308(a)(3)(i)、164.308(a)(4)(ii)(A)、164.308(a)(4)(ii)(C)、164.312(a)(1)、164.312(e)(1); PCI: 1.2,1.3,1.2.1,1.3.1,1.3.1,1.3.1,1.3.2; |
| ams-nist-cis-rds-storage-encrypted | RDS | 設定の変更 | レポートを行う | CIS: CIS.13,CIS.5,CIS.6; NIST-CSF: DE.AE-1,DE.AE-3,PR.DS-1,PR.PT-1; HIPAA: 164.312(a)(2)(iv)、164.312(b)、164.312(e)(2)(ii); PCI: 3.4,10.1,10.2.1,10.2.3,10.2.2,10.2.410.2.5,10.3.1,,,10.3.610.3.210.3.310.3.410.3.5,,8.2.1; |
| ams-nist-cis-redshift-cluster-configuration-check | RedShift | 設定の変更 | レポートを行う | CIS: CIS.6、CIS.13、CIS.5、NIST-CSF: DE.AE-1、DE.AE-3、PR.DS-1、PR.PT-1、HIPAA: 164.312(a)(2)(iv)、164.312(b)、164.312(e)(2)(ii)、PCI: 3.4、8.2.1、10.1、10.2.1、10.2.210.2.3、10.2.4、10.2.510.3.110.3.2、10.3.3、10.3.4、、、10.3.5、、10.3.6 |

| ルール名 | サービス | Trigger トリガー) | アクション | フレームワーク |
| --- | --- | --- | --- | --- |
| ams-nist-cis-redshift-cluster-public-access-check | RedShift | 設定の変更 | レポートを行う | CIS: CIS.12、CIS.14、CIS.9、NIST-CSF: PR.AC-3、PR.AC-4、PR.AC-5、PR.DS-5、PR.PT-3、PR.PT-4、HIPAA: 164.308(a)(3)(i)、164.308(a)(4)(ii)(A)、164.308(a)(4)(ii)(C)、164.312(a)(1)、164.312(e)(1)、PCI: 1.2,1.3,1.2.1,1.3.1,1.3.1,1.3.2,1.3.2; |
| ams-nist-cis-redshift-require-tls-ssl | RedShift | 定期的 | レポートを行う | CIS: CIS.13、CIS.14、NIST-CSF: PR.DS-2、HIPAA: 164.312(a)(2)(iv)、164.312(e)(1)、164.312(e)(2)(i)、164.312(e)(2)(ii)、PCI: 2.3,4.1、 |
| ams-nist-cis-root-account-hardware-mfa-enabled | IAM | 定期的 | レポートを行う | CIS: CIS.16、CIS.4、NIST-CSF: PR.AC-7、HIPAA: 164.312(d)、PCI: 2.2,8.3、 |
| ams-nist-cis-root-account-mfa-enabled | IAM | 定期的 | レポートを行う | CIS: CIS.16、CIS.4、NIST-CSF: PR.AC-7、HIPAA: 164.312(d)、PCI: 2.2,8.3、 |

| ルール名 | サービス | Trigger トリガー) | アクション | フレームワーク |
| --- | --- | --- | --- | --- |
| ams-nist-cis-s3-bucket-default-lock-enabled | S3 | 設定の変更 | レポートを行う | CIS: CIS.14,CIS.13; NIST-CSF: ID.BE-5,PR.PT-5,RC.RP-1; HIPAA: NA; PCI: NA; |
| ams-nist-cis-s3-bucket-logging-enabled | S3 | 設定の変更 | レポートを行う | CIS: CIS.6; NIST-CSF: DE.AE-1,DE.AE-3,PR.DS-5,PR.PT-1; HIPAA: 164.308(a)(3)(ii)(A)、164.312(b); PCI: 2.2,10.1,10.2.1,10.2.2,10.2.3,10.2.4,10.2.5,10.3.110.2.7,10.3.2,,10.3.3,,10.3.4,,10.3.5,10.3.6; |
| ams-nist-cis-s3-bucket-replication-enabled | S3 | 設定の変更 | レポートを行う | CIS: CIS.10、NIST-CSF: ID.BE-5、PR.DS-4、PR.IP-4、PR.PT-5、RC.RP-1、HIPAA: 164.308(a)(7)(i)、164.308(a)(7)(ii)(A)、164.308(a)(7)(ii)(B)、PCI: 2.2,10.5.3。 |
| ams-nist-cis-s3-bucket-ssl-requests-only | S3 | 設定の変更 | レポートを行う | CIS: CIS.13,CIS.14; NIST-CSF: PR.DS-2; HIPAA: 164.312(a)(2)(iv)、164.312(c)(2)、164.312(e)(1)、164.312(e)(2)(i)、164.312(e)(2)(ii)、PCI: 2.2,4.1,8.2.1; |

| ルール名 | サービス | Trigger トリガー) | アクション | フレームワーク |
| --- | --- | --- | --- | --- |
| ams-nist-cis-s3-bucket-versioning-enabled | S3 | 定期的 | レポートを行う | CIS: CIS.10、NIST-CSF: ID.BE-5、PR.DS-4、PR.DS-6、PR.IP-4、PR.PT-5、RC.RP-1、HIPAA: 164.308(a)(7)(i)、164.308(a)(7)(ii)(A)、164.308(a)(7)(ii)(B)、164.312(c)(1)、164.312(c)(2)、PCI: 10.5.3、 |
| ams-nist-cis-sagemaker-endpoint-configuration-kms-key-configured | SageMaker | 定期的 | レポートを行う | CIS: CIS.13、CIS.14、NIST-CSF: PR.DS-1、HIPAA: 164.312(a)(2)(iv)、164.312(e)(2)(ii)、PCI: 3.4,8.2.1、 |
| ams-nist-cis-sagemaker-notebook-instance-kms-key-configured | SageMaker | 定期的 | レポートを行う | CIS: CIS.13、CIS.14、NIST-CSF: PR.DS-1、HIPAA: 164.312(a)(2)(iv)、164.312(e)(2)(ii)、PCI: 3.4,8.2.1、 |

| ルール名 | サービス | Trigger トリガー) | アクション | フレームワーク |
| --- | --- | --- | --- | --- |
| ams-nist-cis-sagemaker-notebook-no-direct-internet-access | SageMaker | 定期的 | レポートを行う | CIS: CIS.12,CIS.9; NIST-CSF: PR.AC-3,PR.AC-4,PR.AC-5,PR.DS-5,PR.PT-3,PR.PT-4; HIPAA: 164.308(a)(3)(i),164.308(a)(4)(ii)(A)、164.308(a)(4)(ii)(C)、164.312(a)(1)、164.312(e)(1); PCI: 1.2,1.3,1.2.1,1.3.1,1.3.2,1.3.4,1.3.6,2.2.2 |
| ams-nist-cis-secretsmanager-rotation-enabled-check | Secrets Manager | 設定の変更 | レポートを行う | CIS: CIS.16、NIST-CSF: PR.AC-1、HIPAA: 164.308(a)(4)(ii)(B)、PCI: NA、 |
| ams-nist-cis-secretsmanager-scheduled-rotation-success-check | Secrets Manager | 設定の変更 | レポートを行う | CIS: CIS.16、NIST-CSF: PR.AC-1、HIPAA: 164.308(a)(4)(ii)(B)、PCI: NA、 |
| ams-nist-cis-sns-encrypted-kms | SNS | 設定の変更 | レポートを行う | CIS: CIS.13、CIS.14、NIST-CSF: PR.DS-1、HIPAA: 164.312(a)(2)(iv)、164.312(e)(2)(ii)、PCI: 8.2.1、 |

| ルール名 | サービス | Trigger トリガー) | アクション | フレームワーク |
| --- | --- | --- | --- | --- |
| ams-nist-cis-vpc-sg-open-only-to-authorized-ports | VPC | 設定の変更 | レポートを行う | CIS: CIS.11、CIS.12、CIS.9、NIST-CSF: DE.AE-1、PR.AC-3、PR.AC-5、PR.PT-4、HIPAA: 164.312(e)(1)、PCI: 1.2、1.3、1.2.1、1.3.1、1.3.2、2.2.2。 |
| ams-nist-vpc-vpn-2-tunnels-up | VPC | 設定の変更 | レポートを行う | CIS: NA、NIST-CSF: ID.BE-5、PR.DS-4、PR.PT-5、RC.RP-1、HIPAA: 164.308 (a)(7)(i)、PCI: NA、 |
| ams-cis-ec2-ebs-encryption-by-default | EC2 | 定期的 | レポートを行う | CIS: CIS.13、CIS.14、NIST-CSF: PR.DS-1、HIPAA: 164.312(a)(2)(iv)、164.312(e)(2)(ii)、PCI: 2.2、3.4、8.2.1、 |
| ams-cis-rds-snapshot-encrypted | RDS | 設定の変更 | レポートを行う | CIS: CIS.13、CIS.14、NIST-CSF: PR.DS-1、HIPAA: 164.312(a)(2)(iv)、164.312(e)(2)(ii)、PCI: 3.4,8.2.1、 |
| ams-cis-redshift-cluster-maintenance settings-check | RedShift | 設定の変更 | レポートを行う | CIS: CIS.5、NIST-CSF: PR.DS-4、PR.IP-1、PR.IP-4、HIPAA: 164.308(a)(5)(ii)(A)、164.308(a)(7)(ii)(A)、PCI: 6.2、 |

# Accelerate での違反への対応

すべての Config ルール違反が設定レポートに表示されます。これはユニバーサルレスポンスです。ルールの修復カテゴリ (重要度) によっては、AMS が追加のアクションを実行する場合があります。詳細については、次の表を参照してください。特定のルールのアクションコードをカスタマイズする方法の詳細については、「」を参照してくださいカスタマイズされた検出結果のレスポンス。

修復アクション

| アクションコード | AMS アクション |
| --- | --- |
| Report | 1. を Config レポートに追加する |
| Incident | 1. を Config レポートに追加する<br>2. Accelerate の自動インシデントレポート |
| Remediate | 1. を Config レポートに追加する<br>2. Accelerate の自動インシデントレポート<br>3. Accelerate の自動修復 |

追加のヘルプのリクエスト

> **Note**
>
> AMS は、修復カテゴリに関係なく、違反を修復できます。ヘルプをリクエストするには、サービスリクエストを送信し、AMS が修正するリソースを「AMS 設定ルールの修正の一環として、非苦情リソース *RESOURCE_ARNS_OR_IDs* リソース ARNs」などのコメントで指定し、違反を修正するために必要な入力を追加します。 IDs

AMS Accelerate には、非準拠のリソースの修復に役立つ AWS Systems Manager 自動化ドキュメントとランブックのライブラリがあります。

## を Config レポートに追加する

AMS は、アカウント内のすべてのルールとリソースのコンプライアンスステータスを追跡する Config レポートを生成します。CSDM にレポートをリクエストできます。Config コンソール、

AWS CLI、または AWS AWS Config API からコンプライアンスステータスを確認することもできます。Config レポートには以下が含まれます。

- 潜在的な脅威や設定ミスを検出するための、環境内の上位の非準拠リソース
- 時間の経過に伴うリソースと設定ルールのコンプライアンス
- Config ルールの説明、ルールの重要度、および非準拠リソースを修正するための推奨される修復手順

リソースが非準拠状態になると、Config レポートでリソースステータス (およびルールステータス) が非準拠になります。ルールが Config レポート専用修復カテゴリに属している場合、デフォルトでは AMS はそれ以上のアクションを実行しません。サービスリクエストをいつでも作成して、AMS に追加のヘルプや修復をリクエストできます。

詳細については、AWS 「Config Reporting」を参照してください。

## Accelerate の自動インシデントレポート

やや重大なルール違反の場合、AMS は自動的にインシデントレポートを作成し、リソースが非準拠状態になったことを通知し、実行するアクションを尋ねます。インシデントに対応するときは、次のオプションがあります。

- インシデントにリストされている非準拠リソースを AMS で修復するようリクエストします。次に、非準拠のリソースを修復し、基盤となるインシデントが解決されたら通知します。
- 非準拠の項目は、コンソールまたは自動デプロイシステム (CI/CD Pipeline テンプレートの更新など) で手動で解決できます。その後、インシデントを解決できます。非準拠リソースはルールのスケジュールに従って再評価され、リソースが非準拠として評価された場合、新しいインシデントレポートが作成されます。
- 非準拠のリソースを解決せず、単にインシデントを解決することを選択できます。後でリソースの設定を更新すると、 AWS Config は再評価をトリガーし、そのリソースのコンプライアンス違反を評価するように再度警告されます。

## Accelerate の自動修復

最も重要なルールは、自動修復カテゴリに属します。これらのルールに従わないと、アカウントのセキュリティと可用性に大きな影響を与える可能性があります。リソースが次のいずれかのルールに違反した場合：

1. AMS はインシデントレポートで自動的に通知します。

2. AMS は、自動 SSM ドキュメントを使用して自動修復を開始します。

3. AMS は、自動修復の成功または失敗でインシデントレポートを更新します。

4. 自動修復が失敗した場合、AMS エンジニアは問題を調査します。

## Accelerate でのルール例外の作成

AWS Config ルール リソース例外機能を使用すると、特定のルールの特定の非準拠リソースのレポートを抑制することができます。

> **Note**
>
> 除外されたリソースは、引き続き Config Service AWS コンソールで非準拠として表示されます。除外されたリソースには、Config レポート (resource_exception:True) に特別なフラグが表示されます。CSDMs は、レポートの生成時に、その列に従ってそれらのリソースを除外できます。

準拠していないことがわかっているリソースがある場合は、Config レポートで特定の設定ルールの特定のリソースを削除できます。これを実行するには:

レポートから除外される設定ルールとリソースのリストとともに、アカウントに対して Accelerate のサービスリクエストを送信します。明示的なビジネス上の根拠を提供する必要があります (たとえば、*resource_name_1* と *resource_name_2* はバックアップされないため、バックアップされないことを報告する必要はありません ) 。Accelerate サービスリクエストの送信については、「」を参照してくださいAccelerate でのサービスリクエストの作成。

リクエストに次の入力を貼り付け (図に示すように、すべての必須フィールドを含む個別のブロックをリソースごとに追加 ) 、送信します。

```
[
    {
        "resource_name": "resource_name_1",
        "config_rule_name": "config_rule_name_1",
        "business_justification": "REASON_TO_EXEMPT_RESOURCE",
        "resource_type": "resource_type"
    },
    {
        "resource_name": "resource_name_2",
```

```
        "config_rule_name": "config_rule_name_2",
        "business_justification": "REASON_TO_EXEMPT_RESOURCE",
        "resource_type": "resource_type"
    }
]
```

## Accelerate の AWS Config コストを削減する

オプションを使用してAWS::EC2::Instanceリソースタイプを定期的に記録することで、AWS Config のコストを削減できます。定期的な記録では、リソースの最新の設定変更を 24 時間に 1 回キャプチャし、配信される変更の数を減らします。有効にすると、 は 24 時間の終了時にリソースの最新の設定 AWS Config のみを記録します。これにより、継続的なモニタリングを必要としない特定の運用計画、コンプライアンス、監査のユースケースに合わせて設定データをカスタマイズできます。この変更は、エフェメラルアーキテクチャに依存するアプリケーションがある場合にのみ推奨されます。つまり、インスタンスの数を常にスケールアップまたはスケールダウンします。

AWS::EC2::Instance リソースタイプの定期的な記録をオプトインするには、AMS 配信チームにお問い合わせください。

## カスタマイズされた検出結果のレスポンス

AMS Accelerate が一部の検出結果にどのように応答するかを選択できます (非準拠の Config ルール )。検出結果に応答するように AMS を設定するには、検出結果を修正するか、修正の承認を求めるか、次回の月次ビジネスレビュー (MBR) で報告します。AMS Accelerate Config ルールのデフォルトのレスポンスを変更できます。ルールを確認するには、「Configuration Compliance > Table of rules」を参照するか、ルールテーブルを ZIP ファイル ams_config_rules.zip としてダウンロードします。

デフォルトのレスポンスを変更すると、より多くの検出結果を修復できるため、アカウントのセキュリティとコンプライアンスの状態を向上させることができます。さらに多くの検出結果を修復すると、手動によるレビューと承認を待つ必要があるケースが少なくなります。AMS 修復ランブックの広範なライブラリは、非準拠のリソースを常に修正し、必要な場合にのみ連絡されます。

カスタマイズされたレスポンスは、新しいリソースまたは新しいイベントを持つ既存のリソースでのみ使用されます。例えば、変更後に非準拠になったリソースなどです。これは、古いリソースは修復前により詳細な検査を必要とする傾向があり、作成または変更時にリソース修復を適用する方が簡単なためです。任意のリソースの結果の修復をいつでもリクエストするには、サービスリクエストを送信します。

## デフォルトレスポンスの変更のリクエスト

クラウドアーキテクト (CAs) は、オンボーディング中にユーザーと協力して設定を収集します。その後CAs は内部 AMS システムで初期設定をセットアップします。オンボーディング後、サービスリクエストを作成して、設定の更新をリクエストします。設定の更新は、必要な回数だけリクエストできます。Operations は、サービスリクエストが作成されたアカウントの設定のみを更新することに注意してください。複数のアカウントを同時に更新する必要がある場合は、Cloud Architect にお問い合わせください。CA は、監査目的で、ユーザー設定でサービスリクエストをカットするように要求します。

## 検出結果とアカウントのデフォルトレスポンスの変更

各アカウントと検出結果には、常にレスポンス設定が必要です。AMS はデフォルトのレスポンスを提供するため (「設定コンプライアンス」を参照 ) 、この設定はオプションです。各検出結果のデフォルトのレスポンスを次のオプションに変更できます。

- 修復: AMS は検出結果を手動でまたは自動的に修復します。AMS は修復を確認し、失敗したかどうかを知らせます。
- リクエストの承認: AMS は、結果を通知するアウトバウンドケースを作成します。このオプションは、修復を承認または除外する前に検出結果を確認する場合に使用します。その後、AMS は必要なアクションを実行します。
- アクションなし (レポートのみ): AMS は検出結果を修復またはエスカレーションするアクションを実行しません。結果は引き続きコンソールに表示され、レポートは MBRs中に表示されます。

> **Note**
>
> AMS で修正する必要があるルールの設定は変更できません。例えば、Amazon GuardDuty と VPC フローログを有効にします。

## リソースによるデフォルトのレスポンスの変更

タグを使用して、特定のリソースへのレスポンスをさらに設定できます。Resource Tagger を使用して、既存のタグまたはタグリソースを使用できます。詳細については、「」を参照してくださいリソースタガーの高速化 ) 。タグ付きのリソースの設定は、検出結果のデフォルトアクションよりも優先されます。リソースに関連付けられた設定が異なる複数のタグがある場合、AMS はカスタマイズされた修復を実行できません。代わりに、AMS は状況を通知するアウトバウンドサービスリクエス

トを送信します。たとえば、s3-bucket-server-side-encryption-enabled の検出結果では、次のことができます。

- タグキー値ペアが「Regulated: True」の「remediate」の暗号化されていない S3 バケットにレスポンスを変更します。
- 暗号化されていない S3 バケットに「規制: False」というタグが付いている場合、レスポンスを「アクションなし」に変更します。
- 暗号化されていない S3 バケットのデフォルトのレスポンスを「承認を求める」に変更します。これは、「Regulated: True」または「Regulated: False」というタグを持たないすべての S3 バケットに適用されます。

カスタム結果レスポンスを実行するために必要な入力を追加することもできます。たとえば、暗号化キーを必要とする修復の場合は、キー IDs を AMS に提供できます。修復ランブックの入力パラメータは変更できますが、AMS はカスタムランブックとの統合をサポートしていません。Config レポートの AMS 修復ランブックの説明については、「」を参照してくださいAWS Config コントロールコンプライアンスレポート。

# Accelerate でのインシデント対応

アラートを受信すると、AMS チームは自動修復と手動修復を使用してリソースを正常な状態に戻します。修復に失敗すると、AMS はインシデント管理プロセスを開始し、チームとコラボレーションします。設定ファイルのデフォルト設定を更新することで、ベースラインを変更できます。

## AMS Accelerate でのインシデント対応とオンボーディング

オンボーディング中、AMS Accelerate は既存の非準拠リソースの自動インシデント作成を抑制します。代わりに、Cloud Service Deliver Manager (CSDM) は、レビュー用のすべての非準拠ルールとリソースを含むレポートを提供します。AMS で修正するルールを特定したら、そのルールとリソースを示すサービスリクエストを サポート センターコンソールで作成します。次のサービスリクエストテンプレートは、非準拠リソースを手動で修復するための AMS への顧客リクエストの例です。AMS にその他の質問がある場合、サービスリクエストでお客様と協力して必要な情報を収集します。

```
Hello,
Please remediate the following resources for the Config Rule "ENCRYPTED_VOLUMES".
Resource List:
    "Vol-12345678"
    "Vol-87654312"
```

```
Thank you
```

オンボーディングプロセスが完了すると、AMS Accelerate は自動インシデントとしてマークされたルールの非準拠リソースごとにインシデントを自動的に作成します。

## Accelerate の耐障害性

AWS グローバルインフラストラクチャは、 AWS リージョン とアベイラビリティー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、物理的に分離された複数のアベイラビリティーゾーン AWS リージョン を提供します。アベイラビリティーゾーンを使用すると、中断することなくゾーン間で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できます。 アベイラビリティーゾーンは、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、耐障害性、スケーラビリティに優れています。

AWS リージョン およびアベイラビリティー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。

AMS Accelerate 継続性管理の詳細については、「」を参照してくださいAMS Accelerate での継続的な管理。

## 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「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。

## Accelerate のセキュリティのベストプラクティス

AMS Accelerate はコンフォーマンスパックを使用します。コンフォーマンスパックは、マネージドアクションまたはカスタム AWS Config ルール アクションと AWS Config 修復アクションを使用して、セキュリティ、運用、またはコスト最適化のガバナンスチェックを作成できるように設計された汎用コンプライアンスフレームワークを提供します。これらのコンフォーマンスパックを最適に設定する方法については、 AWS Config「Operational Best Practices for NIST CSF」および「Operational Best Practices for CIS Top 20」を参照してください。

## 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 Accelerate の技術標準 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 Accelerate 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、変更レビューは承認されたセキュリティ担当者によって承認または拒否されます。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。

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に対応できます。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、リクエ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 Accelerate の技術標準

Accelerate の技術標準カテゴリは次のとおりです。

| ID | カテゴリ |
| --- | --- |
| AMS-STD-X002 | AWS Identity and Access Management |
| AMS-STD-X003 | ネットワークセキュリティ |
| AMS-STD-X004 | 侵入テスト |
| AMS-STD-X005 | Amazon GuardDuty |
| AMS-STD-X007 | ログ記録 |

## AMS Accelerate 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-X002 - 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 | Microsoft Windows Server の RDP セッションタイムアウトは 15 分に設定され、ユースケースに基づいて延長できます。 |
| 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 | 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。 |
| 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 バケットのオブジェクト (S3:GetObject など) の読み取りは許可されません。 |
| 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はリスク通知になります。 |

| ID | 技術標準 |
| --- | --- |
| | ただし、アカウント内のすべての S3 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 | 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 (書き込みとアクセス許可の管理) を持つコンソールおよびプログラムによるアクセス用の IAM ユーザーとロールは、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。 |
| 3.3 | Microsoft Windows Server では、Microsoft グループ Managed Service Account (gMSA) のみを作成する必要があります。 |
| 4.0 | ポリシー、アクション、APIs |
| 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。 |
| 4.6 | 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。 |
| 4.8 | Amazon Route 53 の AMS インフラストラクチャ DNS レコードへの変更は許可されません。 |

| ID | 技術標準 |
| --- | --- |
| 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。 |
| 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。 |
| 4.12 | IAM ポリシーには、AMS Amazon CloudWatch ロググループの 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 | 顧客アカウントでまだ作成されていない S3 バケット ARN へのアクセスは、サービス固有の S3 条件キー s3:ResourceAccount を使用してアカウント番号を指定することで、バケットへのアクセスを顧客アカウントに制限することで提供できます。 |
| 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 関連のフルアクセス許可は、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。 |
| 4.17 | CLI の代わりに、お客様のロールにアクセス AWS CloudShell 許可を付与できます。 |

| ID | 技術標準 |
| --- | --- |
| 4.18 | 信頼できるプリンシパルとして AWS サービスを使用する IAM ロールも、IAM 技術標準に準拠して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) は、IAM サービスチームによって構築および管理されるため、AMS IAM 技術標準の対象ではありません。 |
| 4.20 | IAM ポリシーでは、アカウント内のすべての S3 バケットのオブジェクト (S3:GetObject など) の読み取りを許可しないでください。 |
| 4.21 | リソースタイプ「savingsplan」のすべての 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 オブジェクト、データベースなど) を手動でコピーまたは移動することはできません。 Amazon Relational Database Service DynamoDB |
| 6.0 | クロスアカウントポリシー |
| 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 ) 。 |

| ID | 技術標準 |
| --- | --- |
| 6.3 | IAM ロールは、リスクを受け入れることなく、AMS アカウントとサードパーティーアカウント間の信頼ポリシーを設定することはできません。 |
| 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。 |
| 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。 |

| ID | 技術標準 |
| --- | --- |
| 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 ) 。 |
| 6.10 | 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。 |
| 6.11 | 書き込みアクセス権を持つ 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 |

| ID | 技術標準 |
| --- | --- |
| 7.1 | 読み取り専用アクセス許可と非ミューテーション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 |
| 8.4 | 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 | 顧客が別のポリシーを明示的に指定しない限り、顧客リソースには最小特権のリソースベースのポリシーを設定する必要があります。 |

AMS-STD-X003 - ネットワークセキュリティ

X003 - Network Security の標準コントロールは次のとおりです。

| ID | 技術標準 |
| --- | --- |
| | ネットワーク |
| 1.0 | 将来のコントロール用に予約済み |
| 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。 |
| 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 |

| ID | 技術標準 |
| --- | --- |
| 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 の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、セキュリティグループ経由で 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 | お客様のプライベート 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。 |

| ID | 技術標準 |
| --- | --- |
| 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 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参照します。 |
| 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す。 |
| 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。 |

| ID | 技術標準 |
| --- | --- |
| 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。 |
| 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 | 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。 |
| 24.0 | 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。 |
| 25.0 | 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。 |
| 26.0 | 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。 |

| ID | 技術標準 |
| --- | --- |
| 27.0 | セキュリティグループ共有 |
| 27.1 | セキュリティグループがこのセキュリティ基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。 |
| 27.2 | 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-X004 - 侵入テスト

X004 - 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-X005 - GuardDuty

X005 - GuardDuty の標準コントロールを次に示します。

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. 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。

3. 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。

AMS-STD-X007 - ログ記録

X007 - ログ記録の標準コントロールを次に示します。

| 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 サーバーアクセスログ記録: 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。 |
| 1.7 | 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 |

| ID | 技術標準 |
| --- | --- |
| | 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 |
| 2.3 | 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、お客様が認可したセキュリティ担当者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。 |

| ID | 技術標準 |
| --- | --- |
| 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 日間以上保持できる必要があります。 |
| 4.0 | Encryption |
| 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 |
| 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。つまり、AMS チームに必要な AWS CloudTrail 証跡に「ログファイルの検証」を設定します。 |
| 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 | すべてのログを AMS から非 AMS アカウントに転送できるのは、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 (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 PAYER リンクアカウントと照合する) のみです。 |

# 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

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力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。
- High_Risk-LOG-002: VPC フローログを無効にします。
- 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 (顧客が所有していない) 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) による口グ転送
- High_Risk-LOG-004: CloudTrail に非 AMS 証跡を使用する

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

# セキュリティに関するよくある質問

AMS は、グローバルオペレーションセンターを通じて 24 時間 365 follow-the-sunサポートを提供します。専有 AMS オペレーションエンジニアは、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ます。通常、AMS は自動化を通じてアカウントを管理します。特定のトラブルシューティングやデプロイの専門知識を必要とするまれな状況では、AMS オペレーションエンジニアがアカウントにアクセスすることがあります AWS 。

以下は、AMS Accelerate が AMS オペレーションエンジニアまたはオートメーションがアカウントにアクセスするときに使用するセキュリティのベストプラクティス、コントロール、アクセスモデル、監査メカニズムに関する一般的な質問です。

## AMS オペレーションエンジニアはいつ環境にアクセスしますか？

AMS オペレーションエンジニアは、アカウントまたはインスタンスに永続的にアクセスできません。顧客アカウントへのアクセスは、アラート、インシデント、変更リクエストなどの正当なビジネ

スユースケースに対してのみ AMS オペレーターに付与されます。アクセスは AWS CloudTrail ログに記録されます。

アクセスの根拠、トリガー、トリガーイニシエータについては、「」を参照してくださいAMS カスタマーアカウントアクセストリガー。

## AMS オペレーションエンジニアは、アカウントにアクセスするときにどのようなロールを引き受けますか？

環境への人的介入を必要とするまれなケース (約 5%) では、AMS オペレーションエンジニアはデフォルトの読み取り専用アクセスロールを使用してアカウントにログインします。デフォルトのロールは、Amazon Simple Storage Service、Amazon Relational Database Service、Amazon DynamoDB、Amazon Redshift、Amazon ElastiCache など、データストアに一般的に保存されているコンテンツにアクセスできません。

AMS オペレーションエンジニアとシステムがアカウントでサービスを提供するために必要なロールのリストについては、「」を参照してくださいAMS カスタマーアカウントアクセス IAM ロール。

## AMS オペレーションエンジニアが自分のアカウントにアクセスする方法

カスタマーアカウントにアクセスするために、AMS オペレーションエンジニアは AWS 内部 AMS アクセスサービスを使用します。この内部サービスは、アカウントへのアクセスが安全で監査されるように、安全なプライベートチャネルを介してのみ使用できます。

1. AMS オペレーションエンジニアは、内部 AMS アクセスサービス認証と 2 要素認証を使用します。また、オペレーションエンジニアは、 AWS アカウントへのアクセスの必要性を概説するビジネス上の根拠 (インシデントチケットまたはサービスリクエスト ID) を提供する必要があります。
2. オペレーションエンジニアの認可に基づいて、AMS アクセスサービスは、適切なロール (only/Operator/Admin) と AWS コンソールへのログイン URL をエンジニアに提供します。アカウントへのアクセスは有効期間が短く、期限があります。
3. Amazon EC2 インスタンスにアクセスするために、AMS オペレーションエンジニアはブローカーと同じ内部 AMS アクセスサービスを使用します。アクセスが許可されると、AMS オペレーションエンジニアは AWS Systems Manager Session Manager を使用して、存続期間の短いセッション認証情報でインスタンスにアクセスします。

   Windows インスタンスの RDP アクセスを提供するために、オペレーションエンジニアは Amazon EC2 Systems Manager を使用してインスタンスにローカルユーザーを作成し、インス

タンスへのポート転送を確立します。オペレーションエンジニアは、インスタンスへの RDP アクセスにローカルユーザー認証情報を使用します。ローカルユーザーの認証情報は、セッションの終了時に削除されます。

次の図は、AMS オペレーションエンジニアがアカウントにアクセスするために使用するプロセスの概要を示しています。

## AMS マネージド AWS アカウントで AMS によって行われた変更を追跡するにはどうすればよいですか？

### アカウントアクセス

自動化または AMS Accelerate オペレーションチームによる変更を追跡しやすくするために、AMS は Amazon Athena コンソールと AMS Accelerate ログで変更レコード SQL インターフェイスを提供します。これらのリソースは、以下の情報を提供します。

- アカウントにアクセスしたユーザー。
- アカウントがいつアクセスされたか。
- アカウントへのアクセスに使用された権限。
- アカウントで AMS Accelerate によってどのような変更が行われたか。
- アカウントで変更が行われた理由。

### リソース設定

CloudTrail ログを表示して、過去 90 日間の AWS リソースの設定を追跡します。設定が 90 日より古い場合は、Amazon S3 のログにアクセスします。

### インスタンスログ

Amazon CloudWatch エージェントはオペレーティングシステムのログを収集します。CloudWatch ログを表示して、オペレーティングシステムがサポートするログインログやその他のアクションログを確認します。

詳細については、「AMS Accelerate アカウントの変更の追跡」を参照してください。

## AMS オペレーションエンジニアが自分のアカウントにアクセスするためのプロセスコントロールは何ですか？

AMS に参加する前に、オペレーションエンジニアは犯罪の身元調査を行います。AMS エンジニアはお客様のインフラストラクチャを管理するため、毎年のバックグラウンドチェックも必須です。エンジニアがバックグラウンドチェックに失敗すると、アクセスは取り消されます。

すべての AMS オペレーションエンジニアは、リソースへのアクセスを許可する前に、インフラストラクチャセキュリティ、データセキュリティ、インシデント対応などの必須のセキュリティトレーニングを完了する必要があります。

## 特権アクセスはどのように管理されますか？

ユーザーのサブセットは、追加のトレーニングを完了し、昇格されたアクセス権を維持する必要があります。アクセスと使用状況は検査および監査されます。AMS は、特権アクセスを例外的な状況、または最小特権アクセスがリクエストを満たせない状況に制限します。特権アクセスも時間制限があります。

## AMS オペレーションエンジニアは MFA を使用していますか？

はい。すべてのユーザーは、MFA とプレゼンス証明を使用してサービスを提供する必要があります。

## AMS 従業員が組織を離れたり、職務を変更したりした場合、アクセスはどうなりますか？

お客様のアカウントとリソースへのアクセスは、内部グループメンバーシップを通じてプロビジョニングされます。メンバーシップは、特定の職務ロール、レポートマネージャー、AMS での雇用ステータスなど、厳格な基準に基づいています。オペレーションエンジニアのジョブファミリーが変更されるか、そのユーザー ID が無効になっている場合、アクセスは取り消されます。

## アカウントへの AMS オペレーションエンジニアのアクセスを管理するアクセスコントロールは何ですか？

環境へのアクセスに「知る必要がある」原則と「最小特権」原則を適用するには、複数の技術的コントロールレイヤーがあります。アクセスコントロールのリストを次に示します。

- カスタマーアカウントとリソースにアクセスするには、すべてのオペレーションエンジニアが特定の内部 AWS グループの一部である必要があります。グループメンバーシップは、厳密に知る必要性に基づいており、事前定義された基準で自動化されています。
- AMS は、環境への「非永続化」アクセスを実践します。つまり、AMS オペレーションによる AWS アカウントへのアクセスは、有効期間の短い認証情報によるjust-in-time」です。アカウントへのアクセスは、社内のビジネスケースの根拠 (サービスリクエスト、インシデント、変更管理リクエストなど) が送信およびレビューされた後にのみ提供されます。
- AMS は最小特権の原則に従います。したがって、承認されたオペレーションエンジニアはデフォルトで読み取り専用アクセスを引き受けます。書き込みアクセスは、インシデントまたは変更リクエストのために環境の変更が必要な場合にのみ、エンジニアが使用します。
- AMS は、「ams」プレフィックスを使用してアカウントをモニタリングおよび管理する、標準で簡単に識別できる AWS Identity and Access Management ロールを使用します。すべてのアクセスは、監査のためにログイン AWS CloudTrail されます。
- AMS は、自動バックエンドツールを使用して、変更実行の顧客情報検証フェーズ中にアカウントへの不正な変更を検出します。

## AMS はルートユーザーアクセスをどのようにモニタリングしますか？

ルートアクセスは常にインシデント対応プロセスをトリガーします。AMS は Amazon GuardDuty 検出を使用してルートユーザーのアクティビティをモニタリングします。GuardDuty がアラートを生成すると、AMS はさらに調査するためのイベントを作成します。AMS は、予期しないルートアカウントアクティビティが検出されると通知し、AMS セキュリティチームが調査を開始します。

## AMS はセキュリティインシデントにどのように対応しますか？

AMS は、Amazon GuardDuty、Amazon Macie などの検出サービス、およびお客様が報告したセキュリティ問題から生成されたセキュリティイベントを調査します。AMS はセキュリティ対応チームと協力して、セキュリティインシデント対応 (SIR) プロセスを実行します。AMS SIR プロセスは、NIST SP 800-61 Rev. 2、Computer Security Incident Handling Guide フレームワークに基づいており、24/7/365 follow-the-sunセキュリティレスポンスを提供します。AMS はお客様と協力して、セキュリティインシデントを迅速に分析して封じ込めます。

## AMS はどのような業界標準の認定とフレームワークに準拠していますか？

他の AWS サービスと同様に、AWS Managed Services は
OSPAR、HIPAA、HITRUST、GDPR、SOC*、ISO*、FedRAMP (Medium/High)、IRAP、PCI の認

定を受けています。 AWS に沿った顧客コンプライアンス証明書、規制、フレームワークの詳細については、「AWS Compliance」を参照してください。

セキュリティガードレール

AWS Managed Services は、複数のコントロールを使用して情報アセットを保護し、 AWS インフラストラクチャを安全に保つのに役立ちます。AMS Accelerate は、アカウントがセキュリティと運用の整合性に関する業界標準に準拠していることを確認するために、 AWS Config ルールと修復アクションのライブラリを維持します。 AWS Config ルールは、記録されたリソースの設定変更を継続的に追跡します。変更がルールの条件に違反すると、AMS はその検出結果を報告します。違反の重大度に応じて、違反を自動またはリクエストで修正できます。

AMS は AWS Config ルールを使用して、以下の規格の要件を満たすのに役立ちます。

- Center for Internet Security (CIS)
- 米国国立標準技術研究所 (NIST) クラウドセキュリティフレームワーク (CSF)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry (PCI) データセキュリティ標準 (DSS)

詳細については、AMS Accelerate のセキュリティ管理を参照してください。

## セキュリティ証明書、フレームワーク、コンプライアンスに関する最新のレポートにアクセスするにはどうすればよいですか AWS？

AWS サービスの現在のセキュリティおよびコンプライアンスレポートは、次の方法で確認できます。

- を使用してAWS Artifact、 AWS サービスのセキュリティ、可用性、機密性に関する最新のレポートをダウンロードすることができます。
- グローバルコンプライアンスフレームワークに準拠している AWS Managed Services を含むほとんどの AWS サービスのリストについては、「」を参照してくださいhttps://aws.amazon.com/compliance/services-in-scope/。たとえば、PCI を選択し、AWS Managed Servicesを検索します。

  「AMS」を検索して、AMS マネージド AWS アカウントから AMS 固有のセキュリティアーティファクトを検索できます。AWS Managed Services SOC 3 の対象です。

- AWS SOC 2 (System and Organizations Controls) レポートが AWS Artifact リポジトリに発行されます。このレポートは、米国認定会計士協会 (AICPA) TSP セクション 100、Trust Services Criteria のセキュリティ、可用性、機密性の基準を満たす AWS コントロールを評価します。

## AMS は、AMS 機能のさまざまな側面のリファレンスアーキテクチャ図を共有していますか？

AMS リファレンスアーキテクチャを表示するには、AWS Managed Services for Proactive Monitoring PDF をダウンロードします。

## AMS は、アカウントにアクセスするユーザーと、アクセスのためのビジネスニーズをどのように追跡しますか？

サービスの継続性とアカウントのセキュリティをサポートするために、AMS は、プロアクティブなヘルスまたはメンテナンス、ヘルスまたはセキュリティイベント、計画されたアクティビティ、または顧客のリクエストに応答してのみ、アカウントまたはインスタンスにアクセスします。アカウントへのアクセスは、AMS Accelerate のアクセスモデルで説明されているように、AMS プロセスを通じて承認されます。これらの認可フローには、意図しないアクセスや不適切なアクセスを防ぐためのガードレールが含まれています。アクセスフローの一環として、AMS はビジネスニーズを認可システムに提供します。このビジネスニーズは、AMS で開いたケースなど、アカウントに関連付けられた作業項目である場合があります。または、ビジネスニーズは、パッチソリューションなどの承認されたワークフローである可能性があります。すべてのアクセスには、アクセスリクエストをビジネスニーズに合わせるために、ビジネスルールに基づいて内部 AMS システムによってリアルタイムで検証、検証、承認される根拠が必要です。

AMS オペレーションエンジニアには、有効なビジネスニーズがないとアカウントにアクセスするためのパスは与えられません。すべてのアカウントアクセスおよび関連するビジネスニーズは、 AWS アカウント内の AWS CloudTrail エントリに出力されます。これにより、完全な透明性が得られ、独自の監査と検査を実行する機会が得られます。検査に加えて、AMS は自動検査を行い、必要に応じてアクセスリクエストの手動検査を行い、ツールと人間によるアクセスの監査を実行して異常なアクセスを確認します。

## AMS エンジニアは、Amazon S3、Amazon RDS、DynamoDB、Amazon Redshift などの AWS データストレージサービスに保存されているデータにアクセスできますか？

AMS エンジニアは、データストレージに一般的に使用される AWS サービスに保存されている顧客コンテンツにアクセスできません。これらのサービスのデータの読み取り、書き込み、変更、または削除に使用される AWS APIs へのアクセスは、AMS エンジニアアクセスに使用される IAM ロールに関連付けられた明示的な IAM 拒否ポリシーによって制限されます。さらに、内部 AMS ガードレールとオートメーションにより、AMS オペレーションエンジニアは拒否条件を削除または変更できなくなります。

## AMS エンジニアは、Amazon EBS、Amazon EFS、Amazon FSx に保存されている顧客データにアクセスできますか？

AMS エンジニアは、管理者として Amazon EC2 インスタンスにログインできます。オペレーティングシステム (OS) の問題やパッチ障害など、特定のシナリオでの修復には管理者アクセスが必要です。AMS エンジニアは通常、検出された問題を修正するためにシステムボリュームにアクセスします。ただし、AMS エンジニアのアクセスは、システムボリュームに制限または制限されません。

## 環境に対する高い権限を持つオートメーションロールのアクセスは、どのように制限または制御されますか？

`ams-access-admin` ロールは AMS オートメーションでのみ使用されます。これらのオートメーションは、テレメトリ、ヘルス、セキュリティのデータ収集のために AMS が環境にデプロイして運用機能を実行するために必要なリソースをデプロイ、管理、維持します。AMS エンジニアは自動化ロールを引き受けることができず、内部システムのロールマッピングによって制限されます。実行時に、AMS はスコープダウンされた最小特権セッションポリシーをすべてのオートメーションに動的に適用します。このセッションポリシーは、オートメーションの機能とアクセス許可を制限します。

## AMS は、自動化ロールの AWS Well-Architected フレームワークで提唱されている最小特権の原則をどのように実装していますか？

実行時に、AMS はスコープダウンされた最小特権のセッションポリシーをすべてのオートメーションに適用します。このスコープダウンされたセッションポリシーは、自動化の機能とアクセス許可を制限します。IAM リソースを作成するアクセス許可を持つセッションポリシーには、アクセス許可の境界をアタッチする必要もあります。このアクセス許可の境界により、特権のエスカレーションリ

スクが軽減されます。すべてのチームは、そのチームによってのみ使用されるセッションポリシーをオンボードします。

## オートメーションロールに関連する不正アクセスの試みや疑わしいアクティビティを検出するために、どのようなログ記録およびモニタリングシステムが使用されますか？

AWS は、 AWS サービスチームによる内部使用のためのコアログアーカイブ機能を提供する一元化されたリポジトリを維持します。これらのログは、スケーラビリティ、耐久性、可用性を高めるために Amazon S3 に保存されます。 AWS サービスチームは、中央ログサービスでサービスログを収集、アーカイブ、表示できます。

の本番稼働用ホスト AWS は、マスターベースラインイメージを使用してデプロイされます。ベースラインイメージには、セキュリティ上の理由からログ記録とモニタリングを含む標準的な設定と関数のセットが用意されています。これらのログは、 AWS セキュリティインシデントが疑われる場合に根本原因分析のためにセキュリティチームによって保存され、アクセス可能です。

特定のホストのログは、そのホストを所有するチームが利用できます。チームは、運用分析とセキュリティ分析のためにログを検索できます。

## オートメーションインフラストラクチャに関するセキュリティインシデントや違反はどのように処理され、どのようなプロトコルが迅速な対応と緩和に役立ちますか？

AWS 緊急時対応計画とインシデント対応プレイブックでは、セキュリティインシデントを検出、軽減、調査、評価するためのツールとプロセスを定義し、テストしています。これらの計画とプレイブックには、契約上および規制上の要件に従って潜在的なデータ侵害に対応するためのガイドラインが含まれています。

## オートメーションインフラストラクチャでは、定期的なセキュリティ評価、脆弱性スキャン、侵入テストを実施していますか？

AWS セキュリティは、さまざまなツールを使用して AWS 、環境内のホストオペレーティングシステム、ウェブアプリケーション、データベースに対して定期的に脆弱性スキャンを実行します。 AWS セキュリティチームは、該当するベンダーの欠陥に関するニュースフィードをサブスクライブし、ベンダーのウェブサイトやその他の関連コンセントに新しいパッチがないかプロアクティブにモニタリングします。

## オートメーションインフラストラクチャへのアクセスは、承認された担当者のみに制限されるのですか？

AWS システムへのアクセスは、最小特権に基づいて割り当てられ、承認された個人によって承認されます。 AWS システムの不正または意図しない変更や誤用を減らすために、職務と責任領域 (アクセスのリクエストと承認、変更管理のリクエストと承認、変更の開発、テストとデプロイなど) は異なる個人間で分離されます。グループアカウントまたは共有アカウントは、システム境界内では許可されません。

## セキュリティ標準を維持し、オートメーションパイプラインでの不正アクセスやデータ侵害を防ぐために、どのような対策が実装されていますか？

サービス、ホスト、ネットワークデバイス、Windows および UNIX グループなどのリソースへのアクセスは、適切な所有者またはマネージャーによって AWS 独自のアクセス許可管理システムで承認されます。アクセス許可管理ツールログは、アクセス変更のリクエストをキャプチャします。ジョブ関数の変更により、従業員のリソースへのアクセスが自動的に取り消されます。その従業員の継続的なアクセスは、リクエストおよび承認される必要があります。

AWS では、リモートロケーションから内部 AWS ネットワークへの認証に、承認された暗号化チャネルを介した 2 要素認証が必要です。ファイアウォールデバイスは、コンピューティング環境へのアクセスを制限し、コンピューティングクラスターの境界を適用し、本番稼働用ネットワークへのアクセスを制限します。

プロセスは、監査情報と監査ツールを不正アクセス、変更、削除から保護するために実装されます。監査レコードには、必要な分析要件をサポートするために、一連のデータ要素が含まれています。さらに、監査レコードは、セキュリティ関連またはビジネスに影響を与えるイベントに応じて、承認されたユーザーがオンデマンドで検査または分析できます。

AWS システム (ネットワーク、アプリケーション、ツールなど) へのユーザーアクセス権は、終了または非アクティブ化されてから 24 時間以内に取り消されます。非アクティブなユーザーアカウントは、少なくとも 90 日ごとに無効または削除されます。

## 特権のエスカレーションやアクセスの誤用を検出して AMS チームにプロアクティブに警告するために、アクセスログ記録または監査ログ記録に対して異常検出またはモニタリングが有効になっていますか？

の本番稼働用ホスト AWS には、セキュリティ上の理由から ログ記録が用意されています。このサービスは、ログオン、失敗したログオン試行、ログオフなど、ホストに対するヒューマンアクション

を口グに記録します。これらの口グは、 AWS セキュリティインシデントが疑われる場合に根本原因分析のためにセキュリティチームによって保存され、アクセス可能です。特定のホストの口グは、そのホストを所有するチームでも利用できます。フロントエンドログ分析ツールは、サービスチームが運用およびセキュリティ分析のために口グを検索するために使用できます。プロセスは、口グと監査ツールを不正アクセス、変更、削除から保護するために実装されています。 AWS セキュリティチームは口グ分析を実行して、定義されたリスク管理パラメータに基づいてイベントを特定します。

## AMS マネージドアカウントから抽出される顧客データの種類と、その使用および保存方法

AMS は、お客様のコンテンツにいかなる目的でもアクセスまたは使用しません。AMS は、お客様またはエンドユーザーがお客様のアカウント AWS のサービス に関連して によって処理、保存、またはホスティング AWS するために に転送するソフトウェア (マシンイメージを含む ) 、データ、テキスト、オーディオ、ビデオ、またはイメージ、およびお客様またはエンドユーザーが の使用を通じて上記から派生する計算結果として、お客様のコンテンツを定義します AWS のサービス。

# AMS Accelerate でのモニタリングとイベント管理

AMS Accelerate 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 Accelerate 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、これらのリソースをモニタリングして、必要に応じて修復を実行します。

AMS Accelerate モニタリングシステムは、Resource Tagger や Alarm Manager などの内部ツールに依存し、 AWS のサービス、、Amazon CloudWatch (CloudWatch)AWS AppConfig、Amazon EventBridge (旧称 CloudWatch)、Amazon GuardDuty、Amazon Macie、 などの を活用します AWS Health。

AMS Accelerate は、運用上の優秀性の実現に役立つさまざまな運用サービスを提供します AWS。24 時間 365 日体制のヘルプデスク、プロアクティブモニタリング、セキュリティ、パッチ適用、ログ記録、バックアップなど、いくつかの主要な運用機能 AWS クラウド を使用して、AMS がで全体的な運用上の優秀性を達成するのに役立つ方法をすばやく理解するには、「AMS リファレンスアーキテクチャ図」を参照してください。

トピック

- モニタリングとは
- モニタリングの仕組み
- AMS でのベースラインモニタリングからのアラート
- AMS でのアプリケーション対応インシデント通知
- アラームマネージャーの高速化
- アラートの AMS 自動修復
- AMS での Amazon EventBridge マネージドルールの使用
- AMS の信頼された修復

Amazon EKS のモニタリングについては、「」を参照してください。 AMS Accelerate での Amazon EKS のモニタリングとインシデント管理

## モニタリングとは

AMS Accelerate モニタリングには以下の利点があります。

- 選択したすべての またはサポートされている AWS リソースについて、マネージドアカウント全体でポリシーを作成、管理、デプロイするデフォルト設定。
- マネージドアカウントに対して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持つモニタリングベースライン。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。
- 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 AMS オペレーションによるアラートの自動修復。たとえば、スタンドアロンの 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を可視化します。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
- アラートを調査して、適切なアクションを決定します。詳細については、「AMS Accelerate でのインシデント管理」を参照してください。
- 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。

# 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 Accelerate のモニタリングアーキテクチャを示しています。

リソースが Resource Tagger を使用して定義されたポリシーに基づいてタグ付けされ、アラーム定義がデプロイされた後、次のリストで AMS モニタリングプロセスについて説明します。

- 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。
- 集約: 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 Amazon 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。
- 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が作成され、AMS はインシデント管理プロセスに従います。

    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: Amazon EC2 インスタンスでの 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. 解決後: 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。最後のケースコレスポンデンスからの時間が、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: `key = OwnerTeamEmail`、 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*。タグ付け戦略に関する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 でのベースラインモニタリングからのアラート

AMS Accelerate の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 Accelerate 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、カスタム設定ドキュメントで変更することも、サービスリクエストを送信することもできます。カスタムアラーム設定を変更する手順については、「」を参照してくださいAccelerate アラーム設定の変更。アラームがしきい値を超えたときに通知を受け取るには、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できます。手順については、「アラームマネージャーの高速化」を参照してください。

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 Accelerate 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

Accelerate 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。

ベースラインモニタリングからのアラート

| サービス/リソースタイプ | アラートソースとトリガーの条件 | アラート名とメモ |
| --- | --- | --- |
| 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 は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、Direct-Customer-Alerts SNS トピックにオプトインすると、これらのアラートは E メールに直接送信されます。 | | |
| Application Load Balancer インスタンス | ApplicationLoadBalancerErrorCount<br><br>(HTTPCode_ELB_5XX_Count/RequestCount)*100<br><br>sum > 15% for 1 min, 5 consecutive times。 | Application LoadBalancer HTTP 5XX エラー数<br><br>Loadbalancer によって生成された過剰な数の HTTP 5XX レスポンスコードに対する CloudWatch アラーム。 |
| Application Load Balancer インスタンス | RejectedConnectionCount<br><br>sum > 0% for 1 min, 5 consecutive times。 | Application LoadBalancer が拒否した接続数<br><br>ロードバランサーが最大数に達したために拒否された接続の数がある場合の CloudWatch アラーム |
| Application Load Balancer ターゲット | TargetConnectionErrorCount<br><br>(HTTPCode_Target_5XX_Count/RequestCount)*100<br><br>sum > 15% for 1 min, 5 consecutive times。 | ${ElasticLoadBalancingV2::TargetGroup::FullName} - Application LoadBalancer ターゲット接続エラー数 - ${ElasticLoadBalancingV2::TargetGroup::UUID} |

| サービス/リソースタイプ | アラートソースとトリガーの条件 | アラート名とメモ |
| --- | --- | --- |
| | | ターゲットによって生成された HTTP 5XX レスポンスコードの超過数に関する CloudWatch アラーム。 |
| Application Load Balancer ターゲット | ApplicationLoadBalancerTargetGroupErrorCount<br><br>sum > 0% for 1 min, 5 consecutive times。 | ${ElasticLoadBalancingV2::TargetGroup::FullName} - Application LoadBalancer ターゲット HTTP 5XX エラー数 - ${ElasticLoadBalancingV2::TargetGroup::UUID}<br><br>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 - すべての OSs | CPUUtilization*<br><br>> 5 分間 95%、連続 6 回。 | ${EC2::InstanceId}: CPU が高すぎる<br><br>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。<br><br>これらは Direct-Customer-Alerts アラームです。 |

| サービス/リソースタイプ | アラートソースとトリガーの条件 | アラート名とメモ |
| --- | --- | --- |
| Amazon EC2 インスタンス - すべての OSs | StatusCheckFailed<br><br>> 0%、5 分間、3 回連続。 | ${EC2::InstanceId}: ステータスチェックに失敗しました<br><br>CloudWatch アラーム。ステータスチェック失敗 は、指定された ID を持つ Amazon EC2 インスタンスが 1 つ以上の自動ステータスチェックに失敗したことを示します。つまり、インスタンスが正しく動作したり、到達できない問題が発生しています。 |
| Amazon EC2 インスタンス - Linux | 最小 mem_used_percent<br><br>>= 5 分間 95%、連続 6 回。 | ${EC2::InstanceId}: メモリフリー<br><br>CloudWatch アラーム。Memory Free は、指定された Amazon EC2 インスタンスで使用可能なメモリ (RAM) が定義されたしきい値を下回ったことを示します。これにより、メモリの問題、システムのクラッシュが発生し、インスタンスがより多くの RAM を必要とする可能性があることを示します。<br><br>これらは Direct-Customer-Alerts アラームです。 |

| サービス/リソースタイプ | アラートソースとトリガーの条件 | アラート名とメモ |
| --- | --- | --- |
| Amazon EC2 インスタンス - Linux | 平均 Swap_used_percent<br><br>>= 5 分間 95%、連続 6 回。 | ${EC2::InstanceId}: スワップ無料<br><br>CloudWatch アラーム。Amazon EC2 インスタンスの平均 Swap_used_percent は、現在使用されている割り当てられたスワップ領域の平均割合が事前定義されたしきい値を超えていることを示します。これにより、パフォーマンスの低下、ボトルネック、メモリの問題が発生する可能性があります。<br><br>これらは Direct-Customer-Alerts アラームです。 |
| Amazon EC2 インスタンス - Linux | 最大 disk_used_percent<br><br>>= 5 分間 95%、連続 6 回。 | ${EC2::InstanceId}: ディスク使用率が高すぎる - ${EC2::Disk::UUID}<br><br>CloudWatch アラーム。ディスク使用率が高すぎるとは、特定の Amazon EC2 または識別されたディスクのディスク使用率が容量に近づいていることを示します。これにより、パフォーマンスの低下、アプリケーションエラー、システムの不安定性が発生する可能性があります。<br><br>これらは Direct-Customer-Alerts アラームです。 |

| サービス/リソースタイプ | アラートソースとトリガーの条件 | アラート名とメモ |
| --- | --- | --- |
| Amazon EC2 インスタンス - Windows | 使用中の最小メモリコミットバイト率<br><br>>= 5 分間 95%、連続 6 回。 | ${EC2::InstanceId}: メモリフリー<br><br>CloudWatch アラーム。Memory Free は、指定された Amazon EC2 インスタンスで使用可能なメモリ (RAM) が定義されたしきい値を下回ったことを示します。これにより、メモリの問題、システムのクラッシュが発生し、インスタンスがより多くの RAM を必要とする可能性があることを示します。<br><br>これらは Direct-Customer-Alerts アラームです。 |
| Amazon EC2 インスタンス - Windows | 最大 LogicalDisk % 空き容量<br><br><= 5%、5 分間、6 回連続。 | ${EC2::InstanceId}: ディスク使用率が高すぎる - ${EC2::Disk::UUID}<br><br>CloudWatch アラーム。Amazon EC2 Windows インスタンス内の論理ディスク (ファイルシステムパーティション) の空き領域の割合が、事前定義されたしきい値を超えていることを示します。ディスク容量が不足すると、ディスク容量が不足する可能性があります。<br><br>これらは Direct-Customer-Alerts アラームです。 |

| サービス/リソースタイプ | アラートソースとトリガーの条件 | アラート名とメモ |
| --- | --- | --- |
| Amazon EFS | AMSEFSBurstCreditBalanceExhausted。<br><br>BurstCreditBalance が 15 分間 1000 未満。 | ${EFS::FileSystemId}: EFS: バーストクレジット残高<br><br>Amazon EFS ファイルシステムの BurstCreditBalance の CloudWatch アラーム。 |
| Amazon EFS | AMSEFSClientConnectionsLimit。<br><br>ClientConnections > 24,000 を 15 分間。 | ${EFS::FileSystemId}: EFS: クライアント接続の制限<br><br>Amazon EFS ファイルシステムの ClientConnections の CloudWatch アラーム。 |
| Amazon EFS | AMSEFSThroughputUtilizationLimit。<br><br>EFS スループット使用率 > 80% を 1 時間。 | ${EFS::FileSystemId}: EFS: スループット使用率の制限<br><br>Amazon EFS ファイルシステムのスループット使用率に関する CloudWatch アラーム。 |
| Amazon EFS | AMSEFSPercentIOLimit。<br><br>PercentIOLimit > 95 を 75 分間。 | ${EFS::FileSystemId}: EFS: PercentIOLimit<br><br>Amazon EFS ファイルシステムの PercentIOLimit の CloudWatch アラーム。 |
| Amazon EKS | 「Amazon EKS」を参照してくださいAMS Accelerate での Amazon EKS のモニタリングとインシデント管理のベースラインアラート。 | |

| サービス/リソースタイプ | アラートソースとトリガーの条件 | アラート名とメモ |
| --- | --- | --- |
| Elastic Load Balancing インスタンス | SpilloverCountBackendConnectionErrors<br><br>> 1 を 1 分間、15 回連続。 | Classic LoadBalancer のスピルオーバーカウントアラーム<br><br>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。 |
| Elastic Load Balancing インスタンス | HTTPCode_ELB_5XX_Count<br><br>合計 > 0 を 5 分間、連続 3 回。 | 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。 |
| Elastic Load Balancing インスタンス | SurgeQueueLength<br><br>> 100 を 1 分間、15 回連続。 | Classic LoadBalancer サージキューの長さアラーム。<br><br>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。 |
| FSx for ONTAP | AMSFSXONTAPIOPSUtilization。<br><br>FSX:ONTAP IOPS 使用率 > 80% を 2 時間。 | ${FSx::FileSystemId}: FSX:ONTAP IOPS 使用率<br><br>FSx for ONTAP インスタンスの IOPS 使用率制限に関する CloudWatch アラーム。 |
| FSx for ONTAP | AMSFSXONTAPThroughputUtilization。<br><br>FSX:ONTAP スループット使用率 > 80% を 2 時間。 | ${FSx::FileSystemId}: FSX:ONTAP スループット使用率<br><br>FSx for ONTAP ボリュームのスループット制限に関する CloudWatch アラーム。 |

| サービス/リソースタイプ | アラートソースとトリガーの条件 | アラート名とメモ |
| --- | --- | --- |
| FSx for ONTAP | AMSFSXONTAPVolumeInodeUtilization。<br><br>FSX:ONTAP Inode 使用率 > 80% を 2 時間。 | ${FSx::FileSystemId}: ${FSx::ONTAP::VolumeId} FSX:ONTAP Inode 使用率<br><br>FSx for ONTAP ボリュームのファイル容量使用率制限に関する CloudWatch アラーム。 |
| FSx for ONTAP | AMSFSXONTAPVolumeCapacityUtilization。<br><br>FSX:ONTAP ボリューム容量使用率 > 80% を 2 時間。 | ${FSx::FileSystemId}:${FSx::ONTAP::VolumeId}<br><br>FSx for ONTAP ボリュームのボリューム容量使用率制限に関する CloudWatch アラーム。 |
| FSx for Windows File Server | AMSFSXWindowsThroughputUtilization。<br><br>FSX:Windows スループット使用率 > 80% を 2 時間。 | ${FSx::FileSystemId}: FSX:Windows スループット使用率<br><br>FSx for Windows File Server インスタンスのスループット制限に関する CloudWatch アラーム。 |
| FSx for Windows File Server | AMSFSXWindowsIOPSUtilization。<br><br>FSX:Windows IOPS 使用率 > 80% を 2 時間。 | ${FSx::FileSystemId}: FSX:Windows IOPS 使用率<br><br>FSx for Windows File Server インスタンスの IOPS 使用率制限に関する CloudWatch アラーム。 |

| サービス/リソースタイプ | アラートソースとトリガーの条件 | アラート名とメモ |
| --- | --- | --- |
| GuardDuty サービス | 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。<br><br>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。 | サポートされている GuardDuty 検出結果タイプのリストについては、GuardDuty Active Finding Types」を参照してください。 |
| ヘルス | AWS Health Dashboard | AMS によってモニタリングされるサービスに関連して AWS Health Dashboard（ AWS Health) イベントのステータスが変更されると、通知が送信されます。詳細については、「サポートされているサービス」を参照してください。 |
| IAM | Amazon EC2 IAM インスタンスプロファイルが存在しません。<br><br>IAM インスタンスプロファイルがありません。 | Amazon EC2 IAM インスタンスプロファイルを置き換える手順については、「IAM ロールを置き換える」の「IAM ドキュメント」を参照してください。 |

| サービス/リソースタイプ | アラートソースとトリガーの条件 | アラート名とメモ |
| --- | --- | --- |
| IAM | Amazon EC2 IAM インスタンスプロファイルのポリシーが多すぎます。<br><br>IAM インスタンスプロファイルには 10 個のポリシーがあり、追加のポリシーを追加することはできません。 | • IAM のサービス AWS クォータを変更して、ロールあたりの管理ポリシーの数を 20 に増やします。サービスクォータの詳細については、「サービスクォータの表示」を参照してください。<br>• これらのインスタンスに関連付けられた IAM ロールの不要な管理ポリシーを削除することで、管理ポリシーの数を現在の IAM クォータより低くします。AMS に必要なポリシーを必ず保持してください。<br>• これらのインスタンスに関連付けられた IAM ロールのポリシーを統合することで、管理ポリシーの数を現在の IAM クォータより低くします。AMS に必要なポリシーを必ず保持してください。<br><br>AMS に必要なポリシーについては、「AMS Accelerate ユーザーガイド: 」を参照してくださいIAM アクセス許可の変更の詳細。 |

| サービス/リソースタイプ | アラートソースとトリガーの条件 | アラート名とメモ |
| --- | --- | --- |
| Macie | 新しく生成されたアラートと既存のアラートの更新。<br><br>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。 | Amazon Macie アラート。サポートされている Amazon Macie アラートタイプのリストについては、Amazon Macie の検出結果の分析」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。 |
| NATGateways | PacketsDropCount : packetsdropcount が 15 分間で > 0 の場合に警告 | NatGateway PacketsDropCount<br><br>値が 0 より大きい場合は、NAT ゲートウェイで進行中の一時的な問題を示している可能性があります。 |
| NATGateways | ErrorPortAllocation : NAT ゲートウェイが 15 分間の評価期間にわたってポートを割り当てられなかった場合のアラーム | NatGateway ErrorPortAllocation<br><br>NAT ゲートウェイが送信元ポートを割り当てられなかった回数。0 より大きい値は、開いている同時接続が多すぎることを示します。 |

| サービス/リソースタイプ | アラートソースとトリガーの条件 | アラート名とメモ |
| --- | --- | --- |
| OpenSearch クラスター | ClusterStatus<br><br>赤の最大値は >= 1 で 1 分間、連続 1 回です。 | ClusterStatus Red<br><br>CloudWatch アラーム。ドメイン内の保管中のデータの暗号化に使用される AWS KMS 暗号化キーは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、「Red Cluster Status」を参照してください。 |
| OpenSearch ドメイン | KMSKeyError<br><br>>= 1 を 1 分間、連続 1 回。 | KMS キーエラー<br><br>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、「Amazon OpenSearch Service の保管中のデータの暗号化」を参照してください。 |
| OpenSearch ドメイン | KMSKeyInaccessible<br><br>>= 1 を 1 分間、連続 1 回。 | KMS キーにアクセスできないエラー<br><br>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、「Amazon OpenSearch Service の保管中のデータの暗号化」を参照してください。 |

| サービス/リソースタイプ | アラートソースとトリガーの条件 | アラート名とメモ |
| --- | --- | --- |
| OpenSearch ドメイン | ClusterStatus<br><br>黄色の最大値は >= 1 で 1 分間、連続 1 回です。 | ClusterStatus 黄<br><br>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、「黄色のクラスターステータス」を参照してください。 |
| OpenSearch ドメイン | FreeStorageSpace<br><br>最小は <= 20480 で 1 分間、連続して 1 回です。 | 空きストレージ容量が少ない<br><br>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、「使用可能なストレージ容量がない」を参照してください。 |
| OpenSearch ドメイン | ClusterIndexWritesBlocked<br><br>>= 1 を 5 分間、1 回連続。 | クラスターインデックスの書き込みがブロックされました<br><br>クラスターは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、「ClusterBlockException」を参照してください。 |

| サービス/リソースタイプ | アラートソースとトリガーの条件 | アラート名とメモ |
| --- | --- | --- |
| OpenSearch ドメイン | ノード<br><br>最小 < x 1 日、連続 1 回。 | ノードダウン<br><br>x 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、「失敗したクラスターノード」を参照してください。 |
| OpenSearch ドメイン | CPUUtilization<br><br>平均 >= 15 分間 80%、連続 3 回。 | データノードの CPU 使用率が高い<br><br>100% の CPU 使用率は珍しくありませんが、高い平均値が持続する場合は問題があります。既存のインスタンスタイプの適切なサイズ設定やインスタンスの追加を検討してください。 |

| サービス/リソースタイプ | アラートソースとトリガーの条件 | アラート名とメモ |
| --- | --- | --- |
| OpenSearch ドメイン | JVMMemoryPressure<br><br>最大 >= 5 分間 80%、連続 3 回。 | データノードのメモリ使用率が高い<br><br>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。OpenSearch 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。 |
| OpenSearch ドメイン | MasterCPUUtilization<br><br>平均 >= 15 分間 50%、連続 3 回。 | マスターノード CPU 使用率が高い<br><br>専用マスターノードには、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 Blue/Green デプロイに関わるため、専用マスターノードの CPU の平均使用率はデータノードよりも低くする必要があります。 |

| サービス/リソースタイプ | アラートソースとトリガーの条件 | アラート名とメモ |
| --- | --- | --- |
| OpenSearch ドメイン | MasterJVMMemoryPressure<br><br>最大 >= 15 分間 80%、連続 1 回。 | マスターノードの JVM メモリプレッシャーが高い<br><br>専用マスターノードには、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 Blue/Green デプロイに関わるため、専用マスターノードの CPU の平均使用率はデータノードよりも低くする必要があります。 |
| OpenSearch インスタンス | AutomatedSnapshotFailure<br><br>maximum は >= 1 で 1 分間、連続 1 回です。 | 自動スナップショットの失敗<br><br>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。詳細については、「Red Cluster Status」を参照してください。 |
| Amazon RDS | 平均 CPU 使用率<br><br>> 15 分間 90%、2 回連続。 | ${RDS::DBInstanceIdentifier}: CPUUtilization<br><br>CloudWatch アラーム。 |
| Amazon RDS | DiskQueueDepth の合計<br><br>> 1 分間 75%、連続 15 回。 | ${RDS::DBInstanceIdentifier}: DiskQueue<br><br>CloudWatch アラーム。 |

| サービス/リソースタイプ | アラートソースとトリガーの条件 | アラート名とメモ |
| --- | --- | --- |
| Amazon RDS | 平均 FreeStorageSpace<br><br>< 1,073,741,824 バイト、5 分間、2 回連続。 | ${RDS::DBInstanceIdentifier}: FreeStorageSpace<br><br>CloudWatch アラーム。 |
| Amazon RDS | 低ストレージアラート<br><br>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トリガーされます。 | RDS-EVENT-0007 の詳細については、「Amazon RDS イベント通知の使用」を参照してください。 |
| Amazon RDS | 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。 | RDS-EVENT-0031 の詳細については、「Amazon RDS イベントカテゴリとイベントメッセージ」を参照してください。 |
| Amazon RDS | RDS -0034 フェイルオーバーは試行されません。<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。 | RDS-EVENT-0034 の詳細については、「Amazon RDS イベントカテゴリとイベントメッセージ」を参照してください。 |

| サービス/リソースタイプ | アラートソースとトリガーの条件 | アラート名とメモ |
| --- | --- | --- |
| Amazon RDS | RDS - 0035 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に対して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、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。 | RDS-EVENT-0035 の詳細については、「Amazon RDS イベントカテゴリとイベントメッセージ」を参照してください。 |
| Amazon RDS | 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 の詳細については、「Amazon RDS イベントカテゴリとイベントメッセージ」を参照してください。 |
| Amazon RDS | RDS-0045 DB インスタンスのリードレプリカエラー<br><br>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、MySQL リードレプリカの問題のトラブルシューティング」を参照してください。 | RDS-EVENT-0045 の詳細については、「Amazon RDS イベントカテゴリとイベントメッセージ」を参照してください。 |

| サービス/リソースタイプ | アラートソースとトリガーの条件 | アラート名とメモ |
| --- | --- | --- |
| Amazon RDS | RDS-0057 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<br><br>リードレプリカのレプリケーションが終了しました。 | サービスイベント。RDS-EVENT-0057 の詳細については、「Amazon RDS イベントカテゴリとイベントメッセージ」を参照してください。 |
| Amazon RDS | RDS-0058 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<br><br>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。 | サービスイベント。RDS-EVENT-0058 の詳細については、「Amazon RDS イベントカテゴリとイベントメッセージ」を参照してください。 |
| Amazon RDS | 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 の詳細については、Amazon RDS イベントカテゴリとイベントメッセージを参照してください。 |

| サービス/リソースタイプ | アラートソースとトリガーの条件 | アラート名とメモ |
| --- | --- | --- |
| Amazon RDS | 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、「Amazon RDS イベントカテゴリとイベントメッセージ」を参照してください。 |
| Amazon RDS | 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、「ネイティブバックアップと復元のセットアップ」を参照してください。 | サービスイベント。RDS-EVENT-0081 の詳細については、Amazon RDS イベントカテゴリとイベントメッセージを参照してください。 |
| Amazon RDS | 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、「Amazon RDS イベントカテゴリとイベントメッセージ」を参照してください。 |
| Amazon RDS | 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。 | サービスイベント。RDS-EVENT-0089 の詳細については、Amazon RDS イベントカテゴリとイベントメッセージを参照してください。 |

| サービス/リソースタイプ | アラートソースとトリガーの条件 | アラート名とメモ |
| --- | --- | --- |
| Amazon RDS | Aurora Serverless DB クラスターのスケーリングが失敗したときの通知サービス。 | サービスイベント。RDS-EVENT-0143 は、Amazon RDS イベントカテゴリとイベントメッセージで詳細を表示します。 |
| Amazon RDS | 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。オートスケーリングは後で再試行されます。 | RDS-EVENT-0219 の詳細については、「Amazon RDS イベントカテゴリとイベントメッセージ」を参照してください。 |
| Amazon RDS | 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、「Amazon RDS イベントカテゴリとイベントメッセージ」を参照してください。 |
| Amazon RDS | このイベントは、Amazon RDS インスタンスストレージの自動スケーリングがスケーリングできないことを示します。自動スケー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、「Amazon RDS イベントカテゴリとイベントメッセージ」を参照してください。 |
| Amazon RDS | 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、「Amazon RDS イベントカテゴリとイベントメッセージ」を参照してください。 |

| サービス/リソースタイプ | アラートソースとトリガーの条件 | アラート名とメモ |
| --- | --- | --- |
| Amazon RDS | DB インスタンスのストレージタイプが、アベイラビリティー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、「Amazon RDS イベントカテゴリとイベントメッセージ」を参照してください。 |
| Amazon RDS | サブネットに十分な IP アドレスがないため、Amazon 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、「Amazon RDS イベントカテゴリとイベントメッセージ」を参照してください。 |
| Amazon RDS | のストレージ AWS アカウント 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、「Amazon RDS イベントカテゴリとイベントメッセージ」を参照してください。 |
| Amazon Redshift クラスター | メンテナンスモードでない場合のクラスターの状態<br><br>< 1 で 5 分間 | RedshiftClusterHealthStatus<br><br>詳細については、CloudWatch メトリクスを使用した Amazon Redshift のモニタリング」を参照してください。 |
| Site-to-Site VPN | VPNTunnelDown<br><br>TunnelState <= 1 分間 0、連続 20 回。 | ${AWS::EC2::VpnConnectionId} - VPNTunnelDown<br><br>TunnelState は、両方のトンネルがダウンしている場合は 0、1 つのトンネルがアップしている場合は .5、両方のトンネルがアップしている場合は 1.0 です。 |

| サービス/リソースタイプ | アラートソースとトリガーの条件 | アラート名とメモ |
| --- | --- | --- |
| Systems Manager エージェント | Systems Manager によって管理されていない EC2 インスタンス<br><br>SSM エージェントがインストールされていません。SSM エージェントはインスタンスにインストールされていますが、エージェントサービスは実行されていません。SSM エージェントには、 AWS Systems Manager サービスへのネットワークルートがありません。 | Systems Manager エージェントを中断させる追加の条件があります。詳細については、「マネージドノードの可用性のトラブルシューティング」を参照してください。 |

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)

## 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通信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 AWS Service Catalog AppRegistry にオンボードする必要があります。

AMS Accelerate の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 Accelerate でのモニタリングとイベント管理。

# AppRegistry にオンボードしてアプリケーションを作成する

AppRegistry にオンボードするには、AppRegistry 管理者ガイドの「AppRegistry の開始方法」を参照してください。 AWS Service Catalog AppRegistry  オンボーディング後、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。
3. AMS オートメーション： アプリケーション登録プロセスを簡素化するために、AMS は SSM オートメーションドキュメント を提供しますAWSManagedServices-CreateAppRegistryApplication。この方法を使用するには、https://console.aws.amazon.com/systems-manager/ の AWS Systems Manager コンソールから、または次の例で説明 AWS CLI されているように を使用して、 ドキュメントを呼び出します。

```
# The following registers a new application with customized severity
aws ssm start-automation-execution \
  --document-name "AWSManagedServices-CreateAppRegistryApplication" \
  --parameters '{"ResourceAssociationType":["TAGS"],"AppTagValue":
["MyApp"],"CFNStackNames":[],"ApplicationName":
["BananaStand"],"ApplicationDescription":["This is my banana stand
 application"],"AppCriticality":["normal"],"AutomationAssumeRole":
["arn:aws:iam::123456789012:role/SSMAdminRole"]}' \
  --region us-east-1
# The following registers a new application with no customizations
aws ssm start-automation-execution \
  --document-name "AWSManagedServices-CreateAppRegistryApplication" \
  --parameters '{"ResourceAssociationType":["TAGS"],"AppTagValue":
["MyApp"],"CFNStackNames":[],"ApplicationName":
["BananaStand"],"ApplicationDescription":["This is my banana stand
 application"],"AppCriticality":["unset"],"AutomationAssumeRole":
["arn:aws:iam::123456789012:role/SSMAdminRole"]}' \
  --region us-east-1
# You can also register applications using CloudFormation stacks
aws ssm start-automation-execution \
  --document-name "AWSManagedServices-CreateAppRegistryApplication" \
```

```
  --parameters '{"ResourceAssociationType":["STACKS"],"AppTagValue":
[""],"CFNStackNames":["arn:aws:cloudformation:us-east-1:123456789012:stack/
stack-2343eddq/1a2b3c4d-5e6f-7g8h-9i0j-1k2l3m4n5o6p"],"ApplicationName":
["BananaStand"],"ApplicationDescription":["This is my banana stand
 application"],"AppCriticality":["unset"],"AutomationAssumeRole":
["arn:aws:iam::123456789012:role/SSMAdminRole"]}' \
  --region us-east-1
```

## 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。

プレフィックスが付いたタグams:rt:は、Resource Tagger を通じて適用されます。

| タグキー | タグ値 |
| --- | --- |
| ams マネージド | true |
| ams:rt:ams-managed | 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。

| スキーマバージョニング | 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-*
```

# アラームマネージャーの高速化

AMS Accelerate は、タグベースのアラームマネージャーを使用して AWS リソースにアラームを適用し、ベースラインモニタリング戦略を実装し、すべての AWS リソースがモニタリングおよび保護されるようにします。タグベースの Alarm Manager と統合することで、リソースのタイプ、プラットフォーム、その他のタグに基づいてリソースの設定 AWS をカスタマイズして、リソースがモニタリングされるようにできます。Alarm Manager は、オンボーディング中に Accelerate アカウントにデプロイされます。

## Alarm Manager の仕組み

アカウントが AMS Accelerate にオンボーディングされると、設定プロファイルと呼ばれる 2 つの JSON ドキュメントが AWS AppConfig のアカウントにデプロイされます。どちらのプロファイルドキュメントも、Alarm Manager アプリケーションと AMS Accelerate インフラストラクチャ環境にあります。

2 つの設定プロファイルには、AMSManagedAlarms (デフォルトの設定プロファイル) とCustomerManagedAlarms (カスタマイズ設定プロファイル) という名前が付けられています。

- デフォルトの設定プロファイル：
  - このプロファイルにある設定には、AMS Accelerate がすべてのカスタマーアカウントにデプロイするデフォルト設定が含まれています。この設定にはデフォルトの AMS Accelerate モニタリングポリシーが含まれています。AMS Accelerate はいつでもこのプロファイルを更新し、変更を消去できるため、変更しないでください。

  - これらの定義のいずれかを変更または無効にする場合は、Accelerate アラームのデフォルト設定の変更「」および「」を参照してくださいデフォルトの Accelerate アラーム設定を無効にする。
- カスタマイズ設定プロファイル：
  - このプロファイルの設定はすべてお客様によって完全に管理されます。明示的にリクエストしない限り、AMS Accelerate はこのプロファイルを上書きしません。
  - このプロファイルで任意のカスタムアラーム定義を指定でき、AMS Accelerate が管理するデフォルト設定への変更を指定することもできます。詳細については、「Accelerate アラームのデフォルト設定の変更」および「デフォルトの Accelerate アラーム設定を無効にする」を参照してください。
  - このプロファイルを更新すると、Alarm Manager は AWS アカウント内のすべての関連リソースで変更を自動的に適用します。変更は自動的に有効になりますが、有効になるまでに最大 60 分かかる場合があります。
  - このプロファイルは、 AWS マネジメントコンソール または AWS CLI/SDK ツールを使用して更新できます。設定の更新手順については、AWS AppConfig ユーザーガイドを参照してください。
  - カスタマイズプロファイルは最初は空ですが、デフォルト設定に加えて、プロファイルドキュメントに配置されたアラーム定義が適用されます。

Alarm Manager によって作成されたすべての CloudWatch アラームには、タグキー ams:alarm-manager:managed とタグ値 true が含まれています。これは、Alarm Manager が作成したアラームのみを管理し、独自のアラームに干渉しないようにするためです。これらのタグは、Amazon CloudWatch ListTagsForResource API を使用して確認できます。

> **Important**
>
> カスタムアラーム定義とデフォルトのアラーム定義が同じ ConfigurationID で指定されている場合 (「」を参照高速設定プロファイル: モニタリング )、カスタム定義はデフォルトのルールよりも優先されます。

## Accelerate Alarm Manager の開始方法

デフォルトでは、AMS Accelerate を使用してオンボードすると、設定が にデプロイされ AWS AppConfig、リソースのアラームベースラインが定義されます。アラーム定義は、ams:rt:* タグを

持つリソースにのみ適用されます。これらのタグは、 を使用して適用することをお勧めしますリソースタガーの高速化。AMS Accelerate に管理するリソースを知らせるために、基本的な Resource Tagger 設定をセットアップします。

Resource Tagger を使用して、タグキー ams:rt:ams-managedwith tag value true を AMS Accelerate でモニタリングするすべてのリソースに適用します。

以下は、すべての Amazon EC2 インスタンスのモニタリングをオプトインするために使用できる Resource Tagger カスタマイズプロファイルの例です。一般情報については、「リソースタガーの高速化」を参照してください。

```
{
    "AWS::EC2::Instance": {
        "AMSManageAllEC2Instances": {
            "Enabled": true,
            "Filter": {
                "InstanceId": "*"
            },
            "Tags": [
                {
                    "Key": "ams:rt:ams-managed",
                    "Value": "true"
                }
            ]
        }
    }
}
```

この Resource Tagger 設定を適用する方法については、「」を参照してくださいResource Tagger 設定の表示または変更。

## アラームマネージャータグの高速化

デフォルトでは、AMS Accelerate を使用してオンボードすると、設定が にデプロイされ AWS AppConfig、リソースのアラームベースラインが定義されます。アラーム定義は、ams:rt:* タグを持つリソースにのみ適用されます。これらのタグは、 を使用して適用することをお勧めしますリソースタガーの高速化。AMS Accelerate に管理するリソースを知らせるために、基本的な Resource Tagger 設定をセットアップします。

Resource Tagger を使用して、タグキー ams:rt:ams-managedwith tag value true を AMS Accelerate でモニタリングするすべてのリソースに適用します。

トピック


- Resource Tagger を使用してタグを高速化する
- Resource Tagger を使用せずにタグを高速化する
- を使用してタグを高速化する CloudFormation
- Terraform を使用してタグを高速化する


## Resource Tagger を使用してタグを高速化する

タグベースのアラームマネージャーは、リソースごとの CloudWatch アラームのライフサイクルを管理しますが、マネージドリソースには AMS Accelerate で定義された特定のタグが必要です。Resource Tagger を使用して AMS マネージドアラームのデフォルトセットを Linux および Windows ベースのインスタンスの両方に適用するには、次の手順に従います。

1. アカウント内の AppConfig コンソールを参照します。
2. ResourceTagger アプリケーションを選択します。
3. 設定プロファイルタブを選択し、CustomerManagedTags を選択します。
4. Create をクリックして、新しいプロファイルを作成します。
5. JSON を選択し、設定を定義します。フィルターとプラットフォームの定義のその他の例については、「」を参照してくださいリソースタガーの高速化。

```
{
"AWS::EC2::Instance": {
   "MonitorAllInstances": {
       "Enabled": true,
       "Filter": {
           "Platform": "*"
       },
       "Tags": [
           {
               "Key": "ams:rt:ams-managed",
               "Value": "true"
           }
       ]
   }
}
}
```

6. ホストされた設定バージョンの作成 をクリックします。

7. デプロイの開始 をクリックします。
8. 次のデプロイの詳細を定義します。

```
Environment: AMSInfrastructure Hosted configuration version: <Select the version
 that you have just created>
              Deployment Strategy: AMSNoBakeDeployment
```

9. デプロイの開始 をクリックします。

インスタンスにタグが付けられ`"ams:rt:ams-managed": "true"`、 インスタンスに追加の`"ams:rt:ams-monitoring-policy": "ams-monitored"`と `"ams:rt:ams-monitoring-policy-platform": "ams-monitored-linux"`が適用されます。これらのタグにより、インスタンスに適切なアラームが作成されます。このプロセスの詳細については、「Accelerate でのモニタリング」を参照してください。

ヒマンシュウのビデオを視聴して詳細を確認する (11:04)

## Resource Tagger を使用せずにタグを高速化する

タグベースのアラームマネージャーは、リソースごとの CloudWatch アラームのライフサイクルを管理しますが、マネージドリソースには AMS Accelerate で定義された特定のタグが必要です。AMS Accelerate には、タグが Resource Tagger によって適用されていることを前提とするデフォルトの設定プロファイルが用意されています。

Resource Tagger ではなく、 や Terraform などの CloudFormation リソースにタグを適用する代替方法を使用する場合は、リソースにタグを適用せず、選択したタグ付け方法と競合しないように Resource Tagger を無効にする必要があります。カスタム Resource Tagger 設定プロファイルを変更して読み取り専用モードを有効にする手順については、「」を参照してくださいResource Tagger によるリソースの変更の防止。

Resource Tagger が読み取り専用モードに設定され、設定プロファイルがデプロイされたら、選択したタグ付け方法を使用して、次のガイドラインに従ってリソースにタグを適用します。

| リソースタイプ | タグキー | タグ値 |
| --- | --- | --- |
| サポートされているすべてのリソース (この表で説明 ) | ams:rt:ams-monitoring-policy | ams-monitored |

| リソースタイプ | タグキー | タグ値 |
| --- | --- | --- |
| EC2 インスタンス (Linux) | ams:rt:ams-monitoring-policy-platform | ams-monitored-linux |
| EC2 インスタンス (Windows) | ams:rt:ams-monitoring-policy-platform | ams-monitored-windows |
| KMS を使用した OpenSearch ドメイン | ams:rt:ams-monitoring-with-kms | ams-monitored-with-kms |
| 専用マスターノードを使用した OpenSearch ドメイン | ams:rt:ams-monitoring-with-master | ams-monitored-with-master |

これらのタグキーと値を持つリソースは、AMS Accelerate Alarm Manager によって管理されます。

### を使用してタグを高速化する CloudFormation

> **Note**
>
> を使用してタグを適用する前に、まず Resource Tagger を読み取り専用モードに設定してください。設定されていない場合 CloudFormation、Resource Tagger は設定プロファイルに基づいてタグを変更することがあります。Resource Tagger を読み取り専用モードに設定する方法、および独自のタグの提供に関するガイドラインについては、「」を参照してくださいResource Tagger を使用せずにタグを高速化する。

を使用してタグを適用するには CloudFormation、スタックレベルでタグを適用するか (CloudFormation リソースタグ」を参照 )、個々のリソースレベルでタグを適用できます (例えば、EC2 インスタンスタグの作成」を参照 )。

以下は、AMS Accelerate アラーム管理タグを によって管理される Amazon EC2 インスタンスに適用する方法の例です CloudFormation。

```
Type: AWS::EC2::Instance
Properties:
 InstanceType: "t3.micro"

 # ...other properties...
```

```
Tags:
  - Key: "aws:rt:ams-monitoring-policy"
    Value: "ams-monitored"
  - Key: "aws:rt:ams-monitoring-policy-platform"
    Value: "ams-monitored-linux"
```

以下は、 が管理する Auto Scaling グループに AMS Accelerate アラーム管理タグを適用する方法の例です CloudFormation。Auto Scaling グループは、作成した Amazon EC2 インスタンスにタグを伝達することに注意してください。

```
Type: AWS::AutoScaling::AutoScalingGroup
Properties:
 AutoScalingGroupName: "TestASG"

 # ...other properties...

 Tags:
   - Key: "aws:rt:ams-monitoring-policy"
     Value: "ams-monitored"
   - Key: "aws:rt:ams-monitoring-policy-platform"
     Value: "ams-monitored-linux"
```

### Terraform を使用してタグを高速化する

> **Note**
>
> を使用してタグを適用する前に、まず Resource Tagger を読み取り専用モードに設定してください。設定されていない場合 CloudFormation、Resource Tagger は設定プロファイルに基づいてタグを変更することがあります。Resource Tagger を読み取り専用モードに設定する方法、および独自のタグの提供に関するガイドラインについては、「」を参照してくださいResource Tagger を使用せずにタグを高速化する。

Terraform を使用してリソースタグを管理する方法の詳細については、Terraform ドキュメントのリソースタグ付けを参照してください。

以下は、Terraform によって管理される Amazon EC2 インスタンスに AMS Accelerate アラーム管理タグを適用する方法の例です。

```
resource "aws_instance" "test_linux_instance" {
```

```
    # ...ami and other properties...

    instance_type = "t3.micro"

    tags = {
      "aws:rt:ams-monitoring-policy" = "ams-monitored"
      "aws:rt:ams-monitoring-policy-platform" = "ams-monitored-linux"
    }
  }
```

以下は、Terraform が管理する Auto Scaling グループに AMS アラーム管理タグを適用する方法の例です。Auto Scaling グループは、作成した EC2 インスタンスにタグを伝達することに注意してください。

```
resource "aws_autoscaling_group" "test_asg" {
name = "terraform-test"
# ...other properties...

tags = {
  "aws:rt:ams-monitoring-policy" = "ams-monitored"
  "aws:rt:ams-monitoring-policy-platform" = "ams-monitored-linux"
}
}
```

## Alarm Manager 設定プロファイルの高速化

アカウントが AMS Accelerate にオンボーディングされると、設定プロファイルと呼ばれる 2 つの JSON ドキュメントが AWS AppConfig を使用してアカウントにデプロイされます (「What is AWS AppConfig」を参照 )。どちらのプロファイルドキュメントも、Alarm Manager アプリケーションと AMS Accelerate インフラストラクチャ環境にあります。

トピック

- 高速設定プロファイル: モニタリング
- Accelerate 設定プロファイル: 擬似パラメータ置換
- アラーム設定の高速化の例
- Accelerate Alarm Manager 設定の表示
- Accelerate アラーム設定の変更
- Accelerate アラームのデフォルト設定の変更

- Accelerate アラーム設定変更のデプロイ
- ロールバック Accelerate アラームの変更
- Accelerate アラームの保持
- デフォルトの Accelerate アラーム設定を無効にする

## 高速設定プロファイル: モニタリング

デフォルトの設定プロファイルドキュメントとカスタマイズ設定プロファイルドキュメントの両方が同じ構造 に従います。

```
  {
    "<ResourceType>": {
        "<ConfigurationID>": {
            "Enabled": true,

            "Tag": {
                "Key": "...",
                "Value": "..."
            },
            "AlarmDefinition": {
                ...
            }
        },
        "<ConfigurationID>": {
            ...
        }
    },
    "<ResourceType>": {
        ...
    }
}
```

- ResourceType: このキーは、サポートされている次の文字列のいずれかである必要があります。この JSON オブジェクト内の設定は、指定された AWS リソースタイプにのみ関連します。サポートされているリソースタイプは以下のとおりです。

```
AWS::EC2::Instance
AWS::EC2::Instance::Disk
AWS::RDS::DBInstance
AWS::RDS::DBCluster
```

```
AWS::Elasticsearch::Domain
AWS::OpenSearch::Domain
AWS::Redshift::Cluster
AWS::ElasticLoadBalancingV2::LoadBalancer
AWS::ElasticLoadBalancingV2::LoadBalancer::TargetGroup
AWS::ElasticLoadBalancing::LoadBalancer
AWS::FSx::FileSystem::ONTAP
AWS::FSx::FileSystem::ONTAP::Volume
AWS::FSx::FileSystem::Windows
AWS::EFS::FileSystem
AWS::EC2::NatGateway
AWS::EC2::VPNConnection
```

- ConfigurationID: このキーはプロファイル内で一意である必要があり、次の設定ブロックに一意に名前を付けます。同じ ResourceType ブロック内の 2 つの設定ブロックが同じ ConfigurationID を持つ場合、プロファイルで最新の設定ブロックが有効になります。カスタマイズプロファイルでデフォルトプロファイルで指定されたものと同じ ConfigurationID を指定すると、カスタマイズプロファイルで定義された設定ブロックが有効になります。
  - 有効: (オプション、default=true) 設定ブロックを有効にするかどうかを指定します。設定ブロックを無効にするには、これを false に設定します。無効になっている設定ブロックは、プロファイルに存在しないかのように動作します。
  - タグ: このアラーム定義が適用されるタグを指定します。このタグキーと値を持つ (適切なリソースタイプの) リソースには、指定された定義で CloudWatch アラームが作成されます。このフィールドは、次のフィールドを持つ JSON オブジェクトです。
    - キー: 一致するタグのキー。Resource Tagger を使用してリソースにタグを適用する場合、タグのキーは常にams:rt: で始まることに注意してください。
    - 値: 一致するタグの値。
  - AlarmDefinition: 作成するアラームを定義します。これは、フィールドがそのまま CloudWatch `PutMetricAlarm` API コールに渡される JSON オブジェクトです (擬似パラメータを除く。詳細については、「」を参照してくださいAccelerate 設定プロファイル: 擬似パラメータ置換 )。必須フィールドの詳細については、PutMetricAlarm ドキュメントを参照してください。

    または

    CompositeAlarmDefinition: 作成する複合アラームを定義します。複合アラームを作成するときは、作成した他のアラームのアラーム状態を考慮したアラームのルール式を指定します。これは、フィールドがそのまま に渡される JSON オブジェクトですCloudWatch`PutCompositeAlarm`。複合アラームは、ルールのすべての条件が満たされた

場合に限り、ALARM 状態になります。複合アラームのルール式で指定されたアラームには、メトリクスアラームやその他の複合アラームを含めることができます。必須フィールドの詳細については、PutCompositeAlarm ドキュメントを参照してください。

どちらのオプションにも次のフィールドがあります。

- AlarmName: リソース用に作成するアラームの名前を指定します。このフィールドには、PutMetricAlarm ドキュメントで指定されているものと同じルールがすべて含まれています。ただし、アラーム名はリージョン内で一意である必要があるため、アラームマネージャーには 1 つの追加要件があります。アラーム名に一意の識別子の擬似パラメータを指定する必要があります (それ以外の場合は、アラームマネージャーはリソースの一意の識別子をアラーム名の先頭に追加します )。たとえば、AWS::EC2::Instance リソースタイプの場合、アラーム名`${EC2::InstanceId}`に を指定する必要があります。指定しない場合、アラーム名の先頭に暗黙的に追加されます。識別子のリストについては、「」を参照してくださいAccelerate 設定プロファイル: 擬似パラメータ置換。

  他のすべてのフィールドは、PutMetricAlarm または PutCompositeAlarm ドキュメントで指定されているとおりです。

- AlarmRule: この複合アラームの状態を判断するために評価する他のアラームを指定します。参照するアラームごとに、CloudWatch に存在するか、アカウントの Alarm Manager 設定プロファイルで指定する必要があります。

> **Important**
>
> AlarmDefinition または CompositeAlarmDefinition のいずれかを Alarm Manager 設定ドキュメントで指定できますが、両方を同時に使用することはできません。

次の例では、2 つの指定されたメトリクスアラームがしきい値を超えたときにアラームが作成されます。

```
{
  "AWS::EC2::Instance": {
    "LinuxResourceAlarm": {
      "Enabled": true,
      "Tag": {
        "Key": "ams:rt:mylinuxinstance",
        "Value": "true"
      },
```

```
      "CompositeAlarmDefinition": {
        "AlarmName": "${EC2::InstanceId} Resource Usage High",
        "AlarmDescription": "Alarm when a linux EC2 instance is using too much CPU and
 too much Disk",
        "AlarmRule": "ALARM(\"${EC2::InstanceId}: Disk Usage Too High -
 ${EC2::Disk::UUID}\") AND ALARM(\"${EC2::InstanceId}: CPU Too High\")"
      }
    }
  }
}
```

**Important**

設定が壊れたためにアラームを作成または削除できない場合、Alarm Manager は Direct-Customer-Alerts SNS トピックに通知を送信します。このアラームは AlarmDependencyError と呼ばれます。
この SNS トピックへのサブスクリプションを確認することを強くお勧めします。トピックに発行されたメッセージを受信するには、トピックにエンドポイントをサブスクライブする必要があります。詳細については、「ステップ 1: トピックを作成する」を参照してください。

**Note**

異常検出アラームが作成されると、Alarm Manager は指定されたメトリクスに必要な異常検出モデルを自動的に作成します。異常検出アラームが削除されても、Alarm Manager は関連する異常検出モデルを削除しません。
Amazon CloudWatch は、特定のリージョンに保持できる異常検出モデルの数を制限します。 AWS モデルクォータを超えると、Alarm Manager は新しい異常検出アラームを作成しません。未使用のモデルを削除するか、AMS パートナーと協力して制限の引き上げをリクエストする必要があります。
AMS Accelerate が提供するベースラインアラーム定義の多くは、SNS トピックである MMS-Topic をターゲットとして一覧表示します。これは AMS Accelerate モニタリングサービスで使用するためのもので、アラーム通知が AMS Accelerate に到達するためのトランスポートメカニズムです。サービスは不明なアラームを無視するため、ベースラインで指定されたアラーム (および同じ の上書き) 以外のアラームのターゲットとして MMS-Topic を指定しないでください。AMS Accelerate がカスタムアラームで動作することはありません。

## Accelerate 設定プロファイル: 擬似パラメータ置換

どちらの設定プロファイルでも、次のように置き換えられる擬似パラメータを指定できます。

- グローバル - プロファイル内の任意の場所：
  - ${AWS::AccountId}: を AWS アカウント ID に置き換えました
  - ${AWS::Partition}: AWS リージョン リソースのパーティションに置き換えました (ほとんどのリージョンでは「aws」です ) 。詳細については、ARN リファレンスの「パーティションのエントリ」を参照してください。
  - ${AWS::Region}: リソースがデプロイされているリージョンのリージョン名に置き換えられます (us-east-1 など )
- AWS::EC2::Instance リソースタイプブロックの場合：
  - ${EC2::InstanceId}: (識別子) を Amazon EC2 インスタンスのインスタンス ID に置き換えます。
  - ${EC2::InstanceName}: を Amazon EC2 インスタンスの名前に置き換えます。
- AWS::EC2::Instance::Disk リソースタイプブロックの場合：
  - ${EC2::InstanceId}: (識別子) Amazon EC2 インスタンスのインスタンス ID に置き換えます。
  - ${EC2::InstanceName}: Amazon EC2 インスタンスの名前に置き換えます。
  - ${EC2::Disk::Device}: (識別子) ディスクの名前に置き換えます。(Linux のみ、CloudWatch エージェントによって管理されるインスタンス ) 。
  - ${EC2::Disk::FSType}: (識別子) ディスクのファイルシステムタイプに置き換えられます。(Linux のみ、CloudWatchAgent によって管理されるインスタンスの場合 ) 。
  - ${EC2::Disk::Path}: (識別子) ディスクパスに置き換えます。Linux では、これはディスクのマウントポイント (/ など) であり、Windows ではドライブラベル (c:/ など) です (CloudWatch エージェントによって管理されるインスタンスでのみ ) 。
  - ${EC2::Disk::UUID}: (識別子) ディスクを一意に識別する生成された UUID に置き換えます。これはアラームの名前で指定する必要があります。AWS::EC2::Instance::Disk リソースタイプでは、ボリュームごとに 1 つのアラームが作成されます。${EC2::Disk::UUID} を指定すると、アラーム名の一意性が維持されます。
- AWS::EKS::Cluster リソースタイプブロックの場合：
  - ${EKS::ClusterName}: (識別子) を EKS クラスターの名前に置き換えます。
- AWS::OpenSearch::Domain リソースタイプブロックの場合：
  - ${OpenSearch::DomainName}: (識別子) を EKS ドメインの名前に置き換えます。
- AWS::ElasticLoadBalancing::LoadBalancer リソースタイプブロックの場合：

  - ${ElasticLoadBalancing::LoadBalancer::Name}: (識別子) を V1 Load Balancer の名前に置き換えます。
- AWS::ElasticLoadBalancingV2::LoadBalancer リソースタイプブロックの場合：
  - ${ElasticLoadBalancingV2::LoadBalancer::Arn}: (識別子) を V2 Load Balancer の ARN に置き換えます。
  - ${ElasticLoadBalancingV2::LoadBalancer::Name}: (識別子) を V2 Load Balancer の名前に置き換えます。
  - ${ElasticLoadBalancingV2::LoadBalancer::FullName}: (識別子) を V2 Load Balancer のフルネームに置き換えます。
- AWS::ElasticLoadBalancingV2::LoadBalancer::TargetGroup リソースタイプブロックの場合：
  - ${ElasticLoadBalancingV2::TargetGroup::FullName}: (識別子) を V2 Load Balancer のターゲットグループ名に置き換えます。
  - ${ElasticLoadBalancingV2::TargetGroup::UUID}: (識別子) を V2 Load Balancer 用に生成された UUID に置き換えます。
- AWS::EC2::NatGateway リソースタイプブロックの場合：
  - ${NatGateway::NatGatewayId}: (識別子) を NAT ゲートウェイ ID に置き換えます。
- AWS::RDS::DBInstance リソースタイプブロックの場合：
  - ${RDS::DBInstanceIdentifier}: (識別子) を RDS DB インスタンス識別子に置き換えます。
- AWS::RDS::DBCluster リソースタイプブロックの場合：
  - ${RDS::DBClusterIdentifier}: (識別子) を RDS DB クラスター識別子に置き換えます。
- AWS::Redshift::Cluster リソースタイプブロックの場合：
  - ${Redshift::ClusterIdentifier}: (識別子) を Redshift クラスター識別子に置き換えます。
- AWS::Synthetics::Canary リソースタイプブロックの場合：
  - ${Synthetics::CanaryName}: (識別子) を CloudWatch Synthetics Canary の名前に置き換えます。
- AWS::EC2::VPNConnection リソースタイプブロックの場合：
  - ${AWS::EC2::VpnConnectionId}: (識別子) を VPN ID に置き換えます。
- AWS::EFS::FileSystem リソースタイプブロックの場合：
  - ${EFS::FileSystemId}: (識別子) EFS ファイルシステムのファイルシステム ID に置き換えます。
- AWS::FSx::FileSystem::ONTAP リソースタイプブロックの場合：
  - ${FSx::FileSystemId}: (識別子) FSX ファイルシステムのファイルシステム ID に置き換えます。

  - ${FSx::FileSystem::Throughput}: FSX ファイルシステムのスループットに置き換えます。
  - ${FSx::FileSystem::Iops}: FSX ファイルシステムの IOPS に置き換えます。
- AWS::FSx::FileSystem::ONTAP::Volume リソースタイプブロックの場合：
  - ${FSx::FileSystemId}: (識別子) FSX ファイルシステムのファイルシステム ID に置き換えます。
  - ${FSx::ONTAP::VolumeId}: (識別子) ボリューム ID に置き換えられます。
- AWS::FSx::FileSystem::Windows リソースタイプブロックの場合：
  - ${FSx::FileSystemId}: (識別子) FSX ファイルシステムのファイルシステム ID に置き換えます。
  - ${FSx::FileSystem::Throughput}: FSX ファイルシステムのスループットに置き換えます。

> **Note**
>
> 識別子でマークされたすべてのパラメータは、アラーム名にその識別子を指定しない限り、作成されたアラームの名前のプレフィックスとして使用されます。

## アラーム設定の高速化の例

次の例では、システムは一致する Linux インスタンスにアタッチされたディスクごとにアラームを作成します。

```
{
    "AWS::EC2::Instance::Disk": {
        "LinuxDiskAlarm": {
            "Tag": {
                "Key": "ams:rt:mylinuxinstance",
                "Value": "true"
            },
            "AlarmDefinition": {
                "MetricName": "disk_used_percent",
                "Namespace": "CWAgent",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
                    },
                    {
                        "Name": "device",
                        "Value": "${EC2::Disk::Device}"
```

```
                    },
                    {
                        "Name": "fstype",
                        "Value": "${EC2::Disk::FSType}"
                    },
                    {
                        "Name": "path",
                        "Value": "${EC2::Disk::Path}"
                    }
                ],
                "AlarmName": "${EC2::InstanceId}: Disk Usage Too High -
 ${EC2::Disk::UUID}"
                ...
            }
        }
    }
}
```

次の例では、システムは一致する Windows インスタンスにアタッチされたディスクごとにアラームを作成します。

```
{
     "AWS::EC2::Instance::Disk": {
        "WindowsDiskAlarm": {
            "Tag": {
                "Key": "ams:rt:mywindowsinstance",
                "Value": "true"
            },
            "AlarmDefinition": {
                "MetricName": "LogicalDisk % Free Space",
                "Namespace": "CWAgent",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
                    },
                    {
                        "Name": "objectname",
                        "Value": "LogicalDisk"
                    },
                    {
                        "Name": "instance",
                        "Value": "${EC2::Disk::Path}"
```

```
                    }
                ],
                "AlarmName": "${EC2::InstanceId}: Disk Usage Too High -
 ${EC2::Disk::UUID}"
                ...
            }
        }
    }
}
```

## Accelerate Alarm Manager 設定の表示

AMSManagedAlarms と CustomerManagedAlarms の両方を AppConfigwith GetConfiguration で確認できます。

GetConfiguration 呼び出しの例を次に示します。

```
aws appconfig get-configuration --application AMSAlarmManager --environment
 AMSInfrastructure --configuration AMSManagedAlarms --client-id
      any-string outfile.json
```

- アプリケーション: これは機能を提供するための AppConfig の論理ユニットです。Alarm Manager の場合、これは AMSAlarmManager
- 環境: これは AMSInfrastructure 環境です
- 設定: AMS Accelerate ベースラインアラームを表示するには、値は ですAMSManagedAlarms。お客様のアラーム定義を表示するには、設定は です。 CustomerManagedAlarms
- クライアント ID: これは一意のアプリケーションインスタンス識別子であり、任意の文字列にすることができます。
- アラーム定義は、指定された出力ファイルで表示できます。この場合、 outfile.json

AMSInfrastructure 環境で過去のデプロイを表示することで、アカウントにデプロイされている設定のバージョンを確認できます。

## Accelerate アラーム設定の変更

新しいアラーム定義を追加または更新するには、設定ドキュメント をデプロイするかCloudFormation を使用した Accelerate 設定変更のデプロイ、CreateHostedConfigurationVersion API を呼び出します。

これは base64 でパラメータ値を生成する Linux コマンドラインコマンドです。これは AppConfig CLI コマンドで想定されています。詳細については、 AWS CLI ドキュメント「Binary/Blob (バイナリラージオブジェクト )」を参照してください。

例:

```
aws appconfig create-hosted-configuration-version --application-id application-id --
configuration-profile-id configuration-profile-id --content base64-string
      --content-type application/json
```

- アプリケーション ID: アプリケーション AMS AlarmManager の ID。これは ListApplications API コールで確認できます。
- 設定プロファイル ID: CustomerManagedAlarms 設定の ID。これは ListConfigurationProfiles API コールで確認できます。
- コンテンツ: Base64 でエンコードして作成するコンテンツの Base64 文字列: cat alarms-v2.json | base64 (「Binary/Blob (binary large object)」を参照 )。

  コンテンツタイプ: アラーム定義は JSON で記述`application/json`されるため、MIME タイプ。

> **Important**
>
> StartDeployment および StopDeployment API アクションへのアクセスを、ターゲットに新しい設定をデプロイする責任と結果を理解している信頼できるユーザーにのみ制限します。

AWS AppConfig 機能を使用して設定を作成およびデプロイする方法の詳細については、「AWS AppConfig の使用」を参照してください。

## Accelerate アラームのデフォルト設定の変更

デフォルトの設定プロファイルを変更することはできませんが、カスタマイズプロファイルでデフォルトの設定ブロックと同じ ConfigurationID で設定ブロックを指定することで、デフォルトを上書きできます。これを行うと、設定ブロック全体が、タグ付け設定を適用するデフォルトの設定ブロックを上書きします。

たとえば、次のデフォルトの設定プロファイルを考えてみましょう。

```
{
```

```
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": true,
            "Tag": {
                "Key": "ams:rt:ams-monitoring-policy",
                "Value": "ams-monitored"
            },
            "AlarmDefinition": {
                "AlarmName": "${EC2::InstanceId}: AMS Default Alarm",
                "Namespace": "AWS/EC2",
                "MetricName": "CPUUtilization",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
                    }
                ],
                "Threshold": 5,
                ...
            }
        }
    }
}
```

このアラームのしきい値を 10 に変更するには、変更する部分だけでなく、アラーム定義全体を指定する必要があります。たとえば、次のカスタマイズプロファイルを指定できます。

```
{
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": true,
            "Tag": {
                "Key": "ams:rt:ams-monitoring-policy",
                "Value": "ams-monitored"
            },
            "AlarmDefinition": {
                "AlarmName": "${EC2::InstanceId}: AMS Default Alarm",
                "Namespace": "AWS/EC2",
                "MetricName": "CPUUtilization",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
```

```
                    }
                ],
                "Threshold": 10,
                ...
            }
        }
    }
}
```

> **Important**
>
> 設定の変更を行った後は、必ずデプロイしてください。SSM AppConfig では、作成後に設定の新しいバージョンをデプロイする必要があります。

## Accelerate アラーム設定変更のデプロイ

カスタマイズが完了したら、AppConfig または を使用してデプロイする必要があります CloudFormation。

トピック

- AppConfig を使用して Accelerate アラーム設定の変更をデプロイする
- CloudFormation を使用した Accelerate 設定変更のデプロイ

### AppConfig を使用して Accelerate アラーム設定の変更をデプロイする

カスタマイズが完了したら、AppConfig を使用して StartDeployment で変更をデプロイします。

```
  aws appconfig start-deployment --application-id application_id
   --environment-id environment_id Vdeployment-strategy-id
   deployment_strategy_id --configuration-profile-id configuration_profile_id --
configuration-version 1
```

- アプリケーション ID: アプリケーションの ID。これは ListApplications API コールで`AMSAlarmManager`確認できます。
- 環境 ID: これは ListEnvironments API コールで確認できます。
- デプロイ戦略 ID: これは ListDeploymentStrategies API コールで確認できます。

- 設定プロファイル ID: の IDCustomerManagedAlarms。これは ListConfigurationProfiles API コールで確認できます。
- 設定バージョン: デプロイする設定プロファイルのバージョン。

> **Important**
>
> Alarm Manager は、設定プロファイルで指定されたアラーム定義を適用します。または CloudWatch CLI/SDK を使用して AWS マネジメントコンソール CloudWatch アラームに手動で行った変更は、自動的に元に戻されるため、変更が Alarm Manager で定義されていることを確認してください。Alarm Manager によって作成されるアラームを理解するには、値のams:alarm-manager:managedタグを探しますtrue。
> StartDeployment および StopDeployment API アクションへのアクセスを、ターゲットに新しい設定をデプロイする責任と結果を理解している信頼されたユーザーに制限します。

AWS AppConfig 機能を使用して設定を作成およびデプロイする方法の詳細については、AWS AppConfig ドキュメントを参照してください。

CloudFormation を使用した Accelerate 設定変更のデプロイ

を使用してCustomerManagedAlarms設定プロファイルをデプロイする場合は CloudFormation、次の CloudFormation テンプレートを使用できます。目的の JSON 設定を AMSAlarmManagerConfigurationVersion.Contentフィールドに入力します。

CloudFormation スタックまたはスタックセットにテンプレートをデプロイすると、設定に必要な JSON 形式に従わない場合、AMSResourceTaggerDeploymentリソースのデプロイは失敗します。予想される形式の詳細については、高速設定プロファイル: モニタリング「」を参照してください。

これらのテンプレートを CloudFormation スタックまたはスタックセットとしてデプロイする方法については、以下の関連する AWS CloudFormation ドキュメントを参照してください。

- AWS CloudFormation コンソールでのスタックの作成
- AWS CLI を使用したスタックの作成
- スタックセットの作成

> **Note**
>
> これらのテンプレートのいずれかを使用して設定バージョンをデプロイし、その後 CloudFormation スタック/スタックセットを削除すると、テンプレート設定バージョンは現在のデプロイ済みバージョンのままになり、追加のデプロイは行われません。デフォルト設定に戻す場合は、スタックを削除するのではなく、手動で空の設定 ({} のみ) をデプロイするか、スタックを空の設定に更新する必要があります。

JSON

```
{
  "Description": "Custom configuration for the AMS Alarm Manager.",
  "Resources": {
    "AMSAlarmManagerConfigurationVersion": {
      "Type": "AWS::AppConfig::HostedConfigurationVersion",
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-ApplicationId"
        },
        "ConfigurationProfileId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-
ProfileID"
        },
        "Content": "{}",
        "ContentType": "application/json"
      }
    },
    "AMSAlarmManagerDeployment": {
      "Type": "AWS::AppConfig::Deployment",
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-ApplicationId"
        },
        "ConfigurationProfileId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-
ProfileID"
        },
        "ConfigurationVersion": {
          "Ref": "AMSAlarmManagerConfigurationVersion"
        },
        "DeploymentStrategyId": {
```

```
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-Deployment-StrategyID"
        },
        "EnvironmentId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-EnvironmentId"
        }
      }
    }
  }
}
```

YAML

```
Description: Custom configuration for the AMS Alarm Manager.
Resources:
  AMSAlarmManagerConfigurationVersion:
    Type: AWS::AppConfig::HostedConfigurationVersion
    Properties:
      ApplicationId:
        !ImportValue AMS-Alarm-Manager-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-ProfileID
      Content: |
        {

        }
      ContentType: application/json
  AMSAlarmManagerDeployment:
    Type: AWS::AppConfig::Deployment
    Properties:
      ApplicationId:
        !ImportValue AMS-Alarm-Manager-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-ProfileID
      ConfigurationVersion:
        !Ref AMSAlarmManagerConfigurationVersion
      DeploymentStrategyId:
        !ImportValue AMS-Alarm-Manager-Configuration-Deployment-StrategyID
      EnvironmentId:
        !ImportValue AMS-Alarm-Manager-Configuration-EnvironmentId
```

## ロールバック Accelerate アラームの変更

以前の設定プロファイルバージョンを指定して StartDeployment を実行することで、同じデプロイメカニズムを通じてアラーム定義をロールバックできます。

## Accelerate アラームの保持

AMS によってモニタリングされるリソースが削除されると、それらのリソースに対して Alarm Manager によって作成されたアラームは、Alarm Manager によって自動的に削除されます。監査、コンプライアンス、または履歴の目的で特定のアラームを保持する必要がある場合は、Alarm Manager の保持タグ付け機能を使用します。

モニタリング対象のリソースが削除された後でもアラームを保持するには、次の例に示すように、アラームのカスタム設定に `"ams:alarm-manager:retain"` タグを追加します。

```
{
  "AWS::EC2::Instance": {
    "AMSCpuAlarm": {
      "Enabled": true,
      "Tag": {
        "Key": "ams:rt:ams-monitoring-policy",
        "Value": "ams-monitored"
      },
      "AlarmDefinition": {
        "AlarmName": "${EC2::InstanceId}: CPU Too High",
        "AlarmDescription": "AMS Baseline Alarm for EC2 CPUUtilization",
        [...]
        "Tags": [
          {
            "Key": "ams:alarm-manager:retain",
            "Value": "true"
          }
        ]
      }
    }
  }
}
```

`"ams:alarm-manager:retain"` タグで設定されたアラームは、モニタリング対象のリソースが終了しても、アラームマネージャーによって自動的に削除されません。保持されたアラームは、CloudWatch を使用して手動で削除するまで CloudWatch で無期限に保持されます。

## デフォルトの Accelerate アラーム設定を無効にする

AMS Accelerate は、ベースラインアラームに基づいてアカウントのデフォルトの設定プロファイルを提供します。ただし、このデフォルト設定を無効にするには、アラーム定義のいずれかを上書きします。カスタマイズ設定プロファイルでルールの ConfigurationID を上書きし、false の値で有効になっているフィールドを指定します。

たとえば、デフォルトの設定プロファイルに次の設定がある場合です。

```
{
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": true,
            "Tag": {
                "Key": "ams:rt:ams-monitoring-policy",
                "Value": "ams-monitored"
            },
            "AlarmDefinition": {
                ...
            }
        }
    }
```

このタグ付けルールを無効にするには、カスタマイズ設定プロファイルに以下を含めます。

```
{
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": false
        }
    }
}
```

これらの変更を行うには、CreateHostedConfigurationVersion API を JSON プロファイルドキュメントで呼び出す必要があり (「」を参照Accelerate アラーム設定の変更 )、その後デプロイする必要があります (「」を参照 ) Accelerate アラーム設定変更のデプロイ。新しい設定バージョンを作成するときは、以前に作成したカスタムアラームを JSON プロファイルドキュメントに含める必要もあります。

> **Important**
>
> AMS Accelerate がデフォルトの設定プロファイルを更新すると、設定されたカスタムアラームに対してキャリブレーションされないため、カスタマイズ設定プロファイルでアラームを上書きするときにデフォルトのアラームへの変更を確認します。

## Accelerate 用の追加の CloudWatch アラームの作成

Amazon EC2 インスタンスのカスタム CloudWatch メトリクスとアラームを使用して、AMS Accelerate 用の追加の CloudWatch アラームを作成できます。

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 CloudWatch モニタリングスクリプトは、カスタム CloudWatch メトリクスを生成して使用する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。

> **Important**
>
> AMS Accelerate 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。

## Alarm Manager for Accelerate によってモニタリングされるリソースの数の表示

Alarm Manager は、 `AMS/AlarmManager`名前空間の Amazon CloudWatch に 1 時間ごとにメトリクスを送信します。メトリクスは、Alarm Manager でサポートされているリソースタイプに対してのみ出力されます。

| メトリクス名 | ディメンション | 説明 |
| --- | --- | --- |
| ResourceCount | コンポーネント、ResourceType | 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。 |

| メトリクス名 | ディメンション | 説明 |
| --- | --- | --- |
| | | 単位: カウント |
| ResourcesMissingManagedAlarms | コンポーネント、ResourceType | マネージドアラームを必要とする (指定されたリソースタイプの) リソースの数。ただし、Alarm Manager はアラームをまだ適用していません。<br><br>単位: カウント |
| UnmanagedResources | コンポーネント、ResourceType | Alarm Manager によって管理されたアラームが適用されていないリソース (指定されたリソースタイプ) の数。通常、これらのリソースはどの Alarm Manager 設定ブロックとも一致しないか、設定ブロックから明示的に除外されます。<br><br>単位: カウント |
| MatchingResourceCount | コンポーネント、ResourceType、ConfigClauseName | Alarm Manager 設定ブロックに一致する (指定されたリソースタイプの) リソースの数。リソースが設定ブロックと一致するには、ブロックを有効にし、設定ブロックで同じタグを指定する必要があります。<br><br>単位: カウント |

これらのメトリクスは、AMS-Alarm-Manager-Reporting-Dashboard でグラフとしても表示できます。ダッシュボードを表示するには、 AWS CloudWatch マネジメントコンソールから AMS-Alarm-Manager-Reporting-Dashboard を選択します。デフォルトでは、このダッシュボードのグラフには過去 12 時間のデータが表示されます。

AMS Accelerate は CloudWatch アラームをアカウントにデプロイして、AMS Alarm Manager によって管理から除外されたリソースなど、アンマネージドリソースの数の大幅な増加を検出します。AMS オペレーションは、同じタイプの 3 つのリソース、または同じタイプのすべてのリソースの 50% を超えるアンマネージドリソースの増加を調査します。変更が意図的なものではないと思われる場合、AMS オペレーションから変更の確認を求められることがあります。

# 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 |
| --- | --- | --- | --- |
| ステータスチェックに失敗 | 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。 |
| AMSWindowsDiskUsage | 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 |

| アラート名 | 説明 | しきい値 | アクション |
| --- | --- | --- | --- |
| | | | 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-EVENT-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。 | 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。<br><br>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。 `"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".` |

| 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。 | 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。<br><br>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。 `"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".` |

| 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。 | 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% 増やそうとします。リソースが CloudFormation を介して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。<br><br>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。 `"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".` |

| 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。 | 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。<br><br>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。 `"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".` |

## 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により、制御された限られた拡張で成長の必要性のバランスが取れます。
- 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 "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。
- 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。
  - Amazon RDS インスタンスは CloudFormation スタック内のリソースではありません。
- 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。

# AMS での Amazon EventBridge マネージドルールの使用

AMS Accelerate 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 Accelerate 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 |
| --- | --- | --- |
| AmsAccessRolesRule | このルールは、特定の AMS Accelerate ロールとポリシーの変更をリッスンします。 | {<br>"source": ["aws.iam"],<br>"detail-type": ["AWS API Call via CloudTrail"],<br>"detail": {<br>"eventName": [<br>"DeleteRole",<br>"DeletePolicy",<br>"CreatePolicyVersion",<br>"AttachRolePolicy",<br>"DetachRolePolicy"<br>],<br>"requestParameters": {<br>"$or": [<br>{<br>"roleName": [<br>"ams-access-admin",<br>"ams-access-admin-operations",<br>"ams-access-operations",<br>"ams-access-read-only",<br>"ams-access-security-analyst",<br>"ams-access-security-analyst-read-only"<br>]<br>},<br>{<br>"policyArn": [<br>"arn:*:iam::*:policy/ams-access-allow-pass-role",<br>"arn:*:iam::*:policy/ams-access-deny-cloudshell-policy", |

| ルール名 | 説明 | 定義 |
| --- | --- | --- |
| | | "arn:*:iam::*:policy/ams-access-deny-operations-policy",<br>"arn:*:iam::*:policy/ams-access-deny-update-iam-policy",<br>"arn:*:iam::*:policy/ams-access-ssr-policy",<br>"arn:*:iam::*:policy/ams-access-security-analyst-read-only-policy",<br>"arn:*:iam::*:policy/ams-access-security-analyst-policy",<br>"arn:*:iam::*:policy/ams-access-security-analyst-extended-policy",<br>"arn:*:iam::*:policy/ams-access-admin-policy",<br>"arn:*:iam::*:policy/ams-access-admin-operations-policy"<br>]<br>},<br>]<br>},<br>},<br>} |

| ルール名 | 説明 | 定義 |
| --- | --- | --- |
| AMSCoreRule | このルールは、 AWS Config および Amazon CloudWatch イベントを AMS Config 修復および AMS モニタリングサービスに適切に転送します。 AWS Config イベントは、 AWS Systems Manager OpsItems を作成して解決します。Amazon CloudWatch イベントは CloudWatch アラームをモニタリングします。 | <pre>{<br>    {<br>        "source": ["aws.config", "aws.cloudwatch"],<br>        "detail-type": ["Config Rules Compliance Change", "CloudWatch Alarm State Change"],<br>    }<br>}</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 のマネージドルールの削除

マネージドル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ルールを削除します。

AMS がオフボーディング中にマネージドル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、マネージドル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、マネージドルールの強制削除を実行する必要があります。

# AMS の信頼された修復

Trusted Remediator は、 AWS Trusted Advisorおよび レコメンデAWS Compute Optimizerーション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 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。

## Trusted Remediator 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 チェックと AWS Compute Optimizer レコメンデーションの修復： 設定後、信頼された修復者は選択したチェックの修復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 環境内の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、 の評価 Trusted Advisor と Compute Optimizer の推奨事項 AWS アカウントを評価し、OpsCenter に OpsItems を作成します AWS Systems Manager 。 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 OpsItem を作成して確認できるようにします。確認したら、オートメーションドキュメントを起動します。

修復ログは Amazon S3 バケットに保存されます。S3 バケットのデータを使用して、レポート用のカスタム QuickSight 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。詳細については、「信頼できる修復レポート」を参照してください。

## 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 および AWS Compute Optimizer： AWS Trusted Advisor および Compute Optimizer が提供するクラウド最適化サービスは、環境 AWS 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」および「AWS Compute Optimizer」を参照してください。

- Trusted Remediator: Trusted Advisorチェックと AWS Compute Optimizerレコメンデーションのための 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 チェックと Compute Optimizer の推奨事項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 リソースで 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 運用上の問題を追跡して解決するの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、 のー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。 AWS AppConfig コンソールまたは API を使用して設定を編集できます。
- 実行モード： 実行モードは、各 Trusted Advisor チェック結果の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 Trusted Remediator 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 Accelerate 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 および Compute Optimizer 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。オンボーディング後、 AWS AppConfig コンソールまたは API を使用して設定を管理できます。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。

## 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 チェックと Compute Optimizer の推奨事項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 チェック修復のために厳選された 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レTrusted Advisorコメンデーションと Compute Optimizer レコメンデーションのリスト、または関連する 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. 選択した Trusted Advisor チェックの修復を有効にするには、設定を更新します。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[信頼できる修復ツールで修復を追跡する]。OpsCenter

### 信頼できる修復ツールで手動修復を実行する

Trusted Advisor チェックを手動で修正できます。手動修復を開始すると、信頼された修復者は手動実行 OpsItem を作成します。OpsItems を修正するには、SSM オートメーションドキュメントを確認して開始する必要があります。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でチェックの修正を有効にする前に、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 | | |
| [Amazon EC2 インスタンスのレコメンデーション] | AWSManagedServices-TrustedRemediatorResizeInstanceByComputeOptimizerRecommendation<br><br>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 | • 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 日間です。<br><br>制約なし<br>• CreateAMIBeforeResize: サイズ変更前にインスタンス AMI を |

| 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 |
| --- | --- | --- |
| | 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。 | バックアップとして作成するには、「True」に設定します。バックアップを作成しない場合は、「False」に設定します。デフォルトは「True」です。<br><br>制約なし |

| 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 |
| --- | --- | --- |
| Amazon EBS ボリュームレコメンデーション | AWSManagedServices-ModifyEBSVolume<br><br>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。 | • 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、「False」に設定します。デフォルトは「True」です。<br><br>制約なし<br>• 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。<br><br>制約なし<br>• 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。<br><br>制約なし<br>• 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。<br><br>制約なし<br>• 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 |

| 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 |
| --- | --- | --- |
| | | タは gp3 ボリュームでのみ有効です。<br><br>制約なし<br>• 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、「True」に設定します。ドリフト修復を試行しない場合は、「False」に設定します。デフォルトは「True」です。<br><br>制約なし |
| Lambda 関数のレコメンデーション | AWSManagedServices-TrustedRemediatorOptimizeLambdaMemory<br><br>AWS Lambda Compute Optimizer の推奨事項に従って最適化された 関数メモリ。 | 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。<br><br>制約なし |
| アイドル状態のリソース | | |

| 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 |
| --- | --- | --- |
| アイドル状態の Amazon EBS ボリューム | AWSManagedServices-DeleteUnusedEBSVolume<br><br>アタッチされていない Amazon EBS ボリュームは削除されます。 | • 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、「False」に設定します。デフォルトは「True」です。<br><br>制約なし<br>• 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。<br><br>制約なし |
| アイドル状態の Amazon EC2 インスタンス | AWSManagedServices-StopEC2Instance<br><br>アイドル状態の 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的に停止するには、「True」に設定します。強制停止しない場合は、「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。<br><br>制約なし |

| 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 |
| --- | --- | --- |
| アイドル状態の Amazon RDS インスタンス | AWSManagedServices-StopIdleRDSInstance<br><br>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。 | 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 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 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 でのコントロールの有効化」を参照してください。事前設定された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 |
| --- | --- | --- |
| Z4AUBRNSmz<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 |
| c18d2gz150 - 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。 | • 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。<br>• 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。<br><br>制約なし |
| c18d2gz128<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 |
| DAvU99Dc4C<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 | • 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 |

| 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。 | 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。<br>• 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確認しず、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 です7。<br><br>制約なし |
| hjLMh88uM8<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。 | 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。<br><br>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。 |

| 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 |
| --- | --- | --- |
| Ti39halfu8<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 |
| COr6dfpM05<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。 |
| Qch7DwouX1<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。のデフォルト値は、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 |
| --- | --- | --- |
| Qch7DwouX1<br><br>低稼働率の Amazon EC2 インスタンス | AWSManagedServices-ResizeInstanceByOneLevel<br><br>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。このオートメーションは、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。 | • 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。<br>• 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。<br>• ResizeIfStopped: 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。<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 |
| --- | --- | --- |
| Qch7DwouX1<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 グループに含まれておらず、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 |
| G31sQ1E9U<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 |
| c1cj39rr6v<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 |
| c1z7kmr00n<br><br>インスタンスの Amazon EC2 コスト最適化の推奨事項 | 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信頼できる修復者がサポートする Compute Optimizer の推奨事項。 | 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 |
|---|---|---|
| c1z7kmr02n<br><br>ボリュームの Amazon EBS コスト最適化の推奨事項 | の Amazon EBS ボリューム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信頼できる修復者がサポートする Compute Optimizer の推奨事項。 | 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 |
| c1z7kmr03n<br><br>DB インスタンスの Amazon RDS コスト最適化の推奨事項 | からアイドル状態の Amazon RDS インスタンスを使用します信頼できる修復者がサポートする Compute Optimizer の推奨事項。 | 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 |
| c1z7kmr05n<br><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信頼できる修復者がサポートする Compute Optimizer の推奨事項。 | 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 |
|---|---|---|
| 12Fnkpl8Y5<br><br>露出したアクセスキー | AWSManagedServices-TrustedRemediatorDeactivateIAMAccessKey<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 |
| --- | --- | --- |
| Hs4Ma3G127 - 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<br><br>対応する AWS Security Hub CSPM チェック: APIGateway.1 | 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。 | 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。<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、「API Gateway で REST API の CloudWatch ログ記録を設定する APIs」を参照してください。 |
| Hs4Ma3G129 - 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<br><br>対応する AWS Security Hub CSPM チェック: APIGateway.3 | AWSManagedServices-EnableApiGateWayXRayTracing<br><br>X-Ray トレースは 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>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 |
| --- | --- | --- |
| 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<br><br>対応する AWS Security Hub CSPM チェック: APIGateway.5 | AWSManagedServices-EnableAPIGatewayCacheEncryption<br><br>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。 | 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 |
| Hs4Ma3G177 -<br><br>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 AutoScaling.1 | AWSManagedServices-TrustedRemediatorEnableAutoScalingGroupELBHealthCheck<br><br>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。 | 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。<br><br>Elastic Load Balancing ヘルスチェックを有効にすると、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、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」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 |
| --- | --- | --- |
| Hs4Ma3G245 - CloudFormation スタックは Amazon Simple Notification Service と統合する必要があります<br><br>対応する AWS Security Hub CSPM チェック: CloudFormation.1 | AWSManagedServices-EnableCFNStackNotification<br><br>CloudFormation スタックを通知用の Amazon SNS トピックに関連付けます。 | NotificationARNs 選択した CloudFormation スタックに関連付ける Amazon SNS トピックの ARNs。<br><br>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。 |

| 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 |
| --- | --- | --- |
| Hs4Ma3G210 - CloudFront ディストリビューションでは口グ記録が有効になっている必要があります<br><br>対応する AWS Security Hub CSPM チェック: CloudFront.2 | AWSManagedServices-EnableCloudFrontDistributionLogging<br><br>口グ記録は Amazon CloudFront ディストリビューションで有効になっています。 | • BucketName: アクセスログを保存する Amazon S3 バケットの名前。<br>• S3KeyPrefix: theAmazon CloudFront ディ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。<br>• IncludeCookies: アクセスログに Cookie を含めるかどうかを示します。<br><br>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。<br><br>• BucketName<br>• S3KeyPrefix<br>• IncludeCookies<br><br>この修復の制約については、CloudFront ディストリビューションの口グ記録を有効にするにはどうすればよいですか？」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 |
| --- | --- | --- |
| Hs4Ma3G109 - CloudTrail ログファイルの検証を有効にする必要があります<br><br>対応する AWS Security Hub CSPM チェック: CloudTrail.4 | AWSManagedServices-TrustedRemediatorEnableCloudTrailLogValidation<br><br>CloudTrail 証跡ログの検証を有効にします。 | 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 |
| Hs4Ma3G108 - CloudTrail 証跡は Amazon CloudWatch Logs と統合する必要があります<br><br>対応する AWS Security Hub CSPM チェック: CloudTrail.5 | AWSManagedServices-IntegrateCloudTrailWithCloudWatch<br><br>AWS CloudTrail は CloudWatch Logs と統合されています。 | • 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。<br>• 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。<br><br>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。<br><br>• CloudWatchLogsLogGroupName<br>• CloudWatchLogsRoleName |

| 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 |
| --- | --- | --- |
| Hs4Ma3G217 - CodeBuild プロジェクト環境にはログ記録 AWS 設定が必要です<br><br>対応する AWS Security Hub CSPM チェック: CodeBuild.4 | AWSManagedServices-TrustedRemediatorEnableCodeBuildLoggingConfig<br><br>CodeBuild プロジェクトのログ記録を有効にします。 | 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 |
| 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<br><br>対応する AWS Security Hub CSPM チェック: DocumentDB.3 | AWSManagedServices-TrustedRemediatorDisablePublicAccessOnDocumentDBSnapshot<br><br>Amazon DocumentDB 手動クラスタースナップショットからパブリックアクセスを削除します。 | 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 |
| 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<br><br>対応する AWS Security Hub CSPM チェック: DocumentDB.5 | AWSManagedServices-TrustedRemediatorEnableDocumentDBClusterDeletionProtection<br><br>Amazon DocumentDB クラスターの削除保護を有効にします。 | 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 |

| 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 |
| --- | --- | --- |
| 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<br><br>対応する AWS Security Hub CSPM チェック: DynamoDB.6 | AWSManagedServices-TrustedRemediatorEnableDynamoDBTableDeletionProtection<br><br>AMS 以外の DynamoDB テーブルの削除保護を有効にします。 | 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 |
| ePs02jT06w - Amazon EBS パブリックスナップショット | AWSManagedServices-TrustedRemediatorDisablePublicAccessOnEBSSnapshot<br><br>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。 | 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 |
| 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<br><br>対応する AWS Security Hub CSPM チェック: EC2.2 | AWSManagedServices-TrustedRemediatorRemoveAllRulesFromDefaultSG<br><br>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。 | 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 |
| --- | --- | --- |
| 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<br><br>対応する AWS Security Hub CSPM チェック: EC2.3 | AWSManagedServices-EncryptInstanceVolume<br><br>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。 | • ボリュームを暗号化するための KMSKeyId: AWS KMS key ID または ARN。<br>• 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。<br><br>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。 |
| 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<br><br>対応する AWS Security Hub CSPM チェック: EC2.4 | 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 SSM ドキュメント )<br><br>30 日間停止した Amazon EC2 インスタンスは終了します。 | 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。<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 |
| --- | --- | --- |
| 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<br><br>対応する AWS Security Hub CSPM チェック: EC2.4 | 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。 | 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。<br><br>制約なし |
| 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<br><br>対応する AWS Security Hub CSPM チェック: EC2.7 | AWSManagedServices-EncryptEBSByDefault<br><br>特定の に対して 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 | 事前設定済みのパラメータは許可されません。<br><br>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。 |

| 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 |
| --- | --- | --- |
| Hs4Ma3G124 - 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<br><br>対応する AWS Security Hub CSPM チェック: EC2.8 | AWSManagedServices-TrustedRemediatorEnableEC2InstanceIMDSv2<br><br>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。 | • 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。<br>• 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。<br><br>制約なし |
| 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<br><br>対応する AWS Security Hub CSPM チェック: EC2.15 | AWSManagedServices-UpdateAutoAssignPublicIpv4Addresses<br><br>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。 | 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 |
| --- | --- | --- |
| 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す<br><br>対応する AWS Security Hub CSPM チェック: EC2.16 | AWSManagedServices-DeleteUnusedNACL<br><br>未使用のネットワーク ACL を削除する | 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 |
| 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<br><br>対応する AWS Security Hub CSPM チェック: EC2.22 | AWSManagedServices-DeleteSecurityGroups<br><br>未使用のセキュリティグループを削除します。 | 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 |

| 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 |
| --- | --- | --- |
| 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<br><br>対応する AWS Security Hub CSPM チェック: EC2.23 | AWSManagedServices-TrustedRemediatorDisableTGWAutoVPCAttach - 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。 | 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 |
| Hs4Ma3G235 - ECR プライベート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<br><br>対応する AWS Security Hub CSPM チェック: ECR.2 | AWSManagedServices-TrustedRemediatorSetImageTagImmutability<br><br>指定されたリ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。 | 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 |
| --- | --- | --- |
| 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<br><br>対応する AWS Security Hub CSPM チェック: ECR.3 | AWSManagedServices-PutECRRepositoryLifecyclePolicy<br><br>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。 | 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。<br><br>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。<br><br>LifecyclePolicyText |
| 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<br><br>対応する AWS Security Hub CSPM チェック: EKS.8 | AWSManagedServices-TrustedRemediatorEnableEKSAuditLog<br><br>監査ログは EKS クラスター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 |

| 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 |
| --- | --- | --- |
| 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<br><br>対応する AWS Security Hub CSPM チェック: ELB.4 | AWSConfigRemediation-DropInvalidHeadersForALB<br><br>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。 | 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 |
| 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<br><br>対応する AWS Security Hub CSPM チェック: ELB.5 | 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 ）<br><br>Application Load Balancer と Classic Load Balancer のログ記録が有効になっています。 | • 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。<br>• 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。<br><br>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。<br><br>• BucketName<br>• S3KeyPrefix<br><br>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。 |

| 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 |
| --- | --- | --- |
| 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<br><br>対応する AWS Security Hub CSPM チェック: ELB.5 | AWSManagedServices-EnableELBLoggingV2<br><br>Application Load Balancer と Classic Load Balancer のログ記録が有効になっています。 | • 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。<br>• 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。<br>• 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、「プレフィックスを使用してオブジェクトを整理する」を参照してください。<br><br>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。<br>• TargetBucketTagKey<br>• TargetBucketTagValue<br>• S3BucketPrefix |

| 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。 |
| 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<br><br>対応する AWS Security Hub CSPM チェック: EMR.2 | AWSManagedServices-TrustedRemediatorEnableEMRBlockPublicAccess<br><br>アカウントの Amazon EMR ブロックパブリックアクセス設定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 |
| Hs4Ma3G135 - AWS KMS キーを意図せずに削除しないでください<br><br>対応する AWS Security Hub CSPM チェック: KMS.3 | AWSManagedServices-CancelKeyDeletion<br><br>AWS KMS キーの削除はキャンセルされます。 | 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 |

| 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 |
| --- | --- | --- |
| Hs4Ma3G299 - Amazon DocumentDB 手動クラスタースナップショットは公開しないでください<br><br>対応する AWS Security Hub CSPM チェック: Neptune.4 | AWSManagedServices-TrustedRemediatorEnableNeptuneDBClusterDeletionProtection<br><br>Amazon Neptune クラスターの削除保護を有効にします。 | 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 |
| 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<br><br>対応する AWS Security Hub CSPM チェック: NetworkFirewall.9 | AWSManagedServices-TrustedRemediatorEnableNetworkFirewallDeletionProtection - AWS Network Firewall の削除保護を有効にします。 | 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 |

| 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 |
| --- | --- | --- |
| 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<br><br>対応する AWS Security Hub CSPM チェック: OpenSearch.3 | AWSManagedServices-EnableOpenSearchNodeToNodeEncryption<br><br>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。 | 事前設定済みのパラメータは許可されません。<br><br>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。 |
| 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<br><br>対応する AWS Security Hub CSPM チェック: Opensearch.4 | AWSManagedServices-EnableOpenSearchLogging<br><br>OpenSearch ドメインでエラーログ記録が有効になっています。 | CloudWatchLogGroupArn: anAmazon CloudWatch Logs ロググループの ARN。<br><br>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。<br><br>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「監査ログの有効化」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 |
| --- | --- | --- |
| 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<br><br>対応する AWS Security Hub CSPM チェック: Opensearch.5 | AWSManagedServices-EnableOpenSearchLogging<br><br>OpenSearch ドメインは、監査ログ記録を有効にして設定されます。 | CloudWatchLogGroupArn: ログを発行する CloudWatch Logs グループの ARN。<br><br>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<br><br>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「監査ログの有効化」を参照してください。 |
| 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<br><br>対応する AWS Security Hub CSPM チェック: Opensearch.8 | AWSManagedServices-EnableOpenSearchEndpointEncryptionTLS1.2<br><br>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。 | 事前設定済みのパラメータは許可されません。<br><br>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。 |

| 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 |
| --- | --- | --- |
| 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<br><br>対応する AWS Security Hub CSPM チェック: RDS.1 | AWSManagedServices-DisablePublicAccessOnRDSSnapshotV2<br><br>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。 | 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 |
| 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<br><br>対応する AWS Security Hub CSPM チェック: RDS.2 | AWSManagedServices-TrustedRemediatorDisablePublicAccessOnRDSInstance<br><br>RDS DB インスタンスのパブリックアクセスを無効にします。 | 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 |

| 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 |
| --- | --- | --- |
| Hs4Ma3G189 - Amazon RDS DB インスタンス用に拡張モニタリングが設定されています<br><br>対応する AWS Security Hub CSPM チェック: RDS.6 | AWSManagedServices-TrustedRemediatorEnableRDSEnhancedMonitoring<br><br>Amazon RDS DB インスタンスの拡張モニタリングを有効にする | • 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。<br>• 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。<br><br>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。 |

| 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 |
| --- | --- | --- |
| 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<br><br>対応する AWS Security Hub CSPM チェック: RDS.7 | AWSManagedServices-TrustedRemediatorEnableRDSDeletionProtection<br><br>削除保護は Amazon RDS クラスター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 |
| 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<br><br>対応する AWS Security Hub CSPM チェック: RDS.8 | AWSManagedServices-TrustedRemediatorEnableRDSDeletionProtection<br><br>削除保護は Amazon RDS インスタンス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 |

| 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 |
|---|---|---|
| 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<br><br>対応する AWS Security Hub CSPM チェック: RDS.9 | AWSManagedServices-TrustedRemediatorEnableRDSLogExports<br><br>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。 | 事前設定済みのパラメータは許可されません。<br><br>サービスにリンクされたロール AWSServiceRoleForRDS が必要です。 |
| Hs4Ma3G160 - RDS インスタンスには IAM 認証を設定する必要があります<br><br>対応する AWS Security Hub CSPM チェック: RDS.10 | AWSManagedServices-UpdateRDSIAMDatabaseAuthentication<br><br>AWS Identity and Access Management 認証は RDS インスタンスに対して有効になっています。 | 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、 を選択しますtrue。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、 を選択しますfalse。<br><br>制約なし |
| Hs4Ma3G161 - RDS クラスターには IAM 認証を設定する必要があります<br><br>対応する AWS Security Hub CSPM チェック: RDS.12 | AWSManagedServices-UpdateRDSIAMDatabaseAuthentication<br><br>RDS クラスターで IAM 認証が有効になっています。 | 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、 を選択しますtrue。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、 を選択しますfalse。<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 |
| --- | --- | --- |
| 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<br><br>対応する AWS Security Hub CSPM チェック: RDS.13 | AWSManagedServices-UpdateRDSInstanceMinorVersionUpgrade<br><br>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。 | 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。 |
| 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<br><br>対応する AWS Security Hub CSPM チェック: RDS.16 | AWSManagedServices-UpdateRDSCopyTagsToSnapshots<br><br>`CopyTagtosnapshot` Amazon RDS クラスターの 設定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。 |

| 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 |
| --- | --- | --- |
| 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<br><br>対応する AWS Security Hub CSPM チェック: RDS.17 | AWSManagedServices-UpdateRDSCopyTagsToSnapshots<br><br>CopyTagsToSnapshot Amazon RDS の 設定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。 |
| rSs93HQwa1<br><br>Amazon RDS パブリックスナップショット | AWSManagedServices-DisablePublicAccessOnRDSSnapshotV2<br><br>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。 | 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 |
| 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<br><br>対応する AWS Security Hub CSPM チェック: Redshift.1 | AWSManagedServices-DisablePublicAccessOnRedshiftCluster<br><br>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。 | 事前設定済みのパラメータは許可されません。<br><br>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。 |

| 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 |
| --- | --- | --- |
| 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<br><br>対応する AWS Security Hub CSPM チェック: Redshift.4 | AWSManagedServices-TrustedRemediatorEnableRedshiftClusterAuditLogging<br><br>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。 | 事前設定済みのパラメータは許可されません。<br><br>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。<br><br>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。<br><br>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。 |
| 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<br><br>対応する AWS Security Hub CSPM チェック: Redshift.6 | 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。 | 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 |
| --- | --- | --- |
| 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<br><br>対応する AWS Security Hub CSPM チェック: Redshift.7 | AWSManagedServices-TrustedRemediatorEnableRedshiftClusterEnhancedVPCRouting<br><br>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。 | 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 |
| 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<br><br>対応する AWS Security Hub CSPM チェック: S3.8 | AWSManagedServices-TrustedRemediatorBlockS3BucketPublicAccess<br><br>バケットレベルのパブリックアクセスブロックは、Amazon S3 バケットに適用されます。 | 事前設定済みのパラメータは許可されません。<br><br>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の詳細については、Amazon S3ストレージへのパブリックアクセスのブロック」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 |
| --- | --- | --- |
| 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<br><br>対応する AWS Security Hub CSPM チェック: S3.9 | 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 )<br><br>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。 | • TargetBucket: サーバーアクセスログを保存する S3 バケットの名前。<br>• 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。<br><br>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。 |

| 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、「Amazon S3 サーバーアクセスログを有効にします」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 |
| --- | --- | --- |
| 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<br><br>対応する AWS Security Hub CSPM チェック: S3.9 | AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV2 - Amazon S3 バケットのログ記録が有効になっています。 | • 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。<br>• 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。<br>• 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。 |

| 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 |
| --- | --- | --- |
| | | 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。<br><br>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、「Amazon S3 サーバーアクセスログを有効にします」を参照してください。 |
| Pfx0RwqBli<br><br>Amazon S3 バケット許可 | AWSManagedServices-TrustedRemediatorBlockS3BucketPublicAccess<br><br>パブリックアクセスをブロックする | 事前設定済みのパラメータは許可されません。<br><br>このチェックは、複数のアラート条件で構成されます。この自動化は、パブリックアクセスの問題を修正します。で Trusted Advisor フラグ付けされた他の設定の問題の修復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。 |

| 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 |
| --- | --- | --- |
| Hs4Ma3G272 - ユーザーには SageMaker ノートブックインスタンスへのルートアクセスを許可しないでください<br><br>対応する AWS Security Hub CSPM チェック: SageMaker.3 | AWSManagedServices-TrustedRemediatorDisableSageMakerNotebookInstanceRootAccess<br><br>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。 | 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。 |
| 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<br><br>対応する AWS Security Hub CSPM チェック: SNS.1 | AWSManagedServices-EnableSNSEncryptionAtRest<br><br>SNS トピックはサーバー側の暗号化で設定されます。 | 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。<br><br>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、Amazon SNSを有効にする」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 |
| --- | --- | --- |
| Hs4Ma3G158 - SSM ドキュメントは公開しないでください<br><br>対応する AWS Security Hub CSPM チェック: SSM.4 | AWSManagedServices-TrustedRemediatorDisableSSMDocPublicSharing - SSM ドキュメントのパブリック共有を無効にします。 | 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 |

| 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 |
| --- | --- | --- |
| Hs4Ma3G136 - Amazon SQS キューは保管時に暗号化する必要があります<br><br>対応する AWS Security Hub CSPM チェック: SQS.1 | AWSManagedServices-EnableSQSEncryptionAtRest<br><br>Amazon SQS のメッセージは暗号化されます。 | • SqsManagedSseEnabled: 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を有効にするtrueには を、 AWS KMS キーを使用したサーバー側のキュー暗号化を有効にするfalseには に設定します。<br>• 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。<br>• 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。<br><br>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。 |

# 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 |
|---|---|---|
| c18d2gz138<br><br>Amazon 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 |
| R365s2Qddf<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-000000000000 など) の修復をサポートしていません。 |
| BueAdJ7NrP<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。 | • TargetBucket: サーバーアクセスログを保存する S3 バケットの名前。<br>• 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 |

| 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 |
| --- | --- | --- |
| | | クスに 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。<br><br>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。<br><br>• TargetBucket<br><br>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、「Amazon S3 サーバーアクセスログを有効にします」を参照してください。 |
| f2iK5R6Dep<br><br>Amazon RDS 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。 | 事前設定済みのパラメータは許可されません。<br><br>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。 |

| 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 |
| --- | --- | --- |
| H7IgTzjTYb<br><br>Amazon EBS スナップショット | AWSManagedServices-TrustedRemediatorCreateEBSSnapshot<br><br>Amazon EBSsnapshotsが作成されます。 | 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 |
| opQPADkZvH<br><br>RDS バックアップ | AWSManagedServices-EnableRDSBackupRetention<br><br>DB に対して Amazon RDS バックアップ保持が有効になっています。 | • BackupRetentionPeriod: 自動バックアップを保持する日数 (1 ~ 35)。<br>• 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。<br><br>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。 |

| 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 |
| --- | --- | --- |
| c1qf5bt013<br><br>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 | 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。 | • MaxAllocatedStorageIncreasePercentage: AllocatedStorage の増加率。 MaxAllocatedStorage デフォルトでは 26 に設定されています。<br><br>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、「Managing capacity automatically with Amazon Relational Database Service storage autoscaling」を参照してください。<br><br>制約なし |
| 7qGXsKIUw<br><br>Classic Load Balancer 接続ドレイン | AWSManagedServices-TrustedRemediatorEnableCLBConnectionDraining<br><br>Classic Load Balancer で接続ドレイニングが有効になっています。 | 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。<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 |
| --- | --- | --- |
| c18d2gz106<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。<br><br>• TagKey<br>• TagValue<br><br>制約なし |
| c18d2gz107<br><br>Amazon DynamoDB テーブルが AWS Backup プランに含まれていない | AWSManagedServices-TrustedRemediatorAddDynamoDBToBackupPlanAddDynamoDBToBackupPlan<br><br>Amazon DynamoDB テーブルは AWS Backup プランに含まれています。 | 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。<br><br>• TagKey<br>• TagValue<br><br>制約なし |
| c18d2gz117<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。<br><br>• TagKey<br>• TagValue<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 |
| --- | --- | --- |
| c18d2gz105<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 |
| c1qf5bt026<br><br>Amazon RDS `synchronous_commit` パラメータがオフになっている | AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter<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 |
| c1qf5bt030<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-TrustedRemediatorRemediateRDSParameterGroupParameter<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 |
| c1qf5bt031<br><br>Amazon RDS `sync_binlog` パラメータがオフになっている | AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter<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 |
|---|---|---|
| c1qf5bt036<br><br>Amazon RDS `innodb_default_row_format` パラメータ設定が安全ではない | AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter<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 |
| c18d2gz144<br><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 |
|---|---|---|
| COr6dfpM06<br><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 関数の推奨メモリ割り当て。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。 |
| ZRxQlPsb6c<br><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 | • 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 |

| 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 |
| --- | --- | --- |
| | 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。 | 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。<br>• 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。<br>• ResizeIfStopped: 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 |

| 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 |
| --- | --- | --- |
| c1qf5bt021<br><br>最適値未満を使用する Amazon RDS `innodb_change_buffering` パラメータ | AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter<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 |
| c1qf5bt025<br><br>Amazon RDS `autovacuum` パラメータがオフになっている | AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter<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 |
| c1qf5bt028<br><br>Amazon RDS `enable_indexonlyscan` パラメータがオフになっている | AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter<br><br>Amazon RDS のパラメータ`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 |
| c1qf5bt029<br><br>Amazon RDS `enable_indexscan` パラメータがオフになっている | AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter<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 |
|---|---|---|
| c1qf5bt032<br><br>Amazon RDS `innodb_stats_persistent` パラメータがオフになっている | AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter<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 |
| c1qf5bt037<br><br>Amazon RDS `general_logging` パラメータがオンになっている | AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter<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 |
|---|---|---|
| lN7RR0l7J9<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。 |
| kM7QQ0l7J9<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 |
| --- | --- | --- |
| | ストされます。デフォルトでは、制限は 3 つ増加します。 | 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。 |
| jL7PP0l7J9<br><br>VPC | AWSManagedServices-IncreaseServiceQuota<br><br>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。 |
| fW7HH0l7J9<br><br>Auto Scaling グループ | AWSManagedServices-IncreaseServiceQuota<br><br>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。 |
| 3Njm0DJQO9<br><br>RDS オプショングループ | AWSManagedServices-IncreaseServiceQuota<br><br>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。 |
| EM8b3yLRTr<br><br>ELB Application Load Balancer | AWSManagedServices-IncreaseServiceQuota<br><br>ELB Application 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。 |

| 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 |
| --- | --- | --- |
| 8wlqYSt25K<br><br>ELB Network Load Balancer | AWSManagedServices-IncreaseServiceQuota<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。 |

## 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 |
| --- | --- | --- |
| c18d2gz125<br><br>Amazon API Gateway が実行ログを記録しない | AWSManagedServices-TrustedRemediatorEnableAPIGateWayExecutionLogging<br><br>API ステージで実行ログ記録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>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、「API Gateway で REST API の CloudWatch ログ記録を設定する APIs」を参照してください。 |
| c18d2gz168<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 |
| --- | --- | --- |
| c1qf5bt012<br><br>Amazon RDS Performance Insights は無効になっています | AWSManagedServices-TrustedRemediatorEnableRDSPerformanceInsights<br><br>Amazon RDS で Performance Insights が有効になっています。 | • 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。<br>• 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。<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 |
| --- | --- | --- |
| c1fd6b96l4<br><br>Amazon S3 アクセスログが有効 | AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV2<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。 | • 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。<br>• 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。 |

| 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 |
| --- | --- | --- |
| | | 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。<br><br>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、「Amazon S3 サーバーアクセスログを有効にします」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

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 に保存されます。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、「チェックカテゴリを表示する」を参照してください。

修復は、リソースベースまたは Trusted Advisor チェックベースで設定できます。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、今後これが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。 AWS Systems Manager OpsCenter コンソールの OpsItem から SSM ドキュメントを確認して手動で実行します。
  - 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 を参照して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。
  - 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、 のチェックにはQch7DwouX1、AWSManagedServices-StopEC2InstanceAWSManagedServices-ResizeInstanceByOneLevel、および 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、自動的に修正するチェックのリソースタグ (1 つ以上のタグペア、カンマ区切り) を指定します。
- 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、デフォルト設定および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. 次のキーと値を使用して、リソースにタグを追加します。

    - 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。OpsItem から修復を手動で確認して実行します。
  - 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。

## 実行モードの決定ワークフロー

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. https://console.aws.amazon.com/systems-manager/appconfig で AWS AppConfig コンソールを開きます。

   委任管理者アカウントとしてサインインしていることを確認してください。
2. 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。
3. コスト最適化設定プロファイルを選択します。

4. 使用率の低い Amazon EBS ボリュームフラグを選択します。
5. 実行モードの場合は、手動 を選択します。
6. automated-for-tagged-only属性とmanual-for-tagged-only属性が空白であることを確認します。これらの属性は、一致するタグを持つリソースのデフォルトの実行モードを上書きするために使用されます。

   以下は、automated-for-tagged-onlyおよび manual-for-tagged-only と Manual for execution-mode の値が空白の属性セクションの例です。

7. 保存を選択して値を更新し、新しいバージョンを保存を選択して変更を適用します。変更を認識するには、信頼できる修復のために新しいバージョンを保存を選択する必要があります。
8. Amazon EBS ボリュームに キーを含むタグがないことを確認しますTR-DAvU99Dc4C-Execution-Mode。このタグキーは、その EBS ボリュームのデフォルトの実行モードを上書きします。

## 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. https://console.aws.amazon.com/systems-manager/appconfig で AWS AppConfig コンソールを開きます。

   委任管理者アカウントとしてサインインしていることを確認してください。
2. アプリケーションのリストから Trusted Remediator を選択します。
3. コスト最適化設定プロファイルを選択します。
4. 使用率の低い Amazon EBS ボリュームフラグを選択します。
5. 実行モードの場合は、自動 を選択します。
6. automated-for-tagged-only属性とmanual-for-tagged-only属性が空白であることを確認します。これらの属性は、一致するタグを持つリソースのデフォルトの実行モードを上書きするために使用されます。

以下は、automated-for-tagged-onlyとmanual-for-tagged-onlyタグ付け専用と自動実行モードの値が空白の属性セクションの例です。

7. 保存を選択して値を更新し、新しいバージョンを保存を選択して変更を適用します。変更を認識するには、信頼できる修復のために新しいバージョンを保存を選択する必要があります。

   この時点で、すべての Amazon EBS ボリュームは自動修復用に設定されます。

8. 選択した Amazon EBS ボリュームの自動修復を上書きします。

   a. Amazon EC2 コンソールの https://console.aws.amazon.com/ec2/ を開いてください。
   b. Elastic Block Store、ボリュームを選択します。
   c. [タグ] を選択します。
   d. [Manage tags (タグの管理)] を選択します。
   e. 次のタグを追加します。

      - キー： TR-DAvU99Dc4C-Execution-Mode
      - 値： 非アクティブ

      以下は、キーフィールドと値フィールドを示すタグセクションの例です。

   f. 修復から除外するすべての Amazon EBS ボリュームについて、ステップ 2～5 を繰り返します。

## 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. https://console.aws.amazon.com/systems-manager/appconfig で AWS AppConfig コンソールを開きます。

   委任管理者アカウントとしてサインインしていることを確認してください。

2. 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。
3. コスト最適化設定プロファイルを選択します。
4. 使用率の低い Amazon EBS ボリュームフラグを選択します。
5. execution-mode で、Conditional を選択します。
6. automated-for-tagged-onlyを に設定しますStage=NonProd。この属性は、一致するタグを持つリソースexecution-modeのデフォルトを上書きします。manual-for-tagged-only属性が空白であることを確認します。

   以下は、automated-for-tagged-onlyが Stage=NonProd に設定され、実行モードの条件付きである属性セクションの例です。

7. 必要に応じて、事前設定済みパラメータを次のいずれかに設定します。

   - CreateSnapshot=false 削除前に Amazon EBS ボリュームのスナップショットを作成しないようにするには
   - MinimumUnattachedDays=10 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を 10 日間に設定するには
   - CreateSnapshot=false上記の両方MinimumUnattachedDays=10について、
8. 保存を選択して値を更新し、新しいバージョンを保存を選択して変更を適用します。変更を認識するには、信頼できる修復のために新しいバージョンを保存を選択する必要があります。
9. Amazon EBS ボリュームに キーを含むタグがないことを確認しますTR-DAvU99Dc4C-Execution-Mode。このタグキーは、その EBS ボリュームのデフォルトの実行モードを上書きします。

# Trusted Remediator で修復を操作する

## 信頼できる修復ツールで修復を追跡する

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 を手動で修復するには、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。
6. OpsItem を手動で修復するには、次の手順を実行します。
   a. ランブックから、関連するランブック (SSM ドキュメント) のいずれかを選択します。
   b. [実行] を選択してください。

c. AutomationAssumeRole で、 を選択します `arn:aws:iam::AWS ##### ID:role/ams_ssm_automation_role`。 AWS アカウント ID を修復を実行するアカウント ID に置き換えます。その他のパラメータ値については、「オペレーションデータ」を参照してください。

リソースを手動で修復するには、 への認証に使用されるロールまたはユーザーに、IAM ロール の`iam:PassRole`アクセス許可 AWS アカウント が必要です`ams-ssm-automation-role`。詳細については、「 にロールを渡すアクセス許可をユーザーに付与する AWS のサービス」または「Cloud Architect」を参照してください。

d. [実行] を選択してください。

e. Latest status and results 列で SSM ドキュメントの実行の進行状況をモニタリングします。

f. ドキュメントが完了したら、Set Status, Resolved を選択して OpsItem を手動で解決します。ドキュメントが失敗した場合は、詳細を確認して SSMdocumentを再実行します。トラブルシューティングのサポートを追加するには、サービスリクエストを作成します。

修復せずに OpsItem を解決するには、「ステータスを解決済みに設定」を選択します。

7. 残りのすべての手動修復 OpsItems について、ステップ 3 と 4 を繰り返します。

## 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. 次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 にお問い合わせください。

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、SSM ドキュメントを手動で再度実行します。
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. Failed 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。この問題が再発しないようにするには、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。QuickSight にログファイルをインポートして、カスタマイズされた修復レポートを生成できます。

詳細については、「信頼できる修復ツールと QuickSight の統合」を参照してください。

### 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`*`-`*`Trusted Advisor 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

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
}
```

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"
}
```

## 自動修復実行ログ、Compute Optimizer、 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

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

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"}
```

## メンバーアカウントログ

Trusted Remediator は、アカウントのオンボーディング時またはオフボードMember accounts log時に を作成します。を使用して、各メンバーアカウントのアカウント ID、オンボーディングされた AWS リージョン、および実行時間Member accounts logを検索できます。

メンバーアカウントのログの場所

s3://ams-trusted-remediator-*delegated-administrator-account-id*-logs/configuration_logs/member_accounts.json

メンバーアカウントのログファイル URL

s3://ams-trusted-remediator-*111122223333*-logs/configuration_logs/member_accounts.json

メンバーアカウントのログ形式

```
{
    "delegated_administrator_account_id": Delegated Administrator account id,
    "appconfig_configuration_region": Trusted Remediator AppConfig Region,
    "member_accounts": [
        {
            "account_id": Member account id
            "account_partition": Member account partition (for example, aws),
            "regions": [
                {
                    "execution_time": Remediation execution time in cron schedule
 expression,
```

```
                    "execution_timezone": Timezone for the remediation execution time,
                    "region_name": AWS ##### name
                }
                ...
            ]
        }
        ...
    ],
    "updated_at": Log update time,
}
```

メンバーアカウントのログ形式のサンプルコンテンツ

```
{
    "delegated_administrator_account_id": "111122223333",
    "appconfig_configuration_region": "ap-southeast-2",
    "member_accounts": [
        {
            "account_id": "222233334444",
            "account_partition": "aws",
            "regions": [
                {
                    "execution_time": "0 9 * * 6",
                    "execution_timezone": "Australia/Sydney",
                    "region_name": "ap-southeast-2"
                },
                {
                    "execution_time": "0 5 * * 7",
                    "execution_timezone": "UTC",
                    "region_name": "us-east-1"
                }
            ]
        },
        {
            "account_id": "333344445555",
            "account_partition": "aws",
            "regions": [
                {
                    "execution_time": "0 1 * * 5",
                    "execution_timezone": "Asia/Seoul",
                    "region_name": "ap-northeast-2"
                }
            ]
```

```
        }
    ],
    "updated_at": "1730869607"
}
```

## 信頼できる修復ツールと QuickSight の統合

Amazon S3 に保存されている信頼された修復ログを QuickSight と統合して、カスタマイズされた修復レポートを構築できます。 QuickSight QuickSight の統合はオプションです。この機能を使用すると、 ログを使用してカスタムレポートダッシュボードを構築できます。Trusted Remediator のオンリクエストレポートを取得するには、CSDM にお問い合わせください。利用可能な信頼された修復レポートの詳細については、「」を参照してください信頼できる修復レポート。

QuickSight でのデータの視覚化の詳細については、QuickSight でのデータの視覚化」を参照してください。

### 修復項目ログのデータセットを QuickSight に追加する

修復項目ログの QuickSight にデータセットを追加するには、次の手順に従います。

1. QuickSight コンソールにログインします。QuickSight レポートは、QuickSight がサポート AWS リージョン するQuickSightで作成できます。ただし、パフォーマンスを向上させ、コストを削減するには、信頼された修復者のログ記録バケットがあるリージョンにレポートを作成するのがベストプラクティスです。
2. [データセット] を選択します。
3. [S3] を選択します。
4. 新しい S3 データソースで、次の値を入力します。

    - データソース名： `trusted-remediator-`*`delegated_administrator_account_id`*`-`*`account_region`*`-remediation-items`。
    - マニフェストファイルをアップロードする： 次の内容の JSON ファイルを作成し、使用します。ファイルを作成するときは、URIPrefixes キー`logging_bucket_name`で を置き換えます。

    ```
    {
        "fileLocations": [
            {
                "URIPrefixes": [
    ```

```
                "s3://{logging_bucket_name}/remediation_items/"
            ]
        }
    ],
    "globalUploadSettings": {
        "format": "JSON",
        "delimiter": ",",
        "textqualifier": "'",
        "containsHeader": "true"
    }
}
```

- [接続] を選択します。
- データセット作成の完了ウィンドウから、視覚化を選択します。
- QuickSight は新しい分析シートページを開きます。これで、修復項目ログを使用して新しい分析を作成する準備ができました。

以下はサンプル分析です。

## 自動修復実行ログのデータセットを QuickSight に追加する

1. QuickSight コンソールにログインします。QuickSight レポートは、QuickSight がサポート AWS リージョン するQuickSightで作成できます。ただし、パフォーマンスを向上させ、コストを削減するには、信頼された修復者のログ記録バケットがあるリージョンにレポートを作成するのがベストプラクティスです。
2. [データセット] を選択します。
3. [S3] を選択します。
4. 新しい S3 データソースで、次の値を入力します。

   - データソース名: `trusted-remediator-`*`delegated_administrator_account_id`*`-`*`account_region`*`-remediation-executions`。
   - マニフェストファイルをアップロードする : 次の内容の JSON ファイルを作成し、このファイルを使用します。ファイルを作成するときは、URIPrefixes キー`logging_bucket_name`で を置き換えます。

```
{
```

```
    "fileLocations": [
        {
            "URIPrefixes": [
                "s3://{logging_bucket_name}/remediation_executions/"
            ]
        }
    ],
    "globalUploadSettings": {
        "format": "JSON",
        "delimiter": ",",
        "textqualifier": "'",
        "containsHeader": "true"
    }
}
```

- [接続] を選択します。
- データセット作成の完了ウィンドウから、視覚化を選択します。
- QuickSight は新しい分析シートページを開きます。これで、修復項目ログを使用して新しい分析を作成する準備ができました。

以下はサンプル分析です。

## 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、信頼できる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、どのような利点がありますか？

コンプライアンス違反が Compute Optimizer によって特定された場合、 Trusted Advisor またはレコメンデーションが Compute Optimizer によって発行された場合、Trusted Remediator は、修正の適用、手動修復による承認の依頼、または今後の月次ビジネスレビュー (MBR) 中に修正を報告することで、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 チェックと Compute Optimizer の推奨事項にアクセスできます。Trusted Remediator は、 および Compute Optimizer と Trusted Advisor 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、QuickSight 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？

アカウントの設定はユーザーが所有します。設定の管理はお客様の責任となります。設定の管理については、CA または CDSM にお問い合わせください。設定サポート、手動修復、および修復失敗のトラブルシューティングのサービスリクエストを通じて AMS に連絡することもできます。

SSM オートメーショ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 オートメーションドキュメントは、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 Accelerate 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 オートメーションドキュメントは 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 Trusted Remediator 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？

信頼できる修復は、 AWS AppConfig アプリケーションから無効にできます。信頼できる修復を一時停止または停止するには、次の手順を実行します。

1. https://console.aws.amazon.com/systems-manager/appconfig で AWS AppConfig コンソールを開きます。
2. Trusted Remediator を選択します。
3. 設定プロファイルの設定を選択します。
4. Suspend Trusted Remediator フラグを選択します。
5. `suspended` 属性の値を `true` に設定します。

> **Note**
>
> この手順を使用すると、委任管理者アカウントにリンクされたすべてのアカウントの信頼された修復が停止されるため、注意が必要です。

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 と AWS Config 修復はどのように異なりますか？

AWS Config 修復は、クラウドリソースを最適化し、ベストプラクティスへの準拠を維持するのに役立つもう 1 つのソリューションです。以下は、2 つのソリューション間の運用上の違いの一部です。

- Trusted Remediator は検出メカニズムとして Trusted Advisor と Compute Optimizer を使用します。 AWS Config Remediation は検出メカニズムとして AWS Config ルールを使用します。

- Trusted Remediator の場合、修復は事前定義された修復スケジュールで行われます。では AWS Config、修復はリアルタイムで行われます。
- Trusted Remediator の各修復のパラメータは、ユースケースに基づいて簡単にカスタマイズでき、リソースにタグを追加することで修復を自動化または手動で行うことができます。
- Trusted Remediator はレポート機能を提供します。
- Trusted Remediator は、修復のリストと修復ステータスが記載された E メール通知を送信します。

一部の Trusted Advisor チェックと Compute Optimizer レコメンデーションには、同じルールが含まれている場合があります AWS Config。一致する AWS Config ルールと Trusted Advisor チェックがある場合は、1 つの修復のみを有効にすることをお勧めします。各 Trusted Advisor チェックの AWS Config ルールについては、「」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。

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 委任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 形式でを作成し、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 チェックと Compute Optimizer の推奨事項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。

# AMS Accelerate での Amazon EKS のモニタリングとインシデント管理

Amazon EKS のモニタリングとインシデント管理は、Amazon EKS 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 Accelerate は、Amazon Managed Service for Prometheus アラートマネージャールールを設定およびデプロイし、アラートをモニタリングしてから、これらのアラートがトリガーされたときにインシデント管理を実行します。Amazon EKS のモニタリングとインシデント管理は AMS Alarm Manager に依存し、Amazon Managed Service for Prometheus、Amazon Managed Grafana、Amazon GuardDuty、AWS Lambda、 などのネイティブ AWS サービスを活用しますAWS Config。

> **Note**
>
> Amazon EKS のモニタリングとインシデント管理は AWS GovCloud (US)、、Windows ノード、または Windows コンテナをサポートしていません。

## AMS Accelerate での Amazon EKS のモニタリングとインシデント管理とは

Amazon EKS のモニタリングとインシデント管理には、次の機能があります。

- 選択した Amazon EKS クラスターのマネージドアカウント全体でモニターとポリシーを作成、管理、デプロイするデフォルト設定。
- Amazon EKS クラスターに他のモニタリングを設定していない場合でも、Amazon EKS ワークロードの可用性を向上させるためのモニタリングベースライン。詳細については、「AMS Accelerate での Amazon EKS のモニタリングとインシデント管理のベースラインアラート」を参照してください。
- Amazon EKS クラスター用に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る通知。これらの通知はアラートと呼ばれます。アラートは、差し迫った障害、進行中の障害、回復中の障害、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が発生した場合に生成されます。アラートの例としては、Prometheus アラート、イベント、Amazon GuardDuty などの AWS サービスからの検出結果などがあります。

- 実行できる適切な修復アクションに関するガイダンスとともに、調査をアラートします。詳細については、「AMS Accelerate でのインシデントレポートとサービスリクエスト」を参照してください。
- AMS オペレーションによるアラートとインシデントの修復は、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、可能な場合はお客様の承認を得て行います。詳細については、「AMS Accelerate でのインシデントレポートとサービスリクエスト」を参照してください。
- リソース使用率、パフォーマンス、CoreDNS の正常性、アクティブなアラート、以前に解決されたアラートを可視化するオプションの定義済み Amazon Managed Grafana ダッシュボード。AMS が提供するテンプレートを使用して Amazon Managed Grafana を設定する場合は、Amazon Managed Grafana コンソールを開いて、Amazon EKS クラスターのメトリクスとアラートを表示できます。

# AMS Accelerate での Amazon EKS のモニタリングとインシデント管理の仕組み

生成： EKS のオンボーディングモニタリングとインシデント管理の一環として、AMS はマネージドアカウントで選択した Amazon EKS クラスターのベースラインモニタリングを設定します。AMS は、Amazon Managed Service for Prometheus アラートマネージャールールと Amazon CloudWatch イベントルールを組み合わせて、ベースラインモニタリングを設定します。クラスター内の AMS 設定の Prometheus サーバーは、Prometheus メトリクスをスクレイプし、同じリージョン内の Amazon Managed Service for Prometheus エンドポイントにリモート書き込みます。ベースラインモニタリング設定は、Prometheus アラートマネージャールールがトリガーされるか、CloudWatch イベントが生成されるとアラートを生成します。

集約： AMS は、リソースが生成するすべてのアラートを AMS によって管理される Amazon Simple Notification Service トピックに送信することで、AMS モニタリングシステムに送信します。

処理と影響の分析： 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。AMS はアラートを次のように分類します。

- 既知の顧客への影響があるアラート： これらのアラートの場合、AMS はインシデント管理プロセスを使用して新しいインシデントレポートを作成します。
- 顧客への影響が不明なアラート： これらのアラートの場合、AMS はインシデントレポートを送信します。多くの場合、これらのアラートでは、AMS がアクションを実行する前に影響を確認するように求められます。このようなアラートの場合、AMS は詳細を含むアラート通知を送信し、アラートに緩和アクションが必要かどうかを確認します。AMS には、通知内のアクションを軽減す

るためのオプションが用意されています。返信でアラートがインシデントであることを確認した場合、AMS は新しいインシデントレポートの作成をトリガーし、インシデント管理プロセスを開始します。「顧客への影響なし」または 3 日間応答をまったく受信しないサービス通知は、解決済みとしてマークされます。また、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、アラートは閉じられます。

## AMS 責任マトリックス (RACI)

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。次の表は、Amazon EKS のモニタリングとインシデント管理を使用するアプリケーション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。

- 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。
- は、説明責任を負う当事者を表します。
- 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。
- 多くの場合、タスクまたは成果物の完了時にのみ、進行状況が通知される当事者である、情報に基づく当事者です。

| アクティビティ | お客様 | AMS |
|---|---|---|
| Discovery for AMS の要件 | I | R |
| クラスターアクセスの AMS アクセス許可 (RBAC) を有効にする | R | C |
| ワーカーノードに Amazon EC2 Systems Manager Agent がまだ存在しない場合はインストールする | R | C |
| 必要に応じて、Prometheus、Prometheus Node Exporter、 | C | R |

| アクティビティ | お客様 | AMS |
| --- | --- | --- |
| kube-state-metrics などのクラスター上の AMS コンポーネントを AMS 名前空間にデプロイします。 | | |
| AMS コントロールプレーンで Amazon Managed Service for Prometheus をプロビジョニングする | I | R |
| AMS コントロールプレーンで Prometheus アラートマネージャーを設定する | I | R |
| Amazon Managed Grafana テンプレートを提供し、設定を支援する | C | R |
| GuardDuty EKS 監査ログのモニタリングを有効にする | C | R |
| Amazon EKS コントロールプレーンのログ記録を有効にする | I | R |
| Amazon EKS コントロールプレーンの状態とパフォーマンスをモニタリングする | I | R |
| Amazon EKS クラスター (クラスター、ノード、ワークロード、ポッド、API Server、CoreDNS) の状態とパフォーマンスをモニタリングする | I | R |

| アクティビティ | お客様 | AMS |
| --- | --- | --- |
| アラートをトリアージし、Amazon EKS のインシデント対応を提供する | I | R |
| インシデント中に診断コマンドを実行する | I | R |
| インシデント中のログを分析する (コントロールプレーンとポッドログ ) | I | R |
| AWS ネットワーク問題のインシデント対応 | I | R |
| GuardDuty EKS 監査ログのモニタリング結果への対応 | I | R |
| 可能であれば、インシデントを修正するためのアクションについて顧客ガイダンスを提供する | I | R |

# AMS Accelerate での Amazon EKS のモニタリングとインシデント管理のベースラインアラート

アラートを確認した後、AMS は Amazon EKS に対して次のアラートを有効にし、選択した Amazon EKS クラスターのモニタリングとインシデント管理を行います。応答時間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) は、選択したアカウントサービス階層 (Plus、Premium) によって異なります。詳細については、「AMS Accelerate でのインシデントレポートとサービスリクエスト」を参照してください。

## アラートとアクション

次の表に、Amazon EKS アラートと、AMS が実行する各アクションを示します。

| アラート | しきい値 | アクション |
| --- | --- | --- |
| コンテナ OOM が強制終了されました | 過去 10 分以内にコンテナを再起動した合計数は 1 回以上で、ポッド内の Kubernetes コンテナは過去 10 分以内に OOMKilled」という理由で終了しています。 | AMS は、OOM の強制終了の原因がコンテナ制限またはメモリ制限のオーバーコミットに達したかどうかを調査し、是正措置についてアドバイスします。 |
| ポッドジョブ失敗 | Kubernetes ジョブの完了に失敗します。失敗は、少なくとも 1 つの失敗したジョブステータスの存在によって示されます。 | AMS は、Kubernetes ジョブまたは対応する cron ジョブが失敗した理由を調査し、是正措置についてアドバイスします。 |
| StatefulSetダウン | トラフィックを処理する準備ができているレプリカの数が、少なくとも 1 分間、StatefulSetあたりの既存のレプリカの現在の数と一致しません。 | AMS は、ポッドイベントのエラーメッセージとポッドログのエラーログスニペットを確認することで、ポッドの準備が整っていない理由を判断し、是正措置についてアドバイスします。 |
| HPA スケーリング機能 | ステータス条件AbleToScale」が少なくとも 2 分間 false であるため、Horizontal Pod Autoscaler (HPA) はスケーリングできません。 | AMS は、デプロイやStatefulSetなど、後続のワークロードリソースのポッドをスケーリングできない Kubernetes Horizontal Pod Autoscaler (HPA) を決定します。 |
| HPA メトリクスの可用性 | Horizontal Pod Autoscaler (HPA) は、ステータス条件ScalingActive」が少なくとも 2 分間 false であるため、メトリクスを収集できません。 | AMS は、サーバー設定の問題や RBAC 認可の問題に関連するメトリクスなど、HPA がメトリクスを収集できない理由を決定します。 |

| アラート | しきい値 | アクション |
| --- | --- | --- |
| ポッドの準備中 | Kubernetes ポッドは、15 分以上実行されていない状態 (保留中、不明、失敗など) のままになります。 | AMS は、影響を受けるポッド (複数可) の詳細を調査し、ポッドログに関連するエラーやイベントを確認し、是正措置についてアドバイスします。 |
| ポッドクラッシュループ | ポッドコンテナは、少なくとも 15 分ごとに 1 時間再起動します。 | AMS は、リソースの不足、別のコンテナによってロックされたファイル、別のコンテナによってロックされたデータベース、サービスの依存関係の失敗、外部サービスの DNS 問題、設定ミスなど、ポッドが起動しない理由を調査します。 |
| デーモンセットのスケジュールミス | 10 分間に 1 つ以上の Kubernetes Daemonset ポッドが誤ってスケジュールされています。 | AMS は、実行すべきではないノードでデーモンセットがスケジュールされている理由を決定します。これは、間違ったポッドnodeSelector/taints/affinitiesがデーモンセットポッドに適用された場合、またはノード (ノードプール) がテイントされ、既存のポッドが工ビクション用にスケジュールされていない場合に発生する可能性があります。 |

| アラート | しきい値 | アクション |
| --- | --- | --- |
| Kubernetes API エラー | Kubernetes API サーバーのエラー率が 2 分間で 3% を超えています。 | AMS はコントロールプレーンログを分析して、このアラートの原因となっているエラーの量とタイプを判断し、マスターノードまたは etcd 自動スケーリンググループのリソース競合の問題を特定します。API サーバーが復旧しない場合、AMS は Amazon EKS サービスチームを関与させます。 |
| Kubernetes API レイテンシー | Kubernetes API サーバーへのリクエストの 99 パーセンタイルレイテンシーは、2 分間で 1 秒を超えています。 | AMS はコントロールプレーンログを分析して、レイテンシーの原因となっているエラーの量とタイプを判断し、マスターノードまたは etcd 自動スケーリンググループのリソース競合の問題を特定します。API サーバーが復旧しない場合、AMS は Amazon EKS サービスチームを関与させます。 |
| Kubernetes クライアント証明書の有効期限切れ | Kubernetes API サーバーへの認証に使用されるクライアント証明書は、24 時間以内に期限切れになります。 | AMS はこの通知を送信して、クラスター証明書が 24 時間後に期限切れになることを通知します。 |
| ノードが準備中 | Node の「準備完了」条件ステータスが少なくとも 10 分間 false です。 | AMS は、API サーバーへの kubelet アクセスを妨げるネットワークの問題などのノード条件とイベントを調査します。 |

| アラート | しきい値 | アクション |
| --- | --- | --- |
| ノード高 CPU | CPU 負荷が 5 分間で 80% を超えています。 | AMS は、1 つ以上のポッドが異常に大量の CPU を消費しているかどうかを決定します。次に、AMS はリクエスト、制限、ポッドアクティビティが想定どおりであることを確認します。 |
| ノード OOM の強制終了が検出されました | 4 分間にノードによって少なくとも 1 つのホスト OOM 強制終了が報告されています。 | AMS は、OOM の強制終了の原因がコンテナの制限に達したか、ノードのオーバーコミットであるかを判断します。アプリケーションアクティビティが正常である場合、AMS はオーバーコミットとポッド制限の改訂のリクエストと制限についてアドバイスします。 |
| ノード Conntrack の制限 | 接続追跡エントリの現在の数と最大制限の比率が 5 分間で 80% を超えています。 | AMS は、コアあたりの推奨 conntrack 値についてアドバイスします。Kubernetes ノードは、ノードの合計メモリ容量に比例して conntrack 最大値を設定します。高負荷アプリケーション、特に小さなノードでは、conntrack の最大値を簡単に超えるため、接続のリセットとタイムアウトが発生する可能性があります。 |
| ノードクロックが同期されていません | 2 分間の最小同期ステータスは 0 で、秒単位の最大エラーは 16 以上です。 | AMS は、Network Time Protocol (NTP) がインストールされ、正常に機能しているかどうかを判断します。 |

| アラート | しきい値 | アクション |
| --- | --- | --- |
| Pod 高 CPU | コンテナの CPU 使用率が 3 分間のレートで 80% を最低 2 分間超える。 | AMS はポッドログを調査して、大量の CPU を消費するポッドタスクを決定します。 |
| ポッドハイメモリ | コンテナのメモリ使用量が 2 分間で指定されたメモリ制限の 80% を超えています。 | AMS はポッドログを調査して、大量のメモリを消費するポッドタスクを決定します。 |
| CoreDNS ダウン | CoreDNS が Prometheus ターゲット検出から 15 分以上消えました。 | これは、内部または外部のクラスターサービスのドメイン名解決が停止したことを示す重要なアラートです。AMS は CoreDNS ポッドのステータスをチェックし、CoreDNS 設定を検証し、CoreDNS ポッドを CoreDNS エンドポイントを検証し、CoreDNS 制限を検証し、承認があれば CoreDNS デバッグログ記録を有効にします。 |
| CoreDNS エラー | CoreDNS は、10 分間に DNS リクエストの 3% 以上について SERVFAIL エラーを返します。 | このアラートは、アプリケーションの問題や設定ミスを示している可能性があります。AMS は CoreDNS ポッドのステータスをチェックし、CoreDNS 設定を検証し、CoreDNS ポッドをCoreDNS エンドポイントを検証し、CoreDNS 制限を検証し、承認があれば CoreDNS デバッグログ記録を有効にします。 |

| アラート | しきい値 | アクション |
| --- | --- | --- |
| CoreDNS レイテンシー | DNS リクエスト期間の 99 パーセンタイルが 10 分間 4 秒を超えています。 | このアラート CoreDNS が過負荷になっている可能性があることを示します。AMS は CoreDNS ポッドのステータスをチェックし、CoreDNS 設定を検証し、CoreDNS ポッドをポイントする DNS エンドポイントを検証し、CoreDNS 制限を検証し、お客様の承認により CoreDNS デバッグログ記録を有効にします。 |
| CoreDNS 転送レイテンシー | kube-dns への CoreDNS 転送リクエストの応答時間の 99 パーセンタイルが 10 分間で 4 秒を超えています。 | CoreDNS が権威サーバーでない場合、またはドマニン名のキャッシュエントリがない場合、CoreDNS は DNS リクエストをアップストリーム DNS サーバーに転送します。このアラートは、CoreDNS が過負荷になっているか、アップストリーム DNS サーバーに問題がある可能性があることを示します。AMS は CoreDNS ポッドのステータスをチェックし、CoreDNS 設定を検証し、CoreDNS ポッドをCoreDNS エンドポイントを検証し、CoreDNS 制限を検証し、お客様の承認により CoreDNS デバッグログ記録を有効にします。 |

| アラート | しきい値 | アクション |
| --- | --- | --- |
| CoreDNS 転送エラー | DNS クエリの 3% 以上が 5 分間失敗しています。 | CoreDNS が権威サーバーでない場合、またはドマニン名のキャッシュエントリがない場合、CoreDNS は DNS リクエストをアップストリーム DNS サーバーに転送します。このアラートは、設定ミスの可能性やアップストリーム DNS サーバーの問題を示します。AMS は CoreDNS ポッドのステータスをチェックし、CoreDNS 設定を検証し、CoreDNS ポッドをCoreDNS エンドポイントを検証し、CoreDNS 制限を検証し、お客様の承認により CoreDNS デバッグログ記録を有効にします。 |

# AMS Accelerate での Amazon EKS のモニタリングとインシデント管理の要件

これらは、Amazon EKS for AMS Accelerate のモニタリングとインシデント管理にサポートおよび/または必要なリソースです。

- サポートされている Kubernetes バージョン：「Amazon EKS ユーザーガイド」の「Amazon EKS Kubernetes バージョン」を参照してください。
- ノードタイプ： Amazon EKS マネージドノードがサポートされています。Windows ノードとコンテナはサポートされていません。
- Kubernetes クラスターアクセス： AMS には system:masters RBAC クラスターロールとクラスターユーザーが必要です。

- Amazon EC2 ノードの SSM エージェント： Bottle Rocket と Amazon EKS AMIsに SSM Agent がプリインストールされています。SSM Agent がカスタム AMIs と Amazon EC2 ノードにインストールされていることを確認します。
- Service Quotas 詳細については、Amazon Managed Service for Prometheus および Amazon Managed Grafana のサービスクォータを参照してください。
- サポートされている AWS リージョン：

| リージョン名 | リージョン | メトリクスストレージリージョン |
|---|---|---|
| 米国東部 ( オハイオ ) | us-east-2 | us-east-2 |
| 米国東部 (バージニア北部) | us-east-1 | us-east-1 |
| 米国西部 (オレゴン ) | us-west-2 | us-west-2 |
| アジアパシフィック (東京) | ap-northeast-1 | ap-northeast-1 |
| アジアパシフィック (ソウル) | ap-northeast-2 | ap-northeast-2 |
| アジアパシフィック (シンガポール) | ap-southeast-1 | ap-southeast-1 |
| アジアパシフィック (シドニー) | ap-southeast-2 | ap-southeast-2 |
| 欧州 (フランクフルト) | eu-central-1 | eu-central-1 |
| 欧州 (アイルランド) | eu-west-1 | eu-west-1 |
| 欧州 (ロンドン) | eu-west-2 | eu-west-2 |
| アフリカ (ケープタウン) | af-south-1 | eu-west-1<br>eu-west-2 |
| アジアパシフィック (香港) | ap-east-1 | ap-northeast-1<br>ap-northeast-2 |

> **Note**
>
> アフリカ (ケープタウン) の af-south-1 とアジアパシフィック (香港) の ap-east-1 の Amazon EKS クラスターのメトリクスは AWS リージョン、それぞれ同じ の AMS モニタリングサービスにエクスポートされます。これらのメトリクス AWS リージョン は、AMS モニタリングサービス内で処理および保存される異なるリージョンに転送されます。AMS モニタリングサービスがメトリクスの保存に使用するリージョンについては、前の表を参照してください。

# AMS Accelerate で Amazon EKS のモニタリングとインシデント管理にオンボードする

Amazon EKS のモニタリングとインシデント管理にオンボードするには、次の手順を実行します。

1. Amazon EKS コスト最適化タグを有効にする：「Amazon EKS ユーザーガイド」の「請求用のリソースのタグ付け」を参照してください。
2. EKS のモニタリングとインシデント管理のオンボーディングを開始する： オンボーディングするアカウント IDs とクラスター名を使用して Cloud Service Delivery Manager (CSDM) にお問い合わせください。
3. 要件の検証： Cloud Architect (CA) は、オンボーディングを開始する前にすべての要件が満たされていることを検証します。
4. Kubernetes ロールベースのアクセスコントロール (RBAC): AMS は、これらの変更を実装するための`eksctl`コマンドを共有します。これらの変更を確認してからデプロイできます。AMS がユーザーに代わってコマンドを実行するアクセス許可を持つように、RBAC 更新をデプロイする必要があります。これらの更新には、AMS IAM ロールの Kubernetes ユーザーへのマッピング、AMS 用の新しい Kubernetes クラスターロールの作成、AMS Kubernetes クラスターロールのユーザーへのバインドが含まれます。
5. クラスターコンポーネントのデプロイ： AMS は、クラスターの AMS マネージド名前空間に次のコンポーネントをデプロイします。
   - Prometheus サーバー
   - Prometheus ノードエクスポーター (該当なし AWS Fargate )
   - kube-state-metrics

6. Prometheus 設定の更新を実行する： AMS はメトリクスのリモート書き込みを有効にするように Prometheus を設定します。
7. （ オプション) ダッシュボードを設定する： CA は、アカウントで Amazon Managed Grafana ダッシュボードを設定するのに役立ちます。

> **Note**
>
> Amazon EKS クラスターがオンボーディングされると、AMS はアラートシグナルを分析し、ベースライン評価を実行してクラスター内の既存の問題を特定します。ベースライン評価が完了すると、AMS は Trusted Advisor とクラスター内の問題に対処するために使用できるサービスリクエストを通じて検出結果と修復の推奨事項を共有します。評価から、AMS はアカウントレベルのアラームしきい値を調整して、EKS クラスターに固有の Amazon EKS モニタリングベースラインを作成します。これらの結果に対する重複する AMS レスポンスを排除するために、これらのアラートシグナルを除外するようにモニタリングを調整します。CSDM から根本的な問題が修正されたことが通知されたら、シグナルを含めるようにモニタリングを再調整します。

# AMS Accelerate での Amazon EKS のモニタリングとインシデント管理からのオフボード

アカウント IDs とクラスター名を Cloud Service Delivery Manager (CSDM) に通知し、オフボーディングプロセスを開始します。オフボード後、アラート処理、メトリクスストレージ、メトリクスクエリは停止され、メトリクスはデフォルトの Amazon Managed Service for Prometheus データ保持ポリシーに従って削除されます。

AMS は、次のオフボーディングステップを実行します。

1. AMS は、ユーザーおよび AMS オペレーションに送信されるアラートを無効にします。
2. AMS は、Amazon EKS クラスターから Prometheus インスタンスを削除します。
3. AMS は、IAM ロールや AWS Config ルールなど、アカウントにインストールされている他の AWS リソースを削除します。

これらのステップが完了したら、以下のオフボーディングステップを完了する必要があります。

1. eksctl を使用して、 から Kubernetes RBAC aws-auth アクセス許可を削除しますConfigMap。
2. 以前にインストールした場合は、AMS に接続するように設定した Amazon Managed Grafana インスタンスを削除します。

# AMS Accelerate での継続的な管理

AMS は AWS Backup を活用して、 AWS サービス間のデータのバックアップを一元化および自動化します。AMS バックアッププランは、さまざまなユースケースのベストプラクティスを提供しますが、既存のバックアッププランを引き続き使用できます。AMS バックアップ管理にオンボードすると、AMS はバックアップレポートを提供し、AMS の専門家はバックアップタスクを継続的にモニタリングして、信頼性の高いバックアップソリューションがあることを確認します。

詳細については、AWS Backup「: How It Works and Supported AWS resources and third-party applications」を参照してください。

AMS Accelerate は、運用上の優秀性の実現に役立つさまざまな運用サービスを提供します AWS。24 時間 365 日体制のヘルプデスク、プロアクティブモニタリング、セキュリティ、パッチ適用、ログ記録、バックアップなど、いくつかの主要な運用機能 AWS クラウド を使用して、AMS がで全体的な運用上の優秀性を達成するのに役立つ方法をすばやく理解するには、「AMS リファレンスアーキテクチャ図」を参照してください。

詳細については、Carl の動画をご覧ください (9:29)

トピック

- AMS での継続性管理の仕組み
- AMS バックアッププランを選択する
- リソースにタグを付けて AMS バックアッププランを適用する
- AMS ボールトでバックアップを表示する
- AMS バックアップのモニタリングとレポート

## AMS での継続性管理の仕組み

AMS バックアッププランは、データのバックアップ頻度とバックアップの保持ポリシーを定義します。AMS バックアップボールトは、バックアップデータを整理します。リソースがバックアッププランに関連付けられると、互換性のあるリソースは段階的にバックアップされます。最初のバックアップはフルコピーで、それ以降のバックアップは増分変更をキャプチャします。選択したリソースと AMS バックアッププランに応じて、Point-in-time復元 (PITR) を使用すると、復旧時間を選択してリソースを巻き戻すことができます。AMS Backup Management の使用を開始するには、AMS バックアッププランを選択し、リソースにタグを付けます。

> **Note**
>
> 「Getting Started 1: Service Opt-in」の手順に従って AWS リージョン、各アカウント、およびリソースタイプで AWS Backup が有効になっていることを確認します。
> 開始方法 2: オンデマンドバックアップの作成に進む必要はありません。

からの関連トピック AWS Backup

- バックアップの操作 (作成、編集、コピー、復元、削除 )
- オンデマンドバックアップを作成する
- でのバックアップコピーの作成 AWS リージョン
- AWS Backup サポートされるサービス
- Point-in-time復元
- AWS Backup 特徴

# AMS バックアッププランを選択する

AMS は、オンボーディング中のコストを最小限に抑えるために、3 つの異なるバックアッププランと 4 番目のバックアッププランを提供します。サポートされているリソースごとに AMS バックアッププランを選択するには、そのリソースにプランに関連付けられたタグを付けます。Accelerate にオンボードすると、AMS はユーザーと協力して、ニーズに最適なバックアッププランを特定します。

> **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。詳細については、「バックアッププランの作成」を参照してください。

## デフォルトの AMS バックアッププラン

AWS Backup このバックアッププランでは継続的バックアップは有効になっていません。詳細については、point-in-time復元 (PITR) を使用した指定時刻への復元」を参照してください。

タグキー: `ams:rt:backup-orchestrator`

タグ値: `true`

| 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 4:00 UTC | 7 days |
| weekly backup | Saturday, 2:00 UTC | 4 weeks |
| monthly backup | 1st of the month, 2:00 UTC | 26 weeks |
| yearly backup | Jan 1st, 2:00 UTC | 2 years |

## 拡張バックアッププラン

AWS Backup 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 日間) で有効になります。詳細については、point-in-time復元 (PITR) を使用した指定時刻への復元」およびpoint-in-time復元 (PITR) でサポートされているサービスとアプリケーション」を参照してください。

タグキー: `ams:rt:backup-orchestrator-enhanced`

タグ値: `true`

| 拡張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 日間 |
| weekly backup | Saturday, 2:00 UTC | 6 週間 |
| monthly backup | 1st of the month, 2:00 UTC | 26 weeks |
| yearly backup | Jan 1st, 2:00 UTC | 2 years |

## データ機密性の高いバックアッププラン

AWS Backup 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。詳細については、point-in-time復元 (PITR) を使用した指定時刻への復元」およびpoint-in-time復元 (PITR) でサポートされているサービスとアプリケーション」を参照してください。

タグキー: `ams:rt:backup-orchestrator-data-sensitive`

タグ値: `true`

| データ機密性の高いバックアッププラン | 開始時刻 | Retention |
|---|---|---|
| hourly backup | every hour | 7 日間 |
| daily backup | daily 4:00 UTC | 31 日間 |
| weekly backup | Saturday, 2:00 UTC | 6 週間 |
| monthly backup | 1st of the month, 2:00 UTC | 26 weeks |
| yearly backup | Jan 1st, 2:00 UTC | 2 years |

## AMS Accelerate オンボーディングバックアッププラン

AWS Backup 継続的バックアップは、このバックアッププランでは有効になっていません。詳細については、point-in-time復元 (PITR) を使用した指定時刻への復元」を参照してください。

タグキー: `ams:rt:backup-orchestrator-onboarding`

タグ値: `true`

| AMS Accelerate オンボーディングバックアッププラン | 開始時刻 | Retention |
|---|---|---|
| hourly backup | every hour | 2 週間 |
| daily backup | N/A | N/A |
| weekly backup | N/A | N/A |

| AMS Accelerate オンボーディングバックアッププラン | 開始時刻 | Retention |
| --- | --- | --- |
| monthly backup | N/A | N/A |
| yearly backup | N/A | N/A |

関連 AWS Backup トピック

- バックアッププランの作成
- Point-in-time復元 (PITR) により、サポートされているリソースの継続的なバックアップが可能になり、復旧に特定の時間を選択できます。サポートされているリソースのリストについては、「リソース別の機能の可用性」を参照してください。

# リソースにタグを付けて AMS バックアッププランを適用する

リソースを AMS バックアッププランに割り当てるには、リソースにプランのタグキーと値のペアをタグ付けします。AMS Resource Tagger を使用して、リソースのサブセットまたはアカウントでサポートされているすべてのリソースに AMS バックアッププランを適用できます。別の方法を使用して AWS CloudFormation や Terraform などのリソースにタグを適用する場合は、選択したタグ付け方法と競合しないように Resource Tagger をオフにします。詳細については、「Resource Tagger によるリソースの変更の防止」を参照してください。

次の例は、Resource Tagger を使用して、アカウントの Amazon Elastic Compute Cloud インスタンスにデフォルトの AMS バックアッププランを適用する方法を示しています。このバックアッププランでは、タグキー `ams:rt:backup-orchestrator` と値 を適用しますtrue。別のバックアッププランを使用するには、目的のバックアッププランのタグキーと一致するようにキーを変更します。AMS Resource Tagger の詳細と、以下の参照プロファイルを Accelerate アカウントの現在の (既に設定されている) プロファイルと統合する方法については、「」を参照してくださいリソースタガーの高速化。

1. https://console.aws.amazon.com/systems-manager/appconfig で AWS AppConfig コンソールを開きます。
2. ResourceTagger アプリケーションを選択します。
3. 設定プロファイルタブを選択し、CustomerManagedTags を選択します。
4. Create を選択して新しいバージョンを作成します。

5. JSON を選択し、次の JSON オブジェクトをコピーして貼り付けます。

```
{
    "AWS::EC2::Instance": {
        "AccelerateBackupPlan": {
            "Enabled": true,
            "Filter": {
                "Fn::AND": [
                    {
                        "Platform": "*"
                    }
                ]
            },
            "Tags": [
                {
                    "Key": "ams:rt:backup-orchestrator",
                    "Value": "true"
                }
            ]
        }
    }
}
```

6. ホスト設定バージョンの作成 を選択します。
7. デプロイの開始 を選択します。
8. 次のデプロイの詳細を定義します。

```
Environment: AMSInfrastructure
Hosted configuration version: Select the version that you have just created.
Deployment Strategy: AMSNoBakeDeployment
```

9. デプロイの開始 を選択します。Resource Tagger はインスタンスにタグを付けams:rt:backup-orchestrator: true、インスタンスがデフォルトの AMS バックアッププランに従ってバックアップされるようにします。

# AMS ボールトでバックアップを表示する

タグを使用して、バックアップボールト通知を個々のボールトレベルで制御できます。タグを追加AMSNotificationOptOutし、特定のボールトTrueの値を に設定することで、特定のボールトの通知をオプトアウトできます。ボールト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、バックアップボールトを選択し、次の表から AMS バックアップボールトのいずれかを選択します。Backups セクションで、バックアップボールト内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 Backup Plans のボールト

| AMS ボールト名 | AMS Backup Plan タグキー |
| --- | --- |
| ams-automated-backups | ams:rt:backup-orchestrator |
| ams-automated-enhanced-backups | ams:rt:backup-orchestrator-enhanced |
| ams-automated-data-sensitive-backups | ams:rt:backup-orchestrator-data-sensitive |
| ams-onboarding-backups | ams:rt:backup-orchestrator-onboarding |

その他の AMS ボールト

| AMS ボールト名 | 説明 |
| --- | --- |
| ams-manual-backups | This vault contains manually started backups created by the `AWSManagedServices -StartBackupJob` SSM Automation document and pre-patch backups created by AMS patch automations before patching. |
| ams-custom-backups | This is the recommended vault for backups created outside of AMS backup plans. |

関連 AWS Backup トピック

- リソース別にバックアップを表示する
- バックアップの使用

# 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、毎日のセルフサービスレポートと、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。

# AMS Accelerate でのパッチ管理を理解する

**Important**

Accelerate Patch レポートは、 AWS Glue リソースベースのポリシーを定期的にデプロイします。パッチシステムへの AMS 更新は、既存の AWS Glue リソースベースのポリシーを上書きすることに注意してください。

**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

AMS Accelerate パッチシステムである Patch Add-On を使用して、セキュリティ関連の更新やその他のタイプの更新でインスタンスにパッチを適用できます。Accelerate Patch アドオンは、AMS インスタンスにタグベースのパッチを適用する機能です。 ( AWS Systems Manager SSM) 機能を利用すると、インスタンスにタグを付け、設定したベースラインとウィンドウを使用してそれらのインスタンスにパッチを適用できます。AMS Accelerate Patch アドオンはオンボーディングオプションです。 Accelerate アカウントのオンボーディング中に取得しなかった場合は、クラウドサービスデリバリーマネージャー (CSDM) に連絡して取得してください。

AMS Accelerate パッチ管理では、Systems Manager のパッチベースライン機能を使用して、インスタンスに適用されるパッチの定義を制御します。パッチベースラインには、すべてのセキュリティパッチなど、事前承認されたパッチのリストが含まれます。インスタンスのコンプライアンスは、インスタンスに関連付けられたパッチベースラインに対して測定されます。AMS Accelerate はデフォルトで、インスタンスを最新の状態に保つために使用可能なすべてのパッチをインストールします。

> **Note**
>
> AMS Accelerate はオペレーティングシステム (OS) パッチのみを適用します。たとえば、Windows の場合、Windows 更新プログラムのみが適用され、Microsoft 更新プログラムは適用されません。

レポートの詳細については、「」を参照してくださいAMS ホスト管理レポート。

AMS Accelerate は、運用上の優秀性の実現に役立つさまざまな運用サービスを提供しますAWS。24 時間 365 日体制のヘルプデスク、プロアクティブモニタリング、セキュリティ、パッチ適用、ログ記録、バックアップなど、いくつかの主要な運用機能 AWS クラウド を使用して、AMS がで全体的な運用上の優秀性を達成するのに役立つ方法をすばやく理解するには、「AMS リファレンスアーキテクチャ図」を参照してください。

トピック

- パッチ適用に関する推奨事項
- AMS でパッチメンテナンスウィンドウを作成する
- フックを使用したパッチ
- AMS Accelerate パッチベースライン
- AMS Accelerate のオンデマンドパッチ適用用の IAM ロールの作成
- AMS Accelerate のパッチ通知とパッチ障害を理解する

# パッチ適用に関する推奨事項

アプリケーションやインフラストラクチャの運用に携わっている方なら、アプリケーションチームからの多様な要件に対応できる柔軟性と拡張性を備えたオペレーティングシステム (OS) パッチソリューションの重要性を理解していることでしょう。一般的な組織では、不変インスタンスを含むアーキテクチャを使用するアプリケーションチームもあれば、可変インスタンスにアプリケーションをデプロイするアプリケーションチームもあります。

パッチ適用に関する AWS 規範ガイダンスの詳細については、「 を使用したハイブリッドクラウドのミュータブルインスタンスの自動パッチ適用 AWS Systems Manager」を参照してください。

> **Note**
>
> Accelerate Patch アドオンは、AMS インスタンスにタグベースのパッチを適用する機能です。( AWS Systems Manager SSM) 機能を利用すると、インスタンスにタグを付け、設定したベースラインとウィンドウを使用してそれらのインスタンスにパッチを適用できます。AMS Accelerate Patch アドオンはオンボーディングオプションです。 Accelerate アカウントのオンボーディング中に取得しなかった場合は、クラウドサービスデリバリーマネージャー (CSDM) に連絡して取得してください。

## パッチ責任に関する推奨事項

永続インスタンスのパッチ適用プロセスには、次のチームとアクションが必要です。

- アプリケーション (DevOps) チームは、アプリケーション環境、OS タイプ、またはその他の基準に基づいてサーバーのパッチグループを定義します。また、各パッチグループ固有のメンテナンスウィンドウも定義します。この情報は、インスタンスにアタッチされたタグに保存する必要があります。推奨されるタグ名は「パッチグループ」と「メンテナンスウィンドウ」です。各パッチサイクル中、アプリケーションチームはパッチ適用の準備、パッチ適用後のアプリケーションのテスト、パッチ適用中のアプリケーションと OS の問題のトラブルシューティングを行います。
- セキュリティオペレーションチームは、アプリケーションチームが使用するさまざまな OS タイプのパッチベースラインを定義し、Systems Manager Patch Manager を通じてパッチを利用できるようにします。
- 自動パッチソリューションは定期的に実行され、ユーザー定義のパッチグループとメンテナンスウィンドウに基づいて、パッチベースラインで定義されたパッチをデプロイします。
- ガバナンスチームとコンプライアンスチームは、パッチ適用ガイドラインと例外プロセスとメカニズムを定義します。

詳細については、「ミュータブル EC2 インスタンスのパッチソリューション設計」を参照してください。

## アプリケーションチーム向けガイダンス

- メンテナンスウィンドウの作成と管理を確認し、理解してください。詳細については、AWS Systems Manager 「メンテナンスウィンドウ」と「パッチ適用用の SSM メンテナンスウィンドウの作成」を参照してください。メンテナンスウィンドウの一般的な構造と使用方法を理解する

と、メンテナンスウィンドウを作成しているユーザーでない場合に提供する情報を理解するのに役立ちます。

- 高可用性 (HA) セットアップの場合、アベイラビリティーゾーンと環境 (Dev/Test/Prod) ごとに 1 つのメンテナンスウィンドウを計画します。これにより、パッチ適用中の可用性が維持されます。
- 推奨されるメンテナンスウィンドウ期間は 4 時間で、カットオフは 1 時間、さらにインスタンス 50 個あたり 1 時間です。
- 開発バージョンとテストバージョンに、本番稼働用パッチ適用の前に潜在的な問題を特定できるように、各バージョンの間に十分な時間をかけてパッチを適用します。
- SSM オートメーションを使用してパッチ適用前後の一般的なタスクを自動化し、メンテナンスウィンドウタスクとして実行します。パッチ後のタスクでは、カットオフに達するとタスクは起動しないため、十分な時間が割り当てられていることを確認する必要があります。
- パッチベースラインとその機能、特に、開発/テストで適用されたパッチのみが後日本番環境で適用されるようにするために使用できるパッチ重要度タイプの自動承認の遅延について知識を深めてください。詳細については、「パッチベースラインについて」を参照してください。

## セキュリティ運用チーム向けのガイダンス

- パッチベースラインを確認し、理解します。パッチの承認は自動化された方法で処理され、さまざまなルールオプションがあります。詳細については、「パッチベースラインについて」を参照してください。
- Dev/Test/Prod へのパッチ適用に関するニーズをアプリケーションチームと話し合い、これらのニーズに合わせて複数のベースラインを作成します。

## ガバナンスチームとコンプライアンスチームのガイダンス

- パッチ適用は「オプトアウト」関数である必要があります。パッチが適用されないように、デフォルトのメンテナンスウィンドウと自動タグ付けが存在する必要があります。AMS Resource Tagger はこれに役立ちます。このオプションについては、クラウドアーキテクト (CA) またはクラウドサービスデリバリーマネージャー (CSDM) と話し合い、実装に関するガイダンスを得てください。
- パッチ適用の免除をリクエストするには、免除を正当化するドキュメントが必要です。最高情報セキュリティ責任者 (CISO) またはその他の承認責任者は、リクエストを承認または拒否する必要があります。

- パッチコンプライアンスは、Patch Manager コンソール、Security Hub、または脆弱性スキャナーを介して定期的に確認する必要があります。

## 高可用性 Windows アプリケーションの設計例

概要：

- AZ ごとに 1 つのメンテナンスウィンドウ。
- 環境ごとに 1 セットのメンテナンスウィンドウ。
- 環境ごとに 1 つのパッチベースライン：
  - 開発: 0 日後にすべての重要度と分類を承認します。
  - テスト: 0 日後に重要なセキュリティ更新パッチを承認し、7 日後に他のすべての重要度と分類を承認します。
  - 製品: 0 日後に重要なセキュリティ更新パッチを承認し、14 日後に他のすべての重要度と分類を承認します。

CloudFormation スクリプト：

これらのスクリプトは、上記のベースライン承認設定を使用して、2 つのアベイラビリティーゾーン Windows HA EC2 アプリケーションのメンテナンスウィンドウ、ベースライン、パッチ適用タスクを構築するように設定されています。

- Windows 開発 CFN スタックの例: HA-Patching-Dev-Stack.json
- Windows テスト CFN スタックの例: HA-Patching-Test-Stack.json
- Windows Prod CFN スタックの例: HA-Patching-Prod-Stack.json

## パッチレコメンデーションFAQs

Q: 「0」日間のエクスプロイトに対して予定外のパッチ適用を処理するにはどうすればよいですか？

A: SSM は、インスタンスの OS の現在のデフォルトベースラインを使用する Patch Now 機能をサポートしています。AMS は、0 日後にすべてのパッチを承認するパッチベースラインのデフォルトセットをデプロイします。ただし、Patch Now 機能を使用する場合、このコマンドは AWS-

RunPatchBaseline SSM ドキュメントを実行するため、パッチ前スナップショットは作成されません。パッチを適用する前に、手動バックアップを取ることをお勧めします。

Q: AMS は Auto Scaling Group (ASGs) のインスタンスのパッチ適用をサポートしていますか？

A: いいえ。現時点では、ASG パッチ適用は Accelerate のお客様ではサポートされていません。

Q: メンテナンスウィンドウに留意すべき制限はありますか？

A: はい、注意すべき制限がいくつかあります。

- アカウントあたりのメンテナンスウィンドウ: 50
- メンテナンスウィンドウあたりのタスク数: 20
- メンテナンスウィンドウあたりの同時オートメーションの最大数: 20
- 同時メンテナンスウィンドウの最大数: 5

デフォルトの SSM 制限の完全なリストについては、AWS Systems Manager 「エンドポイントとクォータ」を参照してください。

# AMS でパッチメンテナンスウィンドウを作成する

パッチメンテナンスウィンドウは、ターゲットの Amazon EC2 インスタンスに対して設定されたスケジュールで AMS パッチオートメーションを実行します。ターゲットは、インスタンスのグループのタグによって定義されます。パッチ火曜日の日時に基づいてスケジュールを設定することも、cron 式を使用してスケジュールを定義することもできます。詳細については、「AWS Systems Manager ユーザーガイド」の「リファレンス: Systems Manager の Cron 式および rate 式」を参照してください。パッチを適用する前に、AMS は各インスタンスのルートボリュームのスナップショットを作成します。パッチ適用がインスタンスの状態に影響することを AMS が検出した場合、またはパッチ適用によるアプリケーションへの影響を AMS に通知した場合、AMS はこのスナップショットを使用してルートボリュームをパッチ前の状態に復元します。

## AMS Accelerate パッチメンテナンスウィンドウの制限

AMS パッチ適用では AWS Systems Manager (Systems Manager) を使用します。Systems Manager のサービス制限に加えて、AMS パッチ適用には、パッチメンテナンスウィンドウあたり 300 個のターゲットインスタンスの制限があります。インスタンスあたりの一般的なパッチ完了時間が 30 分の場合、次の表にメンテナンスウィンドウの数と期間の例を示します。

| パッチを適用するインスタンス | メンテナンスウィンドウの期間 (時間 ) | 必要な同時メンテナンスウィンドウ |
|---|---|---|
| 100 | 1 | 1 |
| 200 | 1 | 1 |
| 300 | 2 | 1 |
| 600 | 3 | 2 |
| 800 | 4 | 3 |
| 1200 | 6 | 4 |
| 1500 | 8 | 5 |

**Important**

これらの例では、他の Systems Manager メンテナンスウィンドウがアクティブではなく、他のオートメーションも実行されていないことを前提としています。

制限の詳細については、AWS Systems Manager 「 エンドポイントとクォータ」を参照してください。

トピック

- AMS コンソールから定期的な「パッチ火曜日」メンテナンスウィンドウを作成する (推奨 )
- CloudFormation for AMS Accelerate を使用してパッチメンテナンスウィンドウを作成する
- AMS Accelerate の Systems Manager コンソールからメンテナンスウィンドウを作成する
- AMS Accelerate 用の Systems Manager コマンドラインインターフェイス (CLI) を使用してメンテナンスウィンドウを作成する

# AMS コンソールから定期的な「パッチ火曜日」メンテナンスウィンドウを作成する (推奨 )

Microsoft は、毎月第 2 火曜日にオペレーティングシステムのパッチをリリースします。これはパッチ火曜日とも呼ばれます。パッチ火曜日を基準に、Windows インスタンスと Linux インスタンスの両方のパッチ適用をスケジュールするのが一般的です。パッチ火曜日の 1 回目または 2 回目の週末に定期的なパッチメンテナンスウィンドウをスケジュールするには、AMS コンソールにアクセスし、次の手順に従います。

1. パッチメンテナンスウィンドウの名前を指定します。
2. 〔オプション] パッチメンテナンスウィンドウの説明を入力します。
3. パッチ火曜日を基準にした日を選択します。
4. パッチメンテナンスウィンドウが開始する時間を hh:mm で入力します。たとえば、午前 0 時と午後 11 時が 23 時です。次に、タイムゾーンを選択します。
5. 〔オプション] 必要に応じて期間を変更します。AMS では、4 時間の最小期間を推奨しています。
6. ターゲットのパッチタグキーと値を入力します。詳細については、「タグとは」を参照してください。
7. 〔オプション] オプションのパラメータを展開して、同時実行数、エラー率、メンテナンスウィンドウのカットオフを調整します。

    1. 同時実行は、同時にパッチを適用するターゲットインスタンスの数を制御します。例えば、10 個のターゲットインスタンスの 50% の同時実行は一度に 5 個以下のインスタンスにパッチを適用し、100% の同時実行は一度に 10 個すべてのインスタンスにパッチを適用します。
    2. エラーレートは、パッチ適用が中断される前のエラーの許容度を制御します。たとえば、10 個のターゲットインスタンスのエラー率が 100% の場合、失敗の数に関係なくすべてのインスタンスにパッチが適用されますが、5 個のインスタンスがパッチ適用に失敗すると、50% のエラー率はパッチ適用を停止します。AMS では、100% のエラー率を推奨しています。
    3. パッチメンテナンスウィンドウのカットオフは、パッチメンテナンスウィンドウの終了前に新しいパッチ適用アクティビティの開始を停止することで、パッチメンテナンスウィンドウの違反を防止します。たとえば、カットオフの 1 時間 (推奨) は、パッチメンテナンスウィンドウが終了する 1 時間前に新しいパッチアクティビティを停止します。

> **Important**
>
> 次の実行時間を確認します。
> SSM メンテナンスウィンドウコンソール にアクセスし、新しく作成したパッチメンテナンスウィンドウを検索して、次の実行時間を確認します。ご質問がある場合、またはパッチメンテナンスウィンドウを編集する必要がある場合は、AMS パッチエキスパートと相談するためのサービスリクエストを作成します。

CloudFormation を使用して CRON ベースのパッチメンテナンスウィンドウをスケジュールするには、「」を参照してくださいCloudFormation for AMS Accelerate を使用してパッチメンテナンスウィンドウを作成する。

## CloudFormation for AMS Accelerate を使用してパッチメンテナンスウィンドウを作成する

を使用して AMS Accelerate パッチメンテナンスウィンドウを作成するには AWS CloudFormation、まず Accelerate アカウントにログインし、 AWS リージョン ターゲットインスタンスが存在する を選択します。次に、https://console.aws.amazon.com/cloudformation で以下のステップに従います。

1. 2 つのカスタム Accelerate パッチ適用 CloudFormation テンプレートのいずれかを選択します。

   - パッチ火曜日のスケジュール: Microsoft は、毎月第 2 火曜日にオペレーティングシステムのパッチをリリースします。これはパッチ火曜日とも呼ばれ、パッチ火曜日の後の第 1 または第 2 週末にパッチメンテナンスウィンドウをスケジュールします。 Accelerate コンソールにログインしたら、このリンク PatchTuesdayScheduling CloudFormation テンプレートを使用します。
   - CRON スケジューリング: CRON を使用してパッチメンテナンスウィンドウを作成して開始日を定義するには、このリンク CRONScheduling CloudFormation テンプレートを使用します。Systems Manager CRON 番号は 1～7 日目です (Systems Manager CRON の詳細については、「リファレンス: Systems Manager の Cron 式と rate 式」を参照してください )。

   これらのリンクのいずれかを選択すると、テンプレートは CloudFormation コンソールに自動的にロードされます。次に、[次へ] をクリックします。
2. スタックの詳細の指定ページ (スタックの作成ページのステップ 2) で、スタック名とテンプレートパラメータを入力します (デフォルトパラメータは AMS が推奨するデフォルトです。ユースケースの日時を選択します )。完了したら、[次へ] をクリックします。

3. スタックオプションを設定する (オプション ) 。オプションの詳細については、AWS CloudFormation スタックオプションの設定」を参照してください。完了したら、[次へ] をクリックします。
4. スタック値を確認します (オプション ) 。スタックの詳細を確認してコストを見積もる方法については、「スタックの確認」と「スタックコストの見積もり」を参照してください。準備ができたら、スタックの作成をクリックします。

   スタックの作成には最大 1 分かかる場合があります。スタックが正常に作成されると、パッチメンテナンスウィンドウは指定された時間に実行されます。パッチメンテナンスウィンドウを変更するには、CloudFormation 変更セットを作成して実行するか (推奨) (詳細については、「変更セットを使用したスタックの作成」を参照 ) 、Systems Manager メンテナンスウィンドウコンソール () でパッチメンテナンスウィンドウを更新しますhttps://console.aws.amazon.com/systems-manager/maintenance-windows。

詳細については、Namrata の動画をご覧ください (5:41)

## AMS Accelerate の Systems Manager コンソールからメンテナンスウィンドウを作成する

Systems Manager コンソールから AMS Accelerate メンテナンスウィンドウを作成するには、次の手順に従います。

1. 変更管理エリアの左側のナビゲーションバーで、メンテナンスウィンドウをクリックし、画面の右上にあるメンテナンスウィンドウの作成をクリックします。フォームに入力します。オプションの詳細については、「メンテナンスウィンドウの作成 (コンソール ) 」を参照してください。完了したら、メンテナンスウィンドウの作成をクリックします。

   メンテナンスウィンドウのリストページが開きます。
2. 新しく作成したメンテナンスウィンドウを選択します。

   メンテナンスウィンドウの詳細ページが開きます。
3. ターゲットタブに移動し、ターゲットの登録を選択します。

   ターゲットの登録ページが開きます。
4. Accelerate ターゲットを追加します。ターゲットの詳細については、「メンテナンスウィンドウにターゲットを割り当てる (コンソール ) 」を参照してください。完了したら、ターゲットの登録をクリックします。後で必要になったら、ターゲットを書き留めます。

メンテナンスウィンドウの詳細ページがターゲットタブで再び開き、新しいターゲットを含むリストが表示されます。

5. メンテナンスウィンドウの詳細ページのタスクタブで、タスクの登録を選択し、ドロップダウンリストからオートメーションの登録タスクを選択します。フォームに入力します。Accelerate の注意事項：

   - 意味のあるタスク名を指定します。例: AcceleratePatch。
   - 自動化ドキュメントエリアで、検索ボックスで「所有者」を選択し、「共有ドキュメント」を選択します。
   - 検索ボックスをクリックし、ドキュメント名のプレフィックス --> Equals を選択し、AWSManagedServices-PatchInstance」と入力します。次に、ラジオボタンを選択して AWSManagedServices-PatchInstance ドキュメントを選択します。
   - ドキュメントバージョンで、実行時にデフォルトバージョンを選択します。
   - 「ターゲット」セクションで、次の操作を行います。
     - 「Set Target by:」を「Selecting registered target groups」に設定します。
     - ターゲットのリストで、Targets タブで登録したターゲットを選択します。
   - 入力パラメータセクションで、 フォームを入力します。
     - InstanceId: {{*TARGET_ID*}}
     - StartInactiveInstances: パッチメンテナンスウィンドウ中にインスタンスが停止した場合にインスタンス`True`を起動します。

     > **Note**
     >
     > InstanceId パラメータ値は大文字と小文字が区別され、StartInactiveInstances パラメータ値は True または False のいずれかになります。
     > タグの対象となると、停止したインスタンスを開始することはできません。詳細については、「No Invocations to Execute」を参照してください。

   - レート制御セクションで、パーセンテージを選択します。AMS Accelerate では、自動化エラーに関係なく、同時実行に 100%、エラーしきい値に 100% を指定して、すべてのインスタンスに同時にパッチを適用することをお勧めします。一度にターゲットの半分にパッチを適用する場合、例えば、ターゲットインスタンスの半分をロードバランサーの背後で実行し続けるには、同時実行数を 50% に設定します。

- IAM サービスロールセクションで、カスタムサービスロールを使用するを選択し、ams_ssm_automation_role を選択します。

自動化タスクの登録をクリックします。

パッチ適用メンテナンスウィンドウが作成されます。説明タブに、次の実行時間が表示されます。

## AMS Accelerate 用の Systems Manager コマンドラインインターフェイス (CLI) を使用してメンテナンスウィンドウを作成する

コマンドラインインターフェイスを使用して AMS Accelerate メンテナンスウィンドウを作成するには：

1. 「SSM チュートリアル: メンテナンスウィンドウ (AWS CLI) を作成して設定する」に従います。チュートリアルの各ステップで、パッチ適用用のサンプル CLI コマンドを次に示します。

> **Note**
>
> これらの例は Linux または macOS に固有のものです。コマンドを実行することもできます。 AWS CloudShell このコマンドは、ローカルマシンawscliで を設定するよりも簡単です。詳細については、「 の使用 AWS CloudShell」を参照してください。

a. チュートリアルのステップ 1 では、メンテナンスウィンドウを作成します。

```
aws ssm create-maintenance-window \
                --name Sample-Maintenance-Window \
                --schedule "cron(0 30 23 ? * TUE#2 *)" \
                --duration 4 \
                --cutoff 1 \
                --allow-unassociated-targets \
                --tags "Key=Environment,Value=Production"
```

正常に完了すると、 window-id が返されます。

b. チュートリアルのステップ 2 では、ターゲットノードを登録します。

```
aws ssm register-target-with-maintenance-window \
                --window-id "mw-xxxxxxxxx" \
                --resource-type "INSTANCE" \
                --target "Key=tag:Environment,Values=Prod"
```

正常に完了すると、 WindowTargetIDが返されます。

c. チュートリアルのステップ 3 で、タスクを登録するには：

```
aws ssm register-task-with-maintenance-window \
    --window-id "mw-xxxxxx" \
    --targets "Key=WindowTargetIds,Values=63d4f63c-xxxxxx-9b1d-xxxxxfff" \
    --task-arn "AWSManagedServices-PatchInstance" \
    --service-role-arn "arn:aws:iam::AWS-Account-ID:role/ams_ssm_automation_role"
 \
    --task-invocation-parameters "{\"Automation\":{\"DocumentVersion\":\"\$DEFAULT
\",\"Parameters\":{\"InstanceId\":[\"{{TARGET_ID}}\"],\"StartInactiveInstances\":
[\"True\"]}}}" \
    --max-concurrency 50 \
    --max-errors 50 \
    --name "AutomationExample" \
    --description "Sample Description" \
    --task-type=AUTOMATION
```

# フックを使用したパッチ

AMS パッチフックを使用して、パッチ適用の前後にオペレーティングシステム (OS) レベルのコマンドを実行するように AMS パッチを設定できます。AMS パッチフックを使用して SSM コマンドドキュメントを実行し、パッチ適用前にサービスを停止してからパッチ適用後にサービスを開始するか、コマンドを実行してパッチ適用後にアプリケーションが正常であることを確認します。

AMS パッチフックを使用するには、以下を実行する必要があります。

1. パッチフックとして使用する SSM コマンドドキュメントを作成します。
2. AMS パッチメンテナンスウィンドウを作成するか、既存の AMS パッチメンテナンスウィンドウを使用します。詳細については、「AMS パッチメンテナンスウィンドウ」を参照してください。
3. AMS パッチメンテナンスウィンドウを設定して、AMS パッチフックに SSM コマンドドキュメントを使用します。

# AMS パッチフック RACI

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。次の表は、AMS パッチフックを使用するアプリケーション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。

- 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。
- は、説明責任を負う当事者を表します。
- 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、双方向のコミュニケーションがある当事者を表します。
- 「情報」を意味します。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。

| アクティビティ | お客様 | AMS |
| --- | --- | --- |
| パッチ前後の SSM コマンドドキュメントとドキュメントコンテンツを作成する | R | C |
| AMS パッチ適用のパッチフックパラメータを設定する | R | C |
| パッチ前後の SSM コマンドドキュメントを実行する | I | R |
| パッチフックの障害をトリアージして応答する | I | R |
| パッチフックの障害を顧客に通知する | I | R |
| お客様からリクエストされた場合は、パッチ適用前の状態にロールバックする | C | R |

# パッチフックの SSM ドキュメントを作成する

AMS パッチフックは、パッチ適用中に Amazon EC2 Systems Manager (SSM) ドキュメントを使用します。パッチ適用が発生するアカウントで、SSM コマンドドキュメントを作成するか、既存の SSM コマンドドキュメントを共有します。制限を含む SSM ドキュメントの詳細については、「SSM ドキュメントの共有」を参照してください。

SSM コマンドドキュメントを作成するには、次の手順に従います。

1. ドキュメントタイプが「コマンド」の SSM ドキュメントを作成します。
2. コンテンツセクションにコマンド (複数可) を入力します。詳細については、「SSM ドキュメントコンテンツの作成」を参照してください。

> **Note**
>
> AMS パッチフックの SSM ドキュメントは、 AWS CLI または を使用して作成することもできます CloudFormation。AMS パッチフックの SSM ドキュメントの作成についてサポートが必要な場合は、Cloud Architect にお問い合わせください。

# SSM コマンドドキュメントを AMS パッチフックとして使用するように AMS パッチメンテナンスウィンドウを設定する

AMS パッチメンテナンスウィンドウは、設定された AMS パッチオートメーションを実行する Systems Manager メンテナンスウィンドウです。

パッチフックを使用するように AMS パッチメンテナンスウィンドウを編集するには、次の手順に従います。

1. https://console.aws.amazon.com/systems-manager/ の左側のナビゲーションペインの変更管理ツールで、メンテナンスウィンドウを選択します。

   既存のメンテナンスウィンドウを一覧表示するページが開きます。
2. mw- で始まるウィンドウ ID を選択します。

   そのメンテナンスウィンドウの詳細ページが開きます。
3. タスクタブと AMS-PatchInstance のタスク ARN を持つウィンドウタスク ID を選択し、編集をクリックします。

4. パラメータセクションまでスクロールし、次のパラメータを更新します。

AMS パッチフックパラメータ：

- PrePatchHook: パッチ適用前に実行する「コマンド」タイプの SSM ドキュメントの名前。パッチ適用前にコマンドを実行していない場合は、空白のままにするか、「AWS-Noop」と入力します (大文字と小文字を区別します )。
- PostPatchHook: パッチ適用後に実行する「コマンド」タイプの SSM ドキュメントの名前。パッチ適用後にコマンドを実行しない場合は、空白のままにするか、「AWS-Noop」と入力します (大文字と小文字を区別します )。
- ExecutePatchBasedOnPreHookStatus: PrePatchHook 実行の成功または失敗に基づいてパッチ適用を実行するには、次のいずれかを選択します。
  - OnPreHookSuccess: PrePatchHook が成功した場合にのみ AMS パッチオートメーションを実行します。
  - 常に: PrePatchHook が成功したときと失敗したときに AMS パッチオートメーションを実行します。
  - OnPreHookFailure - PrePatchHook が失敗した場合にのみ AMS パッチオートメーションを実行します。
  - なし: AMS パッチオートメーションを実行しないでください。これは、PrePatchHook をテストする場合に便利です。
- ExecutePostHookBasedOnPatchStatus: AMS パッチオートメーションの成功または失敗に基づいてパッチ後フックを実行し、次のいずれかを選択します。
  - OnPatchSuccess: AMS パッチオートメーションが正常に実行された場合にのみ PostPatchHook を実行します。
  - 常に: AMS パッチの自動化が成功したときと失敗したときに PostPatchHook を実行します。
  - OnPatchFailure - AMS パッチの自動化が失敗した場合にのみ PostPatchHook を実行します。

> **Note**
>
> これらの変数のいずれかにテキストボックスがない場合は、同じページの Automation ドキュメントセクションまでスクロールし、別のドキュメントを選択してから元のドキュメン

トを再選択することで、この問題を解決します。これにより、入力パラメータが更新され、編集できるようになります。

# AMS Accelerate パッチベースライン

パッチベースラインは、インスタンスへのインストールを承認するパッチを定義します。パッチの承認または拒否は個別に指定できます。また、自動承認ルールを作成して特定のタイプの更新 (例: 重要な更新) を自動承認するよう指定できます。拒否済みリストは、これらのルールと承認リストの両方に優先します。

## デフォルトのパッチベースライン

AMS Accelerate パッチ適用にオンボードすると、デフォルトのパッチベースラインは、次のオペレーティングシステムの AMS Accelerate のデフォルトのパッチベースラインによって上書きされます。

- Windows
- Amazon Linux 1
- Amazon Linux 2
- CentOS
- Suse
- Rhel
- Ubuntu

**Important**

デフォルトのパッチベースラインは AMS によって管理されます。変更が失われる可能性があるため、デフォルトのパッチベースラインを編集しないでください。代わりに、カスタムパッチベースラインを作成します。「AMS Accelerate を使用したカスタムパッチベースライン」を参照してください。

> **Note**
>
> 製品 = * として定義された AMS Accelerate パッチベースラインは、すべてのパッチがすべてのセキュリティと分類のインスタンスに適用されることを意味します。

## AMS Accelerate を使用したカスタムパッチベースライン

AMS Accelerate でカスタムパッチベースラインを使用するには、まずパッチグループがあることを確認し、カスタムベースラインを作成します。

詳細については、以下のリソースを参照してください。

- パッチグループの使用
- カスタムパッチベースラインの作成 (Windows)
- カスタムパッチベースラインの作成 (Linux)
- カスタムパッチベースラインの更新または削除 (コンソール )

# AMS Accelerate のオンデマンドパッチ適用用の IAM ロールの作成

アカウントが AMS Accelerate パッチ適用にオンボーディングされると、AMS Accelerate は管理ポリシーである amspatchmanagedpolicy をデプロイします。このポリシーには、AMS オートメーションドキュメント を使用したオンデマンドパッチ適用に必要なアクセス許可が含まれていますAWSManagedServices-PatchInstance。この自動化ドキュメントを使用するには、アカウント管理者がユーザーの IAM ロールを作成します。以下の手順に従ってください。

以下を使用してロールを作成します AWS マネジメントコンソール。

1. にサインイン AWS マネジメントコンソール し、IAM コンソールを開きます。
2. コンソールのナビゲーションペインで、ロールを選択し、ロールを作成します。
3. Anotherrole AWS アカウント タイプを選択します。
4. アカウント ID には、リソースへのアクセスを許可する AWS アカウント ID を入力します。

   指定したアカウントの管理者は、そのアカウントのすべての IAM ユーザーに、このロールを引き受ける許可を付与できます。これを行うには、管理者は、sts:AssumeRoleaction のアクセス許可を付与するポリシーをユーザーまたはグループにアタッチします。このポリシーでは、ロールの

Amazon リソースネーム (ARN) をリソースとして指定する必要があります。次の点に注意してください。

- 自分が管理していないアカウントのユーザーにアクセス許可を付与していて、ユーザーがこのロールをプログラムで引き受ける場合は、「外部 ID を要求する」を選択します。外部 ID は、お客様とサードパーティーのアカウントの管理者との間で同意した任意の単語または数値です。このオプションは、リクエストに correctsts:ExternalID が含まれている場合にのみユーザーがロールを引き受けることを可能にする条件を信頼ポリシーに自動的に追加します。詳細については、AWS「リソースへのアクセスを第三者に付与するときに外部 ID を使用する方法」を参照してください。
- ロールを多要素認証 (MFA) でサインインするユーザーに制限する場合は、「MFA を要求」を選択します。これにより、MFA によるサインインの有無を確認する条件がロールの信頼ポリシーに追加されます。ロールを引き受けるユーザーは、設定した MFA デバイスから一時的なワンタイムパスワードを使用してサインインする必要があります。MFA 認証のないユーザーはロールを引き受けることができません。MFA の詳細については、「 での多要素認証 (MFA) AWSの使用」を参照してください。

5. [Next: Permissions] (次のステップ: 許可) を選択します。

   IAM には、アカウント内のポリシーのリストが含まれます。アクセス許可の追加で、フィルターボックスに amspatchmanagedpolicy と入力し、このアクセス許可ポリシーのチェックボックスをオンにします。[次へ] をクリックします。

6. ロールの詳細の下に、PatchRole などのロール名を入力し、ロールの説明を追加し (推奨 ) 、このロールを識別するのに役立つタグも追加します。ロール名では大文字と小文字は区別されませんが、 内で一意である必要があります AWS アカウント。完了したら、ロールの作成をクリックします。

> **Note**
>
> ロール名は、作成後に編集することはできません。

# AMS Accelerate のパッチ通知とパッチ障害を理解する

> **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。

## パッチサービスリクエストと E メール通知

AMS は、次のパッチメンテナンスウィンドウの 4 日前に新しいサービスリクエストを作成します。たとえば、App1 PROD という名前のパッチメンテナンスウィンドウが実行される 4 日前に、AMS はアカウント [アカウント ID] の App1 Prod の 4 月のパッチメンテナンスウィンドウというタイトルのサービスリクエストを作成します。スケジュールされたパッチを調整する必要がある場合は、パッチサービスリクエストを使用して AMS と通信するか、今後のパッチをスキップします。サービスリクエストが作成されると、サービスリクエストへのリンクが記載された E メールがパッチ通知アドレスに送信されます。AMS がサービスリクエストを更新するたびに、追加の E メールが送信されます。

> **Note**
>
> AMS は、パッチメンテナンスウィンドウが実行スケジュールの 4 日以内に作成された場合でも、新しいサービスリクエストを作成します。
> サービスリクエスト通知を受信するには、パッチメンテナンスウィンドウが「有効」状態である必要があります。

パッチ適用が開始される 1 時間前に、AMS はパッチサービスリクエストを通じて通知します。パッチ適用が完了すると、AMS はパッチマネージャーコンソールへのリンクを使用してパッチサービスリクエストを更新します。リンクを使用して、パッチメンテナンスウィンドウの対象となるインスタンスのパッチコンプライアンスを表示します。

> **Note**
>
> Patch Manager コンソールのリンクには、インスタンスの現在のコンプライアンスが表示されます。パッチマネージャーは、AMS がパッチ適用を完了してからリンクにアクセスするまでの間に新しいパッチがリリースされた場合、インスタンスを非準拠として表示します。

## CloudWatch Events を介したパッチ通知

AMS は、パッチプロセス中に以下を含む CloudWatch Events を 3 回送信します。

- パッチメンテナンスウィンドウが実行される 4 日前。
- パッチメンテナンスウィンドウが実行される 1 時間前。
- パッチメンテナンスウィンドウが完了したら。

以下は、パッチメンテナンスウィンドウのアドバンスト通知イベントスキーマです。

```
{
    "version": "0",
    "id": "37004d81-458d-2cef-fe1c-8afa8af30406",
    "detail-type": "AMS Patch Window Execution State Change",
    "source": "aws.managedservices",
    "account": "145917996532",
    "time": "2021-05-20T02:00:00Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/mw-00000001235",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaab"
    ],
    "detail": {
        "State": "PREEMPTIVE",
        "StartTime": "2021-05-24T02:00:00.000000",
        "WindowArn": "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/
mw-00000001235",
        "Results": "[{\"instanceId\": \"i-0000000aaaaaaaaaa\"}, {\"instanceId\":
 \"i-0000000aaaaaaaaab\"}]"
    }
}
```

次の表は、パッチメンテナンスウィンドウの事前通知イベントスキーマを示しています。

パッチ通知の詳細

| プロパティ名 | 説明 | サンプル値 |
| --- | --- | --- |
| State | パッチ適用メンテナンスウィンドウの状態 | PREEMPTIVE - 間もなく開始される予定のパッチ適用ウィンドウ |
| ステータス | パッチ適用メンテナンスウィンドウのステータス | 成功 - すべてのインスタンスに障害なくパッチが適用されました<br><br>FAILED – 少なくとも 1 つのインスタンスがパッチ適用に失敗しました |

| プロパティ名 | 説明 | サンプル値 |
| --- | --- | --- |
| StartTime | パッチ適用メンテナンスウィンドウの開始時刻、ISO 形式 | 2021-02-03T22:14:05.814308 |
| WindowArn | パッチ適用メンテナンスウィンドウの一意の識別子 | arn:aws:ssm:us-east-1:123456789012:maintenancewindow/mw-00000001235 |
| 結果 | パッチウィンドウの対象となるインスタンスのリスト | InstanceId – ターゲットインスタンスのインスタンス ID |

以下は、パッチメンテナンスウィンドウの終了イベントスキーマです。

```
{"version": "0",
    "id": "0f25add5-44a9-0702-d2bc-bd2102affefe",
    "detail-type": "AMS Patch Window Execution State Change",
    "source": "aws.managedservices",
    "account": "123456789012",
    "time": "2021-02-03T22:14:06Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/mw-00000001235",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaab"
    ],
    "detail": {"State": "[COMPLETED]",
        "Status": "SUCCESS",
        "StartTime": "2021-02-03T22:12:00.814308",
        "EndTime": "2021-02-03T22:14:05.814309",
        "WindowArn": "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/
mw-00000001235",
        "WindowExecutionId": "e32088eb-c05f-4c63-b766-6866e163c818",
        "Results": "[{\"instanceId\": \"i-0000000aaaaaaaaaa\", \"status\":
 \"Success\", \"missing_critical_patch_count\": 0, \"missing_total_patch_count
\": 0} }, {\"instanceId\": \"i-0000000aaaaaaaaab\", \"status\": Success},
 \"missing_critical_patch_count\": 0, \"missing_total_patch_count\": 0}]"
    }
}
```

次の表に、パッチメンテナンスウィンドウの終了イベントスキーマを示します。

パッチウィンドウの終了の詳細

| プロパティ名 | 説明 | サンプル値 |
| --- | --- | --- |
| State | パッチ適用メンテナンスウィンドウの状態 | COMPLETED – パッチ適用ウィンドウが終了しました |
| ステータス | パッチ適用メンテナンスウィンドウのステータス | 成功 - すべてのインスタンスに障害なくパッチが適用されました<br><br>FAILED – 少なくとも 1 つのインスタンスがパッチ適用に失敗しました |
| StartTime | パッチ適用メンテナンスウィンドウの開始時刻、ISO 形式 | 2021-02-03T22:14:05.814308 |
| EndTime | パッチ適用メンテナンスウィンドウの終了時刻、ISO 形式 | 2021-02-03T23:14:05.814308 |
| WindowArn | パッチ適用メンテナンスウィンドウの一意の識別子。 | arn:aws:ssm:us-east-1:123456789012:maintenancewindow/mw-000000001235 |
| WindowExecutionId | SSM メンテナンスウィンドウコンソールから確認できるウィンドウ実行 ID | e32088eb-c05f-4c63-b766-6866e163c818 |
| 結果 | パッチウィンドウの対象となるインスタンスのリスト | InstanceId – ターゲットのインスタンス ID<br><br>status – インスタンスパッチのステータス |

| プロパティ名 | 説明 | サンプル値 |
| --- | --- | --- |
| | | missing_critical_patch_count - インスタンスに欠落している重要なパッチの数<br><br>missing_total_patch_count - インスタンスで欠落しているパッチの合計数 |

CloudWatch Events イベントを使用して、パッチ適用メンテナンスウィンドウの事前通知が送信されたときに通知する CloudWatch ルールをトリガーできます。これを行うには、次の設定で CloudWatch ルールを設定します。

```
{
    "source": [
        "aws.managedservices"
    ],
    "detail-type": [
        "AMS Patch Window Execution State Change"
    ],
    "detail": {
        "State": ["PREEMPTIVE"]
    }
}
```

> **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。

## AMS でのパッチ障害の調査

AWS Managed Services (AMS) はパッチ適用を管理し、パッチ障害の修復を含めます。パッチ適用が失敗すると、AMS オペレーションはアラートを受け取り、 AWS と AMS のベストプラクティスに従って問題に対処することで修復を試みます。

パッチが失敗した場合、AMS は、AWS Managed Services – Patch Instance failure for instance <instance-id> というタイトルの SSM OpsItem をアカウントに作成します。

次に、AMS は OpsItem を調査します。AMS がユーザーの介入なしに障害を修正できる場合、AMS は OpsItem を解決します。介入が必要な場合、AMS は調査結果と推奨される修復手順を含むサービスリクエストを通じて通知します。問題を解決するためのアクションを実行しない場合、AMS は次にスケジュールされたパッチメンテナンスウィンドウ中にインスタンスにパッチを適用しようとします。

> **Note**
>
> パッチ障害 OpsItems は、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、またはパッチメンテナンスウィンドウ中に停止状態にあるインスタンスでは作成されません。

# AMS Resource Scheduler によるコスト最適化

AMS Resource Scheduler on AWS ソリューションを使用すると、使用されていないリソースを停止し、容量が必要な場合にリソースを開始することで、 AWS と AMS のコストを削減できます。たとえば、開発環境の AWS で AMS Resource Scheduler を使用して、毎日営業時間外にインスタンスを自動的に停止できます。すべてのインスタンスをフル使用率で実行したままにすると、このソリューションによってインスタンス使用率が低下し、設定したスケジュールに基づいて全体的なコストが削減される可能性があります。

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 Auto Scaling グループ、Amazon EC2 インスタンス、Amazon 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 AWS Instance Scheduler 上に構築されていますが、AMS のお客様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。カスタマイズには、Auto Scaling グループのスケジューリングのサポート、Elastic Load Balancing アラームの CloudWatch アラームサプレッサー、Amazon EC2 の複数の AWS Systems Manager メンテナンスウィンドウのサポート、コスト削減推定器、AMS の運用サポートが含まれます。

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、リソースを実行する時刻を定義します。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、休止などの追加の設定が含まれており、リソースを実行するタイミングを指定します。AMS が提供する AWS Systems Manager オートメーションランブックを使用して、これらの期間とスケジュールを設定できます。各スケジュールには、インスタンスを実行する時間を定義する期間を少なくとも 1 つ含める必要があります。スケジュールには複数の期間を含めることができます。スケジュールで複数の期間を使用する場合、インスタンススケジューラは、期間ルールの少なくとも 1 つが true であるときに適切な開始アクションを適用します。スケジュールと期間の詳細については、「AWS Instance Scheduler のソリューションコンポーネント」を参照してください。

AMS Resource Scheduler は、 AWS リソースタグを使用してスケジュールを 1 つ以上のリソースに関連付け、スケジュールされた開始アクションと停止アクションをターゲットにします。スケジュール名を値として、スケジューラで設定されたタグキー (デフォルトは `Schedule`) でリソースにタグ付けします。コスト削減を追跡およびレポートするために、スケジューラのコスト見積り機能 AWS Cost Explorer について、 のコスト配分タグと同じタグキーを設定します。

AMS Resource Scheduler は、アカウントごとに有効にできるオプトイン機能です。

# AMS Resource Scheduler でのリソースの使用

Amazon EC2

- 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、個別に処理されず、AMS Resource Scheduler によってスキップされません。
- ターゲットインスタンスのルートボリュームが AWS 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、CMK のリストを値として CloudFormation スタック を更新して`ams-resource-scheduler`、 アクセス許可を `UseCMK`パラメータに追加できます (KMS エイリアス`arn:`*`partition`*`:kms:`*`region`*`:`*`account-id`*`:key/`*`key-id`*の代わりに 形式の 1 つ以上の CMK キー ARNs を使用します ) 。
- Amazon EC2 インスタンスが特定のソフトウェア、または によって管理されるベンダーライセンスで設定されている場合 AWS License Manager、Resource Scheduler AWS License Manager はインスタンスを起動するために特定のライセンスに対するアクセス許可が必要です。CloudFormation スタック () の EC2 インスタンスのライセンスマネージャーライセンスパラメータに AWS License Manager ライセンスの ARN (複数可) のリストを追加することで、Resource Scheduler に必要なアクセス許可を付与できます`ams-resource-scheduler`。

Amazon EC2 Auto Scaling

- 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。
- Auto Scaling 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

- 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、Create RDS Instance Snapshot AWS 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ーゾーン (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。

> **Note**
>
> Resource Scheduler は、リソースが開始または停止されたことを検証しません。これにより、関連するサービスの API コールが行われ、続行されます。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。
> AMS Resource Scheduler は AWS Backup ウィンドウをサポートしていません。 AWS Backup有効な RDS インスタンスを Resource Scheduler スケジュールにマッピングする場合、バックアップを期待どおりに機能させるには、バックアップウィンドウがスケジュールの実行ウィンドウ内にある必要があります。

# AMS リソーススケジューラのオンボーディング

アカウントが AMS Accelerate オペレーションプランにオンボーディングされている場合、アカウントは AMS Resource Scheduler に自動的にオンボーディングされません。ただし、AMS Accelerate オペレーションプランへのアカウントのオンボーディングの一環として、またはその後いつでも、Cloud Service Delivery Manager (CSDM) にアカウントを AMS Resource Scheduler にオンボードするようにリクエストできます。CSDM がアカウントをオンボードすると、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。

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。

# AMS リソーススケジューラのカスタマイズ

オンボーディングされると、AMS Resource Scheduler は、AMS Accelerate アカウントのプライマリ AWS リージョンams-resource-schedulerに、 という名前の CloudFormation スタックとしてデプロイされます。CloudFormation スタックパラメータを使用して、設定に基づいて AMS Resource Scheduler のプロパティを設定し、スタックの更新を実行できます。CloudFormation スタックの更新については、「スタックを直接更新する」を参照してください。

最適な機能を得るには、次のプロパティをカスタマイズし、残りをデフォルトのままにすることをお勧めします。

- 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。
- スケジュールするサービス (複数可 ) : 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。
- 暗号化された EBS ボリュームの CMK: 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。
- EC2 インスタンスのライセンスマネージャーライセンス: その Resource Scheduler に対する AWS Licence Manager ARNs のカンマ区切りリストにアクセス許可を付与できます。

> **Note**
>
> AMS は、アカウントで AMS Resource Scheduler を最新の状態に保つための機能と修正をリリースすることがあります。この場合、スタックパラメータを使用して AMS Resource Scheduler スタックに対して行ったカスタマイズは保持されます。
> AMS Resource Scheduler のコンポーネントリソースに直接カスタマイズしないことを強くお勧めします。これにより、Resource Scheduler の機能や AMS が最新の状態に保つ能力に影響します。

# AMS リソーススケジューラの使用

AMS Accelerate アカウントで AMS Resource Scheduler 期間を使用する方法。

次の AWS Systems Manager オートメーションランブックのセットを使用して、AMS Resource Scheduler で必要なスケジュールと期間を管理します。

> **Note**
>
> これらの SSM オートメーションランブックは、アカウントのプライマリ AWS リージョンで使用できます。

- `AWSManagedServices-AddOrUpdatePeriod`
- `AWSManagedServices-AddOrUpdateSchedule`
- `AWSManagedServices-DeleteScheduleOrPeriod`
- `AWSManagedServices-DescribeScheduleOrPeriods`
- `AWSManagedServices-EnableOrDisableAMSResourceScheduler`

さらに、AMS は、ランブックを使用するために AWS Systems Manager と `ams_resource_scheduler_ssm_automation_role`が必要とする AWS Identity and Access Management ロールをプロビジョニングします。IAM ロールは、ランブックの機能に必要な SSM アクセス許可を付与する最小権限のインラインポリシーでスコープダウンされます。

前提条件

SSM オートメーションランブックと AMS リソーススケジューラの使用を開始する前に、次の手順を実行します。

オートメーションランブックを使用して AMS Resource Scheduler でスケジュールと期間を管理することを許可する適切な IAM エンティティ (ユーザー、グループ、またはロール) に、次のポリシーをアタッチします。IAM エンティティにアカウントの管理者または PowerUser アクセス許可がある場合、ポリシーは必要ありません。

JSON

```
{
    "Version":"2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "AllowPassingResourceSchedulerRole",
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::111122223333:role/
ams_resource_scheduler_ssm_automation_role",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "ssm.amazonaws.com"
                }
            }
        },
        {
            "Sid": "ListAndDescribeAutomationExecutions",
            "Effect": "Allow",
            "Action": [
                "ssm:GetAutomationExecution",
                "ssm:DescribeAutomationStepExecutions"
            ],
            "Resource": "arn:aws:ssm:*:111122223333:automation-execution/*"
        },
        {
            "Sid": "ListAndDescribeResourceSchedulerSSMDocuments",
            "Effect": "Allow",
            "Action": [
                "ssm:ListDocumentVersions",
                "ssm:DescribeDocument",
                "ssm:ListDocumentMetadataHistory",
                "ssm:DescribeDocumentParameters",
                "ssm:GetDocument",
                "ssm:DescribeDocumentPermission"
            ],
            "Resource": [
                "arn:aws:ssm:*::document/AWSManagedServices-AddOrUpdatePeriod",
                "arn:aws:ssm:*::document/AWSManagedServices-AddOrUpdateSchedule",
                "arn:aws:ssm:*::document/AWSManagedServices-
DeleteScheduleOrPeriod",
                "arn:aws:ssm:*::document/AWSManagedServices-
DescribeScheduleOrPeriods",
                "arn:aws:ssm:*::document/AWSManagedServices-
EnableOrDisableAMSResourceScheduler"
            ]
        },
```

```
        {
            "Sid": "AllowExecutionOfResourceSchedulerSSMDocuments",
            "Effect": "Allow",
            "Action": [
                "ssm:StartAutomationExecution"
            ],
            "Resource": [
                "arn:aws:ssm:*::automation-definition/AWSManagedServices-
AddOrUpdatePeriod:*",
                "arn:aws:ssm:*::automation-definition/AWSManagedServices-
AddOrUpdateSchedule:*",
                "arn:aws:ssm:*::automation-definition/AWSManagedServices-
DeleteScheduleOrPeriod:*",
                "arn:aws:ssm:*::automation-definition/AWSManagedServices-
DescribeScheduleOrPeriods:*",
                "arn:aws:ssm:*::automation-definition/AWSManagedServices-
EnableOrDisableAMSResourceScheduler:*"
            ]
        },
        {
            "Sid": "AllowListingAllDocuments",
            "Effect": "Allow",
            "Action": "ssm:ListDocuments",
            "Resource": "*"
        },
        {
            "Sid": "AllowListingAllSSMExecutions",
            "Effect": "Allow",
            "Action": "ssm:DescribeAutomationExecutions",
            "Resource": "*"
        },
        {
            "Sid": "AllowListingIAMRolesForStartingExecutionViaConsole",
            "Effect": "Allow",
            "Action": "iam:ListRoles",
            "Resource": "*"
        }
    ]
}
```

オートメーションは、 AWS Systems Manager コンソールまたは CLI AWS を使用して実行できます。 AWS CLI を使用している場合は、インストールして設定するか、PowerShell 用の AWS ツール

をまだインストールしていない場合は設定する必要があります。詳細については、AWS「コマンドラインツール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。

詳細については、Navish の動画をご覧ください (4:52)

# AWS Managed Services Resource Scheduler で期間とスケジュールを操作する

AMS Resource Scheduler を使用して、AMS Accelerate アカウントのスケジュールまたは期間を追加、更新、または削除できます。

## AMS Resource Scheduler で期間を追加または更新する

AMS アカウントで Resource Scheduler 期間を追加または更新します。

必要なデータ：

- アクション: 実行するオペレーションのタイプ。期間を追加する場合は「追加」を使用し、既存の期間を更新する場合は「更新」を使用します。
- 名前: 期間の名前。新しい期間を追加する場合は、一意の値を指定する必要があります。
- AutomationAssumeRole: ランブックがユーザーに代わって期間を追加または更新することを許可する AWS Identity and Access Management (IAM) ロールの ARN。ロールを として指定しますams_resource_scheduler_ssm_automation_role。
- 説明 (オプション): 期間の意味のある説明。
- BeginTime (オプション): リソースを開始する HH:MM 形式の時間。
- EndTime (オプション): リソースを停止する HH:MM 形式の時間。
- 月 (オプション): リソースを実行する月またはハイフンで区切られた月の範囲のカンマ区切りリスト。
- MonthDays (オプション): リソースを実行する曜日のカンマ区切りリストまたはハイフンで囲まれた範囲。
- WeekDays (オプション): リソースを実行する曜日または曜日の範囲のカンマ区切りリスト。

これを行う方法：

- AWSManagedServices-AddOrUpdatePeriod でドキュメントを表示します (オンボーディングされたリージョンを選択する必要がある場合があります )。

入力パラメータセクションで要件を指定し、実行を選択します。オペレーションが完了したら、出力タブで結果を表示します。

- AWS CLI:

  オートメーションを開始するには、次のコマンドを実行します。*#########*独自の情報に置き換えます。

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
AddOrUpdatePeriod" --document-version "\$DEFAULT"
     --parameters '{"Action":["add" or "update"], "Name":["NAME"],
    "Description":["DESCRIPTION"],"BeginTime":["TIME"], "EndTime":["TIME"],
    "Months":["MONTH"],"MonthDays":["DAY"], "WeekDays":["DAY"],
    "AutomationAssumeRole" : ["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"] }' --region ONBOARDED_REGION
```

例:

次の例は、 AWS Systems Manager コンソールを使用して新しい期間を追加する方法を示しています。Period-Name という期間を指定し、毎月の最初の 15 日間、月曜日から金曜日の9AM-6PM 時をカバーするように設定しました。

1. AWSManagedServices-AddOrUpdatePeriod で AWS Systems Manager オートメーションドキュメントを表示します (オンボーディングされたリージョンを選択する必要がある場合があります ) 。

2. パラメータの値を指定します。

3. 実行 をクリックし、自動化が完了するまで待ちます。

## AMS Resource Scheduler でスケジュールを追加または更新する

AMS Accelerate アカウントで Resource Scheduler スケジュールを追加または更新します。

必要なデータ :

- アクション: 実行するオペレーションのタイプ。スケジュールを追加する場合は「追加」を使用し、既存のスケジュールを更新する場合は「更新」を使用します。

- 名前: スケジュールの名前。新しいスケジュールを追加する場合は、一意の値を指定する必要があります。
- AutomationAssumeRole: ランブックがユーザーに代わってスケジュールを追加または更新することを許可する AWS Identity and Access Management (IAM) ロールの ARN。ロール を指定しますams_resource_scheduler_ssm_automation_role。
- 説明 (オプション): スケジュールのわかりやすい説明。
- スケジュール (オプション): このスケジュールで使用する期間のカンマ区切りリストを指定します。各期間は既に作成されている必要があります。
- RetainRunning (オプション): 実行中の Perod の開始前にリソースを手動で開始した場合、Resource Scheduler が実行中のリソースを実行中の期間の終了時に停止しないようにするには、「true」を指定します。デフォルトでは、Resource Scheduler はリソースを停止します。
- StopNewInstances (オプション): 実行期間外に実行されている場合、リソーススケジューラが最初にタグ付けされたときにリソースを停止しないようにするには、「false」を指定します。デフォルトでは、Resource Scheduler はリソースを停止します。
- SSMMaintenanceWindow (オプション): スケジュールの実行期間として追加する AWS Systems Manager (SSM) メンテナンスウィンドウのカンマ区切りリストを指定します。また、「UseMaintenanceWindow」プロパティを「true」に指定する必要があります。
- TimeZone (オプション): Resource Scheduler で使用するタイムゾーンを指定します。デフォルトでは、Resource Scheduler は UTC を使用します。
- UseMaintenanceWindow (オプション): Resource Scheduler が Amazon Relational Database Service (RDS) メンテナンスウィンドウを Amazon RDS インスタンススケジュールの実行期間と見なす場合、または AWS Systems Manager (SSM) メンテナンスウィンドウを Amazon EC2 インスタンススケジュールの実行期間として追加する場合は、「true」を指定します。
- UseMetrics (オプション): スケジュールレベルで CloudWatch メトリクスを有効にするには「true」を指定し、CloudWatch メトリクスを無効にするには「false」を指定します。このプロパティを指定すると、スタックレベルで設定された CloudWatch メトリクス設定が上書きされます。

これを行う方法：

- AWSManagedServices-AddOrUpdateSchedule でドキュメントを表示します (オンボーディングされたリージョンを選択する必要がある場合があります )。

  入力パラメータセクションで要件を指定し、実行を選択します。オペレーションが完了したら、出力タブで結果を表示します。
- AWS CLI:

オートメーションを開始するには、次のコマンドを実行します。*#########*独自の情報に置き換えます。

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
AddOrUpdateSchedule" --document-version "\$DEFAULT"
     --parameters '{"Action":["add" or "update"], "Name":["NAME"], "Description":
["DESCRIPTION"],
    "Hibernate":["true or false"],"Enforced":["true or false"],
    "OverrideStatus":["running or stopped"],"Periods":["PERIOD-A, PERIOD-B"],
    "RetainRunning":["true or false"],"StopNewInstances":["true or false"],
    "SSMMaintenanceWindow":["WINDOW-NAME"],"TimeZone":["TIMEZONE"],
    "UseMaintenanceWindow":["true or false"],"UseMetrics":["true or false"],
    "AutomationAssumeRole" : ["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"] }' --region ONBOARDED_REGION
```

例:

次の例は、AMS Resource Scheduler のスケジュールを追加する方法を示しています。この例では、CustomPeriod を使用して CustomSchedule という名前のスケジュールを追加します。CustomPeriod

1. AWSManagedServices-AddOrUpdateSchedule で AWS Systems Manager オートメーションドキュメントを表示します (オンボーディングされたリージョンを選択する必要がある場合があります )。

2. パラメータの値を指定します。

3. 実行 をクリックし、自動化が完了するまで待ちます。

## AMS Resource Scheduler で期間またはスケジュールを削除する

AMS Accelerate アカウントで Resource Scheduler の期間またはスケジュールを削除するには、次のデータが必要です。

- ConfigurationType: 削除する設定のタイプ。期間を削除する場合は「ピリオド」を使用し、スケジュールを削除する場合は「スケジュール」を使用します。
- 名前: 削除するスケジュールまたは期間の名前。

- AutomationAssumeRole: ランブックがユーザーに代わってスケジュールまたは期間を削除できるようにする AWS Identity and Access Management (IAM) ロールの ARN。ロール を指定しますams_resource_scheduler_ssm_automation_role。

これを行う方法：

- AWSManagedServices-DeleteScheduleOrPeriod でドキュメントを表示します (オンボーディングされたリージョンを選択する必要が生じる場合があります )。

  入力パラメータセクションで要件を指定し、実行を選択します。オペレーションが完了したら、出力タブで結果を表示します。

- AWS CLI:

  オートメーションを開始するには、次のコマンドを実行します。*#########*独自の情報に置き換えます。

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
DeleteScheduleOrPeriod" --document-version "\$DEFAULT"
--parameters '{"ConfigurationType":["period" or "schedule"],"Name":["NAME"],
    "AutomationAssumeRole":["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"]}' --region ONBOARDED_REGION
```

例:

次の例は、 AWS Systems Manager コンソールを使用して期間を削除する方法を示しています。

1. AWSManagedServices-DeleteScheduleOrPeriod で AWS Systems Manager オートメーションドキュメントを表示します (オンボーディングされたリージョンを選択する必要がある場合があります )。

2. パラメータの値を指定します。

3. 実行 をクリックし、自動化が完了するまで待ちます。

## AMS Resource Scheduler での期間またはスケジュールの説明

AMS Accelerate アカウントで Resource Scheduler の期間またはスケジュールを記述 (詳細を表示) するには、次のデータが必要です。

- ConfigurationType: 記述する設定のタイプ。すべての期間を記述する場合は「ピリオド」を使用し、すべてのスケジュールを記述する場合は「スケジュール」を使用します。
- AutomationAssumeRole: ランブックがユーザーに代わってスケジュールまたは期間を記述できるようにする AWS Identity and Access Management (IAM) ロールの ARN。ロール を指定しますams_resource_scheduler_ssm_automation_role。

これを行う方法：

- AWSManagedServices-DescribeScheduleOrPeriods でドキュメントを表示します (オンボーディングされたリージョンを選択する必要がある場合があります )。
  1. 入力パラメータセクションで要件を指定し、実行を選択します。
  2. オペレーションが完了したら、出力タブで結果を表示します。
- AWS CLI:
  1. オートメーションを開始するには、次のコマンドを実行します。*#########*独自の情報に置き換えます。

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
DescribeScheduleOrPeriods" --document-version "\$DEFAULT"
                --parameters '{"ConfigurationType":["period" or
 "schedule"],"AutomationAssumeRole":["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"]}'
                --region ONBOARDED_REGION
```

例:

次の例は、 AWS Systems Manager コンソールを使用して期間を記述する方法を示しています。

1. AWSManagedServices-DescribeScheduleOrPeriods で AWS Systems Manager オートメーションドキュメントを表示します (オンボーディングされたリージョンを選択する必要がある場合があります )。

2. パラメータの値を指定します。

3. 実行 をクリックし、自動化が完了するまで待ちます。

## AMS Resource Scheduler のリソースのタグ付け

AMS Resource Scheduler のリソースのタグ付け。

スケジュールと期間を AMS Resource Schedule に追加したら、Resource Scheduler タグ名をタグキーとして、またはカスタマイズしたタグ名をタグ値としてリソースにタグ付けする必要があります。AMS Accelerate アカウントのリソースにタグを付ける方法の詳細については、「」を参照してくださいAMS Accelerate でのタグ付け。

> **Note**
>
> Resource Tagger を使用してリソースにタグを付ける場合、Resource Scheduler のデフォルトのタグキーは、リソースタグガーによって適用される`ams:rt:`すべてのタグにキープレフィックス " があるため、プレフィックス 'ams:rt:' を持つようにカスタマイズする必要があります。それ以外の場合、リソースタガーでタグ付けされたリソースは Resource Scheduler によって管理されません。Resource Scheduler のデフォルトのタグキーのカスタマイズの詳細については、「」を参照してくださいAMS リソーススケジューラのカスタマイズ。

## AMS Resource Scheduler のコスト推定器

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 Amazon 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、その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 24x0.125 = 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」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、そのデータが使用可能になると、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。

> **Note**
>
> 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。

## AMS Resource Scheduler のアラームサプレッサー

AMS Resource Scheduler には CloudWatch アラームサプレッサーが付属しており、Elastic Load Balancing、Application Load Balancer、または Network Load Balancer の背後にあるインスタンスのアラームAMSAlarmSuppressorを抑制する という名前の個別の Lambda 関数としてデプロイされます。関数は 5 分ごとに実行され、アカウントに存在するすべてのアラームを取得し、名前空間に基づいてグループ化します。たとえば、AWS/ELB、AWS/ApplicationELB、AWS/NetworkELB。サプレッサーがアラームディメンションからロードバランサー名やターゲットグルー

プ (ALB/NLB の場合) を検出し、ロードバランサーやターゲットグループに登録されているインスタンスを検索し、インスタンスの状態をチェックして、インスタンスが AMS Resource Scheduler によってスケジュールされているかどうかを確認します。インスタンスが Resource Scheduler によってスケジュールされ、Resource Scheduler によって停止された場合、サプレッサーはアラームをマークして無効にします。登録されたインスタンスリストの少なくとも 1 つのインスタンスが実行されている場合、サプレッサーは対応するアラームをマークして、有効とマークされたアラームを有効にし、無効とマークされたアラームを無効にします。このログは`/aws/lambda/AMSAlarmSuppressor`グループに保存されます。

# AMS Accelerate でのログ管理

AMS Accelerate は、ログを収集するためにサポートされている AWS サービスを設定します。これらのログは、アカウント内のリソースのコンプライアンスと監査を確保するために AMS Accelerate によって使用されます。

AMS Accelerate は、AWS での運用上の優秀性の実現に役立つさまざまな運用サービスを提供します。24 時間 365 日体制のヘルプデスク、プロアクティブモニタリング、セキュリティ、パッチ適用、ログ記録、バックアップなど、いくつかの主要な運用機能を使用して、AMS が AWS クラウドで全体的な運用上の優秀性を達成するのに役立つ方法をすばやく理解するには、「AMS リファレンスアーキテクチャ図」を参照してください。

トピック

- ログ管理 — AWS CloudTrail
- ログ管理 — Amazon EC2
- ログ管理 — Amazon VPC フローログ

## ログ管理 — AWS CloudTrail

AWS CloudTrail は、コンプライアンス、運用監査、リスク監査など、アカウントガバナンスに使用されるサービスです。CloudTrail を使用すると、 AWS インフラストラクチャ全体のアクションに関連するアカウントアクティビティをログに記録し、継続的にモニタリングし、保持できます。

AMS Accelerate では、アカウント内のすべてのリソースの監査とコンプライアンスを管理するための AWS CloudTrail ログ記録が必要です。オンボーディング中に、次のいずれかのオプションを選択できます。

- AMS がデプロイした証跡: このオプションを選択すると、AMS はアカウント内の既存の証跡とは無関係に、プライマリ AWS リージョンで CloudTrail マルチリージョン証跡を作成、デプロイ、管理します。
- 独自の証跡を作成する: 独自のアカウントまたは組織の CloudTrail 証跡を提供することを選択した場合は、Cloud Architect (CA) と協力して、Accelerate に必要な設定を満たしていることを確認する必要があります。このオプションを選択しても独自の証跡を提供しない場合、 Accelerate は独自の CloudTrail 証跡を自動的にデプロイして、継続的なセキュリティと監査カバレッジを維持します。後で独自の証跡を指定すると、AMS は冗長性と追加コストを回避するためにデプロイされ

た証跡を削除します。このアプローチは、アカウントで 1 つのアクティブな CloudTrail 証跡を維持し、重複するログ記録コストを防ぐのに役立ちます。

> **Note**
>
> アカウントに既存の CloudTrail 証跡があり、オンボーディング中に AMS マネージド証跡を特別に設定またはリクエストしていない場合、AMS Accelerate はアカウントから AMS デプロイされた証跡を自動的に削除します。これにより、ログ記録の重複を防ぎ、リソースの使用量を最適化し、追加コストを節約できます。

AMS Accelerate は、イベント配信先として Accelerate がデプロイした CloudTrail 証跡用の Amazon S3 バケットを作成し、 AWS Key Management Service （ AWS KMS) 暗号化を使用します。CloudTrail 証跡イベントは、調査と診断の目的で AMS Accelerate オペレーターによってアクセスされます。アカウントに既存の CloudTrail 証跡がすでに有効になっている場合、オンボーディング中に Accelerate に Accelerate マネージド証跡をデプロイさせることを選択した場合、この証跡はそれに追加されます。

AMS Accelerate は、デプロイされた CloudTrail 証跡の高速化など、CloudTrail アカウントの証跡が正しく設定および暗号化されるように AWS Config ルールをデプロイします。詳細についてはAWS Configを参照してください。これらは使用されるルールであり、それらを説明する AWS ドキュメントへのリンクとして表示されます。

- multi-region-cloudtrail-enabled。AMS Accelerate CloudTrail が正しく設定されていることを確認します。
- cloud-trail-encryption-enabled。 AWS KMS カスタマーマスターキー (CMK) 暗号化でサーバー側の暗号化 (SSE) を使用するよう AWS CloudTrail に設定されている をチェックします。
- cloud-trail-log-file-validation-enabled。有効にすると、 が AWS CloudTrail ログを含む署名付きダイジェストファイルを作成することを確認します。すべての証跡でファイル検証を有効にすることを強くお勧めします。
- s3-bucket-default-lock-enabled。有効にすると、Amazon S3 バケットでロックが有効になっていることを確認します。
- s3-bucket-logging-enabled。有効にすると、Amazon S3 バケットのログ記録が有効になっているかどうかを確認します。

AMS Accelerate は、 AWS KMS を使用して、アカウントにデプロイされた Accelerate の CloudTrail 証跡のログイベントを暗号化します。このキーは、アカウント管理者、AMS Accelerate オペレーター、および CloudTrail によって制御され、アクセスできます。詳細については AWS KMS、「AWS Key Management Service の機能の製品ドキュメント」を参照してください。

## CloudTrail ログへのアクセスと監査

AMS Accelerate がデプロイした CloudTrail 証跡の CloudTrail ログは、アカウント内の Amazon S3 バケットに保存されます。Amazon S3 バケットに保存されている証跡データは、CloudTrail リソースのプロビジョニング時に作成された AWS KMS キーを使用して暗号化されます。

Amazon S3 バケットは、ams-*aaws ##### id*-cloudtrail-*AWS #####* (例: ams-a123456789-cloudtrail-us-east-1a) の命名パターンを活用し、すべてのイベントは AWS/CloudTrail プレフィックスとともに保存されます。プライマリバケットへのすべてのアクセスはログに記録され、ログオブジェクトは監査目的で暗号化およびバージョニングされます。

変更の追跡とログのクエリの詳細については、「」を参照してくださいAMS Accelerate アカウントの変更の追跡。

## CloudTrail ログの保護と保持

AMS Accelerate では、デプロイされた CloudTrail 証跡 Accelerate のガバナンスモードで Amazon S3 オブジェクトをロックできるため、ユーザーは特別なアクセス許可なしでオブジェクトバージョンを上書きまたは削除したり、ロック設定を変更したりすることはできません。詳細については、Amazon S3 オブジェクトロック」を参照してください。

デフォルトでは、このバケット内のすべてのログは無期限に保持されます。保持期間を変更する場合は、 AWS サポート センターを通じてサービスリクエストを送信して、別の保持ポリシーを設定できます。

## Amazon EC2 ログへのアクセス

を使用して Amazon EC2 インスタンスログにアクセスできます AWS マネジメントコンソール。インスタンスと AWS サービスによって生成されたログはCloudWatch Logs で入手できます。CloudWatch Logs は、AMS Accelerate によって管理される各アカウントで利用できます。ログへのアクセスの詳細については、CloudWatch Logs ドキュメントを参照してください。

## Amazon EC2 ログの保持

Amazon EC2 インスタンスログは、デフォルトで無期限に保持されます。保持期間を変更する場合は、 AWS サポート センターを通じてサービスリクエストを送信して、別の保持ポリシーを設定できます。

# ログ管理 — Amazon EC2

AMS Accelerate は、AMS Accelerate マネージドとして識別したすべての Amazon EC2 インスタンスに CloudWatch エージェントをインストールします。このエージェントは、システムレベルのログを Amazon CloudWatch Logs に送信します。詳細については、Amazon CloudWatch Logs とは」を参照してください。

次のログファイルは、ログと同じ名前のロググループに CloudWatch Logs に送信されます。各ロググループ内で、Amazon EC2 インスタンス ID に従って という名前のログストリームが各 Amazon EC2 インスタンスに作成されます。

Linux

- /var/log/amazon/ssm/amazon-ssm-agent.log
- /var/log/amazon/ssm/errors.log
- /var/log/audit/audit.log
- /var/log/auth.log
- /var/log/cloud-init-output.log
- /var/log/cron
- /var/log/dnf.log
- /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

詳細については、CloudWatch エージェント設定ファイルを手動で作成または編集する」を参照してください。

Windows

- AmazonSSMAgentLog
- AmazonCloudWatchAgentLog
- AmazonSSMErrorLog
- AmazonCloudFormationLog
- ApplicationEventLog
- EC2ConfigServiceEventLog
- MicrosoftWindowsAppLockerEXEAndDLLEventLog
- MicrosoftWindowsAppLockerMSIAndScriptEventLog
- MicrosoftWindowsGroupPolicyOperationalEventLog
- SecurityEventLog
- SystemEventLog

詳細については、「クイックスタート: Windows Server 2016 を実行している Amazon EC2 インスタンスが CloudWatch Logs エージェントを使用して CloudWatch Logs にログを送信できるようにする」を参照してください。

# ログ管理 — Amazon VPC フローログ

VPC フローログは、VPC 内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をキャプチャする機能です。フローログデータは、Amazon CloudWatch logsまたは Amazon S3 に発行できます。フローログデータ収集は、ネットワークのスループットやレイテンシーには影響しません。ネットワークパフォーマンスに影響を与えることなく、フローログを作成または削除できます。

フローログは、以下のような多くのタスクに役立ちます。

- 過度に制限されたセキュリティグループルールの診断
- インスタンスに到達するトラフィックのモニタリング
- ネットワークインターフェイスに出入りするトラフィックの方向を決定する

Accelerate アカウントで新しく作成された VPC ごとに VPC フローログを有効にする必要はありません。AMS は、ams-nist-cis-vpc-flow-logs-enabled Config ルールを使用して、VPC にフローログがあるかどうかを自動的に検出します。VPC フローログが有効になっていない場合、AMS はカスタムフィールドで VPC フローログを作成して自動的に修正します。これらの追加フィールドを使用すると、AMS とお客様は VPC トラフィックのモニタリング、ネットワークの依存関係の把握、ネットワーク接続の問題のトラブルシューティング、ネットワークの脅威の特定を行うことができます。

フローログの表示と検索については、「フローログの操作」を参照してください。

# AMS Accelerate アカウントの変更の追跡

**Important**

Change Record サービスは、2025 年 7 月 1 日をもって廃止されました。
新しいアカウントを Change Record サービスにオンボーディングすることはできません。
AMS Accelerate アカウントの CloudTrail データをクエリするには、次のサービスを使用できます。

- で AWS CloudTrail、イベント履歴を選択し、ルックアップ属性を使用してイベントをフィルタリングします。時間範囲フィルターを使用して、`s3.amazon.aws.com`指定したイベントソースでイベント履歴をフィルタリングするか、ユーザー名でイベント履歴をフィルタリングするかを選択できます。詳細については、CloudTrail イベント履歴の使用」を参照してください。
- AWS CloudTrail Lake を使用して、クエリを通じてデータを収集します。Lake AWS CloudTrail を選択し、Query を選択します。独自のクエリを作成したり、クエリジェネレーターを使用したり、サンプルクエリを使用してイベントベースのデータを収集したりできます。例えば、先週 Amazon EC2 インスタンスを削除したユーザーを尋ねることができます。詳細については、AWS CloudTrail 「ソースからデータレイクを作成する」およびCloudTrailLake クエリ」を参照してください。
- で Amazon Athena テーブルを作成し AWS CloudTrail 、ストレージの場所を証跡に関連付けられた Amazon S3 バケットとして設定します。証跡のホームリージョンと Amazon S3 バケットが同じであることを確認します。Amazon Athena では、クエリエディタを使用して、Athena コンソールで使用するために Accelerate が提供するデフォルトのクエリを実行します。への Athena テーブルを作成して CloudTrail ログをクエリする方法の詳細については、「クエリ AWS CloudTrail ログ」を参照してください。

トピック


- 変更レコードの表示
- デフォルトクエリ
- レコードのアクセス許可を変更する

AWS Managed Services は、Amazon Athena (Athena) コンソールと AMS Accelerate ログ管理を使用してクエリ可能なインターフェイスを提供することで、AMS Accelerate Operations チームおよび AMS Accelerate Automation による変更を追跡するのに役立ちます。

Athena は、標準の構造化クエリ言語 (SQL) を使用して Amazon S3 内のデータを分析するために使用できるインタラクティブなクエリサービスです (Amazon Athena の SQL リファレンスを参照 ) 。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。AMS Accelerate は、CloudTrail ログを介して毎日のパーティションを持つ Athena テーブルを作成し、プライマリ AWS リージョンと ams-change-record ワークグループ内でクエリを提供します。デフォルトのクエリのいずれかを選択し、必要に応じて実行できます。Athena ワークグループの詳細については、「ワークグループの仕組み」を参照してください。

> **Note**
>
> Accelerate が CloudTrail Organization 証跡と統合されている場合、Athena を使用して Accelerate アカウントの CloudTrail イベントをクエリできるのは Accelerate のみです。ただし、オンボーディング中に Athena を使用してアカウント内の CloudTrail イベントをクエリおよび分析するための IAM ロールを Organization 管理者がデプロイした場合を除きます。

変更レコードを使用すると、次のような質問に簡単に回答できます。

- アカウントにアクセスしたユーザー (AMS Accelerate Systems または AMS Accelerate Operators)
- アカウントで AMS Accelerate によってどのような変更が行われたか
- AMS Accelerate がアカウントで変更を実行したのはいつですか
- アカウントで行われた変更を表示する場所
- AMS Accelerate がアカウントに変更を加える必要があった理由
- クエリを変更して、AMS 以外の変更に対するすべての質問に対する回答を取得する方法

# 変更レコードの表示

Athena クエリを使用するには、 AWS マネジメントコンソールにサインインし、プライマリ AWS リージョンの Athena コンソールに移動します。

> **Note**
>
> いずれかのステップの実行中に Amazon Athena の開始方法ページが表示された場合は、開始方法 をクリックします。これは、変更レコードインフラストラクチャがすでに配置されている場合でも表示されることがあります。

1. Athena コンソールの上部ナビゲーションパネルからワークグループを選択します。
2. ams-change-record ワークグループを選択し、ワークグループの切り替えをクリックします。
3. データベースコンボボックスから ams-change-record-database を選択します。ams-change-record-database には、ams-change-record-table テーブルが含まれています。
4. 上部のナビゲーションパネルから保存されたクエリを選択します。
5. 保存済みクエリウィンドウには、AMS Accelerate が提供するクエリのリストが表示され、これを実行できます。保存済みクエリリストから実行するクエリを選択します。例えば、ams_session_accesses_v1 クエリなどです。

   プリセット AMS Accelerate クエリの完全なリストについては、「」を参照してくださいデフォルトクエリ。
6. 必要に応じてクエリエディタボックスの日時フィルターを調整します。デフォルトでは、クエリは最終日からの変更のみをチェックします。
7. [Run query] (クエリの実行) を選択します。

# デフォルトクエリ

AMS Accelerate には、Athena コンソールで使用できるデフォルトのクエリがいくつか用意されています。デフォルトのクエリを次の表に示します。

> **Note**
>
> - すべてのクエリは、日時範囲をオプションのフィルターとして受け入れます。すべてのクエリは、デフォルトで過去 24 時間にわたって実行されます。予想される入力については、次のサブセクション「」を参照してくださいクエリでの日時フィルターの変更。
> - 変更できる、または変更する必要があるパラメータ入力は、角括弧付きの *<PARAMETER_NAME>* としてクエリに表示されます。プレースホルダーと角括弧をパラメータ値に置き換えます。

- すべてのフィルターはオプションです。クエリでは、一部のオプションのフィルターが行の先頭に二重ダッシュ (--) でコメントアウトされます。すべてのクエリは、デフォルトのパラメータを使用して、それらなしで実行されます。これらのオプションのフィルターにパラメータ値を指定する場合は、行の先頭にある二重ダッシュ (--) を削除し、必要に応じて パラメータを置き換えます。
- すべてのクエリは出力IAM SessionIdで IAM PincipalIdと を返します。
- クエリを実行するための計算コストは、アカウントに対して生成される CloudTrail ログの数によって異なります。コストを計算するには、AWS Athena 料金計算ツールを使用します。

既定クエリ

| 目的/説明 | 入力 | 出力 |
|---|---|---|
| クエリ名: ams_access_session_query_v1 | | |
| AMS Accelerate アクセスセッションの追跡<br><br>特定の AMS Accelerate アクセスセッションに関する情報を提供します。クエリは IAM プリンシパル ID をオプションのフィルターとして受け入れ、イベント時間、アカウントへのアクセスのビジネスニーズ、リクエスタなどを返します。<br><br>行のコメントを解除し、プレースホルダー IAM PrincipalId *######### ### ID ######### #### IAM Principal Id* プリンシパル ID を | ( オプション) IAM PrincipalId ：アクセスしようとしているリソースの IAM プリンシパル識別子。形式は *UNIQUE_ID ENTIFIER* ：*RESOURCE_NAME* です。詳細については、「一意の識別子」を参照してください。このフィルターなしでクエリを実行して、 でフィルタリングする正確な IAM PrincipalId を決定できます。 | • EventTime: アクセスを取得する時刻<br>• EventName: AWS イベント名 (AssumeRole)<br>• EventRegion: リクエストを取得する AWS リージョン<br>• EventId: CloudTrail イベント ID<br>• BusinessNeed タイプ: アカウントにアクセスするためのビジネス上の理由タイプ。使用できる値は、SupportCase、OpsItem、Issue、Text です。<br>• BusinessNeed: ビジネスはアカウントにアクセスする必要があります。例えば、Support Case ID、Ops Item ID などです。<br>• リクエスタ: アカウントにアクセスするオペレーター ID、またはアカウントにアクセスするオートメーションシステム。 |

| 目的/説明 | 入力 | 出力 |
| --- | --- | --- |
| フィルタリングできます。<br><br>クエリの WHERE 句の useragent フィルターラインを削除して、AMS 以外のアクセスセッションを一覧表示することもできます。 | | • RequestAccessType: リクエスタタイプ (System、OpsConsole、OpsAPI、Unset) |
| クエリ名: ams_events_query_v1 | | |
| AMS Accelerate によって行われたすべての変更アクションを追跡する<br><br>AMS Accelerate ロールフィルターを使用してアカウントで実行されたすべての書き込みアクションを返します。<br><br>また、クエリの WHERE 句から useridentity.arn フィルター行を削除することで、非 AMS ロールによって実行された変更アクションを追跡することもできます。 | (オプション)<br><br>日時範囲のみ。「クエリでの日時フィルターの変更」を参照してください。 | • AccountId: AWS アカウント ID<br>• RoleArn: リクエスタの RoleArn<br>• EventTime: アクセスを取得する時刻<br>• EventName: AWS イベント名 (AssumeRole)<br>• EventRegion: リクエストを取得する AWS リージョン<br>• EventId: CloudTrail イベント ID<br>• RequestParameters : リクエストのリクエストパラメータ<br>• ResponseElements: レスポンスのレスポンス要素。<br>• UserAgent: AWS CloudTrail ユーザーエージェント |
| クエリ名: ams_instance_access_sessions_query_v1 | | |

| 目的/説明 | 入力 | 出力 |
| --- | --- | --- |
| AMS Accelerate によるインスタンスアクセスの追跡<br><br>AMS Accelerate インスタンスアクセスのリストを返します。すべてのレコードには、イベント時間、イベントリージョン、インスタンス ID、IAM プリンシパル ID、IAM セッション ID、SSM セッション ID が含まれます。IAM プリンシパル ID を使用して、Athena `ams_access_sessions_query_v1` クエリを使用してインスタンスにアクセスするためのビジネスニーズの詳細を取得できます。SSM セッション ID を使用して、セッションの開始時刻と終了時刻、ログの詳細、インスタンスの AWS リージョンの AWS Session Manager コンソールの使用など、インスタンスアクセスセッションの詳細を取得できます。<br><br>ユーザーは、クエリの WHERE 句のユーザー ID フィルター行を削除し | `datetime range` のみ。「クエリでの日時フィルターの変更」を参照してください。 | • InstanceId: インスタンス ID<br>• SSMSession ID: SSM セッション ID<br>• RoleArn: リクエスタの RoleArn<br>• EventTime: アクセスを取得する時刻<br>• EventName: AWS イベント名 (AssumeRole)<br>• EventRegion: リクエストを取得する AWS リージョン<br>• EventId: CloudTrail イベント ID |

| 目的/説明 | 入力 | 出力 |
| --- | --- | --- |
| て、AMS 以外のインスタンスアクセスを一覧表示することもできます。 | | |

クエリ名: ams_privilege_escalation_events_query_v1

| 目的/説明 | 入力 | 出力 |
| --- | --- | --- |
| AMS ユーザーと非 AMS ユーザーのアクセス許可 (エスカレーション) イベントを追跡する<br><br>直接、または特権エスカレーションにつながる可能性のあるイベントのリストを提供します。クエリは、オプションのフィルターとして ActionedBy を受け入れ、EventName、EventId、EventTime などを返します。イベントに関連付けられたすべてのフィールドも返されます。そのイベントに該当しない場合、フィールドは空白になります。ActionedBy フィルターはデフォルトで無効になっています。有効にするには、その行から「--」を削除します。<br><br>デフォルトでは、ActionedBy フィルターは無効になっています (すべてのユーザーからの特権エスカレーションイベントが表示されます )。特定のユーザーまたはロールのイベントを表示するには、WH | ( オプション) `ACTIONEDBY_PUT_USER_NAME` : actionedBy ユーザーのユーザー名。これは IAM ロールまたはユーザーのいずれかです。例えば、ams-access-admin です。<br><br>( オプション) `datetime range`。「クエリでの日時フィルターの変更」を参照してください。 | • AccountId: アカウント ID<br>• ActionedBy: ActionedBy ユーザー名<br>• EventTime: アクセスを取得する時刻<br>• EventName: AWS イベント名 (AssumeRole)。<br>• EventRegion: リクエストを取得する AWS リージョン<br>• EventId: CloudTrail イベント ID |

| 目的/説明 | 入力 | 出力 |
| --- | --- | --- |
| ERE 句のユーザー ID フィルターラインから二重ダッシュ (--) を削除し、プレースホルダー *ACTIONEDBY_PUT_USER_NAME_HERE* を IAM ユーザーまたはロール名に置き換えます。フィルターなしでクエリを実行して、フィルタリングする正確なユーザーを決定できます。 | | |
| クエリ名: ams_resource_events_query_v1 | | |
| 特定のリソース AMS または非 AMS の書き込みイベントを追跡する<br><br>特定のリソースで実行されたイベントのリストを提供します。クエリは、フィルターの一部としてリソース ID を受け入れ (クエリの WHERE 句でプレースホルダー *RESOURCE_INFO* を置き換える )、そのリソースに対して実行されたすべての書き込みアクションを返します。 | ( 必須) RESOURCE_INFO ：リソース識別子は、アカウント内の任意の AWS リソースの ID にすることができます。これをリソース ARNs と混同しないでください。たとえば、EC2 インスタンスのインスタンス ID、DynamoDB テーブルのテーブル名、CloudWatch Log の logGroupName などです。<br><br>( オプション) datetime range。「クエリでの日時フィルターの変更」を参照してください。 | • AccountId: アカウント ID<br>• ActionedBy: ActionedBy ユーザー名<br>• EventTime: アクセスを取得する時刻<br>• EventName: AWS イベント名 (AssumeRole)。<br>• EventRegion: リクエストを取得する AWS リージョン<br>• EventId: CloudTrail イベント ID |
| クエリ名: ams_session_events_query_v1 | | |

| 目的/説明 | 入力 | 出力 |
| --- | --- | --- |
| 特定のセッション中に AMS Accelerate によって実行された書き込みアクションを追跡する<br><br>特定のセッションで実行されたイベントのリストを提供します。クエリは、フィルターの一部として IAM プリンシパル ID を受け入れ (クエリの WHERE 句でプレースホルダー *PRINCIPAL_ID* を置き換える )、そのリソースに対して実行されたすべての書き込みアクションを返します。 | ( 必須) PRINCIPAL_ID ：セッションのプリンシパル ID。形式は *UNIQUE_ID ENTIFIER* ：*RESOURCE_NAME* です。詳細については、「一意の識別子」を参照してください。クエリ「ams_session_ids_by_requester_v1IDs のリストを取得できます。このフィルターなしでクエリを実行して、フィルタリングする正確な IAM PrincipalId を決定することもできます。<br><br>( オプション) datetime range。「クエリでの日時フィルターの変更」を参照してください。 | • AccountId: アカウント ID<br>• ActionedBy: ActionedBy ユーザー名<br>• EventTime: アクセスを取得する時刻<br>• EventName: AWS イベント名 (AssumeRole)<br>• EventRegion: リクエストを取得する AWS リージョン<br>• EventId: CloudTrail イベント ID |
| クエリ名: ams_session_ids_by_requester_v1 | | |

| 目的/説明 | 入力 | 出力 |
| --- | --- | --- |
| 特定のリクエスタの IAM プリンシパル/セッション IDs を追跡します。<br><br>クエリは「リクエスタ」を受け入れ (クエリの WHERE 句でプレースホルダー#####を置き換える )、指定された時間範囲内でリクエスタによってすべての IAM プリンシパル ID を返します。 | ( 必須) `Requester` : アカウントにアクセスするオペレータ ID (オペレータのエイリアスなど )、またはアカウントにアクセスするオートメーションシステム (OsConfiguration、AlarmManager など )。<br><br>( オプション) `datetime range`。「クエリでの日時フィルターの変更」を参照してください。 | • IAM PrincipalId - セッションの IAM プリンシパル ID。形式は *UNIQUE_ID ENTIFIER* : *RESOURCE_NAME* です。詳細については、「一意の識別子」を参照してください。このフィルターなしでクエリを実行して、フィルタリングする正確な IAM PrincipalId を決定できます。<br>• IAM SessionId - アクセスセッションの IAM セッション ID<br>• EventTime: アクセスを取得する時刻 |

## クエリでの日時フィルターの変更

すべてのクエリは、日時範囲をオプションのフィルターとして受け入れます。デフォルトでは、すべてのクエリは過去 1 日間に実行されます。

日時フィールドに使用される形式は yyyy/MM/dd (例: 2021/01/01) です。タイムスタンプ全体ではなく、日付のみを保存することに注意してください。タイムスタンプ全体については、フィールド eventime を使用します。このフィールドには、ISO 8601 形式 yyyy-MM-ddT HH:mm:ssZ (例: 2021-01-01T23:59:59Z) でタイムスタンプが格納されます。ただし、テーブルは日時フィールドでパーティション化されているため、日時フィルターとイベント時フィルターの両方をクエリに渡す必要があります。次の 例を参照してください。

> **Note**
>
> 範囲を変更できる受け入れられたすべての方法を確認するには、日付と時刻の関数と演算子に現在使用されている Athena エンジンバージョンに基づく最新の Presto 関数ドキュメントを参照して、範囲を変更できる受け入れられたすべての方法を確認してください。

日付レベル: 過去 1 日または過去 24 時間 (デフォルト ) の例: CURRENT_DATE='2021/01/01' の場合、フィルターは現在の日付から 1 日を引いて日時 > '2020/12/31' としてフォーマットします

```
datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
```

日付レベル: 過去 2 か月の例 :

```
datetime > date_format(date_add('month', - 2, CURRENT_DATE), '%Y/%m/%d')
```

日付レベル: 2 つの日付の間の例 :

```
datetime > '2021/01/01'
      AND
      datetime < '2021/01/10'
```

タイムスタンプレベル: 過去 12 時間の例 :

過去 1 日にスキャンされたデータをパーティション化し、過去 12 時間以内にすべてのイベントをフィルタリングする

```
datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND
      eventtime > date_format(date_add('hour', - 12, CURRENT_TIMESTAMP), '%Y-%m-%dT%H:
%i:%sZ')
```

タイムスタンプレベル: 2 つのタイムスタンプの間の例 :

2021 年 1 月 1 日午後 12 時 ~ 2021 年 1 月 10 日午後 3 時の間にイベントを取得します。

```
datetime > '2021/01/01' AND datetime < '2021/01/10'
      AND
      eventtime > '2021-01-01T12:00:00Z' AND eventtime < '2021-01-10T15:00:00Z'
```

# デフォルトのクエリ例

### ams_access_session_query_v1

```
Name: ams_access_session_query_v1

Description: >-
   The query provides more information on specific AMS access session.
```

```
    The query accepts IAM Principal Id as an optional filter and returns event time,
  business need for accessing the account, requester, ... etc.
    By default; the query filter last day events only, the user can change the datetime
  filter to search for more wide time range.
    By default; the IAM PrincipalId filter is disabled. To enable it, remove "-- " from
  that line.

AthenaQueryString: |-
    /*
      The query provides list of AMS access sessions during specific time range.
      The query accepts IAM Principal Id as an optional filter and returns event time,
  business need for accessing the account, requester, ... etc.

      By default, the query filters the last day's events only; you can change the
  "datetime" filter to search for a wider time range.

      By default; the IAM Principal ID filter is disabled (it shows access sessions for
  all IAM principals).
      If you want to only show access sessions for a particular IAM principal ID, remove
  the double-dash (--) from
      the "IAM Principal ID" filter line in the WHERE clause of the query, and replace
  the placeholder "<IAM PrincipalId>" with the specific ID that you want.
      You can run the query without the filter to determine the exact IAM PrincipalId
  you want to filter with.

      By default; the query only shows AMS access sessions. If you also want to show
  non-AMS access sessions,
      remove the "useragent" filter in the WHERE clause of the query.

      For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
  in your AMS Accelerate accounts -> Default Queries
    */

    SELECT
       json_extract_scalar(responseelements, '$.assumedRoleUser.assumedRoleId') AS "IAM
  PrincipalId",
       json_extract_scalar(responseelements, '$.credentials.accessKeyId') AS "IAM
  SessionId",
       eventtime AS "EventTime",
       eventname AS "EventName",
       awsregion AS "EventRegion",
       eventid AS "EventId",
       json_extract_scalar(requestparameters, '$.tags[0].value') AS "BusinessNeed",
       json_extract_scalar(requestparameters, '$.tags[1].value') AS "BusinessNeedType",
```

```
      json_extract_scalar(requestparameters, '$.tags[2].value') AS "Requester",
      json_extract_scalar(requestparameters, '$.tags[3].value') AS "AccessRequestType"
   FROM
       "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
   WHERE
      datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND eventname = 'AssumeRole'
      AND useragent = 'access.managedservices.amazonaws.com'
      -- AND  json_extract_scalar(responseelements, '$.assumedRoleUser.assumedRoleId')
 = '<IAM PrincipalId>'
   ORDER BY eventtime

InsightsQueryString: |-
   # The query provides list of AMS access sessions during specific time range.
   # The query accepts IAM Principal Id as an optional filter and returns event time,
 business need for accessing the account, requester, ... etc.
   #
   # By default; the IAM Principal ID filter is disabled (it shows access sessions for
 all IAM principals).
   # If you want to only show access sessions for a particular IAM principal ID, remove
 the # (#) from
   # the "IAM Principal ID" filter of the query, and replace the placeholder "<IAM
 PrincipalId>" with the specific ID that you want.
   # You can run the query without the filter to determine the exact IAM PrincipalId
 you want to filter with.
   #
   # By default; the query only shows AMS access sessions. If you also want to show
 non-AMS access sessions,
   # remove the "useragent" filter from the query.
   #
   # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries

   filter eventName="AssumeRole" AND userAgent="access.managedservices.amazonaws.com"
   # | filter responseElements.assumedRoleUser.assumedRoleId= "<IAM PrincipalId>"
   | sort eventTime desc
   | fields
      responseElements.assumedRoleUser.assumedRoleId as IAMPrincipalId,
      responseElements.credentials.accessKeyId as IAMSessionId,
      eventTime as EventTime,
      eventName as EventName,
      awsRegion as EventRegion,
      eventID as EventId,
      requestParameters.tags.0.value as BusinessNeed,
```

```
      requestParameters.tags.1.value as BusinessNeedType,
      requestParameters.tags.2.value as Requester,
      requestParameters.tags.3.value as AccessRequestType
```

### ams_events_query_v1

```
ams_events_query_v1.yaml
/*
  The query provides list of events to track write actions for all AMS changes.
  The query returns all write actions done on the account using that AMS role filter.

  By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

  You can also track mutating actions done by non-AMS roles by removing the
 "useridentity.arn" filter lines from the WHERE clause of the query.

  For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes in
 your AMS Accelerate accounts -> Default Queries
*/

SELECT
   useridentity.principalId AS "IAM PrincipalId",
   useridentity.accesskeyid AS "IAM SessionId",
   useridentity.accountid AS "AccountId",
   useridentity.arn AS "RoleArn",
   eventid AS "EventId",
   eventname AS "EventName",
   awsregion AS "EventRegion",
   eventsource AS "EventService",
   eventtime AS "EventTime",
   requestparameters As "RequestParameters",
   responseelements AS "ResponseElements",
   useragent AS "UserAgent"
FROM
   "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
WHERE
   readonly <> 'true'
   AND
   (
      LOWER(useridentity.arn) LIKE '%/ams%'
      OR LOWER(useridentity.arn) LIKE '%/customer_ssm_automation_role%'
```

```
   )
ORDER BY eventtime
```

### ams_instance_access_sessions_query_v1

```
ams_instance_access_sessions_query_v1
/*
  The query provides list of AMS Instance accesses during specific time range.

  The query returns the list of AMS instance accesses; every record includes the event
 time, the event AWS Region, the instance ID, the IAM session ID, and the SSM session
 ID.
  You can use the IAM Principal ID to get more details on the business need for
 accessing the instance by using ams_access_session_query_v1 athena query.
  You can use the SSM session ID to get more details on the instance access session,
 including the start and end time of the session and log details, using the AWS Session
 Manager Console in the instance's AWS Region.

  You can also list non-AMS instance accesses by removing the "useridentity" filter
 line in the WHERE clause of the query.

  By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

  For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes in
 your AMS Accelerate accounts -> Default Queries
*/

SELECT
   useridentity.principalId AS "IAM PrincipalId",
   useridentity.accesskeyid AS "IAM SessionId",
   json_extract_scalar(requestparameters, '$.target') AS "InstanceId",
   json_extract_scalar(responseelements, '$.sessionId') AS "SSM SessionId",
   eventname AS "EventName",
   awsregion AS "EventRegion",
   eventid AS "EventId",
   eventsource AS "EventService",
   eventtime AS "EventTime"
FROM
   "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
WHERE
   useridentity.sessionContext.sessionIssuer.arn like '%/ams_%'
   AND eventname = 'StartSession'
```

```
ORDER BY eventtime
```

### ams_privilege_escalation_events_query_v1

```
ams_privilege_escalation_events_query_v1.yaml
/*
  The query provides list of events that can directly or potentially lead to a
 privilege escalation.

  The query accepts ActionedBy as an optional filter and returns EventName, EventId,
 EventTime, ... etc.
  All fields associated with the event are also returned. Some fields are blank if not
 applicable for that event.
  You can use the IAM Session ID to get more details about events happened in that
 session by using ams_session_events_query_v1 query.

  By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

  By default, the ActionedBy filter is disabled (it shows privilege escalation events
 from all users).
  To show events for a particular user or role, remove the double-dash (--) from the
 useridentity filter line in the WHERE clause of the query
  and replace the placeholder "<ACTIONEDBY_PUT_USER_NAME_HERE>" with an IAM user or
 role name.
  You can run the query without the filter to determine the exact user you want to
 filter with.

  For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes in
 your AMS Accelerate accounts -> Default Queries
*/

SELECT
   useridentity.principalId AS "IAM PrincipalId",
   useridentity.accesskeyid AS "IAM SessionId",
   useridentity.accountid AS "AccountId",
   reverse(split_part(reverse(useridentity.arn), ':', 1)) AS "ActionedBy",
   eventname AS "EventName",
   awsregion AS "EventRegion",
   eventid AS "EventId",
   eventtime AS "EventTime",
   json_extract_scalar(requestparameters, '$.userName') AS "UserName",
   json_extract_scalar(requestparameters, '$.roleName') AS "RoleName",
```

```
   json_extract_scalar(requestparameters, '$.groupName') AS "GroupName",
   json_extract_scalar(requestparameters, '$.policyArn') AS "PolicyArn",
   json_extract_scalar(requestparameters, '$.policyName') AS "PolicyName",
   json_extract_scalar(requestparameters, '$.permissionsBoundary') AS
 "PermissionsBoundary",
   json_extract_scalar(requestparameters, '$.instanceProfileName') AS
 "InstanceProfileName",
   json_extract_scalar(requestparameters, '$.openIDConnectProviderArn') AS
 "OpenIDConnectProviderArn",
   json_extract_scalar(requestparameters, '$.serialNumber') AS "SerialNumber",
   json_extract_scalar(requestparameters, '$.serverCertificateName') AS
 "ServerCertificateName",
   json_extract_scalar(requestparameters, '$.accessKeyId') AS "AccessKeyId",
   json_extract_scalar(requestparameters, '$.certificateId') AS "CertificateId",
   json_extract_scalar(requestparameters, '$.newUserName') AS "NewUserName",
   json_extract_scalar(requestparameters, '$.newGroupName') AS "NewGroupName",
   json_extract_scalar(requestparameters, '$.newServerCertificateName') AS
 "NewServerCertificateName",
   json_extract_scalar(requestparameters, '$.name') AS "SAMLProviderName",
   json_extract_scalar(requestparameters, '$.sAMLProviderArn') AS "SAMLProviderArn",
   json_extract_scalar(requestparameters, '$.sSHPublicKeyId') AS "SSHPublicKeyId",
   json_extract_scalar(requestparameters, '$.virtualMFADeviceName') AS
 "VirtualMFADeviceName"
FROM
   "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
WHERE
   (
     -- More event names can be found at https://docs.aws.amazon.com/IAM/latest/
UserGuide/list_identityandaccessmanagement.html
     eventname LIKE 'Add%' OR
     eventname LIKE 'Attach%' OR
     eventname LIKE 'Delete%' AND eventname != 'DeleteAccountAlias' OR
     eventname LIKE 'Detach%' OR
     eventname LIKE 'Create%' AND eventname != 'CreateAccountAlias' OR
     eventname LIKE 'Put%' OR
     eventname LIKE 'Remove%' OR
     eventname LIKE 'Update%' OR
     eventname LIKE 'Upload%' OR
     eventname = 'DeactivateMFADevice' OR
     eventname = 'EnableMFADevice' OR
     eventname = 'ResetServiceSpecificCredential' OR
     eventname = 'SetDefaultPolicyVersion'
   )
   AND eventsource = 'iam.amazonaws.com'
```

```
ORDER BY eventtime
```

### ams_resource_events_query_v1

```
Name: ams_resource_events_query_v1

Description: >-
   The query provides list of events done on specific resource.
   The query accepts resource id as part of the filters, and return all write actions
 done on that resource.
   By default; the query list the accesses for last day, the user can change the time
 range by changing the datetime filter.

AthenaQueryString: |-
   /*
     The query provides list of events done on specific resource.

     The query accepts the resource ID as part of the filters (replace the placeholder
 "<RESOURCE_INFO>" in the WHERE clause of the query),
     and returns all write actions done on that resource. The resource ID can be an ID
 for any AWS resource in the account.
     Example: An instance ID for an EC2 instance, table name for a DynamoDB table,
 logGroupName for a CloudWatch Log, etc.

     By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

     For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
   */

   SELECT
      useridentity.principalId AS "IAM PrincipalId",
      useridentity.accesskeyid AS "IAM SessionId",
      useridentity.accountid AS "AccountId",
      reverse(split_part(reverse(useridentity.arn), ':', 1)) AS "ActionedBy",
      eventname AS "EventName",
      awsregion AS "EventRegion",
      eventid AS "EventId",
      eventsource AS "EventService",
      eventtime AS "EventTime"
   FROM
       "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
```

```
   WHERE
      datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND readonly <> 'true'
      AND
      (
         requestparameters LIKE '%<RESOURCE_INFO>%'
         OR responseelements LIKE '%<RESOURCE_INFO>%'
      )
   ORDER BY eventtime

InsightsQueryString: |-
   # The query provides list of events done on specific resource.
   #
   # The query accepts the resource ID as part of the filters (replace the placeholder
 "<RESOURCE_INFO>" in the filter of the query),
   # and returns all write actions done on that resource. The resource ID can be an ID
 for any AWS resource in the account.
   # Example: An instance ID for an EC2 instance, table name for a DynamoDB table,
 logGroupName for a CloudWatch Log, etc.
   #
   # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries

   filter readOnly=0
   | parse @message '"requestParameters":{*}' as RequestParameters
   | parse @message '"responseElements":{*}' as ResponseElements
   # | filter RequestParameters like "RESOURCE_INFO" or ResponseElements like
 "<RESOURCE_INFO>"
   | fields
      userIdentity.principalId as IAMPrincipalId,
      userIdentity.accessKeyId as IAMSessionId,
      userIdentity.accountId as AccountId,
      userIdentity.arn as ActionedBy,
      eventName as EventName,
      awsRegion as EventRegion,
      eventID as EventId,
      eventSource as EventService,
      eventTime as EventTime
   | display IAMPrincipalId, IAMSessionId, AccountId, ActionedBy, EventName,
 EventRegion, EventId, EventService, EventTime
   | sort eventTime desc
```

### ams_session_events_query_v1

```
Name: ams_session_events_query_v1

Description: >-
   The query provides list of events done on specific session.
   The query accepts IAM Principal Id as part of the filters, and return all write
 actions done on that resource.
   By default; the query list the accesses for last day, the user can change the time
 range by changing the datetime filter.

AthenaQueryString: |-
   /*
     The query provides a list of events executed on a specific session.

     The query accepts the IAM principal ID as part of the filters (replace the
 placeholder "<PRINCIPAL_ID>" in the WHERE clause of the query),
     and returns all write actions done on that resource.

     By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

     For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
   */

   SELECT
      useridentity.principalId AS "IAM PrincipalId",
      useridentity.accesskeyid AS "IAM SessionId",
      useridentity.accountid AS "AccountId",
      reverse(split_part(reverse(useridentity.arn), ':', 1)) AS "ActionedBy",
      eventname AS "EventName",
      awsregion AS "EventRegion",
      eventsource AS "EventService",
      eventtime AS "EventTime",
      requestparameters As "RequestParameters",
      responseelements AS "ResponseElements",
      useragent AS "UserAgent"
   FROM
       "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate   WHERE
      useridentity.principalid = '<PRINCIPAL_ID>'
      AND datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND readonly <> 'true'
   ORDER BY eventtime
```

```
InsightsQueryString: |-
   # The query provides a list of events executed on a specific session.
   #
   # The query accepts the IAM principal ID as part of the filters (replace the
 placeholder "<PRINCIPAL_ID>" in the filter of the query),
   # and returns all write actions done on that resource.
   #
   # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries

   filter readOnly=0 AND userIdentity.principalId = "<IAM Principal>"
   | sort eventTime desc
   | fields
      userIdentity.accessKeyId as IAMSessionId,
      userIdentity.principalId as IAMPrincipalId,
      userIdentity.accountId as AccountId,
      userIdentity.arn as ActionedBy,
      eventName as EventName,
      awsRegion as EventRegion,
      eventSource as EventService,
      eventTime as EventTime,
      userAgent as UserAgent
   | parse @message '"requestParameters":{*}' as RequestParameters
   | parse @message '"responseElements":{*}' as ResponseElements
```

### ams_session_ids_by_requester_v1

```
Name: ams_session_ids_by_requester_v1

Description: >-
   The query provides list of IAM Principal/Session Ids for specific requester.
   The query accepts requester and return all IAM Principal/Session Ids by that
 requester during specific time range.
   By default; the query list the accesses for last day, the user can change the time
 range by changing the datetime filter.

AthenaQueryString: |-
   /*
     The query provides list of IAM Principal IDs for a specific requester.

     The query accepts the requester (replace placeholder "<Requester>" in the WHERE
 clause of the query),
```

```
    and returns all IAM Principal IDs by that requester during a specific time range.

    By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

    For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
  */

  SELECT
     json_extract_scalar(responseelements, '$.assumedRoleUser.assumedRoleId') AS "IAM
 PrincipalId",
     json_extract_scalar(responseelements, '$.credentials.accessKeyId') AS "IAM
 SessionIId",
     eventtime AS "EventTime"
  FROM
      "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
  WHERE
     datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
     AND json_extract_scalar(requestparameters, '$.tags[2].value') = '<Requester>'
  ORDER BY eventtime

InsightsQueryString: |-
  # The query provides list of IAM Principal IDs for a specific requester.
  #
  # The query accepts the requester (replace placeholder "<Requester>" in the filter
 of the query),
  # and returns all IAM Principal IDs by that requester during a specific time range.
  #
  # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
  filter eventName="AssumeRole" AND requestParameters.tags.2.value="<Requester>"
  | sort eventTime desc
  | fields
     responseElements.assumedRoleUser.assumedRoleId as IAMPrincipalId,
     responseElements.credentials.accessKeyId as IAMSessionId,
     eventTime as EventTime
```

# レコードのアクセス許可を変更する

変更レコードクエリを実行するには、次のアクセス許可が必要です。

- Athena

  - athena:GetWorkGroup
  - athena:StartQueryExecution
  - athena:ListDataCatalogs
  - athena:GetQueryExecution
  - athena:GetQueryResults
  - athena:BatchGetNamedQuery
  - athena:ListWorkGroups
  - athena:UpdateWorkGroup
  - athena:GetNamedQuery
  - athena:ListQueryExecutions
  - athena:ListNamedQueries
- AWS KMS
  - kms:Decrypt
  - AWS KMS Accelerate が SSE-KMS 暗号化を使用して CloudTrail AMSCloudTrailLogManagement の AWS KMS キー ID、またはキー ID (複数可 ) 。 Amazon S3
- AWS Glue
  - glue:GetDatabase
  - glue:GetTables
  - glue:GetDatabases
  - glue:GetTable
- Amazon S3 の読み取りアクセス
  - Amazon S3 バケット CloudTrail データストア: ams-a*AccountId*-cloudtrail-*primary region*、または Amazon S3 バケット名、CloudTrail 証跡イベント Amazon S3 バケットデータストア。
- Amazon S3 書き込みアクセス
  - Athena イベントクエリ結果 Amazon S3 バケット: ams-a*AccountId* athena-results-*primary region*

# AWS Systems Manager Accelerate 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 アカウントでのみ共有され、常に予約済みプレフィックス (AWSManagedServices-*) で始まり、Amazon が所有する Systems Manager コンソールに表示されます。SSM ドキュメントの開発と公開の AMS プロセスは AWS のベストプラクティスに従っており、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 の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 Accelerate SSM ドキュメント

AMS Accelerate SSM ドキュメントは、AMS Accelerate 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 Accelerate 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. 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 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 Accelerate 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 Accelerate 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 Accelerate 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 AWS リージョンのドキュメントの更新ごとに増加します。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 Accelerate SSM ドキュメントを比較する場合は、ハッシュを と比較することをお勧めします AWS CLI。

```
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。

## Systems Manager の料金

AMS Accelerate SSM ドキュメントへのアクセスにはコストはかかりません。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 Accelerate ユーザーガイドのドキュメント履歴

次の表に、AMS Accelerate 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。

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| 更新されたログ管理 — AWS CloudTrail セクション | AWS CloudTrail ログ記録に関する新しい情報と注意事項。 | 2025 年 9 月 25 日 |
| 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 | 次のコスト最適化チェックを追加しました。<br>• c1z7kmr00n - インスタンスの Amazon EC2 コスト最適化の推奨事項<br>• c1z7kmr02n - ボリュームの Amazon EBS コスト最適化に関する推奨事項<br>• c1z7kmr03n - DB インスタンスの Amazon RDS コスト最適化の推奨事項<br>• c1z7kmr05n - 関数の AWS Lambda コスト最適化に関する推奨事項 | 2025 年 9 月 22 日 |
| Change Record サービスの廃止に関する注意事項を更新 | 代替ソリューションを使用した変更レコードサービスの非推奨ノートを更新しました。 | 2025 年 9 月 11 日 |
| Trusted Remediator でサポートされている Trusted Advisor セキュリティチェックの更新 | 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 - 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 |

| | | |
|---|---|---|
| Trusted Remediator でサポートされている Trusted Advisor セキュリティチェックの更新 | セキュリティ Trusted Advisor 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 の口グ記録を有効にする必要があります | 2025 年 9 月 5 日 |
| 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 | Trusted Remediator 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 |
| 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 | 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 |
| TOC 用語集リンクを削除しました | AWS 用語集。 | 2025 年 8 月 8 日 |
| TOC 用語集リンクを削除しました | AWS 用語集。 | 2025 年 8 月 8 日 |
| Patch Daily レポートの新しいフィールド | インスタンスタグ: Amazon EC2 インスタンス ID に関連付けられたタグ。 | 2025 年 8 月 8 日 |

| | | |
|---|---|---|
| 新しい信頼された修復者のチェック | Trusted Advisor Trusted Remediator Hs4Ma3G120–AWSManagedServices-TerminateEC2InstanceStoppedForPeriodOfTime、Hs4Ma3G230–AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV2、および c18d2gz150–AWSManagedServices-TerminateEC2InstanceStoppedForPeriodOfTime でサポートされている Trusted Remediator セキュリティチェックでサポートされているコスト最適化チェック。 Trusted Advisor Hs4Ma3G120 AWSManagedServices-TerminateEC2InstanceStoppedForPeriodOfTime Hs4Ma3G230AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV2 AWSManagedServices-TerminateEC2InstanceStoppedForPeriodOfTime | 2025 年 8 月 8 日 |
| ポイント 3.2 での IAM 標準の更新 | 言語を明確にし、タグ付けに関する言及を削除しました。 | 2025 年 7 月 25 日 |
| Accelerate でのリソースタグ設定プロファイルの更新 | Accelerate の Resource Tagger Configuration Profiles に新しい AvailabilityZone フィルターを追加しました。 | 2025 年 7 月 25 日 |

| | | |
|---|---|---|
| Accelerate のインシデントレポート、サービスリクエスト、請求に関する質問を更新しました。 | Plus および Premium サービス階層への参照をサービス SLA へのリンクに置き換えました。 | 2025 年 7 月 25 日 |
| Accelerate のインシデント管理を更新しました。 | オペレーションセンターに関する情報を更新しました。 | 2025 年 7 月 25 日 |
| AMS パターンページを正しいリンクで更新しました。 | SLA と SLO リンクを修正しました。 | 2025 年 7 月 25 日 |
| アラートオプトアウトオプションの更新 | タグを追加すると、追加の 2 つのアラートをオプトアウトできます。 | 2025 年 7 月 25 日 |
| バックアップの新機能 | 新しいタグを使用して、バックアップボールトの通知をカスタマイズします。 | 2025 年 7 月 25 日 |
| Accelerate 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 | Accelerate 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 26 日 |
| Accelerate でのパッチ管理のタグの管理ページを削除 | この機能が廃止されたため、Accelerate でパッチ管理のタグを管理するページを削除しました。 | 2025 年 6 月 19 日 |
| 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。 | AMS Accelerate 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 |

| | | |
|---|---|---|
| AMS Accelerate 変更レコードの廃止。 | AMS Accelerate Change Record サービスは、2025 年 7 月 1 日をもって廃止されます。 | 2025 年 5 月 27 日 |
| サポートされているオペレーティングシステムの更新。 | AMS Accelerate 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 |
| 中東 (UAE) リージョンでサポートされているサービスの注意点。 | 中東 (アラブ首長国連邦) リージョンの一部のサービスに対するサポートが制限されました。 | 2025 年 5 月 22 日 |
| 内部専用 APIs。 | 一部の CloudWatch ログに表示される内部専用 APIs。 | 2025 年 5 月 22 日 |
| 欠落しているログの場所を追加しました。 | 一部の欠落している Windows ログの場所が追加されました。 | 2025 年 5 月 22 日 |
| AMS Accelerate Trusted Remediator の更新。 | 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 |

| | | |
|---|---|---|
| AMS Accelerate Trusted Remediator に関するよくある質問と更新。 | 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。Trusted Advisor「Trusted Remediator でサポートされているチェック」も参照してください。 | 2025 年 5 月 8 日 |
| AMS Accelerate Standard セキュリティコントロールの更新。 | 「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 |
| モニタリングアラートの更新を高速化します。 | 追加のアラートが追加され、アラート名がメモ列に追加されました。 | 2025 年 4 月 28 日 |
| リソースインベントリを高速化します。 | リソースインベントリスプレッドシートファイル (圧縮) が更新されました。 | 2025 年 4 月 24 日 |
| ログの場所を高速化します。 | 追加のログの場所が追加されました。 | 2025 年 4 月 24 日 |
| セキュリティインシデント対応の新しい役割と責任 (RACI) を加速します。 | セキュリティインシデント対応の RACI。 | 2025 年 3 月 27 日 |
| 新しい Amazon RDS 自動修復アラートを高速化します。 | 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 |

| | | |
|---|---|---|
| オンボーディングロールテンプレートの更新を高速化します。 | AMS Accelerate オンボーディングロールテンプレートが更新され、AWS GovCloud リージョンがサポートされました。 | 2025 年 3 月 25 日 |
| 新しい自動修復 RDS アラートを高速化します。 | RDS-EVENT-0224 を追加しました。 | 2025 年 3 月 17 日 |
| 新機能の高速化: インシデント通知。 | 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 |
| RDS アラームモニタリングしきい値の更新を高速化します。 | 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 |
| アラートテーブルの AMS 自動修復の高速化。 | アラート修復テーブルが新しいコンテンツで拡張されました。 | 2025 年 2 月 20 日 |
| Accelerate 新機能: アラームを保持します。 | 自動削除の代わりに CloudWatch でアラームを保持するように Alarm Manager を設定できます。 | 2025 年 2 月 20 日 |

| | | |
|---|---|---|
| 集約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の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。<br>• パッチレポート (毎日 )<br>• バックアップレポート (毎日 )<br>• インシデントレポート (毎週 )<br>• Resource Tagger ダッシュボード<br>• セキュリティ設定ルールダッシュボード | 2025 年 1月 28 日 |

| | | |
|---|---|---|
| Trusted Remediator でサポートされている追加の AWS Trusted Advisor チェックを追加しました | 信頼された修復ツールで次の Trusted Advisor チェックがサポートされるようになりました。<br>• コスト最適化<br>  • c1cj39rr6v - Amazon S3 不完全なマルチパートアップロード中止設定<br>• セキュリティ<br>  • 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<br>  • 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<br>  • Hs4Ma3G272 - ユーザーは SageMaker AI 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<br>  • Hs4Ma3G325 - EKS クラスターでは監査ログ記録を有効にする必要があります<br>  • HHs4Ma3G118 - VPC のデフォルト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 | 2025 年 1月 28 日 |

    - Hs4Ma3G127 - 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
    - Hs4Ma3G124 - 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
- 耐障害性
    - c1qf5bt013 - 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オフになっている
    - 7qGXsKIUw - Classic Load Balancer 接続ドレイン
    - c18d2gz106 - Amazon EBS は AWS Backup プランに含まれていません
    - c18d2gz107 - Amazon DynamoDB テーブルが AWS Backupプランに含まれていない
    - cc18d2gz117 - Amazon EFS AWS Backupプランに含まれていない
    - c18d2gz105 - Network Load Balancer クロスロードバランシング

- c1qf5bt026 - Amazon RDS synchrono us_commit パラメータがオフになっています
- c1qf5bt030 - Amazon RDS innodb_flush_log_at_trx_commit パラメータが 1 ではありません
- c1qf5bt031 - Amazon RDS sync_binlog パラメータがオフになっています
- c1qf5bt036 - Amazon RDS innodb_default_row_format パラメータ設定が安全ではありません
- c18d2gz144 - Amazon EC2 詳細モニタリングが有効ではありません

- 運用上の優秀性
  - c18d2gz125 - Amazon API Gateway が実行ログを記録しない
  - c18d2gz168 - Elastic Load BalancingDeletion Protection Not Enabled for Load Balancer
  - c1qf5bt012 - Amazon RDS Performance Insights はオフになっています

- パフォーマンス
  - c1qf5bt021 - 最適値未満を使用する Amazon RDS

| | | |
|---|---|---|
| | innodb_change_buffering パラメータ<br>• c1qf5bt025 - Amazon RDS autovacuum パラメータがオフになっています<br>• c1qf5bt028 - Amazon RDS enable_indexonlyscan パラメータがオフになっています<br>• c1qf5bt029 - Amazon RDS enable_indexscan パラメータがオフになっています<br>• c1qf5bt032 - Amazon RDS innodb_stats_persistent パラメータがオフになっています<br>• c1qf5bt037 - Amazon RDSgeneral_logging パラメータがオンになっています | |
| 更新されたリソースインベントリスプレッドシート | リソースインベントリスプレッドシートを更新しました。 | 2025年1月23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 |

| | | |
|---|---|---|
| 新しい Accelerate パッチ適用機能: パッチフック | この機能を使用して、パッチ適用の前後にオペレーティングシステムレベルのコマンドを実行するように SSM コマンドドキュメントで「フック」を設定します。 | 2025 年 1 月 16 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 |
| EKS モニタリングとインシデント管理のオンボーディングセクションの更新 | アラートシグナルが中断および再開されるタイミングを明確にするために、オンボーディング手順の注意事項を更新しました。 | 2024 年 12 月 19 日 |
| Trusted Remediator に追加されたメンバーアカウントログ | メンバーアカウントログを使用して、各メンバーアカウントのアカウント ID、オンボーディング AWS リージョン、実行時間を検索できます。 | 2024 年 12 月 19 日 |
| SSM エージェント使用の前提条件 | アウトバウンドトラフィックのブロックに関するコンテンツが更新されます。 | 2024 年 12 月 4 日 |
| EKS の高速モニタリングとインシデント管理がアジアパシフィック (香港) でサポートされるようになりました AWS リージョン | アジアパシフィック (香港) が EKS の高速モニタリングとインシデント管理でサポートされるようになりました | 2024 年 11 月 21 日 |

| | | |
|---|---|---|
| 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。<br>• Microsoft Windows 2016 から Microsoft Windows 2022 以降 | 2024 年 11 月 11 日 |
| EKS の高速モニタリングとインシデント管理がアフリカ (ケープタウン) でサポートされるようになりました AWS リージョン。 | アフリカ (ケープタウン) が EKS の高速モニタリングとインシデント管理でサポートされるようになりました | 2024 年 11 月 4 日 |
| 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。<br>• Microsoft Windows 2012 R2 から Microsoft Windows 2016 以降<br>• Red Hat Enterprise Linux 7 から Red Hat Enterprise Linux 8 へ<br>• Red Hat Enterprise Linux 8 から Red Hat Enterprise Linux 9<br>• Oracle Linux 7 から Oracle Linux 8 へ | 2024 年 11 月 1 日 |
| 更新されたクイックスタートテンプレート | 図、テンプレートパラメータ、および yaml テンプレートファイルを更新しました。 | 2024 年 10 月 28 日 |

| | | |
|---|---|---|
| Trusted Advisor AMS で信頼された修復に追加された チェック | 信頼された修復で次の Trusted Advisor チェックが利用可能になりました。<br>• Z4AUBRNSmz - 関連付けられていない Elastic IP アドレス<br>• c18d2gz128 - 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<br>• c18d2gz138 - DynamoDB Point-in-timeリカバリ<br>• Hs4Ma3G323 - DynamoDBtables では削除保護が有効になっている必要があります<br>• 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<br>• 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<br>• Hs4Ma3G299 - 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<br>• Hs4Ma3G306 - Amazon DocumentDB 手動クラスタースナップショットは公開しないでください<br>• Hs4Ma3G109 - CloudTrail ログファイルの検証を有効にする必要があります | 2024 年 10 月 25 日 |

| | | |
|---|---|---|
| | • Hs4Ma3G217 - CodeBuild プロジェクト環境にはログ記録 AWS Configuration4 が必要です<br>• Hs4Ma3G158 - SSM ドキュメントは公開しないでください<br>• 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 | |
| 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 Accelerate からオフボードに新しいセクションが追加されました | AMS Accelerate から Offboard に追加された Alarm Manager と Resource Tagger の依存関係を使用してオフボードする手順。 | 2024 年 10 月 24 日 |
| Resource Tagger ダッシュボードが利用可能になりました。 | Resource Tagger ダッシュボードがセルフサービスレポートで使用できるようになりました。 | 2024 年 9 月 26 日 |
| 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。 | 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 |
| AMS Accelerate の制限が AMS パッチ管理に含まれるようになりました。 | AMS Accelerate の制限は、パッチ管理 - パッチメンテナンスウィンドウの作成に含まれています。 | 2024 年 8 月 30 日 |

| | | |
|---|---|---|
| AMS Accelerate Account Discovery の更新 | Amazon EC2 インスタンス評価用のアカウント検出の新しいセクションが追加されました。 | 2024 年 8 月 29 日 |
| AMS Accelerate のデフォルトのパッチベースラインが Ubuntu オペレーティングシステムで使用できるようになりました。 | AMS Accelerate のデフォルトのパッチベースラインが Ubuntu オペレーティングシステムで利用可能になりました。 | 2024 年 8 月 22 日 |
| AMS Accelerate Account Discovery の更新 | オペレーションチェックテーブル AWS CloudTrail の評価セクションに 4 つの新しい AWS API コールが追加されました。 | 2024 年 8 月 2 日 |
| Trusted Remediator が追加のチェックをサポートするようになりました | Trusted Remediator がセキュリティチェック Hs4Ma3G192 をサポートするようになりました。RDS DB インスタンスはパブリックアクセスを禁止する必要があります。 | 2024 年 7 月 30 日 |
| AMS が Amazon Route 53 Resolver DNS Firewall をサポートするようになりました | 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 |
| AMS Accelerate onboarding_role_minimal.zip に Terraform コードが含まれるようになりました | AMS Accelerate onboarding_role_minimal.zip に Terraform コードが含まれるようになりました。 | 2024 年 7 月 30 日 |
| セキュリティ設定ルールダッシュボード | 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用できるようになりました。 | 2024 年 7 月 24 日 |

| | | |
|---|---|---|
| AMS Accelerate 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。 | AMS Accelerate 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 |
| AMS Accelerate アカウント検出プロセスが更新されました。 | AMS Accelerate AWS アカウント へのオンボーディング時に使用されるアカウント検出プロセスが更新されました。 | 2024 年 7 月 1 日 |
| Trusted Remediator が利用可能になりました。 | 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。 | 2024 年 6 月 24 日 |
| 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。 | 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 |
| サポートされているオペレーティングシステムの更新 | AMS Accelerate が AlmaLinux 8.3-8.9、9.0-9.2 をサポートするようになりました (AlmaLinux は x86 アーキテクチャでのみサポートされています ) | 2024 年 6 月 19 日 |
| デフォルトが満たされると、インスタンスプロファイルの自動制限が引き上げられるようになりました。 | AMS は、デフォルトのインスタンスプロファイル制限である 10 に達すると、デフォルトのインスタンスプロファイル制限を 20 に引き上げるようになりました。 | 2024 年 6 月 18 日 |

| | | |
|---|---|---|
| AMS SSM エージェントの自動インストール機能がデフォルトで有効になりました。 | AMS SSM エージェントの自動インストール機能は、6/03/2024 以降にオンボーディングされたアカウントではデフォルトで有効になっています。 | 2024 年 6 月 7 日 |
| セキュリティ管理にセキュリティに関するよくある質問が追加されました。 | AMS オペレーションエンジニアまたはオートメーションがアカウントにアクセスするときに使用されるセキュリティのベストプラクティス、コントロール、アクセスモデル、監査メカニズムに関する一般的な質問をカバーするセキュリティに関するよくある質問が利用可能になりました。 | 2024 年 6 月 3 日 |
| Amazon EKS のモニタリングとインシデント管理でサポートされる追加の AWS リージョン。 | Amazon EKS のモニタリングとインシデント管理で 3 つの追加 AWS リージョンがサポートされるようになりました。 | 2024 年 5 月 23 日 |
| サービスリクエストのパッチ通知は、パッチメンテナンスウィンドウの前に送信されるようになりました。 | AMS Accelerate パッチ適用は、パッチメンテナンスウィンドウの 4 日前に新しいサービスリクエストを作成します。サービスリクエストを使用して、パッチの調整やパッチのスキップのために AMS と通信できます。 | 2024 年 5 月 3 日 |
| AMS Accelerate EKS モニタリングベースラインアラートテーブルに追加されたアラートしきい値。 | 詳細なアラートしきい値が Amazon EKS モニタリングのベースラインアラートテーブルで利用可能になりました。 | 2024 年 5 月 3 日 |

| | | |
|---|---|---|
| 更新: Alarm Manager 設定プロファイル。 | Alarm Manager を使用した異常検出アラームの作成に関する注意事項を追加しました。 | 2024 年 4 月 25 日 |
| Resource Tagger 設定プロファイルの追加。 | DynamoDB テーブルと Amazon S3 バケットが Resource Tagger で利用可能になりました | 2024 年 4 月 25 日 |
| 計画イベント管理 (PEM) 情報セクションを追加しました。 | PEM サービスの詳細については、AMS Accelerate ユーザーガイドを参照してください。 | 2024 年 4 月 25 日 |
| AMS は Red Hat Enterpise Linux (RHEL) 9.x をサポートしています。 | AMS は Red Hat Enterprise Linux (RHEL) 9.x をサポートしています。 | 2024 年 4 月 25 日 |
| AMS Accelerate は、すべての AWS リージョン設定のレポートをサポートしています。 | AMS Accelerate は、すべての AWS リージョン設定で SSM インベントリレポートをサポートしています。 | 2024 年 4 月 25 日 |
| 更新: AWS 管理ポリシー。 | AWSManagedServices DeploymentToolkitPolicy を新しい ECR アクセス許可で更新しました。 | 2024 年 4 月 4 日 |
| 更新: Resource Tagger Configuration Profiles セクション | ResourceType リスト `AWS::EFS::FileSystem` に追加されました。 | 2024 年 3 月 21 日 |
| 更新: Accelerate セクションのインシデントレポートとサービスリクエスト。 | Accelerate のトピックタイトルをインシデントレポート、サービスリクエスト、請求に関する質問に変更しました。請求に関する質問という新しいセクションを追加しました。 | 2024 年 3 月 21 日 |

| | | |
|---|---|---|
| 更新: サービスリクエスト管理の仕組みセクション。 | 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 |
| 更新: CloudFormation セクションを使用して aws_managedservices_onboarding_role ロールを作成する | ロールを作成するコマンドを追加しました AWS CloudShell。 | 2024 年 3 月 21 日 |
| 更新: (オプション) クイックスタートテンプレート | テンプレートをダウンロードするコマンドを追加しました AWS CloudShell。 | 2024 年 3 月 21 日 |
| Alarm Manager 設定プロファイルで使用できる新しいリソースタイプ。 | Amazon FSx、Amazon EFS、Elasticsearch のリソースタイプを Alarm Manager 設定プロファイルに追加しました。 | 2024 年 3 月 21 日 |
| 設定プロファイルで使用できる追加の擬似パラメータ置換。 | Amazon EFS と Amazon FSx の擬似パラメータ置換を追加しました。 | 2024 年 3 月 21 日 |
| サービスの説明トピックの 機能に新しいセクションを追加しました。 | AMS Accelerate 機能でサービスリクエスト管理という新しいセクションを追加しました。 | 2024 年 3 月 21 日 |
| セルフサービスレポート週間インシデントレポートに追加された新しい列 | 週次インシデントレポートに新しい列が追加され、インシデントが作成または解決された四半期、月、週、または日に基づいてインシデントをフィルタリングできるようになりました。 | 2024 年 3 月 11 日 |

# 以前の更新

次の表は、2024 年 3 月以前の AMS Accelerate 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 | 日付 |
| --- | --- | --- |
| AMS Accelerate CloudTrail 証跡オンボーディングの改善 | AMS Accelerate CloudTrail 証跡オンボーディングの改善：<br>• すべてのバケットポリシーを 1 つのブロックに収集する<br>• ポリシーステートメントの 2 番目の AWS Organization ID を削除する<br>• お客様の環境要件を明確にする<br><br>詳細については、「設定を確認して更新し、AMS Accelerate が CloudTrail 証跡を使用できるようにします。」を参照してください。 | 2024 年 2 月 23 日 |
| 更新: アカウントのオンボーディングプロセス。 | アカウントのオンボーディングプロセスセクションを再構築し、手順を明確にしました。また、オンボーディング機能用にオプションのクイックスタートテンプレートを追加しました。<br><br>「( オプション) Accelerate のクイックスタートテンプレート」を参照してください。 | 2024 年 2 月 22 日 |
| 更新: AMS Accelerate のオフボーディング。 | AMS Accelerate オフボーディングに関する考慮事項セクションを更新し、`ams-access-management` CloudFormation スタックと `ams-access-management` IAM ロールがオフボーディングプロセスによって削除されないことを示しました。<br><br>「AMS Accelerate オフボーディング効果」を参照してください。 | 2024 年 2 月 22 日 |

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| 更新: Accelerate の設定コンプライアンス。 | これらの用語の混乱を避けるため、必要に応じて「インシデントレポート」を「サービスリクエスト」に変更しました。<br><br>「Accelerate の設定コンプライアンス」を参照してください。 | 2024 年 2 月 22 日 |
| 更新: Accelerate でのアカウント検出。 | Accelerate でアカウント検出を再編成し、関連するセクションで前提条件をより適切にグループ化しました。<br><br>「ステップ 1. Accelerate でのアカウント検出」を参照してください。 | 2024 年 2 月 22 日 |
| 名前変更: AMS ホスト管理への AMS パッチレポート。 | AMS パッチレポートの名前を AMS ホスト管理に変更し、レポート、パッチ詳細レポートの名前を SSM エージェントカバレッジレポートに変更しました。<br><br>「AMS ホスト管理レポート」を参照してください。 | 2024 年 2 月 22 日 |
| オンデマンドカタログでのオペレーションの更新 | オファリングの Operations on Demand カタログテーブルを更新し、 の「ヘルス」への参照を削除しましたAmazon EKS cluster maintenance 。<br><br>「オンデマンドでの AMS オペレーションのリクエスト」を参照してください。 | 2024 年 2 月 22 日 |
| AMS イベントルーターの更新 | AMS イベントルーターセクションAMSCoreRule の を更新しました。<br><br>「AMS での Amazon EventBridge マネージドルールの使用」を参照してください。 | 2024 年 2 月 22 日 |

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| 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。 | 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。<br><br>「サポートされている設定」を参照してください。 | 2024 年 2 月 22 日 |
| EC2 ボリューム使用量修復の自動化を更新 | EC2 ボリューム使用量変更自動化セクションを正しい容量拡張スケジュールで更新しました。<br><br>「EC2 ボリューム使用量修復の自動化」を参照してください。 | 2024 年 2 月 22 日 |
| 更新: 設定を確認して更新し、Accelerate が CloudTrail 証跡を使用できるようにします。 | AMS Accelerate Organization CloudTrail S3 バケットポリシーセクションを更新しました。「設定を確認して更新し、AMS Accelerate が CloudTrail 証跡を使用できるようにします。」を参照してください。 | 2024 年 2 月 15 日 |
| 新機能の追加: SSM Agent 自動インストール | 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<br><br>「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。 | 2024 年 1 月 26 日 |
| 更新: サポートされている設定 | サポートされている のバージョンに関する情報を追加しました。 AWS Control Tower<br><br>「サポートされている設定」を参照してください。 | 2024 年 1 月 26 日 |

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| 更新: AMS パッチレポート。 | AMS パッチレポートから 3 つのセクションを削除しました。<br>• パッチインスタンスの詳細の概要レポート<br>• パッチ詳細レポート<br>• 欠落パッチが報告するインスタンス<br>「AMS ホスト管理レポート」を参照してください。 | 2023 年 12 月 22 日 |
| 更新: オンボーディングの前提条件を高速化。 | AMS Accelerate のオンボードに必要なサポートプランを更新しました。<br>「オンボーディングの前提条件を加速する」を参照してください。 | 2023 年 12 月 15 日 |
| 更新: パッチメンテナンスウィンドウを作成します。 | この機能が廃止されたため、デフォルトのパッチサイクルセクティオを削除しました。<br>「AMS でパッチメンテナンスウィンドウを作成する」を参照してください。 | 2023 年 12 月 13 日 |
| 更新: Accelerate の通知設定。 | 通知に使用される E メールを明確にしました。<br>詳細については「Accelerate の通知設定」を参照してください。 | 2023 年 12 月 12 日 |
| 更新: `AMSAccelerateCustomerAccessPolicies` テンプレート。 | テンプレートを更新`AMSAccelerateCustomerAccessPolicies` して構文エラーを修正しました。<br>詳細については「AMS 機能を使用するためのアクセス許可」を参照してください。 | 2023 年 12 月 12 日 |

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| 追加: 変更リクエストのセキュリティレビュー | セキュリティ管理に新しいセクション「変更リクエストのセキュリティレビュー」を追加しました。<br><br>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。 | 2023 年 12 月 11 日 |
| 更新: resource_inventory.xlsx | resource_inventory.xlsx を更新し、セキュリティアナリストのロールを追加しました。<br><br>詳細については「Accelerate のリソースインベントリ」を参照してください。 | 2023 年 11 月 17 日 |
| 更新: ams-access-admin-operations ロールの説明 | ams-access-admin-operations の説明を更新しました。<br><br>詳細については、「AMS がアカウントにアクセスする理由とタイミング」と「AMS Accelerate での ID による認証」を参照してください。 | 2023 年 11 月 17 日 |
| 更新: AMS Accelerate オフボーディングに関する考慮事項 | セキュリティセクションを更新して、Amazon GuardDuty から利用できる内容と、オフボーディング後の AWS Config ルールを明確にしました。<br><br>詳細については「AMS Accelerate オフボーディング効果」を参照してください。 | 2023 年 11 月 17 日 |
| 追加: Amazon EKS のモニタリングとインシデント管理 | Amazon EKS のモニタリングとインシデント管理は、Amazon EKS 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。<br><br>詳細については「AMS Accelerate での Amazon EKS のモニタリングとインシデント管理」を参照してください。 | 2023 年 11 月 14 日 |

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| 更新: タグ付け | お客様が用意したタグ付けに関する情報を追加しました。<br><br>詳細については「Accelerate のお客様が用意したタグ」を参照してください。 | 2023 年 11 月 7 日 |
| 更新: Resource Tagger 設定プロファイル | フィルターセクションに AWS::AutoScaling::AutoScalingGroup、AWS::EKS::Cluster、AWS::Elasticsearch::Domain、および AWS::FSx::FileSystem を追加しました。<br><br>詳細については「AMS Accelerate のリソースタグ付け設定プロファイル」を参照してください。 | 2023 年 10 月 27 日 |
| 更新: サービスの説明 | サポートされているオペレーティングシステムに Ubuntu 22.04 を追加しました。「サービスの説明」を参照してください。 | 2023 年 9 月 29 日 |
| 更新: AMS Accelerate オンボーディングの前提条件 | CloudFormation テンプレートを含めるように AMS Accelerate VPC エンドポイントにメモを追加しました。「オンボーディングの前提条件を加速する」を参照してください。 | 2023 年 9 月 29 日 |
| 更新: 検出 | AMS Accelerate セキュリティレスポンスからエンドポイント保護タイプを削除しました。「検出」を参照してください。 | 2023 年 9 月 29 日 |
| 更新: AMS でのベースラインモニタリングからのアラート | ベースラインモニタリングからのアラートテーブル AWS Outposts に追加されました。検出 monitoring-default-metrics」を参照してください。 | 2023 年 9 月 29 日 |

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| 更新: で aws_managedservices_onboarding_role ロールを作成する CloudFormation | スタックの詳細の指定のスクリーンショットを更新しました。「for Accelerate CloudFormation aws_managedservices_onboarding_role で を作成する」を参照してください。 | 2023 年 9 月 29 日 |
| 更新: AMS Accelerate によってデプロイされた Amazon EventBridge マネージドルール | 新しい AMS Accelerate Amazon EventBridge マネージドルール AMSCoreRule を追加しました。<br><br>AMS Accelerate Amazon EventBridge マネージドルール AMSAccessRolesRule を更新して、新しいロールを追加しました。<br><br>詳細については「AMS によってデプロイされた Amazon EventBridge マネージドルール」を参照してください。 | 2023 年 9 月 19 日 |
| 更新: Alarm Manager 設定プロファイル | AWS Outposts 擬似パラメータ置換識別子を追加しました。「AMS Accelerate でのモニタリングとイベント管理」を参照してください。 | 2023 年 9 月 11 日 |
| 更新: Resource Tagger 設定プロファイル | AWS Outposts リソースタイプを追加しました。「Accelerate 設定プロファイル: 擬似パラメータ置換」を参照してください。 | 2023 年 9 月 11 日 |
| 更新: サポートされているサービス | CloudWatch アラームでモニタリングされるサービスセクションに Amazon Elastic File System を追加しました。<br><br>詳細については「サービスの説明」を参照してください。 | 2023 年 9 月 6 日 |

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| 更新: パッチモニタリングと障害修復 | 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。<br><br>「オペレーティングシステムがサポートされていないインスタンス、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」<br><br>詳細については「AMS Accelerate でのパッチ管理を理解する」を参照してください。 | 2023 年 9 月 6 日 |
| 更新: マルウェアイベントランブックへの Clarified Response | セキュリティインシデント対応のためのマルウェアイベントランブックへの対応を明確にしました。詳細については「AMS のセキュリティインシデント対応」を参照してください。 | 2023 年 9 月 6 日 |
| 更新: Accelerate アカウントを Transit Gateway に接続する | 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) 手順を明確にしました。詳細については、withTransit Accelerate アカウントを接続する」を参照してください。 | 2023 年 9 月 5 日 |
| 更新: AMS でのベースラインモニタリングからのアラート | 廃止された 2 つのアラーム AMSReadLatencyAlarm と AMSWriteLatencyAlarm への参照を削除しました。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。 | 2023 年 9 月 5 日 |
| 追加: AMS イベントルーター | AMS イベントルーターのドキュメントを追加しました。詳細についてはAMS での Amazon EventBridge マネージドルールの使用、「」を参照してください。 | 2023 年 9 月 5 日 |

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| 更新: Alarm Manager の擬似パラメータのリスト。 | Alarm Manager の擬似パラメータのリストを更新しました。EC2 インスタンス名パラメータが EC2 インスタンスと EC2 ディスクアラーム設定に追加されました。詳細については「Accelerate 設定プロファイル: 擬似パラメータ置換」を参照してください。 | 2023 年 8 月 29 日 |
| 追加: AMS アクセスオフボーディング | AMS アクセスをオフボーディングする際の考慮事項を追加しました。「AMS Accelerate オフボーディング効果」を参照してください。 | 2023 年 8 月 24 日 |
| 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。「AMS のセキュリティインシデント対応」を参照してください。 | 2023 年 8 月 18 日 |
| 更新: AMS Accelerate アクセスロール | ロール名のタイプミスを修正しました。「AWS Identity and Access Management AMS Accelerate での」を参照してください。 | 2023 年 8 月 10 日 |
| 更新: ポリシーステートメント | ハードコードされたロール名をワイルドカードに置き換えました。「設定を確認して更新し、AMS Accelerate が CloudTrail 証跡を使用できるようにします。」を参照してください。 | 2023 年 8 月 10 日 |
| 更新: EFS アラートを含むモニタリング対象サービスのリスト。 | AMS ベースラインモニタリング用の新しい EFS アラートでモニタリングサービスのリストを更新しました。4 つの新しい EFS アラートタイプが追加されました。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。 | 2023 年 8 月 3 日 |
| 更新: リソースインベントリテーブルの高速化 | ams-backup-config-rule-stack および関連リソースを削除しました。「Accelerate のリソースインベントリ」を参照してください。 | 2023 年 7 月 18 日 |

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| 更新: AMS Accelerate アクセスロール | ロール ams-backup-config-rule-st-amsBackupAlertConfigRule-<8 桁のハッシュ> および ams-backup-config-rule-st-amsBackupPlanConfigRuleH-<8 桁のハッシュ> を削除しました。「AWS Identity and Access Management AMS Accelerate での」を参照してください。 | 2023 年 7 月 18 日 |
| 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。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。 | 2023 年 6 月 19 日 |
| 新規: AMS Accelerate アクセスロール | AMS Security の新しいアクセスロールを追加しました。 | 2023 年 6 月 16 日 |
| 新規: AMS Accelerate CloudTrail ログ管理でお客様の CloudTrail 証跡を使用できるようになりました。 | Accelerate がデプロイした証跡、カスタマーマネージド CloudTrail アカウントまたは Organization 証跡との統合など、CloudTrail ログ管理でサポートされているオプションを更新しました。詳細については「設定を確認して更新し、AMS Accelerate が CloudTrail 証跡を使用できるようにします。」を参照してください。 | 2023 年 6 月 9 日 |
| 更新: AMS Accelerate Config Rules Response Configuration Report。 | Config Rules Response Configuration Report AWS のリクエスト時レポートを更新しました。「リクエスト時のレポートの更新を高速化する」を参照してください。「AMS Config Rules Response Configuration レポート」を参照してください。 | 2023 年 5 月 26 日 |
| 更新: サービス請求開始日ポリシー。 | の請求開始日の定義を更新しましたAMS の主要な用語。 | 2023 年 5 月 15 日 |

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| 更新: AWS 管理ポリシー。 | AWSManagedServicesDeploymentToolkitPolicy を新しい CFN および ECR アクセス許可で更新し、ワイルドカードで既存のアクションの範囲を絞り込みました。「サービスにリンクされたロールの更新を高速化する」を参照してください。「サービスにリンクされたロールの更新を高速化する」を参照してください。 | 2023 年 5 月 9 日 |
| 更新: ロールポリシーのリンクにアクセスします。 | アクセスロールを Accelerate S3 バケットの場所から直接ダウンロードできるようになりました。<br><br>「AMS がアカウントにアクセスする理由とタイミング」および「AWS Identity and Access Management AMS Accelerate での」を参照してください。 | |
| 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。<br><br>「請求レポート (毎月 ) 」を参照してください。 | 2023 年 4 月 13 日 |
| 更新: アラートのリスト。 | CloudTrail リファレンスを削除しました。<br><br>「AMS Accelerate でのログ管理」を参照してください。 | 2023 年 4 月 13 日 |
| 更新: アラートのリスト。 | 3 つの新しい SSM エージェントアラートを追加しました。<br><br>「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。 | 2023 年 4 月 13 日 |

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| 更新: Accelerate の前提条件。 | Accelerate では、4 つの AWS サポートプランのうち 1 つが必要であり、開発者プランを除外することを明確にしました。<br><br>「オンボーディングの前提条件を加速する」を参照してください。 | 2023 年 4 月 13 日 |
| 更新: サービスにリンクされたロールポリシーの高速化。 | Contacts Service ポリシー zip ファイルが更新されました。<br><br>「AWS AMS Accelerate の マネージドポリシー」を参照してください。 | 2023 年 4 月 13 日 |
| 更新: AMS リソーススケジューラ。 | ロール名 AWSManagedServices-DescribeScheduleOrPeriod が AWSManagedServices-DescribeScheduleOrPeriods に修正されました。「AMS Resource Scheduler によるコスト最適化」を参照してください。 | 2023 年 4 月 13 日 |
| 更新: AWS 管理ポリシー。 | 単一または複数のアカウントのカスタムレスポンスを更新する手順カスタマイズされた検出結果のレスポンスを更新しました。 | 2023 年 4 月 13 日 |
| 更新: Resource Tagger | AMS 管理の設定を同じ名前で誤って上書きする可能性があるため、「新しい設定の名前の指定 (提供された例では SampleConfigurationBlock)」に関する警告を追加しました。「AMS Accelerate のリソースタグ付けのユースケース」を参照してください。 | 2023 年 3 月 16 日 |
| 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。「サービスの説明」を参照してください。 | 2023 年 3 月 16 日 |
| 更新: デプロイツールキット SLR JSON のアクション | ポリシーとアクションを更新しました。「AMS Accelerate 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。 | 2023 年 3 月 16 日 |

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| 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。「アラートの AMS 自動修復」を参照してください。 | 2023 年 3 月 16 日 |
| 更新: オンボーディングの高速化。 | ロールの使用、特に最小限のロール を明確にしましたAMS ロールを作成するテンプレート。 | 2023 年 3 月 16 日 |
| 更新: セルフサービスレポート。 | 日次バックアップレポートで、プライマリリージョンとセカンダリリージョンがサポートされるようになりました。どちらも のリソースリージョンフィールドで報告されますバックアップレポート (毎日 )。 | 2023 年 3 月 16 日 |
| 更新: パッチ適用ガイダンス | AMS によって管理されるデフォルトのパッチベースラインをカスタマイズしない警告を追加しました。代わりに、新しいカスタムパッチベースラインを作成します。デフォルトのパッチベースライン 「」および「」を参照してくださいAMS Accelerate を使用したカスタムパッチベースライン。 | 2023 年 3 月 16 日 |
| サービス終了ポリシーを更新しました。 | でのサービス終了とサービス終了日の定義を更新しましたAMS の主要な用語。終了通知は、過去 1 か月の 20 日までに発行する必要があります。 | 2023 年 3 月 16 日 |
| 更新: AWS 管理ポリシー。 | ポリシー名を明確にしました: AMS Accelerate のサービスにリンクされたロールに連絡する。 | 2023 年 2 月 16 日 |
| 新規: AWS 管理ポリシー。 | ポリシー を追加しましたAMS Accelerate のサービスにリンクされたロールに連絡する。 | 2023 年 2 月 16 日 |
| 更新: 設定コンプライアンス。 | 「」でスペルミスのある単語を修正しましたAccelerate の設定コンプライアンス。 | 2023 年 2 月 16 日 |

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| 新しいコンテンツ: サポートされていない OSes | AMS がサポートされていないオペレーティングシステム (OSes「」を参照してくださいAccelerate 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。 | 2023 年 2 月 16 日 |
| 更新: パッチウィンドウの作成 | CloudShell を使用するためのリンクを に追加しましたAMS Accelerate 用の Systems Manager コマンドラインインターフェイス (CLI) を使用してメンテナンスウィンドウを作成する。 | 2023 年 2 月 16 日 |
| 更新されたコンテンツ: 管理リソースのオンボーディング | の圧縮された JSON テンプレートを更新しましたAMS ロールを作成するテンプレート。 | 2023 年 2 月 16 日 |
| 新しいコンテンツ: 設定コンプライアンス | 新しいトピック を追加しましたカスタマイズされた検出結果のレスポンス。 | 2023 年 2 月 16 日 |
| 新規: AWS 管理ポリシー。 | 追加されたポリシー: AMS Accelerate の Amazon EventBridge ルールサービスにリンクされたロール。 | 2023 年 2 月 7 日 |
| 更新: AWS 管理ポリシー。 | を新しい S3 アクセス許可`AWSManagedServicesDeploymentToolkitPolicy` で更新しました。「サービスにリンクされたロールの更新を高速化する」を参照してください。 | 2023 年 1 月 30 日 |
| 新しいオプトインリージョン: CPT。 | AMS Accelerate がケープタウン (CPT) オプトインリージョンで利用可能になりました。オプトインするには、「 の管理 AWS リージョン」を参照してください。 | 2023 年 1 月 12 日 |
| 更新: サービスの説明。 | CloudWatch アラームでモニタリングされる FSx サービスを に追加しましたサービスの説明。 | 2023 年 1 月 12 日 |

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| 更新: デフォルトのメトリクスのモニタリング。 | に 6 つの FSx アラームを追加しましたAMS でのベースラインモニタリングからのアラート。 | 2023 年 1 月 12 日 |
| 更新: AMS パターン。 | Cloudwatch アラーム通知のカスタマイズを に追加しましたAMS パターン。 | 2023 年 1 月 12 日 |
| 更新: 管理リソースのオンボーディング。 | テンプレートのテーブルを更新し、 `ams-onboarding-ssm-execution-role` にの行を追加しましたAMS ロールを作成するテンプレート。 | 2023 年 1 月 12 日 |
| 更新: 設定コンプライアンス。 | でカスタム修復をリクエストするための追加の詳細 (重要ボックス内 ) Accelerate の設定コンプライアンス。 | 2023 年 1 月 12 日 |
| 更新: Service-linked-roleアクセス許可。 | 古いアクセス許可または重複したアクセス許可を削除しました。「AMS Accelerate 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。 | 2022 年 12 月 15 日 |
| 更新: パッチ管理、メンテナンスウィンドウ。 | メンテナンスウィンドウを作成するためのコンソールの手順、ステップ 5 のガイダンスを追加しました。「AMS Accelerate の Systems Manager コンソールからメンテナンスウィンドウを作成する」を参照してください。 | 2022 年 12 月 15 日 |
| 新規: パッチ管理セクション。 | パッチ火曜日のメンテナンスウィンドウのセクションを追加しました。「AMS コンソールから定期的な「パッチ火曜日」メンテナンスウィンドウを作成する (推奨 ) 」を参照してください。 | 2022 年 12 月 15 日 |
| 更新: AMS リソーススケジューラ。 | CloudFormation スタック名を更新しました。「AMS Resource Scheduler でのリソースの使用」を参照してください。 | 2022 年 12 月 15 日 |

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| 更新: バックアップ用にリソースにタグを付けます。 | AMS Resource Tagger を使用するためのガイダンスを追加しました。「リソースにタグを付けて AMS バックアッププランを適用する」を参照してください。 | 2022 年 12 月 15 日 |
| 更新: バックアッププランを選択します。 | 継続的バックアップを提供するプランを示します。「AMS バックアッププランを選択する」を参照してください。 | 2022 年 12 月 15 日 |
| 更新: AMS リソーススケジューラ。 | 期間またはスケジュールを削除するための AWS CLI の例を更新しました。「AWS Managed Services Resource Scheduler で期間とスケジュールを操作する」を参照してください。 | 2022 年 12 月 15 日 |
| 更新: AWS 管理ポリシー。 | を追加しましたAWSManagedServices DeploymentToolkitPolicy 。「AWS AMS Accelerate の マネージドポリシー」を参照してください。 | 2022 年 12 月 15 日 |
| 新規: AMS の新しいサービスにリンクされたロール AWSServiceRoleForManagedServices_DetectiveControlsConfig について説明するセクションを追加しました。 | GovCloud のリージョンとアクセス許可を追加しました。「AMS Accelerate のサービスにリンクされたロールを Detective が制御する」を参照してください。 | 2022 年 12 月 15 日 |

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| 新しい: AWSマネージドポリシー | AWSサービスにリンクされたロールポリシー AWSManagedServices_AlarmManagerPermissionsBoundary がサービスにリンクされたロールポリシー AWSManagedServices_AlarmManager_ServiceRolePolicy で使用され、サービスにリンクされたロール AWSServiceRoleForManagedServices_AlarmManager によって作成された IAM ロールのアクセス許可を制限する方法を説明するセクションを追加しました。「AWS AMS Accelerate の マネージドポリシー」を参照してください。 | 2022 年 12 月 15 日 |
| 更新: オンデマンドオペレーション。 | サービスの追加: EC2 オペレーションの SQL Server と AMI の構築と販売。「オンデマンドオペレーション」を参照してください。 | 2022 年 11 月 10 日 |
| 更新: モニタリングとイベント管理。 | 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。「モニタリングの仕組み」を参照してください。 | 2022 年 11 月 10 日 |
| 更新: サービスにリンクされたロールリージョン | GovCloud のリージョンとアクセス許可を追加しました。「AMS Accelerate 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。 | 2022 年 11 月 10 日 |
| 新規: サービスにリンクされたロール。 | 新しいロール を追加しましたAWSServiceRoleForAMSDetectiveControls 。<br><br>「AMS Accelerate のサービスにリンクされたロールを Detective が制御する」を参照してください。 | 2022 年 11 月 10 日 |
| 更新: アクセス管理。 | 手順を改善してサブセクションを更新しました。「AMS Accelerate でのアクセス管理」を参照してください。 | 2022 年 11 月 10 日 |

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| 更新: サービスの説明。 | RACI マトリックスの AMS パターンを更新しました。「サービスの説明」を参照してください。 | 2022 年 11 月 10 日 |
| 更新: AMS パターン。 | お客様はパターンのデプロイを担当します。「AMS パターン」を参照してください。 | 2022 年 11 月 10 日 |
| 更新: オフボーディング。 | オフボーディング中に特定の Backup リソースと Monitoring リソースがどうなるかの詳細を追加しました。「AMS Accelerate からのオフボード」を参照してください。 | 2022 年 11 月 10 日 |
| 更新: パッチ管理。 | IAM ポリシーに関するガイダンスを更新し、短縮しました。「AMS Accelerate のオンデマンドパッチ適用用の IAM ロールの作成」を参照してください。 | 2022 年 11 月 10 日 |
| 新規: アーキテクチャ図へのリンク。 | AMS リファレンスアーキテクチャ図へのリンクをさまざまなトピックに追加しました。例については、「AMS Accelerate でのモニタリングとイベント管理」を参照してください。 | 2022 年 11 月 10 日 |
| 新規: Operations on Demand の提供 | 「ランディングゾーンアクセラレーターオペレーション」を追加しました。「オンデマンドオペレーション」を参照してください。 | 2022 年 10 月 13 日 |
| 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 | モニタリングの仕組み. | 2022 年 10 月 13 日 |
| 新規: Accelerate-custom CFN テンプレートを使用したパッチメンテナンスウィンドウの作成 | CloudFormation パッチウィンドウ設定テンプレート。「AMS でパッチメンテナンスウィンドウを作成する」を参照してください。 | 2022 年 9 月 15 日 |

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| 更新: オフボーディング | Accelerate のバックアッププランがオフボーディング後に機能しなくなったことを強調しました。「AMS Accelerate からのオフボード」を参照してください。 | 2022 年 9 月 15 日 |
| 更新: CloudWatch 設定変更の詳細 | Windows と Linux の例の誤りを修正しました。「CloudWatch 設定変更の詳細」を参照してください。 | 2022 年 9 月 15 日 |
| 更新: AMS Resource Scheduler の使用 | コスト配分タグに関するガイダンスを追加しました。「AMS Resource Scheduler のコスト推定器」を参照してください。 | 2022 年 9 月 15 日 |
| 更新: AMS Config ルールライブラリ | ルールの表に 2 ams-eks- つの設定ルールを追加しました。「AMS Config ルールライブラリ」を参照してください。 | 2022 年 9 月 15 日 |
| 更新: バックアップ管理 | バックアッププランのタイトルと説明から誤解を招くラベル PITR (point-in-time-recovery) を削除しました。「AMS バックアッププランを選択する」を参照してください。 | 2022 年 9 月 15 日 |
| 更新: Accelerate サービスの説明 | 設定ルールと Canary の説明を更新しました。「サービスの説明」を参照してください。 | 2022 年 9 月 15 日 |
| 更新: サービスの説明、サポートされている設定 | Windows 2008 R2 end-of-serviceを削除しました。Accelerate は Windows 2008 をサポートしていません。「サポートされている設定」を参照してください。 | 2022 年 8 月 11 日 |
| 更新: サービスの説明、役割と責任 | RACI テーブルを更新しました。ネットワークセクションの最後の行から ELB アクセスログを削除しました。Accelerate のお客様の ELB アクセスログは有効にしません。「役割と責任」を参照してください。 | 2022 年 8 月 11 日 |

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| 更新: 設定コンプライアンス | Table of Rules, Frameworks 列の誤字を修正しました。NIST-CSF が NIST-CIS として誤ってリストされました。「Accelerate の設定コンプライアンス」を参照してください。 | 2022 年 8 月 11 日 |
| 新規: オフボーディングを高速化する | オフボーディングに関する考慮事項とプロセス。「AMS Accelerate のオフボーディング」を参照してください。 | 2022 年 8 月 11 日 |
| 更新: プリインストールされた SSM エージェントのオペレーティングシステムのリスト | リストに「Ubuntu Linux 18.04 および 20.04」を追加しました。「高速化のための EC2 インスタンスのオンボーディング」を参照してください。 | 2022 年 8 月 11 日 |
| 新規: Resource Scheduler | AMS Resource Scheduler を使用して、必要に応じてリソースを停止および開始することでコストを最適化します。「AMS Resource Scheduler によるコスト最適化」を参照してください。 | 2022 年 7 月 14 日 |
| 更新: Resource Scheduler のサービスの説明 | 新しい Resource Scheduler サービスについて、サービスの説明のいくつかのセクションが更新されました。「サービスの説明」を参照してください。 | 2022 年 7 月 14 日 |
| 新規: AMS パターン | AMS にはパターンテンプレートが用意されています。これは、AMS マネージド環境の一連のユースケースを解決する一般的なソリューションです。オファーの最初のパターン: AMS パターン。 | 2022 年 7 月 14 日 |
| 新規: コスト最適化メモ | リソースの使用に伴ってコストがどのように増加するかを説明するメモを追加しました。「Accelerate のリソースインベントリ」を参照してください。 | 2022 年 7 月 14 日 |

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| 更新: AMS Config ルール | のテーブルを再編成しましたAMS Config ルールライブラリ。HTML テーブルの列数が少ないため、一目で読みやすくなります。ダウンロード可能なスプレッドシートには、ソートとフィルタリングを可能にする追加の列があります。 | 2022 年 7 月 14 日 |
| 更新: アクセス管理 | のサンプル CloudFormation テンプレートを更新しましたAMS 機能を使用するためのアクセス許可。`AMSAccelerateAdminAccess` ポリシーに `AmsResourceSchedulerPassRolePolicy` および `IAMReadOnlyPolicy` ポリシーが含まれるようになりました。 | 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。で「重要」というラベルのボックスを参照してくださいセルフサービスレポート。 | 2022 年 7 月 14 日 |
| 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。 AMS でのベースラインモニタリングからのアラート | 2022 年 7 月 14 日 |
| 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。 サービスの説明 | 2022 年 7 月 14 日 |
| 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。 レポートとオプション | 2022 年 7 月 14 日 |

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| Resource Scheduler | AMS リソーススケジューラのオンボーディングと使用に関する情報を追加し、リソースの停止時間と開始時間をスケジュールすることでコストの最適化を支援しました。また、Accelerate サービスの説明を更新し、Resource Scheduler についての説明を追加しました。さらに、Amazon Linux 2 のサポート終了日を 2024 年に更新しました。AMS Resource Scheduler によるコスト最適化 および サービスの説明 を参照してください。 | 2022 年 6 月 30 日 |
| 新しいアラーム | AWS Backup アラームを追加しました。 AMS でのベースラインモニタリングからのアラート | 2022 年 6 月 21 日 |
| 新しいコンテンツ | サービスにリンクされたロールのコンテンツを追加しました。 AMS Accelerate のサービスにリンクされたロールの使用 | 2022 年 6 月 16 日 |
| | AWS Network Firewall Operations が Operations on Demand (OOD) サービスのカタログに追加されました。 オンデマンドオペレーション | 2022 年 6 月 16 日 |
| | 問題管理機能の説明を追加しました。 サービスの説明 | 2022 年 6 月 16 日 |
| | が特定のオプトインリージョンでサポートしていない設定ルールのセットに関する注意を追加しました。 Accelerate の設定コンプライアンス | 2022 年 6 月 16 日 |
| 更新された内容 | 設定コンプライアンス。「AMS Config Rule library」->「Table of rules」が更新され、ZIP のみに削除されました。 Accelerate の設定コンプライアンス | 2022 年 6 月 16 日 |

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| | エスカレーション E メールを削除しました。エスカレーションパス | 2022 年 6 月 16 日 |
| | トピックリストを開いた段落の下に移動しました。 AMS Accelerate とは | 2022 年 6 月 16 日 |
| | 自動修正の内容を更新しました。アラートの AMS 自動修復 | 2022 年 6 月 16 日 |
| 更新された内容: サービスの説明 | で AMS Config ルールによってモニタリングされるサービスのリストに EKS を追加しましたサポートされる サービス。<br><br>の RACI テーブルのモニタリングの説明を更新しました役割と責任。 | 2022 年 5 月 12 日 |
| 更新された内容: 設定コンプライアンス | EKS 関連の設定ルールを追加しました。「Accelerate の設定コンプライアンス」を参照してください。 | 2022 年 5 月 12 日 |
| 更新された内容: 開始方法、アカウント検出 | に AwsAccountDiscoveryCli スクリプトの新しいバージョン (Account Discovery Changelog zip ファイル内) を追加しましたステップ 1. Accelerate でのアカウント検出。 | 2022 年 5 月 12 日 |
| 更新された内容: モニタリング、デフォルトメトリクス | ALB 関連のメトリクスのトリガー条件を更新しました。「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。 | 2022 年 5 月 12 日 |
| 更新されたコンテンツ: パッチオンボーディング | 明示的なパッチ適用の前提条件を追加しました。EBS にオプトインする必要があります。「Accelerate でのオンボーディングパッチ適用」を参照してください。 | 2022 年 5 月 12 日 |

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| 更新された内容: リソースインベントリテーブルの高速化 | ams-detective-controls-config-rules-cdk ルールを変更し、ams-detective-controls-recorder-cdk および ams-detective-controls-infrastructure-cdk のルールを追加しました。「Accelerate のリソースインベントリ」を参照してください。 | 2022 年 4 月 14 日 |
| 更新された内容: 設定コンプライアンス | 業界標準、設定ルール、レスポンスのタイプの概要。顧客は個々の設定ルールやレスポンスを選択しないことを強調しますAccelerate の設定コンプライアンス。 | 2022 年 4 月 14 日 |
| 更新された内容: サービスの説明 | 「役割と責任」の「既存の変更範囲」セクションを移動しました。「役割と責任」を参照してください。 | 2022 年 4 月 14 日 |
| 更新された内容: タグ付けとモニタリング | タグ付けとモニタリングに許可されているリソースタイプのリスト`AWS::Synthetics:Canary` に追加されました。「AMS Accelerate のリソースタグ付け設定プロファイル」および「Accelerate 設定プロファイル: 擬似パラメータ置換」を参照してください。 | 2022 年 4 月 14 日 |
| 更新された内容: Accelerate の前提条件 | SSM に必要なバケットのアクセス許可をに追加しましたAccelerate の Amazon EC2 Systems Manager。 | 2022 年 4 月 14 日 |
| 新しいコンテンツ: パッチ適用とモニタリング | Cloudformation を使用してタグ付けとモニタリングの設定をデプロイするためのサンプルコードを追加しました。「CloudFormation for Accelerate を使用して設定プロファイルをデプロイする」および「CloudFormation を使用した Accelerate 設定変更のデプロイ」を参照してください。 | 2022 年 3 月 10 日 |

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| 更新された内容: パッチメンテナンスコンソール | コンソールインターフェイスと一致するAMS Accelerate の Systems Manager コンソールからメンテナンスウィンドウを作成するようにのステップの順序を変更しました。 | 2022 年 3 月 10 日 |
| 更新された内容: パッチメンテナンス CLI | の CLI パラメータ (スケジュール、期間、カットオフ) を更新しました AMS Accelerate 用の Systems Manager コマンドラインインターフェイス (CLI) を使用してメンテナンスウィンドウを作成する | 2022 年 3 月 10 日 |
| 新しいコンテンツ: Auto Instance Config | AMSInstanceProfileBasePolicy に の定義を追加 IAM アクセス許可の変更の詳細 | 2022 年 3 月 10 日 |
| 新しいコンテンツ: オンボーディング | にサンプル Linux コマンドを追加しました Accelerate でのアウトバウンドインターネット接続 | 2022 年 3 月 10 日 |
| 新しいコンテンツ: オンボーディング | 最小特権オプションを に追加しましたAMS ロールを作成するテンプレート。 | 2022 年 3 月 10 日 |
| 更新された内容: エスカレーション手順の高速化 | にガイダンス、リンク、E メール連絡先を追加 エスカレーションパス | 2022 年 3 月 10 日 |
| 更新された内容: サポートされている設定 | AMS は、2023 年 3 月 14 日に RHEL 6 と CentOsのサポートを終了する予定です。「サポートされている設定」を参照してください。 | 2022 年 3 月 10 日 |
| 更新された内容: リソーステーブル | Accelerate のリソースインベントリ リソーステーブルに AMS アクセス IAM ロールを追加 | 2022 年 3 月 10 日 |
| 更新された内容: オンボーディングとバックアップ | Accelerate AWS Backup でのオンボーディング と にオプトイン AWS Backup する手順を追加しました AMS Accelerate での継続的な管理 | 2022 年 3 月 10 日 |

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| 更新された内容: アクセス管理 | Accelerate ガイダンス からアドバンスト固有の手順を削除しました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。 | 2022 年 3 月 10 日 |
| 更新された内容: サポートされている設定 | AMS は、Oracle Linux 8.3 および Ubuntu 18.04 および 20.04 をサポートするようになりました。「サポートされている設定」を参照してください。 | 2022 年 2 月 28 日 |
| 更新された内容: サービスレベルアグリーメント | でダウンロード可能なサービスレベルアグリーメントを更新しましたサポートされる サービス。 | 2022 年 2 月 28 日 |
| 更新された内容: アクセス管理 | AMS オペレータコンソールロールFAQsと、変更または削除しないという警告AMS がアカウントにアクセスする方法を更新しました。 | 2022 年 2 月 28 日 |
| 更新された内容: Alarm Manager | 更新済み 高速設定プロファイル: モニタリング。Alarm Manager は単一メトリクスアラームに制限されなくなりました。 | 2022 年 2 月 28 日 |
| 更新された内容: 開始方法 | 更新済み ステップ 2. Accelerate での管理リソースのオンボーディング。リソースのオンボーディングのための最小限のアクセスを持つ IAM ロールを追加しました。 | 2022 年 2 月 28 日 |
| 新しいコンテンツ: Service Description の変更範囲 | AMS Accelerate が実行しない境界とアクションを強調する新しいセクションAMS Accelerate によって実行される変更の範囲を追加しました。 | 2022 年 2 月 10 日 |

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| 更新された内容: 開始方法 | 新しいオンボーディングプロセスは、カスタマイズする前にデフォルトの機能と設定をセットアップすることから始まります。サブセクションには、機能固有の目標と関連するリンクが含まれています。「AMS Accelerate の開始方法」を参照してください。 | 2022 年 2 月 10 日 |
| 更新された内容: AMS Backup Management。 | 読みやすくするためにAMS Accelerate での継続的な管理章を短縮し、再編成しました。 | 2022 年 2 月 10 日 |
| 更新された内容: タグ付け | CloudFormation およびその他のツールのコードサンプルに対応するために、タグ付けツールセクションを追加しました。「AMS Accelerate でのタグ付け」を参照してください。 | 2022 年 2 月 10 日 |
| 更新された内容: Baseline Monitoring | RedShift クラスターアラームのトリガー条件が改善され、メンテナンス中の誤アラームが軽減されました。「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。 | 2022 年 2 月 10 日 |
| 更新された内容: パッチ適用 | サンプル CLI コマンドを更新して、メンテナンスウィンドウを登録しました。「AMS Accelerate 用の Systems Manager コマンドラインインターフェイス (CLI) を使用してメンテナンスウィンドウを作成する」を参照してください。 | 2022 年 2 月 10 日 |
| content: AWS Config Rules Inventory を更新しました。 | Config Rules Inventory テーブル`ams-nist-cis-ec2-security-group-attached-to-eni` から非推奨 AWS の設定ルールを削除しました。「ルールの表」を参照してください。 | 2022 年 1 月 27 日 |

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| 新しいコンテンツ: パッチメンテナンスウィンドウの作成。 | コマンドラインからパッチメンテナンスウィンドウを作成するための SSM チュートリアルとサンプルコマンドへのリンクを追加しました。「AMS Accelerate 用の Systems Manager コマンドラインインターフェイス (CLI) を使用してメンテナンスウィンドウを作成する」を参照してください。 | 2022 年 1 月 27 日 |
| 新しいコンテンツ: Resource Tagger は、新しい Auto Scaling Groups (ASG) リソースタイプを認識します。 | Resource Tagger 設定プロファイルでフィルタリング可能なリソースタイプに Auto Scaling グループを追加しました。「構文と構造」を参照してください。 | 2022 年 1 月 13 日 |
| 新しいコンテンツ: 追加のバックアッププランとボールト。 | ランサムウェア攻撃などの高リスクシナリオを軽減するための新しいバックアッププランとボールトを追加しました。「AMS ボールトでバックアップを表示する」および「AMS ボールトでバックアップを表示する」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。