AMS アドバンストアカウントのオンボーディング情報

AMS アドバンストオンボーディングガイド

Version September 25, 2025

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

AMS アドバンストオンボーディングガイド: AMS アドバンストアカウントのオンボーディング情報

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 が所有していない他のすべての商標は、それぞれの所有者の所有物であり、Amazon と提携、接続、または後援されている場合とされていない場合があります。

Table of Contents

AWS Managed Servicesオンボーディングの概要 1
AMS について 1
重要な用語 2
AMS モード 8
AMS モードとアプリケーションまたはワークロード 9
AMS アカウント後規範ガイダンス 16
何をするか、何をしないか 16
AMS 出力トラフィック管理 17
IAM ユーザーロール 18
MALZ: デフォルトの IAM ユーザーロール 19
SALZ: デフォルトの IAM ユーザーロール 32
デフォルトのアクセスファイアウォールルール 40
Linux スタックインスタンスポート 40
Windows スタックインスタンスポート 41
サービス管理 43
アカウントガバナンス 43
サービス開始 43
顧客関係管理 (CRM) 44
CRM プロセス 45
CRM 会議 45
CRM ミーティングの手配 47
CRM 月次レポート 47
コスト最適化 48
コスト最適化フレームワーク 49
コスト最適化責任マトリックス 51
サービス時間 53
ヘルプの利用 53
変更管理モード 54
モードの概要 55
AMS のモードとアカウントのタイプ 55
AMS モードとアプリケーションまたはワークロード 59
AMS モードの実際のユースケース 66
RFC モード 69
RFCsの詳細 70

変更タイプとは? 107
RFC エラーのトラブルシューティング 120
直接変更モード 130
直接変更モードの開始方法 131
セキュリティとコンプライアンス 133
直接変更モードでの変更管理 138
Direct Change モードを使用したスタックの作成 140
直接変更モードのユースケース 144
デベロッパーモード 144
デベロッパーモードの開始方法 146
セキュリティとコンプライアンス 148
変更管理 150
インフラストラクチャーのプロビジョニングをします。 156
「発見的コントロール」 156
ログ記録、モニタリング、イベント管理 156
インシデント管理 156
パッチ管理 157
継続性管理 157
セキュリティとアクセスの管理 157
AMS でのセルフサービスプロビジョニングモード 158
AMS での SSP モードの開始方法 159
Amazon API Gateway 159
Alexa for Business 160
Amazon AppStream 2.0 162
Amazon Athena 165
Amazon Bedrock 166
Amazon CloudSearch 167
Amazon CloudWatch Synthetics 168
Amazon Cognito 169
Amazon Comprehend 171
Amazon Connect 172
Amazon Data Firehose 174
Amazon DevOps Guru 175
Amazon DocumentDB (MongoDB 互換性) 176
Amazon DynamoDB 177
Amazon Elastic Container Registry 179

EC2 イメージビルダー 180
での Amazon ECS AWS Fargate 182
での Amazon EKS AWS Fargate 184
Amazon EMR 187
Amazon EventBridge 190
Amazon Forecast 192
Amazon FSx 195
Amazon FSx for OpenZFS 197
Amazon FSx for NetApp ONTAP 198
Amazon Inspector Classic 200
Amazon Kendra 201
Amazon Kinesis Data Streams 202
Amazon Kinesis Video Streams 203
Amazon Lex 204
Amazon MQ 205
Amazon Managed Service for Apache Flink 206
Amazon Managed Streaming for Apache Kafka 207
Amazon Managed Service for Prometheus 208
Amazon Personalize 209
Amazon QuickSight 212
Amazon Rekognition 214
Amazon SageMaker AI 215
Amazon Simple Email Service 218
Amazon Simple Workflow Service 220
Amazon Textract 221
Amazon Transcribe 221
Amazon WorkSpaces 223
AMS コードサービス 225
AWS Amplify 228
AWS AppSync 229
AWS App Mesh 230
AWS Audit Manager 231
AWS Batch 232
AWS Certificate Manager 233
AWS Private Certificate Authority 235
AWS CloudEndure 237

AWS CloudHSM 239
AWS CodeBuild 240
AWS CodeCommit 242
AWS CodeDeploy 243
AWS CodePipeline 245
AWS Compute Optimizer 246
AWS DataSync 248
AWS Device Farm 249
AWS Elastic Disaster Recovery 250
AWS Elemental MediaConvert 252
AWS Elemental MediaLive 252
AWS Elemental MediaPackage 253
AWS Elemental MediaStore 254
AWS Elemental MediaTailor 255
AWS Global Accelerator 256
AWS Glue 257
AWS Lake Formation 259
AWS Lambda 260
AWS License Manager 262
AWS Migration Hub 263
AWS Outposts 263
AWS Resilience Hub 264
AWS Secrets Manager 265
AWS Security Hub CSPM 269
AWS Service Catalog AppRegistry 269
AWS Shield 270
AWS Snowball Edge 272
AWS Step Functions 273
AWS Systems Manager パラメータストア 274
AWS Systems Manager Automation 276
AWS Transfer Family 279
AWS Transit Gateway 281
AWS WAF 282
AWS Well-Architected Tool 283
AWS X-Ray 284
VM Import/Export 285

カスタマーマネージドモード 286
カスタマーマネージドモードの開始方法 287
AMS と AWS Service Catalog 287
Service Catalog の開始方法 287
開始する前に AMS の Service Catalog 288
AMS マルチアカウントランディングゾーン (MALZ) オンボーディング 292
MALZ ネットワークアーキテクチャ 292
マルチアカウントランディングゾーンのネットワークアーキテクチャについて 292
単一の MALZ または複数の MALZsの選択 294
マルチアカウントランディングゾーンアカウント 300
MALZ: Core アカウントのオンボーディング 334
AWS マルチアカウントランディングゾーンコアアカウントを作成する 334
AMS がアカウントにアクセスするための IAM ロールを作成する 336
ルートユーザーの多要素認証 (MFA) を使用して新しいアカウントを保護する 337
EPS AWS Marketplace の をサブスクライブする 337
ネットワークを設定する 338
アクセス管理を設定する 342
MALZ: アプリケーションアカウントのオンボーディング 347
新しいアプリケーションアカウントのリクエスト 348
AMS IAM ロールへのアクセスをフェデレーションするように Active Directory を設定する 349
新しいアプリケーションアカウントとのネットワークの設定 352
アプリケーションアカウントで追加の VPCs を設定する 354
付録: マルチアカウントランディングゾーン (MALZ) オンボーディングに関する考慮事項リスト 354
アカウント設定 355
AMS マルチアカウントランディングゾーンモニタリングアラート 356
ネットワーク構成 356
Active Directory の設定 357
Trend Micro Endpoint Protection (EPS) 357
アクセス: 踏み台、SSH、RDP 358
フェデレーション 359
AMS シングルアカウントランディングゾーン (SALZ) オンボーディング 360
AMS SALZ オンボーディングプロセス 360
SALZ ネットワークアーキテクチャ 361
AMS シングルアカウントランディングゾーン共有サービス 362

SALZ: AMS の新しい AWS アカウントを作成する 363
を作成する AWS アカウント 363
一括請求を設定する – 新しいアカウントを支払いアカウントにリンクする 366
AMS アクセス AWS アカウント 用に を設定する 367
EPS AWS Marketplace の をサブスクライブする 369
AWS Marketplace for CentOS 7.6 をサブスクライブする 370
ルートユーザーの多要素認証 (MFA) を使用して新しいアカウントを保護する 370
SALZ: ネットワークの設定 371
AMS 環境に IP スペースを割り当てる 371
AWS へのプライベートネットワーク接続を確立する 372
ファイアウォールをセットアップする 373
アプリケーション移行/オンボーディング中の AMS 踏み台オプション 374
SALZ: アクセス管理を設定する 375
Active Directory (AD) 信頼を確立する 376
AMS AWS Identity and Access Management ロールを使用して Active Directory をフェデレーションする 381
SALZ: デフォルト設定 387
エンドポイントセキュリティ (EPS) 387
セキュリティグループ 392
EC2 IAM インスタンスプロファイル 398
モニタリングされたメトリクスのデフォルト 405
ログの保持とローテーションのデフォルト 424
継続性管理のデフォルト 425
パッチ適用のデフォルト 426
AMS サービスの検証 (SALZ) 427
アカウント設定の検索 427
インスタンス ID または IP アドレスの検索 431
DNS フレンドリ踏み台名 434
踏み台 IP アドレスの検索 436
EC2 インスタンス: の作成 436
アクセス、リクエスト 445
その他 | その他の RFC、作成 (CLI) 453
スタック: 削除、再起動、開始、停止 455
アクセスの例 466
インシデントの報告 477
サービスリクエストの作成 479

オンボーディング後のステップ 482
チュートリアル 482
付録: SALZ オンボーディングアンケート 509
デプロイの概要 510
環境アーキテクチャに関する考慮事項 510
単一アカウントランディングゾーンのモニタリングアラート 511
メンテナンスウィンドウ 511
次のステップ 512
付録: ActiveDirectory フェデレーションサービス (ADFS) クレームルールと SAML 設定 513
ADFS クレームルールの設定 513
ウェブコンソール 514
SAML による API および CLI アクセス 514
スクリプト設定 514
Windows 設定 514
Linux 設定 516
ドキュメント履歴 518
..... dxxi

AWS Managed Servicesオンボーディングの概要

AWS Managed Services (AMS) へようこそ。AMS は、AWS インフラストラクチャを継続的に管理するエンタープライズサービスです。このガイドは、AMS の新しいアカウントのセットアップ、ネットワークと AMS へのアクセスの設定、オンボーディング設定の検証など、AMS の使用を開始するのに役立つように設計されています。

これは、AMS サービスを新しい AWS アカウントにオンボードするために必要なタスクの準備と実行を担当する IT 管理者を対象としています。AMS サービスのオンボーディングには、Active Directory の信頼を設定し、他のネットワークレベルのタスクを完了するための特別な権限が必要です。マルチアカウントランディングゾーンアカウントとシングルアカウントランディングゾーンアカウントのどちらを使用するかを決定する方法については、「単一の MALZ または複数の MALZs」を参照してください。

> **Important**
>
> このガイドは、この導入後に 2 つのパートに分かれています。1 つはマルチアカウントランディングゾーンアカウント用、もう 1 つはシングルアカウントランディングゾーンアカウント用です。オンボーディングは 2 つで大きく異なります。状況に適用されるガイドの「」セクションの横に進んでください。

トピック

- AMS について
- AMS の主要な用語
- AMS モード
- AMS アカウント後規範ガイダンス
- 何をするか、何をしないか
- AMS 出力トラフィック管理
- AMS の IAM ユーザーロール
- デフォルトのアクセスファイアウォールルール

AMS について

AMS をよりよく理解するには、以下の AMS ユーザーガイドのセクションを参照してください。

- AWS Managed Services とは AMS サービスを導入し、主要な機能、オペレーション、インターフェイス、一般的な AMS マネージドネットワークアーキテクチャについて説明します。この章では、AMS が管理するリソースへのアクセス方法や踏み台の使用など、アクセス管理についても説明します。
- 主要用語は、AMS 用語の定義と説明を提供します。
- AMS のデフォルトを理解すると、基本環境コンポーネント、IAM および EC2、プロキシ、モニタリング対象メトリクス、ログ記録、エンドポイントセキュリティ (EPS)、バックアップ、パッチ適用のデフォルト値など、AMS が使用するデフォルト値が提供されます。
- 変更管理は、変更リクエスト (RFCs) と変更タイプ (CTs) の仕組みの詳細と、AMS RFCs の使用例を提供します。
- いくつかの追加の章では、AWS コンソール、AMS CLI、AMS 変更管理システム、AMS SKMS、セキュリティ、サービスリクエスト、インシデント、モニタリング、ログ、EPS、バックアップ、パッチ管理の使用について説明します。

AMS マルチアカウントランディングゾーンアーキテクチャの詳細については、「マルチアカウントランディングゾーンネットワークアーキテクチャ」を参照してください。

AMS シングルアカウントランディングゾーンアーキテクチャの詳細については、「シングルアカウントランディングゾーンネットワークアーキテクチャ」を参照してください。

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や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、開発と運用の従来分離された機能をオートメーションの基盤の上に統合することで、開発サイクルの短縮、デプロイ頻度の増加、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、問題や問題がより迅速に発見されて解決され、ビジネス目標がより簡単に達成されます。
- ITIL: Information Technology Infrastructure Library (ITIL) は、IT サービスのライフサイクルを標準化するために設計された ITSM フレームワークです。ITIL は、IT サービスのライフサイクルをカバーする 5 つの段階で構成されています。サービス戦略、サービス設計、サービス移行、サービス運用、サービス改善です。
- IT サービス管理 (ITSM): IT サービスをビジネスニーズに合わせる一連のプラクティス。
- Managed Monitoring Services (MMS): AMS は、独自のモニタリングシステムである Managed Monitoring Service (MMS) を運用します。これは、 AWS ヘルスイベントを消費し、Amazon CloudWatch データ、および他の からのデータを集約し AWS のサービス、Amazon Simple Notification Service (Amazon SNS) トピックを通じて作成されたアラームを AMS オペレーター (オンライン 24 時間 365 日) に通知します。
- 名前空間: IAM ポリシーを作成するとき、または Amazon リソースネーム (ARNs) を操作するときに、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。

AMS モード

これを使用して、ビジネス成果を達成するための柔軟性と規範的ガバナンスの望ましい組み合わせに基づいて、アプリケーションをホストするための適切な AWS Managed Services (AMS) モードを選択します。

この情報の対象となる対象者は次のとおりです。

- ランディングゾーンの戦略とガバナンスを担当するカスタマーチーム。この情報は、チームが内部および外部の顧客に提供する AMS モードを使用して、AMS が管理するランディングゾーンの基盤を構築するのに役立ちます。
- アプリケーションの AMS への移行を担当するビジネスおよびアプリケーションの所有者。この情報は、アプリケーションの移行/ホストに適した AMS モードを使用して、アプリケーションの移行を計画するのに役立ちます。ソフトウェア開発ライフサイクル (SDLC) ライフサイクルのさまざまなフェーズで、同じアプリケーションを複数の AMS モードでホストできます。
- AMS パートナーには、AMS を構築して移行するためのさまざまなオプションについて顧客をガイドする役割があります。

この情報では、AMS を活用してクラウドへの移行を加速するという決定が既に下されていることを前提としています。クラウド移行ジャーニーの 2 つのポイントでこのホワイトペーパーを参照してください。まず、AMS マネージドプラットフォームをセットアップする基盤フェーズです。次に、基盤からクラウド導入ジャーニーの移行フェーズに移行する場合、AMS へのオンボーディングが完了した直後に、アプリケーションのガバナンスと運用に焦点を当てます。

AMS モードとアプリケーションまたはワークロード

新しいアプリケーションアカウントをリクエストするか、既存のアプリケーションアカウントでアプリケーションをホストして、適切なモードを選択するときは、アプリケーションの運用要件とガバナンス要件を検討してください。各アプリケーションまたはワークロードに適した AMS モードの選択は、次の要因によって異なります。

- 環境が提供する SDLC ライフサイクル関数のタイプ (変更がモデレートされていないサンドボックス、頻繁に変更される UAT、最小限の変更と高度に規制された本番稼働など)
- 必要なガバナンスポリシー (OU レベルで SCPs を通じて実施)
- 運用モデル (運用責任を所有する場合、または AMS にそれを外部委託する場合)
- クラウドでの運用にかかる時間や運用コストなど、期待されるビジネス成果。

> **Note**
>
> AMS サービスごとのモードタイプの詳細については、「AMS のモードとアカウントのタイプ」を参照してください。
> さまざまなモードの実際のユースケースについては、「AMS モードの実際のユースケース」を参照してください。

次の表は、アプリケーション所有者が最適な AMS モードを決定するための重要な考慮事項の概要を示しています。アプリケーション所有者は、特定のアプリケーションに適用されるモードを完全に理解するために、アプリケーション移行の前に評価フェーズを含める必要があります。例: クラウドネイティブサービスまたはサーバーレスアーキテクチャに基づくアプリケーションの場合、最適なオプションは、開発者モードで構築と反復を開始し、AMS Managed – SSP モードを使用して最終的な Infrastructure as Code をデプロイすることです。この場合、自動デプロイ用に作成された CloudFormation テンプレートが AMS によって定められた取り込みガイドラインを満たしていることを確認するために、軽いリファクタリングが必要になる場合があります。さらに、IAM アクセス許可は、最小特権モデルに従っていることを確認するために、AMS Security によって承認される必要があります。

アプリケーションをホストするために選択された AMS モードは、希望するクラウド運用モデルに向けて構築するのに役立ちます。

> **Note**
>
> 複数のクラウド運用モデルは、アプリケーションをホストするために選択されたさまざまな AMS モードに基づいて、単一の AMS Managed Landing Zone に存在できます。

決定の問題	標準 CM モード/ OOD*	AWS Service Catalog	直接変更モード	セルフサービスプロビジョニング	デベロッパーモード	カスタマー管理
運用準備状況						
ログ記録、モニタリング、イベント管理	すべてのマネージドインフラストラクチャを担当する AMS			セルフサービスプロビジョニングサービス (SSP) を担当するお客様	AMS CM システムの外部で開発者 IAM ロールを使用してプロビジョニングされたリソースを担当するお客様	お客様の責任
継続性管理	お客様が選択したバックアッププランを実行する AMS 責任			セルフサービスプロビジョニングサービス (SSP) を担当するお客様	AMS CM システムの外部で開発者 IAM ロールを使用してプロビジョニングされたリソースを担当するお客様	

決定の問題	標準 CM モード/ OOD*	AWS Service Catalog	直接変更モード	セルフサービスプロビジョニング	デベロッパーモード	カスタマー管理
インスタンスレベルのアクセス管理	オンプレミスドメインによる一方向 AD 信頼を通じて AMS 管理。マネージドインフラストラクチャが AMS ドメインに参加する必要がある			該当しない	AMS CM システムの外部で開発者 IAM ロールを使用してプロビジョニングされたリソースを担当するお客様	
セキュリティ管理とアカウントレベルのアクセス管理	すべてのマネージドアカウントの AMS 責任			すべてのマネージドアカウントを担当する AMS	AMS CM システムの外部で開発者 IAM ロールを使用してプロビジョニングされたリソースを担当するお客様	
パッチ管理	すべてのマネージドアカウントの AMS 責任			セルフサービスプロビジョニングサービス (SSP) を担当するお客様	AMS CM システムの外部で開発者 IAM ロールを使用してプロビジョニングされたリソースを担当するお客様	

決定の問題	標準 CM モード/ OOD*	AWS Service Catalog	直接変更モード	セルフサービスプロビジョニング	デベロッパーモード	カスタマー管理
変更管理	すべてのマネージドアカウントの AMS 責任			セルフサービスプロビジョニングサービス (SSP) を担当するお客様	AMS CM システムの外部で開発者 IAM ロールを使用してプロビジョニングされたリソースを担当するお客様	
プロビジョニング管理	AMS で提供されるプロビジョニングオプションの規範的および標準化	AMS 規範標準に従って AWS Service Catalog 用の AWS サービス API を直接使用する柔軟性	AMS 規範標準に従って AWS サービス API を直接使用する柔軟性	SSP サービスAPIs を直接使用する柔軟性	プロビジョニングに AWS サービス API を直接使用する柔軟性	

決定の問題	標準 CM モード/ OOD*	AWS Service Catalog	直接変更モード	セルフサービスプロビジョニング	デベロッパーモード	カスタマー管理
インシデント管理と監査	すべてのマネージドアカウントの AMS 責任				AMS 変更管理システムの外部で開発者 IAM ロールを使用してプロビジョニングされたリソースを担当するお客様	
GuardRails と共有インフラストラクチャ (ネットワーク) とセキュリティフレームワーク	AMS Core アカウントを活用した規範的および標準化					AMS Core アカウントを柔軟にカスタマイズ
アプリケーションの準備状況						

決定の問題	標準 CM モード/ OOD*	AWS Service Catalog	直接変更モード	セルフサービスプロビジョニング	デベロッパーモード	カスタマー管理
アプリケーションのリファクタリング	ライトリファクタリングが必要				ライトリファクタリングが必要 (AMS Standard CM を使用してプロビジョニングした場合)	リファクタリングが不要
AWS サービスのサポート	AMS でサポートされているものに限定					無制限
ビジネス上の考慮事項						
運用準備までの時間	3 ~ 6 か月			6 か月 + 顧客のアプリケーションオペレーションのコンピテンシーに依存する		お客様のインフラストラクチャとアプリケーション運用のコンピテンシーに応じて 6 ~ 18 か月
コスト	$$$$			$$$	$$	$

決定の問題	標準 CM モード/ OOD*	AWS Service Catalog	直接変更モード	セルフサービスプロビジョニング	デベロッパーモード	カスタマー管理
アプリケーション例	3 層スタックの Webserver、コンプライアンスと規制要件のアプリケーション			API Gateway を使用するウェブサーバー、ECS/EKS を活用したコンテナ化されたアプリケーション	Lambda、Glue、Athena などを使用する Data Lake アプリケーションでの反復/最適化	サンドボックス、サードパーティーマネージドアプリケーションなどの分散型アカウント/アプリケーション

*Operations On Demand (OOD) には、標準 CM モードを使用して、専用のリソースを通じて変更を管理するためのサービスがあります。詳細については、「Operations on Demand catalog of offerings」および「Cloud Service Delivery Manager (CSDM)」を参照してください。

> **Note**
>
> SSP モードとデベロッパーモードの料金比較では、同じ AWS サービスがプロビジョニングされていることを前提としています。

AMS モードとビジネスおよび IT 目標の比較

図に示すように、アプリケーション用に高度に制御され標準化されたガバナンスモデルをお探しの場合は、AMS 管理の標準変更モード、AWS Service Catalog モード、または直接変更モードが最適です。運用準備を必要とせずにアプリケーションのイノベーションに焦点を当てたカスタムガバナンスモデルが必要な場合は、カスタマーマネージドモードを選択します。カスタマーマネージドモードでは、インシデント管理、設定管理、プロビジョニング管理、セキュリティ管理、パッチ管理などの運用機能をサポートする人員、プロセス、ツールを確立する責任を負うため、アプリケーションの運用に時間がかかる場合があります。

AMS アカウント後規範ガイダンス

組織が分散運用と DevOps プラクティスを採用するにつれて、 Well Architected の柱を満たすためにワークロードをデプロイする前に、すべてのアカウントに適用する必要がある運用機能のコアセットがあります。

このリンクは、Word ドキュメントを含む ZIP ファイルと、スクリプトと例を含む ZIP ファイルをダウンロードします。自動アカウントセットアップは、新しいアプリケーションアカウントのセットアップを自動化またはブートストラップするための一連のスクリプトです。

新しいアカウントが販売され、ワークロードがデプロイされる前に、運用、セキュリティ、管理の観点からアカウントを準備するために、デフォルトのバックアッププラン、パッチウィンドウ、暗号化 (その他) を設定します。アプリケーションアカウントのセットアップの俊敏性、一貫性、応答性を向上させるために、次のサンプル「方法」が参照用に提供されています。

自動アカウントセットアップ。

何をするか、何をしないか

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

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

- 当社の業務：

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

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

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

- 行わないこと：

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

AMS 出力トラフィック管理

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

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

- 暗黙的な (透過的な) プロキシとして機能します。

  and

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

いくつか例を挙げます。

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

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

> **Note**
>
> - この情報は包括的ではありません。必須の外部サイトの一部はここには記載されていません。
> - このリストを拒否リストまたはブロック戦略で使用しないでください。
> - このリストは、出力フィルタリングルールセットの開始点として意図されており、実際のトラフィックがリストのどこから逸脱するかを正確に判断するためにレポートツールが使用されることを期待しています。

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

AMS の IAM ユーザーロール

IAM ロールは、 AWS アイデンティティができることとできないことを決定するアクセス許可ポリシーを持つアイデンティティであるという点で、IAM ユーザーと似ています AWS。ただし、ユーザーは 1 人の特定の人に一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。

現在、標準 AMS アカウントCustomer_ReadOnly_Roleには 1 つの AMS デフォルトユーザーロール があり、マネージド Active Directory を持つ AMS アカウントcustomer_managed_ad_user_roleには追加のロールがあります。

ロールポリシーは、CloudWatch および Amazon S3 ログアクション、AMS コンソールアクセス、ほとんどの に対する読み取り専用制限 AWS のサービス、アカウント S3 コンソールへのアクセス制限、AMS 変更タイプアクセスのアクセス許可を設定します。

さらに、 Customer_ReadOnly_Roleには、インスタンスを予約できる可変リザーブドインスタンスのアクセス許可があります。これにはいくつかのコスト削減値があるため、長期間一定数の Amazon EC2 インスタンスが必要になることがわかっている場合は、これらの APIs呼び出すことができます。詳細については、Amazon EC2 リザーブドインスタンス」を参照してください。

> **Note**
>
> IAM ユーザーのカスタム IAM ポリシーを作成するための AMS サービスレベル目標 (SLO) は、既存のポリシーが再利用されない限り、4 営業日です。既存の IAM ユーザーロールを変更する場合、または新しいロールを追加する場合は、IAM: エンティティの更新または IAM: エンティティ RFC の作成をそれぞれ送信します。

Amazon IAM ロールに慣れていない場合は、「IAM ロール」で重要な情報を確認してください。

マルチアカウントランディングゾーン (MALZ): AMS マルチアカウントランディングゾーンのデフォルト、カスタマイズされていないユーザーロールポリシーを確認するには、MALZ: デフォルトの IAM ユーザーロール次の「」を参照してください。

MALZ: デフォルトの IAM ユーザーロール

デフォルトのマルチアカウント AMS マルチアカウントランディングゾーンユーザーロールの JSON ポリシーステートメント。

> **Note**
>
> ユーザーロールはカスタマイズ可能で、アカウントごとに異なる場合があります。ロールの検索手順が表示されます。

これらは、デフォルトの MALZ ユーザーロールの例です。必要なポリシーが設定されていることを確認するには、AWS コマンドを実行するget-roleか、AWS Management -> IAM コンソールにサインインし、ナビゲーションペインでロールを選択します。

コア OU アカウントロール

コアアカウントは、MALZ が管理するインフラストラクチャアカウントです。AMS マルチアカウントランディングゾーン Core アカウントには、管理アカウントとネットワークアカウントが含まれます。

Core OU アカウント: 一般的なロールとポリシー

ロール	ポリシー
AWSManagedServicesReadOnlyRole	ReadOnlyAccess (パブリック AWS 管理ポリシー)。
AWSManagedServicesCaseRole	ReadOnlyAccess
	AWSSupportAccess (パブリック AWS 管理ポリシー)。
AWSManagedServicesChangeManagementRole (コアアカウントバージョン)	ReadOnlyAccess
	AWSSupportAccess
	AMSChangeManagementReadOnlyPolicy
	AMSChangeManagementInfrastructurePolicy

Core OU アカウント: 管理アカウントのロールとポリシー

ロール	ポリシー
AWSManagedServicesBillingRole	AMSBillingPolicy (AMSBillingPolicy)。
AWSManagedServicesReadOnlyRole	ReadOnlyAccess (パブリック AWS 管理ポリシー)。
AWSManagedServicesCaseRole	ReadOnlyAccess

ロール	ポリシー
	AWSSupportAccess (パブリック AWS 管理ポリシー)。
AWSManagedServicesChangeManagementRole (管理アカウントバージョン)	ReadOnlyAccess
	AWSSupportAccess
	AMSChangeManagementReadOnlyPolicy
	AMSChangeManagementInfrastructurePolicy
	AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

Core OU アカウント: ネットワークアカウントのロールとポリシー

ロール	ポリシー
AWSManagedServicesReadOnlyRole	ReadOnlyAccess (パブリック AWS 管理ポリシー)。
AWSManagedServicesCaseRole	ReadOnlyAccess
	AWSSupportAccess (パブリック AWS 管理ポリシー)。
AWSManagedServicesChangeManagementRole (ネットワークアカウントバージョン)	ReadOnlyAccess
	AWSSupportAccess
	AMSChangeManagementReadOnlyPolicy
	AMSChangeManagementInfrastructurePolicy
	AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

アプリケーションアカウントロール

アプリケーションアカウントロールは、アプリケーション固有のアカウントに適用されます。

アプリケーションアカウント: ロールとポリシー

ロール	ポリシー
AWSManagedServicesReadOnlyRole	ReadOnlyAccess (パブリック AWS 管理ポリシー)。
AWSManagedServicesCaseRole	ReadOnlyAccess
	AWSSupportAccess (パブリック AWS 管理ポリシー)。 このポリシーは、すべてのサポートオペレーションとリソースへのアクセスを提供します。詳細については、「AWS サポートの開始方法」を参照してください。
AWSManagedServicesSecurityOpsRole	ReadOnlyAccess
	AWSSupportAccess の例 このポリシーは、すべてのサポートオペレーションとリソースへのアクセスを提供します。
	AWSCertificateManagerFullAccess information、 (パブリック AWS 管理ポリシー)
	AWSWAFFullAccess information、 (パブリック AWS 管理ポリシー)。このポリシーは、AWS WAF リソースへのフルアクセスを許可します。
	AMSSecretsManagerSharedPolicy
AWSManagedServicesChangeManagementRole (アプリケーションアカウントバージョン)	ReadOnlyAccess

ロール	ポリシー
AWSManagedServicesAdminRole	AWSSupportAccess (パブリック AWS 管理ポリシー) 。 このポリシーは、すべてのサポートオペレーションとリソースへのアクセスを提供します。詳細については、「AWS サポートの開始方法」を参照してください。
	AMSSecretsManagerSharedPolicy
	AMSChangeManagementPolicy
	AMSReservedInstancesPolicy
	AMSS3Policy
	ReadOnlyAccess
	AWSSupportAccess
	AMSChangeManagementInfrastructurePolicy
	AWSMarketplaceManageSubscriptions
	AMSSecretsManagerSharedPolicy
	AMSChangeManagementPolicy
	AWSCertificateManagerFullAccess
	AWSWAFFullAccess
	AMSS3Policy
	AMSReservedInstancesPolicy

ポリシーの例

使用するほとんどのポリシーの例を示します。ReadOnlyAccess ポリシー (すべての AWS サービスへの読み取り専用アクセスを提供するページ) を表示するには、アクティブな AWS アカウント: ReadOnlyAccess がある場合、このリンクを使用できます。また、要約バージョンがここに含まれています。

AMSBillingPolicy

AMSBillingPolicy

新しい請求ロールは、経理部門が管理アカウントの請求情報またはアカウント設定を表示および変更するために使用できます。代替連絡先などの情報にアクセスしたり、アカウントリソースの使用状況を表示したり、請求のタブを保持したり、支払い方法を変更したりするには、このロールを使用します。この新しいロールは、AWS Billing IAM アクションのウェブページに記載されているすべてのアクセス許可で構成されます。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "aws-portal:ViewBilling",
                "aws-portal:ModifyBilling"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToBilling"
        },
        {
            "Action": [
                "aws-portal:ViewAccount",
                "aws-portal:ModifyAccount"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToAccountSettings"
        },
        {
            "Action": [
```

```
                "budgets:ViewBudget",
                "budgets:ModifyBudget"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToAccountBudget"
        },
        {
            "Action": [
                "aws-portal:ViewPaymentMethods",
                "aws-portal:ModifyPaymentMethods"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToPaymentMethods"
        },
        {
            "Action": [
                "aws-portal:ViewUsage"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToUsage"
        },
        {
            "Action": [
                "cur:DescribeReportDefinitions",
                "cur:PutReportDefinition",
                "cur:DeleteReportDefinition",
                "cur:ModifyReportDefinition"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToCostAndUsageReport"
        },
        {
            "Action": [
                "pricing:DescribeServices",
                "pricing:GetAttributeValues",
                "pricing:GetProducts"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToPricing"
```

```
        },
        {
            "Action": [
                "ce:*",
                "compute-optimizer:*"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToCostExplorerComputeOptimizer"
        },
        {
            "Action": [
                "purchase-orders:ViewPurchaseOrders",
                "purchase-orders:ModifyPurchaseOrders"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToPurchaseOrders"
        },
        {
            "Action": [
                "redshift:AcceptReservedNodeExchange",
                "redshift:PurchaseReservedNodeOffering"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToRedshiftAction"
        },
        {
            "Action": "savingsplans:*",
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AWSSavingsPlansFullAccess"
        }
    ]
}
```

AMSChangeManagementReadOnlyPolicy

AMSChangeManagementReadOnlyPolicy

すべての AMS 変更タイプと、リクエストされた変更タイプの履歴を表示するアクセス許可。

AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

デプロイをリクエストするアクセス許可 | マネージドランディングゾーン | 管理アカウント | アプリケーションアカウントを作成する (VPC を使用) 変更タイプ。

AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

デプロイをリクエストするアクセス許可 | マネージドランディングゾーン | ネットワークアカウント | アプリケーションルートテーブルの変更タイプを作成します。

AMSChangeManagementInfrastructurePolicy

AMSChangeManagementInfrastructurePolicy (管理用 | その他 | その他 CTs)

管理をリクエストするアクセス許可 | その他 | その他 | 作成、管理 | その他 | その他 | 変更タイプを更新する。

AMSSecretsManagerSharedPolicy

AMSSecretsManagerSharedPolicy

を通じて AMS によって共有されているシークレットパスワード/ハッシュを表示するアクセス許可 AWS Secrets Manager（監査用のインフラストラクチャへのパスワードなど）。

AMS と共有するためのシークレットパスワード/ハッシュを作成するアクセス許可 (デプロイする必要がある製品のライセンスキーなど）。

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
   "Sid": "AllowAccessToSharedNameSpaces",
   "Effect": "Allow",
   "Action": "secretsmanager:*",
   "Resource": [
    "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
```

```
    "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
   ]
  },
  {
   "Sid": "DenyGetSecretOnCustomerNamespace",
   "Effect": "Deny",
   "Action": "secretsmanager:GetSecretValue",
   "Resource": "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
  },
  {
   "Sid": "AllowReadAccessToAMSNameSpace",
   "Effect": "Deny",
   "NotAction": [
    "secretsmanager:Describe*",
    "secretsmanager:Get*",
    "secretsmanager:List*"
   ],
   "Resource": "arn:aws:secretsmanager:*:*:secret:ams-shared/*"
  }
 ]
}
```

AMSChangeManagementPolicy

`AMSChangeManagementPolicy`

すべての AMS 変更タイプをリクエストおよび表示するアクセス許可、およびリクエストされた変更タイプの履歴。

AMSReservedInstancesPolicy

`AMSReservedInstancesPolicy`

Amazon EC2 リザーブドインスタンスを管理するアクセス許可。料金情報については、Amazon EC2 リザーブドインスタンス」を参照してください。

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
  "Sid": "AllowReservedInstancesManagement",
```

```
  "Effect": "Allow",
  "Action": [
   "ec2:ModifyReservedInstances",
   "ec2:PurchaseReservedInstancesOffering"
  ],
  "Resource": [
   "*"
  ]
 }]
}
```

AMSS3Policy

AMSS3Policy

既存の Amazon S3 バケットからファイルを作成および削除するアクセス許可。

> **Note**
>
> これらのアクセス許可は、S3 バケットを作成する機能を付与しません。これは、デプロイ | 高度なスタックコンポーネント | S3 ストレージ | 変更タイプの作成で実行する必要があります。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:PutObject"
            ],
            "Resource": "*"
        }
    ]
}
```

AWSSupportAccess

AWSSupportAccess

へのフルアクセス サポート。詳細については、「 の開始方法 サポート」を参照してください。プレミアムサポートの詳細については、「」を参照してくださいサポート。

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
  "Effect": "Allow",
  "Action": [
   "support:*"
  ],
  "Resource": "*"
 }]
}
```

AWSMarketplaceManageSubscriptions

AWSMarketplaceManageSubscriptions (パブリック AWS管理ポリシー)

AWS Marketplace サブスクリプションをサブスクライブ、サブスクライブ解除、表示するアクセス許可。

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
  "Action": [
   "aws-marketplace:ViewSubscriptions",
   "aws-marketplace:Subscribe",
   "aws-marketplace:Unsubscribe"
  ],
  "Effect": "Allow",
  "Resource": "*"
 }]
```

```
}
```

AWSCertificateManagerFullAccess

`AWSCertificateManagerFullAccess`

へのフルアクセス AWS Certificate Manager。詳細については、「AWS Certificate Manager」を参照してください。

`AWSCertificateManagerFullAccess` information、 (パブリック AWS 管理ポリシー) 。

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
  "Effect": "Allow",
  "Action": [
   "acm:*"
  ],
  "Resource": "*"
 }]
}
```

AWSWAFFullAccess

`AWSWAFFullAccess`

へのフルアクセス AWS WAF。詳細については、「 AWS WAF - Web Application Firewall」を参照してください。

`AWSWAFFullAccess` information、 (パブリック AWS 管理ポリシー) 。このポリシーは、 AWS WAF リソースへのフルアクセスを許可します。

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
```

```
  "Action": [
   "waf:*",
   "waf-regional:*",
   "elasticloadbalancing:SetWebACL"
  ],
  "Effect": "Allow",
  "Resource": "*"
 }]
}
```

ReadOnlyAccess

`ReadOnlyAccess`

AWS コンソール上のすべての AWS サービスとリソースへの読み取り専用アクセス。が新しいサービス AWS を起動すると、AMS は ReadOnlyAccess ポリシーを更新して、新しいサービスの読み取り専用アクセス許可を追加します。更新されたアクセス権限は、ポリシーがアタッチされているすべてのプリンシパルエンティティに適用されます。

これにより、EC2 ホストまたはデータベースホストにログインすることはできません。

アクティブな がある場合は AWS アカウント、このリンク ReadOnlyAccess を使用して ReadOnlyAccess ポリシー全体を表示できます。ReadOnlyAccess ポリシー全体は、すべてへの読み取り専用アクセスを提供する限り、非常に長くなります AWS のサービス。以下は、ReadOnlyAccess ポリシーの一部の抜粋です。

単一アカウントランディングゾーン (SALZ): AMS シングルアカウントランディングゾーンのデフォルト、カスタマイズされていないユーザーロールポリシーを確認するには、SALZ: デフォルトの IAM ユーザーロール次の「」を参照してください。

SALZ: デフォルトの IAM ユーザーロール

デフォルトの AMS シングルアカウントランディングゾーンユーザーロールの JSON ポリシーステートメント。

> **Note**
>
> SALZ のデフォルトのユーザーロールはカスタマイズ可能で、アカウントごとに異なる場合があります。ロールの検索手順が表示されます。

デフォルトの SALZ ユーザーロールの例を次に示します。ポリシーが設定されていることを確認するには、 get-role コマンドを実行します。または、https://console.aws.amazon.com/iam/ で AWS Identity and Access Management コンソールにサインインし、ロールを選択します。

顧客の読み取り専用ロールは、複数のポリシーの組み合わせです。ロール (JSON) の内訳は次のとおりです。

マネージドサービス監査ポリシー :

マネージドサービス IAM ReadOnly ポリシー

マネージドサービスユーザーポリシー

```
{
 "Version": "2012-10-17",
 "Statement": [
   {
     "Sid": "AllowCustomerToListTheLogBucketLogs",
     "Effect": "Allow",
     "Action": [
       "s3:ListBucket"
     ],
     "Resource": [
       "arn:aws:s3:::mc-a*-logs-*"
     ],
     "Condition": {
       "StringLike": {
         "s3:prefix": [
           "aws/*",
           "app/*",
           "encrypted",
           "encrypted/",
           "encrypted/app/*"
         ]
       }
     }
   },
   {
     "Sid": "BasicAccessRequiredByS3Console",
     "Effect": "Allow",
     "Action": [
       "s3:ListAllMyBuckets",
       "s3:GetBucketLocation"
```

```
      ],
      "Resource": [
        "arn:aws:s3:::*"
      ]
    },
    {
      "Sid": "AllowCustomerToGetLogs",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject*"
      ],
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*/aws/*",
        "arn:aws:s3:::mc-a*-logs-*/encrypted/app/*"
      ]
    },
    {
      "Sid": "AllowAccessToOtherObjects",
      "Effect": "Allow",
      "Action": [
        "s3:DeleteObject*",
        "s3:Get*",
        "s3:List*",
        "s3:PutObject*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AllowCustomerToListTheLogBucketRoot",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*"
      ],
      "Condition": {
        "StringEquals": {
          "s3:prefix": [
            "",
            "/"
          ]
```

```
        }
      }
    },
    {
      "Sid": "AllowCustomerCWLConsole",
      "Effect": "Allow",
      "Action": [
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Sid": "AllowCustomerCWLAccessLogs",
      "Effect": "Allow",
      "Action": [
        "logs:FilterLogEvents",
        "logs:GetLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:/aws/*",
        "arn:aws:logs:*:*:log-group:/infra/*",
        "arn:aws:logs:*:*:log-group:/app/*",
        "arn:aws:logs:*:*:log-group:RDSOSMetrics:*:*"
      ]
    },
    {
      "Sid": "AWSManagedServicesFullAccess",
      "Effect": "Allow",
      "Action": [
        "amscm:*",
        "amsskms:*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "ModifyAWSBillingPortal",
      "Effect": "Allow",
      "Action": [
        "aws-portal:Modify*"
```

```
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "DenyDeleteCWL",
      "Effect": "Deny",
      "Action": [
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Sid": "DenyMCCWL",
      "Effect": "Deny",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:PutLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:/mc/*"
      ]
    },
    {
      "Sid": "DenyS3MCNamespace",
      "Effect": "Deny",
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*/encrypted/mc/*",
        "arn:aws:s3:::mc-a*-logs-*/mc/*",
        "arn:aws:s3:::mc-a*-logs-*-audit/*",
        "arn:aws:s3:::mc-a*-internal-*/*",
        "arn:aws:s3:::mc-a*-internal-*"
      ]
```

```
    },
    {
      "Sid": "ExplicitDenyS3CfnBucket",
      "Effect": "Deny",
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::cf-templates-*"
      ]
    },
    {
      "Sid": "DenyListBucketS3LogsMC",
      "Action": [
        "s3:ListBucket"
      ],
      "Effect": "Deny",
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*"
      ],
      "Condition": {
        "StringLike": {
          "s3:prefix": [
            "auditlog/*",
            "encrypted/mc/*",
            "mc/*"
          ]
        }
      }
    },
    {
      "Sid": "DenyS3LogsDelete",
      "Effect": "Deny",
      "Action": [
        "s3:Delete*",
        "s3:Put*"
      ],
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*/*"
      ]
    },
    {
      "Sid": "DenyAccessToKmsKeysStartingWithMC",
      "Effect": "Deny",
```

```
      "Action": [
        "kms:*"
      ],
      "Resource": [
        "arn:aws:kms::*:key/mc-*",
        "arn:aws:kms::*:alias/mc-*"
      ]
    },
    {
      "Sid": "DenyListingOfStacksStartingWithMC",
      "Effect": "Deny",
      "Action": [
        "cloudformation:*"
      ],
      "Resource": [
        "arn:aws:cloudformation:*:*:stack/mc-*"
      ]
    },
    {
      "Sid": "AllowCreateCWMetricsAndManageDashboards",
      "Effect": "Allow",
      "Action": [
        "cloudwatch:PutMetricData"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AllowCreateandDeleteCWDashboards",
      "Effect": "Allow",
      "Action": [
        "cloudwatch:DeleteDashboards",
        "cloudwatch:PutDashboard"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Customer Secrets Manager 共有ポリシー

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSecretsManagerListSecrets",
      "Effect": "Allow",
      "Action": "secretsmanager:listSecrets",
      "Resource": "*"
    },
    {
      "Sid": "AllowCustomerAdminAccessToSharedNameSpaces",
      "Effect": "Allow",
      "Action": "secretsmanager:*",
      "Resource": [
        "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
        "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
      ]
    },
   {
      "Sid": "DenyCustomerGetSecretCustomerNamespace",
      "Effect": "Deny",
      "Action": "secretsmanager:GetSecretValue",
      "Resource": "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
    },
    {
      "Sid": "AllowCustomerReadOnlyAccessToAMSNameSpace",
      "Effect": "Deny",
      "NotAction": [
        "secretsmanager:Describe*",
        "secretsmanager:Get*",
        "secretsmanager:List*"
      ],
      "Resource": "arn:aws:secretsmanager:*:*:secret:ams-shared/*"
    }
  ]
}
```

Customer Marketplace サブスクライブポリシー

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowMarketPlaceSubscriptions",
      "Effect": "Allow",
      "Action": [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Subscribe"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

デフォルトのアクセスファイアウォールルール

これらは、インスタンスへのアクセスに必要なデフォルトのファイアウォールルールです。

> **Note**
>
> AD の一方向信頼を確立するために必要なファイアウォールルールとポートの詳細については、AWS Artifact コンソール -> レポートタブに移動し、AWS Managed Servicesを検索して、AMS セキュリティガイドを参照してください。

Linux スタックインスタンスポート

これらのルールは、AMS Linux スタックへの認証に必要です。

Linux インスタンスポートルール FROM: Linux スタックインスタンス TO: CORP ドメインコントローラー

ポート	プロトコル	サービス	[Direction] (方向)
389	TCP	LDAP	Ingress
389	UDP	LDAP	Ingress
88	TCP	Kerberos	Ingress
88	UDP	Kerberos	Ingress

Windows スタックインスタンスポート

これらのルールは、AMS Windows スタックへの認証に必要です。

FROM: Windows スタックインスタンス TO: CORP ドメインコントローラー

ポート	プロトコル	サービス	[Direction] (方向)
88	TCP | UDP	Kerberos	イングレスとエグレス
135	TCP | UDP	DCE/RPC ロケーターサービス	イングレスとエグレス
389	TCP | UDP	LDAP	イングレスとエグレス
3268	TCP | UDP	msft-gc、Microsoft Global Catalog (Active Directory フォレストからのデータを含む LDAP サービス)	イングレスとエグレス
445	TCP	Microsoft-DS Active Directory 、Windows 共有	イングレスとエグレス
49152 - 65535	TCP	IANA に登録できない動的ポートまたはプライベートポート。この範囲は、プライベートサービス、カスタ	イングレスとエグレス

ポート	プロトコル	サービス	[Direction] (方向)
		マイズされたサービス、または一時的な目的、およびエフェメラルポートの自動割り当てに使用されます。	

AWS Managed Services でのサービス管理

トピック

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

AMS サービスの仕組み。

AWS Managed Services でのアカウントガバナンス

このセクションでは、AMS アカウントガバナンスについて説明します。

お客様は、AMS 全体でアドバイザリ支援を提供するクラウドサービスデリバリーマネージャー (CSDM) として指定され、マネージド環境のユースケースとテクノロジーアーキテクチャを詳細に理解しています。CSDMs、必要に応じてアカウントマネージャー、テクニカルアカウントマネージャー、AWS Managed Services クラウドアーキテクト (CAs)、および AWS ソリューションアーキテクト (SAs) と連携して、新しいプロジェクトの立ち上げを支援し、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 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。

AWS Managed Services でのサービス開始

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

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

サービスの開始

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

サービス開始

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

顧客関係管理 (CRM)

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

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

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

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

CRM プロセス

CRM プロセスには、次のアクティビティが含まれます。

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

CRM 会議

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

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

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

CRM ミーティングの手配

AMS CSDM は、以下を含む会議を文書化する責任があります。

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

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

> **Note**
>
> CSDM はお客様と協力してアカウントガバナンスを確立します。

CRM 月次レポート

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

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

> **Note**
>
> 説明されている情報に加えて、CSDM は、AMS による運用活動のための下請業者の使用など、範囲または条件の重要な変更についても通知します。
> AMS は、CSDM が月次レポートに含めるパッチ適用とバックアップに関するレポートを生成します。レポート生成システムの一部として、AMS はアクセスできないインフラストラクチャをアカウントに追加します。
>
> - 未加工データが報告された S3 バケット
> - データをクエリするためのクエリ定義を含む Athena インスタンス
> - S3 バケットから raw データを読み取る Glue クローラ

AWS Managed Servicesコスト最適化

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

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

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

コスト最適化フレームワーク

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

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

マネージド環境のコスト最適化手段を特定する

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

最適化に関する推奨事項には、次のようなものがあります。

アーキテクチャ最適化の推奨事項：

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

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

EC2 インスタンスに焦点を当てた推奨事項

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

アカウントに焦点を当てたレコメンデーション

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

顧客に提示し、計画を支援する

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

レコメンデーションの実装を支援し、コストへの影響を測定する

AMS は、コストへの影響と最適化の変更の達成と測定を支援します。

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

コスト最適化責任マトリックス

AMS コスト最適化の責任。

コスト最適化 RACI

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

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

AWS Managed Services のサービス時間

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

AWS Managed Services でのヘルプの取得

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

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

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

変更管理モード

AWS Managed Services (AMS) は、変更管理モードを使用して AMS Advanced の変更を保護します。変更管理モードは、環境の高い運用基準を維持し、リスクを制御し、悪影響を防ぐのに役立ちます。AMS Advanced には、さまざまなレベルのコントロールとリスクを提供するさまざまなモードがあります。カスタマー管理モードを除くすべてのモードは、AMS によって管理されます。使用可能な変更管理モードは次のとおりです。

- RFC モード (以前の標準 CM モード): 「変更のリクエスト」 (RFC) システムと AMS カスタム変更タイプ (CTs
- 直接変更モード: RFC モードと同じで、AWS APIs とコンソールを使用して AMS マネージドリソースを作成する
- AMS での AWS Service Catalog: Direct Change モードと同様ですが、AMS 変更管理システム (RFCs) を使用する代わりに、 AWS Service Catalog を使用して AMS が管理するリソースを作成します。
- デベロッパーモード: 直接変更モードと同じですが、AWS APIs とコンソールで作成したリソースのみが AMS 管理対象ではなく、その管理はお客様の責任となります。
- セルフサービスプロビジョニング (SSP) モード: AMS 変更管理システムにアクセスできない (RFCs なし) 点を除き、デベロッパーモードと同じ
- カスタマーマネージドモード: AMS はマルチアカウントランディングゾーンランディングゾーンを提供しますが、すべてのリソース管理はお客様の責任となります。

AWS Managed Services (AMS) 変更管理システムは、変更管理 (CM) API を使用して、マルチアカウントランディングゾーン (MALZ) アカウントとシングルアカウントランディングゾーン (SALZ) アカウントの両方の変更リクエスト (RFCs) を作成および管理するためのオペレーションを提供します。

変更リクエスト (RFC) は、AMS インターフェイスを介してユーザーまたは AMS がマネージド環境に変更を加えるために作成したリクエストであり、特定のオペレーションの変更タイプ (CT) ID が含まれます。

AMS 変更管理 (CM) API は、変更リクエスト (RFCs) を作成および管理するためのオペレーションを提供します。RFCs を作成、更新、送信、承認、拒否、キャンセルできます。AMS 演算子は、RFCs を作成、更新、送信、承認、拒否、キャンセル、およびクローズとしてマークできます。

タグや他の名前で使用されない AMS リザーブドプレフィックスのリストについては、「リザーブドプレフィックス」を参照してください。

スキーマや例など、各変更タイプの詳細については、「AMS 変更タイプリファレンス」を参照してください。

> **Note**
>
> すべての変更管理 API コールは AWS CloudTrail に記録されます。詳細については、「ログへのアクセス」を参照してください。

モードの概要

この情報を使用して、ビジネス成果を達成するための柔軟性と規範的なガバナンスの望ましい組み合わせに基づいて、アプリケーションをホストするための適切な AWS Managed Services (AMS) モードを選択します。

この情報の対象となる対象者は次のとおりです。

- ランディングゾーンの戦略とガバナンスを担当するカスタマーチーム。この情報は、チームが内部および外部の顧客に提供する AMS モードを使用して、AMS が管理するランディングゾーンの基盤を構築するのに役立ちます。
- アプリケーションの AMS への移行を担当するビジネスオーナーとアプリケーションオーナー。この情報は、アプリケーションの移行/ホストに適した AMS モードを使用して、アプリケーションの移行を計画するのに役立ちます。ソフトウェア開発ライフサイクル (SDLC) ライフサイクルのさまざまなフェーズで、同じアプリケーションを複数の AMS モードでホストできます。
- AMS パートナーには、AMS を構築して移行するためのさまざまなオプションについて顧客をガイドする役割があります。

この情報は、AMS マネージドプラットフォームを設定する基盤フェーズ中、および基盤からクラウド導入ジャーニーの移行フェーズに移行するときに、AMS へのオンボーディングが完了し、アプリケーションのガバナンスと運用に重点を置いている直後に最も役立ちます。

AMS のモードとアカウントのタイプ

AWS Managed Services (AMS) モードは、各モードの特定のガバナンスフレームワークの下で AMS サービスとやり取りする方法として定義できます。ランディングゾーンの違い、マルチアカウントランディングゾーンまたは MALZ とシングルアカウントランディングゾーンまたは SALZ が記録されます。

> **Note**
>
> アプリケーションのデプロイと適切な AMS モードの選択の詳細については、「AMS モードとアプリケーションまたはワークロード」を参照してください。
> さまざまなモードの実際のユースケースについては、「AMS モードの実際のユースケース」を参照してください。

次の表は、AMS サービスあたりのモードの説明です。

AMS 機能	RFC モード (以前の標準 CM モード)/ OOD*	直接変更モード	AWS Service Catalog	セルフサービスプロビジョニング/デベロッパーモード	カスタマー管理
ランディングゾーンの設定	MALZ と SALZ	MALZ と SALZ	MALZ と SALZ		
変更管理	変更スケジュール、手動変更のレビュー、変更レコード	IAM やセキュリティグループなどの高リスクの変更の RFC モードと同じ	なし		
ログ記録、モニタリング、ガードレール、イベント管理	はい (サポートされているリソース)			なし	
継続性管理	はい (サポートされているリソース)			該当なし/いいえ	なし
セキュリティ管理	インスタンスレベルのセキュリティコントロールとアカウントレベルのコントロール			アカウントレベルのコントロール	AWS 組織レベルのコントロール

AMS 機能	RFC モード (以前の標準 CM モード)/ OOD*	直接変更モード	AWS Service Catalog	セルフサービスプロビジョニング/デベロッパーモード	カスタマー管理
パッチ管理	あり			該当なし/いいえ	なし
インシデントと問題の管理	AMS がサポートするリソースの応答と解決の SLA			結果のリソースのレスポンス SLA	なし
レポート作成	あり			なし	
サービスリクエスト管理	あり			サポートリクエストのみ	なし

*Operations On Demand (OOD) には、RFC モードを使用して、専用のリソースを通じて変更を管理するためのサービスがあります。詳細については、「Operations on Demand catalog of offerings」および「Cloud Service Delivery Manager (CSDM)」を参照してください。

> **Note**
>
> AMS でのセルフサービスプロビジョニングモード と はどちらも、ネイティブ AWS サービスに根ざした複雑なアーキテクチャを持つアプリケーションに適しているように見えるAMS Advanced Developer モード場合があります。ワークロードを設計するときは、ビジネスコンテキストに基づいて、運用上の優秀性と俊敏性のトレードオフを行います。これは、アプリケーションの SSP モードまたはデベロッパーモードの選択を検討する良い方法です。選択は、アプリケーションの SDLC フェーズに基づいて変更される場合があります。例: アプリケーションが本番環境に対応している場合、このモードでは AMS ガードレールが厳しくなるため、SSP モードの方が適切なオプションである可能性があります。ガードレールは、アプリケーション OU レベルで IAM 更新や SCPs の RFC ベースの変更管理などの予防的コントロールの形式で適用されます。これらのビジネス上の意思決定がエンジニアリングの優先度を左右する可能性があります。ガバナンスと運用サポートを犠牲にして、「事前生産」フェーズでアプリケーション所有者の柔軟性を高めるように最適化できます。

MALZ アーキテクチャと関連する AMS モード

AMS マルチアカウントランディングゾーン (MALZ) では、デフォルトの組織単位 (OU)、カスタマーマネージド OU、マネージド OU、または開発 OU でアプリケーションアカウント (またはリソースアカウント) を自動的にプロビジョニングできます。これらの各 OUs で作成されたアプリケーションアカウントでプロビジョニングされるインフラストラクチャは、これらの基本 OUs によって提供される特定の AMS モードの対象となります。同じアプリケーションアカウントで 2 つ以上のモードの組み合わせを見つけるのが一般的です。例えば、RFC モードと SSP モードは、トリガー関数には API Gateway と Lambda、取り込みとオーケストレーションには EC2, S3、SQS で構成されるパイプラインアーキテクチャをホストする AMS マネージドアカウントに共存できます。この場合、SSP モードは Lambda と API Gateway に適用されます。

図 1 は、AMS の基本的な OUs を通じてさまざまなモードがどのように提供されるかを示しています。AMS で新しいアプリケーションアカウントをリクエストする場合は、アカウントの OU を選択する必要があります。

MALZ アーキテクチャと関連する AMS モード

AMS は、サービスコントロールポリシー (SCP) OUs を活用します。 SCPs これは、各 AMS モードを使用してガバナンスフレームワークを適用する方法として機能します。基礎 OUs に適用されるガバナンスとセキュリティガードレール (SCPsの形式) も、カスタム/子 OUs に自動的に適用されます。子 OUs に追加の SCPs をリクエストできます。アプリケーションアカウントはモードと同じではないことを理解することが重要です。モードは、アカウント内でプロビジョニングされたインフラストラクチャに適用され、AMS と顧客間の運用責任を定義します。

図 1: MALZ アーキテクチャと関連する AMS モード

> **Note**
>
> 「制限OUs のカスタムポリシーをリクエストできることを意味します。ポリシーは、AMS の機能に干渉して運用上の優秀性を提供しないように、case-by-caseで AMS によって承認されます。AMS ガードレールの詳細なリストについては、 ユーザーガイドの「AMS ガードレール」を参照してください。

AMS モードとアプリケーションまたはワークロード

新しいアプリケーションアカウントをリクエストするか、既存のアプリケーションアカウントでアプリケーションをホストして、適切なモードを選択するときは、アプリケーションの運用要件とガバナンス要件を検討してください。各アプリケーションまたはワークロードに適した AMS モードの選択は、次の要因によって異なります。

- 環境が提供する SDLC ライフサイクル関数のタイプ (変更がモデレートされていないサンドボックス、頻繁に変更される UAT、最小限の変更と高度に規制された本番稼働など)
- 必要なガバナンスポリシー (OU レベルで SCPs を通じて実施)
- 運用モデル (運用責任を所有する場合、またはそれを AMS に外部委託する場合)
- クラウドでの運用にかかる時間や運用コストなど、期待されるビジネス成果。

> **Note**
>
> AMS サービスごとのモードタイプの詳細については、「AMS のモードとアカウントのタイプ」を参照してください。
> さまざまなモードの実際のユースケースについては、「AMS モードの実際のユースケース」を参照してください。

次の表は、アプリケーション所有者が最適な AMS モードを決定するための重要な考慮事項の概要を示しています。アプリケーション所有者は、特定のアプリケーションに適用されるモードを完全に理解するために、アプリケーション移行の前に評価フェーズを含める必要があります。例: クラウドネイティブサービスまたはサーバーレスアーキテクチャに基づくアプリケーションの場合、最適なオプションは、開発者モードで構築と反復を開始し、AMS Managed – SSP モードを使用して最終的な Infrastructure as Code をデプロイすることです。この場合、自動デプロイ用に作成された CloudFormation テンプレートが AMS によって定められた取り込みガイドラインを確実に満たすために、軽いリファクタリングが必要になる場合があります。さらに、IAM アクセス許可は、最小特権モデルに従っていることを確認するために、AMS Security によって承認される必要があります。

アプリケーションをホストするために選択された AMS モードは、希望するクラウド運用モデルに向けて構築するのに役立ちます。

> **Note**
>
> 複数のクラウド運用モデルは、アプリケーションをホストするために選択されたさまざまな AMS モードに基づいて、単一の AMS Managed Landing Zone に存在できます。

決定の問題	標準 CM モード/ OOD*	AWS Service Catalog	直接変更モード	セルフサービスプロビジョニング	デベロッパーモード	カスタマーマネージド
運用準備状況						
ログ記録、モニタリング、イベント管理	すべてのマネージドインフラストラクチャを担当する AMS			セルフサービスプロビジョニングサービス (SSP) を担当するお客様	AMS CM システムの外部で開発者 IAM ロールを使用してプロビジョニングされたリソースを担当するお客様	お客様の責任
継続性管理	お客様が選択したバックアッププランを実行する AMS 責任			セルフサービスプロビジョニングサービス (SSP) を担当するお客様	AMS CM システムの外部で開発者 IAM ロールを使用してプロビジョニングされたリソースを担当するお客様	
インスタンスレベ	オンプレミスドメインによる一方向 AD 信頼を通じて AMS 管理。マネージ			該当しない	AMS CM システムの外部で開発者	

決定の問題	標準 CM モード/ OOD*	AWS Service Catalog	直接変更モード	セルフサービスプロビジョニング	デベロッパーモード	カスタマーマネージド
ルのアクセス管理	ドインフラストラクチャが AMS ドメインに参加する必要がある				IAM ロールを使用してプロビジョニングされたリソースを担当するお客様	
セキュリティ管理とアカウントレベルのアクセス管理	すべてのマネージドアカウントの AMS 責任			すべてのマネージドアカウントを担当する AMS	AMS CM システムの外部で開発者 IAM ロールを使用してプロビジョニングされたリソースを担当するお客様	
パッチ管理	すべてのマネージドアカウントの AMS 責任			セルフサービスプロビジョニングサービス (SSP) を担当するお客様	AMS CM システムの外部で開発者 IAM ロールを使用してプロビジョニングされたリソースを担当するお客様	

決定の問題	標準 CM モード/ OOD*	AWS Service Catalog	直接変更モード	セルフサービスプロビジョニング	デベロッパーモード	カスタマーマネージド
変更管理	すべてのマネージドアカウントの AMS 責任			セルフサービスプロビジョニングサービス (SSP) を担当するお客様	AMS CM システムの外部で開発者 IAM ロールを使用してプロビジョニングされたリソースを担当するお客様	
プロビジョニング管理	AMS で提供されるプロビジョニングオプションの規範的および標準化	AMS 規範標準に従って AWS Service Catalog 用の AWS サービス API を直接使用する柔軟性	AMS 規範標準に従って AWS サービス API を直接使用する柔軟性	SSP サービスAPIs を直接使用する柔軟性	プロビジョニングに AWS サービス API を直接使用する柔軟性	

決定の問題	標準 CM モード/ OOD*	AWS Service Catalog	直接変更モード	セルフサービスプロビジョニング	デベロッパーモード	カスタマーマネージド
インシデント管理と監査	すべてのマネージドアカウントの AMS 責任				AMS 変更管理システムの外部で開発者 IAM ロールを使用してプロビジョニングされたリソースを担当するお客様	
GuardRails と共有インフラストラクチャ (ネットワーク) とセキュリティフレームワーク	AMS Core アカウントを活用した規範的および標準化					AMS Core アカウントを柔軟にカスタマイズ
アプリケーションの準備状況						

決定の問題	標準 CM モード/ OOD*	AWS Service Catalog	直接変更モード	セルフサービスプロビジョニング	デベロッパーモード	カスタマーマネージド
アプリケーションのリファクタリング	ライトリファクタリングが必要				ライトリファクタリングが必要 (AMS Standard CM を使用してプロビジョニングされている場合)	リファクタリングが不要
AWS サービスのサポート	AMS でサポートされているものに限定					無制限
ビジネス上の考慮事項						
運用準備時間	3 ~ 6 か月			6 か月 + 顧客のアプリケーションオペレーションのコンピテンシーに依存する		お客様のインフラストラクチャとアプリケーション運用のコンピテンシーに応じて 6 ~ 18 か月
コスト	$$$$			$$$	$$	$

決定の問題	標準 CM モード/ OOD*	AWS Service Catalog	直接変更モード	セルフサービスプロビジョニング	デベロッパーモード	カスタマーマネージド
アプリケーション例	3 層スタックの Webserver、コンプライアンスと規制要件のアプリケーション			API Gateway を使用するウェブサーバー、ECS/EKS を活用したコンテナ化されたアプリケーション	Lambda、Glue、Athena などを使用する Data Lake アプリケーションでの反復/最適化	サンドボックス、サードパーティーマネージドアプリケーションなどの分散型アカウント/アプリケーション

*Operations On Demand (OOD) には、標準 CM モードを使用して、専用のリソースを通じて変更を管理するお客様向けのサービスがあります。詳細については、「Operations on Demand catalog of offerings」および「Cloud Service Delivery Manager (CSDM)」を参照してください。

> **Note**
>
> SSP モードとデベロッパーモードの料金比較では、同じ AWS サービスがプロビジョニングされていることを前提としています。

AMS モードとビジネス目標および IT 目標の比較

図に示すように、アプリケーション用に高度に制御され標準化されたガバナンスモデルをお探しの場合は、AMS 管理の標準変更モード、AWS Service Catalog モード、または直接変更モードが最適です。運用準備を必要とせずにアプリケーションのイノベーションに焦点を当てたカスタムガバナンスモデルが必要な場合は、カスタマーマネージドモードを選択します。カスタマーマネージドモードでは、インシデント管理、設定管理、プロビジョニング管理、セキュリティ管理、パッチ管理などの運用機能をサポートする人員、プロセス、ツールを確立する責任を負うため、アプリケーションの運用に時間がかかる場合があります。

AMS モードの実際のユースケース

これらを調べて、AMS モードの使用方法を判断します。

- ユースケース 1 は、時間的制約のあるデータセンターの出口でコストを削減するためのビジネス上の課題です。データセンターの出口など、魅力的なビジネスイベントがある企業は、オンプレミスアプリケーションをクラウド上で再ホストすることに関心を持っています。オンプレミスインベントリのほとんどは、オペレーティングシステムのバージョンが混在する Windows サーバーと Linux サーバーで構成されます。そうすることで、お客様はクラウドへの移行によるコスト削減を活用し、アプリケーションの技術的およびセキュリティ上の体制を改善したいと考えています。お客様は迅速に移行したいと考えていますが、社内のクラウド運用の専門知識はまだ構築されていません。お客様はリファクタリングのバランスを見つける必要があります。リファクタリングが多すぎると、厳しいタイムラインに対してリスクが高くなります。ただし、OS バージョンの更新やデータベースの最適化などのリファクタリングにより、アプリケーションは次のレベルのパフォーマンスを達成できます。この例では、お客様は AMS マネージド RFC モードを選択して、ほとんどのアプリケーションをリホストできます。AMS はインフラストラクチャオペレーションを提供し、クラウドでの安全な運用に関するベストプラクティスについてお客様の運用チームをガイドします。

  AMS 管理の AWS Service Catalog および AMS 管理の Direct Change モードは、同じビジネス成果と目標を達成しながら、お客様にさらなる柔軟性を提供します。さらに、お客様は AMS Operations On Demand (OOD) サービスを使用して、専用の AMS オペレーションエンジニアが変更リクエスト (RFCs) の実行に優先順位を付けることができます。

  差別化されていないインフラストラクチャの運用タスク (パッチ適用、バックアップ、アカウント管理など) を AMS にオフロードしながら、お客様は引き続きアプリケーションの最適化とクラウド運用に関する社内チームの強化に集中できます。AMS は、コスト削減に関する月次レポートを顧客に提供し、リソースの最適化に関するレコメンデーションを行います。このユースケースでは、Windows 2003 や 2008 などのレガシー OS バージョンでホストされているend-of-lifeアプリケーションがリファクタリングしないことを決定した場合、それらを AMS に移行し、カスタマーマネージドモードを利用するアカウントでホストすることもできます。
- ユースケース 2: 安全な AMS 境界内に Lambda、Glue、Athena を使用してデータレイクを構築する: 企業は、AMS の複数のアプリケーションのレポートニーズを満たすために Data Lake をセットアップしようとしています。お客様は、データセットの保存に S3 バケットを使用し、AWS Athena を使用して各レポートのデータセットに対してクエリを実行したいと考えています。S3 と AWS Athena は、別々の AMS マネージドアカウントにデプロイされます。S3 のアカウントには、データ取り込みパイプラインを構築するための Glue、Lambda、Step Functions などの他の

サービスもあります。この場合、Glue、Lambda、Athena、Step Functions はセルフサービスプロビジョニング (SSP) サービスと見なされます。顧客は、アドホックツール/スクリプトサーバーとして機能する EC2 インスタンスをアカウントにデプロイしました。まず、AMS マネージドアカウントで SSP サービスを有効にするように AMS にリクエストします。AMS は、ロールが顧客のフェデレーションソリューションにオンボーディングされると、顧客が引き受けることができるサービスごとに IAM ロールをプロビジョニングします。管理を容易にするために、お客様は個別の IAM ロールのポリシーを 1 つのカスタムロールに結合することもできます。これにより、AWS のサービス間で作業するときにロールを切り替える必要がなくなります。アカウントでロールを有効にすると、顧客は要件に従ってサービスを設定できます。ただし、お客様は AMS 変更管理システムと協力して、ユースケースに応じて追加のアクセス許可をリクエストする必要があります。

たとえば、 Glue クローラにアクセスするには、 Glue によって追加のアクセス許可が必要です。Lambda のイベントソースを作成するには、追加のアクセス許可も必要です。お客様は AMS と協力して IAM ロールを更新し、Athena が S3 バケットをクエリするためのクロスアカウントアクセスを許可します。サービスロールまたはサービスにリンクされたロールの更新も、Lambda が Step Functions サービスを呼び出し、Glue がすべての S3 バケットを読み書きするための AMS 変更管理を通じて必要になります。AMS はお客様と協力して、最小特権のアクセスモデルに従い、リクエストされた IAM の変更が過度に許容されず、環境が不要なリスクにさらされないようにします。顧客のデータレイクチームは、顧客のアーキテクチャに固有のサービスに必要なすべての IAM アクセス許可の計画に時間を費やし、それらを有効にするために AMS をリクエストします。これは、すべての IAM 変更が手動で処理され、AMS セキュリティチームからレビューされるためです。これらのリクエストを処理する時間は、アプリケーションのデプロイスケジュールで考慮する必要があります。

SSP サービスはアカウントで運用されているため、お客様は AMS インシデント管理とサービスリクエストを通じてサポートをリクエストし、問題を報告できます。ただし、AMS は Lambda のパフォーマンスと同時実行メトリクス、または Glue のジョブメトリクスを積極的にモニタリングしません。SSP サービスで適切なログ記録とモニタリングが有効になっていることを確認するのはお客様の責任です。アカウントの EC2 インスタンスと S3 バケットは、AMS によって完全に管理されます。

- ユースケース 3、AMS での CICD デプロイパイプラインの迅速かつ柔軟なセットアップ: お客様は、AMS 内のすべてのアプリケーションアカウントにコードパイプラインをデプロイするために Jenkins ベースの CICD パイプラインをセットアップしようとしています。お客様は、この CICD パイプラインを AMS 管理の直接変更モード (DCM) または AMS 管理のデベロッパーモードでホストするのが最も適している場合があります。これにより、EC2 で必要なカスタム設定で Jenkins サーバーを柔軟に設定し、アーティファクトリポジトリをホストする CloudFormation および S3 バケットにアクセスするための必要な IAM アクセス許可を付与できるためです。これは AMS 管

理 RFC モードで実行することもできますが、カスタマーチームは、IAM ロール用に複数の手動 RFCs を作成して、AMS によって手動でレビューされる、承認された最小限のアクセス許可のセットで反復する必要があります。DCM を使用すると、AMS マネージド RFCs モードを使用するときに、IAM ロール用に複数の手動 RFC を作成して、AMS によって手動でレビューされる最小限の許可セットを反復処理する必要がなくなります。これには時間がかかり、AMS プロセスとツールを強化するために顧客側の教育も必要です。開発者モードを使用すると、ネイティブ AWS APIs」から始めることができます。このパイプラインをセットアップする最も迅速かつ柔軟な方法は、AMS Managed-Developer モードを使用することです。デベロッパーモードは、運用統合を犠牲にしながら、最も迅速かつ簡単な方法を提供します。一方、DCM は柔軟性が低くなりますが、RFC モードと同じレベルの運用サポートを提供します。

- ユースケース 4、AMS 基盤内のカスタマイズされた運用モデル: 顧客は、期限駆動型のデータセンターの終了を検討しており、エンタープライズアプリケーションの 1 つは、アプリケーション運用やインフラストラクチャ運用を含むサードパーティーの MSP によって完全に管理されています。このアプリケーションを AMS で操作できるようにリファクタリングする時間がスケジュールにないと仮定すると、カスタマーマネージドモードが適切なオプションです。お客様は、AMS マネージドランディングゾーンの自動的かつ迅速なセットアップを活用できます。一元化されたネットワークアカウントを通じて、アカウントの供給と接続を制御する一元化されたアカウント管理を活用できます。また、AMS Payer アカウントを通じてすべてのカスタマーマネージドアカウントの料金を統合することで、請求を簡素化します。お客様は、AMS マネージドアカウントに使用される標準アクセス管理とは別に、MSP を使用してカスタムアクセス管理モデルを柔軟に設定できます。これにより、カスタマーマネージドモードを使用して、オンプレミス環境から退避するというビジネス要件を満たしながら、AMS マネージド環境をセットアップできます。この場合、お客様がクラウドに移行する Windows ベースのアプリケーションも持っていて、それらをカスタマーマネージドアカウントに移動することを選択した場合、お客様はクラウド運用モデルを作成する責任があります。これは、従来の IT プロセスを変革し、人材をトレーニングする顧客の能力によっては、複雑でコストが高く、時間がかかる場合があります。お客様は、このようなワークロードを「リフトアンドシフト」して AMS マネージドアカウントにし、インフラストラクチャオペレーションを AMS にオフロードすることで、時間とコストを削減できます。

> **Note**
>
> お客様は、RFC または SSP モードのガバナンスフレームワークとデベロッパーモードの間でアプリケーションアカウントを移動する必要があると感じることがあります。たとえば、お客様は最初のリフトアンドシフト移行の一環として AMS マネージドモードでアプリケーションをホストできますが、時間の経過とともにアプリケーションを書き換えてクラウドネイティブの AWS サービス用に最適化したいと考えています。本番稼働前のアカウントのモードを AMS マネージド RFC から AMS マネージド開発者モードに変更し、イ

ンフラストラクチャをプロビジョニングするための柔軟性と俊敏性を提供できます。ただし、「開発者ロール」を使用してインフラストラクチャのプロビジョニングが変更されると、同じインフラストラクチャを AMS マネージド RFC モードに戻すことはできません。これは、AMS が AMS 変更管理システムの外部でプロビジョニングされたインフラストラクチャのオペレーションを保証できないためです。お客様は、AMS マネージド RFC モードを提供する新しいアプリケーションアカウントを作成し、CloudFormation テンプレートまたは AMS マネージドアカウントに取り込まれたカスタム AMIs を使用して「最適化」インフラストラクチャ設定を再デプロイする必要がある場合があります。これは、本番稼働用設定をデプロイするためのクリーンな方法です。デプロイされると、アプリケーションは規範的な AMS ガバナンスと運用の下に置かれます。カスタマーマネージドモードと AMS マネージドモード間のモードの切り替えにも同じことが当てはまります。

RFC モード

RFC モードは、AMS Advanced オペレーションプランのお客様向けのデフォルトモードです。これには、変更または RFCs のリクエストを含む変更管理システムと、アカウントに必要な追加または変更をリクエストするために使用する変更タイプのカタログが含まれます。この変更管理システムは、アカウントを変更できるユーザーを制限するためのセキュリティレベルを提供します。

AMS Advanced 変更タイプの詳細については、「AMS 変更タイプとは」を参照してください。

AMS Advanced へのオンボーディングの詳細については、AWS Managed Servicesオンボーディングの概要」を参照してください。

変更タイプのウォークスルーの例については、AMS Advanced Change Type Reference Change Types by Classification セクションの関連する変更タイプの「追加情報」セクションを参照してください。

> **Note**
>
> RFC モードは、以前は「変更管理モード」または「標準 CM モード」と呼ばれていました。

トピック

- RFCsの詳細
- 変更タイプとは?
- AMS での RFC エラーのトラブルシューティング

RFCsの詳細

変更のリクエスト、または RFCs、2 つの方法で機能します。まず、RFC 自体に必要なパラメータがあります。これらは CreateRfc API のオプションです。次に、RFC のアクションに必要なパラメータ (実行パラメータ) があります。CreateRfc オプションの詳細については、AMS API リファレンスの CreateRfc セクションを参照してください。これらのオプションは通常、RFC ページの作成の追加設定領域に表示されます。

CreateRfc API、CLI、または AMS aws amscm create-rfc コンソールの RFC ページの作成を使用して、RFC を作成して送信できます。RFC の作成に関するチュートリアルについては、「」を参照してくださいRFC を作成する。

トピック

- RFCs
- AMS API/CLI を使用する場合の認証
- RFC セキュリティレビューを理解する
- RFC 変更タイプの分類を理解する
- RFC アクションとアクティビティの状態を理解する
- RFC ステータスコードを理解する
- RFC 更新 CTsと CloudFormation テンプレートドリフト検出を理解する
- RFCs
- RFCs
- RFC の制限された実行期間をリクエストする
- RFCs の作成、クローン作成、更新、検索、キャンセル
- RFCs
- 一般的な RFC パラメータについて説明します。
- RFC の毎日の E メールにサインアップする

RFCs

変更のリクエスト、つまり RFC は、AMS が管理する環境を変更する方法、またはユーザーに代わって変更を行うように AMS に依頼する方法です。RFC を作成するには、AMS 変更タイプから選択し、RFC パラメータ (スケジュールなど) を選択し、AMS コンソールまたは API コマンド CreateRfc と SubmitRfc を使用してリクエストを送信します。

RFC には 2 つの仕様が含まれています。1 つは RFC 自体用で、もう 1 つは変更タイプ (CT) パラメータ用です。コマンドラインでは、インライン RFC コマンド、または作成した CT JSON スキーマファイル (CT パラメータに基づく) とともに入力して送信する JSON 形式の標準の CreateRfc テンプレートを使用できます。CT 名は、CT の非公式な説明です。CSIO (カテゴリ、サブカテゴリ、項目、オペレーション) は、CT のより正式な説明です。RFC を作成するときは、CT ID のみを指定する必要があります。

AMS は、変更が正常に完了した (成功) か失敗した (失敗) ときに通知します。

> **Note**
>
> RFC 障害のトラブルシューティングについては、「」を参照してくださいAMS での RFC エラーのトラブルシューティング。

次の図は、ユーザーが送信した RFC のワークフローを示しています。

AMS API/CLI を使用する場合の認証

AMS API/CLI を使用する場合は、一時的な認証情報を使用して認証する必要があります。フェデレーティッドユーザーの一時的なセキュリティ認証情報をリクエストするには、cal GetFederationToken、AssumeRole、AssumeRoleWithSAML、または AssumeRoleWithWebIdentity AWS セキュリティトークンサービス (STS) APIs。

一般的な選択肢は SAML です。セットアップ後、呼び出す各オペレーションに 引数を追加します。例: `aws --profile saml amscm list-change-type-categories`。

SAML 2.0 プロファイルのショートカットは、 を使用して各 API/CLI の開始時にプロファイル変数を設定することです `set AWS_DEFAULT_PROFILE=saml` (Windows の場合、Linux の場合、 になりますexport `AWS_DEFAULT_PROFILE=saml`) 。CLI 環境変数の設定については、「AWS コマンドラインインターフェイスの設定、環境変数」を参照してください。

RFC セキュリティレビューを理解する

AWS Managed Services (AMS) 変更管理承認プロセスにより、アカウントに加えた変更のセキュリティレビューが確実に実行されます。

AMS は、AMS 技術標準に照らしてすべての変更リクエスト (RFCs) を評価します。技術標準から逸脱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

ビューの対象となります。セキュリティレビュー中、AMS は関連するリスクを強調し、セキュリティリスクが高い、または非常に高い場合は、承認されたセキュリティ担当者が RFC を承認または拒否します。すべての変更は、AMS の運用能力への悪影響を評価するためにも評価されます。潜在的な悪影響が見つかった場合は、AMS 内で追加のレビューと承認が必要です。

AMS 技術標準

AMS 技術標準は、アカウントのベースラインセキュリティを確立するための最小限のセキュリティ基準、設定、プロセスを定義します。これらの標準には、AMS とユーザーの両方が従う必要があります。

技術標準から逸脱することでアカウントのセキュリティ体制を低下させる可能性のある変更は、リスク受理プロセスを経て、関連するリスクが AMS によって強調表示され、承認されたセキュリティ担当者がユーザーから承認または拒否します。そのような変更はすべて、アカウントを運用する AMS の能力に悪影響があるかどうかを評価するために評価され、その場合は AMS 内で追加のレビューと承認が必要になります。

RFC カスタマーセキュリティリスク管理 (CSRM) プロセス

組織の誰かがマネージド環境への変更をリクエストすると、AMS は変更を確認して、リクエストが技術標準に違反してアカウントのセキュリティ体制を悪化させる可能性があるかどうかを判断します。リクエストがアカウントのセキュリティ体制を低下させ、AMS がセキュリティチームの連絡先に関連リスクを伝えて変更を実行する場合、または変更が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場合、AMS はセキュリティチームの連絡先にリスク承諾の形式で明示的な承認を求めます (次に説明) 。AMS 顧客リスク承諾プロセスは、以下を目的として設計されています。

- リスクが明確に特定され、適切な所有者に伝えられるようにする
- 環境に対する特定されたリスクを最小限に抑える
- 組織のリスクプロファイルを理解している指定されたセキュリティ担当者から承認を取得して文書化する
- 特定されたリスクに対する継続的な運用オーバーヘッドを削減する

技術標準と高リスクまたは非常に高いリスクにアクセスする方法

AMS 技術標準ドキュメントをレポートとして https://console.aws.amazon.com/artifact/ で参照できるようにしました。AMS 技術標準ドキュメントを使用して、変更リクエスト (RFC) を送信する前に、承認されたセキュリティ担当者から変更のリスクを受け入れる必要があるかどうかを理解します。

デフォルトの AWS Managed Services (AMS) Technical Standards」を検索して、技術標準レポートを検索します。 AWS Artifact AWSManagedServicesChangeManagementRole

> **Note**
>
> AMS 技術標準ドキュメントは、単一アカウントランディングゾーンの Customer_ReadOnly_Role からアクセスできます。マルチアカウントランディングゾーンでは、セキュリティ管理者が使用する AWSManagedServicesAdminRole と、アプリケーションチームが使用する AWSManagedServicesChangeManagementRole を使用して、ドキュメントにアクセスできます。チームがカスタムロールを使用している場合は、その他 | その他の RFC を作成してアクセスをリクエストすると、指定されたカスタムロールが更新されます。

RFC 変更タイプの分類を理解する

RFC の送信時に使用する変更タイプは、次の 2 つのカテゴリに分かれています。

- デプロイ: この分類はリソースの作成用です。
- 管理: この分類は、リソースを更新または削除するために使用します。管理カテゴリには、インスタンスへのアクセス、AMIs暗号化または共有、スタックの開始、停止、再起動、または削除のための変更タイプも含まれています。

RFC アクションとアクティビティの状態を理解する

`RfcActionState` (API) / Activity State (コンソール) は、RFC に対する人間の介入またはアクションのステータスを理解するのに役立ちます。手動 RFCs に主に使用される は、ユーザーまたは AMS オペレーションがいつアクションを必要とするか`RfcActionState`を理解し、AMS オペレーションが RFC でアクティブに動作しているかを確認するのに役立ちます。これにより、RFC のライフサイクル中に RFC に対して実行されるアクションの透明性が向上します。

`RfcActionState` (API) / アクティビティ状態 (コンソール) 定義：

- AwsOperatorAssigned: AWS オペレーターが RFC でアクティブに作業しています。
- AwsActionPending: AWS からのレスポンスまたはアクションが必要です。
- CustomerActionPending: 顧客からのレスポンスまたはアクションが期待されます。
- NoActionPending: AWS または顧客からのアクションは必要ありません。

- NotApplicable: この状態は AWS オペレーターまたはお客様が設定することはできません。この機能がリリースされる前に作成された RFCs にのみ使用されます。

RFC アクションの状態は、送信された変更タイプが手動レビューを必要とし、スケジュールが ASAP に設定されているかどうかによって異なります。

- RFC ActionState は、遅延スケジューリングを使用した手動変更タイプのレビュー、承認、開始中に変更されます。
  - スケジュールされた手動 RFC を送信すると、ActionState は自動的に AwsActionPending に変更され、オペレータが RFC を確認して承認する必要があることを示します。
  - オペレーターが RFC のアクティブレビューを開始すると、ActionState は AwsOperatorAssigned に変わります。
  - オペレータが RFC を承認すると、RFC ステータスはスケジュール済みに変わり、ActionState は自動的に NoActionPending に変わります。
  - RFC のスケジュールされた開始時刻に達すると、RFC ステータスは InProgress に変わり、ActionState は自動的に AwsActionPending に変わり、RFC のレビューのためにオペレータを割り当てる必要があることを示します。
  - オペレータが RFC のアクティブ実行を開始すると、ActionState が AwsOperatorAssigned に変更されます。
  - 完了すると、オペレータは RFC を閉じます。これにより、ActionState が自動的に NoActionPending に変更されます。

⚠ Important

- アクションの状態を設定することはできません。RFC の変更に基づいて自動的に設定するか、AMS 演算子によって手動で設定されます。
- RFC にコレスポンデンスを追加すると、ActionState は自動的に AwsActionPending に設定されます。
- RFC が作成されると、ActionState は自動的に NoActionPending に設定されます。
- RFC が送信されると、ActionState は自動的に AwsActionPending に設定されます。
- RFC が拒否、キャンセル、または完了され、ステータスが Success または Failure の場合、ActionState は自動的に NoActionPending にリセットされます。

- アクション状態は自動 RFCs の両方で有効になりますが、これらのタイプの RFCs では通信が必要になることが多いため、主に手動 RFCs では重要です。

RFC アクションの状態を確認するユースケースの例

ユースケース: 手動 RFC プロセスの可視性

- 手動 RFC を送信すると、RFC アクションの状態は自動的に に変わりAwsActionPending、オペレータが RFC を確認して承認する必要があることを示します。オペレーターが RFC のアクティブレビューを開始すると、RFC アクションの状態は に変わりますAwsOperatorAssigned。
- 承認され、スケジュールされ、実行を開始する準備ができている手動 RFC を検討してください。RFC ステータスが に変わるとInProgress、RFC アクションの状態は自動的に に変わりますAwsActionPending。オペレーターAwsOperatorAssignedが RFC のアクティブ実行を開始すると、再び に変わります。
- 手動 RFC が完了 (「成功」または「失敗」としてクローズ) すると、RFC アクションの状態が に変わりNoActionPending、顧客またはオペレーターからそれ以上のアクションが不要であることを示します。

ユースケース: RFC 対応

- 手動 RFC が の場合Pending Approval、AMS オペレーターからさらに情報が必要になる場合があります。オペレーターは RFC にコレスポンデンスを投稿し、RFC アクションの状態を に変更しますCustomerActionPending。新しい RFC 対応を追加して応答すると、RFC アクションの状態は自動的に に変わりますAwsActionPending。
- 自動または手動 RFC が失敗した場合は、RFC の詳細にコレスポンデンスを追加し、RFC が失敗した理由を AMS オペレーターに尋ねることができます。コレスポンデンスが追加されると、RFC アクションの状態は自動的に に設定されますAwsActionPending。AMS オペレーターが RFC をピックアップしてコレスポンデンスを表示すると、RFC アクションの状態は に変わりますAwsOperatorAssigned。オペレータが新しい RFC コレスポンデンスを追加して応答すると、RFC アクションの状態を に設定してCustomerActionPending、顧客からの別の応答が予想されることを示すか、 に設定してNoActionPending、顧客からの応答が不要または予想されることを示すことができます。

RFC ステータスコードを理解する

RFC ステータスコードは、リクエストの追跡に役立ちます。これらのステータスコードは、CLI 出力の RFC 実行中、またはコンソールの RFC リストページを更新することで確認できます。

RFC のコードは、RFC の詳細ページでも確認できます。

送信していない RFC がリストに表示される場合があります。AMS 演算子が内部専用 CT を使用する場合は、RFC に送信され、RFC リストに表示されます。詳細については、「内部のみの変更タイプ」を参照してください。

> **Important**
>
> RFC の状態変更の通知をリクエストできます。詳細については、「RFC 状態変更通知」を参照してください。

RFC ステータスコード

Success (成功)	失敗
編集中: RFC は作成されていますが、送信されていません PendingApproval / Submitted: RFC が送信され、システムは承認が必要かどうかを判断し、必要に応じてその承認を取得します。 AWS による承認/顧客による承認: RFC が承認されました。自動 RFCsは AWS によって承認され、手動 RFCsはオペレーターによって承認され、場合によっては顧客によって承認されます。 スケジュール済み: RFC は構文と要件チェックに合格し、実行がスケジュールされています InProgress: RFC が実行されています。複数のリソースをプロビジョニングする、または	拒否: RFCsは通常、検証に失敗するため拒否されます。たとえば、使用できないリソース、つまりサブネットが指定されます。 キャンセル済み: RFCsは通常、設定された開始時刻が経過する前に検証に合格しないためキャンセルされます。 Failure: RFC が失敗しました。失敗の理由については、出力の StatusReason を参照してください。AMS オペレーションは自動的にトラブルチケットを作成し、必要に応じてユーザーと通信します。

Success (成功)	失敗
UserData が長時間実行される RFCs の実行には時間がかかることに注意してください。 実行済み: RFC が実行されました Success/Succeeded: RFC が正常に完了しました	

> **Note**
>
> キャンセルまたは拒否された RFCs「」も参照してくださいRFCsを更新する。 UpdateRfc

RFC が必要なすべての条件に合格した場合 (たとえば、すべての必須パラメータが指定されている場合) 、ステータスは に変わります `PendingApproval` (自動 CTsでも承認が必要で、構文とパラメータチェックが合格すると自動的に行われます) 。合格しない場合、ステータスは に変わりますRejected。`StatusReason` は拒否に関する情報を提供し、 `ExecutionOutput`フィールドは承認と完了に関する情報を提供します。エラーコードには以下が含まれます。

- InvalidRfcStateException: RFC は、呼び出されたオペレーションを許可しないステータスです。たとえば、RFC が送信済み状態に移行した場合、変更できなくなります。
- InvalidRfcScheduleException: StartTime、EndTime、または TimeoutInMinutes パラメータが超過しました。
- InternalServerError: システムに問題が発生しました。
- InvalidArgumentException: パラメータが正しく指定されていません。たとえば、許容できない値が使用されます。
- ResourceNotFoundException: スタック ID などの値が見つかりません。

変更が承認される前に、スケジュールされたリクエストの開始時刻と終了時刻 (変更実行ウィンドウとも呼ばれます) が発生した場合、RFC ステータスは に変わりますCanceled。変更が承認されると、RFC ステータスは に変わりますScheduled。ASAP RFCs の変更実行ウィンドウは、送信された時刻に CT `ExpectedExecutionDuration`の値を加えたものです。

変更実行ウィンドウの到着前であればいつでも、スケジュールされた変更 (CLI RequestedStartTimeの で送信) を変更またはキャンセルできます。スケジュールされた変更が変更された場合は、再送信する必要があります。

変更開始時刻 (スケジュールまたは ASAP) が到着し、承認が完了すると、ステータスは に変わりInProgress、変更を加えることはできません。指定された変更実行ウィンドウ内に変更が完了すると、ステータスは に変わりますSuccess。変更の一部が失敗した場合、または変更実行ウィンドウ終了時に変更がまだ進行中である場合、ステータスは に変わりますFailure。

> **Note**
>
> InProgress、Success、または の状態Failureの変更中、RFC を変更またはキャンセルすることはできません。

次の図は、CreateRFC 呼び出しから解決までの CreateRFC ステータスを示しています。

RFC 更新 CTsと CloudFormation テンプレートドリフト検出を理解する

AMS でプロビジョニングされたリソースは、変更された CloudFormation テンプレートを使用します。リソースのパラメータがサービスの AWS マネジメントコンソールから直接変更された場合、そのリソースの CloudFormation 作成レコードは同期しなくなります。この場合、AMS 更新変更タイプを使用して AMS のリソースを更新しようとすると、AMS は元のリソース設定を参照し、変更されたパラメータをリセットする可能性があります。このリセットはダメージを与える可能性があるため、追加の AMS 設定変更が検出された場合、AMS は更新変更タイプの RFCs を禁止します。

更新変更タイプのリストについては、コンソールフィルターを使用します。

ドリフト修復FAQs

AMS ドリフト修復に関する質問と回答。ドリフト修復を開始するために使用できる変更タイプは 2 つあります。1 つは実行モード = 手動または「レビューが必要」で、もう 1 つは実行モード = 自動です。

ドリフト修復でサポートされているリソース (ct-3kinq0u4l33zf)

これらは、ドリフト修復変更タイプ (ct-3kinq0u4l33zf) でサポートされているリソースです。 リソースを修正するには、代わりに「必要なレビュー」 (ct-34sxfo53yuzah) 変更タイプを使用します。

```
AWS::EC2::Instance
AWS::EC2::SecurityGroup
AWS::EC2::VPC
AWS::EC2::Subnet
AWS::EC2::NetworkInterface
AWS::EC2::EIP
AWS::EC2::InternetGateway
AWS::EC2::NatGateway
AWS::EC2::NetworkAcl
AWS::EC2::RouteTable
AWS::EC2::Volume
AWS::AutoScaling::AutoScalingGroup
AWS::AutoScaling::LaunchConfiguration
AWS::AutoScaling::LifecycleHook
AWS::AutoScaling::ScalingPolicy
AWS::AutoScaling::ScheduledAction
AWS::ElasticLoadBalancing::LoadBalancer
AWS::ElasticLoadBalancingV2::Listener
AWS::ElasticLoadBalancingV2::ListenerRule
AWS::ElasticLoadBalancingV2::LoadBalancer
AWS::CloudWatch::Alarm
```

ドリフト修復の変更タイプ

AMS ドリフト修復変更タイプの使用に関する質問と回答。

ドリフト修復機能でサポートされているリソースのリストについては、「」を参照してください[ドリフト修復でサポートされているリソース (ct-3kinq0u4l33zf)](#)。

> **Important**
>
> ドリフト修復はスタックテンプレートやパラメータを変更し、最新のスタックテンプレートやパラメータを使用するようにローカルテンプレートリポジトリまたはこれらのスタックを更新するオートメーションを更新する必要があります。同期せずに古いテンプレートやパラメータを使用すると、基盤となるリソースに有害な変更が生じる可能性があります。
> レビュー不要、自動、CT (ct-3kinq0u4l33zf) は、RFC あたり 10 個のリソースの修復のみをサポートしています。残りのリソースを 10 個のバッチで修正するには、すべてのリソースが修正されるまで新しい RFCs を作成します。

どのドリフト修復変更タイプを使用すべきですか？

以下の場合は、レビュー不要の自動 CT (ct-3kinq0u4l33zf) を使用することをお勧めします。

- 自動 CT を使用して既存のスタックリソースの更新を実行しようとすると、スタックが であるため RFC は拒否されますDRIFTED。
- 過去に Update CT を使用していて、スタックが DRIFTED になったため失敗しました。更新を再試行する必要はなく、代わりに必要な手動 CT によるレビューを使用できます。

ドリフト修復でドリフトリソースタイプがサポートされていない場合、自動、CT (ct-3kinq0u4l33zf)、またはドリフト修復が不要、自動、CT が失敗する場合にのみ、必要なレビューの手動 CT (ct-34sxfo53yuzah) を使用することをお勧めします。

修復中にスタックにどのような変更が実行されますか？

修復には、ドリフトするプロパティに応じて、スタックテンプレートやパラメータの更新が必要です。修復は、修復中にスタックのスタックポリシーを更新し、修復が完了するとスタックポリシーを以前の値に復元します。

スタックテンプレートやパラメータに対して実行された変更を確認するにはどうすればよいですか？

RFC へのレスポンスでは、変更の概要に以下の情報が表示されます。

- `ChangeSummaryJson`: ドリフト修復の一環として、スタックテンプレートやパラメータの変更の概要が含まれます。修復は複数のフェーズで実行されます。この変更の概要は、個々のフェーズの変更で構成されます。修復が成功した場合は、最後のフェーズの変更を確認します。順番に実行されるフェーズについては、JSON の ExecutionPlan を参照してください。たとえば、RestoreReferences セクションが存在する場合、常に最後に実行され、修正後の変更のための JSON が含まれます。DryRun モードで修復が実行された場合、これらの変更はスタックに適用されません。
- `PreRemediationStackTemplateAndConfigurationJson`: スタックで修復がトリガーされる前に、テンプレート、パラメータ、出力、StackPolicyBody を含む CloudFormation スタックの設定スナップショットが含まれます。

修復が実行されたら、何をする必要がありますか？

> **Important**
>
> RFC の概要で提供されている最新のテンプレートとパラメータを使用して、修復されたスタックを更新するローカルテンプレートリポジトリまたはオートメーションを更新する必要があります。古いテンプレートやパラメータを使用すると、スタックリソースにさらに破壊的な変更が生じる可能性があるため、これを行うことが重要です。

この修復中にアプリケーションは有効になりますか？

修復は、CloudFormation スタック設定でのみ実行されるオフラインプロセスです。基盤となるリソースでは更新は実行されません。

管理 | その他 | その他の RFCsを引き続き使用して、修復後にリソースを更新できますか？

使用可能な自動 Update CTs を使用して、スタックリソースの更新を常に実行することをお勧めします。利用可能な Update CTsがユースケースをサポートしていない場合は、 管理 | その他 | その他のリクエストを使用します。

修復によってスタックに新しいリソースが作成されますか？

修復では、スタックに新しいリソースは作成されません。ただし、修復は新しい出力を作成し、スタックテンプレートメタデータセクションを更新して、参照用に修復の概要を保存します。

修復は常に成功しますか？

修復するには、テンプレート設定を慎重に分析して検証し、実行できるかどうかを判断する必要があります。これらの検証が失敗した場合、修復プロセスは停止され、スタックテンプレートまたはパラメータに変更は実行されません。また、修復はサポートされているリソースタイプでのみ実行できます。

修復が成功しなかった場合にスタックリソースの更新を実行するにはどうすればよいですか？

Management | Other | Other | Update CT (ct-0xdawir96cy7k) を使用して変更をリクエストできます。AMS はこのようなシナリオをモニタリングし、修復ソリューションの改善に取り組んでいます。

サポートされているリソースタイプとサポートされていないリソースタイプの両方を持つスタックを修復できますか？

はい。ただし、修復は、サポートされているリソースタイプがスタックで DRIFTED が見つかった場合にのみ実行されます。サポートされていないリソースタイプが DRIFTED の場合、修復は続行されません。

CFN 以外の取り込み CTs を使用して作成されたスタックの修復をリクエストできますか？

はい。修正は、スタックの作成に使用される変更タイプに関係なく、スタックで実行できます。

修復前にスタックに実行される変更を知ることはできますか？

はい。どちらの変更タイプも、スタックが修正された場合に実行される変更をリクエストするために使用できる DryRun オプションを提供します。ただし、最終的な修復の変更は、修復時にスタックに存在するドリフトによって異なる場合があります。

RFCs

スケジュール機能を使用すると、RFCs の開始時間を選択できます。スケジューリング機能では、次のオプションを使用できます。

- この変更をできるだけ早く実行する: AMS は、承認されるとすぐに RFC を実行します。ほとんどの CTsは自動的に承認されます。RFC を特定の時間に開始しない場合は、このオプションを使用します。
- この変更をスケジュールする: RFC を実行する日、時刻、タイムゾーンを設定します。自動変更タイプの場合、RFC の送信予定から少なくとも 10 分後に開始時刻をリクエストするのがベストプラクティスです。レビューに必要な変更タイプについては、RFC の送信予定から少なくとも 24 時間後に開始時刻をリクエストする必要があります。RFC が設定された開始時刻までに承認されない場合、RFC は拒否されます。

RFC スケジュールを設定する

RFC をスケジュールするには、次のいずれかの方法を使用します。

この変更をできるだけ早く実行します。

- コンソール: 何もしません。これはデフォルトの RFC スケジュールを使用します。
- API または CLI: RFC の作成オペレーションで `RequestedStartTime`および `RequestedEndTime`オプションを削除します。

送信後 30 日以内に承認されない場合、ASAP 「レビューが必要RFCs は自動的に拒否されます。

この変更をスケジュールします。

- コンソール: この変更のスケジュールラジオボタンを選択します。開始時間領域が開きます。手動で日を入力するか、カレンダーウィジェットを使用して日を選択します。ISO 8601 形式で表される時刻を UTC で入力し、ドロップダウンリストを使用して場所を選択します。デフォルトでは、AMS は ISO 8601 形式 YYYYMMDDThhmmssZ または YYYY-MM-DDThh:mm:ssZ を使用します。どちらの形式も使用できます。

> **Note**
>
> デフォルトの終了時刻は、入力した開始時刻から 4 時間です。スケジュールされた変更の終了時刻を 4 時間を超えて設定するには、API または CLI を使用して変更を実行します。

- API または CLI: RFC 作成オペレーションで RequestedStartTimeおよび RequestedEndTimeパラメータの値を送信します。設定済みの を渡RequestedEndTimeしても、既に開始されている自動変更タイプの実行は停止されません。「レビューが必要」の変更タイプで、AMS オペレーションの研究がまだ進行中に RequestedEndTimeに到達し、AMS と通信している場合は、拡張機能をリクエストするか、RFC の再送信を求められる場合があります。

> **Tip**
>
> UTC タイムリードアウトの例については、Time-is ウェブサイトの「UTC」を参照してください。2:20pm: 2016-2016-12-05T1420161205T142000Z 形式の例。

指定した場合..

- のみRequestedStartTime、RFC はスケジュール済みと見なされ、 RequestedEndTimeは ExecutionDurationInMinutes値を使用して入力されます。
- のみRequestedEndTime、InvalidArgumentException をスローします。
- RequestedStartTime と の両方でRequestedEndTime、指定された開始時刻に ExecutionDurationInMinutes値を加えたRequestedEndTime値で を上書きします。
- RequestedStartTime も も、RequestedEndTimeこれらの値は null のままで、RFC は ASAP RFC として扱われます。

> **Note**
>
> スケジュールされたすべての RFCs について、未指定の終了時刻は、指定された時刻に、送信された変更タイプの ExpectedExecutionDurationInMinutes 属性RequestedStartTimeを加えた時刻として書き込まれます。たとえば、ExpectedExecutionDurationInMinutesが「60」 (分) で、指定された RequestedStartTimeが 2016-12-05T14:20:00Z (2016 年 12 月 5 日午前 4 時 20 分) の場合、実際の終了時刻は 2016 年 12 月 5 日午前 5 時 20 分に設定されます。ExpectedExecutionDurationInMinutes 特定の変更タイプの を検索するには、次のコマンドを実行します。

```
aws amscm --profile saml get-change-type-version --
change-type-id CHANGE_TYPE_ID --query "ChangeTypeVersion.
{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

RFC Priority オプションを使用する

`execution mode = manual` 変更タイプで Priority オプションを使用して、リクエストの緊急性を AMS オペレーションに警告します。

の Priority オプション`execution mode = manual`：

手動 RFC の優先度を High、Medium、または Low に指定します。High に分類されRFCs は、RFCs サービスレベル目標 (SLOs) とその送信時間に従って、Medium に分類される RFC の前にレビューおよび承認されます。優先度が低い、または優先度が指定されていない RFCs は、送信された順序で処理されます。

RFCs

承認が必要な (手動) CTs で送信される RFCs は、ユーザーまたは AMS によって承認される必要があります。事前承認された CTsは自動的に処理されます。詳細については、「CT 承認要件」を参照してください。

> **Note**
>
> 「レビュー必須」CT を使用する場合、AMS では ASAP スケジューリングオプション (コンソールで ASAP を選択し、API/CLI で開始時刻と終了時刻を空白のままにしておく) を使用することをお勧めします。これらの CTs では、AMS オペレータが RFC を調べる必要があり、承認および実行する前にお客様と通信する必要があるためです。これらの RFCsスケジュールする場合は、少なくとも 24 時間かかります。スケジュールされた開始時刻より前に承認が行われない場合、RFC は自動的に拒否されます。

承認が必要な RFC が AMS によって正常に送信された場合は、明示的に承認する必要があります。または、承認が必要な RFC を送信する場合は、AMS によって承認される必要があります。AMS が送信した RFC を承認する必要がある場合は、承認をリクエストする E メールまたはその他の事前定義された通信が送信されます。通信には RFC ID が含まれます。通信が送信されたら、次のいずれかを実行します。

- コンソールの承認または拒否: 関連する RFC の RFC 詳細ページを使用します。

- API / CLI 承認: ApproveRfc は変更を承認済みとしてマークします。アクションは、所有者とオペレーターの両方が必要な場合に実行する必要があります。以下は、CLI 承認コマンドの例です。次の例では、RFC_ID を適切な RFC ID に置き換えます。

```
aws amscm approve-rfc --rfc-id RFC_ID
```

- API / CLI 拒否: RejectRfc は変更を拒否済みとしてマークします。以下は、CLI 拒否コマンドの例です。次の例では、RFC_ID を適切な RFC ID に置き換えます。

```
aws amscm reject-rfc --rfc-id RFC_ID --reason "no longer relevant"
```

RFC の制限された実行期間をリクエストする

以前はブラックアウトデーと呼ばれていましたが、特定の期間の制限をリクエストできます。この間は変更を実行できません。

制限された実行期間を設定するには、UpdateRestrictedExecutionTimes API オペレーションを使用して、UTC で特定の期間を設定します。指定した期間は、指定した以前の期間よりも優先されます。指定された制限された実行時間内に RFC を送信すると、送信は無効な RFC スケジュールというエラーで失敗します。最大 200 の制限期間を指定できます。デフォルトでは、制限された期間は設定されていません。以下は、リクエストコマンドの例です (SAML 認証が設定されている)。

```
aws amscm  --profile saml update-restricted-execution-times --restricted-execution-
times="[{\"TimeRange\":{\"StartTime\":\"2018-01-01T12:00:00Z\",\"EndTime\":
\"2018-01-01T12:00:01Z\"}}]"
```

RestrictedExecutionTimes API オペレーションを実行して、現在の RestrictedExecutionTimes 設定を表示することもできます。 ListRestrictedExecutionTimes 例:

```
aws amscm  --profile saml list-restricted-execution-times
```

指定された制限された実行時間内に RFC を送信する場合は、OverrideRestrictedTimeRanges の値を持つ RestrictedExecutionTimesOverrideId を追加し、通常どおり RFC を送信します。この方法は、緊急または緊急の RFC にのみ使用するのがベストプラクティスです。詳細については、SubmitRfc の API リファレンスを参照してください。

RFCs の作成、クローン作成、更新、検索、キャンセル

以下の例では、さまざまな RFC オペレーションについて説明します。

トピック

- RFC を作成する
- AMS コンソールを使用して RFCs のクローンを作成する (再作成)
- RFCsを更新する
- RFCs の検索
- RFCs

RFC を作成する

コンソールを使用した RFC の作成

以下は、AMS コンソールでの RFC 作成プロセスの最初のページです。クイックカードが開き、変更タイプの参照がアクティブになっています。

以下は、AMS コンソールで RFC 作成プロセスの最初のページで、カテゴリ別に選択がアクティブになっています。

仕組み：

1. RFC の作成ページに移動します。AMS コンソールの左側のナビゲーションペインでRFCs をクリックして RFCsリストページを開き、RFC の作成をクリックします。
2. デフォルトの変更タイプ参照ビューで一般的な変更タイプ (CT) を選択するか、カテゴリ別選択ビューで CT を選択します。
   - 変更タイプ別に参照: クイック作成エリアで一般的な CT をクリックすると、すぐに RFC の実行ページを開くことができます。クイック作成で古い CT バージョンを選択することはできません。

     CTsソートするには、カードビューまたはテーブルビューですべての変更タイプ領域を使用します。どちらのビューでも、CT を選択し、RFC の作成をクリックして RFC の実行ページを開きます。必要に応じて、RFC の作成ボタンの横に古いバージョンで作成オプションが表示されます。

- カテゴリ別に選択: カテゴリ、サブカテゴリ、項目、オペレーションを選択すると、CT 詳細ボックスが開き、必要に応じて古いバージョンで作成するオプションが表示されます。RFC の作成をクリックして、RFC の実行ページを開きます。

3. RFC の実行ページで、CT 名エリアを開き、CT の詳細ボックスを表示します。件名は必須です (変更タイプの参照ビューで CT を選択した場合は入力されます) 。追加設定エリアを開き、RFC に関する情報を追加します。

   実行設定領域で、使用可能なドロップダウンリストを使用するか、必要なパラメータの値を入力します。オプションの実行パラメータを設定するには、追加設定エリアを開きます。
4. 完了したら、実行 をクリックします。エラーがない場合、RFC が正常に作成されたページに、送信された RFC の詳細と最初の実行出力が表示されます。
5. Run parameters エリアを開き、送信した設定を確認します。ページを更新して RFC 実行ステータスを更新します。必要に応じて、RFC をキャンセルするか、ページ上部のオプションを使用してコピーを作成します。

CLI を使用した RFC の作成

仕組み：

1. インライン作成 (すべての RFC と実行パラメータを含むcreate-rfcコマンドを発行) またはテンプレート作成 (2 つの JSON ファイルを作成します。1 つは RFC パラメータ用、もう 1 つは実行パラメータ用) のいずれかを使用し、2 つのファイルを入力としてcreate-rfcコマンドを発行します。どちらの方法もここで説明します。
2. 返された RFC ID を使用して RFC: `aws amscm submit-rfc --rfc-id` *`ID`* コマンドを送信します。

   RFC: `aws amscm get-rfc --rfc-id` *`ID`* コマンドをモニタリングします。

変更タイプのバージョンを確認するには、次のコマンドを使用します。

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> 変更タイプのスキーマの一部であるかどうかにかかわらず、任意の RFC で任意のCreateRfcパラメータを使用できます。たとえば、RFC ステータスが変更されたとき

に通知を受け取るには、リクエストの RFC パラメータ部分 (実行パラメータではなく) --notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"にこの行を追加します。すべての CreateRfc パラメータのリストについては、AMS 変更管理 API リファレンスを参照してください。

インライン作成：

インラインで指定された実行パラメータ (インラインで実行パラメータを指定する場合は引用符をエスケープ) を指定して create RFC コマンドを発行し、返された RFC ID を送信します。たとえば、コンテンツを次のような内容に置き換えることができます。

```
aws amscm create-rfc --change-type-id "CT_ID" --change-type-version "VERSION" --title
 "TITLE" --execution-parameters "{\"Description\": \"example\"}"
```

テンプレートの作成：

> **Note**
>
> RFC を作成するこの例では、Load Balancer (ELB) スタック変更タイプを使用します。

1. 関連する CT を見つけます。次のコマンドは、項目名に「ELB」が含まれている CT 分類の概要を検索し、Category、Item、Operation、ChangeTypeID の出力をテーブル形式で作成します (両方のサブカテゴリは ですAdvanced stack components)。

   ```
   aws amscm list-change-type-classification-summaries --query
    "ChangeTypeClassificationSummaries[?contains(Item,'ELB')].
   [Category,Item,Operation,ChangeTypeId]" --output table
   ```

   ```
   ----------------------------------------------------------------------
   |                            CtSummaries                             |
   +-----------+---------------------------+---------------------------+
   | Deployment| Load balancer (ELB) stack | Create | ct-123h45t6uz7jl |
   | Management| Load balancer (ELB) stack | Update | ct-0ltm873rsebx9 |
   +-----------+---------------------------+---------------------------+
   ```

2. CT の最新バージョンを見つけます。

ChangeTypeId および ChangeTypeVersion: このウォークスルーの変更タイプ ID は ct-123h45t6uz7jl (ELB を作成) です。最新バージョンを確認するには、次のコマンドを実行します。

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=ct-123h45t6uz7jl
```

3. オプションと要件について説明します。次のコマンドは、CreateElbParams.json.

```
aws amscm get-change-type-version --change-type-id "ct-123h45t6uz7jl" --query
 "ChangeTypeVersion.ExecutionInputSchema" --output text > CreateElbParams.json
```

4. 実行パラメータ JSON ファイルを変更して保存します。この例では、CreateElbParams.json.

プロビジョニング CT の場合、StackTemplateId はスキーマに含まれ、実行パラメータで送信する必要があります。

TimeoutInMinutes の場合、RFC が失敗するまでにスタックの作成に許可される分数。この設定では RFC の実行が遅延することはありませんが、十分な時間を与える必要があります (たとえば、「5」を指定しないでください) 。UserData: Create EC2 and Create ASG の実行時間が長い CTs」~「360」です。他のすべてのプロビジョニング CTs」をお勧めします。

スタックを作成する VPC の ID を指定します。VPC ID は CLI コマンド で取得できますaws amsskms list-vpc-summaries。

```
{
"Description":      "ELB-Create-RFC",
"VpcId":            "VPC_ID",
"StackTemplateId":  "stm-sdhopv00000000000",
"Name":             "MyElbInstance",
"TimeoutInMinutes": 60,
"Parameters":   {
    "ELBSubnetIds":                     ["SUBNET_ID"],
    "ELBHealthCheckHealthyThreshold":   4,
    "ELBHealthCheckInterval":           5,
    "ELBHealthCheckTarget":             "HTTP:80/",
    "ELBHealthCheckTimeout":            60,
    "ELBHealthCheckUnhealthyThreshold": 5,
    "ELBScheme":                        false
    }
```

```
}
```

5. RFC JSON テンプレートを CreateElbRfc.json:

```
aws amscm create-rfc --generate-cli-skeleton > CreateElbRfc.json
```

6. CreateElbRfc.json ファイルを変更して保存します。実行パラメータを別のファイルに作成したため、ExecutionParameters行を削除します。たとえば、コンテンツを次のような内容に置き換えることができます。

```
{
"ChangeTypeVersion":    "2.0",
"ChangeTypeId":         "ct-123h45t6uz7jl",
"Title":                "Create ELB"
}
```

7. RFC を作成します。次のコマンドは、実行パラメータファイルと RFC テンプレートファイルを指定します。

```
aws amscm create-rfc --cli-input-json file://CreateElbRfc.json --execution-
parameters file://CreateElbParams.json
```

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

ヒント

> **Note**
>
> AMS API/CLI を使用して、RFC JSON ファイルまたは CT 実行パラメータ JSON ファイルを作成せずに RFC を作成できます。これを行うには、 `create-rfc` コマンドを使用し、必要な RFC および実行パラメータを コマンドに追加します。これは「インライン作成」と呼ばれます。すべてのプロビジョニング CTs には、リソースのパラメータを含むParameters配列がexecution-parametersブロックに含まれていることに注意してください。パラメータには、バックスラッシュ (\) でエスケープされた引用符が必要です。RFC を作成する他の文書化された方法は、「テンプレートの作成」と呼ばれます。ここでは、RFC パラメータ用の JSON ファイルと実行パラメータ用の別の JSON ファイルを作成し、 `create-rfc` コマンドを使用して 2 つのファイルを送信します。これらのファイルはテンプレートとして機能し、将来の RFCs に再利用できます。

テンプレートを使用して RFCs を作成する場合、 コマンドを使用して、次に示すようにコマンドを発行することで、必要な内容の JSON ファイルを作成できます。コマンドは、表示された内容で「parameters.json」という名前のファイルを作成します。これらのコマンドを使用して RFC JSON ファイルを作成することもできます。

AMS コンソールを使用して RFCs のクローンを作成する (再作成)

AMS コンソールを使用して、既存の RFC のクローンを作成できます。

AMS コンソールを使用して RFC のクローンを作成または再作成するには、次の手順に従います。

1. 関連する RFC を見つけます。左側のナビゲーションで、RFCsをクリックします。

   RFCsが開きます。
2. クローンを作成する RFC が見つかるまでページをスクロールします。フィルターオプションを使用してリストを絞り込みます。クローンを作成する RFC を選択します。

   RFC の詳細ページが開きます。
3. コピーの作成をクリックします。

   変更リクエストの作成ページが開き、すべてのオプションが元の RFC で として設定されます。
4. 必要な変更を加えます。追加オプションを設定するには、基本オプションをアドバンストに変更します。すべてのオプションを設定したら、送信を選択します。

   アクティブな RFC の詳細ページが開き、クローン RFC の新しい RFC ID が表示され、クローン RFC が RFC ダッシュボードに表示されます。

RFCsを更新する

RFC を更新して送信するか、再送信することで、拒否された RFC またはまだ送信されていない RFC を再送信できます。ほとんどの RFCs は拒否されることに注意してください。これは、指定された `RequestedStartTime` が送信前に渡されたか、指定された TimeoutInMinutes が RFC の実行に不十分であるためです (TimeoutInMinutes は成功した RFC を延長しないため、Amazon EC2 または長時間実行される UserData を持つ Amazon EC2 Auto Scaling グループでは、常にこれを「60」以上「360」以下に設定することをお勧めします)。このセクションでは、 `UpdateRfc` コマンドの CLI バージョンを使用して、新しい RFC パラメータで RFC を更新する方法、または文字列化された JSON または更新されたパラメータファイルを使用して新しいパラメータを更新する方法について説明します。

この例では、AMS UpdateRfc API の CLI バージョンの使用について説明します (「RFC の更新」を参照) 。一部のリソース (DNS プライベートおよびパブリック、ロードバランサースタック、スタックパッチ適用設定) を更新するための変更タイプがありますが、RFC を更新する CT はありません。

一度に 1 つの UpdateRfc オペレーションを送信することをお勧めします。DNS スタックなどで複数の更新を送信すると、更新が同時に DNS を更新しようとして失敗する可能性があります。

必須データ: `RfcId`: 更新する RFC。

オプションデータ: `ExecutionParameters`: などの必須でないフィールドを更新しない限り`Description`、RFC が拒否またはキャンセルされた原因となった問題に対処するために、変更された実行パラメータを送信します。送信された NULL 以外の値はすべて、元の RFC の値を上書きします。

1. 関連する拒否またはキャンセルされた RFC を見つけて、このコマンドを使用できます (値を に置き換えることができます`Canceled`) 。

   ```
   aws amscm list-rfc-summaries --filter Attribute=RfcStatusId,Value=Rejected
   ```

2. 次のいずれかの RFC パラメータを変更できます。

   ```
   {
       "Description": "string",
       "ExecutionParameters": "string",
       "ExpectedOutcome": "string",
       "ImplementationPlan": "string",
       "RequestedEndTime": "string",
       "RequestedStartTime": "string",
       "RfcId": "string",
       "RollbackPlan": "string",
       "Title": "string",
       "WorstCaseScenario": "string"}
   ```

   説明フィールドを更新するコマンドの例 :

   ```
   aws amscm update-rfc --description "AMSTestNoOpsActionRequired" --rfc-id "RFC_ID"
    --region us-east-1
   ```

   ExecutionParameters VpcId フィールドを更新するコマンドの例 :

```
aws amscm update-rfc  --execution-parameters "{\"VpcId\":\"VPC_ID\"}" --rfc-id
 "RFC_ID" --region us-east-1
```

RFC を、更新を含む実行パラメータファイルで更新するコマンドの例。EC2 スタック | 作成：」のステップ 2 の実行パラメータファイルの例を参照してください。

```
aws amscm update-rfc --execution-parameters file://CreateEc2ParamsUpdate.json --
rfc-id "RFC_ID" --region us-east-1
```

3. submit-rfc と RFC が最初に作成されたときと同じ RFC ID を使用して RFC を再送信します。

```
aws amscm submit-rfc --rfc-id RFC_ID
```

RFC が成功した場合、コマンドラインに確認メッセージやエラーメッセージは表示されません。

4. リクエストのステータスをモニタリングし、実行出力を表示するには、次のコマンドを実行します。

```
aws amscm get-rfc --rfc-id RFC_ID
```

RFCs の検索

コンソールで変更リクエスト (RFC) を検索する

AMS コンソールを使用して RFC を検索するには、次の手順に従います。

> **Note**
>
> この手順は、スケジュールRFCs、つまり ASAP オプションを使用しなかった RFCs にのみ適用されます。

1. 左側のナビゲーションで、RFCsをクリックします。

   RFCsが開きます。

2. リストをスクロールするか、フィルターオプションを使用してリストを絞り込みます。

RFC リストはフィルター条件ごとに変わります。

3. 目的の RFC のサブジェクトリンクを選択します。

   RFC の詳細ページが開き、RFC ID などの情報が表示されます。

4. ダッシュボードに多数の RFCs がある場合は、フィルターオプションを使用して RFC で検索できます。

   - 件名: RFC の作成時に指定された件名またはタイトル (API/CLI 内) 。
   - RFC ID: RFC の識別子。
   - アクティビティ状態: RFC の状態がわかっている場合は、オペレータが現在 RFC を見ていることを示す AwsOperatorAssigned、AwsActionPending のいずれかを選択できます。つまり、AMS オペレータは RFC 実行を続行する前に何かを実行する必要があります。CustomerActionPending は、RFC 実行を続行する前に何らかのアクションを実行する必要があることを意味します。
   - ステータス: RFC ステータスがわかっている場合は、次のいずれかを選択できます。
     - スケジュール: スケジュールされた RFCs。
     - キャンセル済み: キャンセルされた RFCs。
     - 進行中: RFCsが進行中です。
     - Success: 正常に実行された RFCs。
     - 拒否 : 拒否された RFCs。
     - 編集中: 編集中の RFCs。
     - Failure: 失敗した RFCs。
     - 承認保留中: AMS またはユーザーが承認するまで続行できない RFCs。通常、これは RFC を承認する必要があることを示します。サービスリクエストリストにこのサービス通知が表示されます。
   - 変更タイプ: Category、Subcategory、Item、Operation を選択すると、変更タイプ ID が自動的に取得されます。
   - リクエストされた開始時刻またはリクエストされた終了時刻: このフィルターオプションでは、前または後を選択し、日付と、オプションで時刻 (hh:mm とタイムゾーン) を入力できます。このフィルターは、スケジュールされた RFCs (ASAP RFCs。
   - ステータス: スケジュール済み、キャンセル済み、進行中、成功、拒否済み、編集中、または失敗。
   - 件名: RFC に提供した件名 (または RFC が API/CLI で作成された場合はタイトル) 。

- 変更タイプ ID: RFC で送信された変更タイプの識別子を使用します。

次のスクリーンショットに示すように、検索ではフィルターを追加できます。

5. 目的の RFC の件名リンクをクリックします。

RFC の詳細ページが開き、RFC ID などの情報が表示されます。

CLI を使用した変更リクエスト (RFC) の検索

複数のフィルターを使用して RFC を検索できます。

変更タイプのバージョンを確認するには、次のコマンドを使用します。

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> 変更タイプのスキーマの一部であるかどうかにかかわらず、任意の RFC で任意のCreateRfcパラメータを使用できます。たとえば、RFC ステータスが変更されたときに通知を受け取るには、リクエストの RFC パラメータ部分 (実行パラメータではなく) --notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"にこの行を追加します。すべての CreateRfc パラメータのリストについては、AMS 変更管理 API リファレンスを参照してください。

RFC ID を書き留めず、後で見つける必要がある場合は、AMS 変更管理 (CM) システムを使用して ID を検索し、フィルターまたはクエリを使用して結果を絞り込むことができます。

1. CM API ListRfcSummaries オペレーションにはフィルターがあります。論理 AND オペレーションで Attributeと Valueを組み合わせて、または Attribute、、 に基づいてCondition結果をフィルタリングできますValues。

RFC フィルタリング

属性	有効値	有効な条件	デフォルトの条件	注意
ActualEndTime	ISO8601 日時を表す文字列 (例：「20170101T000000Z」)	前、後、間	なし	Before または After 条件は、Values フィールドで 1 つの値のみを受け入れます。Between 条件には、Values フィールドに正確に 2 つの値が必要です。最初の値は、2 番目の値より前の日付を表す必要があります。
ActualStartTime	ISO8601 日時を表す文字列 (例：「20170101T000000Z」)	前、後、間	なし	Before または After 条件は、Values フィールドで 1 つの値のみを受け入れます。Between 条件には、Values フィールドに正確に 2 つの値が必要です。最初の値は、2 番目の値より前の日付を表す必要があります。
AutomationStatusId	手動、自動	Equals (等しい)	Equals (等しい)	自動化ステータスは 2 つだけです
ChangeTypeId	任意の有効な変更タイプ ID。例: ct-123h45t6uz7jl	Equals (等しい)	Equals (等しい)	変更タイプまたは CSIO の検索

属性	有効値	有効な条件	デフォルトの条件	注意
ChangeTypeVersion	有効な変更タイプ ID。例: 1.0	Equals (等しい)	Equals (等しい)	変更タイプまたは CSIO の検索
CreatedBy	任意の文字列 (最大許容長は 2048 文字)	を含む	を含む	RFC の CreatedBy フィールドには、RFC を作成したユーザーの ARN が含まれます。
CreatedTime	ISO8601 日時を表す文字列 (例 :「20170101T000000Z」)	前、後、間	なし	Before または After 条件は、Values フィールドで 1 つの値のみを受け入れます。Between 条件には、Values フィールドに正確に 2 つの値が必要です。最初の値は、2 番目の値より前の日付を表す必要があります。
LastModifiedTime	ISO8601 日時を表す文字列 (例 :「20170101T000000Z」)	前、後、間	なし	Before または After 条件は、Values フィールドで 1 つの値のみを受け入れます。Between 条件には、Values フィールドに正確に 2 つの値が必要です。最初の値は、2 番目の値より前の日付を表す必要があります。

属性	有効値	有効な条件	デフォルトの条件	注意
LastSubmittedTime	ISO8601 日時を表す文字列 (例：「20170101T000000Z」)	前、後、間	なし	Before または After 条件は、Values フィールドで 1 つの値のみを受け入れます。Between 条件には、Values フィールドに正確に 2 つの値が必要です。最初の値は、2 番目の値より前の日付を表す必要があります。
RequestedEndTime	ISO8601 日時を表す文字列 (例：「20170101T000000Z」)	前、後、間	なし	Before または After 条件は、Values フィールドで 1 つの値のみを受け入れます。Between 条件には、Values フィールドに正確に 2 つの値が必要です。最初の値は、2 番目の値より前の日付を表す必要があります。

属性	有効値	有効な条件	デフォルトの条件	注意
RequestedStartTime	ISO8601 日時を表す文字列 (例：「20170101T000000Z」)	前、後、間	なし	Before または After 条件は、Values フィールドで 1 つの値のみを受け入れます。Between 条件には、Values フィールドに正確に 2 つの値が必要です。最初の値は、2 番目の値より前の日付を表す必要があります。
RfcStatusId	キャンセル済み、編集中、失敗、InProgress、PendingApproval、拒否済み、スケジュール済み、成功	Equals (等しい)	Equals (等しい)	AMS コンソールで RFC リストを更新するか、GetRfc を実行します。
役職	有効な RFC タイトル	を含む	を含む	個々のフィールドの正規表現はサポートされていません。大文字と小文字を区別しない検索

例:

SQS (SQS が CT のアイテム部分に含まれている) に関連するすべての RFCs の IDs を見つけるには、次のコマンドを使用します。

```
list-rfc-summaries --query 'RfcSummaries[?contains(Item.Name,`SQS`)].
[Category.Id,Subcategory.Id,Type.Id,Item.Id,RfcId]' --output table
```

これは次のようなものを返します。

```
-------------------------------------------------------------------------
|                          ListRfcSummaries                             |
+----------+---------------------------------+-------+-------+---------------+
|Deployment| Advanced Stack Components       |SQS    |Create |ct-123h45t6uz7jl|
|Management| Monitoring & Notification  |SQS    |Update |ct-123h45t6uz7jl|
+----------+---------------------------------+-------+-------+---------------+
```

で利用できるもう 1 つのフィルターlist-rfc-summariesはAutomationStatusId、自動または手動RFCs を検索する です。

```
aws amscm list-rfc-summaries --filter Attribute=AutomationStatusId,Value=Automated
```

で使用できるもう 1 つのフィルターlist-rfc-summariesは Title (コンソールの件名) です。

```
 Attribute=Title,Value=RFC-TITLE
```

RFCs を返す JSON の新しいリクエスト構造の例は次のとおりです。

- (タイトル 「Windows 2012」または「Amazon Linux」というフレーズが含まれます) AND
- (RfcStatusId EQUALS "Success" OR "InProgress") AND
- (20170101T00000Z <= RequestedStartTime <= 20170103T000000Z) AND (ActualEndTime <= 20170103T000000Z)

```
{
  "Filters": [
    {
      "Attribute": "Title",
      "Values": ["Windows 2012", "Amazon Linux"],
      "Condition": "Contains"
    },
    {
      "Attribute": "RfcStatusId",
      "Values": ["Success", "InProgress"],
      "Condition": "Equals"
    },
    {
      "Attribute": "RequestedStartTime",
```

```
      "Values": ["20170101T000000Z", "20170103T000000Z"],
      "Condition": "Between"
    },
    {
      "Attribute": "ActualEndTime",
      "Values": ["20170103T000000Z"],
      "Condition": "Before"
    }
  ]
}
```

> **Note**
>
> より高度な ではFilters、AMS は今後のリリースで次のフィールドを廃止する予定です。
>
> - Value: Value フィールドは Filters フィールドの一部です。より高度な機能をサポートする Values フィールドを使用します。
> - RequestedEndTimeRange: より高度な機能をサポートする Filters フィールド内で RequestedEndTime を使用します。
> - RequestedStartTimeRange: より高度な機能をサポートする Filters フィールド内で RequestedStartTime を使用します。

CLI クエリの使用の詳細については、「--query オプションで出力をフィルタリングする方法」および「クエリ言語リファレンス」のJMESPath 仕様」を参照してください。

2. AMS コンソールを使用している場合：

   RFCsリストページに移動します。必要に応じて、RFC サブジェクトをフィルタリングできます。これは、RFC の作成Title時に RFC として入力した内容です。

ヒント

> **Note**
>
> この手順は、スケジュールされた RFCs、つまり ASAP オプションを使用しなかった RFCs にのみ適用されます。

RFCs

コンソールまたは AMS API/CLI を使用して RFC をキャンセルできます。

コンソールで RFC をキャンセルするには、RFC リストで RFC を見つけて開きます。キャンセルをクリックします。

必要なデータ：

- `Reason`: RFC をキャンセルする理由。
- `RfcId`: キャンセルする RFC。

1. 通常、RFC は送信直後にキャンセルします (そのため、RFC ID は便利です)。そうしないと、スケジュールして指定した開始時刻より前でない限りキャンセルできません。RFC ID を見つける必要がある場合は、このコマンドを使用できます (手動で承認された RFC `ValuePendingApproval`の代わりに を使用できます)。

   ```
   aws amscm list-rfc-summaries --filter Attribute=RfcStatusId,Value=Scheduled
   ```

2. RFC をキャンセルするコマンドの例：

   ```
   aws amscm cancel-rfc --reason "Bad Stack ID" --rfc-id "RFC_ID" --profile saml --
   region us-east-1
   ```

RFCs

AMS コンソールには、RFCs。

RFC リストページを使用する (コンソール)

AMS コンソールRFCs リストページには、次のオプションがあります。

- フィルターによる高度な RFC 検索。詳細については、「RFCs の検索」を参照してください。
- RFC が最後に変更された時刻を検索します。この値は、RFC ステータスが最後に変更された時刻を表します。
- RFC サブジェクトを使用した RFC の詳細の表示。このリンクを選択すると、その RFC の詳細ページが開きます。

- RFC ステータスの表示。詳細については、「RFC ステータスコードを理解する」を参照してください。

RFC クイック作成を使用する (コンソール)

RFC クイック作成カードまたはリストテーブルを使用するか、分類別に RFCs の変更タイプを選択します。

詳細についてはRFC を作成するを参照してください。

RFC コレスポンデンスとアタッチメントを追加する (コンソール)

コレスポンデンスは、送信後、承認前に RFC に追加できます。例えば、PendingApproval」の状態です。RFC が承認されると (「スケジュール済み」またはInProgress」の状態)、リクエストの変更として解釈される可能性があるため、コレスポンデンスを追加できません。RFC が完了すると (「キャンセル済み」、「拒否済み」、「成功」、または「失敗」の状態)、通信は再度有効になりますが、RFC が 30 日以上閉じられると通信は無効になります。

> **Note**
>
> 各コレスポンデンスは 5,000 文字に制限されています。

添付ファイルの制限：

- コレスポンデンスごとに 3 つの添付ファイルのみ。
- RFC ごとに 50 個のアタッチメントを制限します。
- 各アタッチメントのサイズは 5 MB 未満である必要があります。
- プレーンテキスト (`.txt`)、カンマ区切り値 ()、JSON (`.csv`)、YAML (`.json`) などのテキストファイルのみが受け入れられます`.yaml`。YAML 形式の場合は、ファイル拡張子 を使用してファイルをアタッチする必要があります`.yaml`。

> **Note**
>
> XML コンテンツを含むテキストファイルは禁止されています。AMS と共有する XML コンテンツがある場合は、サービスリクエストを使用します。

- ファイル名は 255 文字に制限されており、数字、文字、スペース、ダッシュ (-)、アンダースコア (_)、ドット (.) のみを使用できます。
- RFC での添付ファイルの更新と削除は現在サポートされていません。

RFC にコレスポンデンスと添付ファイルを追加するには、次の手順に従います。

1. AMS コンソールの RFC の詳細ページで、ページの下部にある「通信」セクションを見つけます。

   通信前：

   いくつかの通信の後：

2. 新しいコレスポンデンスを追加するには、返信テキストボックスにメッセージを入力します。対応に関連するファイルをアタッチするには、添付ファイルの追加を選択し、必要なファイルを選択します。

3. 完了したら、送信を選択します。

   新しいコレスポンデンスは、添付ファイルへのリンクとともに、RFC の詳細ページのコレスポンデンスリストに表示されます。

RFC E メール通知を設定する (コンソール)

AMS コンソールの変更リクエストの作成ページには、RFC の状態変更の通知を受信する E メールアドレスを追加するオプションがあります。

さらに、次のような変更タイプに通知用の E メールアドレスを追加できます。

```
aws amscm create-rfc --change-type-id <Change type ID>
                     --change-type-version 1.0 --title "TITLE"
                     --notification "{\"Email\": {\"EmailRecipients\" :
 [\"email@example.com\"]}}"
```

パラメータ部分ではなく、RFC パラメータ部分の任意の変更タイプのインラインリクエストまたはテンプレートリクエストに同様の行 (--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}") を追加します。

一般的な RFC パラメータについて説明します。

以下は、送信する必要がある RFC パラメータと、RFCs。

- 変更タイプ情報: ChangeTypeId と ChangeTypeVersion。変更タイプ IDs「変更タイプリファレンス」を参照してください。

  CLI list-change-type-classification-summariesで query引数を使用して を実行し、結果を絞り込みます。たとえば、結果を絞り込んで、Item名前に「アクセス」を含むタイプを変更します。

  ```
  aws amscm list-change-type-classification-summaries --query
   "ChangeTypeClassificationSummaries [?contains (Item, 'access')].
  [Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
  ```

  を実行しget-change-type-version、変更タイプ ID を指定します。次のコマンドは、ct-2tylseo8rxfsc の CT バージョンを取得します。

  ```
  aws amscm get-change-type-version --change-type-id ct-2tylseo8rxfsc
  ```

- タイトル: RFC の名前。これは AMS コンソール RFC リストの RFC のサブジェクトになり、GetRfc コマンドとフィルターを使用して検索できます。 Title
- スケジュール: スケジュールされた RFC が必要な場合は、 パラメータRequestedStartTimeとRequestedEndTimeパラメータを含めるか、この変更のスケジュールコンソールオプションを使用する必要があります。ASAP RFC (承認されるとすぐに実行される) の場合、CLI を使用するときは、 RequestedStartTimeと RequestedEndTime null のままにします。コンソールを使用する場合は、ASAP オプションを受け入れます。

  RequestedStartTime が見つからない場合、RFC は拒否されます。
- CT のプロビジョニング CTs: 実行パラメータ、または Parametersは、リソースのプロビジョニングに必要な特定の設定です。CT によって大きく異なります。
- 非プロビジョニング CTs: アクセス CTsやその他 | その他などのリソースをプロビジョニングしない CT、またはスタックを削除しない CTs は、最小限の実行パラメータを持ち、Parametersブロックはありません。

- RFCs、 を指定するかTimeoutInMinutes、RFC が失敗するまでにスタックの作成に何分かかるかも指定する必要があります。長時間実行される UserData の有効な値は 60 (分) から 360 までです。を超える前に実行を完了できない場合、RFC TimeoutInMinutes は失敗します。ただし、この設定では RFC の実行が遅延することはありません。
- S3 バケットや ELB などのインスタンスを作成する RFCs は、通常、最大 7 つのタグ (キーと値のペア) を追加できるスキーマを提供します。デプロイ | 高度なスタックコンポーネント | タグ | 変更タイプの作成 (ct-3cx7we852p3af) を使用して RFC を送信することで、S3 バケットにタグを追加できます。EC2、EFS、RDS、および多層 (HA 2 階層および HA 1 階層) スキーマでは、最大 50 個のタグを使用できます。タグはスキーマの ExecutionParameters部分で指定されます。タグを提供することは大きな価値があります。詳細については、「Amazon EC2 リソースにタグを付ける」を参照してください。

  AMS コンソールを使用する場合は、タグを追加するには追加設定エリアを開く必要があります。

> **Tip**
>
> 多くの CT スキーマには、スキーマの上部近くに Description および Nameフィールドがあります。これらのフィールドは、スタックまたはスタックコンポーネントに名前を付けるために使用されます。作成するリソースには名前を付けません。一部のスキーマは、作成するリソースに名前を付けるパラメータを提供し、そうでないスキーマもあります。たとえば、Create EC2 スタックの CT スキーマは、EC2 インスタンスに名前を付けるパラメータを提供しません。そのためには、キー「Name」と名前の値を持つタグを作成する必要があります。このようなタグを作成しない場合、EC2 インスタンスは EC2 コンソールに名前属性なしで表示されます。

RFC AWS リージョンオプションを使用する

AMS API および CLI (amscm および amsskms) エンドポイントは にありますus-east-1。Security Assertion Markup Language (SAML) とフェデレーションする場合、 AWS リージョンを us-east-1 に設定するスクリプトがオンボーディング時に提供されます。SAML を使用する場合、コマンドを発行するときに --regionオプションを指定する必要はありません。SAML が us-east-1 を使用するように設定されていても、アカウントがその AWS リージョンにない場合は、他の AWS コマンド (例:) を発行するときに、アカウントオンボーディングリージョンを指定する必要がありますaws s3。

> **Note**
>
> このガイドに記載されているコマンド例のほとんどには、 `--region`オプションは含まれていません。

RFC の毎日の E メールにサインアップする

RFC ダイジェスト機能を使用して、過去 24 時間のアカウントの RFC アクティビティをまとめた毎日の E メールにサインアップできます。RFC ダイジェスト機能は、アカウントの RFCs。RFC ダイジェストは、応答を保留しているアクションを見逃す可能性を減らす可能性があります。

RFC ダイジェスト機能を有効にするには、AMS Cloud Service Delivery Manager (CSDM) にお問い合わせください。CSDM がサブスクライブします。RFC ダイジェスト E メールリストに含める E メールアドレス (またはエイリアス) を最大 20 個リクエストできます。現在の E メールスケジュールは 09:00 UTC-8 に固定されています。

RFC ダイジェスト機能をオフにするには、CSDM に連絡してリクエストしてください。

RFC ダイジェストを設定せず、RFCs に関する通知が必要な場合、または RFCs ダイジェストが提供する情報よりも RFC に関する詳細情報が必要な場合は、変更管理システムを使用して、情報が必要な個々の RFC ごとに CloudWatch Events 通知または E メール通知を設定します。RFC 通知の設定については、「RFC 状態変更通知」を参照してください。

RFC ダイジェストに含まれるトピックは次のとおりです。

- Pending Customer Approval: PendingApproval ステータスの RFCs を一覧表示し、承認待ちにします
- Pending Customer Reply: RFCs 通信に関する返信を待っている RFC を一覧表示します
- AWS 承認または応答の保留中: AMS が応答または承認を待っている RFCs を一覧表示します
- 完了: 成功、失敗、キャンセル、拒否のステータスRFCs を一覧表示します

RFC ダイジェストの例を次に示します。

変更タイプとは?

変更タイプとは、AWS Managed Services (AMS) による変更リクエスト (RFC) が実行し、変更アクション自体、および変更のタイプを手動と自動で含めるアクションを指します。AMS には、他の

Amazon ウェブサービスでは使用されていない変更タイプの大規模なコレクションがあります。これらの変更タイプは、リソースをデプロイ、管理、またはアクセスするための変更リクエスト (RFC) を送信するときに使用します。

トピック

- 自動および手動 CTs
- CT 承認要件
- 変更タイプバージョン
- 変更タイプを作成する
- 変更タイプを更新する
- 内部のみの変更タイプ
- 変更タイプスキーマ
- 変更タイプのアクセス許可の管理
- 変更タイプから機密情報を編集する
- クエリオプションを使用した変更タイプの検索

自動および手動 CTs

変更タイプの制約は、自動か手動かです。これは、AMS コンソールで実行モードと呼ばれる変更タイプの`AutomationStatusId`属性です。

自動変更タイプには期待される結果と実行時間があり、通常は 1 時間以内に AMS 自動システムを通じて実行されます (これは CT がプロビジョニングするリソースに大きく依存します) 。手動変更タイプは一般的ではありませんが、実行する前に AMS オペレーターが RFC を操作する必要があるため、扱いが異なります。つまり、RFC 送信者と通信する場合があるため、手動の変更タイプでは、完了までにさまざまな時間がかかることがあります。

スケジュールされたすべての RFCs について、未指定の終了時刻は、指定された時刻に送信された変更タイプの `ExpectedExecutionDurationInMinutes` 属性を`RequestedStartTime`足した時刻になるように書き込まれます。たとえば、 `ExpectedExecutionDurationInMinutes`が「60」 (分) で、指定された `RequestedStartTime`が `2016-12-05T14:20:00Z` (2016 年 12 月 5 日午前 4 時 20 分) の場合、実際の終了時刻は 2016 年 12 月 5 日午前 5 時 20 分に設定されます。`ExpectedExecutionDurationInMinutes` 特定の変更タイプの を検索するには、次のコマンドを実行します。

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --
query "ChangeTypeVersion.{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

> **Note**
>
> スケジュールされた RFCsの実行モード = コンソールでは、少なくとも 24 時間後に実行するように設定する必要があります。この注意は AMS API/CLI には適用されませんが、少なくとも 8 時間前に手動 RFCs をスケジュールすることが重要です。

> **Note**
>
> 「レビュー必須」CT を使用する場合、AMS では ASAP スケジューリングオプション (コンソールで ASAP を選択し、API/CLI で開始時刻と終了時刻を空白のままにしておく) を使用することをお勧めします。これらの CTs では、AMS オペレータが RFC を調べる必要があり、承認して実行する前に通信する必要があるためです。これらの RFCsスケジュールする場合は、少なくとも 24 時間かかります。スケジュールされた開始時刻より前に承認が行われない場合、RFC は自動的に拒否されます。

AMS は手動 CT に 4 時間以内に応答することを目指しており、できるだけ早く対応しますが、RFC が実際に実行されるまでにかなり時間がかかる場合があります。

手動であり、AMS レビューが必要な CTs「変更タイプ CSV ファイル」を参照してください。

YouTube Video: AMS RFCs の自動変更タイプを見つけるにはどうすればよいですか？

AMS コンソールで CT の実行モードを見つけるには、変更タイプの参照検索オプションを使用する必要があります。結果には、一致する変更タイプまたは変更タイプの実行モードが表示されます。

AMS CLI を使用してAutomationStatus特定の変更タイプの を検索するには、次のコマンドを実行します。

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --
query "ChangeTypeVersion.{AutomationStatus:AutomationStatus.Name}"
```

すべての AMS 変更タイプに関する情報を提供する AMS 変更タイプリファレンスで変更タイプを検索することもできます。

> **Note**
>
> AMS API/CLI は現在、AWS API/CLI の一部ではありません。AMS API/CLI にアクセスするには、AMS コンソールから AMS SDK をダウンロードします。

CT 承認要件

AMS CTs には、常に AwsApprovalId と CustomerApprovalId の 2 つの承認条件があり、RFC が実行を承認するために AMS またはユーザー、あるいは誰かを必要とするかどうかを示します。

承認条件は実行モードと多少関連しています。詳細については、「」を参照してください自動および手動 CTs。

CT の承認条件を確認するには、AMS 変更タイプリファレンスを参照するか、GetChangeTypeVersion を実行します。どちらも CT モードAutomationStatusIdまたは実行モードも提供します。

RFCs を承認するには、AMS コンソールを使用するか、次のコマンドを使用します。

```
aws amscm approve-rfc --rfc-id RFC_ID
```

CT 承認条件

CT 承認条件が の場合	からの承認が必要です	And
`AwsApprovalId: Required`	AMS 変更タイプシステム	アクションは必要ありません。この条件は、自動 CTs。
`AwsApprovalId: NotRequiredIfSubmitter`	送信された RFC が送信されたアカウント用である場合、AMS 変更タイプシステムであり、他に誰もいません。	アクションは必要ありません。この条件は、AMS 演算子によって常にレビューされるため、手動 CTs では一般的です。

CT 承認条件が の場合	からの承認が必要です	And
CustomerApprovalId: NotRequired	AMS 変更タイプシステム	RFC が構文チェックとパラメータチェックに合格すると、自動承認されます。
CustomerApprovalId: Required	AMS 変更タイプシステムとユーザー	通知が送信され、通知に応答するか、ApproveRfc オペレーションを実行して、RFC を明示的に承認する必要があります。
CustomerApprovalId: NotRequiredIfSubmitter	RFC を送信した場合は、AMS 変更タイプシステムであり、他のユーザーではありません。	RFC が構文チェックとパラメータチェックに合格すると、自動承認されます。
緊急のセキュリティインシデントまたはパッチ	AMS	自動承認され、実装されています。

変更タイプバージョン

変更タイプはバージョン管理され、バージョンは変更タイプにメジャーな更新が行われたときに変更されます。

AMS コンソールを使用して変更タイプを選択したら、追加設定エリアを開き、変更タイプバージョンを選択するオプションがあります。API/CLI コマンドラインで変更タイプバージョンを指定することもできます。これは、次のようなさまざまな理由で実行できます。

- 更新する変更タイプのバージョンは、更新するリソースの作成に使用した変更タイプの作成バージョンと一致する必要があります。たとえば、ELB Create change type version 1 で作成した Elastic Load Balancer (ELB) インスタンスがあるとします。更新するには、ELB 更新バージョン 1 を選択します。
- 最新の変更タイプとは異なるオプションを含む変更タイプバージョンを使用します。AMS は主にセキュリティ上の理由から変更タイプを更新するため、これはお勧めしません。常に最新バージョンを選択することをお勧めします。

変更タイプを作成する

変更タイプの作成は、version-to-version更新変更タイプと一致します。つまり、リソースのプロビジョニングに使用する変更タイプバージョンは、後でそのリソースを変更するために使用する更新変更タイプのバージョンと一致する必要があります。例えば、Create S3 Bucket change type version 2.0 で S3 バケットを作成し、後で RFC を送信してその S3 バケットを変更する場合は、バージョン 3.0 の Update S3 Bucket change type version 2.0 があっても、Update S3 Bucket change type version 2.0 も使用する必要があります。

後で Update 変更タイプを使用してリソースを変更する場合に備えて、Create 変更タイプでリソースをプロビジョニングするときに使用する変更タイプ ID とバージョンを記録しておくことをお勧めします。

変更タイプを更新する

AMS には、Create change types で作成されたリソースを更新するための Update change types が用意されています。Update 変更タイプは、リソースのプロビジョニングに最初に使用された Create 変更タイプとversion-to-version一致させる必要があります。

更新しやすいように、リソースをプロビジョニングするときに使用する変更タイプ ID とバージョンを記録しておくことをお勧めします。

YouTube 動画: 更新 CTs を使用して AWS Managed Services (AMS) アカウントのリソースを変更する方法を教えてください。

内部のみの変更タイプ

内部使用のみの変更タイプを確認できます。これにより、AMS が実行できる、または実行するアクションがわかります。使用できる内部のみの変更タイプがある場合は、サービスリクエストを送信します。

例えば、管理 | モニタリングと通知 | CloudWatch アラーム抑制 | CT の更新は内部専用です。AMS はこれを使用してインフラストラクチャの更新 (パッチ適用など) をデプロイし、更新が誤ってトリガーされる可能性のあるアラーム通知をオフにします。この CT が送信されると、RFC リストに CT の RFC が表示されます。RFC にデプロイされている内部専用 CT は、RFC リストに表示されます。

変更タイプスキーマ

すべての変更タイプは、リソースの作成、変更、またはアクセスの入力に JSON スキーマを提供します。スキーマは、変更リクエスト (RFC) を作成するためのパラメータとその説明を提供します。

RFC が正常に実行されると、実行出力になります。RFCsプロビジョニングの場合、実行出力には CloudFormation のスタックを表す「stack_id」が含まれ、CloudFormation コンソールで検索できます。実行出力には、作成されたインスタンスの ID の出力が含まれる場合があり、その ID を使用して対応する AWS コンソールでインスタンスを検索できます。例えば、Create ELB CT 実行出力には、CloudFormation で検索可能な「stack_id」が含まれ、Elastic Load Balancing の Amazon EC2 コンソールで検索可能な key=ELB value=<stack-xxxx> を出力します。

CT スキーマを見てみましょう。これは、かなり小さなスキーマである CodeDeploy Application Create のスキーマです。一部のスキーマには、非常に大きなParameter領域があります。

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "name": "Create CodeDeploy application",
  "description": "Use to create an AWS CodeDeploy applicati
on
  resource with the specified name.",
  "type": "object",
  "properties": {
    "Description": {
      "description": "The reason for the request.",
      "type": "string",
      "minLength": 1,
      "maxLength": 500
    },
    "VpcId": {
      "description": "ID of the vpc to use, in the form
 vpc-0123abcd or vpc-01234567890abcdef.",
      "type": "string",
      "pattern": "^vpc-[a-z0-9]{8}$"
    },
    "StackTemplateId": {
      "description": "Must be stm-sft6rv00000000000",
      "type": "string",
      "enum": ["stm-sft6rv00000000000"]
    },
    "Name":{
      "description": "A name for the stack or stack component
;
      this becomes the Stack Name.",
      "type": "string",
      "minLength": 1,
      "maxLength": 255
```

スキーマの最初の部分は、リクエストされた変更タイプに関する情報を AMS に提供します。

```
    },
    "Tags": {
      "description": "Up to seven tags (key/value pairs) to
      categorize the resource.",
      "type": "array",
      "items": {
        "type": "object",
        "properties": {
          "Key": {
            "type": "string",
            "minLength": 1,
            "maxLength": 127
          },
          "Value": {
            "type": "string",
            "minLength": 1,
            "maxLength": 255
          }
        },
        "additionalProperties": false,
        "required": [
          "Key",
          "Value"
        ]
      },
      "minItems": 1,
      "maxItems": 7
    },
    "TimeoutInMinutes": {
      "description": "The maximum amount of time, in minutes,
to
     allow for execution of the change. This will not prolong
execution,
     but the RFC fails if the change is not completed in the
specified time.
     Valid values are 60 up to 360, for long-running
UserData.",
      "type": "number",
      "minimum": 0,
      "maximum": 60
    },
    "Parameters": {
      "description": "Specifications for the stack.",
      "type": "object",
```

TimeoutInMinutes パラメータを使用すると、変更タイプを実行する境界時間を指定できます。長時間実行される UserData の有効な値は 60 ~ 360 です。

Parameters セクションでは、作成するリソースの設定、またはリクエストするアクションを指定します。

「追加プロパティ」セクションでは、どのパラメータが必要

```
      "properties": {
        "CodeDeployApplicationName": {
          "description": "The name of an AWS CodeDeploy
 application.",
          "type": "string",
          "minLength": 1,
          "maxLength": 100,
          "pattern": "^[a-zA-Z0-9._+=,@-]{1,100}$"
        }
      },
      "additionalProperties": false,
      "required": [
        "CodeDeployApplicationName"
      ]
    }
  },
  "additionalProperties": false,
  "required": [
    "Description",
    "VpcId",
    "StackTemplateId",
    "Name",
    "TimeoutInMinutes",
    "Parameters"
  ]
}
```

で、どれがオプションかがわかります。

> **Note**
>
> このスキーマでは最大 7 つのタグを使用できますが、EC2、EFS、RDS、および多層作成スキーマでは最大 50 個のタグを使用できます。

変更タイプのアクセス許可の管理

カスタムポリシーを使用して、異なるグループまたはユーザーが使用できる変更タイプ (CTs) を制限できます。

これを行う方法の詳細については、「AMS ユーザーガイド」セクション「アクセス許可の設定」を参照してください。

変更タイプから機密情報を編集する

AMS 変更タイプスキーマ`"metadata":"ams:sensitive":"true"`は、パスワードなどの機密情報を含むパラメータに使用されるパラメータ属性を提供します。この属性を設定すると、指定された入力は不明瞭になります。このパラメータ属性は設定できないことに注意してください。ただし、AMS を使用して変更タイプを作成し、入力時に不明瞭にするパラメータがある場合は、これをリクエストできます。

クエリオプションを使用した変更タイプの検索

この例では、AMS コンソールを使用して、送信する RFC の適切な変更タイプを見つける方法を示します。

コンソールまたは API/CLI を使用して、変更タイプ ID (CT) またはバージョンを検索できます。検索または分類の選択の 2 つの方法があります。どちらの選択タイプでも、最も頻繁に使用される、最近使用された、またはアルファベットのいずれかを選択して検索をソートできます。

YouTube 動画: AWS Managed Services CLI を使用して RFC を作成する方法と、CT スキーマの場所を教えてください。

AMS コンソールの RFCs -> RFC の作成ページで、次の操作を行います。

- 変更タイプによる参照 (デフォルト) を選択した場合、次のいずれかを実行します。
  - クイック作成エリアを使用して、AMS の最も一般的な CTs から選択します。ラベルをクリックすると、RFC の実行ページが開き、件名オプションが自動的に入力されます。必要に応じて残りのオプションを完了し、実行をクリックして RFC を送信します。
  - または、すべての変更タイプ領域までスクロールダウンし、オプションボックスに CT 名を入力し始めます。変更タイプ名を完全または完全に設定する必要はありません。関連する単語を入力して、変更タイプ ID、分類、または実行モード (自動または手動) で CT を検索することもできます。

    デフォルトのカードビューを選択すると、入力時に一致する CT カードが表示され、カードを選択して RFC の作成をクリックします。テーブルビューを選択し、関連する CT を選択し、RFC の作成をクリックします。どちらの方法でも、RFC の実行ページが開きます。
- または、変更タイプの選択肢を確認するには、ページ上部の「カテゴリ別に選択」をクリックして、一連のドロップダウンオプションボックスを開きます。
- カテゴリ、サブカテゴリ、項目、オペレーションを選択します。その変更タイプの情報ボックスは、ページの下部にパネルが表示されます。

- 準備ができたら、Enter キーを押すと、一致する変更タイプのリストが表示されます。
- リストから変更タイプを選択します。その変更タイプの情報ボックスがページの下部に表示されます。
- 正しい変更タイプを取得したら、RFC の作成を選択します。

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

> **Note**
>
> AMS API/CLI (amscm および amsskms) エンドポイントは、AWS N. Virginia リージョン にありますus-east-1。認証の設定方法や、アカウントとリソースが存在する AWS リージョンによっては、コマンドの発行`--region us-east-1`時に追加が必要になる場合があります。認証方法である場合は`--profile saml`、 を追加する必要がある場合もあります。

AMS CM API (ListChangeTypeClassificationSummaries を参照) または CLI を使用して変更タイプを検索するには：

フィルターまたはクエリを使用して検索できます。ListChangeTypeClassificationSummaries オペレーションには、`Category`、、`SubcategoryItem`、および のフィルターオプションがありますが`Operation`、値は既存の値と完全に一致する必要があります。CLI を使用する際のより柔軟な結果を得るには、 `--query`オプションを使用できます。

AMS CM API/CLI を使用した変更タイプのフィルタリング

属性	有効値	有効/デフォルト条件	注意
ChangeTypeId	ChangeTypeId を表す任意の文字列 (例: ct-abc123xyz7890)	Equals (等しい)	変更タイプ IDs「変更タイプリファレンス」を参照してください。 変更タイプ IDs「変更タイプまたは CSIO の検索」を参照してください。
カテゴリ	任意の自由形式のテキスト	を含む	個々のフィールドの正規表現はサポートされていません。大文字と小文字を区別しない検索
サブカテゴリ			
Item			
Operation			

1. 変更タイプの分類を一覧表示する例をいくつか示します。

   次のコマンドは、すべての変更タイプカテゴリを一覧表示します。

   ```
   aws amscm list-change-type-categories
   ```

   次の コマンドは、指定されたカテゴリに属するサブカテゴリを一覧表示します。

   ```
   aws amscm list-change-type-subcategories --category CATEGORY
   ```

   次の コマンドは、指定されたカテゴリとサブカテゴリに属する項目を一覧表示します。

   ```
   aws amscm list-change-type-items --category CATEGORY --subcategory SUBCATEGORY
   ```

2. CLI クエリで変更タイプを検索する例をいくつか示します。

次のコマンドは、項目名に「S3」が含まれている CT 分類の概要を検索し、カテゴリ、サブカテゴリ、項目、オペレーション、変更タイプ ID の出力をテーブル形式で作成します。

```
aws amscm list-change-type-classification-summaries --query
 "ChangeTypeClassificationSummaries [?contains(Item, 'S3')].
[Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
```

```
+-------------------------------------------------------------+
|               ListChangeTypeClassificationSummaries         |
+----------+-------------------------+--+------+--------------+
|Deployment|Advanced Stack Components|S3|Create|ct-1a68ck03fn98r|
+----------+-------------------------+--+------+--------------+
```

3. その後、変更タイプ ID を使用して CT スキーマを取得し、パラメータを調べることができます。次のコマンドは、CreateS3Params.schema.json.

```
aws amscm get-change-type-version --change-type-id "ct-1a68ck03fn98r"
 --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
 CreateS3Params.schema.json
```

CLI クエリの使用の詳細については、「--query Option で出力をフィルタリングする方法」および「クエリ言語リファレンス」のJMESPath Specification」を参照してください。

4. 変更タイプ ID を取得したら、変更タイプのバージョンを検証して最新バージョンであることを確認することをお勧めします。次のコマンドを使用して、指定された変更タイプのバージョンを検索します。

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CHANGE_TYPE_ID
```

AutomationStatus 特定の変更タイプの を検索するには、次のコマンドを実行します。

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --
query "ChangeTypeVersion.{AutomationStatus:AutomationStatus.Name}"
```

ExpectedExecutionDurationInMinutes 特定の変更タイプの を検索するには、次のコマンドを実行します。

```
aws amscm --profile saml get-change-type-version --change-type-id ct-14027q0sjyt1h
 --query "ChangeTypeVersion.{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

AMS での RFC エラーのトラブルシューティング

多くの AMS プロビジョニング RFC 障害は、CloudFormation ドキュメントを通じて調査できます。AWS CloudFormation のトラブルシューティング: エラーのトラブルシューティング」を参照してください。

追加のトラブルシューティングの提案については、以下のセクションで説明します。

AMS の「管理」RFC エラー

AMS "Management" カテゴリ変更タイプ (CTs) を使用すると、リソースへのアクセスをリクエストしたり、既存のリソースを管理したりできます。このセクションでは、いくつかの一般的な問題について説明します。

RFC アクセスエラー

- RFC で指定したユーザー名と FQDN が正しく、ドメインに存在することを確認します。FQDN の検索については、「FQDN の検索」を参照してください。
- アクセス用に指定したスタック ID が EC2-relatedスタックであることを確認します。ELB や Amazon Simple Storage Service (S3) などのスタックは、アクセス RFCsの候補ではなく、読み取り専用アクセスロールを使用してこれらのスタックリソースにアクセスします。スタック ID の検索については、「スタック IDs」を参照してください。
- 指定したスタック ID が正しく、関連するアカウントに属していることを確認します。

その他のアクセス RFC 障害については、「アクセス管理」を参照してください。

YouTube 動画: 拒否や失敗を避けるために、変更リクエスト (RFC) を適切に作成するにはどうすればよいですか？

RFC (手動) CT スケジューリングエラー

ほとんどの変更タイプは ExecutionMode=Automated ですが、一部は ExecutionMode=Manual であり、RFC の失敗を避けるためのスケジュール方法に影響します。

ExecutionMode=Manual のスケジュールされた RFCs は、AMS コンソールを使用して RFC を作成する場合は、少なくとも 24 時間後に実行するように設定する必要があります。この注意は AMS API/CLI には適用されませんが、少なくとも 8 時間前に手動 RFCs をスケジュールすることが重要です。

AMS は手動 CT に 4 時間以内に応答することを目指しており、できるだけ早く対応しますが、RFC が実際に実行されるまでにかなり時間がかかる場合があります。

手動更新 CT RFCs の使用 CTs

AMS オペレーションは、更新するスタックのタイプに更新変更タイプがある場合、管理を拒否する | その他 | スタックの更新に関するその他の RFCs。

RFC スタック削除エラー

RFC 削除スタックの失敗: 管理 | 標準スタック | スタック | CT を削除すると、AMS スタック名を持つスタックの詳細なイベントが CloudFormation コンソールに表示されます。スタックは、AMS コンソールの名前と照合することで識別できます。 CloudFormation コンソールには、障害の原因に関する詳細が表示されます。

スタックを削除する前に、スタックの作成方法を考慮する必要があります。AMS CT を使用してスタックを作成し、スタックリソースを追加または編集しなかった場合、問題なく削除できます。ただし、削除スタック RFC を送信する前に、手動で追加されたリソースをスタックから削除することをお勧めします。たとえば、フルスタック CT (HA Two Tier) を使用してスタックを作成する場合、セキュリティグループ - SG1 が含まれます。次に AMS を使用して別のセキュリティグループ SG2 を作成し、フルスタックの一部として作成された SG1 内の新しい SG2 を参照し、削除スタック CT を使用してスタックを削除した場合、SG2 SG1 は削除しません。 SG1

> **Important**
>
> スタックを削除すると、望ましくない結果や予期しない結果が生じる可能性があります。AMS は、この理由から、お客様に代わってスタックまたはスタックリソースを *削除しない* ことを優先します。AMS は、ユーザーに代わって (送信された管理 | その他 | その他 | 変更タイプの更新を通じて) 、削除する適切な自動変更タイプを使用して削除できないリソースのみを削除することに注意してください。追加の考慮事項:
>
> - リソースが「削除保護」に対して有効になっている場合、管理 | その他 | その他 | 変更タイプを更新し、削除保護が削除された後、自動 CT を使用してそのリソースを削除することで、AMS はこれをブロック解除できます。

- スタックに複数のリソースがあり、スタックリソースのサブセットのみを削除する場合は、CloudFormation Update 変更タイプを使用します (CloudFormation Ingest Stack: Updatedating」を参照) 。管理 | その他 | その他 | 更新変更タイプを送信することもできます。AMS エンジニアは、必要に応じて変更セットの作成を支援します。
- ドリフトが原因で CloudFormation Update CT の使用に問題がある場合、AMS は、管理 | その他 | その他 | 更新を送信してドリフトを解決し (AWS CloudFormation サービスでサポートされる限り) 、自動 CT、管理/カスタムスタック/CloudFormation テンプレートからのスタック/変更セットと更新の承認を使用して検証および実行できる ChangeSet を提供できます。

AMS は、予期しないリソースの削除や予期しないリソースの削除がないように、上記の制限を維持します。

詳細については、AWS CloudFormation のトラブルシューティング: スタックの削除が失敗する」を参照してください。

RFC 更新 DNS エラー

DNS ホストゾーンを更新する複数の RFCs は、理由なしに失敗する可能性があります。DNS ホストゾーン (プライベートまたはパブリック) を更新するために複数の RFCs を同時に作成すると、同じスタックを同時に更新しようとしているために、一部の RFCs が失敗する可能性があります。AMS 変更管理は、スタックが別の RFCs によって既に更新されているため、スタックを更新できない RFC を拒否または失敗します。AMS では、一度に 1 つの RFC を作成し、RFC が成功するのを待ってから、同じスタック用に新しい RFC を作成することをお勧めします。

RFC IAM エンティティエラー

AMS は、ニーズを満たすように設計されたいくつかのデフォルトの IAM ロールとプロファイルを AMS アカウントにプロビジョニングします。ただし、追加の IAM リソースをリクエストする必要がある場合があります。

カスタム IAM リソースをリクエストする RFCs を送信するプロセスは、手動 RFCsの標準ワークフローに従いますが、承認プロセスには、適切なセキュリティコントロールが実施されていることを確認するためのセキュリティレビューも含まれています。したがって、通常、このプロセスは他の手動 RFCsよりも時間がかかります。これらの RFCsのサイクル時間を短縮するには、次のガイドラインに従ってください。

IAM レビューの意味と、それが技術標準およびリスク許容プロセスにどのようにマッピングされるかについては、「」を参照してくださいRFC セキュリティレビューを理解する。

一般的な IAM リソースリクエスト：

- CloudEndure などの主要なクラウド互換アプリケーションに関連するポリシーをリクエストする場合は、AMS の事前承認された IAM CloudEndure ポリシー: WIGs Cloud Endure ランディングゾーンの例ファイルを解凍し、 `customer_cloud_endure_policy.json`

> **Note**
>
> より寛容なポリシーが必要な場合は、CloudArchitect/CSDM とニーズについて話し合い、必要に応じて、ポリシーを実装する RFC を送信する前に AMS セキュリティレビューとサインオフを取得します。

- AMS によってアカウントにデプロイされたリソースをデフォルトで変更する場合は、既存のリソースに変更を加えるのではなく、そのリソースの修正されたコピーをリクエストすることをお勧めします。
- (アクセス許可をユーザーにアタッチするのではなく) 人間のユーザーのアクセス許可をリクエストする場合は、アクセス許可をロールにアタッチし、そのロールを引き受けるアクセス許可をユーザーに付与します。これを行う方法の詳細については、「一時的な AMS Advanced コンソールアクセス」を参照してください。
- 一時的な移行またはワークフローに例外的なアクセス許可が必要な場合は、リクエストでそれらのアクセス許可の終了日を指定します。
- リクエストの件名についてセキュリティチームとすでに話し合っている場合は、CSDM に承認の証拠をできるだけ詳しく提供します。

AMS が IAM RFC を拒否する場合は、拒否の明確な理由を指定します。例えば、IAM ポリシー作成リクエストを拒否し、ポリシーが不適切であることについて説明します。その場合は、特定された変更を行い、リクエストを再送信できます。リクエストのステータスをさらに明確にする必要がある場合は、サービスリクエストを送信するか、CSDM にお問い合わせください。

次のリストは、IAM RFCs を確認するときに AMS が軽減を試みる一般的なリスクを示しています。IAM RFC にこれらのリスクがある場合、RFC が拒否される可能性があります。例外が必要な場合、AMS はセキュリティチームの承認を求めます。このような例外を求めるには、CSDM と調整します。

> **Note**
>
> AMS は、何らかの理由で、アカウント内の IAM リソースへの変更を拒否することがあります。RFC 拒否に関する懸念については、サービスリクエストを通じて AMS オペレーションに問い合わせるか、CSDM にお問い合わせください。

- 独自のアクセス許可を変更したり、アカウント内の他のリソースのアクセス許可を変更したりできるアクセス許可など、権限のエスカレーション。例:
  - より特権的な別のロールで `iam:PassRole` を使用する。
  - ロールまたはユーザーから IAM ポリシーをアタッチ/デタッチするアクセス許可。
  - アカウントの IAM ポリシーの変更。
  - 管理インフラストラクチャのコンテキストで API コールを行う機能。
- AMS サービスを提供するために必要なリソースまたはアプリケーションを変更するアクセス許可。例:
  - 踏み台、管理ホスト、EPS インフラストラクチャなどの AMS インフラストラクチャの変更。
  - ログ管理 AWS Lambda 関数、またはログストリームの削除。
  - デフォルトの CloudTrail モニタリングアプリケーションの削除または変更。
  - Directory Services Active Directory (AD) の変更。
  - CloudWatch (CW) アラームを無効にする。
  - ランディングゾーンの一部としてアカウントにデプロイされたプリンシパル、ポリシー、名前空間の変更。
- 情報セキュリティを危険にさらす状態でインフラストラクチャを作成できるアクセス許可など、ベストプラクティス外のインフラストラクチャのデプロイ。例:
  - パブリックまたは暗号化されていない S3 バケットの作成または EBS ボリュームのパブリック共有。
  - パブリック IP アドレスのプロビジョニング。
  - 広範なアクセスを許可するセキュリティグループの変更。
- データ損失、整合性損失、不適切な設定、インフラストラクチャおよびアカウント内のアプリケーションのサービスの中断につながる可能性のあるアクセス許可など、アプリケーションに影響を与える可能性のある過度に広範なアクセス許可。例:
  - や などの APIs を介したネットワークトラフィックの無効化`ModifyNetworkInterfaceAttribute`またはリダイレクト`UpdateRouteTable`。

  - マネージドホストからボリュームをデタッチしてマネージドインフラストラクチャを無効にすること。
- AMS サービスの説明の一部ではなく、AMS でサポートされていないサービスのアクセス許可。

  AMS サービスの説明に記載されていないサービスは、AMS アカウントでは使用できません。機能またはサービスのサポートをリクエストするには、CSDM にお問い合わせください。
- 過度に寛大であるか、保守的であるか、間違ったリソースに適用されるため、指定された目標を達成できないアクセス許可。例:
  - 関連するキーへのアクセス`s3:PutObject`許可のない、必須の KMS 暗号化を持つ S3 バケットへのアクセス`KMS:Encrypt`許可のリクエスト。
  - アカウントに存在しないリソースに関連するアクセス許可。
  - RFCs の説明がリクエストと一致しないように思われる IAM RFC。

「デプロイ」 RFC エラー

AMS "Deployment" カテゴリ変更タイプ (CTs) を使用すると、AMS がサポートするさまざまなリソースをアカウントに追加することをリクエストできます。

リソースを作成するほとんどの AMS CTs は、 CloudFormation テンプレートに基づいています。お客様は、 CloudFormation コンソールを使用して CloudFormation 、スタックの説明に基づいてスタックを表すスタックをすばやく特定 CloudFormationできます。失敗したスタックは DELETE_COMPLETE 状態である可能性があります。 CloudFormation スタックを特定すると、イベントには作成に失敗した特定のリソースとその理由が表示されます。

CloudFormation ドキュメントを使用したトラブルシューティング

ほとんどの AMS プロビジョニング RFCs は CloudFormation テンプレートを使用しており、そのドキュメントはトラブルシューティングに役立ちます。その CloudFormation テンプレートのドキュメントを参照してください。

- アプリケーションロードバランサーの作成の失敗: AWS::ElasticLoadBalancingV2::LoadBalancer (Application Load Balancer)
- Auto Scaling グループの作成: AWS::AutoScaling::AutoScalingGroup (Auto Scaling グループ)
- memcached キャッシュの作成: AWS::ElastiCache::CacheCluster (キャッシュクラスター)
- Redis キャッシュの作成: AWS::ElastiCache::CacheCluster (キャッシュクラスター)

- DNS ホストゾーンの作成 (DNS プライベート/パブリックの作成で使用): AWS::Route53::HostedZone (R53 ホストゾーン)
- DNS レコードセットの作成 (DNS プライベート/パブリックの作成で使用): AWS::Route53::RecordSet (リソースレコードセット)
- EC2 スタックの作成: AWS::EC2::Instance (Elastic Compute Cloud)
- Elastic File System (EFS): AWS::EFS::FileSystem (Elastic File System)
- ロードバランサーの作成: AWS::ElasticLoadBalancing::LoadBalancer (Elastic Load Balancer)
- RDS DB の作成: AWS::RDS::DBInstance (リレーショナルデータベース)
- Amazon S3 の作成: AWS::S3::Bucket (Simple Storage Service)
- キューの作成: AWS::SQS::Queue (簡易キューサービス)

RFC AMI エラーの作成 AMIs

Amazon マシンイメージ (AMI) は、ソフトウェア構成 (オペレーティングシステム、アプリケーションサーバー、アプリケーションなど) を記録したテンプレートです。AMI から、クラウドで仮想サーバーとして実行される AMI のコピーであるインスタンスを起動します。AMIs は非常に有用であり、EC2 インスタンスまたは Auto Scaling グループの作成に必要ですが、いくつかの要件に従う必要があります。

- RFC を成功させるには、 に指定するインスタンスが停止状態`Ec2InstanceId`である必要があります。ASG は停止したインスタンスを終了するため、このパラメータに Auto Scaling グループ (ASG) インスタンスを使用しないでください。
- AMS Amazon マシンイメージ (AMI) を作成するには、AMS インスタンスから始める必要があります。インスタンスを使用して AMI を作成する前に、インスタンスが停止され、そのドメインから切断されていることを確認することで、インスタンスを準備する必要があります。詳細については、「Sysprep を使用して標準 Amazon マシンイメージを作成する」を参照してください。
- 新しい AMI に指定する名前は、アカウント内で一意である必要があります。そうしないと、RFC は失敗します。これを行う方法については、「AMI | Create」で説明されています。詳細については、「」および「AWS AMI Design」を参照してください。

> **Note**
>
> AMI 作成の準備の詳細については、「AMI | 作成」を参照してください。

EC2s または ASGs エラーを作成する RFCs

タイムアウトを伴う EC2 または ASG 障害の場合、AMS では、使用する AMI がカスタマイズされているかどうかを確認することをお勧めします。その場合は、このガイドに含まれている AMI 作成手順 (「AMI | 作成」を参照) を参照して、AMI が正しく作成されたことを確認してください。カスタム AMI を作成する際の一般的な間違いは、 ガイドの手順に従って Sysprep の名前を変更または呼び出すことではありません。

RDS エラーを作成する RFCs

Amazon Relational Database Service (RDS) の障害は、RDS の作成時にさまざまなエンジンを使用でき、各エンジンには独自の要件と制限があるため、さまざまな理由で発生する可能性があります。AMS RDS スタックを作成する前に、AWS RDS パラメータ値を慎重に確認してください。CreateDBInstance」を参照してください。

サイズのレコメンデーションなど、Amazon RDS 全般の詳細については、Amazon Relational Database Service ドキュメント」を参照してください。

Amazon S3s エラーを作成する RFCs

S3 ストレージバケットを作成する際の一般的なエラーの 1 つは、バケットに一意の名前を使用していないことです。以前に送信したものと同じ名前の S3 バケット Create CT を送信した場合、その BucketName に S3 バケットがすでに存在するため、失敗します。これは CloudFormation コンソールで詳しく説明され、スタックイベントにバケット名がすでに使用されていることが示されます。

RFC 検証エラーと実行エラー

RFC の失敗と関連するメッセージは、選択した RFC の AMS コンソール RFC の詳細ページの出力メッセージによって異なります。

- 検証失敗の理由は、ステータスフィールドでのみ使用できます。
- 実行失敗の理由は、実行出力およびステータスフィールドで使用できます。

RFC エラーメッセージ

リストされた変更タイプ (CTs) で次のエラーが発生した場合は、これらのソリューションを使用して問題の原因を見つけて修正できます。

```
{"errorMessage":"An error has occurred during RFC execution. We are
investigating the issue.","errorType":"InternalError"}
```

次のトラブルシューティングオプションを参照してさらにサポートが必要な場合は、RFC 通信を介して AMS をエンゲージするか、サービスリクエストを作成します。詳細については、「RFC の通信と添付ファイル (コンソール)」および「AMS でのサービスリクエストの作成」を参照してください。

ワークロード取り込み (WIGS) エラー

> **Note**
>
> Windows と Linux の両方の検証ツールは、オンプレミスサーバーと AWS の EC2 インスタンスに直接ダウンロードして実行できます。これらは、「AMS Advanced Application Developer's Guide Migrating workloads: Linux pre-ingestion validation」と「Migrating workloads: Windows pre-ingestion validation」で確認できます。

- EC2 インスタンスがターゲット AMS アカウントに存在することを確認します。例えば、AMS 以外のアカウントから AMS アカウントに AMI を共有している場合は、ワークロード取り込み RFC を送信する前に、共有 AMI を使用して AMS アカウントに EC2 インスタンスを作成する必要があります。
- インスタンスにアタッチされたセキュリティグループで送信トラフィックが許可されているかどうかを確認します。SSM エージェントはパブリックエンドポイントに接続できる必要があります。
- インスタンスに SSM エージェントに接続するための適切なアクセス許可があるかどうかを確認します。これらのアクセス許可には が付属`customer-mc-ec2-instance-profile`しています。これは EC2 コンソールで確認できます。

EC2 インスタンススタック停止エラー

- インスタンスが既に停止状態か終了状態かを確認します。
- EC2 インスタンスがオンラインであり、`InternalError`エラーが表示された場合は、AMS が調査するためのサービスリクエストを送信します。
- 変更タイプ Management | Advanced stack components | EC2 instance stack | Stop ct-3mvt2zkyveqj を使用して Auto Scaling グループ (ASG) インスタンスを停止することはできません。ASG インスタンスを停止する必要がある場合は、サービスリクエストを送信します。

EC2 インスタンススタックの作成エラー

メッセージは CloudFormation からの`InternalError`ものです。CREATION_FAILED ステータスの理由です。CloudWatch スタックイベントでは、以下の手順に従ってスタックの障害に関する詳細を確認できます。

- AWS マネジメントコンソールでは、スタックの作成、更新、削除中にスタックイベントのリストを表示できます。このリストから失敗イベントを探して、そのイベントのステータスの理由を確認します。

  ステータスの理由には、問題を理解するのに役立つ AWS CloudFormation または特定のサービスからのエラーメッセージが含まれている場合があります。
- スタックイベントの表示の詳細については、「AWS マネジメントコンソールでの AWS CloudFormation スタックデータとリソースの表示」を参照してください。

EC2 インスタンスボリュームの復元エラー

EC2 インスタンスボリュームの復元が失敗すると、AMS は内部トラブルシューティング RFC を作成します。これは、EC2 インスタンスボリュームの復元がディザスタリカバリ (DR) の重要な部分であり、AMS によってこの内部トラブルシューティング RFC が自動的に作成されるためです。

内部トラブルシューティング RFC が作成されると、バナーが表示され、RFC へのリンクが表示されます。この内部トラブルシューティング RFC は、RFC の障害をより詳細に可視化し、同じエラーにつながる再試行 RFCs を送信したり、この障害について AMS に手動で連絡したりするのではなく、変更を追跡し、障害が AMS によって処理されていることを知ることができます。これにより、AMS Operators がリクエストを待つ代わりに RFC 障害にプロアクティブに取り組むため、変更のtime-to-recovery (TTR) メトリクスも短縮されます。

RFC のヘルプを取得する方法

AMS に連絡して、障害の根本原因を特定できます。AMS の営業時間は、1 日 24 時間、1 週間 7 日、1 年 365 日です。

AMS には、サポートを依頼したり、サービスリクエストを行ったりするためのいくつかの手段が用意されています。

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

- マネージド環境に影響する AWS または AMS サービスのパフォーマンスの問題を報告するには、AMS コンソールを使用してインシデントレポートを送信します。詳細については、「インシデントの報告」を参照してください。AMS インシデント管理の一般的な情報については、「インシデント対応」を参照してください。
- お客様またはお客様のリソースやアプリケーションが AMS とどのように連携しているかに関する具体的な質問、またはインシデントのエスカレーションについては、以下のうち 1 つ以上を E メールで送信してください。
  1. まず、サービスリクエストまたはインシデントレポートのレスポンスに満足できない場合は、CSDM に E メールを送信してください: ams-csdm@amazon.com
  2. 次に、エスカレーションが必要な場合は、AMS Operations Manager に E メールを送信できます (CSDM はおそらくこれを行います): ams-opsmanager@amazon.com
  3. さらなるエスカレーションは、AMS Director: ams-director@amazon.com に行われます。
  4. 最後に、AMS VP にいつでもアクセスできます: ams-vp@amazon.com

AMS の直接変更モード

トピック

- 直接変更モードの開始方法
- セキュリティとコンプライアンス
- 直接変更モードでの変更管理
- Direct Change モードを使用したスタックの作成
- 直接変更モードのユースケース

AWS Managed Services (AMS) Direct Change Mode (DCM) は、リソースをプロビジョニングおよび更新するための AMS Advanced Plus および Premium アカウントへのネイティブ AWS アクセスを提供することで、AMS Advanced 変更管理を拡張します AWS 。DCM では、ネイティブ AWS API (コンソールまたは CLI/SDK) または AMS Advanced Change Management Request for Change (RFCs) を使用するオプションがあり、いずれの場合も、リソースと変更がモニタリング、パッチ、バックアップ、インシデント対応管理など、AMS によって完全にサポートされています。DCM を介してプロビジョニングされたリソースは、AMS サービスナレッジ管理システム (SKMS) に登録され、AMS マネージド Active Directory ドメイン (該当する場合) に結合され、AMS 管理エージェントを実行します。既存のツール (CloudFormation、 AWS SDK、CDK など) を使用して、AMS 管理の CloudFormation スタックを開発およびデプロイします。

> **Note**
>
> 直接変更モードでは、AMS 変更管理 RFCsは削除されません。DCM を使用して AMS RFCs にフルアクセスできます。

詳細については、Akash の動画をご覧ください (6:30)

直接変更モードの開始方法

まず前提条件を確認してから、対象となる AMS Advanced アカウントで変更リクエスト (RFC) を送信します。

1. DCM で使用するアカウントが要件を満たしていることを確認します。
   - アカウントは AMS Advanced Plus または Premium です。
   - アカウントで Service Catalog が有効になっていません。現在、DCM と Service Catalog の両方へのアカウントのオンボーディングはサポートされていません。Service Catalog に既にオンボーディングされているが DCM に関心がある場合は、クラウドサービスデリバリーマネージャー (CSDM) とニーズについて話し合ってください。Service Catalog から DCM に切り替える場合は、Service Catalog をオフボードして変更をリクエストします。AMS での Service Catalog の詳細については、「AMS と Service Catalog」を参照してください。
2. Management | Managed Account | Direct Change Mode | Enable change type (ct-3rd4781c2nnhp) を使用して、変更リクエスト (RFC) を送信します。チュートリアルの例については、「直接変更モード | 有効化」を参照してください。

   CT が処理されると、事前定義された IAM ロールAWSManagedServicesCloudFormationAdminRoleとAWSManagedServicesUpdateRoleが指定されたアカウントにプロビジョニングされます。
3. 内部フェデレーションプロセスを使用して DCM アクセスを必要とするユーザーに適切なロールを割り当てます。

> **Note**
>
> ロールを引き受けるには、任意の数の SAMLIdentityProviders、 AWS Services、IAM エンティティ (ロール、ユーザーなど) を指定できます。、SAMLIdentityProviderARNs、IAMEntityARNsまたは の少なくとも 1 つを指定

する必要がありますAWSServicePrincipals。詳細については、会社の IAM 部門または AMS クラウドアーキテクト (CA) にお問い合わせください。

直接変更モードの IAM ロールとポリシー

アカウントで直接変更モードが有効になっている場合、これらの新しい IAM エンティティがデプロイされます。

AWSManagedServicesCloudFormationAdminRole: このロールは、CloudFormation コンソールへのアクセス、CloudFormation スタックの作成と更新、ドリフトレポートの表示、CloudFormation ChangeSets の作成と実行を許可します。このロールへのアクセスは、SAML プロバイダーを通じて管理されます。

ロールAWSManagedServicesCloudFormationAdminRoleにデプロイおよびアタッチされる管理ポリシーは次のとおりです。

- AMS Advanced マルチアカウントランディングゾーン (MALZ) アプリケーションアカウント
  - AWSManagedServices_CloudFormationAdminPolicy1
  - AWSManagedServices_CloudFormationAdminPolicy2
    - このポリシーは、 に付与されたアクセス許可を表しますAWSManagedServicesCloudFormationAdminRole。このポリシーを使用して、アカウント内の既存のロールへのアクセスを許可し、そのロールがアカウント内の CloudFormation スタックを起動および更新できるようにします。これには、他の IAM エンティティが CloudFormation スタックを起動できるように、追加の AMS サービスコントロールポリシー (SCP) 更新が必要になる場合があります。
- AMS Advanced シングルアカウントランディングゾーン (SALZ) アカウント
  - AWSManagedServices_CloudFormationAdminPolicy1
  - AWSManagedServices_CloudFormationAdminPolicy2
  - cdk-legacy-mode-s3-access [インラインポリシー〕
  - AWS ReadOnlyAccess ポリシー

AWSManagedServicesUpdateRole: このロールは、ダウンストリーム AWS サービス APIs への制限付きアクセスを許可します。ロールは、変更および非変更 API オペレーションを提供する マネージドポリシーでデプロイされますが、一般的には、IAM、KMS、GuardDuty、VPC、AMS インフ

ラストラクチャリソースや設定などの特定のサービスに対して変更オペレーション (Create/Delete/PUT など) を制限します。このロールへのアクセスは、SAML プロバイダーを通じて管理されます。

ロールAWSManagedServicesUpdateRoleにデプロイおよびアタッチされる管理ポリシーは次のとおりです。

- AMS Advanced マルチアカウントランディングゾーンアプリケーションアカウント
  - AWSManagedServicesUpdateBasePolicy
  - AWSManagedServicesUpdateDenyPolicy
  - AWSManagedServicesUpdateDenyProvisioningPolicy
  - AWSManagedServicesUpdateEC2AndRDSPolicy
  - AWSManagedServicesUpdateDenyActionsOnAMSInfraPolicy
- AMS Advanced シングルアカウントランディングゾーンアカウント
  - AWSManagedServicesUpdateBasePolicy
  - AWSManagedServicesUpdateDenyProvisioningPolicy
  - AWSManagedServicesUpdateEC2AndRDSPolicy
  - AWSManagedServicesUpdateDenyActionsOnAMSInfraPolicy1
  - AWSManagedServicesUpdateDenyActionsOnAMSInfraPolicy2

これらに加えて、 マネージドポリシーAWSManagedServicesUpdateRoleロールには AWS マネージドポリシーもアViewOnlyAccessタッチされています。

セキュリティとコンプライアンス

セキュリティとコンプライアンスは、AMS Advanced とお客様との間の責任共有です。AMS Advanced Direct Change モードは、この責任共有を変更しません。

直接変更モードのセキュリティ

AMS Advanced は、規範的なランディングゾーン、変更管理システム、アクセス管理で追加の値を提供します。Direct Change モードを使用する場合、この責任モデルは変更されません。ただし、追加のリスクに注意する必要があります。

Direct Change Mode の「Update」ロール (「」を参照直接変更モードの IAM ロールとポリシー) は、エンティティがアクセスできるようにする昇格されたアクセス許可を提供し、アカウント内の AMS がサポートするサービスのインフラストラクチャリソースを変更します。アクセス許可が引き上げられると、リソース、サービス、アクションに応じてさまざまなリスクが存在します。特に、監

視、ミス、または内部プロセスとコントロールフレームワークへの準拠の欠如が原因で誤った変更が行われた状況では、リスクが異なります。

AMS 技術標準に従って、以下のリスクが特定され、次のようにレコメンデーションが行われます。AMS 技術標準の詳細については、「」を参照してください AWS Artifact。アクセスするには AWS Artifact、CSDM に連絡して手順を確認するか、「 の開始方法 AWS Artifact」を参照してください。

AMS-STD-001: タグ付け

[Standards] (標準)	壊れていますか？	リスク	推奨事項
すべての AMS 所有リソースには、次のキーと値のペアが必要です 上記のタグ以外のすべての AMS 所有タグには、upper/lower/mixMC*の AMS*や などのプレフィックスが必要です。	はい。CloudFormation、CloudTrail、EFS、OpenSearch、CloudWatch Logs、SQS、SSM、タグ付け API のブレーク - これらのサービスは AMS 名前空間のタグ付けを制限するaws:TagsKey 条件をサポートしていないため。 次の表 AMS-STD-003 の標準では、AppId、Environment、AppName は変更できますが、AMS 所有のリソースは変更できません。IAM アクセス許可では達成できません。	AMS リソースのタグ付けが正しくないと、リソースのレポート、アラート、パッチ適用オペレーションに AMS 側で悪影響が及ぶ可能性があります。	AMS チーム以外のすべてのユーザーの AMS のデフォルトのタグ付け要件を変更するには、アクセスを復元する必要があります。
AMS 所有スタックのタグは、変更リク工	はい。CloudFormation は、AMS		

[Standards] (標準)	壊れていますか？	リスク	推奨事項
ストに基づいて削除しないでください。	名前空間のタグを制限するaws:TagsKey 条件をサポートしていません。		
次の表 AMS-AMS-STD-002 タグの命名規則を使用することは許可されていません。	はい。CloudFormation、CloudTrail、Amazon Elastic File System (EFS)、OpenSearch、CloudWatch Logs、Amazon Simple Queue Service (SQS)、Amazon EC2 Systems Manager (SSM)、Tagging API のブレーク。これらのサービスは、AMS 名前空間のタグ付けを制限するaws:TagsKey 条件をサポートしていません。		

AMS-STD-002: Identity and Access Management (IAM)

[Standards] (標準)	壊れていますか？	リスク	推奨事項
4.7 変更管理プロセス (RFC) をバイパスするアクションは、インスタンスの起動または停止、S3 バケットまたは RDS	はい。セルフサービスアクションの目的は、AMS RFC システムをバイパスしてアクションを実行することです。	セキュアアクセスモデルは AMS の主要な技術的側面であり、コンソールまたはプログラムによるアクセス用の IAM	IAM ユーザーには、最小特権とneed-to-knowことに基づいて、時間制限があり、アクセス許可が

[Standards] (標準)	壊れていますか？	リスク	推奨事項
インスタンスの作成などを許可してはいけません。デベロッパーモードアカウントとセルフサービスプロビジョンドモードサービス (SSPS) は、アクションが割り当てられたロールの境界内で実行される限り、除外されます。		ユーザーがこのアクセスコントロールを回避します。IAM ユーザーのアクセスは、AMS 変更管理によってモニタリングされません。アクセスは CloudTrail にのみ記録されます。	付与されている必要があります。

AMS-STD-003: ネットワークセキュリティ

[Standards] (標準)	壊れていますか？	リスク	推奨事項
S2。EC2 インスタンスの Elastic IP は、正式なリスク承諾契約、または内部チームによる有効なユースケースでのみ使用する必要があります。	はい。セルフサービスアクションを使用すると、Elastic IP アドレス (EIP) の関連付けと関連付け解除を行うことができます。	Elastic IP をインスタンスに追加すると、その IP はインターネットに公開されます。これにより、情報開示や不正なアクティビティのリスクが高まります。	セキュリティグループを介してそのインスタンスへの不要なトラフィックをブロックし、セキュリティグループがインスタンスにアタッチされていることを確認し、ビジネス上の理由で必要な場合にのみトラフィックを許可するようにします。
S14。同じ顧客に属するアカウント間の VPC ピアリングと工	はい。IAM ポリシーでは実行できません。	AMS アカウントから出るトラフィックは、アカウントの境	所有している AMS アカウントとのみピア接続することをお勧めします。ユース

[Standards] (標準)	壊れていますか？	リスク	推奨事項
ンドポイント接続を許可できます。		界から出るとモニタリングされません。	ケースでこれが必要な場合は、セキュリティグループとルートテーブルを使用して、関連する接続を介して出力できるトラフィック範囲、リソース、タイプを制限します。
AMS ベース AMIs は、AMS が管理するアカウントとアンマネージドアカウントの間で共有できます。ただし、それらが同じ AWS 組織によって所有されていることを確認できます。		AMIs機密データが含まれており、意図しないアカウントに公開される可能性があります。	組織が所有するアカウントのみと AMIs を共有するか、組織外で共有する前にユースケースとアカウント情報を検証します。

AMS-STD-007: ログ記録

[Standards] (標準)	壊れていますか？	リスク	推奨事項
19. ログは、ある AMS アカウントから同じ顧客の別の AMS アカウントに転送できます。	はい。同じ組織内の顧客アカウントの検証による顧客ログの潜在的なセキュリティ低下は、IAM ポリシーでは達成できません。	ログには機密データが含まれており、意図しないアカウントに公開される可能性があります。	AWS 組織によって管理されているアカウントのみとログを共有するか、組織外と共有する前にユースケースとアカウント情報を検証します。これは複数の方法で検証できます。クラ
20。ログは、AMS 以外のアカウントが同じ AMS 顧客によって所有されている (同じ			

[Standards] (標準)	壊れていますか？	リスク	推奨事項
AWS Organizations アカウントにあることを確認するか、E メールドメインを顧客の会社名と PAYER リンクアカウントと照合する) 場合にのみ、内部ツールを使用して AMS から非 AMS アカウントに転送できます。			ウドサービスデリバリーマネージャー (CSDM) に確認してください。

内部認可および認証チームと協力して、それに応じて Direct Change モードロールへのアクセス許可を制御します。

直接変更モードのコンプライアンス

Direct Change モードは、本番ワークロードと非本番ワークロードの両方と互換性があります。コンプライアンス標準 (PHI、HIPAA、PCI など) を確実に順守し、Direct Change モードの使用が内部管理フレームワークと標準に準拠していることを確認するのはお客様の責任です。

直接変更モードでの変更管理

変更管理は、AMS Advanced が変更リクエストを実装するために使用するプロセスです。変更リクエスト (RFC) は、ユーザーまたは AMS Advanced インターフェイスを介して AMS Advanced によって作成されたリクエストで、マネージド環境に変更を加え、特定のオペレーションの AMS Advanced 変更タイプ (CT) ID が含まれます。詳細については、「変更管理」を参照してください。

> **Note**
>
> 直接変更モードでは、AMS 変更管理 RFCs は削除されません。DCM を使用して AMS RFCs にフルアクセスできます。

AMS Direct Change Mode (DCM) は、リソースをプロビジョニングおよび更新するための AMS Advanced Plus および Premium アカウントへのネイティブ AWS アクセスを提供することで、AMS

Advanced 変更管理を拡張します AWS 。IAM ロールを通じて直接変更モードのアクセス許可を付与されたユーザーは、ネイティブ AWS API アクセスを使用して、AMS Advanced アカウントのリソースをプロビジョニングおよび変更できます。ユーザーは、同じ IAM ロールを使用して AMS Advanced 変更管理 RFCs を引き続き使用できます。どちらの場合も、リソースとその変更は、モニタリング、パッチ、バックアップ、インシデント対応管理など、AMS によって完全にサポートされています。これらのアカウントで適切なロールを持たないユーザーは、AMS Advanced 変更管理 RFC プロセスを使用して変更を行う必要があります。

変更管理のユースケース

セキュリティ上の理由から、AMS Advanced の一部の変更は、変更管理の変更リクエスト (RFC) プロセスを通じてのみ行うことができます。`AWSManagedServicesCloudFormationAdminRole` は、CloudFormation (CFN) を通じて実行されるアクションに制限されます。DCM を使用してスタックを作成する方法の詳細については、「直接変更モードを使用したスタックの作成」を参照してください。`AWSManagedServicesUpdateRole` は、次のアクションに制限されています。

管理 | 管理アカウント | 直接変更モード | 有効化 (ct-3rd4781c2nnhp) 変更タイプを含む各変更タイプのチュートリアルについては、「AMS Advanced Change Type Reference Change Types by Classification」セクションの「Additional Information」セクションを参照してください。

サービス	アクション
AWS Key Management Service (AWS KMS)	更新
AWS Certificate Manager	作成
AWS Identity and Access Management (IAM)	いずれか
Site-to-Site VPN	すべて
AMS リソーススケジューラ	
AWS Backup	バックアッププランを作成する
AMS ワークロード取り込み (WIGs)	いずれか
AMS Egress Filtering (マネージドパロアルト)	
AMS Advanced MALZ アカウントの変更	

サービス	アクション
Amazon GuardDuty	
AMS アドバンストスタックアクセス	いずれか
Amazon Elastic Block Store (EBS) ボリューム	削除
Amazon Elastic Block Store (EBS) のデフォルトの暗号化	デフォルトの暗号化を有効にする
Amazon Elastic Compute Cloud (Amazon EC2)	ホスト名を変更する
Amazon マシンイメージ (AMI)	削除、共有
Amazon EC2 セキュリティグループ	
AMS Advanced SSPS	いずれか
AWS Managed Microsoft AD	
AMS Advanced デベロッパーモード	
Amazon Simple Storage Service (Amazon S3)	S3 バケットポリシーを作成する
AWS Systems Manager	作成

Direct Change モードを使用したスタックの作成

を使用して CloudFormation でスタックを起動する場合`AWSManagedServicesCloudFormationAdminRole`、スタックを AMS で管理するには、次の 2 つの要件があります。

- テンプレートには が含まれている必要があります`AmsStackTransform`。
- スタック名はプレフィックスで始まり、その後に 17 文字の英数字文字列が`stack-`続く必要があります。

> **Note**
>
> を正常に使用するにはAmsStackTransform、 CloudFormation (CFN) がスタックを作成または更新するために、スタックテンプレートに CAPABILITY_AUTO_EXPAND機能が含まれていることを確認する必要があります。これを行うには、 を create-stack リクエストCAPABILITY_AUTO_EXPANDの一部として渡します。がテンプレートに含まれているときにこの機能が確認されない場合、CFN AmsStackTransformはリクエストを拒否します。CFN コンソールでは、テンプレートに 変換がある場合にこの機能を渡すことができますが、APIs を介して CFN とやり取りしている場合、この機能が失われる可能性があります。
> この機能は、次の CFN API コールを使用するたびに渡す必要があります。
>
> - CreateChangeSet
> - CreateStack
> - UpdateStack

DCM を使用してスタックを作成または更新する場合、CFN Ingest および Stack Update CTsCloudFormation 「Ingest Guidelines」、「Best Practices」、および「Limitations」を参照してください。ただし、AMS のデフォルトのセキュリティグループ (SGs) は、Auto Scaling グループ (ASGs) のスタンドアロン EC2 インスタンスまたは EC2 インスタンスにはアタッチされません。スタンドアロン EC2 インスタンスまたは ASGs を使用して CloudFormation テンプレートを作成する場合、デフォルトの SGs をアタッチできます。

> **Note**
>
> IAM ロールを で作成および管理できるようになりましたAWSManagedServicesCloudFormationAdminRole。

AMS デフォルト SGs には、インスタンスが正常に起動し、後で AMS オペレーションとユーザーによって SSH または RDP を介してアクセスできるようにする進入および退出ルールがあります。で AMS のデフォルトのセキュリティグループが許容されすぎることがわかった場合は、より制限の厳しいルールを使用して独自の SGs を作成し、インスタンスにアタッチできます。ただし、インシデント発生時にユーザーと AMS オペレーションがインスタンスにアクセスできる場合に限ります。

AMS のデフォルトのセキュリティグループは次のとおりです。

- SentinelDefaultSecurityGroupPrivateOnly: この SSM パラメータを使用して CFN テンプレートでアクセスできます `/ams/${VpcId}/SentinelDefaultSecurityGroupPrivateOnly`
- SentinelDefaultSecurityGroupPrivateOnlyEgressAll: この SSM パラメータを使用して CFN テンプレートでアクセスできます `/ams/${VpcId}/SentinelDefaultSecurityGroupPrivateOnlyEgressAll`

AMS 変換

CloudFormation テンプレートに`Transform`ステートメントを追加します。これにより、起動時にスタックを検証して AMS に登録する CloudFormation マクロが追加されます。

JSON の例

```
"Transform": {
    "Name": "AmsStackTransform",
    "Parameters": {
      "StackId": {"Ref" : "AWS::StackId"}
    }
  }
```

YAML の例

```
Transform:
  Name: AmsStackTransform
  Parameters:
    StackId: !Ref 'AWS::StackId'
```

また、既存のスタックのテンプレートを更新するときに `Transform`ステートメントを追加します。

JSON の例

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description" : "Create an SNS Topic",
    "Transform": {
      "Name": "AmsStackTransform",
      "Parameters": {
        "StackId": {"Ref" : "AWS::StackId"}
     }
  },
```

```
  "Parameters": {
    "TopicName": {
      "Type": "String",
      "Default": "HelloWorldTopic"
    }
  },
  "Resources": {
    "SnsTopic": {
      "Type": "AWS::SNS::Topic",
      "Properties": {
        "TopicName": {"Ref": "TopicName"}
      }
    }
  }
}
```

YAML の例

```
AWSTemplateFormatVersion: '2010-09-09'
Description: Create an SNS Topic
Transform:
  Name: AmsStackTransform
  Parameters:
    StackId: !Ref 'AWS::StackId'
Parameters:
  TopicName:
    Type: String
    Default: HelloWorldTopic
Resources:
  SnsTopic:
    Type: AWS::SNS::Topic
    Properties:
      TopicName: !Ref TopicName
```

スタック名

スタック名はプレフィックスで始まり、その後に 17 文字の英数字文字列がstack-続く必要があります。これは、AMS スタック IDs。

互換性のあるスタック IDs を生成する方法の例を次に示します。

Bash:

```
echo "stack-$(env LC_CTYPE=C tr -dc 'a-z0-9' < /dev/urandom | head -c 17)"
```

Python:

```
import string
import random

'stack-' + ''.join(random.choices(string.ascii_lowercase + string.digits, k=17))
```

Powershell:

```
"stack-" + ( -join ((0x30..0x39) + ( 0x61..0x7A) | Get-Random -Count 17  | %
 {[char]$_}) )
```

直接変更モードのユースケース

以下は、直接変更モードのユースケースです。

によるリソースのプロビジョニングと管理 CloudFormation

- 既存の CloudFormation ベースのツールとプロセスを統合します。

継続的なリソース管理と更新

- リスクの低い小さなアトミック変更。
- 手動または自動 RFC を通じて実行される変更。
- ネイティブ AWS API アクセスを必要とするツール。
- DCM ロールは、移行段階にある場合に使用できます。移行チームは、DCM のアクセス許可を活用してスタックを作成または変更します。
- DCM ロールは、CI/CD パイプラインで新しい AMIs の構築、Amazon ECS タスクの作成などに使用できます。

AMS Advanced Developer モード

トピック

- AMS Advanced Developer モードの開始方法

- デベロッパーモードでのセキュリティとコンプライアンス
- デベロッパーモードでの変更管理
- AMS Developer モードでのインフラストラクチャのプロビジョニング
- AMS デベロッパーモードでの検出コントロール
- AMS Developer モードでのログ記録、モニタリング、イベント管理
- AMS デベロッパーモードでのインシデント管理
- AMS デベロッパーモードでのパッチ管理
- AMS デベロッパーモードでの継続管理
- AMS Developer モードでのセキュリティとアクセスの管理

AWS Managed Services (AMS) デベロッパーモードでは、AMS Advanced Plus および Premium アカウントの昇格されたアクセス許可を使用して、AMS Advanced 変更管理プロセス外の AWS リソースをプロビジョニングおよび更新します。AMS Advanced Developer モードは、AMS Advanced Virtual Private Cloud (VPC) 内のネイティブ AWS API コールを活用して、マネージド環境でインフラストラクチャとアプリケーションを設計および実装できるようにします。

デベロッパーモードが有効になっているアカウントを使用する場合、AMS Advanced 変更管理プロセスまたは AMS Amazon マシンイメージ (AMI) を使用してプロビジョニングされたリソースには、継続性管理、パッチ管理、変更管理が提供されます。ただし、これらの AMS 管理機能は、ネイティブ AWS APIs を介してプロビジョニングされたリソースには提供されません。

AMS Advanced 変更管理プロセス外でプロビジョニングされるインフラストラクチャリソースをモニタリングする責任があります。デベロッパーモードは、本番ワークロードと非本番ワークロードの両方と互換性があります。アクセス許可が引き上げられると、内部管理を確実に順守する責任が増大します。

> **Important**
>
> デベロッパーモードを使用して作成したリソースは、AMS Advanced 変更管理プロセスを使用して作成された場合にのみ、AMS Advanced によって管理できます。

デベロッパーモードは、使用できる AMS Advanced モードの 1 つです。詳細については、「モードの概要」を参照してください。

AMS Advanced Developer モードの開始方法

AMS Advanced Developer モードを使用するさまざまな AMS Advanced アカウントと、Developer モードを正常に実装する方法について説明します。

トピック

- AMS デベロッパーモードを開始する前に
- AMS デベロッパーモードの前提条件
- AMS Advanced Developer モードを実装する方法
- AMS Advanced Developer モードのアクセス許可

AMS デベロッパーモードを開始する前に

デベロッパーモードを実装する前に、知っておくべきことがいくつかあります。

AMS Advanced は、変更リクエスト (RFCs) を通じて AMS Advanced 変更管理プロセス外で作成された DevMode アカウントの既存のスタックまたはリソースを管理することはできません。ただし、アカウントが DevMode にある間、AMS Advanced は AMS Advanced 変更管理プロセスを通じてプロビジョニングされたリソースを RFCs。

DevMode アカウントから始めて、後で AMS Advanced が管理するアプリケーションアカウントに隠すことはできません。

AMS デベロッパーモードの前提条件

デベロッパーモードを実装するための前提条件は次のとおりです。

- 少なくとも 1 つのオンボードされた AMS Advanced Plus または Premium アカウントを持つ AMS Advanced のお客様である必要があります。
- 使用するアカウントは、AMS Advanced Plus または Premium アカウントである必要があります。
- マルチアカウントランディングゾーン (MALZ): `AWSManagedServicesDevelopmentRole`事前定義された AWS Identity and Access Management (IAM) ロールを使用する必要があります。このロールをリクエストします。次のセクションでは、デベロッパーモードのアクセス許可を取得する方法について説明します。
- 単一アカウントランディングゾーン (SALZ): `customer_developer_role`事前定義された AWS Identity and Access Management (IAM) ロールを使用する必要があります。このロールをリクエス

トします。次のセクションでは、デベロッパーモードのアクセス許可を取得する方法について説明します。

AMS Advanced Developer モードを実装する方法

デベロッパーモードを実装するには、対象の AMS Advanced アカウントを事前定義された IAM ロールでプロビジョニングするようにリクエストします。

- MALZ: `AWSManagedServicesDevelopmentRole`
- SALZ: `customer_developer_role`

次に、フェデレーティッドネットワーク内の関連するユーザーにロールを割り当てます。

デベロッパーモードを使用すると、AMS Advanced マネージドリソースの AMS Advanced 変更管理と、カスタマーが管理するリソースのカスタマーマネージドロールフェデレーションの 2 つの変更ベクトルが作成されるため、AMS Advanced では、デベロッパーモードの使用が内部コントロールフレームワークと標準に準拠していることを確認することをお勧めします。AMS Advanced プロセスは宣言に準拠し続けますが、顧客プロセスとコントロールフレームワークを更新する必要がある場合があります。

AMS Advanced アカウントにデベロッパーモードを実装するには

1. デベロッパーモードで使用するアカウントが、「」に記載されている要件を満たしていることを確認しますAMS デベロッパーモードの前提条件。
2. 変更タイプ (CT) 管理 | マネージドアカウント | デベロッパーモード | 有効化 (レビューが必要) を使用して、変更リクエスト (RFC) を送信します。この CT の使用方法の例については、「デベロッパーモード | 有効 (レビューが必要)」を参照してください。

   CT が処理されると、事前定義された IAM ロール (`AWSManagedServicesDevelopmentRole`MALZ の場合は 、SALZ `customer_developer_role`の場合は) がリクエストされたアカウントにプロビジョニングされます。
3. 内部フェデレーションプロセスを使用して、開発者モードアクセスを必要とするユーザーに適切なロールを割り当てます。

   AMS Advanced では、リソースの望ましくないまたは未承認のプロビジョニングや変更を防ぐためにアクセスを制限することをお勧めします。

AMS Advanced Developer モードのアクセス許可

事前定義されたロール (AWSManagedServicesDevelopmentRoleMALZ の場合は MALZ、SALZ customer_developer_roleの場合は) は、AMS Advanced によって運用されている共有サービスコンポーネント (管理ホスト、ドメインコントローラー、Trend Micro EPS、踏み台、サポートされていない AWS サービスなど) へのアクセスを制限しながら、IAM ロールを含む AMS Advanced VPC 内にアプリケーションインフラストラクチャリソースを作成するアクセス許可を付与します。このロールは、 AWS のサービス Amazon GuardDuty、 AWS Organizations、 AWS Directory Service APIs、AMS Advanced ログへのアクセスも制限します。

ロールでは追加の IAM ロールを作成できますが、デベロッパーモードアクセスに含まれるのと同じアクセス許可の境界は、 によって作成されたすべての IAM ロールに適用されますAWSManagedServicesDevelopmentRole。

デベロッパーモードでのセキュリティとコンプライアンス

セキュリティとコンプライアンスは、AMS Advanced とお客様との間の責任共有です。AMS アドバンストデベロッパーモードは、変更管理プロセス外でプロビジョニングされたリソース、または変更管理を通じてプロビジョニングされたリソースに対して、デベロッパーモードのアクセス許可で更新されたリソースに対する責任共有を移行します。責任共有の詳細については、AWS Managed Services」を参照してください。

注意：

- DevMode を使用すると、ユーザーと承認されたチームは、AMS セキュリティの中核となるdeny-by-defaultの原則を回避できます。利点、セルフサービス、AMS の待機時間の短縮は欠点と照らし合わせて検討する必要があります。セキュリティチームの知識がなくても、誰でも予期しない破壊的なアクションを実行できます。開発モードと直接変更モードを有効にする自動変更タイプが公開され、組織内の承認されたユーザーがこれらの CTsを実行してこれらのモードを有効にすることができます。
- ユーザーベースからの CT 実行のアクセス許可を管理する責任があります。
- AMS は CT 実行アクセス許可を管理しません

推奨事項:

- 保護
  - お客様は、アクセス許可によってこの CT へのアクセスを防ぐことができます。「IAM ロールポリシーステートメントによるアクセス許可の制限」を参照してください。

  - ITSM システムなどのプロキシを実装してこの CT へのアクセスを防止する
  - 必要に応じてポリシーと動作を防止するサービスコントロールポリシー (SCPs「AMS Preventative and Detective Controls Library」を参照してください。
- 検出
  - これらの CTs の RFC をモニタリングし (開発者モード ct-1opjmhuddw194 と直接変更モードを有効にする、ct-3rd4781c2nnhp を有効にする) 、それに応じて応答します。
  - アカウントで IAM リソースの有無を確認および/または監査して、デベロッパーモードまたは直接変更モードがデプロイされているアカウントを特定します。
- 応答
  - 必要に応じてデベロッパーモードでアカウントを削除する

デベロッパーモードのセキュリティ

AMS Advanced は、規範的なランディングゾーン、変更管理システム、アクセス管理で追加の値を提供します。デベロッパーモードを使用する場合、AMS Advanced のセキュリティ値は、ベースライン AMS Advanced セキュリティ強化ネットワークを確立する標準 AMS Advanced アカウントと同じアカウント設定を使用して保持されます。ネットワークは、ロール (`AWSManagedServicesDevelopmentRole`MALZ の場合は MALZ、SALZ `customer_developer_role`の場合は) で強制されるアクセス許可の境界によって保護されます。これにより、ユーザーは、アカウントの設定時に確立されたパラメータ保護を破ることが制限されます。

たとえば、 ロールを持つユーザーは Amazon Route 53 にアクセスできますが、AMS Advanced の内部ホストゾーンは制限されています。によって作成された IAM ロールにも同じアクセス許可の境界が適用され`AWSManagedServicesDevelopmentRole`、アカウント`AWSManagedServicesDevelopmentRole`が AMS Advanced にオンボーディングされたときに確立されたパラメータ保護をユーザーが壊すことを制限するアクセス許可の境界が に強制されます。

デベロッパーモードでのコンプライアンス

デベロッパーモードは、本番ワークロードと非本番ワークロードの両方と互換性があります。コンプライアンス標準 (PHI、HIPAA、PCI など) を確実に順守し、デベロッパーモードの使用が内部管理フレームワークと標準に準拠していることを確認するのはお客様の責任です。

デベロッパーモードでの変更管理

変更管理は、AMS Advanced サービスが変更リクエストを実装するために使用するプロセスです。変更リクエスト (RFC) は、AMS Advanced インターフェイスを介してユーザーまたは AMS Advanced によって作成され、マネージド環境に変更を加えるリクエストであり、特定のオペレーションの変更タイプ (CT) ID が含まれます。詳細については、「変更管理モード」を参照してください。

開発者モードのアクセス許可が付与されている AMS Advanced アカウントでは、変更管理は適用されません。IAM ロール (`AWSManagedServicesDevelopmentRoleMALZ` の場合は 、SALZ `customer_developer_role`の場合は) でデベロッパーモードのアクセス許可を付与されたユーザーは、ネイティブ AWS API アクセスを使用して、AMS Advanced アカウントのリソースをプロビジョニングおよび変更できます。これらのアカウントで適切なロールを持たないユーザーは、AMS Advanced 変更管理プロセスを使用して変更を行う必要があります。

> **Important**
>
> デベロッパーモードを使用して作成したリソースは、AMS Advanced 変更管理プロセスを使用して作成された場合にのみ、AMS Advanced によって管理できます。AMS Advanced 変更管理プロセス外で作成されたリソースについて AMS Advanced に送信された変更のリクエストは、ユーザーが処理する必要があるため、AMS Advanced によって拒否されます。

セルフサービスプロビジョニングサービス API の制限

すべての AMS Advanced セルフプロビジョニングサービスは、 デベロッパーモードでサポートされています。セルフプロビジョニングサービスへのアクセスには、それぞれのユーザーガイドセクションで説明されている制限が適用されます。デベロッパーモードロールでセルフプロビジョニングサービスを使用できない場合は、デベロッパーモードの変更タイプを使用して更新されたロールをリクエストできます。

以下のサービスは、サービス APIs へのフルアクセスを提供しません。

デベロッパーモードで制限されるセルフプロビジョニングサービス

サービス	注意
Amazon API Gateway	を除くすべての Gateway APIsコールが許可されます`SetWebACL` 。

サービス	注意
Application Auto Scaling	スケーラブルターゲットの登録または登録解除、スケーリングポリシーの配置または削除のみが可能です。
AWS CloudFormation	というプレフィックスが付いた名前の CloudFormation スタックにアクセスまたは変更することはできませんmc-。
AWS CloudTrail	ams- および/または というプレフィックスが付いた名前の CloudTrail リソースにアクセスまたは変更することはできませんmc-。
Amazon Cognito (ユーザープール)	ソフトウェアトークンを関連付けることはできません。 ユーザープール、ユーザーインポートジョブ、リソースサーバー、または ID プロバイダーを作成することはできません。

サービス	注意
AWS Directory Service	Connect および WorkSpaces サービスでは、次の Directory Service アクションのみが必要です。他のすべての Directory Service アクションは、デベロッパーモードのアクセス許可境界ポリシーによって拒否されます。 • ds:AuthorizeApplication • ds:CreateAlias • ds:CreateIdentityPoolDirectory • ds:DeleteDirectory • ds:DescribeDirectories • ds:GetAuthorizedApplication Details • ds:ListAuthorizedApplications • ds:UnauthorizeApplication シングルアカウントランディングゾーンアカウントでは、境界ポリシーは、開発モードが有効なアカウントへのアクセスを維持するために AMS Advanced が使用する AMS Advanced マネージドディレクトリへのアクセスを明示的に拒否します。
Amazon Elastic Compute Cloud	、DhcpOptio ns 、Gateway、Subnet、VPCおよび の文字列を含む Amazon EC2 APIs にはアクセスできませんVPN。 、AMS、、ManagementHostASG および/または のプレフィックスが付いたタグを持つ Amazon EC2 mcリソースにアクセスまたは変更することはできませんsentinel。

サービス	注意
Amazon EC2 (レポート)	ビューアクセスのみが付与されます (変更できません) 。注: Amazon EC2 レポートは移動中です。レポートメニュー項目は Amazon EC2 コンソールのナビゲーションメニューから削除されます。削除された Amazon EC2 使用状況レポートを表示するには、 AWS Billing およびコスト管理コンソールを使用します。
AWS Identity and Access Management (IAM)	既存のアクセス許可の境界を削除したり、IAM ユーザーパスワードポリシーを変更したりすることはできません。 正しい IAM ロール (`AWSManagedServices DevelopmentRole` MALZ の場合は 、SALZ `customer_developer_role` の場合は) を使用しない限り、IAM リソースを作成または変更することはできません。 プレフィックスが `ams`、、`customer_deny_policy` 、および/または の IAM `mc`リソースを変更することはできませ`ん`sentinel。 新しい IAM リソース (ロール、ユーザー、またはグループ) を作成するときは、アクセス許可の境界 (MALZ: `AWSManagedServices DevelopmentRolePermissionsBoundary` 、SALZ: `ams-app-infra-permissions-boundary`) をアタッチする必要があります。
AWS Key Management Service (AWS KMS)	AMS Advanced マネージド KMS キーにアクセスまたは変更することはできません。
AWS Lambda	プレフィックスが の AWS Lambda 関数にアクセスまたは変更することはできません`AMS`。

サービス	注意
CloudWatch Logs	、mc、、lambdaおよび/または というプレフィックスが付いた名前の CloudWatch awsロググストリームにはアクセスできませんAMS。
Amazon Relational Database Service (Amazon RDS)	というプレフィックスが付いた名前の Amazon Relational Database Service (Amazon RDS) データベース (DBs) にアクセスまたは変更することはできません。 mc-
AWS Resource Groups	Get、、Listおよび Searchリソースグループ API アクションにのみアクセスできます。
Amazon Route 53	Route53 AMS Advanced が管理するリソースにアクセスまたは変更することはできません。
Amazon S3	、ams-*、、ms-aまたは というプレフィックスが付いた名前の Amazon S3 amsバケットにはアクセスできませんmc-a。
AWS Security Token Service	許可されるセキュリティトークンサービス API は のみですDecodeAuthorizationMessage 。
Amazon SNS	、AMS-、Energon-Topic または というプレフィックスが付いた名前の SNS トピックにはアクセスできませんMMS-Topic 。
AWS Systems Manager マネージャー (SSM)	ams、、mcまたは のプレフィックスが付いた SSM パラメータを変更することはできませんsvc。 ams または のプレフィックスが付いたタグを持つ Amazon EC2 インスタンスSendCommand に対して SSM API を使用することはできませんmc。

サービス	注意
AWS タグ付け	プレフィックスが の AWS タグ付け API アクションにのみアクセスできますGet。
AWS Lake Formation	次の AWS Lake Formation API アクションは拒否されます。 • lakeformation:DescribeResource • lakeformation:GetDataLakeSettings • lakeformation:DeregisterResource • lakeformation:RegisterResource • lakeformation:UpdateResource • lakeformation:PutDataLakeSettings
Amazon Elastic Inference	Elastic Inference API アクション のみを呼び出すことができますelastic-inference:Connect 。このアクセス許可は、 にアタッチcustomer_sagemaker_admin_policy されている に含まれていますcustomer_sagemaker_admin_role 。このアクションにより、Elastic Inference アクセラレーターにアクセスできます。
AWS Shield	このサービスの APIs またはコンソールにはアクセスできません。
Amazon Simple Workflow Service	このサービスの APIs またはコンソールにはアクセスできません。

AMS Developer モードでのインフラストラクチャのプロビジョニング

デベロッパーモードが有効になっているアカウントAWSManagedServicesDevelopmentRoleで、デベロッパーモード IAM ロール を持たないユーザーは、AMS Advanced AMIs を活用する AMS Advanced 変更管理プロセスに従う必要があります。正しいロール (MALZ: AWSManagedServicesDevelopmentRole、SALZ: customer_developer_role) を持つユーザーは、AMS Advanced 変更管理システムと AMS Advanced AMIs を使用できますが、必須ではありません。

> **Note**
>
> AMS Advanced ワークロードの取り込みによって処理されていない、または AMS Advanced アカウントで作成された AWS AMI には、AMS Advanced に必要な設定は含まれません。

AMS デベロッパーモードでの検出コントロール

このセクションは、機密性の高い AMS セキュリティ関連情報が含まれているため、編集されています。この情報は、AMS コンソールのドキュメントから入手できます。AWS Artifact にアクセスするには、CSDM に連絡して手順を確認するか、「AWS Artifact の開始方法」を参照してください。

AMS Developer モードでのログ記録、モニタリング、イベント管理

ログ記録、モニタリング、イベント管理は、AMS Advanced 変更管理プロセス外でプロビジョニングされたリソースや、変更管理を通じてプロビジョニングされ、デベロッパーモードのアクセス許可を使用してアカウントによって変更されたリソースでは使用できません。

AMS デベロッパーモードでのインシデント管理

インシデント対応時間に変更はありません。インシデント解決は、変更管理プロセス外でプロビジョニングされたリソース、または変更管理を通じてプロビジョニングされ、デベロッパーモードのアクセス許可を使用してアカウントによって変更されたリソースのベストエフォートです。

> **Note**
>
> AMS サービスレベルアグリーメント (SLA) は、AMS 変更管理システムの外部で作成または更新されたリソース (変更または RFCs のリクエスト) には適用されません。デベロッパー

モードが含まれるため、デベロッパーモードで更新または作成されたリソースは自動的に P3 に低下し、AMS サポートがベストエフォートです。

AMS デベロッパーモードでのパッチ管理

パッチ管理は、AMS Advanced 変更管理プロセス外でプロビジョニングされたリソース、または変更管理を通じてプロビジョニングされ、デベロッパーモードのアクセス許可を使用してアカウントによって変更されたリソースでは使用できません。パッチ適用時間：

- 重要なセキュリティ更新の場合: ベンダーによるリリースから 10 営業日以内に、変更管理によってプロビジョニングされ、デベロッパーモードのアクセス許可を使用してアカウントによって変更されたリソース。
- 重要な更新の場合: ベンダーによるリリースから 2 か月以内に、変更管理によってプロビジョニングされ、デベロッパーモードのアクセス許可を使用してアカウントによって変更されたリソース。

AMS デベロッパーモードでの継続管理

継続性管理は、AMS Advanced 変更管理プロセス外でプロビジョニングされたリソース、または変更管理を通じてプロビジョニングされ、デベロッパーモードのアクセス許可を使用してアカウントによって変更されたリソースでは使用できません。

環境復旧の開始時間は、AMS Advanced 変更管理プロセス外でプロビジョニングされたリソース、または変更管理を通じてプロビジョニングされ、デベロッパーモードのアクセス許可を使用してアカウントによって変更されたリソースの場合、最大 12 時間かかることがあります。

AMS Developer モードでのセキュリティとアクセスの管理

マルウェア対策保護は、AMS Advanced 変更管理プロセス外でプロビジョニングされたリソース、または変更管理を通じてプロビジョニングされ、デベロッパーモードのアクセス許可を使用してアカウントによって変更されたリソースに対するお客様の責任です。AMS Advanced 変更管理によってプロビジョニングされていない Amazon Elastic Compute Cloud (Amazon EC2) インスタンスへのアクセスは、フェデレーティッドアクセスを提供する代わりに、キーペアによって制御される場合があります。

AMS でのセルフサービスプロビジョニングモード

AWS Managed Services (AMS) セルフサービスプロビジョニング (SSP) モードは、AMS マネージドアカウントのネイティブ AWS サービスと API 機能へのフルアクセスを提供します。標準化、スコープダウン、 AWS Identity and Access Management ロールを通じてサービスにアクセスします。AMS はサービスリクエストとインシデント管理を提供します。アラート、モニタリング、ログ記録、パッチ適用、バックアップ、変更管理はお客様の責任となります。多くの場合、セルフサービスプロビジョニングサービス (SSPS) はセルフマネージド型またはサーバーレスであり、パッチ適用などの特定の運用タスクを管理する必要はありません。AMS ガードレールで定義された環境境界内でこれらのサービスを使用すると、プラットフォームのベースラインセキュリティを維持するために、IAM の変更 (サービスにリンクされたロール、サービスロール、クロスアカウントロール、ポリシーの更新を含む) を AMS オペレーションで承認する必要があります。テンプレートを活用して CloudFormation これらのサービスのデプロイを自動化できますが、これはすべての SSP サービスでサポートされているわけではありません。

> **Important**
>
> AWS Managed Services (AMS) アカウントで SSP モードを使用して、サービスにアクセスして採用します。ただし AWS 、記載されている制限があります。

AMS アカウントには、AMS 管理なしで AWS のサービス 使用できるものもあります。セルフサービスプロビジョニングモードサービス、つまり略して SSPS を AMS アカウントに追加する方法とそれぞれのよくある質問FAQs「」セクションで説明します。

セルフサービスプロビジョニングサービスはそのまま提供され、管理するのはお客様の責任です。AMS は、これらのサービスに関連付けられたリソースに対してアラート、モニタリング、ログ記録、またはパッチ適用を行いません。AMS には、AMS アカウントでサービスを安全に使用できる IAM ロールが用意されています。AMS SLAs は適用されません。

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

AMS での SSP モードの開始方法

セルフサービスプロビジョニングは、マルチアカウントランディングゾーン (MALZ) に使用できる AMS モードの 1 つです。詳細については、「モードの概要」を参照してください。

セルフサービスプロビジョニング機能を提供するために、AMS は、直接 AWS のサービス アクセスからの意図しない変更を制限するためのアクセス許可の境界を持つ昇格された IAM ロールを作成しました。ロールによってすべての変更が妨げられるわけではなく、内部コントロールとコンプライアンスポリシーに準拠し、使用されているすべての AWS のサービス が必須の証明書を満たしていることを確認する必要があります。これはセルフサービスプロビジョニングモードです。 AWS コンプライアンス要件の詳細については、AWS 「コンプライアンス」を参照してください。

マルチアカウントランディングゾーンアプリケーションアカウントにセルフサービスプロビジョニングサービスを追加するには、サービスの指示に従って、 Management | AWS service | Self-provisioned service | Add change type (CT) を使用します。

> **Note**
>
> AMS に追加のセルフサービスプロビジョニングサービスを提供するようにリクエストするには、サービスリクエストを提出します。

AMS SSP を使用して AMS アカウントに Amazon API Gateway をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon API Gateway 機能に直接アクセスします。Amazon API Gateway は、デベロッパーがあらゆる規模で API の公開、保守、モニタリング、セキュリティ保護を簡単に行えるフルマネージドサービスです。を使用すると AWS マネジメントコンソール 、アプリケーションが Amazon Elastic Compute Cloud (Amazon Amazon EC2) で実行されているワークロード、 で実行されているコード、ウェブアプリケーション、リアルタイム通信アプリケーションなど、バックエンドサービスからデータ、ビジネスロジック、機能にアクセスするためのフロントドアとして機能する AWS LambdaREST および WebSocket APIs を作成できます。

API Gateway は、トラフィック管理、認可とアクセスコントロール、モニタリング、API バージョン管理など、最大数十万の同時 API コールの受け入れと処理に関連するすべてのタスクを処理します。API Gateway には最低料金やスタートアップコストはありません。支払いは、受信した API コールと転送されたデータ量に対してのみ発生し、API Gateway 階層型料金モデルを使用

すると、API 使用量が拡大するにつれてコストを削減できます。詳細については、Amazon API Gateway」を参照してください。

よくある質問: AMS の API Gateway

Q: AMS アカウントの Amazon API Gateway へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) change type で RFC を送信して API Gateway へのアクセスをリクエストします。この RFC は、`customer_apigateway_author_role`および の IAM ロールをアカウントにプロビジョニングしますcustomer_apigateway_cloudwatch_role。アカウントでプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon API Gateway の使用にはどのような制限がありますか？

- API Gateway の設定は、AMS インフラストラクチャへの変更を防ぐために、 `MC-` `AMS-`または プレフィックスのないリソースに制限されます。
- `CREATE` Elastic Load Balancer の規制されていない作成を防ぐために、VPCLink の 権限は無効になっています。VPCLinksApplication Load Balancer | Create」を参照してください。

Q: AMS アカウントで Amazon API Gateway を使用するための前提条件または依存関係は何ですか？

デプロイする API Gateway のタイプによって異なります。スタンドアロンサービスでもかまいませんが、既存のサービス (Network Load Balancer など) へのアクセスをリクエストすることもできます。

AMS SSP を使用して AMS アカウントで Alexa for Business をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Alexa for Business 機能に直接アクセスします。Alexa for Business は、組織と従業員が Alexa を使用してより多くの作業を完了できるようにするサービスです。Alexa for Business を使用すると、Alexa をインテリジェントアシスタントとして使用して、会議室、デスク、自宅や外出先で既に使用している Alexa デバイスでも生産性を高めることができます。IT および施設マネージャーは、Alexa for Business を使用して、職場の既存の会議室の使用率を測定し、向上させることができます。

詳細については、Alexa for Business」を参照してください。

AWS Managed Servicesでの Alexa for Business に関するよくある質問

Q: AMS アカウントで Alexa for Business へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (レビューが必要) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_alexa_console_role`。`customer_alexa_device_setup_user` は、Alexa for Business が提供する Device Setup Tool にも作成されます。その後、この Device Setup Tool を使用してデバイスをセットアップできます。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Alexa for Business ゲートウェイを使用すると、Alexa for Business を Cisco Webex エンドポイントと Poly Group Series エンドポイントに接続して、音声で会議を制御できます。ゲートウェイソフトウェアは、オンプレミスのハードウェアで実行され、Alexa for Business から Cisco エンドポイントへの会議ディレクティブを安全にプロキシします。ゲートウェイは、Alexa for Business と通信するために 2 組の AWS 認証情報を必要とします。アクセスが制限されcustomer_alexa_gateway_execution_userた IAM ユーザーを 2 人用意しています。`customer_alexa_gateway_installer_user`1 つは Alexa for Business ゲートウェイのインストール用、もう 1 つはゲートウェイの運用用です。これらは、デプロイ | 高度なスタックコンポーネント | Identity and Access Management (IAM) | Create entity or policy (review required) change type (ct-3dpd8mdd9jn1r) を使用して RFC を送信することでリクエストできます。

> **Note**
>
> 使用状況レポートを生成して Amazon S3 に送信するには、セルフプロビジョニングサービス RFC で Amazon S3 バケット名を指定します。

Q: AMS アカウントで Alexa for Business を使用するにはどのような制限がありますか？

制限はありません。Alexa for Business の全機能は、Alexa for Business の自己プロビジョニング型サービスロールで使用できます。

Q: AMS アカウントで Alexa for Business を使用する際の前提条件または依存関係は何ですか？

- WPA2 Enterprise Wi-Fi を使用して共有デバイスをセットアップする場合は、 AWS Private Certificate Authority が必要な Device Setup Tool でこのネットワークセキュリティタイプを指定します。
- AMS は、名前空間「A4B」で始まるシークレットキーのみを作成します。これは、この名前空間にのみ制限されます。

Q: Alexa for Business のどの機能に個別の RFCsが必要ですか？

Alexa Voice Service (AVS) デバイスを Alexa for Business に登録するには、Alexa 組み込みデバイスメーカーへのアクセスを提供します。これを行うには、管理 | その他 | その他の変更タイプを使用してデプロイできる IAM ロールを Alexa for Business コンソールで作成する必要があります。これにより、AVS デバイスメーカーはユーザーに代わって Alexa for Business にデバイスを登録および管理できます。

AMS SSP を使用して AMS アカウントに Amazon AppStream 2.0 をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon AppStream 2.0 (AppStream 2.0) 機能に直接アクセスします。AppStream 2.0 では、デスクトップアプリケーションを書き換えることなく AWSに移動できます。AppStream 2.0 にアプリケーションをインストールし、起動設定を設定し、ユーザーがアプリケーションを利用できるようにします。AppStream 2.0 には、さまざまな仮想マシンオプションが用意されているため、アプリケーション要件に最適なインスタンスタイプを選択し、エンドユーザーのニーズに合わせて簡単に自動スケーリングパラメータを設定できます。AppStream 2.0 では、独自のネットワークでアプリケーションを起動できます。つまり、アプリケーションは既存の AWS リソースとやり取りできます。

Amazon AppStream 2.0 では、Image Builder を使用してアプリケーションをすばやく簡単にインストール、テスト、更新できます。Microsoft Windows Server 2012 R2、Windows Server 2016、または Windows Server 2019 で実行されるアプリケーションはサポートされており、変更を加える必要はありません。テストが完了したら、アプリケーションの起動設定、デフォルトのユーザー設定を設定し、ユーザーがアクセスできるようにイメージを発行できます。

詳細については、AppStream 2.0」を参照してください。

AWS Managed Services の AppStream 2.0 に関するよくある質問

Q: AMS アカウントで AppStream 2.0 へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (ct-3qe6io8t6jtny) 変更タイプで RFC を送信して、AppStream 2.0 へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_appstream_console_role`。

`customer_appstream_stream_role` は、Active Directory ログイン認証情報を使用してユーザーを認証する必要があるアプリケーションをストリーミングするためにもデプロイされます。

アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの AppStream 2.0 の使用にはどのような制限がありますか？

- 以下の機能は AMS サポートチームが設定する必要があり、特定の RFCsが必要です。追加機能のリクエスト手順については、セクション 4 を参照してください。
  - インターフェイス VPC エンドポイントからの作成とストリーミング。
  - ホームフォルダの Amazon S3 エンドポイントとプライベートネットワークでのアプリケーション設定の永続化のサポート。
  - すべてのフリートストリーミングインスタンスで使用できる IAM ロールを作成して選択します。
  - AppStream 2.0 フリートと Image Builder の Microsoft Active Directory ドメインに参加します。
  - AppStream 2.0 カスタム使用状況レポートの作成。
  - カスタムブランドは現在サポートされていません。

Q: AMS アカウントで AppStream 2.0 を使用するための前提条件または依存関係は何ですか？

AppStream 2.0 のオンボードに RFC を送信するときは、AppStream 2.0 使用状況レポートに使用する Amazon S3 バケット名を含めます。バケット名は、AppStream 2.0 `customer-appstream-usagereports-policy`のオンボーディング時に作成される に追加されます。

Q: 個別の RFC を必要とする AppStream 2.0 の機能は何ですか? RFCs

- AppStream 2.0 のインターフェイス VPC エンドポイントを選択するには、管理 | その他 | その他 | 変更タイプ RFC を更新して、アカウントに VPC エンドポイントを作成します。AppStream 2.0 のカスタムエンドポイントを作成する手順については、AppStream 2.0 ユーザーガイドの「インターフェイス VPC エンドポイントからの作成とストリーミング」を参照してください。
- ホームフォルダの Amazon S3 エンドポイントとプライベートネットワークでのアプリケーション設定の永続性のサポートは、 管理 | その他 | その他 | 変更タイプ RFC の作成で Amazon S3 VPC

エンドポイントをリクエストすることで設定できます。RFC には、ホームフォルダのコンテンツをホストするターゲット Amazon S3 バケット、またはアプリケーション設定 Amazon S3 バケットをそれぞれ含める必要があります。この RFC は、Amazon S3 VPC エンドポイントにアクセスするために必要なアクセス許可を AppStream 2.0 に提供します。 Amazon S3 ストリームのカスタムエンドポイントを作成する手順については、AppStream 2.0 ユーザーガイドの「ホームフォルダの Amazon S3 VPC エンドポイントの使用」と「アプリケーション設定の永続化」を参照してください。

- すべてのフリートストリーミングインスタンスで使用できる IAM ロールを作成して選択するには、デプロイ | 高度なスタックコンポーネント | Identity and Access Management (IAM) | エンティティまたはポリシーの作成 (レビューが必要) 変更タイプ (ct-3dpd8mdd9jn1r) RFC を送信し、必要なポリシーで IAM ロールをリクエストします。IAM ロール名は常にプレフィックス「customer_appstream」で始まる必要があります。
- Amazon AppStream 2.0 フリートと Image Builder は、Active Directory (AD) でサービスアカウントを作成するための管理 | その他 | その他 | 更新変更タイプ RFC を送信することで、Microsoft Active Directory のドメインに参加できます。Microsoft Active Directory に参加するために必要な最小限のアクセス許可は、AppStream 2.0 ドキュメントの「Active Directory コンピュータオブジェクトを作成および管理するためのアクセス許可の付与」で定義されています。
- カスタム AppStream 2.0 使用状況レポートを作成するには、管理 | その他 | その他 | 以下をリクエストする変更タイプ RFC を作成します。
  - AppStreamUsageReports」CFN スタックの作成
  - アカウントで「customer_appstream_usagereports_role」をプロビジョニングする
  - また、以下の詳細を指定します。
    - クローラの実行をスケジュールする CRON 式を指定します。デフォルトでは、毎日 23:00 UTC です。
    - Athena クエリ結果に使用される Amazon S3 バケット ARN。このバケットにはプレフィックスが必要です。 `aws-athena-query-results`
    - AppStream 2.0 使用状況レポートログの Amazon S3 バケット ARN。

  ロールがプロビジョニングされたら、フェデレーションソリューションとログインにロールをオンボードし、 AWS GlueAWS Glue と Athena にアクセスして、使用状況レポートロールを使用してカスタムレポートを生成します。AppStream 2.0 使用状況レポートの使用の詳細については、AppStream 2.0 ドキュメントの「カスタムレポートの作成」と「AppStream 2.0 使用状況データの分析」を参照してください。 AppStream

AMS SSP を使用して AMS アカウントに Amazon Athena をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Athena (Athena) 機能に直接アクセスします。Athena は、標準 SQL を使用して Amazon S3 内のデータを分析するためのインタラクティブなクエリサービスです。Athena はサーバーレスであることから管理するインフラストラクチャがなく、実行したクエリの料金のみを支払います。Amazon S3 のデータにポイントし、スキーマを定義して、標準 SQL を使用してクエリを開始します。ほとんどの結果は数秒以内に配信されます。Athena を使用すると、分析用にデータを準備するための複雑なextract-transform-load (ETL) ジョブは必要ありません。これにより、SQL スキルを持つすべてのユーザーが大規模なデータセットをすばやく分析できます。詳細については、Amazon Athena」を参照してください。

よくある質問: AMS の Athena

Q: AMS アカウントの Amazon Athena へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) change type で RFC を送信して、Athena へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_athena_console_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon Athena の使用にはどのような制限がありますか？

制限はありません。Amazon Athena の完全な機能は、AMS アカウントで使用できます。

Q: AMS アカウントで Amazon Athena を使用するための前提条件または依存関係は何ですか？

Athena は、 で作成されたデータカタログ/メタストアを使用するため、 AWS Glue サービスに大きく依存します AWS Glue。したがって、 AWS Glue アクセス許可は成功した Athena RFC に含まれます。

ロールには、Amazon S3 バケットの前提条件`customer_athena_console_role`があります。新しいバケットを作成するには、自動 CT `ct-1a68ck03fn98r` (デプロイ | 高度なスタックコンポーネント | S3 ストレージ | 作成) を使用します。この自動 CT を使用して Athena の S3 バケットを作成する場合、バケット名はプレフィックス で始まる必要がありますathena-query-results-*。

AMS SSP を使用して AMS アカウントに Amazon Bedrock をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Bedrock 機能に直接アクセスします。Amazon Bedrock は、主要な AI スタートアップから高性能な基盤モデル (FMs) を提供し、統合された API AWS を通じて使用できるフルマネージドサービスです。さまざまな基盤モデルから選択して、ユースケースに最適なモデルを見つけることができます。Amazon Bedrock には、セキュリティ、プライバシー、責任のある AI を備えた生成 AI アプリケーションを構築するためのさまざまな機能も用意されています。Amazon Bedrock を使用すると、ユースケースに適した最善の基盤モデルを簡単に試して評価したり、ファインチューニングや検索拡張生成 (RAG) などの手法を使用して基盤モデルをデータでプライベートにカスタマイズしたり、エンタープライズシステムやデータソースを使用してタスクを実行するエージェントを構築したりできます。

Amazon Bedrock のサーバーレスエクスペリエンスを使用すると、インフラストラクチャを管理することなく、すばやく開始し、独自のデータを使用して基盤モデルをプライベートにカスタマイズし、AWS ツールを使用してアプリケーションに簡単かつ安全に統合してデプロイできます。詳細については、「Amazon Bedrock とは」を参照してください。

よくある質問: AMS の Amazon Bedrock

Q: AMS アカウントの Amazon Bedrock へのアクセスをリクエストするにはどうすればよいですか？

Amazon Bedrock へのアクセスをリクエストするには、 管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (レビューが必要) (ct-3qe6io8t6jtny) 変更タイプを使用して RFC を送信します。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_bedrock_console_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon Bedrock の使用にはどのような制限がありますか？

- Amazon Bedrock ナレッジベースは、現在 AMS でサポートされていない Amazon OpenSearch Service Serverless に依存しているため、SSPS ロールの一部としてデフォルトではサポートされていません。
- Bedrock Studio は、Amazon DataZone などのサポートされていないサービスに依存しているため、サポートされていません。

Q: AMS アカウントで Amazon Bedrock を使用するための前提条件または依存関係は何ですか？

- AWS Marketplace アクセス許可を必要とするサードパーティーモデルのサブスクリプションは、デフォルトのロール (AWSManagedServicesAdminRoleMALZ では 、SALZ Customer_ReadOnly_Roleでは) で実行する必要があります。これは、デフォルトのロールに AWS Marketplace アクセス許可が含まれているためです。
- データ暗号化を使用する場合は、コンソールロールの作成をリクエストするときに AWS KMS キー ARN を指定する必要があります。また、使用する Amazon S3 バケットの名前に「bedrock」が含まれている必要があります。

AMS SSP を使用して AMS アカウントで Amazon CloudSearch をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon CloudSearch 機能に直接アクセスします。Amazon CloudSearch は、ウェブサイトまたはアプリケーションの検索ソリューションのセットアップ、管理、スケーリングを費用対効果の高い方法で行うために使用する AWS クラウド内のマネージドサービスです。Amazon CloudSearch は、34 の言語と、強調表示、オートコンプリート、地理空間検索などの一般的な検索機能をサポートしています。詳細については、Amazon CloudSearch」を参照してください。

> **Note**
>
> AWS は、2024 年 7 月 25 日に Amazon CloudSearch への新しい顧客アクセスを閉鎖しました。Amazon CloudSearch の既存のお客様は、引き続きこのサービスを通常どおり使用できます。 AWS は引き続き Amazon CloudSearch のセキュリティ、可用性、パフォーマンスの向上に投資しますが、新機能を導入する予定はありません。
> Amazon CloudSearch と Amazon OpenSearch Service の違いと OpenSearch Service への移行方法を理解するには、クラウドアーキテクト (CA) に連絡してガイダンスを受けてください。OpenSearch Service への移行の詳細については、Amazon CloudSearch から Amazon OpenSearch Service サービスへの移行」を参照してください。

AWS Managed Servicesでの Amazon CloudSearch に関するよくある質問

Q: AMS アカウントの Amazon CloudSearch へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) change type で RFC を送信して、Amazon CloudSearch へのアクセスをリクエストします。この RFC は、

customer_csearch_admin_roleおよび の IAM ロールをアカウントにプロビジョニングしますcustomer_csearch_dev_role。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon CloudSearch の使用にはどのような制限がありますか？

Amazon CloudSearch の全機能は、AMS アカウントで使用できます。AMS がサポートするすべてのデータベースソリューションは、現在 Amazon CloudSearch でサポートされています。現在、インデックスを作成できないマネージド AWS データベースソリューションは DynamoDB のみです。

Q: AMS アカウントで Amazon CloudSearch を使用するための前提条件または依存関係は何ですか？

Amazon CloudSearch はAmazon S3 が ID プロバイダーと連携して入力データを自動的に分析し、テーブルフィールドを決定します。Amazon S3 へのアクセスはこの RFC では提供されておらず、サービスリクエストで個別にリクエストする必要があります。

AMS SSP を使用して AMS アカウントで Amazon CloudWatch Synthetics をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon CloudWatch Synthetics 機能に直接アクセスします。Amazon CloudWatch Synthetics を使用して「canaryAPIs をモニタリングできます。

Canary は、Node.js または Python で記述された設定可能なスクリプトで、スケジュールに従って実行されます。Node.js または Python をフレームワークとして使用する Lambda 関数をアカウント内に作成します。Canary は、HTTP プロトコルと HTTPS プロトコルの両方で動作します。Canary はエンドポイントの可用性とレイテンシーをチェックし、ロードタイムデータと UI スクリーンショットを保存できます。REST API、URL、ウェブサイトのコンテンツをモニターリングし、フィッシング、コードインジェクション、およびクロスサイトスクリプティングによる不正な変更をチェックできます。

Canary は顧客と同じルートに従って同じアクションを実行するため、アプリケーションに顧客トラフィックがない場合でもカスタマーエクスペリエンスを継続的に検証できます。Canary を使用すると、顧客が問題を検出する前に問題を検出できます。詳細については、Amazon CloudWatch: 合成モニタリングの使用」を参照してください。

AWS Managed Services の Amazon CloudWatch Synthetics に関するよくある質問

Q: AMS アカウントの Amazon CloudWatch Synthetics へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) 変更タイプで RFC を送信して、Amazon CloudWatch Synthetics へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: 'customer_cw_synthetics_console_role' および 'customer_cw_synthetics_canary_lambda_role'。アカウントにプロビジョニングされたら、フェデレーションソリューションで「customer_cw_synthetics_console_role」ロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon CloudWatch Synthetics の使用にはどのような制限がありますか？

AMS アカウントでの Amazon CloudWatch Synthetics の使用に制限はありません。AMS が提供するサービスロールcustomer_cw_synthetics_canary_lambda_role」以外の Canary のロールの作成は禁止されています。

Q: AMS アカウントで Amazon CloudWatch Synthetics を使用するための前提条件または依存関係は何ですか？

Canary は、デフォルトの Amazon CloudWatch Synthetics S3 バケットを作成および使用します。cw-syn-results-*${accountnumber}-${default-region}*」

AMS SSP を使用して AMS アカウントに Amazon Cognito ユーザープールをプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Cognito ユーザープール機能に直接アクセスします。Amazon Cognito ユーザープールは、何億人ものユーザーにスケールする安全なユーザーディレクトリを提供します。フルマネージドサービスである Amazon Cognito ユーザープールは、サーバーインフラストラクチャの立ち上げを心配することなくセットアップできます。このサービスを使用すると、内部アプリケーションとの統合に使用できる最終ユーザーのプールを管理できます。このサービスでは、カスタマイズされたデータベースまたはウェブアプリケーションやモバイルアプリケーションの最終ユーザーのディレクトリの代わりに使用できます。同時に、Amazon Cognito ユーザープールは、パスワードポリシー、多要素認証、パスワード復旧、サービスへの自己サインアップなど、ディレクトリサービスのフルセットの機能を提供します。また、アプリケーションは OpenID、Facebook、Amazon、Google などの一般的なパブリックサービスでアクセスをフェデレーションすることもできます。

Amazon Cognito は 2 つの主要製品に分かれています。Amazon Cognito ユーザープールと Amazon Cognito ID プロバイダー。このセクションでは、Amazon S3 や DynamoDB などの他のサービスへのアクセスを提供する Amazon Cognito ユーザープールに焦点を当てます。 AWS Amazon S3 DynamoDB このサービスでは、Amazon Cognito ユーザープールまたはサードパーティーの ID プロバイダーを使用して、 AWS サービスへのアクセスを提供できます。また、匿名ゲストアクセスを使用して AWS サービスへのアクセスも提供します。Amazon Cognito ユーザープールの強力な性質により、アカウントへの潜在的なセキュリティ侵害を避けるために、運用手動サービスとしてcase-by-caseで手動で管理されます。詳細については、Amazon Cognito ユーザープール」を参照してください。

AWS Managed Services の Amazon Cognito ユーザープールに関するよくある質問

よくある質問と回答：

Q: AMS アカウントの Amazon Cognito ユーザープールへのアクセスをリクエストするにはどうすればよいですか？

AMS での Amazon Cognito ユーザープールの実装は、2 ステップのプロセスです。

1. 管理を送信する | その他 | その他 | 変更タイプ (ct-1e1xtak34nx76) を作成し、AMS アカウントで Amazon Cognito ユーザープールの作成をリクエストします。次の情報を含めてください。
   - AWS リージョン。
   - Cognito ユーザープールの名前。
   - デフォルトの内部 Cognito メールサービスの代わりに Amazon Simple Email Service (Amazon SES) を使用してメッセージと通知を送信する場合、お客様はアカウントで Amazon SES Service の検証済みの E メールアドレスを提供する必要があります。このアドレスは、メッセージの「From」フィールドと「REPLY-TO」フィールドに使用されます。また、Amazon SES がアクティブ化されたリージョン (us-east-1、eu-west-1、または us-west-2) も指定する必要があります。
   - ワンタイムパスワードと検証に SMS メッセージを使用する場合は、顧客が指定する必要があります。
2. Management | AWS service | Self-provisioned service | Add change type (ct-1w8z66n899dct) を送信してユーザーアクセスをリクエストします。この RFC は、`customer_cognito_admin_role`および の IAM ロールをアカウントにプロビジョニングします`customer_cognito_importjob_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。これらのロールを使用すると、Amazon Cognito ユーザープールの管理、プール内のユーザーとグループの管理、ユーザー

のインポートジョブの作成、通知メッセージとサブスクリプションメッセージの変更、ユーザープールへのアプリケーションの関連付け、プールへのフェデレーションサービスの追加の自己管理、および既に作成されたプールの削除を行うことができます。

Q: AMS アカウントでの Amazon Cognito ユーザープールの使用にはどのような制限がありますか？

Amazon Cognito ユーザープールを作成することはできません。このアクションでは、Amazon SES や Amazon Cognito が使用するサービスを活用するための IAM ロールを作成する必要があります。Amazon SNS

Q: AMS アカウントで Amazon Cognito ユーザープールを使用するための前提条件または依存関係は何ですか？

Amazon SES を使用してユーザープールに E メールでメッセージと通知を送信する場合は、アカウントで Amazon SES サービスをアクティブ化し、送信された E メールの「FROM」フィールドと「REPLY-TO」フィールドで使用する E メールアドレスを既に検証する必要があります。Amazon SES を使用した E メールアドレスの検証の詳細については、Amazon SES での E メールアドレスの検証」を参照してください。

AMS SSP を使用して AMS アカウントに Amazon Comprehend をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Comprehend 機能に直接アクセスします。Amazon Comprehend は、機械学習を使用してテキストでインサイトや関係を見つける自然言語処理 (NLP) サービスであり、機械学習の経験は必要ありません。Amazon Comprehend は機械学習を使用して、非構造化データ内のインサイトと関係を明らかにするのに役立ちます。このサービスは、テキストの言語を識別し、主要なフレーズ、場所、人物、ブランド、またはイベントを抽出し、テキストがどの程度肯定的または否定的であるかを理解し、トークン化と音声部分を使用してテキストを分析し、トピックごとにテキストファイルのコレクションを自動的に整理します。Amazon Comprehend の AutoML 機能を使用して、組織のニーズに合わせて一意にカスタマイズされたエンティティまたはテキスト分類モデルのカスタムセットを構築することもできます。詳細については、Amazon Comprehend」を参照してください。

AWS Managed Services の Amazon Comprehend に関するよくある質問

Q: AMS アカウントの Amazon Comprehend へのアクセスをリクエストするにはどうすればよいですか？

Amazon Comprehend コンソールとデータアクセスロールは、2 つの AMS Service RFCs を送信することでリクエストできます。

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (レビューが必要) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_comprehend_console_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon Comprehend の使用にはどのような制限がありますか？

Amazon Comprehend コンソールを使用して新しい IAM ロールを作成する機能は制限されています。それ以外の場合、Amazon Comprehend の全機能が AMS アカウントで使用できます。

Q: AMS アカウントで Amazon Comprehend を使用するための前提条件または依存関係は何ですか？

Amazon S3 バケットが AWS KMS キーで暗号化されている場合、Amazon Comprehend を使用するには Amazon S3 と AWS Key Management Service（ AWS KMS) が必要です。

AMS SSP を使用して AMS アカウントに Amazon Connect をプロビジョニングする

> **Note**
>
> 慎重に検討した結果、2026 年 5 月 20 日をもって Amazon Connect Voice ID のサポートを終了することにしました。Amazon Connect Voice ID は、2025 年 5 月 20 日以降、新規顧客を受け入れなくなります。2025 年 5 月 20 日より前にサービスにサインアップしたアカウントを持つ既存のお客様は、引き続き Amazon Connect Voice ID 機能を使用できます。2026 年 5 月 20 日以降、Amazon Connect Voice ID を使用することはできません。

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Connect 機能に直接アクセスします。Amazon Connect は、企業が優れたカスタマーサービスを低コストで提供できるようにするオムニチャネルクラウドコンタクトセンターです。Amazon Connect は、顧客とエージェントに音声とチャット全体でシームレスなエクスペリエンスを提供します。これには、スキルベースのルーティング、強力なリアルタイム分析と履歴分析、easy-to-use直感的な管理ツールのセットが含まれます。これらはすべてpay-as-you-goです。

仮想コンタクトセンターインスタンスの 1 つ以上のインスタンスは、AMS マルチアカウントランディングゾーンまたはシングルアカウントランディングゾーンアカウントに作成できます。エージェ

ントアクセスには既存の SAML 2.0 ID プロバイダーを使用するか、ユーザーライフサイクル管理には Amazon Connect ネイティブサポートを使用できます。

さらに、Amazon Connect コンソールから各 Amazon Connect インスタンスの通話料無料/直通ダイヤルの電話番号を要求できます。 Amazon Connect リッチな問い合わせフローを作成して、easy-to-useグラフィカルユーザーインターフェイスを使用して、望ましいカスタマーエクスペリエンスとルーティングを実現できます。問い合わせフローでは、 AWS Lambda 関数を活用して、オンプレミスのデータストアや API と統合できます。Kinesis Streams と Firehose を使用してデータストリーミングを有効にすることもできます。

通話録音、チャットトランスクリプト、およびレポートは、 AWS KMS キーを使用して暗号化された Amazon S3 バケットに保存されます。問い合わせフローログは CloudWatch ロググループに保存できます。

詳細については、Amazon Connect」を参照してください。

AWS Managed Services での Amazon Connect に関するよくある質問

Q: AMS アカウントで Amazon Connect へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (レビューが必要) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、`customer_connect_console_role`および の IAM ロールをアカウントにプロビジョニングします`customer_connect_user_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon Connect の使用にはどのような制限がありますか？

制限はありません。Amazon Connect の完全な機能は、AMS アカウントで使用できます。

Q: AMS アカウントで Amazon Connect を使用するための前提条件または依存関係は何ですか？

- 標準の AMS RFCs を使用して AWS KMS キーと Amazon S3 バケットを作成する必要があります。通話録音とチャットトランスクリプトを保存するにはAmazon S3 バケットが必要です。
- Active Directory (AD) と統合する場合は、AMS がホストする Amazon Connect インスタンスとオンプレミスのディレクトリサービスの統合に AD Connector が必要です。AD Connector は、「管理 | その他 | その他」 RFC をリクエストすることで、アカウントで設定できます。
- 問い合わせフローの要件に基づいて、以下のオプションのセルフプロビジョニングサービスを有効にできます。

- AWS Lambda: Lambda 関数を使用して問い合わせフローを拡張し、既存のオンプレミスデータストアまたは APIsを活用できます。Lambda 自己プロビジョニングサービスを使用して Lambda 関数を作成できます。
- Amazon Kinesis Data Streams: データストリームを作成して、外部アプリケーションへのデータストリーミングを有効にできます。問い合わせトレースレコードまたはエージェントイベントをストリーミングできます。
- Amazon Kinesis Data Firehose: Data Firehose を作成して、大量の問い合わせトレースレコードを外部アプリケーションにストリーミングできます。
- Amazon Lex: Amazon Lex Chatbots を活用して、Amazon Alexa サービスを活用したスマートな問い合わせフローを作成し、豊富なカスタマーエクスペリエンスと自動化を実現できます。

- Q: 発信通話または着信通話の国のリストの追加をリクエストするにはどうすればよいですか？

  アウトバウンド通話またはインバウンド通話の国のリストを追加するには、サービスリクエストを AMS に送信します。

AMS SSP を使用して AMS アカウントに Amazon Data Firehose をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Data Firehose 機能に直接アクセスします。Firehose は、ストリーミングデータをデータレイク、データストア、分析ツールに確実にロードする最も簡単な方法です。ストリーミングデータを Amazon S3、Amazon Redshift、Amazon OpenSearch Service、Splunk にキャプチャ、変換、ロードできるため、現在使用している既存のビジネスインテリジェンスツールやダッシュボードでほぼリアルタイムの分析が可能になります。これは、データのスループットに合わせて自動的にスケーリングするフルマネージドサービスであり、継続的な管理は必要ありません。また、データをロードする前にバッチ処理、圧縮、変換、暗号化して、送信先で使用されるストレージの量を最小限に抑え、セキュリティを強化することもできます。詳細については、「Amazon Data Firehose とは」を参照してください。

AWS Managed Services の Firehose に関するよくある質問

一般的な質問と回答：

Q: AMS アカウントの Amazon Data Firehose へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (レビューが必要) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_kinesis_firehose_user_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Firehose の使用にはどのような制限がありますか？

制限はありません。Amazon Data Firehose の全機能は、AMS アカウントで使用できます。

Q: AMS アカウントで Firehose を使用するための前提条件または依存関係は何ですか？

新しいサービスにリンクされた IAM ロールは、配信ストリームごとにリクエストする必要があります。また、必要なリソースアクセス許可 (S3 バケット/KMS キー/Lambda 関数/Kinesis ストリームを含む) でロールポリシーを更新することで、すべてのストリームに対して単一のサービスにリンクされたロールを再利用することもできます。

RFC を送信して Firehose を追加すると、AMS オペレーションエンジニアが Data Firehose に接続するリソース (S3 AWS KMS、Lambda、Kinesis Streams など) の ARNs のサービスリクエストを通じてお客様に連絡します。

AMS SSP を使用して AMS アカウントに Amazon DevOpsGuru をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon DevOpsGuru 機能に直接アクセスします。Amazon DevOpsGuru は、開発者やオペレーターがアプリケーションのパフォーマンスと可用性を簡単に改善できるようにするフルマネージド型のオペレーションサービスです。DevOps Guru は、運用上の問題の特定に関連する管理タスクをオフロードし、アプリケーションを改善するためのリコメンデーションを迅速に実装できるようにします。DevOps Guru は、アプリケーションを今すぐ改善するために使用できる事後対応型のインサイトを作成します。また、将来アプリケーションに影響を与える可能性のある運用上の問題を回避するために事前対応型インサイトを作成します。DevOps Guru は、機械学習を適用して、運用データとアプリケーションのメトリクスおよびイベントを分析し、通常の運用パターンから逸脱する動作を特定します。DevOps Guru が運用上の問題またはリスクを検出すると通知が行われます。DevOps Guru は、各問題について、現在および予測される将来の運用上の問題に対処するためのインテリジェントなレコメンデーションを提示します。

詳細については、「Amazon DevOpsGuru とは」を参照してください。

AWS Managed Services の Amazon DevOpsGuru に関するよくある質問

Q: AMS アカウントの Amazon DevOpsGuru へのアクセスをリクエストするにはどうすればよいですか？

アクセスをリクエストするには、管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (レビューが必要) (ct-3qe6io8t6jtny) 変更タイプを送信します。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_devopsguru_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon DevOpsGuru の使用にはどのような制限がありますか？

制限はありません。Amazon DevOpsGuru のフル機能は、AMS アカウントで使用できます。

Q: AMS アカウントで Amazon DevOpsGuru を使用するための前提条件または依存関係は何ですか？

前提条件はありません。DevOpsGuru は、Amazon CloudWatch Logs、RDS Insights AWS X-Ray、および AWS Lambda AWS のサービスを活用します AWS CloudTrail。

AMS SSP を使用して AMS アカウントに Amazon DocumentDB (MongoDB 互換) をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon DocumentDB (MongoDB 互換) 機能に直接アクセスします。Amazon DocumentDB (MongoDB 互換) は、MongoDB ワークロードをサポートする高速、スケーラブル、高可用性、フルマネージド型のドキュメントデータベースサービスです。Amazon DocumentDB は、ミッションクリティカルな MongoDB ワークロードを大規模に運用するために必要なパフォーマンス、スケーラビリティ、可用性を提供します。Amazon DocumentDB は、MongoDB クライアントが MongoDB サーバーに期待するレスポンスをエミュレートすることで、Apache 2.0 オープンソースの MongoDB 3.6 API を実装します。これにより、Amazon DocumentDB で既存の MongoDB ドライバーとツールを使用できます。 MongoDB Amazon DocumentDB では、ストレージとコンピューティングが分離されるため、それぞれが独立してスケールでき、データのサイズに関係なく、最大 15 個の低レイテンシーのリードレプリカを追加することで、読み取り容量を 1 秒あたり数百万のリクエストに増やすことができます。Amazon DocumentDB は 99.99% の可用性を実現するように設計されており、データの 6 つのコピーを 3 つの AWS アベイラビリティーゾーン (AZs。 AWS Database Migration Service (DMS) を無料で (6 か月間) 使用して、オンプレミスまたは Amazon Elastic Compute Cloud (Amazon EC2) MongoDB データベースを Amazon DocumentDB にほぼダウンタイムなしで移行できます。詳細については、Amazon DocumentDB (MongoDB 互換) 」を参照してください。

AWS Managed Services の Amazon DocumentDB に関するよくある質問

Q: AMS アカウントの Amazon DocumentDB へのアクセスをリクエストするにはどうすればよいですか？

Amazon DocumentDB コンソールとデータアクセスロールは、コンソールアクセスとデータアクセスの 2 つの AMS RFCs を送信することでリクエストできます。

管理 | AWS サービス | セルフプロビジョニングサービス | (ct-1w8z66n899dct) 変更タイプで RFC を送信して Amazon DocumentDB へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_documentdb_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon DocumentDB の使用にはどのような制限がありますか？

Amazon DocumentDB には、Amazon RDS 固有のアクセス許可が必要です。AMS は Amazon RDS を完全に管理するため、Amazon DocumentDB の IAM ロールには Amazon RDS でのアクションに対するいくつかの制限が含まれています。以下の制限が適用されます。

- `DeleteDBInstance` および `DeleteDBCluster` APIs へのアクセスが制限されています。これらの削除 APIs を使用するには、 管理 | 高度なスタックコンポーネント | Identity and Access Management (IAM) | 更新エンティティまたはポリシー (レビューが必要) 変更タイプ (ct-27tuth19k52b4) で RFC を送信します。
- Amazon RDS インスタンスにタグを追加または削除することはできません。
- Amazon DocumentDB インスタンスを公開することはできません。

Q: AMS アカウントで Amazon DocumentDB を使用するための前提条件または依存関係は何ですか？

Amazon S3 バケット AWS KMS が AWS KMS キーで暗号化されている場合、Amazon DocumentDB を使用するには Amazon S3 と が必要です。

AMS SSP を使用して AMS アカウントに Amazon DynamoDB をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon DynamoDB (DynamoDB) 機能に直接アクセスします。Amazon DynamoDB は、あらゆる規模で 1 桁ミリ秒のパフォーマンスを実現するキー値およびドキュメントデータベースです。これ

は、セキュリティ、バックアップと復元、インターネットスケールアプリケーション用のインメモリキャッシュが組み込まれた、フルマネージド型のマルチリージョンのマルチアクティブデータベースです。詳細についてはAmazon DynamoDBを参照してください。

Amazon DynamoDB Accelerator (DAX) は、DynamoDB テーブルにキャッシュを追加するプロセスを簡素化するために設計された書き込みスルーキャッシュサービスです。DAX は、高パフォーマンスの読み込みを必要とするアプリケーションを対象としています。

AWS Managed Services の DynamoDB に関するよくある質問

Q: AMS アカウントの DynamoDB と DAX へのアクセスをリクエストするにはどうすればよいですか？

管理 | サービス | AWS セルフプロビジョニングサービス | 追加 (ct-1w8z66n899dct) 変更タイプで RFC を送信して、DynamoDB と DAX へのアクセスをリクエストします。この RFC は、次の IAM ロールとポリシーをアカウントにプロビジョニングします。

- DynamoDB ロール名: `customer_dynamodb_role`

  DAX サービスロール名: `customer_dax_service_role`
- DynamoDB ポリシー名: `customer_dynamodb_policy`

  DAX サービスポリシー: `customer_dax_service_policy`

アカウントにプロビジョニングされたら、フェデレーションソリューション`customer_dynamodb_role`で をオンボードする必要があります。

Q: AMS アカウントでの DynamoDB の使用にはどのような制限がありますか？

DynamoDB Accelerator (DAX) を含むすべての DynamoDB 機能がサポートされています。

特定のテーブルに対してアラームを作成する場合、アラーム名には「customer*」というプレフィックスを付ける必要があります`customer-employee-table-high-put-latency`。たとえば、。

DynamoDB 用の Amazon SNS トピックを作成するときは、 という名前にする必要があります`dynamodb`。

DynamoDB によって作成された Amazon SNS トピックを削除するには、管理 | その他 | その他 | 更新変更タイプ RFC を送信します。

Q: AMS アカウントで DynamoDB を使用するための前提条件または依存関係は何ですか？

AMS アカウントで DynamoDB を使用するための前提条件や依存関係はありません。

AMS SSP を使用して AMS アカウントに Amazon Elastic Container Registry をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Elastic Container Registry (Amazon ECR) 機能に直接アクセスします。Amazon Elastic Container Registry は、開発者が Docker コンテナイメージを簡単に保存、管理、デプロイできるようにするフルマネージド型の Docker コンテナレジストリです。Amazon ECR は Amazon Elastic Container Service (Amazon ECS) と統合されているため、本番環境への開発ワークフローが簡素化されます。Amazon ECR を使用すると、独自のコンテナリポジトリを運用したり、基盤となるインフラストラクチャのスケーリングを心配する必要がなくなります。Amazon ECS は、高可用性でスケーラブルなアーキテクチャでイメージをホストするため、アプリケーションのコンテナを確実にデプロイできます。 AWS Identity and Access Management (IAM) との統合により、各リポジトリのリソースレベルの制御が可能になります。Amazon ECR では、前払い料金やコミットメントはありません。リポジトリに保存したデータの量とインターネットに転送されたデータに対してのみ料金が発生します。

詳細については、「Amazon Elastic Container Registry」を参照してください。

AWS Managed Services の Amazon Elastic Container Registry に関するよくある質問

Q: AMS アカウントの Amazon ECR へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) change type で RFC を送信して Amazon ECR へのアクセスをリクエストします。この RFC は、次の IAM ロールをアカウントにプロビジョニングします: `customer_ecr_console_role`、、および関連する IAM ポリシー`customer_ecr_poweruser_instance_profile`を持つ`customer_ecr_poweruser_instance_profile_policy`、`customer_ecr_console_policy`および 。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon ECR の使用にはどのような制限がありますか？

AMS アカウントでの Amazon ECR の使用には、AMS 名前空間に関する制限があります。コンテナイメージには「AMS-」または「Sentinel-」のプレフィックスを付けることはできません。

Q: AMS アカウントで Amazon ECR を使用するための前提条件または依存関係は何ですか？

AMS アカウントで Amazon ECR を使用するための前提条件や依存関係はありません。

AMS SSP を使用して AMS アカウントに EC2 Image Builder をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで EC2 Image Builder 機能に直接アクセスします。EC2 Image Builder は、カスタマイズされ、安全で up-to-date「ゴールデン」サーバーイメージの作成、管理、デプロイを簡単に自動化できるフルマネージド AWS サービスです。これらのイメージは、特定の IT 標準を満たすためのソフトウェアと設定がプリインストールされ、事前設定されています。

AWS マネジメントコンソール、 AWS CLI、または APIs を使用して、 AWS アカウントにカスタムイメージを作成できます。を使用すると AWS マネジメントコンソール、Amazon EC2 Image Builder ウィザードが以下のステップをガイドします。

- 開始アーティファクトを指定する
- ソフトウェアの追加と削除
- 設定とスクリプトをカスタマイズ
- 選択したテストを実行する
- AWS イメージをリージョンに配布する

ビルドするイメージはアカウントで作成され、オペレーティングシステムのパッチ用に継続的に設定できます。詳細については、EC2 Image Builder」を参照してください。

AWS Managed Services の EC2 Image Builder に関するよくある質問

一般的な質問と回答：

Q: AMS アカウントの EC2 Image Builder へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (レビューが必要) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC を通じて、次の IAM ロールがアカウントにプロビジョニングされます: `customer_ec2_imagebuilder_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: EC2 Image Builder にはどのような制限がありますか？

AMS は、インフラストラクチャ設定でのサービスデフォルトの使用をサポートしていません。新しいインフラストラクチャ設定を作成することも、既存の設定を使用することもできます。

AMS は現在、コンテナレシピの作成をサポートしていません。

Q: EC2 Image Builder を有効にするための前提条件または依存関係は何ですか？

- EC2 Image Builder サービスにリンクされたロール: サービスにリンクされたロールを手動で作成する必要はありません。、 CLI AWS マネジメントコンソール、または AWS API で最初の Image Builder AWS リソースを作成すると、Image Builder によってサービスにリンクされたロールが作成されます。
- Image Builder を使用してイメージを構築し、テストを実行するために使用されるインスタンスは、Systems Manager サービスにアクセスできる必要があります。SSM エージェントは、ソースイメージがまだ存在しない場合はインストールされ、イメージが作成される前に削除されます。
- AWS IAM: インスタンスプロファイルに関連付ける IAM ロールには、イメージに含まれるビルドコンポーネントとテストコンポーネントを実行するアクセス許可が必要です。インスタンスプロファイルに関連付けられている IAM ロールには、`EC2InstanceProfileForImageBuilder`および の IAM ロールポリシーをアタッチする必要がありま`AmazonSSMManagedInstanceCore`す。IAM ロール名には `*imagebuilder*`キーワードを含める必要があります。
- ロギングを設定する場合、インフラストラクチャ構成で指定されたインスタンスプロファイルは、ターゲットバケット(`arn:aws:s3:::`*`{bucket-name}`*`/*`)に対して`s3:PutObject`の権限を持っている必要があります。例:

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::{bucket-name}/*"
        }
    ]
}
```

- EC2 Image Builder からアラートと通知を受信するには、「imagebuilder」という名前の SNS トピックを作成します。

AMS SSP を使用して AMS アカウントの AWS Fargate で Amazon ECS をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS Fargate 機能で Amazon ECS に直接アクセスします。 AWS Fargate は、Amazon EC2 インスタンスのAmazon EC2 で使用できるテクノロジーです (「 のコンテナ AWS」を参照)。を使用すると AWS Fargate、コンテナを実行するために仮想マシンのクラスターをプロビジョニング、設定、スケーリングする必要がなくなります。これにより、サーバータイプの選択、クラスターをスケールするタイミングの決定、クラスターのパッキングの最適化を行う必要がなくなります。

詳細については、「Amazon ECS on AWS Fargate」を参照してください。

AWS Managed Servicesでの Fargate での Amazon ECS に関するよくある質問

Q: AMS アカウントの Fargate で Amazon ECS へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (ct-1w8z66n899dct) 変更タイプで RFC を送信して、Fargate で Amazon ECS へのアクセスをリクエストします。この RFC は、次の IAM ロールをアカウントにプロビジョニングします: `customer_ecs_fargate_console_role` (ECS ポリシーを関連付けるための既存の IAM ロールが指定されていない場合) `customer_ecs_fargate_events_service_role`、、`customer_ecs_task_execution_servic` および `AWSServiceRoleForApplicationAutoScaling_ECSService`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントで Fargate で Amazon ECS を使用することにはどのような制限がありますか？

- Amazon ECS タスクのモニタリングとログ記録は、コンテナレベルのアクティビティがハイパーバイザーを超えて発生し、Fargate の Amazon ECS によってログ記録機能が制限されるため、お客様の責任と見なされます。Fargate 上の Amazon ECS のユーザーは、Amazon ECS タスクのログ記録を有効にするために必要な手順を実行することをお勧めします。詳細については、「コンテナの awslogs ログドライバーの有効化」を参照してください。
- コンテナレベルでのセキュリティとマルウェアの保護もお客様の責任と見なされます。Fargate の Amazon ECS には、Trend Micro または事前設定されたネットワークセキュリティコンポーネントは含まれません。

- このサービスは、マルチアカウントランディングゾーンとシングルアカウントランディングゾーンの両方の AMS アカウントで使用できます。
- Amazon ECS Service Discovery は、Route 53 プライベートホストゾーンの作成には昇格されたアクセス許可が必要であるため、セルフプロビジョニングロールではデフォルトで制限されています。サービスでサービス検出を有効にするには、管理 | その他 | その他 | 変更タイプを更新します。Amazon ECS サービスのサービス検出を有効にするために必要な情報については、「サービス検出マニュアル」を参照してください。
- AMS は現在、Amazon ECS Fargate へのコンテナのデプロイに使用されるイメージを管理または制限していません。Amazon ECR、Docker Hub、またはその他のプライベートイメージリポジトリからイメージをデプロイできます。したがって、パブリックイメージやセキュリティで保護されていないイメージは、アカウントで悪意のあるアクティビティが発生する可能性があるため、デプロイしないことをお勧めします。

Q: AMS アカウントで Fargate で Amazon ECS を使用する際の前提条件または依存関係は何ですか？

- 以下は、Fargate 上の Amazon ECS の依存関係です。ただし、自己プロビジョニングロールでこれらのサービスを有効にするための追加のアクションは必要ありません。
  - CloudWatch ログ
  - CloudWatch events
  - CloudWatch アラーム
  - CodeDeploy
  - App Mesh
  - クラウドマップ
  - Route 53
- ユースケースに応じて、Amazon ECS が依存するリソースを以下に示します。アカウントで Fargate で Amazon ECS を使用する前に必要になる場合があります。
  - Amazon ECS サービスで使用するセキュリティグループ。デプロイ | 高度なスタックコンポーネント | セキュリティグループ | 作成 (自動) (ct-3pc215bnwb6p7) を使用するか、セキュリティグループで特別なルールが必要な場合は、デプロイ | 高度なスタックコンポーネント | セキュリティグループ | 作成 (レビューが必要) (ct-1oxx2g2d7hc90) を使用できます。注: Amazon ECS で選択するセキュリティグループは、Amazon ECS サービスまたはクラスターが存在する Amazon ECS 専用に作成する必要があります。詳細については、「Security Group」セクション

の「Setting Up with Amazon ECS and Security in Amazon Elastic Container Service」を参照してください。

- Application Load Balancer (ALB)、Network Load Balancer (NLB)、Classic Load Balancer (ELB)。
- ALBs のターゲットグループ。
- Amazon ECS クラスターと統合するためのアプリメッシュリソース (仮想ルーター、仮想サービス、仮想ノードなど) 。

- 現在、標準 AMS 変更タイプ以外で作成された場合、AMS がセキュリティグループのアクセス許可のサポートに関連するリスクを自動的に軽減する方法はありません。Amazon ECS で使用するために指定されていないセキュリティグループを使用する可能性を制限するために、Fargate クラスターで使用する特定のセキュリティグループをリクエストすることをお勧めします。

AMS SSP を使用して AMS アカウントの AWS Fargate で Amazon EKS をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS Fargate 機能で Amazon EKS に直接アクセスします。 AWS Fargate は、コンテナに適したサイズのコンピューティングキャパシティをオンデマンドで提供するテクノロジーです (コンテナを理解するには、「コンテナとは」を参照してください) 。を使用すると AWS Fargate、コンテナを実行するために仮想マシンのグループをプロビジョニング、設定、またはスケールする必要がなくなります。これにより、サーバータイプの選択、ノードグループをスケールするタイミングの決定、クラスターのパッキングの最適化を行う必要がなくなります。

Amazon Elastic Kubernetes Service (Amazon EKS) は、Kubernetes が提供するアップストリームの拡張可能なモデル AWS Fargate を使用して構築されたコントローラー AWS を使用して、Kubernetes を と統合します。これらのコントローラーは、Amazon EKS が管理する Kubernetes コントロールプレーンの一部として実行され、ネイティブ Kubernetes ポッドを Fargate にスケジューリングします。Fargate コントローラーには、いくつかの変更と検証アドミッションコントローラーに加えて、デフォルトの Kubernetes スケジューラーとともに実行される新しいスケジューラが含まれています。Fargate で実行する条件を満たすポッドを起動すると、クラスターで実行されている Fargate コントローラーはポッドを認識し、更新し、Fargate にスケジューリングします。

詳細については、「Amazon EKS on AWS Fargate Now generally Available」および「Amazon EKS Best Practices Guide for Security」 (「Review and revoke unnecessary anonymous access」などの「Recommendations」を含む) を参照してください。

> **Tip**
>
> AMS には、Amazon EKS で使用できる変更タイプである Deployment | Advanced stack components | Identity and Access Managment (IAM) | Create OpenID Connect provider (ct-30ecvfi3tq4k3) があります。例については、「Identity and Access Management (IAM) | Create OpenID Connect Provider」を参照してください。

AWS Managed Services AWS Fargate の「Amazon EKS on」に関するよくある質問

Q: AMS アカウントの Fargate で Amazon EKS へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、次の IAM ロールをアカウントにプロビジョニングします。

- `customer_eks_fargate_console_role`.

  アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。
- これらのサービスロールは、ユーザーに代わって他の AWS サービスを呼び出すアクセス許可を Amazon EKS on Fargate に付与します。
  - `customer_eks_pod_execution_role`
  - `customer_eks_cluster_service_role`

Q: AMS アカウントで Fargate で Amazon EKS を使用することにはどのような制限がありますか？

- マネージド EC2 ノードグループまたはセルフマネージド EC2 ノードグループの作成は、AMS ではサポートされていません。 EC2 EC2 ワーカーノードを使用する必要がある場合は、AMS Cloud Service Delivery Manager (CSDM) または Cloud Architect (CA) にお問い合わせください。
- AMS には、Trend Micro またはコンテナイメージ用に事前設定されたネットワークセキュリティコンポーネントは含まれません。デプロイ前に悪意のあるコンテナイメージを検出するために、独自のイメージスキャンサービスを管理する必要があります。
- CloudFormation の相互依存関係のため、EKSCTL はサポートされていません。
- クラスターの作成中に、クラスターコントロールプレーンのログ記録を無効にするアクセス許可があります。詳細については、「Amazon EKS コントロールプレーンのログ記録」を参照してくだ

さい。クラスターの作成時に、すべての重要な API、認証、監査ログを有効にすることをお勧めします。

- クラスターの作成中、Amazon EKS クラスターのクラスターエンドポイントアクセスはデフォルトでパブリックになります。詳細については、「Amazon EKS クラスターエンドポイントアクセスコントロール」を参照してください。Amazon EKS エンドポイントはプライベートに設定することをお勧めします。パブリックアクセスにエンドポイントが必要な場合は、特定の CIDR 範囲に対してのみパブリックに設定することをお勧めします。
- AMS には、Amazon EKS Fargate 上のコンテナへのデプロイに使用されるイメージを強制および制限する方法はありません。Amazon ECR、Docker Hub、またはその他のプライベートイメージリポジトリからイメージをデプロイできます。したがって、アカウントで悪意のあるアクティビティを実行する可能性のあるパブリックイメージをデプロイするリスクがあります。
- Cloud Development Kit (CDK) または CloudFormation Ingest を使用した EKS クラスターのデプロイは、AMS ではサポートされていません。
- ct-3pc215bnwb6p7 Deployment | Advanced stack components | Security group | Create and reference in the manifest file for Ingress creation を使用して、必要なセキュリティグループを作成する必要があります。これは、ロールにセキュリティグループを作成する権限`customer-eks-alb-ingress-controller-role`がないためです。

Q: AMS アカウントで Fargate で Amazon EKS を使用するための前提条件または依存関係は何ですか？

サービスを使用するには、次の依存関係を設定する必要があります。

- サービスに対して認証するには、KUBECTL と aws-iam-authenticator の両方をインストールする必要があります。詳細については、「クラスター認証の管理」を参照してください。
- Kubernetes は「サービスアカウント」と呼ばれる概念に依存しています。EKS 上の kubernetes クラスター内でサービスアカウント機能を利用するには、次の入力を使用して管理 | その他 | その他 | RFC を更新する必要があります。
  - 〔必須] Amazon EKS クラスター名
  - 〔必須] サービスアカウント (SA) がデプロイされる Amazon EKS クラスター名前空間。
  - 〔必須] Amazon EKS クラスター SA 名。
  - 〔必須] 関連付ける IAM ポリシー名とアクセス許可/ドキュメント。
  - 〔必須] リクエストされている IAM ロール名。
  - 〔オプション] OpenID Connect プロバイダー URL。詳細については、次を参照してください。
    - クラスターのサービスアカウントの IAM ロールの有効化

    - サービスアカウントのきめ細かな IAM ロールの紹介
- Config ルールを設定してモニタリングすることをお勧めします。
    - パブリッククラスターエンドポイント
    - 無効化された API ログ記録

    これらの Config ルールをモニタリングして修正するのはユーザーの責任です。

ALB Ingress Controller をデプロイする場合は、管理 | その他 | その他の更新 RFC を送信して、ALB Ingress Controller ポッドで使用するために必要な IAM ロールをプロビジョニングします。ALB Ingress Controller (RFC にこれらを含める) に関連付ける IAM リソースを作成するには、次の入力が必要です。

- 〔必須] Amazon EKS クラスター名
- 〔オプション] OpenID Connect プロバイダー URL
- 〔オプション] Application Load Balancer (ALB) Ingress Controller サービスをデプロイする Amazon EKS クラスター名前空間。〔デフォルト: kube-system]
- 〔オプション] Amazon EKS クラスターサービスアカウント (SA) 名。〔デフォルト: aws-load-balancer-controller]

クラスターでエンベロープシークレットの暗号化を有効にする場合は (推奨) 、使用する KMS キー IDs を RFC の説明フィールドに入力してサービスを追加します (Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct)。エンベロープ暗号化の詳細については、「Amazon EKS adds envelope encryption for secrets with AWS KMS」を参照してください。

AMS SSP を使用して AMS アカウントに Amazon EMR をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon EMR 機能に直接アクセスします。Amazon EMR は、Apache Spark、Apache Hive、Apache HBase、Apache Flink、Apache Hudi、Presto などのオープンソースツールを使用して大量のデータを処理するための、業界をリードするクラウドビッグデータプラットフォームです。Amazon EMR を使用すると、従来のオンプレミスソリューションのコストの半分未満で、標準の Apache Spark の 3 倍以上の速度で Petabyte スケール分析を実行できます。実行時間の短いジョブでは、クラスターをスピンアップおよびスピンダウンし、使用したインスタンスに対して 1 秒あ

たりの料金を支払うことができます。長時間実行されるワークロードの場合、需要に合わせて自動的にスケーリングする高可用性クラスターを作成できます。

Amazon EMR クラスターの 1 つ以上のインスタンスを AMS マルチアカウントランディングゾーンまたはシングルアカウントランディングゾーンアカウントに作成して、一時的および永続的な Amazon EMR クラスターの両方をサポートできます。Kerberos 認証を有効にして、オンプレミスの Active Directory ドメインからユーザーを認証することもできます。

Amazon EMR クラスターで複数のデータストアを活用して、ユースケース固有の Hadoop ツールとライブラリをサポートできます。Amazon EMR クラスターは、OnDemandインスタンスまたはスポットインスタンスを使用して作成し、容量を管理し、コストを削減するように自動スケーリングを設定できます。

クラスターログファイルは、ログ記録とデバッグのために Amazon S3 バケットにアーカイブできます。Amazon EMR クラスターでホストされているウェブインターフェイスにアクセスして、hadoop 管理要件をサポートしたり、顧客のノートブックエクスペリエンスをサポートしたりすることもできます。

詳細については、「Amazon EMR」を参照してください。

AWS Managed Services での Amazon EMR に関するよくある質問

Q: AMS アカウントの Amazon EMR へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (レビューが必要) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、次の IAM ロールをアカウントにプロビジョニングします。

- `customer_emr_cluster_instance_profile`
- `customer_emr_cluster_autoscaling_role`
- `customer_emr_console_role`
- `customer_emr_cluster_service_role`

アカウントにプロビジョニングされたら、フェデレーションソリューションで customer_emr_console_role をオンボードする必要があります。

Q: AMS アカウントでの Amazon EMR の使用にはどのような制限がありますか？

AWS コンソールから EC2 クラスターに Amazon EMR を作成するときは、クラスターの作成 – 詳細オプションを使用することをお勧めします。Amazon EMR クラスターは、キーがfor-use-with-

amazon-emr-managed-policies」、値が「true」のタグを追加して作成する必要があります。セキュリティオプションで次の設定を選択します。

- クラスターのカスタムロールを選択します。
  - EMR ロール: customer_emr_cluster_service_role
  - EC2 インスタンスプロファイル: customer_emr_cluster_instance_profile
  - Auto Scaling ロール: customer_emr_cluster_autoscaling_role
- EC2 セキュリティグループ：
  - マスター : ams-emr-master-security-group
  - コアとタスク: ams-emr-worker-security-group
  - サービスアクセス: ams-emr-serviceaccess-security-group

Q: AMS アカウントで Amazon EMR を使用するための前提条件または依存関係は何ですか？

AMS は、Amazon EMR マスター、ワーカー、およびサービスノードのデフォルトのセキュリティグループを作成します。

Amazon EMR クラスターで使用する起動テンプレートとセキュリティグループには、値「true」のタグキーfor-use-with-amazon-emr-managed-policies」が必要です。

デフォルトの Amazon EMR クラスターインスタンスプロファイルでは、名前に「emr」が含まれている s3 バケットや dynamodb テーブルなどのリソースにアクセスできます。Amazon EMR で使用する追加のリソースを使用するための追加の IAM ポリシーをリクエストできます。customer_emr_cluster_instance_profile を使用して Amazon EMR ジョブで次のリソース ARN を使用できます。

- arn:aws:dynamodb:*:*:table/*emr*
- arn:aws:kinesis:*:*:stream/*emr*
- arn:aws:sns:*:*:*emr*arn:aws:sqs:*:*:*emr*
- arn:aws:sqs:*:*:*emr*
- arn:aws:sqs:*:*:AWS-ElasticMapReduce-*
- arn:aws:sdb:*:*:domain:*emr*
- arn:aws:s3:::*emr*

Amazon EMR クラスターに kerberos 認証が必要な場合：

- カーベライズされた各 Amazon EMR クラスターに使用する領域名とオンプレミスの Active Directory IP アドレスを指定します。
- インフラストラクチャ要件：

  マルチアカウントランディングゾーン (MALZ): RFC を送信して、新しいマネージドアプリケーションアカウントまたは既存のアプリケーションアカウントに新しい VPC を作成します。

  単一アカウントランディングゾーン (SALZ): RFC を送信して VPC に新しいサブネットを作成します。
- オンプレミス Active Directory でクラスターの領域に対する受信信頼を設定します。
- マネージド AD の領域に DNS ゾーンを設定するには、RFC を送信します。
- 領域設定：

  MALZ: 管理 | その他 | その他 | 更新 (ct-0xdawir96cy7k) RFC を送信して、ドメイン名のサフィックスに領域名を使用するように設定された VPC DHCP オプションを更新します。

  SALZ: 管理 | その他 | その他 | 更新 (ct-0xdawir96cy7k) RFC を送信して、ドメイン名のサフィックスに特定の領域を使用する新しい Amazon EMR AMI を生成します。

Amazon EMR Studio をデプロイするには、ロールに Amazon Simple Storage Service バケットの前提条件`customer_emr_cluster_service_role`があります。バケットを作成するには、自動 CT `ct-1a68ck03fn98r` (デプロイ | 高度なスタックコンポーネント | S3 ストレージ | 作成) を使用します。この自動 CT を使用して Amazon EMR 用の Amazon S3 バケットを作成する場合、バケット名はプレフィックス で始まる必要がありま`customer-emr-*`す。また、Amazon EMR クラスターと同じ AWS リージョンにバケットを作成する必要があります。

AMS SSP を使用して AMS アカウントに Amazon EventBridge をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon EventBridge 機能に直接アクセスします。Amazon EventBridge は、アプリケーションをさまざまなイベントソースのデータに簡単に接続できるようにするサーバーレスイベントバスサービスです。EventBridge は、独自のアプリケーション、Software-as-a-Service (SaaS) アプリケーション、および AWS のサービスからリアルタイムデータのストリームを配信し、そのデータを などのターゲットにルーティングします AWS Lambda。お客様は、データの送信先を判断するためのルーティングルールを設定して、すべてのデータソースにリアルタイムで反応するアプリケーションアー

キテクチャを構築できます。EventBridge を使用すると、疎結合かつ分散型のイベント駆動型アーキテクチャの構築が可能になります。

詳細については、「Amazon EventBridge」を参照してください。

AWS Managed Services の EventBridge に関するよくある質問

Q: AMS アカウントの EventBridge へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (ct-1w8z66n899dct) 変更タイプで RFC を送信して EventBridge へのアクセスをリクエストします。この RFC は、`customer_eventbridge_role`および の IAM ロールをアカウントにプロビジョニングしますcustomer_eventbridge_scheduler_execution_role。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

実行ロール`customer_eventbridge_scheduler_execution_role`は、EventBridge スケジューラが AWS のサービス ユーザーに代わって他の とやり取りするために引き受ける IAM ロールです。このロールにアタッチされたアクセス許可ポリシーはEventBridge スケジューラにターゲットを呼び出すためのアクセス許可を付与します。

> **Note**
>
> デフォルトでは、EventBridge スケジューラは EventBridge の AWS 所有キーを使用してデータを暗号化します。EventBridge のカスタマーマネージドキーを使用してデータを暗号化するには、 管理 | AWS サービス | セルフプロビジョニングサービス | サービスプロビジョニング用の変更タイプ (ct-3qe6io8t6jtny) を追加 (レビューが必要) を使用して RFC を送信します。

Q: AMS アカウントでの EventBridge の使用にはどのような制限がありますか？

AMS RFCs を送信し、次のリソースを作成する必要があります。バッチジョブ、SQS キュー、CodeBuild、CodePipeline、SSM コマンドをトリガーするサービスロール。

Q: AMS アカウントで EventBridge を使用するための前提条件または依存関係は何ですか？

EventBridge を使用して Lambda、Amazon SNS、Amazon SQS AWS Batch、Amazon CloudWatch Logs リソースなどの他の AWS リソースをトリガーする前に、デプロイ | 高度なスタックコンポーネント | Identity and Access Management (IAM) | Create entity or policy (review required) change type (ct-3dpd8mdd9jn1r) を使用して RFC で EventBridge サービスロールをリクエストする必要が

あります。 Amazon SNS サービスロールをリクエストするときに呼び出すサービスを指定します。ターゲットの呼び出しに必要なアクセス許可については、EventBridge のリソースベースのポリシーの使用」を参照してください。

EventBridge は AWS CloudTrail、EventBridge のユーザー、ロール、または によって実行されたアクションを記録するサービスEventBridgeと統合 AWS のサービス されています。CloudTrail を有効にして、ログファイルを S3 バケットに保存できるようにする必要があります。注: すべての AMS アカウントで CloudTrail が有効になっているため、アクションは必要ありません。

Q: ロール customer_eventbridge_scheduler_execution_role には、 AWS Key Management Service キーの前提条件があります (暗号化に使用される場合はオプション) 。保管時/転送時のデータ暗号化に AWS KMS CMKs を採用するにはどうすればよいですか ?

デフォルトでは、EventBridge スケジューラは、 AWS 所有キー (保管時の暗号化) に保存するイベントメタデータとメッセージデータを暗号化します。EventBridge スケジューラは、Transport Layer Security (TLS) (転送中の暗号化) を使用して、EventBridge スケジューラと他の サービスの間を通過するデータも暗号化します。

特定のユースケースで、EventBridge スケジューラでデータを保護する暗号化キーを管理および監査する必要がある場合は、カスタマーマネージドキーを使用できます。

Amazon EventBridge を使用してアクセス AWS KMS 許可をオンボードする前に、 管理 | AWS のサービス | セルフプロビジョニングサービス | 追加 (レビューが必要) 変更タイプを使用して RFC をリクエストする必要があります。

AMS SSP を使用して AMS アカウントに Amazon Forecast をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Forecast (Forecast) 機能に直接アクセスします。Amazon Forecast は、機械学習を使用して高精度の予測を提供するフルマネージドサービスです。

> **Note**
>
> AWS は、2024 年 7 月 29 日に Amazon Forecast への新しい顧客アクセスを閉鎖しました。Amazon Forecast の既存のお客様は、通常どおりサービスを引き続き使用できます。AWS は引き続き Amazon Forecast のセキュリティ、可用性、パフォーマンスの向上に投資しますが、新機能を導入する予定 AWS はありません。

Amazon Forecast を使用する場合は、CSDM に連絡して、Amazon Forecast の使用を Amazon SageMaker Canvas に移行する方法について詳しく説明してもらいます。

Amazon.com で使用されているのと同じテクノロジーに基づいて、Forecast は機械学習を使用して時系列データと追加の変数を組み合わせて予測を構築します。Forecast では、開始するために機械学習の経験は必要ありません。履歴データに加えて、予測に影響を与える可能性があると思われる追加データを提供するだけで済みます。例えば、シャツの特定の色の需要は、季節や店舗の場所によって変わる可能性があります。この複雑な関係を単独で判断することは困難ですが、機械学習はそれを認識するのに最適です。データを指定すると、Forecast はデータを自動的に調査し、意味のあるものを特定し、時系列データだけを見るよりも最大 50% 正確な予測を行うことができる予測モデルを生成します。

詳細については、「Amazon Forecast」を参照してください。

AWS Managed Services での Amazon Forecast に関するよくある質問

Q: AMS アカウントの Forecast へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) change type を使用して RFC を送信 AWS Firewall Manager して、 へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_forecast_admin_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントで Forecast を使用することにはどのような制限がありますか？

デフォルトの S3 バケットアクセスでは、「customer-forecast-*」という名前のバケットにのみアクセスできます。データバケットの独自の命名規則がある場合は、Cloud Architect (CA) でバケットの命名と関連するアクセス設定について説明します。例:

- 「AmazonForecast-ExecutionRole-*」などの名前と、関連する適切な S3 バケットアクセスを使用して、特定の Amazon Forecast サービスロールを定義できます。 ExecutionRole S3 IAM コンソールの「サービスロール - AmazonForecast-ExecutionRole-Admin」および「IAM ポリシー - customer_forecast_default_s3_access_policy」を参照してください。
- 関連する S3 バケットアクセスを IAM フェデレーションロールに関連付ける必要がある場合があります。IAM コンソールの「IAM ポリシー - customer_forecast_default_s3_access_policy」を参照してください。

Q: AMS アカウントで Forecast を使用するための前提条件または依存関係は何ですか？

- Forecast を使用する前に、適切な Amazon S3 バケット (複数可) を作成する必要があります。特に、デフォルトの S3 バケットアクセスは命名パターン「customer-forecast-*」です。
- 「customer-forecast-*」以外の S3 バケットに命名パターンを使用する場合は、バケットに対する S3 アクセス許可を持つ新しいサービスロールを作成する必要があります。
  1. 「AmazonForecast-ExecutionRole-{suffix}'」という名前で作成される新しいサービスロール。
  2. customer_forecast_default_s3_access_policy に似ており、新しいサービスロールおよび関連するフェデレーション管理者ロール (「customer_forecast_admin_role」など) に関連付けられている新しい IAM ポリシーを作成する

Q: Amazon Forecast の使用中にデータセキュリティを強化するにはどうすればよいですか？

- 保管中のデータ暗号化の場合、 AWS KMS を使用してカスタマー管理の CMK をプロビジョニングし、Amazon S3 サービス上のデータストレージを保護できます。
  - プロビジョニングキーを使用してバケットでデフォルトの暗号化を有効にし、データの配置中に AWS KMS データ暗号化を受け入れるようにバケットポリシーを設定します。
  - AWS KMS キーユーザーとして Amazon Forecast サービスロールAmazonForecast-ExecutionRole-*」とフェデレーション管理者ロール (「customer_forecast_admin_role」など) を有効にします。
- 転送中のデータ暗号化の場合、Amazon S3 バケットポリシーでオブジェクトを転送するときに必要な HTTPS プロトコルを設定できます。
- アクセスコントロールのさらなる制限により、Amazon Forecast サービスロールAmazonForecast-ExecutionRole-*」と管理者ロール (「customer_forecast_admin_role」など) の承認済みアクセスのバケットポリシーを有効にします。

Q: Amazon Forecast を使用する際のベストプラクティスは何ですか？

- Amazon Forecast で S3 バケットを使用する際は、データ分類のプラクティスを十分に理解し、関連するデータセキュリティのニーズをマッピングする必要があります。
- Amazon S3 バケット設定では、S3 バケットポリシーで HTTPS 適用を有効にすることを強くお勧めします。
- Amazon S3 バケットに対する「customer-forecast_admin_role」サポートの管理者ロール「customer-forecast-*」という名前のアクセス許可 (Get/Delete/Put Amazon S3 オブジェクト) に

注意する必要があります。注: 複数のチームにきめ細かなアクセスコントロールが必要な場合は、次のプラクティスに従ってください。

- 関連する Amazon S3 バケットへの最小特権アクセスを持つチームベースのアクセス IAM ID (ロール/ユーザー) を定義します。
- チーム/プロジェクトベースの AWS KMS CMKs対応する IAM ID への適切なアクセスが許可されます (ユーザーアクセスとAmazonForecast-ExecutionRole-{team/project}'。
- 作成したCMK を使用して S3 バケットのデフォルトの暗号化を設定します。 AWS KMS CMKs
- S3 バケットポリシーで HTTPS プロトコルを使用して S3 API トラフィックを強制します。
- 関連する IAM ID (ユーザーアクセスとAmazonForecast-ExecutionRole-{team/project}」がバケットに承認されたアクセスのために S3 バケット設定を適用します。

- 汎用に「customer_forecast_admin_role」を使用する場合は、前述のポイントを考慮して S3 バケットを保護します。

Q: Amazon Forecast に関するコンプライアンス情報はどこにありますか？

「 AWS サービスコンプライアンスプログラム」を参照してください。

AMS SSP を使用して AMS アカウントに Amazon FSx をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon FSx 機能に直接アクセスします。Amazon FSx は、フルマネージド型のサードパーティーファイルシステムを提供します。Amazon FSx は、Windows ベースのストレージ、ハイパフォーマンスコンピューティング (HPC)、機械学習、電子設計自動化 (EDA) などのワークロード用の機能セットを備えたサードパーティーのファイルシステムのネイティブ互換性を提供します。Amazon FSx は、ハードウェアのプロビジョニング、ソフトウェア設定、パッチ適用、バックアップなど、時間のかかる管理タスクを自動化します。Amazon FSx は、ファイルシステムをクラウドネイティブ AWS サービスと統合するため、より広範なワークロードのセットでさらに役立ちます。

Amazon FSx には、Windows ベースのアプリケーション用の Amazon FSx for Windows File Server と、コンピューティング負荷の高いワークロード用の Amazon FSx for Lustre の 2 つのファイルシステムがあります。詳細については、「Amazon FSx」を参照してください。

AWS Managed Services での Amazon FSx に関するよくある質問

Q: AMS アカウントの Amazon FSx へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (ct-1w8z66n899dct) 変更タイプで RFC を送信して、Amazon FSx へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_fsx_admin_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon FSx の使用にはどのような制限がありますか？

制限はありません。サービスの完全な機能を利用できます。

Q: AMS アカウントで Amazon FSx を使用するための前提条件または依存関係は何ですか？

前提条件はありません。ただし、マルチ AZ などの事前設定を行うには、DFS レプリケーションおよび DFS 名前空間サービスをインストールおよび管理する必要があります。詳細については、「マルチ AZ ファイルシステムのデプロイ」を参照してください。

Q: Amazon FSx ファイルシステムをマルチアカウントランディングゾーン Managed AD と統合するにはどうすればよいですか？

Amazon FSx ファイルシステムを作成するときは、MALZ Managed AD を Windows 認証用のAWS「マネージド Microsoft Active Directory」として指定できます。詳細については、「Microsoft Active Directory での Amazon FSx の使用 AWS Directory Service」を参照してください。

また、最初に Managed AD をアプリケーションアカウントと共有する必要があります。これを行うには、Management | Directory Service | Directory | Share directory change type (ct-369odosk0pd9w) を使用して RFC を送信します。

Q: AWS 委任 FSx 管理者グループに属するユーザーはどれですか？

IT ファイルサーバー管理者のみ。このグループには、すべてのファイル共有に対するフルアクセス権限があります。

Q: FSx システムがプロビジョニングされたときに作成されるデフォルトのファイル共有、共有を使用する必要がありますか？

いいえ。プロビジョニングされたデフォルトのファイル共有、共有を使用することはお勧めしません。すべてのユーザーにフルアクセスを付与します。これは最小特権の原則に違反します。代わりに、ビジネスニーズに合った小さなカスタムファイル共有を作成します。

Q: ビジネス内の特定の組織のカスタムファイル共有を作成するにはどうすればよいですか？

カスタムファイル共有の作成手順については、「ファイル共有」を参照してください。最小特権の原則を使用して、各ファイル共有へのアクセスを制限します。

AMS SSP を使用して AMS アカウントで Amazon FSx for OpenZFS をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon FSx for OpenZFS 機能に直接アクセスします。FSx for OpenZFS は、フルマネージド型のファイルストレージサービスです。これにより、アプリケーションコードやデータ管理方法を変更することなく、オンプレミスの ZFS やその他の Linux ベースのファイルサーバーにあるデータを AWS に簡単に移動できます。オープンソースの OpenZFS ファイルシステム上に構築された、信頼性、スケーラビリティ、パフォーマンス、機能豊富なファイルストレージを提供し、OpenZFS ファイルシステムの使い慣れた機能と機能に、フルマネージド AWS サービスの俊敏性、スケーラビリティ、シンプルさを提供します。クラウドネイティブアプリケーションを構築するデベロッパー向けに、データを操作するための豊富な機能を備えたシンプルで高性能なストレージを提供します。

FSx for OpenZFS ファイルシステムは、業界標準の NFS プロトコル (v3、v4.0、v4.1、v4.2) を使用して、Linux、Windows、macOS コンピューティングインスタンスおよびコンテナから広くアクセスできます。Graviton AWS プロセッサと最新の AWS ディスクおよびネットワークテクノロジー (AWS スケーラブルな信頼性の高い Datagram ネットワークと AWS Nitro システムを含む) を搭載した FSx for OpenZFS は、数百マイクロ秒のレイテンシーで最大 100 万 IOPS を提供します。FSx for OpenZFS は、インスタンpoint-in-timeスナップショットやデータクローニングなどの OpenZFS 機能を完全にサポートしているため、オンプレミスのファイルサーバーを使い慣れたファイルシステム機能を提供する AWS ストレージに簡単に置き換えることができるため、長時間の認定や既存のアプリケーションやツールの変更や再設計を行う必要がなくなります。 OpenZFS また、OpenZFS データ管理機能の能力と最新の AWS テクノロジーの高パフォーマンスとコスト効率を組み合わせることで、FSx for OpenZFS では、高性能でデータ集約型のアプリケーションを構築して実行できます。

フルマネージドサービスである FSx for OpenZFS を使用すると、オンプレミスで実行しているファイルサーバーを置き換え AWS るフルマネージドファイルシステムの起動、実行、スケーリングが簡単になり、俊敏性とコスト削減に役立ちます。FSx for OpenZFS を使用すると、ファイルサーバーとストレージボリュームのセットアップとプロビジョニング、データのレプリケーション、ファイルサーバーソフトウェアのインストールとパッチ適用、ハードウェア障害の検出と対処、バックアップの手動実行について心配する必要がなくなりました。また、 AWS Identity and Access Management (IAM)、 AWS Key Management Service ()、AWS KMS Amazon CloudWatch、 などの他の AWS サービスとの豊富な統合も提供します AWS CloudTrail。

Amazon FSx には、Windows ベースのアプリケーション用の Amazon FSx for Windows File Server と、コンピューティング負荷の高いワークロード用の Amazon FSx for Lustre の 2 つのファイルシステムがあります。詳細については、「Amazon FSx」を参照してください。

AWS Managed Services での Amazon FSx for OpenZFS に関するよくある質問

Q: AMS アカウントで FSx for OpenZFS を使用するためのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (ct-1w8z66n899dct) 変更タイプで RFC を送信して、Amazon FSx OpenZFS へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_fsx_ontap_admin_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントで FSx for OpenZFS を使用することにはどのような制限がありますか？

Amazon FSx Elastic Network Interface (ENIs) のセキュリティグループを置き換えるには、管理 | その他 | その他 | RFCs を更新する必要があります。これは、セキュリティグループが AMS 環境にとって重要な境界であるためです。これが唯一の制限です。

Q: AMS アカウントで FSx for OpenZFS を使用するための前提条件または依存関係は何ですか？

前提条件はありません。ただし、 AMS SSP を使用して AMS アカウントに Amazon FSx をプロビジョニングするがインストールされている必要があります。

AMS SSP を使用して AMS アカウントで Amazon FSx for NetApp ONTAP をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon FSx for NetApp ONTAP 機能に直接アクセスします。Amazon FSx for NetApp ONTAP は、NetApp の人気ある ONTAP ファイルシステム上に構築された、高い信頼性、拡張性、パフォーマンス、機能豊富なファイルストレージを提供するフルマネージド型サービスです。NetApp ファイルシステムの使い慣れた機能、パフォーマンス、機能、APIs に、フルマネージド型の の俊敏性、スケーラビリティ、シンプルさを提供します AWS のサービス。

Amazon FSx for NetApp ONTAP は、 AWS またはオンプレミスで実行されている Linux、Windows、macOS コンピューティングインスタンスから幅広くアクセスできる、機能豊富で高速、柔軟な共有ファイルストレージを提供します。FSx for ONTAP は、ミリ秒未満のレイテンシーを備えた高性能 SSD ストレージを提供し、ボタンをクリックするだけでファイルのスナップショット作成、クローン作成、複製を行えるため、データをすばやく簡単に管理できます。また、データを低コストで伸縮性のあるストレージに自動的に階層化することで、容量のプロビジョニン

グや管理が不要になり、ごく一部のデータに対して SSD ストレージの費用を支払うのみで、ワークロードに対して SSD レベルのパフォーマンスを実現することができます。フルマネージドバックアップとクロスリージョン災害対策のサポートにより、可用性と耐久性に優れたストレージを提供し、一般的なデータセキュリティおよびアンチウイルスアプリケーションをサポートし、データの保護とセキュリティをさらに容易にします。NetApp ONTAP をオンプレミスで使用するお客様にとって、FSx for ONTAP は、アプリケーションコードやデータの管理方法を変更 AWS することなく、ファイルベースのアプリケーションをオンプレミスから に移行、バックアップ、またはバーストするための理想的なソリューションです。

フルマネージドサービスとして、Amazon FSx for NetApp ONTAP は、クラウドでの信頼性、パフォーマンス、安全な共有ファイルストレージを簡単に起動および拡張できます。Amazon FSx for NetApp ONTAP を使用すると、ファイルサーバーとストレージボリュームの設定とプロビジョニング、データのレプリケーション、ファイルサーバーソフトウェアのインストールとパッチ適用、ハードウェア障害の検出と対応、フェイルオーバーとフェイルバックの管理、バックアップの手動実行について心配する必要がなくなります。また、Amazon WorkSpaces AWS のサービスや AWS Identity and Access Managementなど AWS Key Management Service、他の との豊富な統合も提供します AWS CloudTrail。

Amazon FSx には、Windows ベースのアプリケーション用の Amazon FSx for Windows File Server と、コンピューティング負荷の高いワークロード用の Amazon FSx for Lustre の 2 つのファイルシステムがあります。詳細については、「Amazon FSx」を参照してください。

AWS Managed Services の Amazon FSx for NetApp ONTAP に関するよくある質問

Q: AMS アカウントで Amazon FSx for NetApp ONTAP へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (ct-1w8z66n899dct) 変更タイプで RFC を送信して、Amazon FSx for NetApp ONTAP へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_fsx_ontap_admin_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントで Amazon FSx for NetApp ONTAP を使用することにはどのような制限がありますか？

Amazon FSx for NetApp ONTAP Elastic Network Interface (ENIs) のセキュリティグループを置き換えるには、管理 | その他 | その他 | RFCs を更新する必要があります。これは、セキュリティグループが AMS 環境にとって重要な境界であるためです。これが唯一の制限です。

Q: AMS アカウントで Amazon FSx for NetApp ONTAP を使用するための前提条件または依存関係は何ですか？

前提条件はありません。ただし、 AMS SSP を使用して AMS アカウントに Amazon FSx をプロビジョニングするがインストールされている必要があります。

AMS SSP を使用して AMS アカウントに Amazon Inspector Classic をプロビジョニングする

> **Note**
>
> サポート終了通知: 2026 年 5 月 20 日に、 AWS は Amazon Inspector Classic のサポートを終了します。2026 年 5 月 20 日以降、Amazon Inspector Classic コンソールまたは Amazon Inspector Classic リソースにアクセスできなくなります。Amazon Inspector Classic は、新しいアカウント、および過去 6 か月間に評価を完了していないアカウントで利用できなくなります。他のすべてのアカウントでは、アクセスは 2026 年 5 月 20 日まで有効です。その後、Amazon Inspector Classic コンソールまたは Amazon Inspector Classic リソースにアクセスできなくなります。詳細については、Amazon Inspector Classic のサポート終了」を参照してください。

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Inspector Classic 機能に直接アクセスします。Amazon Inspector Classic は、デプロイされたアプリケーションのセキュリティとコンプライアンスを向上させるのに役立つ自動セキュリティ評価サービスです AWS。Amazon Inspector Classic は、アプリケーションの露出、脆弱性、ベストプラクティスからの逸脱を自動的に評価します。評価を実行すると、Amazon Inspector Classic は重要度レベル別に優先順位が付けられたセキュリティ検出結果の詳細なリストを作成します。これらの検出結果は、直接レビューすることも、Amazon Inspector Classic コンソールまたは API から入手できる詳細な評価レポートの一部としてレビューすることもできます。詳細については、Amazon Inspector Classic」を参照してください。

AWS Managed Services の Amazon Inspector に関するよくある質問

Q: AMS アカウントで Amazon Inspector Classic へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) 変更タイプで RFC を送信して、Amazon Inspector Classic へのアクセスをリクエストします。この RFC は、IAM

customer_inspector_admin_role ロールをアカウントにプロビジョニングします。ロールには AWS、 管理の AmazonInspectorFullAccess ポリシーが含まれます。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon Inspector Classic の使用にはどのような制限がありますか？

制限はありません。Amazon Inspector Classic の全機能は、AMS アカウントで使用できます。

Q: AMS アカウントで Amazon Inspector Classic を使用するための前提条件または依存関係は何ですか？

AMS アカウントで Amazon Inspector Classic を使用するための前提条件や依存関係はありません。

AMS で新しい Amazon Inspector を使用する

AMS アカウントで新しい Amazon Inspector を使用できるようになりました。

Amazon Inspector Classic では、 customer-inspector-admin-role-ssm-inspector-agent-policyと が必要AmazonInspectorFullAccessでした。ただし、SSPS ロール が更新されcustomer-inspector-admin-role、追加の が含まれるようになりましたpolicyAmazonInspector2FullAccess。この新しいポリシーは、Amazon Inspector の新しいバージョンの API アクセス許可を付与します。

AMS SSP を使用して AMS アカウントに Amazon Kendra をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Kendra 機能に直接アクセスします。Amazon Kendra は、自然言語処理と高度な機械学習アルゴリズムを使用して、データからの検索質問に対する特定の回答を返すインテリジェントな検索サービスです。従来のキーワードベースの検索とは異なり、Amazon Kendra はセマンティックおよびコンテキスト理解機能を使用して、ドキュメントが検索クエリに関連しているかどうかを判断します。Amazon Kendra は質問に対する特定の回答を返すため、エクスペリエンスは人間の専門家とのやり取りに近いです。Amazon Kendra はスケーラビリティが高く、パフォーマンスの需要を満たすことができ、Amazon S3 や Amazon Lex などの他の AWS サービスと緊密に統合されており、エンタープライズレベルのセキュリティを提供します。詳細については、「Amazon Kendra;」を参照してください。

AWS Managed Services の Amazon Kendra に関するよくある質問

Q: AMS アカウントの Amazon Kendra へのアクセスをリクエストするにはどうすればよいですか？

Amazon Inspector Classic へのアクセスをリクエストするには、 Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny) 変更タイプを使用して RFC を送信します。この RFC は、IAM `customer_kendra_console_role` ロールをアカウントにプロビジョニングします。アカウントでプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon Kendra の使用にはどのような制限がありますか？

制限はありません。Amazon Kendra の完全な機能は、AMS アカウントで使用できます。

Q: AMS アカウントで Amazon Kendra を使用するための前提条件または依存関係は何ですか？

Amazon Kendra の使用を開始するための前提条件や依存関係はありません。ただし、特定のユースケースによっては、他の AWS サービスへのアクセスが必要になる場合があります。

AMS SSP を使用して AMS アカウントに Amazon Kinesis Data Streams をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Kinesis Data Streams (KDS) 機能に直接アクセスします。Amazon Kinesis Data Streams は、スケーラビリティと耐久性に優れたリアルタイムのデータストリーミングサービスです。KDS は、ウェブサイトのクリックストリーム、データベースイベントストリーム、金融取引、ソーシャルメディアフィード、IT ログ、位置追跡イベントなど、数十万のソースから 1 秒あたり数ギガバイトのデータを継続的にキャプチャできます。収集されたデータはミリ秒単位で利用でき、リアルタイムダッシュボード、リアルタイム異常検出、動的料金設定などのリアルタイム分析のユースケースを可能にします。詳細については、Amazon Kinesis Data Streams」を参照してください。

AWS Managed Services での Kinesis Data Streams に関するよくある質問

よくある質問と回答：

Q: AMS アカウントの Amazon Kinesis Data Streams へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 変更タイプを追加 (ct-1w8z66n899dct) で RFC を送信して、Amazon Kinesis Data Streams へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_kinesis_data_streaming_user_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon Kinesis Data Streams の使用にはどのような制限がありますか？

制限はありません。Amazon Kinesis Data Streams のフル機能は、AMS アカウントで使用できます。

Q: AMS アカウントで Amazon Kinesis Data Streams を使用するための前提条件または依存関係は何ですか？

AMS アカウントで Amazon Kinesis Data Streams を使用するための前提条件や依存関係はありません。

AMS SSP を使用して AMS アカウントに Amazon Kinesis Video Streams をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Kinesis Video Streams (KVS) 機能に直接アクセスします。Amazon Kinesis Video Streams を使用すると、接続されたデバイスから にビデオを安全にストリーミングして、 AWS 分析、機械学習 (ML)、再生、その他の処理を行うことができます。Kinesis Video Streams は、何百万ものデバイスからストリーミングビデオデータを取り込むために必要なすべてのインフラストラクチャを自動的にプロビジョニングし、伸縮自在にスケーリングします。また、ビデオデータをストリームに永続的に保存、暗号化、インデックス化し、easy-to-use APIs を介してデータにアクセスできます。Kinesis Video Streams を使用すると、ライブおよびオンデマンド視聴用の動画を再生し、Amazon Rekognition Video との統合、および Apache MxNet、TensorFlow、OpenCV などの ML フレームワーク用のライブラリを通じて、コンピュータビジョンと動画分析を活用するアプリケーションをすばやく構築できます。詳細については、Amazon Kinesis Video Streams」を参照してください。

AWS Managed Services での Amazon Kinesis Video Streams に関するよくある質問

よくある質問と回答：

Q: AMS アカウントの Amazon Kinesis Video Streams へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 変更タイプの追加 (ct-1w8z66n899dct) で RFC を送信して、Amazon Kinesis Video Streams へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_kinesis_video_streaming_user_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon Kinesis Video Streams の使用にはどのような制限がありますか？

制限はありません。Amazon Kinesis Video Streams の全機能は、AMS アカウントで使用できます。

Q: AMS アカウントで Amazon Kinesis Video Streams を使用するための前提条件または依存関係は何ですか？

AMS アカウントで Amazon Kinesis Video Streams を使用するための前提条件や依存関係はありません。

AMS SSP を使用して AMS アカウントに Amazon Lex をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Lex 機能に直接アクセスします。Amazon Lex は、音声とテキストを使用して会話型インターフェイスを任意のアプリケーションに構築するためのサービスです。Amazon Lex は、音声をテキストに変換するための自動音声認識 (ASR) の高度な深層学習機能と、テキストの意図を認識するための自然言語理解 (NLU) を提供し、非常に魅力的なユーザーエクスペリエンスとリアルな会話インタラクションでアプリケーションを構築できるようにします。Amazon Lex では、Amazon Alexa を強化するのと同じ深層学習テクノロジーをすべての開発者が利用できるようになりました。これにより、洗練された自然言語の会話ボットやチャットボットを迅速かつ簡単に構築できます。詳細については、Amazon Lex」を参照してください。

AWS Managed Services の Amazon Lex に関するよくある質問

よくある質問と回答：

Q: AMS アカウントの Amazon Lex へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add change type (ct-1w8z66n899dct) を送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_lex_author_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon Lex の使用にはどのような制限がありますか？

Amazon Lex と Lambda の統合は、AMS インフラストラクチャへの変更を防ぐために、「AMS-」プレフィックスのない Lambda 関数に制限されています。

Q: AMS アカウントで Amazon Lex を使用するための前提条件または依存関係は何ですか？

AMS アカウントで Amazon Lex を使用するための前提条件や依存関係はありません。

AMS SSP を使用して AMS アカウントに Amazon MQ をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon MQ 機能に直接アクセスします。Amazon MQ は Apache ActiveMQ のマネージドメッセージブローカーサービスで、クラウドでのメッセージブローカーのセットアップと運用に役立ちます。メッセージブローカーを使用すると、多くの場合、異なるプログラミング言語と異なるプラットフォームで異なるソフトウェアシステムを使用して、情報を通信および交換できます。Amazon MQ は、一般的なオープンソースメッセージブローカーである ActiveMQ のプロビジョニング、セットアップ、メンテナンスを管理することで、運用負荷を軽減します。現在のアプリケーションを Amazon MQ に接続すると、JMS、NMS、AMQP、STOMP、MQTT、WebSocket などの業界標準 APIs とプロトコルがメッセージングに使用されます。標準を使用すると、ほとんどの場合、移行時にメッセージングコードを書き直す必要はありません AWS。詳細については、Amazon MQ とは」を参照してください。

AWS Managed Services の Amazon MQ に関するよくある質問

よくある質問と回答：

Q: AMS アカウントの Amazon MQ へのアクセスをリクエストするにはどうすればよいですか？

AMS アカウントでの Amazon MQ の使用には、次の 2 つのステップがあります。

1. Amazon MQ ブローカーをプロビジョニングします。これを行うには、Amazon MQ ブローカーを含む CFN テンプレートを、デプロイ | Ingestion | Stack from CloudFormation Template | Create change type (ct-36cn2avfrrj9v) の RFC を通じて送信するか、Management | Other | Other | Create change type (ct-1e1xtak34nx76) change type を使用して RFC を送信してAmazon MQ ブローカーをアカウントでプロビジョニングするようにリクエストします。
2. Amazon MQ コンソールにアクセスします。Amazon MQ ブローカーがプロビジョニングされたら、 Management | AWS service | Self-provisioned service | Add change type (ct-1w8z66n899dct) で RFC を送信して Amazon MQ コンソールへのアクセスを取得します。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_mq_console_role`。

アカウントでロールがプロビジョニングされたら、フェデレーションソリューションにロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon MQ の使用にはどのような制限がありますか？

Amazon MQ の完全な機能は AMS アカウントで使用できますが、必要なアクセス許可が昇格しているため、ポリシーを通じて Amazon MQ ブローカーをプロビジョニングすることはできません。アカウントで Amazon MQ ブローカーをプロビジョニングする方法の詳細については、上記を参照してください。

Q: AMS アカウントで Amazon MQ を使用する際の前提条件または依存関係は何ですか？

AMS アカウントで Amazon MQ を使用するための前提条件や依存関係はありません。

AMS SSP を使用して AMS アカウントで Amazon Managed Service for Apache Flink をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Managed Service for Apache Flink 機能に直接アクセスします。Managed Service for Apache Flink は、ストリーミングデータを分析し、実用的なインサイトを取得し、ビジネスと顧客のニーズにリアルタイムで対応するための最も簡単な方法です。Amazon Managed Service for Apache Flink は、ストリーミングアプリケーションの構築、管理、他の AWS サービスとの統合の複雑さを軽減します。SQL ユーザーは、 テンプレートとインタラクティブな SQL エディタを使用して、ストリーミングデータのクエリやストリーミングアプリケーション全体の構築を簡単に行うことができます。Java 開発者は、オープンソースの Java ライブラリと AWS 統合を使用して高度なストリーミングアプリケーションをすばやく構築し、データをリアルタイムで変換および分析できます。Amazon Managed Service for Apache Flink は、リアルタイムアプリケーションを継続的に実行するために必要なすべてを処理し、受信データのボリュームとスループットに合わせて自動的にスケーリングします。Amazon Managed Service for Apache Flink では、ストリーミングアプリケーションが消費するリソースに対してのみ料金が発生します。最低料金やセットアップ料金はかかりません。詳細については、「Amazon Managed Service for Apache Flink」を参照してください。

AWS Managed Services の「Managed Service for Apache Flink」に関するよくある質問

よくある質問と回答：

Q: AMS アカウントの Amazon Managed Service for Apache Flink へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロ

ビジョニングします: `customer_kinesis_analytics_application_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントで Amazon Managed Service for Apache Flink を使用することにはどのような制限がありますか？

- AMS インフラストラクチャへの変更を防ぐため、設定は「AMS-」または「MC-」プレフィックスのないリソースに限定されます。
- 新しい Kinesis Data Streams または Firehose を削除または作成するアクセス許可がポリシーから削除されました。これを許可する別のポリシーがあります。

Q: AMS アカウントで Amazon Kinesis Data Streams を使用するための前提条件または依存関係は何ですか？

いくつかの依存関係があります。

- Amazon Managed Service for Apache Flink では、Managed Service for Apache Flink でアプリケーションを設定する前に、Kinesis Data Streams または Firehose を作成する必要があります。
- リソースベースのポリシーのアクセス許可は、特定の入力データソースを示す必要があります。

AMS SSP を使用して AMS アカウントに Amazon Managed Streaming for Apache Kafka をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Managed Streaming for Apache Kafka (Amazon MSK) 機能に直接アクセスします。Amazon Managed Streaming for Apache Kafka は、フルマネージド型の AWS ストリーミングデータサービスです。これにより、Apache Kafka クラスターの運用に関するエキスパートになることなく、Apache Kafka を使用してストリーミングデータを処理するアプリケーションを簡単に構築および実行できます。Amazon MSK は、Apache Kafka クラスターと Apache ZooKeeper ノードのプロビジョニング、設定、メンテナンスを管理します。Amazon MSK は AWS 、コンソールに主要な Apache Kafka パフォーマンスメトリクスも表示します。

Amazon MSK は、VPC ネットワークの分離、コントロールプレーン API 認可のための AWS IAM、保管時の暗号化、転送中の TLS 暗号化、TLS ベースの証明書認証、 で保護された SASL/SCRAM 認証など、Apache Kafka クラスターに複数のレベルのセキュリティを提供します AWS Secrets Manager。詳細については、「Amazon MSK」を参照してください。

AWS Managed Services での Amazon MSK に関するよくある質問

一般的な質問と回答：

Q: AMS アカウントの Amazon MSK へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (レビューが必要) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、次の IAM ポリシーとロールをアカウントにプロビジョニングします。

- `customer-msk-admin-policy.json`
- `AmazonMSKFullAccess`
- `customer-msk-admin-role.json`

アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: Amazon MSK の使用にはどのような制限がありますか？

Amazon MSK が設定した宛先にブローカーログを配信するには、`AmazonMSKFullAccess` ポリシーが IAM ロールに添付されていることを確認してください。そのため、フルアクセス許可はすでに設定されています。

Q: Amazon MSK を使用する際の前提条件または依存関係は何ですか？

MSK クラスターを作成する前に、その VPC 内に VPC とサブネットが必要です。デフォルトでは、AMS はこれをデフォルトの AMS VPC 作成の一部として扱います。

Amazon MSK の制限については、「Amazon MSK の制限」を参照してください。

AMS SSP を使用して AMS アカウントで Amazon Managed Service for Prometheus をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Managed Service for Prometheus (AMP) 機能に直接アクセスします。Amazon Managed Service for Prometheus は、コンテナのメトリクスをモニタリングする Prometheus 互換のサーバーレスサービスです。これにより、大規模なコンテナ環境を安全にモニタリングすることが容易になります。Amazon Managed Service for Prometheus では、現在使用されているものと同じオープンソースの Prometheus データモデルとクエリ言語を使用して、コンテナ化されたワークロードのパ

フォーマンスをモニタリングできます。また、基盤のインフラストラクチャを管理する必要なく、スケーラビリティ、可用性、セキュリティを強化できます。

Amazon Managed Service for Prometheus は、ワークロードのスケールアップとスケールダウンに応じて、運用メトリクスの取り込み、ストレージ、クエリを自動的にスケーリングします。これは AWS セキュリティサービスと統合され、データへの高速かつ安全なアクセスを可能にします。詳細については、「Amazon Managed Service for Prometheus とは」を参照してください。

AWS Managed Services での Amazon Managed Service for Prometheus に関するよくある質問

一般的な質問と回答：

Q: AMS アカウントで Amazon Managed Service for Prometheus へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (レビューが必要) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer-prometheus-console-role`。アカウントにプロビジョニングされたら、フェデレーションソリューションで`customer-prometheus-console-role`ロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon Managed Service for Prometheus の使用にはどのような制限がありますか？

すべての機能がサポートされています。

Q: AMS アカウントで Amazon Managed Service for Prometheus を使用するための前提条件または依存関係は何ですか？

Amazon Managed Service for Prometheus の使用を開始するための前提条件や依存関係はありません。ただし、特定のユースケースによっては、他の AWS サービスへのアクセスが必要になる場合があります。

AMS SSP を使用して AMS アカウントに Amazon Personalize をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Personalize 機能に直接アクセスします。Amazon Personalize は、開発者がアプリケーショ

ンを使用して顧客向けにパーソナライズされたレコメンデーションを簡単に作成できるようにする機械学習サービスです。

機械学習は、パーソナライズされた製品とコンテンツのレコメンデーション、カスタマイズされた検索結果、ターゲットを絞ったマーケティングプロモーションを強化することで、カスタマーエンゲージメントを向上させるためにますます使用されています。ただし、これらの高度なレコメンデーションシステムを生成するために必要な機械学習機能の開発は、複雑さのため、現在のほとんどの組織の手の届かないところにあります。Amazon Personalize を使用すると、これまで機械学習の経験がないデベロッパーは、Amazon.com で長年使用されて完成した機械学習テクノロジーを使用して、アプリケーションに高度なパーソナライゼーション機能を簡単に構築できます。

Amazon Personalize では、クリック、ページビュー、サインアップ、購入など、アプリケーションからのアクティビティストリームと、記事、製品、動画、音楽などの推奨アイテムのインベントリを提供します。また、年齢や地理的位置など、ユーザーからの追加の属性情報を Amazon Personalize に提供することもできます。Amazon Personalize は、データの処理と調査、意味のあるものの特定、適切なアルゴリズムの選択、データに合わせてカスタマイズされたパーソナライゼーションモデルのトレーニングと最適化を行います。Amazon Personalize によって分析されるすべてのデータは、プライベートかつ安全に保持され、カスタマイズされたレコメンデーションにのみ使用されます。シンプルな API コールを使用して、パーソナライズされたレコメンデーションの提供を開始できます。お支払いいただくのは使用した分のみです。最低料金や前払い金はありません。

詳細については、「Amazon Personalize」を参照してください。

AWS Managed Servicesでの Amazon Personalize に関するよくある質問

Q: AMS アカウントで Amazon Personalize へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストし、 AWS パーソナライズによってレコメンデーションの生成に使用されるデータを含む S3 バケットを指定する必要があります。この RFC は、`customer_personalize_console_role`および の IAM ロールをアカウントにプロビジョニングします`customer_personalize_service_role`。

- アカウントで `customer_personalize_console_role`がプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。以外の既存のロール`customer_personalize_console_policy`に をアタッチすることもできます`Customer_ReadOnly_Role`。

- customer_personalize_service_role がアカウントに提供されたら、新しいデータセットグループを作成するときに ARN を参照できます。

この時点で、AMS Operations はこのサービスロールをアカウント にもデプロイしますaws_code_pipeline_service_role_policy。

Q: AMS アカウントでの Amazon Personalize の使用にはどのような制限がありますか？

Amazon Personalize の設定は、AMS インフラストラクチャへの変更を防ぐために、「ams-」または「mc-」プレフィックスのないリソースに限定されます。

Q: AMS アカウントで Amazon Personalize を使用するための前提条件または依存関係は何ですか？

- データが保存されている S3 バケットが暗号化されている場合、Amazon Personalize がバケットの復号化に使用するロールを許可できるように、KMS キー ID を指定する必要があります。

  Amazon Personalize は、デフォルトの KMS S3 キーをサポートしていません。KMS を使用する必要がある場合は、カスタムキーを作成し、変更タイプ KMS キー | 作成 (レビューが必要) の RFC を開いて次のポリシーを追加します。

  JSON

```
{
    "Version":"2012-10-17",
    "Id": "key-consolepolicy-3",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
                "Service": "personalize.amazonaws.com"
            },
            "Action": "kms:*",
            "Resource": "*"
        }
    ]
}
```

- S3 バケットは、次のバケットポリシーを使用して作成する必要があります。これを行うには、変更タイプ S3 ストレージ | ポリシーの作成で RFC を送信します。このポリシーは、Amazon Personalize がデータにアクセスすることを許可します。そのバケットには、Amazon Personalize が使用するデータが含まれます。

JSON

```
{
"Version":"2012-10-17",
"Id": "PersonalizeS3BucketAccessPolicy",
"Statement": [
{
"Sid": "PersonalizeS3BucketAccessPolicy",
"Effect": "Allow",
"Principal": {
"Service": "personalize.amazonaws.com"
},
"Action": [
"s3:GetObject",
"s3:ListBucket"
],
"Resource": [
"arn:aws:s3:::bucket-name",
"arn:aws:s3:::bucket-name/*"
]
}
]
}
```

AMS SSP を使用して AMS アカウントに Amazon QuickSight をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで QuickSight 機能に直接アクセスします。QuickSight は、組織内のすべてのユーザーにインサイトを提供する、高速でクラウドを活用したビジネスインテリジェンスサービスです。フルマネージドサービスである QuickSight を使用すると、機械学習 (ML) インサイトを含むインタラクティブなダッシュボードを簡単に作成して公開できます。詳細については、Amazon QuickSight」を参照してください。

AWS Managed Servicesでの QuickSight に関するよくある質問

一般的な質問と回答：

Q: AMS アカウントの QuickSight へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add change type (ct-1w8z66n899dct) を送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_quicksight_console_admin_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの QuickSight の使用にはどのような制限がありますか？

- AWS IAM ポリシーの依存関係のため、QuickSight の リソース設定にはアクセスできません。ただし、AMS チームはリクエストに応じて各リソースを有効にし、サービスを有効にします。
- この機能により、ユーザーは AMS インフラストラクチャを侵害する可能性のある IAM アクセス許可を変更できるため、個々のユーザーとグループのリソースアクセスはこのモデルではサポートされていません。
- QuickSight 内から IAM アイデンティティを招待する機能は、IAM オブジェクトの変更に伴うリスクがあるため、サポートされていません。
- QuickSight サービスには、Enterprise と Standard の 2 つのエディションがあります。どちらも、AMS でサポートされているシングルサインオン (SSO) オプションを提供します。ただし、Enterprise Edition には、QuickSight を Active Directory (AD) と統合するオプションがあります。AMS の QuickSight は、AMS アカウント構造と QuickSight の信頼要件との互換性がないため、AD との統合をサポートしていません。

Q: AMS アカウントで QuickSight を使用するための前提条件または依存関係は何ですか？

- AMS がこの RFC を受信して QuickSight を追加すると、追加情報のサービスリクエストが送信され、以下が提供されます。
  - QuickSight アカウント名 (例: *`CustomerName`*`-quicksight`
  - QuickSight Edition (Standard と Enterprise)
  - QuickSight サービスを有効にする AWS リージョン (デフォルトは AMS AWS リージョン) 。
  - QuickSight アカウントの通知 E メールアドレス。
  - (オプション) 分析するデータファイルがある S3 バケット。
  - QuickSight に接続する VPC とサブネット IDs は、VPC 接続を追加する機能をサポートしています。これにより、QuickSight とアカウント内のリソース間のプライベート接続が可能になります。

AMS オペレーターは、ユーザーに代わってサインアッププロセスを実行し、2 つの QuickSight 機能を設定します。

- データソースへの自動検出。
- VPC 接続。

> **Note**
>
> これらのアクションは、サインインプロセス中に昇格された IAM および VPC アクセス許可が必要なため、AMS オペレーターが実行する必要があります。

AMS SSP を使用して AMS アカウントに Amazon Rekognition をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Rekognition 機能に直接アクセスします。Amazon Rekognition を使用すると、機械学習の専門知識を必要としない、実証済みの高度にスケーラブルな深層学習テクノロジーを使用して、アプリケーションにイメージ分析とビデオ分析を簡単に追加できます。Amazon Rekognition を使用すると、イメージやビデオ内のオブジェクト、人物、テキスト、シーン、アクティビティを特定し、不適切なコンテンツを検出できます。Amazon Rekognition は、さまざまなユーザー検証、人数カウント、公共安全のユースケースで顔を検出、分析、比較するために使用できる、高精度の顔分析および顔検索機能も提供します。

Amazon Rekognition Custom Labels を使用すると、ビジネスニーズに固有のイメージ内のオブジェクトやシーンを特定できます。たとえば、アセンブリライン上の特定の機械部品を分類したり、異常な植物を検出したりするためのモデルを構築できます。Amazon Rekognition Custom Labels はモデル開発の面倒な作業を処理するため、機械学習の経験は必要ありません。識別するオブジェクトまたはシーンのイメージを提供するだけで、サービスは残りを処理します。

詳細については、Amazon Rekognition」を参照してください。

AWS Managed Services の Amazon Rekognition に関するよくある質問

一般的な質問と回答：

Q: AMS アカウントの Amazon Rekognition へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (レビューが必要) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、アカウントに次の

IAM ロールをプロビジョニングします: `customer_rekognition_console_role & customer_rekognition_service_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon Rekognition の使用にはどのような制限がありますか？

Amazon Rekognition の完全な機能は、Amazon Rekognition の自己プロビジョニング型サービスロールで使用できます。

Q: AMS アカウントで Amazon Rekognition を使用するための前提条件または依存関係は何ですか？

Amazon Rekognition Video ストリームプロセッサまたはデータストリームのソースストリーミングビデオを提供する Kinesis Video Streams を Kinesis Data Streams にデータを書き込む送信先として使用する場合は、RFC の作成`kinesisStreamName`時に AMS に を提供してください。

AMS SSP を使用して AMS アカウントに Amazon SageMaker AI をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon SageMaker AI 機能に直接アクセスします。SageMaker AI は、すべての開発者とデータサイエンティストに、機械学習モデルを迅速に構築、トレーニング、デプロイする機能を提供します。Amazon SageMaker AI は、データのラベル付けと準備、アルゴリズムの選択、モデルのトレーニング、デプロイのための調整と最適化、予測、アクションを実行するための機械学習ワークフロー全体をカバーするフルマネージドサービスです。モデルは、はるかに少ない労力と低コストで本番環境に迅速に移行できます。詳細については、Amazon SageMaker AI」を参照してください。

AWS Managed Services での SageMaker AI に関するよくある質問

一般的な質問と回答：

Q: AMS アカウントの SageMaker AI へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) change type を送信してアクセスをリクエストします。この RFC は、IAM ロール `customer_sagemaker_admin_role`とサービスロール をアカウントにプロビジョニングします`AmazonSageMaker-ExecutionRole-Admin`。SageMaker AI がアカウントにプロビジョニングされたら、フェデレーションソリューションで`customer_sagemaker_admin_role`ロールをオンボードする必要があります。サービスロールに直接アクセスすることはできません。SageMaker AI サービスは、「ロールの受け渡し」で説明されているように、さまざまなアクションを実行する際にサービスロールを使用します。

Q: AMS アカウントでの SageMaker AI の使用にはどのような制限がありますか？

- AMS Amazon SageMaker AI IAM ロールでは、次のユースケースはサポートされていません。
  - SageMaker AI Studio は現在サポートされていません。
  - プライベートワークフォースを管理する SageMaker AI Ground Truth はサポートされていません。この機能ではAmazon Cognito リソースへの過度に寛容なアクセスが必要であるためです。プライベートワークフォースの管理が必要な場合は、SageMaker AI と Amazon Cognito アクセス許可を組み合わせたカスタム IAM ロールをリクエストできます。それ以外の場合は、データのラベル付けにパブリックワークフォース (Amazon Mechanical Turk がサポート) または AWS Marketplace サービスプロバイダーを使用することをお勧めします。
- SageMaker AI サービス (aws.sagemaker.{region}.notebook、com.amazonaws.{region}.sagemaker.api & com.amazonaws.{region}.sagemaker.runtime) への API コールをサポートする VPC エンドポイントの作成は、アクセス許可を SageMaker AI 関連サービスのみに限定することはできないためサポートされていません。このユースケースをサポートするには、管理 | その他 | その他の RFC を送信して、関連する VPC エンドポイントを作成します。
- SageMaker AI エンドポイントの自動スケーリングはサポートされていません。SageMaker AI には任意の (「*」) リソースに対する`DeleteAlarm`アクセス許可が必要なためです。エンドポイントの自動スケーリングをサポートするには、管理 | その他 | その他の RFC を送信して、SageMaker AI エンドポイントの自動スケーリングを設定します。

Q: AMS アカウントで SageMaker AI を使用する際の前提条件または依存関係は何ですか？

- 以下のユースケースでは、使用前に特別な設定が必要です。
  - S3 バケットを使用してモデルアーティファクトとデータを保存する場合は、デプロイ | 高度なスタックコンポーネント | S3 ストレージ | RFC の作成で、必要なキーワード (SageMaker」、「Sagemaker」、「sagemaker」、または「aws-glue」) を含む という名前の S3 バケットをリクエストする必要があります。
  - Elastic File Store (EFS) を使用する場合は、EFS ストレージを同じサブネットに設定し、セキュリティグループで許可する必要があります。
  - 他のリソースが SageMaker AI サービス (ノートブック、API、ランタイムなど) に直接アクセスする必要がある場合は、次の方法で設定をリクエストする必要があります。
    - RFC を送信してエンドポイントのセキュリティグループを作成する (デプロイ | 高度なスタックコンポーネント | セキュリティグループ | 作成 (自動))。
    - 管理の送信 | その他 | その他 | RFC を作成して関連する VPC エンドポイントを設定します。

Q: が直接**customer_sagemaker_admin_role**アクセスできるリソースでサポートされている命名規則は何ですか？ (更新および削除のアクセス許可については、以下を参照してください。リソースでサポートされている追加の命名規則が必要な場合は、AMS Cloud Architect に連絡して相談してください。)

- リソース: AmazonSageMaker-ExecutionRole-*ロールを渡す
  - アクセス許可: SageMaker AI セルフプロビジョニングサービスロールは、 AWS Glue、AWS RoboMaker、および での SageMaker AI サービスロール (AmazonSageMaker-ExecutionRole-*) の使用をサポートします AWS Step Functions。
- リソース: Secrets Manager の AWS シークレット
  - アクセス許可: AmazonSageMaker-*プレフィックスを使用してシークレットを記述、作成、取得、更新します。
  - アクセス許可: SageMakerリソースタグが に設定されているときにシークレットを取得するについて説明しますtrue。
- リソース: 上のリポジトリ AWS CodeCommit
  - アクセス許可: AmazonSageMaker-*プレフィックスを持つリポジトリを作成/削除します。
  - アクセス許可: Git Pull/Push on repositories with following prefixes, *sagemaker*, *SageMaker*, and *Sagemaker*。
- リソース: Amazon ECR (Amazon Elastic Container Registry) リポジトリ
  - アクセス許可: アクセス許可: 次のリソース命名規則が使用されている場合、リポジトリポリシーを設定、削除し、コンテナイメージをアップロードします*sagemaker*。
- リソース: Amazon S3 バケット
  - アクセス許可: リソースにプレフィックス 、、 *sagemaker* がある場合、オブジェクトの取得、配置、削除*SageMaker**Sagemaker*、マルチパートアップロード S3 オブジェクトの中止を行いますaws-glue。
  - アクセス許可: SageMaker タグが に設定されているときに S3 オブジェクトを取得しますtrue。
- リソース: Amazon CloudWatch Log Group
  - アクセス許可: ロググループまたはストリームの作成、ログイベントの入力、一覧表示、更新、の作成、プレフィックス を使用したログ配信の削除/aws/sagemaker/*。
- リソース: Amazon CloudWatch メトリクス

  - アクセス許可: 、AWS/SageMaker、AWS/SageMaker/、、aws/SageMaker、、および のプレフィックスを使用する場合はaws/SageMaker/aws/sagemakeraws/sagemaker/、メトリクスデータを配置します/aws/sagemaker/.。
- リソース: Amazon CloudWatch Dashboard
  - アクセス許可: プレフィックス が使用されているときにダッシュボードを作成/削除しますcustomer_*。
- リソース: Amazon SNS (Simple Notification Service) トピック
  - アクセス許可: 、*sagemaker*、および のプレフィックスを使用する場合は*SageMaker*、トピックをサブスクライブ/作成します*Sagemaker*。

Q: **AmazonSageMakerFullAccess**と の違いは何ですか**customer_sagemaker_admin_role**？

customer_sagemaker_admin_role と は、以下を除き、AmazonSageMakerFullAccess とほぼ同じアクセス許可customer_sagemaker_admin_policyを提供します。

- AWS RoboMaker、Amazon Cognito、および AWS Glue リソースに接続するためのアクセス許可。
- SageMaker AI エンドポイントの自動スケーリング。管理 | 高度なスタックコンポーネント | Identity and Access Management (IAM) | エンティティまたはポリシー (レビューが必要) の変更タイプ (ct-27tuth19k52b4) を更新して、自動スケーリングアクセス許可を一時的または永続的に昇格させる必要があります。これは、自動スケーリングには CloudWatch サービスへの許可付きアクセスが必要なためです。

Q: 保管中のデータ暗号化に AWS KMS カスタマーマネージドキーを採用するにはどうすればよいですか？

関連する IAM ユーザーまたはロールがキーを使用できるように、カスタマーマネージドキーでキーポリシーが正しく設定されていることを確認する必要があります。詳細については、AWS KMS「 キーポリシー」ドキュメントを参照してください。

AMS SSP を使用して AMS アカウントに Amazon Simple Email Service をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Simple Email Service (Amazon SES) 機能に直接アクセスします。Amazon Simple Email Service は、デジタルマーケティング担当者やアプリケーション開発者、マーケティング、通知、ト

ランザクション E メールの送信を支援するように設計されたクラウドベースの E メール送信サービスです。

SMTP インターフェイスまたはいずれかの AWS SDKs を使用して、Amazon SES を既存のアプリケーションに直接統合できます。Amazon SES の E メール送信機能を、チケットシステムや E メールクライアントなど、既に使用しているソフトウェアに統合することもできます。

詳細については、「Amazon Simple Email Service」を参照してください。

AWS Managed Services での Amazon SES に関するよくある質問

Q: AMS アカウントの Amazon SES へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (ct-1w8z66n899dct) 変更タイプで RFC を送信して、Amazon SES へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_ses_admin_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントで Amazon SES を使用するための前提条件または依存関係は何ですか？

- Amazon SES がバケットにイベントを発行できるようにするには、S3 バケットポリシーを設定する必要があります。
- Amazon AWS SES が E メールを暗号化し、アカウントに属する Amazon S3、Amazon SES Amazon SNS を使用するか、CMK キーを設定する必要があります。

Q: AMS アカウントでの Amazon SES の使用にはどのような制限がありますか？

次のリソースを作成するにはRFCs を生成する必要があります。

- Kinesis Firehose ストリームへの PutEvents アクセス許可を持つ SMTP ユーザーと IAM サービスロール。
- Amazon SES ルールと設定セットの送信先がそれらの AWS リソースと連携するには、AMS 変更タイプを使用して S3 バケット、Firehose ストリーム、SNS トピックなどの新しいリソースを作成する必要があります。 Amazon SES
- SMTP 認証情報。新しい SMTP 認証情報をリクエストするには、変更タイプ (管理 | その他 | その他 | 作成) を使用します。AMS は認証情報を作成し、Secrets Manager に追加します。

AMS SSP を使用して AMS アカウントに Amazon Simple Workflow Service をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Simple Workflow Service (Amazon SWF) 機能に直接アクセスします。Amazon Simple Workflow Service は、デベロッパーが並列またはシーケンシャルなステップを持つバックグラウンドジョブを構築、実行、スケーリングするのに役立ちます。Amazon SWF は、 クラウドでフルマネージド型のステートトラッカーおよびタスクコーディネーターと考えることができます。アプリケーションのステップが完了するまでに 500 ミリ秒以上かかる場合、処理の状態を追跡する必要がある場合、またはタスクが失敗した場合に復旧または再試行する必要がある場合、Amazon SWF が役立ちます。詳細については、「Amazon Simple Workflow Service」を参照してください。

AWS Managed Services の Amazon SWF に関するよくある質問

一般的な質問と回答：

Q: AMS アカウントの Amazon SWF へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add change type (ct-1w8z66n899dct) を送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_swf_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon SWF の使用にはどのような制限がありますか？

Lambda アクセス`InvokeFunction`許可はこのサービスに含まれていますが、すべての AMS カスタマーロールに追加された AMS `customer_deny_policy`は、AMS Lambda 関数と AMS 所有リソースへのアクセスを明示的に拒否します。Amazon SWF 内のリソースにタグ付けまたはタグ付け解除するには、管理 | その他 | その他の変更タイプを送信します。

Q: AMS アカウントで Amazon SWF を使用するための前提条件または依存関係は何ですか？

Amazon SWF は AWS Lambda サービスに依存するため、このロールの一部として Lambda を呼び出すアクセス許可が提供されており、Amazon SWF から Lambda を呼び出す追加のアクセス許可は必要ありません。それ以外の場合、Amazon SWF を使用するための前提条件はありません。

AMS SSP を使用して AMS アカウントに Amazon Textract をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Textract 機能に直接アクセスします。Amazon Textract は、スキャンされたドキュメントから印刷されたテキスト、手書き、その他のデータを自動的に抽出するフルマネージド型の機械学習サービスで、シンプルな光学文字認識 (OCR) を超えて、フォームやテーブルからデータを識別、理解、抽出します。詳細については、「Amazon Textract」を参照してください。

AWS Managed Services の Amazon Textract に関するよくある質問

一般的な質問と回答：

Q: AMS アカウントで Amazon Textract をセットアップするようにリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (レビューが必要) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、、、customer_textract_console_role、customer_textract_human_review_execution_rol よび の IAM ロールをアカウントにプロビジョニングしますcustomer_ec2_textract_instance_profile。アカウントにプロビジョニングされたら、フェデレーションソリューションcustomer_textract_console_roleでロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon Textract の使用にはどのような制限がありますか？

AMS アカウントでの Amazon Textract の使用に制限はありません。

Q: AMS アカウントで Amazon Textract を使用するための前提条件または依存関係は何ですか？

RFC デプロイ | 高度なスタックコンポーネント |S3 ストレージ | 作成 (ct-1a68ck03fn98r) を送信して、S3 バケットの作成をリクエストする必要があります。

AMS SSP を使用して AMS アカウントに Amazon Transcribe をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Amazon Transcribe 機能に直接アクセスします。Amazon Transcribe は、オーディオファイルからタイムスタンプ付きのテキストトランスクリプトを自動的に生成する、フルマネージドで継続的にトレーニングされた自動音声認識サービスです。Amazon Transcribe を使用すると、開発者はアプリ

ケーションにspeech-to-text機能を簡単に追加できます。コンピュータがオーディオデータを検索して分析することは事実上不可能です。したがって、記録された音声は、アプリケーションで使用する前にテキストに変換する必要があります。これまで、顧客は文字起こしプロバイダーと連携する必要があり、高価な契約に署名する必要があり、このタスクを実行するためにテクノロジースタックに統合するのが困難でした。これらのプロバイダーの多くは、コンタクトセンターで一般的な低忠実度の電話オーディオなど、さまざまなシナリオにうまく適応しない古いテクノロジーを使用しているため、精度が低下します。

Amazon Transcribe は、自動音声認識 (ASR) と呼ばれる深層学習プロセスを使用して、音声をテキストに迅速かつ正確に変換します。Amazon Transcribe を使用して、カスタマーサービスへの電話の文字起こし、クローズドキャプションと字幕の自動化、メディアアセットのメタデータの生成を行い、完全に検索可能なアーカイブを作成できます。Amazon Transcribe Medical を使用して、臨床ドキュメントアプリケーションに医療speech-to-text機能を追加できます。詳細については、Amazon Transcribe」を参照してください。

AWS Managed Services での Amazon Transcribe に関するよくある質問

よくある質問と回答：

Q: Amazon Transcribe を AMS アカウントでセットアップするようにリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_transcribe_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Amazon Transcribe の使用にはどのような制限がありますか？

RA と特に指定がない限り、文字起こしを操作するときは、バケットのプレフィックスとして「customer-transcribe*」を使用する必要があります。

Amazon 文字起こし内で IAM ロールを作成することはできません。

デフォルトの SSPS の出力データにサービスマネージド S3 バケットを使用することはできません (必要な場合は、 アカウント CA にお問い合わせください) 。

AMS 名前空間に属さないカスタマー管理の KMS キーを使用する場合は、リスク承諾を送信する必要があります。

Q: AMS アカウントで Amazon Transcribe を使用するための前提条件または依存関係は何ですか？

S3 は、「customer-transcribe*」という名前のバケットにアクセスできる必要があります。S3 バケットが KMS キーで暗号化されている場合、Amazon Transcribe を使用するには KMS が必要です。バケットを暗号化する必要がない場合は、「KMStranscribeAllow」を削除できます。

AMS SSP を使用して AMS アカウントに Amazon WorkSpaces をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで WorkSpaces 機能に直接アクセスします。WorkSpaces を使用すると、WorkSpaces と呼ばれる仮想クラウドベースの Microsoft Windows または Amazon Linux デスクトップをユーザーにプロビジョニングできます。WorkSpaces は、ハードウェアの調達とデプロイ、または複雑なソフトウェアのインストールの必要性を排除します。必要に応じてユーザーをすばやく追加または削除できます。ユーザーは、サポートされているデバイスからクライアントアプリケーションを使用するか、Windows WorkSpaces の場合はウェブブラウザを使用して WorkSpaces にアクセスし、既存のオンプレミス Active Directory (AD) 認証情報を使用してログインします。 WorkSpaces

詳細については、Amazon WorkSpaces」を参照してください。

AWS Managed Services の WorkSpaces に関するよくある質問

よくある質問と回答：

Q: AMS アカウントの WorkSpaces へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_workspaces_console_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの WorkSpaces の使用にはどのような制限がありますか？

WorkSpaces の完全な機能は、Amazon WorkSpaces のセルフプロビジョニングサービスロールで使用できます。

Q: AMS アカウントで WorkSpaces を使用するための前提条件または依存関係は何ですか？

- WorkSpaces は AWS リージョンによって制限されるため、AD Connector は WorkSpaces インスタンスがホストされているのと同じ AWS リージョンで設定する必要があります。

  お客様は、次の 2 つの方法のいずれかを使用して WorkSpaces をカスタマー AD に接続できます。

1. AD コネクタを使用して認証をオンプレミスの Active Directory サービスにプロキシする (推奨):

   WorkSpaces インスタンスをオンプレミスのディレクトリサービスと統合する前に、AMS アカウントに Active Directory (AD) Connector を設定します。AD Connector は、既存の AD ユーザー (ドメインから) のプロキシとして機能し、既存のオンプレミス AD 認証情報を使用して WorkSpaces に接続します。WorkSpaces はお客様のオンプレミスドメインに直接結合され、リソースフォレストとユーザーフォレストの両方として機能し、お客様側でより細かく制御できるため、これが推奨されます。

   詳細については、Amazon WorkSpaces をデプロイするためのベストプラクティス (シナリオ 1)」を参照してください。

2. AWS Microsoft AD、共有サービス VPC、オンプレミスへの一方向の信頼で AD Connector を使用する :

   また、まず AMS 管理 AD からオンプレミス AD への一方向の送信信頼を確立することで、オンプレミスディレクトリでユーザーを認証することもできます。WorkSpaces は AD Connector を使用して AMS マネージド AD に参加します。その後、WorkSpaces アクセス許可は AMS マネージド AD を介して WorkSpaces インスタンスに委任されます。オンプレミス環境との双方向の信頼を確立する必要はありません。このシナリオでは、ユーザーフォレストはカスタマー AD にあり、リソースフォレストは AMS マネージド AD にあります (AMS マネージド AD への変更は RFC 経由でリクエストできます) 。WorkSpaces VPC と AMS マネージド AD を実行している MALZ 共有サービス VPC 間の接続は、Transit Gateway を介して確立されることに注意してください。

   詳細については、Amazon WorkSpaces をデプロイするためのベストプラクティス (シナリオ 6)」を参照してください。

> **Note**
>
> AD Connector は、管理 | その他 | その他 | 前提条件の AD 設定の詳細を含む変更タイプ RFC を送信することで設定できます。詳細については、「AD Connector の作成」を参照してください。メソッド 2 を使用して AMS マネージド AD でリソースフォレストを作成する場合は、別の管理 | その他 | その他 | AMS マネージド AD を実行して AMS 共有サービスアカウントに変更タイプ RFC を作成します。

AMS SSP を使用して AMS アカウントで AMS Code サービスをプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで AMS Code サービス機能に直接アクセスします。AMS Code サービスは、次に示すように、AWS コード管理サービスの独自のバンドルです。AMS Code サービスを使用して AMS のすべてのサービスをデプロイするか、AMS に個別にデプロイするかを選択できます。

AMS Code サービスには、次のサービスが含まれます。

- AWS CodeCommit: セキュアな Git ベースのリポジトリをホストするフルマネージド型のソースコントロールサービス。これにより、チームは安全でスケーラブルなエコシステムでコードでコラボレーションできます。CodeCommit を使用することにより、独自のソース管理システムを運用したり、そのインフラストラクチャをスケールしたりする必要がなくなります。CodeCommit を使用すると、ソースコードからバイナリまで、あらゆるものを安全に保存でき、既存の Git ツールとシームレスに連携します。詳細については、「AWS CodeCommit」を参照してください。

  AMS Code サービスから独立して AMS アカウントにこれをデプロイするには、「」を参照してくださいAMS SSP を使用して AMS アカウント AWS CodeCommit でプロビジョニングする。
- AWS CodeBuild: ソースコードをコンパイルし、テストを実行し、デプロイ可能なソフトウェアパッケージを生成するフルマネージドの継続的統合サービス。CodeBuild により、ビルドサーバーのプロビジョニング、管理、スケーリングが不要になります。CodeBuild では、継続的にスケーリングされ、複数のビルドが同時にプロセスされるため、ビルドの実行までキューで待機することはありません。パッケージ済みのビルド環境を使用、またはご自分のビルドツールを使用するカスタムビルド環境を作成できることですぐに開始できます。CodeBuild では毎分ごとに使用するコンピューティングリソースの使用量が有料になります。詳細については、「AWS CodeBuild」を参照してください。

  AMS Code サービスから独立して AMS アカウントにこれをデプロイするには、「」を参照してくださいAMS SSP を使用して AMS アカウント AWS CodeBuild でプロビジョニングする。
- AWS CodeDeploy: Amazon EC2 やオンプレミスサーバーなどのさまざまなコンピューティングサービスへのソフトウェアデプロイを自動化するフルマネージドデプロイサービス。 AWS CodeDeploy は、新機能を迅速にリリースし、アプリケーションのデプロイ中のダウンタイムを回避し、アプリケーションの更新の複雑さに対処します。 AWS CodeDeploy を使用してソフトウェアのデプロイを自動化できるため、エラーが発生しやすい手動操作が不要になります。サービスは、デプロイのニーズに合わせてスケーリングされます。詳細については、「AWS CodeDeploy」を参照してください。

AMS Code サービスから独立して AMS アカウントにこれをデプロイするには、「」を参照してくださいAMS SSP を使用して AMS アカウント AWS CodeDeploy でプロビジョニングする。

- AWS CodePipeline: 完全マネージド型の継続的デリバリーサービス。リリースパイプラインを自動化して、アプリケーションとインフラストラクチャを迅速かつ確実に更新できます。CodePipeline はお客様が定義したリリースモデルに基づき、コードチェンジがあった場合のフェーズの構築、テスト、およびデプロイを自動化します。機能とアップデートをすばやく、信頼性の高い方法で配信できます。GitHub などのサードパーティーサービスと AWS CodePipeline 、または独自のカスタムプラグインと簡単に統合できます。では AWS CodePipeline、使用した分のみお支払いいただきます。前払い金や長期契約はありません。詳細については、「AWS CodePipeline」を参照してください。

  AMS Code サービスとは別に AMS アカウントにこれをデプロイするには、「」を参照してくださいAMS SSP を使用して AMS アカウント AWS CodePipeline でプロビジョニングする。

AWS Managed Services の AMS コードサービスに関するよくある質問

Q: AMS アカウントの AMS Code サービスへのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (レビューが必要) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_code_suite_console_role`。アカウントでプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。この時点で、AMS Operations は CodeBuild`customer_codebuild_service_role`、CodeDeploy、CodePipeline `aws_code_pipeline_service_role`サービスのアカウントに `customer_codedeploy_service_role`、、 サービスロールもデプロイします。 CodeBuild に追加の IAM アクセス許可が必要な場合は`customer_codebuild_service_role`、AMS サービスリクエストを送信します。

> **Note**
>
> これらのサービスを個別に追加することもできます。詳細については、AMS SSP を使用して AMS アカウント AWS CodeBuild でプロビジョニングする「」、AMS SSP を使用して AMS アカウント AWS CodeDeploy でプロビジョニングする「」、およびAMS SSP を使用

して AMS アカウント AWS CodePipeline でプロビジョニングする「」をそれぞれ参照してください。

Q: AMS アカウントでの AMS Code サービスの使用にはどのような制限がありますか？

- AWS CodeCommit: CodeCommit のトリガー機能は、SNS トピックを作成する権限が関連付けられているため無効になっています。CodeCommit に対する直接認証は制限されています。ユーザーは 認証情報ヘルパーで認証する必要があります。KMS コマンドには、kms:Encrypt、kms:Decrypt、kms:ReEncrypt、kms:GenereteDataKey、kms:GenerateDataKeyWithou および kms:DescribeKey も制限されています。
- CodeBuild: AWS CodeBuild コンソール管理者アクセスの場合、アクセス許可はリソースレベルで制限されます。たとえば、CloudWatch アクションは特定のリソースに制限され、`iam:PassRole`アクセス許可は制御されます。
- CodeDeploy: 現在、CodeDeploy は Amazon EC2/オンプレミスでのデプロイのみをサポートしています。CodeDeploy を介した ECS および Lambda でのデプロイはサポートされていません。
- CodePipeline: CodePipeline の機能、ステージ、プロバイダーは以下に限定されます。
  - デプロイステージ: Amazon S3 および AWS CodeDeploy
  - ソースステージ: Amazon S3、 AWS CodeCommit、ビットバケット、GitHub
  - ビルドステージ: AWS CodeBuild および Jenkins
  - 承認ステージ: Amazon SNS
  - テストステージ： AWS CodeBuild、Jenkins、BlazeMeter、Ghost Inspector UI テスト、Micro Focus StormRunner Load、Runscope API Monitoring
  - ステージの呼び出し: Step Functions と Lambda

> **Note**
>
> AMS オペレーションは `customer_code_pipeline_lambda_policy`をアカウントにデプロイします。Lambda 呼び出しステージの Lambda 実行ロールにアタッチする必要があります。このポリシーを追加する Lambda サービス/実行ロール名を指定します。カスタム Lambda サービス/実行ロールがない場合、AMS は という名前の新しいロールを作成します。これは `customer_code_pipeline_lambda_execution_role` `customer_lambda_basic_execution_role`と のコピーです`customer_code_pipeline_lambda_policy`。

Q: AMS アカウントで AMS Code サービスを使用するための前提条件または依存関係は何ですか？

- CodeCommit: S3 バケットが AWS KMS キーで暗号化されている場合は、S3 と AWS KMS を使用する必要があります AWS CodeCommit。
- CodeBuild: 定義された AWS CodeBuild サービスロールに追加の IAM アクセス許可が必要な場合は、AMS サービスリクエストを通じてリクエストします。
- CodeDeploy: なし。
- CodePipeline: None. AWS supported services—AWS CodeCommit， AWS CodeBuild， AWS CodeDeploy— は、CodePipeline の起動前または起動と同時に起動する必要があります。ただし、これは AMS エンジニアによって行われます。

AMS SSP を使用して AMS アカウント AWS Amplify でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントの AWS Amplify 機能に直接アクセスします。 AWS Amplify は、フロントエンドのウェブおよびモバイル開発者がフルスタックアプリケーションを簡単に構築、接続、ホストできるようにする完全なソリューションです。Amplify は、ユースケースの進化に応じて幅広い AWS サービスを活用する柔軟性を提供します。Amplify は、フルスタックの iOS、Android、Flutter、Web、React Native アプリケーションを構築するための製品を提供しています。詳細についてはAWS Amplifyを参照してください。

AWS Amplify AWS Managed Servicesに関するよくある質問

一般的な質問と回答：

Q: AMS アカウントでの設定 AWS Amplify をリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (レビューが必要) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_amplify_console_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

さらに、 にはインフラストラクチャの変更許可 AWS Amplify があるため、リスク承諾を提供する必要があります。これを行うには、Cloud Service Delivery Manager (CSDM) を使用します。

Q: AMS アカウント AWS Amplify で を使用することにはどのような制限がありますか？

特に RA と が指定されていない限り、Amplify を使用するときは、バケットのプレフィックス'amplify*'として を使用する必要があります。

Q: AMS アカウント AWS Amplify で を使用するための前提条件または依存関係は何ですか？

AMS アカウント AWS Amplify で を使用するための前提条件はありません。

Malz 環境のみ: Amplify のデフォルトのオンボードロールは「customer_amplify_console_role」です。カスタムロールを使用するには、まず IAM エンティティをデプロイします。次に、追加の RFC を作成して、アプリケーションアカウントのサービスコントロールポリシー許可リストにカスタムロールを追加します。

AMS SSP を使用してプロビジョニングする AWS AppSync

AMS Self-Service Provisioning (SSP) モードを使用して、AMS マネージドアカウント内の AWS AppSync 機能に直接アクセスします。 は、1 つ以上のデータソースのデータに安全にアクセスし、操作し、結合するための柔軟な API を作成できるようにすることで、アプリケーション開発 AWS AppSync を簡素化します。 AWS AppSync は、GraphQL を使用してアプリケーションが必要とするデータを正確に取得できるようにするマネージドサービスです。

を使用すると AWS AppSync、リアルタイムの更新を必要とするアプリケーションを含むスケーラブルなアプリケーションを、NoSQL データストア、リレーショナルデータベース、HTTP APIs、カスタムデータソースなどのさまざまなデータソースで構築できます AWS Lambda。モバイルアプリとウェブアプリの場合、 は AWS AppSync さらに、デバイスがオフラインになったときにローカルデータアクセスを提供し、オンラインに戻ったときにカスタマイズ可能な競合解決によるデータ同期を提供します。詳細についてはAWS AppSyncを参照してください。

AWS AppSync AWS Managed Servicesに関するよくある質問

よくある質問と回答：

Q: AMS アカウントのアクセス AWS AppSync をリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add change type (ct-1w8z66n899dct) を送信してアクセスをリクエストします。この RFC は、 `customer_appsync_service_role`および の IAM ロールをアカウントにプロビジョニングします`customer_appsync_author_role`。アカウントにプロビジョニングされたら、フェデレーションソリューション`customer_appsync_author_role`で をオンボードする必要があります。

Q: の使用にはどのような制限がありますか AWS AppSync？

- AppSync でデータソースを作成する場合、お客様は以前に作成したサービスロールを指定する必要があります。新しいロールの作成は許可されないため、アクセス拒否が返されます。
- AppSync ロールは、AMS インフラストラクチャへの変更を防ぐために、「AMS-」または「MC-」プレフィックスを含むリソースへのアクセス許可を制限するように設定されています。

Q: を使用するための前提条件または依存関係は何ですか AWS AppSync？

このサービスでは、他の複数の サービスをデータソースとして使用できます。これらのサービスを使用するための基本的なアクセス許可はサービスロール (`customer_appsync_service_role`) に含まれていますが、サービスを使用するときはサービスロールを手動で選択する必要があります。

AMS SSP を使用して AMS アカウント AWS App Mesh でプロビジョニングする

AMS Self-Service Provisioning (SSP) モードを使用して、AMS マネージドアカウント内の AWS App Mesh 機能に直接アクセスします。 は、複数のタイプのコンピューティングインフラストラクチャ間でサービスが相互に簡単に通信できるように、アプリケーションレベルのネットワーク AWS App Mesh を提供します。App Mesh は、サービスの通信方法を標準化し、end-to-end可視性を提供し、アプリケーションの高可用性を確保します。

AWS App Mesh は、複数のタイプのコンピューティングインフラストラクチャにまたがって構築されたサービスの一貫した可視性とネットワークトラフィック制御を提供することで、サービスの実行を容易にします。App Mesh を使用すると、アプリケーションコードを更新して、モニタリングデータの収集方法やサービス間のトラフィックのルーティング方法を変更する必要がなくなります。App Mesh は、モニタリングデータをエクスポートするように各サービスを設定し、アプリケーション全体で一貫した通信制御ロジックを実装します。これにより、エラーの正確な場所をすばやく特定し、障害が発生したときやコード変更をデプロイする必要がある場合にネットワークトラフィックを自動的に再ルーティングすることが容易になります。詳細についてはAWS App Meshを参照してください。

AWS App Mesh AWS Managed Servicesに関するよくある質問

一般的な質問と回答：

Q: AMS アカウント AWS App Mesh でアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add change type (ct-1w8z66n899dct) を送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニング

します: customer_app_mesh_console_role。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: の使用にはどのような制限がありますか AWS App Mesh？

のフル機能は AWS App Mesh 、AMS アカウントで使用できます。

Q: を使用するための前提条件または依存関係は何ですか AWS App Mesh？

AMS アカウント AWS App Mesh で使用する前提条件や依存関係はありません。

AMS SSP を使用して AMS アカウント AWS Audit Manager でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Audit Manager 機能に直接アクセスします。Audit Manager は、 AWS 使用状況を継続的に監査し、リスクと規制や業界標準への準拠を評価する方法を簡素化するのに役立ちます。Audit Manager はエビデンスの収集を自動化するため、ポリシー、手順、アクティビティが効果的に機能しているかどうかの評価が容易になります。監査の時期になると、Audit Manager はコントロールのステークホルダーレビューを管理し、手動作業を大幅に削減して監査対応レポートを構築するのに役立ちます。詳細については、「Audit Manager」を参照してください。

AWS Audit Manager AWS Managed Servicesに関するよくある質問

よくある質問と回答：

Q: AWS Audit Manager AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか？

AWS サービス RFC 管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (レビューが必要) (ct-3qe6io8t6jtny) の送信を通じてアクセスをリクエストできます。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: customer-audit-manager-admin-Role。アカウントでプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: の使用にはどのような制限がありますか AWS Audit Manager？

AMS アカウント AWS Audit Manager での の使用に制限はありません。の完全な機能 AWS Audit Manager が提供されます。

Q: を使用するための前提条件または依存関係は何ですか AWS Audit Manager？

1. レポート/評価を配置する s3 バケットを AMS に提供する必要があります。
2. サービスで暗号化する場合は、使用する KMS CMK ARN を AMS に提供する必要があります。
3. トピックに SNS 通知を送信する場合は、トピックまたは ARN の名前を指定する必要があります。
4. （オプション）Audit Manager のマルチアカウントランディングゾーンの一部として Organizations を有効にし、委任管理者アカウントが必要な場合は、追加の前提条件があります。RFC の説明フィールド (Management | AWS service | Compatible Service| Add) で、Audit Manager Setup の一部として委任管理者アカウントを使用するように指定し、以下の詳細を指定します。
   - KMS CMK ARN (最初は Audit Manager のセットアップに使用）
   - Audit Manager がこのマルチアカウントランディングゾーンの一部として使用する委任管理者アカウント ID (MALZ アプリケーションアカウントでもかまいません）

AMS SSP を使用して AMS アカウント AWS Batch でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS Batch 機能に直接アクセスします。 AWS Batch は、開発者、サイエンティスト、エンジニアが数十万のバッチコンピューティングジョブを簡単かつ効率的に実行できるようにします AWS。は、送信されたバッチジョブのボリュームと特定のリソース要件に基づいて、最適な量とタイプのコンピューティングリソース (CPU またはメモリ最適化インスタンスなど) を AWS Batch 動的にプロビジョニングします。を使用すると AWS Batch、ジョブの実行に使用するバッチコンピューティングソフトウェアやサーバークラスターをインストールおよび管理する必要がなくなるため、結果の分析と問題の解決に集中できます。詳細についてはAWS Batchを参照してください。

AWS Batch AWS Managed Servicesに関するよくある質問

一般的な質問と回答：

Q: AWS Batch AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか？

1. へのアクセスをリクエストするには AWS Batch、RFC 管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (ct-1w8z66n899dct) を送信します。この RFC は、アカウントに次の IAM ロールとポリシーをプロビジョニングします。

IAM ロール：

- customer_batch_console_role
- customer_batch_ecs_instance_role
- customer_batch_events_service_role
- customer_batch_service_role
- customer_batch_ecs_task_role

ポリシー:

- customer_batch_console_role_policy
- customer_batch_service_role_policy
- customer_batch_events_service_role_policy

2. アカウントでプロビジョニングしたら、フェデレーションソリューションcustomer_batch_console_roleでロールをオンボードする必要があります。

Q: の使用にはどのような制限がありますか AWS Batch？

コンピューティング環境を作成するときは、EC2 インスタンスを「customer_batch」または「customer-batch」としてタグ付けする必要があります。インスタンスにタグが付けられていない場合、ジョブの完了時にインスタンスはバッチで終了されません。

Q: を使用するための前提条件または依存関係は何ですか AWS Batch？

AMS アカウント AWS Batch で使用する前提条件や依存関係はありません。

AMS SSP を使用して AMS アカウント AWS Certificate Manager でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで AWS Certificate Manager (ACM) 機能に直接アクセスします。 AWS Certificate Manager は、 サービスおよび内部接続リソースで使用するパブリックおよびプライベートの Secure Sockets Layer/Transport Layer Security (SSL/TLS) 証明書をプロビジョニング、管理、デプロイできる AWS サービスです。SSL/TLS 証明書は、ネットワーク通信を保護し、インターネット上のウェブサイトとプライベートネットワーク上のリソースのアイデンティティを確立するために使用されます。 は、SSL/TLS 証明書の購入、アップロード、更新の時間のかかる手動プロセス AWS Certificate Manager を排除します。

を使用すると AWS Certificate Manager、証明書をリクエストし、Elastic Load Balancer、Amazon CloudFront ディストリビューション、API Gateway APIs などの ACM 統合 AWS リソースにデプロイして、 が証明書の更新 AWS Certificate Manager を処理できます。また、内部リソースのプライベート証明書を作成し、証明書のライフサイクルを一元管理することもできます。ACM 統合サービスで使用できる AWS Certificate Manager ように でプロビジョニングされたパブリック証明書とプライベート証明書は無料です。アプリケーションを実行するために作成した AWS リソースに対してのみ料金が発生します。ではAWS Private Certificate Authority、 のオペレーション AWS Private CA と発行するプライベート証明書に対して毎月お支払いいただきます。詳細については、AWS Certificate Manager 「- AWS Documentation」を参照してください。

AWS Managed Services の ACM に関するよくある質問

よくある質問と回答：

Q: AWS Certificate Manager AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add change type (ct-1w8z66n899dct) を送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_acm_create_role`。このロールを使用して、ACM 証明書を作成および管理できます。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

ACM 証明書は、IAM `customer_acm_create_role` ロールを追加していない場合でも、次の変更タイプを使用して作成できます。

- ACM | パブリック証明書の作成
- ACM | プライベート証明書の作成
- 追加の SANs を含む ACM 証明書 | 作成

Q: の使用にはどのような制限がありますか AWS Certificate Manager？

既存の証明書を削除または変更するには、変更リクエスト (RFC) を AMS に送信する必要があります。これらのアクションには完全な管理者アクセスが必要です (管理 | その他 | その他 | 更新変更タイプ (ct-0xdawir96cy7k)。 IAM ポリシーは、タグ名 (mc*、ams* など) に基づいて権限を除外できないことに注意してください。証明書にはコストがかからないため、未使用の証明書を削除しても時間的制約はありません。

Q: Certificate Manager を使用する際の前提条件または依存関係は何ですか？

既存のパブリック DNS 名、および DNS CNAME レコードを作成するためのアクセス。ただし、マネージドアカウントでホストする必要はありません。

AMS SSP を使用して AMS アカウント AWS Private Certificate Authority でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントの AWS Private Certificate Authority 機能に直接アクセスします。プライベート証明書は、プライベートネットワーク上の接続されたリソース間の通信を識別して保護するために使用されます。 サーバー、 モバイル、 および IoT デバイスとアプリケーション。 AWS Private CA は、プライベート証明書のライフサイクルを簡単かつ安全に管理できるマネージドプライベート CA サービスです。 は、独自のプライベート CA を運用するための事前投資や継続的なメンテナンスコストなしで、高可用性のプライベート CA サービス AWS Private CA を提供します。 は、ACM の証明書管理機能をプライベート証明書に AWS Private CA 拡張します。 を使用すると、パブリック証明書とプライベート証明書を一元的に作成および管理できます。 AWS マネジメントコンソールまたは ACM API を使用して、 AWS リソースのプライベート証明書を簡単に作成およびデプロイできます。EC2 インスタンス、コンテナ、IoT デバイス、オンプレミスリソースの場合、プライベート証明書を簡単に作成して追跡し、独自のクライアント側のオートメーションコードを使用してデプロイできます。また、プライベート証明書を作成し、カスタム証明書の有効期間、キーアルゴリズム、またはリソース名を必要とするアプリケーション用に自分で管理することもできます。詳細については、「」を参照してくださいAWS Private CA。

AWS Private CA AWS Managed Servicesに関するよくある質問

よくある質問と回答：

Q: AMS アカウント AWS Private CA でアクセスをリクエストするにはどうすればよいですか？

AWS サービス RFC (管理 | AWS サービス | 互換サービス) の送信を通じてアクセスをリクエストします。この RFC を通じて、次の IAM ロールがアカウントにプロビジョニングされます: `customer_acm_pca_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: の使用にはどのような制限がありますか AWS Private CA？

現在、 AWS Resource Access Manager （ AWS RAM) を使用してクロスアカウントを共有 AWS Private CA することはできません。

Q: を使用するための前提条件または依存関係は何ですか AWS Private CA？

1. CRL を作成する場合は、保存先の S3 バケットが必要です。 AWS Private CA は、指定した Amazon S3 バケットに CRL を自動的に預金し、定期的に更新します。CRL を設定する前に、S3 バケットに以下のバケットポリシーがあることが前提条件です。このリクエストを続行するには、次のように ct-0fpjlxa808sh2 (管理 | 高度なスタックコンポーネント | S3 ストレージ | 更新ポリシー) を使用して RFC を作成します。

- S3 バケット名または ARN を指定します。
- 以下のポリシーを RFC にコピーし、 を目的の S3 バケット名bucket-nameに置き換えます。

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"acm-pca.amazonaws.com"
         },
         "Action":[
            "s3:PutObject",
            "s3:PutObjectAcl",
            "s3:GetBucketAcl",
            "s3:GetBucketLocation"
         ],
         "Resource":[
            "arn:aws:s3:::bucket-name/*",
            "arn:aws:s3:::bucket-name"
         ]
      }
   ]
}
```

2. 上記の S3 バケットが暗号化されている場合、サービスプリンシパル acm-pca.amazonaws.com には復号するためのアクセス許可が必要です。このリクエストを続行するには、次のように ct-3ovo7px2vsa6n (管理 | 高度なスタックコンポーネント | KMS キー | 更新) を使用して RFC を作成します。

- ポリシーを更新する必要がある KMS キー ARN を指定します。

- 以下のポリシーを RFC にコピーし、 を目的の S3 バケット名bucket-nameに置き換えます。

```
{
   "Sid":"Allow ACM-PCA use of the key",
   "Effect":"Allow",
   "Principal":{
      "Service":"acm-pca.amazonaws.com"
   },
   "Action":[
      "kms:GenerateDataKey",
      "kms:Decrypt"
   ],
   "Resource":"*",
   "Condition":{
      "StringLike":{
         "kms:EncryptionContext:aws:s3:arn":[
            "arn:aws:s3:::bucket_name/acm-pca-permission-test-key",
            "arn:aws:s3:::bucket_name/acm-pca-permission-test-key-private",
            "arn:aws:s3:::bucket_name/audit-report/*",
            "arn:aws:s3:::bucket_name/crl/*"
         ]
      }
   }
}
```

3. AWS Private CA CRLs「新しいアクセスコントロールリスト (ACLs」をサポートしていません。S3 「ACM プライベート CA の AWS Private CA CRL を安全に作成して保存する方法」で説明されているように、S3 アカウントとバケットでこの設定を無効にする必要があります。無効にするには、ct-0xdawir96cy7k (管理 | その他 | その他 | 更新) を使用して新しい RFC を作成し、リスク承諾をアタッチします。 CRLs https://aws.amazon.com/blogs/security/how-to-securely-create-and-store-your-crl-for-acm-private-ca/ リスクの受け入れについてご質問がある場合は、 クラウドアーキテクトにお問い合わせください。

AMS SSP を使用して AMS アカウントで AWS CloudEndure をプロビジョニングする

> **Note**
>
> の起動に成功すると AWS Application Migration Service、CloudEndure Migration サービスはすべての AWS リージョンでサポート終了となります。GovCloud リージョンと商用リー

ジョンへの移行 AWS Application Migration Service には、 を使用することをお勧めします。詳細については、「 とは AWS Application Migration Service」を参照してください。
を使用する場合は AWS Application Migration Service、CA に連絡して指示を受けてください。

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで AWS CloudEndure 機能に直接アクセスします。 AWS CloudEndure 移行は、物理、仮想、クラウドベースのインフラストラクチャから への大規模な移行を簡素化、迅速化、自動化します AWS。CloudEndure ディザスタリカバリ (DR) は、ランサムウェアやサーバーの破損などの脅威によるダウンタイムやデータ損失から保護します。

AWS Managed Services でのAWS CloudEndure に関するよくある質問

Q: AMS アカウントの CloudEndure へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (レビューが必要) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、次の IAM ユーザーをアカウントにプロビジョニングします: `customer_cloud_endure_user`。アカウントでプロビジョニングされると、ユーザーのアクセスキーとシークレットキーは AWS Secrets Manager で共有されます。

これらのポリシーは、 `customer_cloud_endure_policy`および のアカウントにもプロビジョニングされます`customer_cloud_endure_deny_policy`。

さらに、アプリケーション統合用の CloudEndure DR ソリューションにはインフラストラクチャ変更のアクセス許可があるため、リスク承諾を提供する必要があります。これを行うには、Cloud Service Delivery Manager (CSDM) を使用します。

Q: AMS アカウントでの CloudEndure の使用にはどのような制限がありますか？

クラウド耐久性レプリケーションおよび変換インスタンスは、指定したサブネットでのみ起動できます。

Q: AMS アカウントで CloudEndure を使用するための前提条件または依存関係は何ですか？ RFC 双方向通信を介して以下を共有します。

- 起動するレプリケーションインスタンスと変換インスタンスの VPC サブネットの詳細。
- EBS ボリュームが暗号化されている場合の KMS キー Amazon リソースネーム (ARN)。

AMS SSP を使用して AMS アカウント AWS CloudHSM でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで AWS CloudHSM 機能に直接アクセスします。 AWS CloudHSM 企業、 契約上の AWS クラウド内で専用のハードウェアセキュリティモジュール (HSM) インスタンスを使用して、データセキュリティに関する および の規制コンプライアンス要件 AWS。 および AWS Marketplace パートナー、 は、AWS プラットフォーム内の機密データを保護するためのさまざまなソリューションを提供します。ただし、暗号化キーの管理に関する契約上または規制上の義務の対象となるアプリケーションやデータについては、 追加の保護が必要になる場合があります。 は既存のデータ保護ソリューションを AWS CloudHSM 補完し、安全なキー管理のために政府の標準に従って設計および検証された HSMs 内の暗号化キーを保護することができます。 AWS CloudHSM を使用すると、 保存、 は、データ暗号化に使用される暗号化キーを、ユーザーのみがキーにアクセスできるように管理します。詳細についてはAWS CloudHSMを参照してください。

AWS CloudHSM AWS Managed Servicesに関するよくある質問

よくある質問と回答：

Q: AWS CloudHSM AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか？

AMS アカウントでの の使用には 2 つのステップがあります。

1. AWS CloudHSM クラスターをリクエストします。これを行うには、管理 | その他 | その他 | 作成 (ct-1e1xtak34nx76) 変更タイプを使用して RFC を送信します。次の詳細を含めます。
   - AWS リージョン。
   - VPC ID/ARN。送信する RFC と同じアカウントにある VPC ID/VPC ARN を指定します。
   - クラスターに少なくとも 2 つのアベイラビリティーゾーンを指定します。
   - HSM クラスターに接続する Amazon EC2 インスタンス ID。
2. AWS CloudHSM コンソールにアクセスします。これを行うには、管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (ct-1w8z66n899dct) 変更タイプで RFC を送信します。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_cloudhsm_console_role`。

アカウントでロールがプロビジョニングされたら、フェデレーションソリューションにロールをオンボードする必要があります。

Q: AMS アカウント AWS CloudHSM で を使用することにはどのような制限がありますか？

AWS CloudHSM コンソールへのアクセスでは、クラスターを作成、終了、または復元することはできません。これらの操作を行うには、管理 | その他 | その他 | 変更タイプの作成 (ct-1e1xtak34nx76) 変更タイプを送信します。

Q: AMS アカウント AWS CloudHSM で を使用するための前提条件または依存関係は何ですか？

VPC 内のクライアント Amazon EC2 インスタンスを介してポート 2225 を使用する TCP トラフィックを許可するか、HSM クラスターへのアクセスを必要とするオンプレミスサーバーに Direct Connect VPN を使用する必要があります。 AWS CloudHSM は、セキュリティグループとネットワークインターフェイスの Amazon EC2 に依存します。ログのモニタリングまたは監査では、HSM はすべてのローカル HSM デバイスアクティビティで CloudTrail (AWS API オペレーション) と CloudWatch Logs に依存します。

Q: AWS CloudHSM クライアントおよび関連するソフトウェアライブラリに更新を適用するのは誰ですか？

ライブラリとクライアントの更新を適用する責任はお客様にあります。リリースの CloudHSM バージョン履歴ページをモニタリングし、CloudHSM クライアントアップグレードを使用して更新を適用します。

> **Note**
>
> HSM アプライアンスのソフトウェアパッチは、常にサービスによって AWS CloudHSM 自動的に適用されます。

AMS SSP を使用して AMS アカウント AWS CodeBuild でプロビジョニングする

AMS Self-Service Provisioning (SSP) モードを使用して、AMS マネージドアカウント内の AWS CodeBuild 機能に直接アクセスします。 AWS CodeBuild は、ソースコードをコンパイルし、テストを実行し、すぐにデプロイできるソフトウェアパッケージを生成するフルマネージドの継続的統合サービスです。CodeBuild により、ビルドサーバーのプロビジョニング、管理、スケーリングが不要になります。CodeBuild では、継続的にスケーリングされ、複数のビルドが同時にプロセスされるため、ビルドの実行までキューで待機することはありません。パッケージ済みのビルド環境を使用、またはご自分のビルドツールを使用するカスタムビルド環境を作成できることですぐに開始できま

す。CodeBuild では毎分ごとに使用するコンピューティングリソースの使用量が有料になります。詳細についてはAWS CodeBuildを参照してください。

> **Note**
>
> CodeCommit、CodeBuild、CodeDeploy、CodePipeline を単一の RFC でオンボードするには、管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (レビューが必要) (ct-3qe6io8t6jtny) 変更タイプを送信し、CodeBuild、CodeDeploy、CodePipeline の 3 つのサービスをリクエストします。次に、、、`customer_codebuild_service_role`、、`customer_codedeploy_service_role`aws_code_pipeline_service_roleの 3 つのロールすべてがアカウントにプロビジョニングされます。アカウントでプロビジョニングした後、フェデレーションソリューションでロールをオンボードする必要があります。

AWS Managed Services での CodeBuild に関するよくある質問

よくある質問と回答：

Q: AWS CodeBuild AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか？

AMS アカウント AWS CodeBuild での の使用には 2 つのステップがあります。

1. S3 バケット、Amazon CloudWatch、ロググループと AWS 調整する`CodeBuild Service Role`ビルドプロセスの をプロビジョニングする
2. CodeBuild コンソールへのアクセスをリクエストする

管理 | AWS サービス | セルフプロビジョニングサービス | 変更タイプの追加 (ct-1w8z66n899dct) を使用して RFC を送信することで、両方の設定を AMS アカウントでリクエストできます。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウント AWS CodeBuild で を使用することにはどのような制限がありますか？

AWS CodeBuild コンソール管理者アクセスの場合、アクセス許可はリソースレベルで制限されます。たとえば、CloudWatch アクションは特定のリソースに制限され、`iam:PassRole`アクセス許可は制御されます。

Q: AMS アカウントで CodeBuild を使用するための前提条件または依存関係は何ですか？

定義された AWS CodeBuild サービスロールに追加の IAM アクセス許可が必要な場合は、AMS サービスリクエストを通じてリクエストします。

AMS SSP を使用して AMS アカウント AWS CodeCommit でプロビジョニングする

> **Note**
>
> AWS は AWS CodeCommit、2024 年 7 月 25 日以降、 への新しいお客様のアクセスを閉鎖しました。 AWS CodeCommit 既存のお客様は、引き続きこのサービスを通常どおり使用できます。 AWS は引き続きセキュリティ、可用性、パフォーマンスの向上に投資しますが AWS CodeCommit、新機能を導入する予定はありません。
> AWS CodeCommit Git リポジトリを他の Git プロバイダーに移行するには、クラウドアーキテクト (CA) に連絡してガイダンスを受けてください。Git リポジトリの移行の詳細については、AWS CodeCommit リポジトリを別の Git プロバイダーに移行する方法」を参照してください。

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントの AWS CodeCommit 機能に直接アクセスします。 AWS CodeCommit は、セキュアな Git ベースのリポジトリをホストするフルマネージド型のソースコントロールサービスです。これにより、チームは安全で高度にスケーラブルなエコシステムでコードに共同作業できます。CodeCommit を使用することにより、独自のソース管理システムを運用したり、そのインフラストラクチャをスケールしたりする必要がなくなります。CodeCommit を使用すると、ソースコードからバイナリまで、あらゆるものを安全に保存でき、既存の Git ツールとシームレスに連携します。詳細についてはAWS CodeCommitを参照してください。

> **Note**
>
> CodeCommit、CodeBuild、CodeDeploy、CodePipeline を単一の RFC でオンボードするには、管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (レビューが必要) (ct-3qe6io8t6jtny) 変更タイプを送信し、CodeBuild、CodeDeploy、CodePipeline の 3 つのサービスをリクエストします。次に、、`customer_codebuild_service_role`、、`customer_codedeploy_service_role`aws_code_pipeline_service_roleの 3 つのロールすべてがアカウントにプロビジョニングされます。アカウントでプロビジョニングした後、フェデレーションソリューションでロールをオンボードする必要があります。

AWS Managed Services の CodeCommit に関するよくある質問

Q: AMS アカウントの CodeCommit へのアクセスをリクエストするにはどうすればよいですか？

AWS CodeCommit コンソールとデータアクセスロールは、2 つの AWS サービス RFCs、コンソールアクセス、データアクセスを送信することでリクエストできます。

- Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) change type を使用して RFC を送信 AWS CodeCommit して、 へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_codecommit_console_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

  データアクセス (トレーニングやエンティティリストなど) には、S3 データソース (必須) 、出力バケット (必須) 、KMS (オプション) を指定する個別の CTs がデータソースごとに必要です。すべてのデータソースにアクセスロールが付与されている限り、 AWS CodeCommit ジョブの作成に制限はありません。データアクセスをリクエストするには、 管理 | その他 | その他 | 作成 (ct-1e1xtak34nx76) を使用して RFC を送信します。

Q: AMS アカウント AWS CodeCommit で を使用することにはどのような制限がありますか？

SNS トピックを作成する権限が関連付けられているため、CodeCommit のトリガー機能は無効になっています。CodeCommit に対する直接認証は制限されているため、ユーザーは 認証情報ヘルパーで認証する必要があります。、`kms:Encrypt`、、`kms:Decrypt`、`kms:ReEncrypt`kms:GenereteDataKey、`kms:GenerateDataKeyWithoutPlaintext`などの KMS コマンドも制限されていますkms:DescribeKey。

Q: AMS アカウント AWS CodeCommit で を使用するための前提条件または依存関係は何ですか？

S3 バケットが KMS キーで暗号化されている場合、 を使用するには S3 と KMS が必要です AWS CodeCommit。

AMS SSP を使用して AMS アカウント AWS CodeDeploy でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS CodeDeploy 機能に直接アクセスします。 AWS CodeDeploy は、Amazon EC2 などのさまざ

まなコンピューティングサービス AWS Fargate AWS Lambdaやオンプレミスサーバーへのソフトウェアデプロイを自動化するフルマネージドデプロイサービスです。 AWS CodeDeploy は、新機能を迅速にリリースし、アプリケーションのデプロイ中のダウンタイムを回避し、アプリケーションの更新の複雑さに対処します。 AWS CodeDeploy を使用してソフトウェアのデプロイを自動化できるため、エラーが発生しやすい手動操作が不要になります。サービスは、デプロイのニーズに合わせてスケーリングされます。詳細についてはAWS CodeDeployを参照してください。

> **Note**
>
> CodeCommit、CodeBuild、CodeDeploy、CodePipeline を単一の RFC でオンボードするには、管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (レビューが必要) (ct-3qe6io8t6jtny) 変更タイプを送信し、CodeBuild、CodeDeploy、CodePipeline の 3 つのサービスをリクエストします。次に、、`customer_codebuild_service_role`、、`customer_codedeploy_service_role`aws_code_pipeline_service_roleの 3 つのロールすべてがアカウントにプロビジョニングされます。アカウントでプロビジョニングした後、フェデレーションソリューションでロールをオンボードする必要があります。

AWS Managed Servicesでの CodeDeploy に関するよくある質問

Q: AMS アカウントの CodeDeploy へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (ct-1w8z66n899dct) 変更タイプで RFC を送信して CodeDeploy へのアクセスをリクエストします。この RFC は、`customer_codedeploy_console_role`および の IAM ロールをアカウントにプロビジョニングしますcustomer_codedeploy_service_role。アカウントにプロビジョニングされたら、フェデレーションソリューションでcustomer_codedeploy_console_roleロールをオンボードする必要があります。

Q: AMS アカウントでの CodeDeploy の使用にはどのような制限がありますか？

現在、Amazon EC2/オンプレミスとしてのみコンピューティングプラットフォームをサポートしています。ブルー/グリーンデプロイはサポートされていません。

Q: AMS アカウントで CodeDeploy を使用するための前提条件または依存関係は何ですか？

AMS アカウントで CodeDeploy を使用するための前提条件や依存関係はありません。

AMS SSP を使用して AMS アカウント AWS CodePipeline でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS CodePipeline 機能に直接アクセスします。 AWS CodePipeline はフルマネージド型の継続的デリバリーサービスであり、リリースパイプラインを自動化して、アプリケーションとインフラストラクチャを迅速かつ確実に更新できます。CodePipeline はお客様が定義したリリースモデルに基づき、コードチェンジがあった場合のフェーズの構築、テスト、およびデプロイを自動化します。機能とアップデートをすばやく、信頼性の高い方法で配信できます。GitHub などのサードパーティーサービスと AWS CodePipeline 、または独自のカスタムプラグインと簡単に統合できます。では AWS CodePipeline、使用した分のみお支払いいただきます。前払い金や長期契約はありません。詳細についてはAWS CodePipelineを参照してください。

> **Note**
>
> CodeCommit、CodeBuild、CodeDeploy、CodePipeline を単一の RFC でオンボードするには、管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (レビューが必要) (ct-3qe6io8t6jtny) 変更タイプを送信し、CodeBuild、CodeDeploy、CodePipeline の 3 つのサービスをリクエストします。次に、、`customer_codebuild_service_role`、、`customer_codedeploy_service_role`aws_code_pipeline_service_roleの 3 つのロールすべてがアカウントにプロビジョニングされます。アカウントでプロビジョニングした後、フェデレーションソリューションでロールをオンボードする必要があります。
> AMS の CodePipeline は、ソースステージのAmazon CloudWatch Events」をサポートしていません。これは、最小特権モデルと AMS 変更管理プロセスをバイパスするサービスロールとポリシーを作成するための昇格されたアクセス許可が必要なためです。

AWS Managed Services の CodePipeline に関するよくある質問

Q: AMS アカウントの CodePipeline へのアクセスをリクエストするにはどうすればよいですか？

関連するアカウントの のサービスリクエストを送信して、CodePipeline `customer_code_pipeline_console_role` へのアクセスをリクエストします。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

現時点では、AMS Operations はこのサービスロールをアカウント にもデプロイしますaws_code_pipeline_service_role_policy。

Q: AMS アカウントでの CodePipeline の使用にはどのような制限がありますか？

はい。CodePipeline の機能、ステージ、プロバイダーは以下に限定されます。

1. デプロイステージ: Amazon S3 に限定、および AWS CodeDeploy
2. ソースステージ: Amazon S3、 AWS CodeCommit、BitBucket、GitHub に限定
3. ビルドステージ: AWS CodeBuildと Jenkins に限定
4. 承認ステージ: Amazon SNS に限定
5. テストステージ: Jenkins AWS CodeBuild、BlazeMeter、Ghost Inspector UI テスト、Micro Focus StormRunner Load、Runscope API Monitoring に限定
6. 呼び出しステージ: Step Functions と Lambda に限定

> **Note**
>
> AMS オペレーションは`customer_code_pipeline_lambda_policy`アカウントにデプロイされます。Lambda 呼び出しステージの Lambda 実行ロールにアタッチする必要があります。このポリシーを追加する Lambda サービス/実行ロール名を指定してください。カスタム Lambda サービス/実行ロールがない場合、AMS は という名前の新しいロールを作成します。これは`customer_code_pipeline_lambda_execution_role`と のコピーになります`customer_lambda_basic_execution_role``customer_code_pipeline_lambda_policy`

Q: AMS アカウントで CodePipeline を使用するための前提条件または依存関係は何ですか？

AWS がサポートする サービスは AWS CodeCommit AWS CodeBuild、CodePipeline の起動前または起動と同時に起動 AWS CodeDeploy する必要があります。

AMS SSP を使用して AMS アカウント AWS Compute Optimizer でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS Compute Optimizer 機能に直接アクセスします。 は、ワークロードに最適な AWS コンピューティングリソース AWS Compute Optimizer を推奨し、機械学習を使用して過去の使用率メトリクスを分析し、コストを削減し、パフォーマンスを向上させます。コンピューティング (Amazon EC2 と ASGs) の過剰プロビジョニングにより、不要なインフラストラクチャコストが発生し、コンピューティングのプロビジョニングが不足すると、アプリケーションのパフォーマンスが低下する可能性が

あります。Compute Optimizer は、使用率データに基づいて、Amazon EC2 Auto Scaling グループの一部であるインスタンスタイプを含め、最適な Amazon EC2 インスタンスタイプを選択するのに役立ちます。詳細についてはAWS Compute Optimizerを参照してください。

AWS Managed Services の Compute Optimizer に関するよくある質問

Q: AMS アカウントの Compute Optimizer へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_compute_optimizer_readonly_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの Compute Optimizer の使用にはどのような制限がありますか？

制限はありません。の完全な機能は AWS Compute Optimizer 、AMS アカウントで使用できます。

Q: AMS アカウントで Compute Optimizer を使用するための前提条件または依存関係は何ですか？

- アカウントでサービスを有効にするには、AMS Ops を承認する RFC (管理 | その他 | その他 | 更新) を送信する必要があります。デプロイ中に、メトリクスの収集とレポートの生成を可能にするサービスリンクロール (SLR) が作成されます。SLR にはAWSServiceRoleForComputeOptimizer」というラベルが付けられています。詳細については、「 のサービスにリンクされたロールの使用」を参照してください。 AWS Compute Optimizer
- CloudWatch メトリクスは、次のメトリクスに対して有効にする必要があります。
  - CPU 使用率: インスタンスで使用されている割り当てられた Amazon EC2 コンピューティングユニットの割合。このメトリクスは、選択したインスタンスでアプリケーションを実行するために必要な処理能力を識別します。
  - メモリ使用率: サンプル期間中に何らかの方法で使用されたメモリの量。このメトリクスは、選択したインスタンスでアプリケーションを実行するために必要なメモリを識別します。メモリ使用率は、統合 CloudWatch エージェントがインストールされているリソースについてのみ分析されます。詳細については、CloudWatch エージェントによるメモリ使用率の有効化」(p. 10) を参照してください。
  - Network in: インスタンスがすべてのネットワークインターフェイスで受信したバイト数。このメトリクスは、単一のインスタンスへの受信ネットワークトラフィックのボリュームを識別します。

- ネットワーク出力: インスタンスによってすべてのネットワークインターフェイスで送信されたバイト数。このメトリクスは、1 つのインスタンスからの送信ネットワークトラフィックの量を識別します。
- ローカルディスク入出力 (I/O): ローカルディスクの入出力オペレーションの数。このメトリクスは、インスタンスのルートボリュームのパフォーマンスを識別します。

AMS SSP を使用して AMS アカウント AWS DataSync でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS DataSync 機能に直接アクセスします。 は、オンプレミスストレージと Amazon S3、Amazon Elastic File System (Amazon Elastic File System)、または Amazon FSx の間で大量のデータをオンライン AWS DataSync に移動します。 Amazon Elastic File System Amazon Elastic File System データ転送に関連する手動タスクは、移行を遅らせ、IT 運用に負担をかける可能性があります。DataSync は、コピージョブのスクリプト作成、転送のスケジュールとモニタリング、データの検証、ネットワーク使用率の最適化など、これらのタスクの多くを排除または自動的に処理します。DataSync ソフトウェアエージェントはネットワークファイルシステム (NFS) およびサーバーメッセージブロック (SMB) ストレージに接続するため、アプリケーションを変更する必要はありません。DataSync は、インターネットまたは AWS Direct Connect リンク経由で、オープンソースツールの最大 10 倍の速度で数百テラバイトと数百万のファイルを転送できます。DataSync を使用して、アクティブなデータセットまたはアーカイブを に移行したり AWS、データをクラウドに転送してタイムリーな分析と処理を行ったり、ビジネス継続 AWS 性のためにデータを にレプリケートしたりできます。

詳細についてはAWS DataSyncを参照してください。

AWS Managed Services での DataSync に関するよくある質問

Q: AMS アカウントの DataSync へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_datasync_console_role`。

アカウントでプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

タスクログをストリーミングするために使用する CloudWatch ロググループは「/aws/datasync」です。

Q: AMS アカウントでの DataSync の使用にはどのような制限がありますか？

のフル機能は AWS DataSync 、AMS アカウントで使用できます。

Q: AMS アカウントで DataSync を使用するための前提条件または依存関係は何ですか？

- DataSync サービスロール を使用して実行される DataSync タスクに関連付けられたすべての S3 バケットには、Amazon S3 ARNs (Amazon DataSync リソースネーム) が必要です`customer_datasync_service_role`。
- DataSync エージェントの VPC エンドポイントとセキュリティグループは、VPC エンドポイントを使用する前に、管理 | その他 | その他 | 作成 (ct-1e1xtak34nx76) 変更タイプを使用して RFC でリクエストする必要があります。
- AWS DataSync エージェントはアプライアンスとして AMS で実行されます。 AWS DataSync エージェントにはパッチが適用され、サービスによって更新されます。詳細については、AWS DataSync 「よくある質問」を参照してください。
- AWS DataSync エージェントを起動するには、管理 | その他 | その他 | 作成 (ct-1e1xtak34nx76) 変更タイプを使用して RFC を送信し、エージェントのデプロイをリクエストします。 AWS DataSync Amazon EC2 AMI ID、インスタンスタイプ、サブネット、セキュリティグループを指定し、既存の Amazon EC2 キーペアを参照するか、新しいキーペアの作成をリクエストします。

> **Note**
>
> AMS は、お客様に代わって AWS DataSync エージェントを手動でプロビジョニングするため、 AWS DataSync Amazon EC2 AMI での WIGS 取り込みプロセスは必要ありません。

AMS SSP を使用して AMS アカウント AWS Device Farm でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS Device Farm 機能に直接アクセスします。 AWS Device Farm は、テストインフラストラクチャをプロビジョニングおよび管理することなく、幅広いデスクトップブラウザと実際のモバイルデバイスでテストすることで、ウェブおよびモバイルアプリケーションの品質を向上させるアプリケーションテストサービスです。このサービスを使用すると、複数のデスクトップブラウザまたは実際の

デバイスでテストを同時に実行してテストスイートの実行を高速化し、ビデオとログを生成して、アプリの問題をすばやく特定できます。

詳細についてはAWS Device Farmを参照してください。

AWS Device Farm AWS Managed Servicesに関するよくある質問

Q: AWS Device Farm AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (レビューが必要) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_devicefarm_role`。

アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウント AWS Device Farm で を使用することにはどのような制限がありますか？

AWS Device Farm サービスへのフルアクセスは、「Name」タグで AMS 名前空間を使用することを除いて提供されます。

Q: AMS アカウント AWS Device Farm で を使用するための前提条件または依存関係は何ですか？

なし。

AMS SSP を使用して AMS アカウント AWS Elastic Disaster Recovery でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS Elastic Disaster Recovery 機能に直接アクセスします。 は、手頃な価格のストレージ、最小限のコンピューティング、point-in-timeリカバリを使用して、オンプレミスおよびクラウドベースのアプリケーションの高速で信頼性の高いリカバリにより、ダウンタイムとデータ損失 AWS Elastic Disaster Recovery を最小限に抑えます。を使用して、サポートされているオペレーティングシステムで実行されているオンプレミスまたはクラウドベースのアプリケーションをレプリケートする場合 AWS Elastic Disaster Recovery 、IT レジリエンスを高めることができます。 AWS マネジメントコンソール を使用して、レプリケーションと起動の設定、データレプリケーションのモニタリング、ドリルまたはリカバリ用のインスタンスの起動を行います。

詳細についてはAWS Elastic Disaster Recoveryを参照してください。

AWS Elastic Disaster Recovery AWS Managed Servicesに関するよくある質問

Q: AWS Elastic Disaster Recovery AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_drs_console_role`。

アカウントでプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウント AWS Elastic Disaster Recovery で を使用することにはどのような制限がありますか？

AMS アカウント AWS Elastic Disaster Recovery で使用する制限はありません。

Q: AMS アカウント AWS Elastic Disaster Recovery で を使用するための前提条件または依存関係は何ですか？

- コンソールロールにアクセスしたら、Elastic Disaster Recovery サービスを初期化して、アカウント内で必要な IAM ロールを作成する必要があります。
  - インスタンスプロファイルのクローンを作成して`AWSElasticDisasterRecoveryEc2InstancePolicy`ポリシーを`customer-mc-ec2-instance-profile`アタッチするには、変更タイプ管理 | アプリケーション | IAM インスタンスプロファイル | 変更タイプ ct-0ixp4ch2tiu04 RFC を作成 (レビューが必要) する必要があります。新しいポリシーをアタッチするマシンを指定する必要があります。
  - インスタンスがデフォルトのインスタンスプロファイルを使用していない場合、AMS は自動化`AWSElasticDisasterRecoveryEc2InstancePolicy`を通じてアタッチできます。
- クロスアカウントリカバリには、顧客所有の KMS キーを使用する必要があります。ターゲットアカウントへのアクセスを許可するには、ソースアカウントの KMS キーをポリシーに従って更新する必要があります。詳細については、「EBS 暗号化キーをターゲットアカウントと共有する」を参照してください。
- ロール`customer_drs_console_role`の表示を切り替える場合は、KMS キーポリシーを更新して、ポリシーの表示を許可する必要があります。
- クロスアカウント、クロスリージョンディザスタリカバリの場合、AMS はソースアカウントとターゲットアカウントを信頼されたアカウントとして設定し、フェイルバックロールとAWS 右サイジングロールをデプロイする必要があります CloudFormation。

AMS SSP を使用して AMS アカウント AWS Elemental MediaConvert でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS Elemental MediaConvert 機能に直接アクセスします。 AWS Elemental MediaConvert は、ブロードキャストグレードの機能を持つファイルベースのビデオトランスコーディングサービスです。これにより、ブロードキャストおよびマルチスクリーン配信用のvideo-on-demand (VOD) コンテンツを大規模に作成できます。このサービスは、高度なビデオおよびオーディオ機能と、シンプルなウェブサービスインターフェイスとpay-as-you-goを組み合わせたものです。を使用すると AWS Elemental MediaConvert、独自のビデオ処理インフラストラクチャの構築と運用の複雑さを心配することなく、魅力的なメディアエクスペリエンスの提供に集中できます。

詳細についてはAWS Elemental MediaConvertを参照してください。

AWS Managed Services での MediaConvert に関するよくある質問

Q: AMS アカウントの MediaConvert へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (レビューが必要) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_mediaconvert_author_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

2 番目のロール が提供されます。これは`customer_MediaConvert_Default_Role`、ソース S3 バケットから読み取り、出力を送信先 S3 バケットに書き込むため、およびデジタル著作権管理 (DRM) が必要な場合に API ゲートウェイを呼び出すために MediaConvert によって使用されます。

Q: AMS アカウントでの MediaConvert の使用にはどのような制限がありますか？

AMS での MediaConvert の使用に制限はありません。

Q: AMS アカウントで MediaConvert を使用するための前提条件または依存関係は何ですか？

AMS アカウントで MediaConvert を使用するための前提条件や依存関係はありません。

AMS SSP を使用して AMS アカウント AWS Elemental MediaLive でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS Elemental MediaLive 機能に直接アクセスします。 AWS Elemental MediaLive はブロードキャストグレードのライブビデオ処理サービスです。これにより、接続されたテレビ、タブレット、ス

マートフォン、セットトップボックスなどTVs、ブロードキャストテレビやインターネットに接続されたマルチスクリーンデバイスに配信するための高品質のビデオストリームを作成できます。このサービスは、ライブビデオストリームをリアルタイムでエンコードし、より大きなサイズのライブビデオソースを取得し、ビューワーに配信するためにより小さなバージョンに圧縮することで機能します。を使用すると AWS Elemental MediaLive、高度なブロードキャスト機能、高可用性、pay-as-you-goで、ライブイベントと 24 時間 365 日対応のチャネルの両方にストリームを簡単に設定できます。 AWS Elemental MediaLive では、ブロードキャストグレードのビデオ処理インフラストラクチャの構築と運用を複雑にすることなく、視聴者に魅力的なライブビデオエクスペリエンスの作成に集中できます。

詳細についてはAWS Elemental MediaLiveを参照してください。

AWS Managed Services での MediaLive に関するよくある質問

Q: AMS アカウントの MediaLive へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_medialive_author_role`。

この RFC の一部として、2 番目のロールがアカウントにデプロイされます。`customer_medialive_service_role`このロールは、Amazon S3、MediaStoreMediaStore、Media Live チャネルと入力に割り当てることができます。CloudWatch

アカウントでロールがプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの MediaLive の使用にはどのような制限がありますか？

AMS での MediaLive の使用に制限はありません。

Q: AMS アカウントで MediaLive を使用するための前提条件または依存関係は何ですか？

AMS アカウントで MediaLive を使用するための前提条件や依存関係はありません。

AMS SSP を使用して AMS アカウント AWS Elemental MediaPackage でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントの AWS Elemental MediaPackage 機能に直接アクセスします。 は、インターネット経由で配信するた

めのビデオ AWS Elemental MediaPackage を確実に準備して保護します。は、単一のビデオ入力から、接続されたTVs、携帯電話、コンピュータ、タブレット、ゲームコンソールで再生できる形式のビデオストリーム AWS Elemental MediaPackage を作成します。これにより、DVRs で一般的に見られるような、視聴者向けの一般的な動画機能 (起動、一時停止、巻き戻しなど) を簡単に実装できます。 AWS Elemental MediaPackage は、デジタル著作権管理 (DRM) を使用してコンテンツを保護することもできます。 は負荷に応じて自動的に AWS Elemental MediaPackage スケーリングされるため、視聴者は必要な容量を事前に正確に予測することなく、常に優れたエクスペリエンスを得ることができます。

詳細についてはAWS Elemental MediaPackageを参照してください。

AWS Managed Servicesでの MediaPackage に関するよくある質問

Q: AWS Elemental MediaPackage AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_mediapackage_author_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

2 番目のロール が提供されます。これは`customer_mediapackage_service_role`、S3 や Secrets Manager などの他のサービスとやり取りするための Media Live チャネルと入力に割り当てることができます。

Q: AMS アカウントでの MediaPackage の使用にはどのような制限がありますか？

AMS での MediaPackage の使用に制限はありません。

Q: AMS アカウントで MediaPackage を使用するための前提条件または依存関係は何ですか？

AMS アカウントで MediaPackage を使用するための前提条件や依存関係はありません。

AMS SSP を使用して AMS アカウント AWS Elemental MediaStore でプロビジョニングする

> **Note**
>
> 慎重に検討した結果、 AWS は 2025 年 11 月 13 日に MediaStore の廃止を決定しました。MediaStore のアクティブなお客様は、サービスのサポートが終了する 2025 年 11 月 13

日まで MediaStore を通常どおり使用できます。この日以降、MediaStore またはこのサービスが提供する機能を使用できなくなります。

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS Elemental MediaStore 機能に直接アクセスします。 AWS Elemental MediaStore は、メディア用に最適化された AWS ストレージサービスです。これにより、ライブストリーミングビデオコンテンツを配信するために必要なパフォーマンス、一貫性、低レイテンシーが得られます。 AWS Elemental MediaStore は、ビデオワークフローのオリジンストアとして機能します。その高性能機能は、最も要求の厳しいメディア配信ワークロードのニーズを満たすとともに、長期的で費用対効果の高いストレージを提供します。詳細についてはAWS Elemental MediaStoreを参照してください。

AWS Managed Services の MediaStore に関するよくある質問

Q: AMS アカウントの MediaStore へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (ct-1w8z66n899dct) 変更タイプで RFC を送信して MediaStore へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_mediastore_author_role`。この RFC の一部として、2 番目のロールがアカウントにデプロイされます。ロールは`MediaStoreAccessLogs`、この機能を有効にすることを選択した場合、MediaStore サービスが CloudWatch でアクティビティをログに記録するために使用されます。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

この時点で、AMS Operations はこのサービスロールをアカウント にもデプロイします`aws_code_pipeline_service_role_policy`。

Q: AMS アカウントでの MediaStore の使用にはどのような制限がありますか？

AMS での MediaStore の使用に制限はありません。

Q: AMS アカウントで MediaStore を使用するための前提条件または依存関係は何ですか？

AMS アカウントで MediaStore を使用するための前提条件や依存関係はありません。

AMS SSP を使用して AMS アカウント AWS Elemental MediaTailor でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS Elemental MediaTailor 機能に直接アクセスします。 AWS Elemental MediaTailor は、ブロード

キャストレベルのquality-of-serviceを犠牲にすることなく、ビデオプロバイダーが個別にターゲットを絞った広告をビデオストリームに挿入します。を使用すると AWS Elemental MediaTailor、ライブビデオまたはオンデマンドビデオの視聴者はそれぞれ、コンテンツとパーソナライズされた広告を組み合わせたストリームを受け取ります。ただし、他のパーソナライズされた広告ソリューションとは異なり、動画と広告は AWS Elemental MediaTailor 、視聴者のエクスペリエンスを向上させるためにブロードキャストグレードの動画品質で配信されます。 は、クライアント側とサーバー側の広告配信メトリクスの両方に基づいて自動レポート AWS Elemental MediaTailor を提供し、広告のインプレッションと視聴者の動作を正確に測定します。を使用して、予想外のオンデマンド視聴イベントを前払いコストなしで簡単に収益化できます AWS Elemental MediaTailor。また、広告配信レートも向上し、すべての動画からより多くの収益を得ることができ、さまざまなコンテンツ配信ネットワーク、広告決定サーバー、クライアントデバイスで動作します。

詳細についてはAWS Elemental MediaTailorを参照してください。

AWS Managed Services の MediaTailor に関するよくある質問

Q: AMS アカウントの MediaTailor へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (ct-1w8z66n899dct) 変更タイプで RFC を送信して MediaTailor へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer-mediatailor-role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの MediaTailor の使用にはどのような制限がありますか？

AMS での MediaTailor の使用に制限はありません。

Q: AMS アカウントで MediaTailor を使用するための前提条件または依存関係は何ですか？

AMS アカウントで MediaTailor を使用するための前提条件や依存関係はありません。

AMS SSP を使用して AMS アカウント AWS Global Accelerator でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Global Accelerator 機能に直接アクセスします。Global Accelerator は、世界中のユーザーが使用するインターネットアプリケーションの可用性とパフォーマンスを向上させるアクセラレーターを作成するネットワークレイヤーサービスです。詳細については、「Global Accelerator」を参照してください。

AWS Managed Services での Global Accelerator に関するよくある質問

一般的な質問と回答：

Q: Global Accelerator を AMS アカウントでセットアップするようにリクエストするにはどうすればよいですか？

AWS サービス RFC (管理 | AWS サービス | セルフプロビジョニングサービス) の送信を通じてアクセスをリクエストします。この RFC を通じて、次の IAM ロールがアカウントにプロビジョニングされます: `customer_global_accelerator_console_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでコンソールロールをオンボードする必要があります。

Q: AMS アカウントでの Global Accelerator の使用にはどのような制限がありますか？

Global Accelerator は、リージョンAWS 表に記載されている複数の AWS リージョンのエンドポイントをサポートするグローバルサービスです。

Q: AMS アカウントで Global Accelerator を使用するための前提条件または依存関係は何ですか？

Global Accelerator でアクセラレーターを設定するときは、静的 IP アドレスを 1 つ以上の AWS リージョンのリージョンエンドポイントに関連付けます。標準アクセラレーターの場合、エンドポイントは Network Load Balancer、Application Load Balancer、Amazon EC2 インスタンス、または Elastic IP アドレスです。カスタムルーティングアクセラレーターの場合、エンドポイントは 1 つ以上の EC2 インスタンスを持つ Virtual Private Cloud (VPC) サブネットです。

AMS SSP を使用して AMS アカウント AWS Glue でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS Glue 機能に直接アクセスします。 AWS Glue は、分析用のデータの準備とロードに役立つフルマネージド型の抽出、変換、ロード (ETL) サービスです。数回クリックするだけで、ETL ジョブを作成して実行できます AWS マネジメントコンソール。に保存されている AWS Glue データをポイントすると AWS、 はデータ AWS Glue を検出し、関連するメタデータ (テーブル定義やスキーマなど) を に保存します AWS Glue Data Catalog。カタログ化されると、データはすぐに検索可能で、クエリ可能で、ETL アクションに使用できます。詳細についてはAWS Glueを参照してください。

AWS Glue AWS Managed Servicesに関するよくある質問

一般的な質問と回答：

Q: AMS アカウントでの設定 AWS Glue をリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 変更タイプを追加 (ct-1w8z66n899dct) で RFC を送信 AWS Glue して、 へのアクセスをリクエストします。この RFC は、次の IAM ロールをアカウントにプロビジョニングします。

- `customer_glue_console_role`
- `customer_glue_service_role`

上記のロールには、以下のアタッチされたポリシーが含まれます。

- `customer_glue_secrets_manager_policy`
- `customer_glue_deny_policy`

アカウントでロールがプロビジョニングされたら、フェデレーションソリューションにロールをオンボードする必要があります。

クローラ、ジョブ、開発エンドポイント (特定のユースケースに必要なロール) にアクセスするには、デプロイ | 高度なスタックコンポーネント | Identity and Access Management (IAM) | エンティティまたはポリシーの作成 (ct-3dpd8mdd9jn1r) を使用して RFC を送信します。

Q: AMS アカウント AWS Glue で を使用することにはどのような制限がありますか？

制限はありません。の完全な機能は AWS Glue 、AMS アカウントで使用できます。ETL スクリプトを作成およびテストできるインタラクティブ環境の場合は、 AWS Glue Studio で Notebooks を使用します。 AWS Glue インタラクティブセッションとジョブノートブックは、 で使用できる AWS Glue AWS Glue のサーバーレス機能であり、 AWS Glue サービスロールを使用します。

AWS Glue 2.0 より前： AWS Glue ノートブックは、アカウントで Amazon EC2 インスタンスを起動する非マネージドリソースです。ベストプラクティスとして、独自の Amazon EC2 インスタンスを起動し、ノートブック環境と開発をサポートするために必要なソフトウェアをインストールします。詳細については、「チュートリアル: ETL スクリプトをテストおよびデバッグするためのローカル Apache Zeppelin ノートブックのセットアップ」および「スクリプトの開発に開発エンドポイントを使用する」を参照してください。

Q: AMS アカウント AWS Glue で を使用するための前提条件または依存関係は何ですか？

AWS Glue は、Amazon S3、CloudWatch、CloudWatch Logs に依存しています。推移的な依存関係はデータソースによって異なり、他の AWS Glue サービス機能が とやり取りしている可能性があります (Amazon Redshift、Amazon RDS、Athena など)。

AMS SSP を使用して AMS アカウント AWS Lake Formation でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS Lake Formation 機能に直接アクセスします。 AWS Lake Formation は、安全なデータレイクを数日で簡単にセットアップできるサービスです。データレイクは、分析用に準備および選別され、セキュリティ保護されたリポジトリで、すべてのデータを元の形式で保存します。データレイクを使用すると、データサイロを分解し、さまざまな種類の分析を組み合わせてインサイトを獲得し、優れたビジネス意思決定を導くことができます。

Lake Formation を使用したデータレイクの作成は、データソースおよび適用するデータアクセスとセキュリティポリシーを定義するのと同様に簡単です。Lake Formation は、データベースやオブジェクトストレージからのデータの収集とカタログ化、新しい Amazon S3 データレイクへのデータの移動、Machine Learning アルゴリズムを使用したデータのクリーンアップと分類、機密データへの安全なアクセスを支援します。ユーザーは、利用可能なデータセットとその適切な使用状況を説明する一元化されたデータカタログにアクセスできます (詳細については、AWS Glue「よくある質問」を参照してください)。その後、ユーザーはこれらのデータセットを、Amazon Redshift、Amazon Athena、Amazon EMR for Apache Spark (ベータ版) などの分析サービスと機械学習サービスの選択で活用します。Lake Formation は、 で利用可能な機能に基づいていますAWS Glue。

詳細についてはAWS Lake Formationを参照してください。

AWS Managed Services での Lake Formation に関するよくある質問

Q: AWS Lake Formation AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (レビューが必要) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_lakeformation_data_analyst_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

さらに、次の 2 つのロールはオプションです。

- `customer_lakeformation_admin_role`
- `customer_lakeformation_workflow_role`

管理者権限の場合、同じ SSPS 変更タイプ (ct-3qe6io8t6jtny) `customer_lakeformation_admin_role`の一部としてロールをオンボードすることを選択できます。

AWS Lake Formation コンソールでブループリントを作成する場合は、 をデプロイするために、管理 | その他 | その他の RFC (ct-1e1xtak34nx76) を送信する必要がありますcustomer_lakeformation_workflow_role。RFC では、ブループリントの作成時にバケットがソースである場合は、S3 バケット名を指定する必要があります。S3 バケットは AWS CloudTrail、設計図タイプが Classic Load Balancer Logs または Application Load Balancer Logs の場合に適用されます。

Q: AMS アカウント AWS Lake Formation で を使用することにはどのような制限がありますか？

Lake Formation の全機能は AMS で利用できます。

Q: AMS アカウント AWS Lake Formation で を使用するための前提条件または依存関係は何ですか？

Lake Formation は AWS Glue サービスと統合されるため、 AWS Glue ユーザーは Lake Formation アクセス許可を持つデータベースとテーブルにのみアクセスできます。さらに、 AWS Athena および Amazon Redshift ユーザーは、Lake Formation アクセス許可を持つ AWS Glue データベースとテーブルのみをクエリできます。

AMS SSP を使用して AMS アカウント AWS Lambda でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントの AWS Lambda 機能に直接アクセスします。サーバーをプロビジョニングまたは管理せずにコードを実行する AWS Lambda 。消費したコンピューティング時間に対してのみ料金が発生します。コードが実行されていない場合は料金は発生しません。Lambda を使用すると、ほぼあらゆるタイプのアプリケーションまたはバックエンドサービスのコードを、すべて管理なしで実行できます。コードをアップロードすると、Lambda はコードの実行とスケールに必要なすべてを高可用性で処理します。他のサービスから自動的にトリガーするようにコードを設定することも AWS 、ウェブやモバイルアプリから直接呼び出すこともできます。詳細についてはAWS Lambdaを参照してください。

AWS Managed Services の Lambda に関するよくある質問

Q: AWS Lambda AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) 変更タイプを送信してアクセスをリクエストします。この RFC は、`customer_lambda_admin_role`および の IAM ロールをアカウントにプロビジョニングしますcustomer_lambda_basic_execution_role。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウント AWS Lambda で を使用することにはどのような制限がありますか？

- Lambda 関数は、イベントソースによって呼び出されるように設計されています。Lambda イベントソースとして使用できるサービスのリストについては、「Using AWS Lambda with Other Services」を参照してください。現在、これらのサービスの一部が AMS アカウントで利用できるわけではありません。利用できないサービスが必要な場合は、AMS CSDM と連携して例外を申請します。
- デフォルトでは、AMS は `AWSLambdaBasicExecutionRole`および アクセスAWSXrayWriteOnlyAccess許可を含む基本的な Lambda 開始ロールを提供します。詳細については、AWS Lambda 「開始ロール」を参照してください。AMS VPC 内で Lambda 関数をプロビジョニングする機能など、追加のアクセス許可が必要な場合は、 管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (レビューが必要)(ct-3qe6io8t6jtny) 変更タイプを使用して RFC を送信します。

Q: AMS アカウント AWS Lambda で を使用するための前提条件または依存関係は何ですか？

開始するための前提条件や依存関係はありません AWS Lambdaが、特定のユースケースによっては、イベントソースを作成するための他の AWS サービスへのアクセスや、関数がさまざまなアクションを実行するための追加のアクセス許可が必要になる場合があります。追加のアクセス許可が必要な場合は、 管理 | AWS サービス | セルフプロビジョニングサービス | 変更タイプの追加 (レビューが必要) (ct-3qe6io8t6jtny) を使用して RFC を送信します。

Q: いずれかのアカウントで Lambda 関数を実行するにはどうすればよいですか？

コアアカウントに Lambda 関数をデプロイするには、次のガイドラインを使用します。

- の SSPS AWS Lambda がオンボードされていることを確認します。
- AMS リソースが保護および準拠している限り、AMS の責任の下でこのデプロイを禁止する特定の制限はありません。
- AMS で Lambda 関数を作成する場合は、まず提供されている SSPS ロールを使用する必要があります AWS Lambda。次に、AMS のサポートで関数をデプロイまたはサポートする場合は、CA に連絡して範囲外 (OOS) プロセスを開始します。

AMS SSP を使用して AMS アカウント AWS License Manager でプロビジョニングする

AMS Self-Service Provisioning (SSP) モードを使用して、AMS マネージドアカウント内の AWS License Manager 機能に直接アクセスします。 は AWS サービスと AWS License Manager 統合して、1 つの AWS アカウントを通じて複数の AWS アカウント、IT カタログ、オンプレミスのライセンスの管理を簡素化します。 AWS License Manager では、管理者はライセンス契約の条件をエミュレートするカスタマイズされたライセンスルールを作成し、Amazon EC2 のインスタンスが起動されたときにこれらのルールを適用できます。のルール AWS License Manager では、インスタンスの起動を物理的に停止するか、侵害について管理者に通知することで、ライセンス違反を制限できます。詳細についてはAWS License Managerを参照してください。

AWS Managed Services の License Manager に関するよくある質問

一般的な質問と回答：

Q: AMS アカウントでの設定 AWS License Manager をリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) change type で RFC を送信 AWS License Manager して、 へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_license_manager_role`。License Manager IAM ロールがアカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウント AWS License Manager で を使用することにはどのような制限がありますか？

所有する AMI に AWS License Manager ルールを関連付けることができます (「Owned by me」でフィルタリングされます)。 AMIs 制限の関連付けを AMI に強制することを選択した場合 (例: この AMI の 100 個の vCPU のみをサポート可能)、制限を使い果たすと、その AMI での今後の起動はブロックされ、「ライセンスなし」というエラーが返されます。これは、このサービスの意図した動作です (ライセンスを使い果たすことはできません)。制限を使い果たしても AMI を再度起動する必要がある場合は、 で設定されたルールを変更する必要があります AWS License Manager。

Q: AMS アカウント AWS License Manager で を使用するための前提条件または依存関係は何ですか？

AMS アカウント AWS License Manager で使用する前提条件や依存関係はありません。

AMS SSP を使用して AMS アカウント AWS Migration Hub でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS Migration Hub 機能に直接アクセスします。 は、複数の AWS およびパートナーソリューション間のアプリケーション移行の進行状況を追跡できる単一の場所 AWS Migration Hub を提供します。Migration Hub を使用すると、アプリケーションポートフォリオ全体の移行のステータスを可視化しながら、ニーズに最適な AWS およびパートナー移行ツールを選択できます。Migration Hub は、移行に使用されているツールに関係なく、個々のアプリケーションの主要なメトリクスと進行状況も提供します。これにより、すべての移行の進行状況の更新をすばやく取得し、問題を簡単に特定してトラブルシューティングし、移行プロジェクトに費やす全体的な時間と労力を削減できます。詳細についてはAWS Migration Hubを参照してください。

AWS Managed Services の Migration Hub に関するよくある質問

よくある質問と回答：

Q: AMS アカウントの Migration Hub へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (ct-1w8z66n899dct) 変更タイプで RFC を送信して Migration Hub へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_migrationhub_author_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: Migration Hub にはどのような制限がありますか？

なし。

Q: Migration Hub を有効にするための前提条件は何ですか？

AMS アカウントで Migration Hub の使用を開始するための前提条件はありません。ただし、Migration Hub 以外のアクセス許可は、サーバー情報をアップロードするためのアクセス許可を Amazon S3 に書き込むなど、サービスの管理中に必要になる場合があります。

AMS SSP を使用して AMS アカウント AWS Outposts でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS Outposts 機能に直接アクセスします。 AWS Outposts は、 AWS インフラストラクチャ、

AWS サービス、APIs、ツールを事実上あらゆるデータセンター、コロケーションスペース、またはオンプレミス施設に拡張し、一貫したハイブリッドエクスペリエンスを実現します。 AWS Outposts は、オンプレミスシステム、ローカルデータ処理、またはローカルデータストレージへの低レイテンシーアクセスを必要とするワークロードに適しています。詳細についてはAWS Outpostsを参照してください。

AWS Outposts AWS Managed Servicesに関するよくある質問

一般的な質問と回答：

Q: AMS アカウントでの設定 AWS Outposts をリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) change type を使用して RFC を送信 AWS Outposts して、 へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_outposts_role`。アカウントにロールがプロビジョニングされたら、フェデレーションソリューションにロールをオンボードする必要があります。

Q: AMS アカウント AWS Outposts で を使用することにはどのような制限がありますか？

AMS アカウント AWS Outposts での の使用に制限はありません。

Q: AMS アカウント AWS Outposts で を使用するための前提条件または依存関係は何ですか？

AMS アカウント AWS Outposts で使用する前提条件や依存関係はありません。

AMS SSP を使用して AMS アカウント AWS Resilience Hub でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントの AWS Resilience Hub 機能に直接アクセスします。 AWS Resilience Hub は AWS 、アプリケーションを事前に準備し、中断から保護するのに役立ちます。Resilience Hub は、ソフトウェア開発ライフサイクルに統合される耐障害性評価と検証を提供し、耐障害性の弱点を明らかにします。Resilience Hub は、アプリケーションが目標復旧時間 (RTO) と目標復旧時点 (RPO) の目標を達成できるかどうかを推定し、本番環境にリリースされる前に問題を解決するのに役立ちます。 AWS アプリケーションを本番環境にデプロイした後、Resilience Hub を使用してアプリケーションの回復体制の追跡を続行できます。停止が発生した場合、Resilience Hub はオペレーターに通知を送信して、関連する復旧プロセスを起動します。

AWS Resilience Hub AWS Managed Servicesに関するよくある質問

よくある質問と回答：

Q: AWS Resilience Hub AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (ct-1w8z66n899dct) 変更タイプで RFC を送信して、Resilience Hub へのアクセスをリクエストします。この RFC は、次の IAM ロールとポリシーをアカウントにプロビジョニングします。

IAM; ロール

- `customer_resiliencehub_console_role`
- `customer_resiliencehub_service_role`

ポリシー

- `customer_resiliencehub_console_policy`
- `customer_resiliencehub_service_policy`

アカウントにロールがプロビジョニングされたら、フェデレーションソリューションcustomer_resiliencehub_console_roleでロールをオンボードする必要があります。

Q: AMS アカウント AWS Resilience Hub で を使用することにはどのような制限がありますか？

制限はありません。Resilience Hub のフル機能は、AMS アカウントで使用できます。

Q: AMS アカウント AWS Resilience Hub で を使用するための前提条件または依存関係は何ですか？

AMS アカウントで Resilience Hub を使用するための前提条件や依存関係はありません。

AMS SSP を使用して AMS アカウント AWS Secrets Manager でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS Secrets Manager 機能に直接アクセスします。アプリケーション、サービス、IT リソースへのアクセスに必要なシークレットを保護する AWS Secrets Manager のに役立ちます。このサービスを使用すると、データベースクレデンシャル、APIキー、およびその他のシークレットをライフ

サイクル全体で簡単にローテーション、管理、および取得できます。ユーザーとアプリケーションは Secrets Manager APIs を呼び出すことでシークレットを取得するため、機密情報をプレーンテキストでハードコードする必要がなくなります。Secrets Manager には、Amazon RDS、Amazon Redshift、Amazon DocumentDB の統合機能が組み込まれたシークレットローテーションが用意されています。また、このサービスは API キーや OAuth トークンなど、他のタイプのシークレットにも拡張できます。詳細についてはAWS Secrets Managerを参照してください。

> **Note**
>
> デフォルトでは、AMS 演算子は、アカウントのデフォルト AWS KMS キー (CMK) を使用して暗号化 AWS Secrets Manager された のシークレットにアクセスできます。シークレットを AMS オペレーションにアクセスできるようにするには、シークレットに保存されているデータに適したアクセス許可を定義する AWS Key Management Service （ AWS KMS) キーポリシーを持つカスタム CMK を使用します。

AWS Managed Services の Secrets Manager に関するよくある質問

Q: AWS Secrets Manager AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (ct-3qe6io8t6jtny) 変更タイプで RFC を送信して Secrets Manager へのアクセスをリクエストします。この RFC は、 `customer_secrets_manager_console_role`および の IAM ロールをアカウントにプロビジョニングします`customer-rotate-secrets-lambda-role`。`customer_secrets_manager_console_role` は、シークレットをプロビジョニングおよび管理するための管理者ロールとして使用され、シークレットをローテーションする Lambda 関数の Lambda 実行ロールとして`customer-rotate-secrets-lambda-role`使用されます。アカウントにプロビジョニングされたら、フェデレーションソリューションで`customer_secrets_manager_console_role`ロールをオンボードする必要があります。

Q: AMS アカウント AWS Secrets Manager での の使用にはどのような制限がありますか？

のフル機能は、シークレットの自動ローテーション機能とともに、AMS アカウントで AWS Secrets Manager 使用できます。ただし、「ローテーションを実行するための新しい Lambda 関数の作成」を使用したローテーションの設定はサポートされていません。これは、変更管理プロセスをバイパスする CloudFormation スタックの作成 (IAM ロールと Lambda 関数の作成) に昇格されたアクセス許可が必要なためです。AMS Advanced は、「既存の Lambda 関数を使用してローテーションを実行

する」のみをサポートします。ここでは、Lambda 関数を管理し、 AWS Lambda SSPS 管理者ロールを使用してシークレットをローテーションします。AMS Advanced は、シークレットをローテーションするために Lambda を作成または管理しません。

Q: AMS アカウント AWS Secrets Manager で を使用するための前提条件または依存関係は何ですか？

次の名前空間は AMS が使用するために予約されており、 への直接アクセスの一部としては使用できません AWS Secrets Manager。

- arn:aws:secretsmanager:*:*:secret:ams-shared/*
- arn:aws:secretsmanager:*:*:secret:customer-shared/*
- arn:aws:secretsmanager:*:*:secret:ams/*

Secrets Manager を使用したキーの共有 (AMS SSPS)

RFC、サービスリクエスト、またはインシデントレポートのプレーンテキストでシークレットを AMS と共有すると、情報開示インシデントが発生し、AMS はケースからの情報とキーを再生成するリクエストを編集します。

AWS Secrets Manager (Secrets Manager) は、この名前空間 で使用できますcustomer-shared。

Secrets Manager を使用したキーの共有に関するよくある質問

Q: Secrets Manager を使用して共有する必要があるシークレットのタイプは何ですか？

例としては、VPN 作成用の事前共有キー、認証キー (IAM、SSH)、ライセンスキー、パスワードなどの機密キーなどがあります。

Q: Secrets Manager を使用して AMS とキーを共有するにはどうすればよいですか？

1. フェデレーティッドアクセスと適切なロールを使用して、 AWS マネジメントコンソールにログインします。

   SALZ の場合は、 Customer_ReadOnly_Role

   MALZ の場合は、AWSManagedServicesChangeManagementRole。
2. AWS Secrets Manager コンソールに移動し、新しいシークレットを保存するをクリックします。

3. [その他のシークレット] を選択します。
4. シークレット値をプレーンテキストとして入力し、デフォルトの KMS 暗号化を使用します。[次へ] をクリックします。
5. シークレット名と説明を入力します。名前は常にカスタマー共有/ で始まります。たとえば、customer-shared/mykey2022 などです。[次へ] をクリックします。
6. 自動ローテーションを無効にしたまま、次へをクリックします。
7. Store を確認してクリックし、シークレットを保存します。
8. シークレットを識別して取得できるように、サービスリクエスト、RFC、またはインシデントレポートを通じてシークレット名を返信してください。

Q: Secrets Manager を使用してキーを共有するには、どのようなアクセス許可が必要ですか？

SALZ: `customer_secrets_manager_shared_policy`マネージド IAM ポリシーを探し、ポリシードキュメントが以下の作成ステップでアタッチされているものと同じであることを確認します。ポリシーが次の IAM ロールにアタッチされていることを確認します: `Customer_ReadOnly_Role`。

MALZ: `ams-shared`名前空間で `GetSecretValue`アクションを許可する`AWSManagedServicesChangeManagementRole`ロールに `AMSSecretsManagerSharedPolicy`がアタッチされていることを確認します。

例:

```
{
 "Action": "secretsmanager:*",
 "Resource": [
 "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
 "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
 ],
 "Effect": "Allow",
 "Sid": "AllowAccessToSharedNameSpaces"
 }
```

> **Note**
>
> セルフサービスプロビジョニングサービス AWS Secrets Manager として を追加すると、必要なアクセス許可が付与されます。

AMS SSP を使用して AMS アカウント AWS Security Hub CSPM でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS Security Hub CSPM 機能に直接アクセスします。 AWS Security Hub CSPM では、 内のセキュリティ状態 AWS と、セキュリティ業界標準およびベストプラクティスへの準拠を包括的に把握できます。Security Hub は、複数の AWS アカウント、サービス、およびサポートされているサードパーティーパートナーからのセキュリティとコンプライアンスの検出結果を一元化して優先順位付けし、セキュリティの傾向を分析し、最も優先度の高いセキュリティ問題を特定するのに役立ちます。詳細についてはAWS Security Hub CSPMを参照してください。

AWS Managed Services の Security Hub に関するよくある質問

Q: AWS Security Hub CSPM AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (ct-1w8z66n899dct) 変更タイプで RFC を送信して、Security Hub へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_securityhub_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントで Security Hub を使用することにはどのような制限がありますか？

アーカイブ機能は、潜在的なセキュリティおよび運用上のリスクとして認識されており、自己プロビジョニングサービスセキュリティロールの一部として制限されています。

Q: AMS アカウント AWS Security Hub CSPM で を使用するための前提条件または依存関係は何ですか？

AMS アカウント AWS Security Hub CSPM で使用する前提条件や依存関係はありません。

AMS SSP を使用して AMS アカウント AWS Service Catalog AppRegistry でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで AppRegistry 機能に直接アクセスします。AppRegistry を使用すると、アプリケーションの検索、レポート、管理アクションを一元的に実行できます。ビルダーが 1 つの AWS アカウントでアプリケーションを作成することはめったにありません。通常、アプリケーションリソースは、開発、テスト、本番稼働などのライフサイクルフェーズごとに分離されます。AppRegistry を使用すると、定義した AWS アカウント全体ですべてのリソースコレクションをグループ化して表示できます。

AppRegistry を使用すると、 AWS アプリケーション、アプリケーションに関連付けられているリソースのコレクション、およびアプリケーション属性グループを保存できます。詳細については、AppRegistry とは」を参照してください。

よくある質問: AMS AWS Service Catalog AppRegistry 内

Q: AWS Service Catalog AppRegistry AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 追加 (レビューが必要) (ct-3qe6io8t6jtny) 変更タイプで RFC を送信して AppRegistry へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer-appregistry-console-role`。アカウントでプロビジョニングしたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウント AWS Service Catalog AppRegistry で を使用することにはどのような制限がありますか？

`'Name'` タグで AMS 名前空間を使用することを除き、AppRegistry サービスへのフルアクセスが提供されます。

Q: AMS アカウント AWS Service Catalog AppRegistry で を使用するための前提条件または依存関係は何ですか？

AMS アカウントで AppRegistry を使用するための前提条件や依存関係はありません。

AMS SSP を使用して AMS アカウント AWS Shield Advanced でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS Shield Advanced 機能に直接アクセスします。 AWS Shield Advanced は、 で実行されているアプリケーションを保護するマネージド型分散型サービス拒否 (DDoS) 保護サービスです AWS。Shield Advanced は、アプリケーションのダウンタイムとレイテンシーを最小限に抑える常時オンの検出と自動インライン緩和を提供するため、DDoS 保護のメリットを享受するために AWS Support を関与させる必要はありません。Standard AWS Shield と Advanced の 2 つの階層があります。AMS には Shield Advanced が用意されています。詳細については、「Shield Advanced」を参照してください。

すべての AWS お客様は AWS Shield Standard、追加料金なしで自動保護を利用できます。 は、ウェブサイトまたはアプリケーションをターゲットとする最も一般的な、頻繁に発生するネッ

トワークおよびトランスポートレイヤーの DDoS 攻撃に対して AWS Shield Standard 防御します。Amazon CloudFront および Amazon Route 53 AWS Shield Standard で を使用すると、すべての既知のインフラストラクチャ (レイヤー 3 および 4) 攻撃に対する包括的な可用性保護が得られます。

Amazon Elastic Compute Cloud (Amazon EC2)、Elastic Load Balancing (ELB)、Amazon CloudFront AWS Global Accelerator、Amazon Route 53 リソースで実行されているアプリケーションをターゲットとする攻撃に対する保護レベルを高めるには、 にサブスクライブできます AWS Shield Advanced。

に付属するネットワークおよびトランスポートレイヤーの保護に加えて AWS Shield Standard、は、大規模で高度な DDoS 攻撃に対する追加の検出と軽減、攻撃に対するほぼリアルタイムの可視性、およびウェブアプリケーションファイアウォールとの統合 AWS Shield Advanced を提供します。 AWS Shield Advanced また AWS WAF、 は AWS Shield 、レスポンスチーム (SRT) への 24 時間 365 日アクセス、および Amazon Elastic Compute Cloud (Amazon EC2)、Elastic Load Balancing (Elastic Load Balancing)、Amazon CloudFront AWS Global Accelerator、および Amazon Route 53 料金の DDoS 関連のスパイクに対する保護も提供します。

AWS Managed Servicesでの Shield Advanced に関するよくある質問

Q: AMS アカウントで Shield Advanced へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) 変更タイプで RFC を送信して、Shield Advanced へのアクセスをリクエストします。この RFC は、 `customer_shield_role`および の IAM ロールをアカウントにプロビジョニングします`aws_drt_shield_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

ロールがアカウントにデプロイされたら、 `customer_shield_role` を使用してアカウントの AWS Shield Advanced へのサブスクリプションを確認できます。

> **Note**
>
> の使用には、月額料金と 1 年間のコミットメントがあることに注意してください AWS Shield Advanced。さらに、AMS AWS Shield Advanced で を使用すると、AMS が AWS Shield (SRT) にエスカレートすることを許可します。SRT は、エスカレートされた分散サービス拒否 (DDoS) インシデント中にウェブアプリケーションファイアウォール (AWS WAF) ルールを変更する可能性があります。これらの変更は、AMS と連携して行われます。

Q: AMS アカウントでの Shield Advanced の使用にはどのような制限がありますか？

制限ではありませんが、Shield Advanced を使用すると がデプロイされるため`aws_drt_shield_role`、 AWS Shield チーム (SRT) はエスカレーションされた DDoS インシデント中に AMS アカウント内の AWS WAF ルールに緊急変更を加えることができます。これは、DDoS 攻撃の迅速な修復のために AMS によって推奨され、SRT への AMS エスカレーション後に行われます。

Q: AMS アカウントで Shield Advanced を使用するための前提条件または依存関係は何ですか？

AMS アカウントで Shield Advanced を使用するための前提条件や依存関係はありません。

AMS SSP を使用して AMS アカウント AWS Snowball Edge でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで Snowball Edge 機能に直接アクセスします。Snowball Edge はペタバイト規模のデータ転送ソリューションで、安全なデバイスを使用して大量のデータを AWS クラウドとの間で転送します。Snowball Edge は、高いネットワークコスト、長い転送時間、セキュリティ上の懸念など、大規模なデータ転送に関する一般的な課題に対処します。Snowball Edge を使用して、分析データ、ゲノムデータ、ビデオライブラリ、イメージリポジトリ、バックアップを移行し、データセンターのシャットダウン、テープ交換、またはアプリケーション移行プロジェクトの一部をアーカイブできます。Snowball Edge によるデータ転送はシンプル、高速、より安全であり、高速インターネットによるデータ転送のコストの 5 分の 1 にすぎません。

Snowball Edge では、データを転送するためにコードを記述したり、ハードウェアを購入したりする必要はありません。まず、 AWS マネジメントコンソールを使用して Snowball のインポートジョブを作成すると、Snowball デバイスが自動的に配送されます。到着したら、デバイスをローカルネットワークに接続し、Snowball クライアント (「クライアント」) をダウンロードして実行して接続を確立し、クライアントを使用してデバイスに転送するファイルディレクトリを選択します。その後、クライアントはファイルを暗号化し、高速でデバイスに転送します。転送が完了し、デバイスを返却する準備ができると、E Ink 配送ラベルが自動的に更新され、Amazon Simple Notification Service (Amazon SNS)、テキストメッセージ、または コンソールで直接ジョブステータスを追跡できます。詳細についてはAWS Snowball Edgeを参照してください。

AWS Managed Services の Snowball Edge に関するよくある質問

一般的な質問と回答：

Q: AWS Snowball Edge AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか？

AMS での Snowball Edge の実装は、2 ステップのプロセスです。

1. 管理を送信する | その他 | その他 | 変更タイプ (ct-1e1xtak34nx76) を作成し、AMS アカウントの Snowball Edge のサービスロールをリクエストします。
2. Management | AWS service | Self-provisioned service | Add change type (ct-1w8z66n899dct) を送信してユーザーアクセスをリクエストします。この RFC は、、`customer_snowball_console_role`、`customer_snowball_export_role`および の IAM ロールをアカウントにプロビジョニングします`customer_snowball_import_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウント AWS Snowball Edge で を使用することにはどのような制限がありますか？

の完全な機能は AWS Snowball Edge 、AMS アカウントで使用できます。

Q: AMS アカウント AWS Snowball Edge で を使用するための前提条件または依存関係は何ですか？

上記のように、サービスロールアカウントが必要です。

AMS SSP を使用して AMS アカウント AWS Step Functions でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS Step Functions 機能に直接アクセスします。 AWS Step Functions は、ビジュアルワークフローを使用して分散アプリケーションとマイクロサービスのコンポーネントを調整できるウェブサービスです。それぞれ別個の関数 (タスク) を実行する個々のコンポーネントからアプリケーションを構築することで、簡単にアプリケーションをスケールおよび変更できます。Step Functions を使えば、安心してコンポーネントを調整し、アプリケーションの関数を配置できます。Step Functions には、アプリケーションのコンポーネントを一連のステップとして視覚化するためのグラフィカルコンソールが用意されています。各ステップを自動的にトリガーして追跡し、エラーが発生したときに再試行するため、アプリケーションは毎回、想定どおりに順番に実行されます。また、Step Functions では各ステップの状態がログに記録されるため、問題が発生した場合は、問題を簡単に診断およびデバッグできます。詳細についてはAWS Step Functionsを参照してください。

AWS Managed Services の Step Functions に関するよくある質問

よくある質問と回答：

Q: AWS Step Functions AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add change type (ct-1w8z66n899dct) を使用して RFC を送信 AWS Step Functions して、 へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_step_functions_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウント AWS Step Functions で を使用することにはどのような制限がありますか？

の完全な機能は AWS Step Functions 、AMS アカウントで使用できます。

Q: AMS アカウント AWS Step Functions で を使用するための前提条件または依存関係は何ですか？

実行時に、Step Functions で使用されるロールは、ステップ関数で使用されるサービスにアクセスできる必要があります。たとえば、ステップ関数は Lambda 関数に依存することができます。ステップ関数を作成するユーザーは、Lambda 関数を同時に作成している可能性があり、そのサービスへのアクセスもリクエストする必要があります。

AMS SSP を使用して AMS AWS Systems Manager アカウントに Parameter Store をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで AWS Systems Manager Parameter Store 機能に直接アクセスします。 AWS Systems Manager Parameter Store は、設定データ管理とシークレット管理のための安全な階層型ストレージを提供します。パスワード、データベース文字列、およびライセンスコードなどのデータをパラメータ値として保存することができます。値はプレーンテキストまたは暗号化されたデータとして保存できます。次に、パラメータの作成時に指定した一意の名前を使用して値を参照できます。スケーラビリティ、可用性、耐久性に優れた Parameter Store は AWS クラウドでサポートされています。詳細については、AWS Systems Manager 「Parameter Store」を参照してください。

> **Note**
>
> ライフサイクル管理を備えた専用シークレットストアが必要な場合は、Parameter Store AMS SSP を使用して AMS アカウント AWS Secrets Manager でプロビジョニングするの

代わりに を使用します。Secrets Manager は、シークレットを自動的にローテーションできるようにすることで、セキュリティとコンプライアンスの要件を満たすのに役立ちます。Secrets Manager は、Amazon RDS 上の MySQL、PostgreSQL、Amazon Aurora の統合を組み込み、Lambda 関数をカスタマイズすることで他のタイプのシークレットに拡張できます。

AWS Systems Manager AWS Managed Services のパラメータストアに関するよくある質問

よくある質問と回答：

Q: AMS アカウントの Systems Manager パラメータストアへのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add change type (ct-1w8z66n899dct) を使用して RFC を送信して、 AWS Systems Manager Parameter Store へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_systemsmanager_parameterstore_console_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの AWS Systems Manager Parameter Store の使用にはどのような制限がありますか？

AWS マネージドキーを使用する必要があります。アクセスはカスタム KMS キーの作成に制限されます。ただし、カスタムキーが必要な場合は、RFC を送信して、Deployment | Advanced Stack Components | KMS Key | Create change type (ct-1d84keiri1jhg) with this IAM role, `customer_systemsmanager_parameterstore_console_role` as the value for the `IAMPrincipalsRequiringDecryptPermissions`および `IAMPrincipalsRequiringEncryptPermissionsPrincipal` parameters を使用してカスタマーマネージドキー (CMK) を作成します。KMS キーを作成したら、それを使用して Secure String を作成できます。

Q: AMS アカウントで AWS Systems Manager Parameter Store を使用するための前提条件または依存関係は何ですか？

前提条件はありませんが、SSM パラメータストアは KMS に依存して Secure String を作成するため、パラメータストアに保存されている値を暗号化および復号できます。

AMS SSP を使用して AMS アカウントに AWS Systems Manager オートメーションをプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで AWS Systems Manager オートメーション機能に直接アクセスします。 AWS Systems Manager Automation は、ランブック、アクション、サービスクォータを使用して、Amazon Elastic Compute Cloud インスタンスおよびその他の AWS リソースの一般的なメンテナンスおよびデプロイタスクを簡素化します。これにより、自動化を大規模に構築、実行、モニタリングできます。Systems Manager Automation は、Systems Manager がマネージドインスタンスで実行するアクションを定義する Systems Manager ドキュメントの一種です。マネージドインスタンス内でコマンドやオートメーションスクリプトを実行するなど、一般的なメンテナンスおよびデプロイタスクを実行するために使用されるランブック。Systems Manager には、Amazon Elastic Compute Cloud タグを使用してインスタンスの大規模なグループをターゲットにするのに役立つ機能と、定義した制限に従って変更をロールアウトするのに役立つ速度制御が含まれています。ランブックは、JavaScript Object Notation (JSON) または YAML を使用して記述されます。ただし、Systems Manager Automation コンソールの [Document Builder (ドキュメントビルダー)] を使用すると、ネイティブの JSON または YAML で作成しなくても、ランブックを作成できます。または、Systems Manager が提供するランブックを、ニーズに合った事前定義されたステップで使用することもできます。詳細については、AWS Systems Manager ドキュメントの「ランブックの使用」を参照してください。

> **Note**
>
> Systems Manager Automation は、ランブックで使用できる 20 のアクションタイプをサポートしていますが、AMS Advanced アカウントで使用するランブックの作成時に使用できるアクションの数は限られています。同様に、Systems Manager が提供するランブックは、限られた数だけ、直接使用することも、独自のランブック内から使用することもできます。詳細については、次の FAQ の制限を参照してください。

AWS Systems Manager AWS Managed Services での自動化に関するよくある質問

一般的な質問と回答：

Q: AMS アカウントの Systems Manager Automation へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add change type (ct-1w8z66n899dct) を使用して RFC を送信して、 AWS Systems Manager オートメーションへのアクセスをリ

クエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_systemsmanager_automation_console_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウントでの AWS Systems Manager オートメーションの使用にはどのような制限がありますか？

マネージドインスタンス内でコマンドやスクリプトを実行するためだけに、自動化のために Systems Manager がサポートするアクションのセットを制限してランブックを作成する必要があります。使用できるアクションと制限の概要は次のとおりです。

AWS Systems Manager 自動化の制限

アクション	説明	制限
aws:assertAwsResourceProperty –	AWS リソースの状態またはイベントの状態をアサートする	EC2 インスタンスのみ
aws:aws:branch –	条件付きオートメーションステップを実行する	制限なし
aws:createTags –	AWS リソースのタグを作成する	作成した SSM オートメーションランブックのみ
aws:executeAutomation –	別のオートメーションを実行する	作成したオートメーションランブックのみ
aws:executeScript –	スクリプトを実行する	サービスに対して API コールを行わないスクリプトのみ
aws:pause –	オートメーションを一時停止する	制限なし
aws:runCommand –	マネージドインスタンスでコマンドを実行する	System Manager が提供するドキュメントのみを使用する - AWS-RunShellScript および AWS-RunPowerShellScript
aws:sleep –	オートメーションの遅延	制限なし

アクション	説明	制限
aws:waitForAwsResourceProperty –	AWS リソースプロパティを待機する	EC2 インスタンスのみ

Systems Manager コンソール内から「Run Command」機能を使用して、Systems Manager が提供するランブック AWS-RunShellScript および AWS-RunPowerShellScript でコマンドまたはスクリプトを直接実行することもできます。これらのランブックをランブック内にネストして、追加の検証前や検証後、または複雑な自動化ロジックに対応することもできます。

ロールは最小特権の原則に従い、マネージドインスタンス内でコマンドやスクリプトを実行することを目的としたランブックの実行の詳細を作成、実行、取得するために必要なアクセス許可のみを提供します。 AWS Systems Manager サービスが提供する他の機能に対するアクセス許可は付与されません。この機能を使用すると自動化ランブックを作成できますが、ランブックの実行を AMS 所有リソースの対象にすることはできません。

Q: AMS アカウントで AWS Systems Manager オートメーションを使用するための前提条件または依存関係は何ですか？

前提条件はありませんが、ランブックの作成中は、内部プロセスやコンプライアンスコントロールが準拠していることを確認する必要があります。また、本番稼働用リソースに対してランブックを実行する前に、ランブックを徹底的にテストすることをお勧めします。

Q: Systems Manager ポリシーを他の IAM ロールにアタッチ**customer_systemsmanager_automation_policy**できますか？

いいえ。他のセルフプロビジョニング対応サービスとは異なり、このポリシーはプロビジョニングされたデフォルトロール にのみ割り当てることができますcustomer_systemsmanager_automation_console_role。

他の SSPS ロールのポリシーとは異なり、この SSM SSPS ポリシーは他のカスタム IAM ロールと共有できません。これは、この AMS サービスがマネージドインスタンス内でコマンドまたはオートメーションスクリプトを実行する場合のみであるためです。これらのアクセス許可を他のカスタム IAM ロールにアタッチすることが許可され、他の のサービスに対するアクセス許可がある場合、許可されるアクションの範囲はマネージドサービスにまで及ぶ可能性があり、アカウントのセキュリティ体制が低下する可能性があります。

AMS 技術標準に照らして変更リクエスト (RFCs「RFC セキュリティレビュー」を参照してください。

> **Note**
>
> AWS Systems Manager では、 アカウントと共有されているランブックを使用できます。共有ランブックを使用する場合は注意を払い、デューディリジェンスチェックを実行することをお勧めします。ランブックを実行する前に、必ずコンテンツを確認して、それらが実行するコマンド/スクリプトを理解してください。詳細については、「共有 SSM ドキュメントのベストプラクティス」を参照してください。

AMS SSP を使用して AMS アカウント AWS Transfer Family でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで AWS Transfer Family (Transfer Family) 機能に直接アクセスします。 AWS Transfer Family は、セキュアファイル転送プロトコル (SFTP) 経由で Amazon Simple Storage Service (Amazon S3) ストレージとの間でファイルを転送できるフルマネージド AWS サービスです。SFTP は、Secure Shell (SSH) ファイル転送プロトコルとも呼ばれています。SFTP は、金融サービス、医療、広告、リテールなどのさまざまな業界間におけるデータ交換ワークフローに使用されます。

SFTP を使用すると、サーバーインフラストラクチャを実行する AWS ことなく、 AWS の SFTP サーバーにアクセスできます。このサービスを使用して、エンドユーザーのクライアントと設定をそのまま維持 AWS しながら、SFTP ベースのワークフローを に移行できます。まずホスト名を SFTP サーバーエンドポイントに関連付け、ユーザーを追加して適切なレベルのアクセスでプロビジョニングします。これを行うと、ユーザーの転送リクエストは SFTP AWS サーバーエンドポイントから直接処理されます。詳細については、AWS Transfer for SFTP「」、「SFTP 対応サーバーの作成」を参照してください。

AWS Transfer for SFTP AWS Managed Servicesに関するよくある質問

一般的な質問と回答：

Q: AWS Transfer for SFTP AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add change type (ct-1w8z66n899dct) を使用して RFC を送信 AWS Transfer for SFTP して、 へのアクセスをリクエストします。この RFC を通じて、次の IAM ロールとポリシーがアカウントにプロビジョニングされます。

- customer_transfer_author_role。 このロールは、 コンソールを使用して SFTP サービスを管理するように設計されています。
- customer_transfer_sftp_server_logging_role。 このロールは、SFTP サーバーにアタッチされるように設計されています。これにより、SFTP サーバーは CloudWatch にログをプルできます。
- customer_transfer_sftp_user_role。 このロールは、SFTP ユーザーにアタッチされるように設計されています。これにより、SFTP ユーザーは S3 バケットとやり取りできます。
- policy customer_transfer_scope_down_policy。 このポリシーは、SFTP ユーザーに適用して、S3 バケットへのアクセスをホームフォルダに制限できるスコープダウンポリシーです。
- customer_transfer_sftp_efs_user_role。 このロールは、SFTP ユーザーにアタッチされるように設計されています。これにより、SFTP ユーザーは EFS ファイルシステムとやり取りできます。

アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウント AWS Transfer for SFTP で を使用することにはどのような制限がありますか？

AWS SFTP 設定の転送は、AMS インフラストラクチャへの変更を防ぐために、「AMS-」または「MC-」プレフィックスのないリソースに制限されます。

Q: AMS アカウント AWS Transfer for SFTP で を使用するための前提条件または依存関係は何ですか？

- AWS Transfer for SFTP サーバーとユーザーを作成する前に、キーワード「転送」を含む名前の Amazon S3 バケットが必要です。
- 「顧客識別プロバイダー」を使用するには、API Gateway、Lambda 関数、ユーザーリポジトリ (AD、Secrets Manager など) をデプロイする必要があります。詳細については、「ID プロバイダー AWS Transfer for SFTP の使用と操作のパスワード認証 AWS Secrets Managerを有効にする」を参照してください。 https://docs.aws.amazon.com/transfer/latest/userguide/authenticating-users.html

AMS SSP を使用して AMS アカウント AWS Transit Gateway でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS Transit Gateway 機能に直接アクセスします。 AWS Transit Gateway は、Amazon Virtual Private Cloud (VPCs) とオンプレミスネットワークを単一のゲートウェイに接続できるサービスです。で実行されているワークロードの数が増えるにつれて AWS、増加に対応するために、複数のアカウントと Amazon VPCs にまたがってネットワークをスケールできる必要があります。現在、ピアリングを使用して Amazon VPCsのペアを接続できます。ただし、接続ポリシーを一元管理することなく、多くの Amazon VPCs point-to-point接続を管理することは、運用コストが高く、面倒な作業になる可能性があります。オンプレミス接続の場合は、 AWS VPN を個々の Amazon VPC にアタッチする必要があります。このソリューションでは、構築に時間がかかり、VPCs 数が数百に増加すると管理が困難になる場合があります。詳細についてはAWS Transit Gatewayを参照してください。

AWS Transit Gateway AWS Managed Servicesに関するよくある質問

一般的な質問と回答：

Q: AWS Transit Gateway AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add change type (ct-1w8z66n899dct) を使用して RFC を送信 AWS Transit Gateway して、 へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_tgw_console_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウント AWS Transit Gateway で を使用することにはどのような制限がありますか？

のフル機能は AWS Transit Gateway 、Transit Gateway ルーティングのルートテーブルの変更を除き、AMS シングルアカウントランディングゾーンアカウントで使用できます。管理 | その他 | その他 | 変更タイプの作成 (ct-1e1xtak34nx76) を送信してルートテーブルの変更をリクエストします。

> **Note**
>
> このサービスは、マルチアカウントランディングゾーン (MALZ) ではなく、シングルアカウントランディングゾーン (SALZ) でのみサポートされています。

Q: AMS アカウント AWS Transit Gateway で を使用するための前提条件または依存関係は何ですか？

AMS アカウント AWS Transit Gateway で使用する前提条件や依存関係はありません。

AMS SSP を使用して AMS アカウントで AWS WAF ウェブアプリケーションファイアウォールをプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウント内の AWS WAF 機能に直接アクセスします。 AWS WAF は、アプリケーションの可用性に影響を与えたり、セキュリティを侵害したり、過剰なリソースを消費したりする一般的なウェブエクスプロイトからウェブアプリケーションを保護するウェブアプリケーションファイアウォール (AWS WAF) AWS WAF です。 は、カスタマイズ可能なウェブセキュリティルールを定義することで、ウェブアプリケーションに対して許可またはブロックするトラフィックを制御します。を使用して AWS WAF 、SQL インジェクションやクロスサイトスクリプティングなどの一般的な攻撃パターンをブロックするカスタムルールと、特定のアプリケーション用に設計されたルールを作成できます。

詳細については、「 AWS WAF - Web Application Firewall」を参照してください。

AMS は、 のモニタリング (CloudWatch アラーム/イベント/MMS アラート) をサポートしていません AWS WAF。の性質上 AWS WAF、アプリケーションのカスタムルールを作成する必要があります。AMS はアプリケーションのコンテキストなしではアラームを定量化および作成できません。詳細については、「 AWS WAF - Web Application Firewall」を参照してください。

AWS WAF AWS Managed Servicesに関するよくある質問

よくある質問と回答：

Q: AMS アカウントでの設定 AWS WAF をリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 変更タイプを追加 (ct-1w8z66n899dct) で RFC を送信 AWS WAF して、 へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_waf_role`。アカウントに IAM AWS WAF ロールがプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: の使用にはどのような制限がありますか AWS WAF？

アクセス許可がプロビジョニングされたら、 のすべての機能を使用できます AWS WAF。

Q: を使用するための前提条件または依存関係は何ですか AWS WAF？

AMS アカウント AWS WAF で使用する前提条件や依存関係はありません。

AMS SSP を使用して AMS アカウント AWS Well-Architected Tool でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントの AWS Well-Architected Tool 機能に直接アクセスします。 AWS Well-Architected Tool は、ワークロードの状態を確認し、最新の AWS アーキテクチャのベストプラクティスと比較するのに役立ちます。このツールは、クラウドアーキテクトが安全で高性能、回復力があり、効率的なアプリケーションインフラストラクチャを構築できるように開発された AWS Well-Architected フレームワークに基づいています。このフレームワークは、アーキテクチャを評価するための一貫したアプローチを提供し、ソリューションアーキテクチャチームによって AWS 数万件のワークロードレビューに使用され、時間の経過とともにアプリケーションのニーズに合わせてスケールする設計を実装するためのガイダンスを提供します。詳細についてはAWS Well-Architected Toolを参照してください。

AWS WA Tool AWS Managed Servicesに関するよくある質問

一般的な質問と回答：

Q: AWS Well-Architected Tool AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか？

管理 | AWS サービス | セルフプロビジョニングサービス | 変更タイプを追加 (ct-1w8z66n899dct) で RFC を送信 AWS Well-Architected Tool して、 へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_well_architected_tool_console_admin_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

Q: AMS アカウント AWS Well-Architected Tool で を使用することにはどのような制限がありますか？

の完全な機能は AWS Well-Architected Tool 、AMS アカウントで使用できます。

Q: AMS アカウント AWS Well-Architected Tool で を使用するための前提条件または依存関係は何ですか？

AMS アカウント AWS Well-Architected Tool で使用する前提条件や依存関係はありません。

AMS SSP を使用して AMS アカウント AWS X-Ray でプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで AWS X-Ray (X-Ray) 機能に直接アクセスします。開発者 AWS X-Ray は、マイクロサービスアーキテクチャを使用して構築されたアプリケーションなど、本番稼働用の分散アプリケーションを分析およびデバッグできます。X-Ray を使用すると、アプリケーションとその基盤となるサービスのパフォーマンスを理解し、パフォーマンスの問題やエラーの根本原因を特定してトラブルシューティングできます。X-Ray は、アプリケーションを通過するリクエストのend-to-endビューを提供し、アプリケーションの基礎となるコンポーネントのマップを表示します。X-Ray を使用して、シンプルな 3 層アプリケーションから何千ものサービスで構成される複雑なマイクロサービスアプリケーションまで、開発中と本番環境の両方のアプリケーションを分析できます。詳細についてはAWS X-Rayを参照してください。

AWS Managed Servicesでの X-Ray に関するよくある質問

一般的な質問と回答：

Q: AWS X-Ray AMS アカウントの へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct) change type を送信してアクセスをリクエストします。この RFC は、アカウントに次の IAM ロールをプロビジョニングします: `customer_xray_console_role`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。さらに、Amazon EC2 インスタンスから X-Ray にデータをプッシュ`customer_xray_daemon_write_instance_profile`するには、 が必要です。このインスタンスプロファイルは、 を受け取ると作成されます`customer_xray_console_role`。

AMS Operations にサービスリクエストを送信して、 `customer_xray_daemon_write_policy`を既存のインスタンスプロファイルに割り当てることも、AMS Operations が X-Ray を有効にしたときに作成されるインスタンスプロファイルを使用することもできます。

Q: AMS アカウント AWS X-Ray で を使用することにはどのような制限がありますか？

のフル機能は、KMS キー (AWS KMS キー) による暗号化を除き、AMS アカウントで使用できます。 AWS X-Ray はデフォルトですべてのトレースデータを AWS X-Ray 暗号化します。デフォルトでは、X-Ray はトレースおよび保管中の関連データを暗号化します。保管中のデータをキーで暗号化する必要がある場合は、 AWSマネージド KMS キー (aws/xray) または KMS カスタマーマネージ

ドキーを選択できます。X-Ray 暗号化用の KMS カスタマーマネージドキーの場合は、管理 | その他 | その他 | 変更タイプの作成 (ct-1e1xtak34nx76) を送信します。

Q: AMS アカウント AWS X-Ray で を使用するための前提条件または依存関係は何ですか？

AWS X-Ray は、AMS アカウントに既に実装されている Amazon S3、CloudWatch、CloudWatch Logs に依存しています。推移的な依存関係は、 機能がやり取り AWS X-Ray しているデータソースやその他の AWS サービス (Amazon Redshift、Amazon RDS、Athena など) によって異なります。

AMS SSP を使用して AMS アカウントで VM Import/Export をプロビジョニングする

AMS セルフサービスプロビジョニング (SSP) モードを使用して、AMS マネージドアカウントで VM Import/Export 機能に直接アクセスします。VM Import/Export を使用すると、既存の環境から Amazon EC2 インスタンスに仮想マシンイメージを簡単にインポートし、オンプレミス環境にエクスポートし直すことができます。この機能により、IT セキュリティ、設定管理、コンプライアンス要件を満たすために構築した仮想マシンへの既存の投資を活用できます。これらの仮想マシンをready-to-useインスタンスとして Amazon EC2 に取り込むことができます。インポートしたインスタンスをオンプレミスの仮想化インフラストラクチャにエクスポートして、IT インフラストラクチャ全体にワークロードをデプロイすることもできます。詳細については、「VM Import/Export」を参照してください。

AWS Managed Services での VM Import/Export に関するよくある質問

一般的な質問と回答：

Q: AMS アカウントの VM Import/Export へのアクセスをリクエストするにはどうすればよいですか？

Management | AWS service | Self-provisioned service | Add change type (ct-1w8z66n899dct) で RFC を送信して VM Import/Export へのアクセスをリクエストします。この RFC は、アカウントに次の IAM ポリシーをプロビジョニングします: `customer_vmimport_policy`。アカウントにプロビジョニングされたら、フェデレーションソリューションでロールをオンボードする必要があります。

サービスがアカウントでアクションを実行するには、VM Import/Export サービスロールという追加のロールが必要です。

Q: AMS アカウントでの VM Import/Export の使用にはどのような制限がありますか？

- カスタムマシンイメージとデータボリュームをインポートする機能は、どちらも AMS VM Import/Export で使用できます。ただし、S3 へのアクセス許可は、アカウント内の情報へのアクセスを制

限customer-vmimport-*するために、名前に一致するバケットにアクションを制限するようにスコープダウンされています。

- イメージとスナップショットのインポートは、AMS VM Import/Export でサポートされています。ただし、セキュリティ対策のため、インスタンスのインポートおよびインスタンスのエクスポート機能は利用できません。
- さらに、制限されたデータや機密データをエクスポートするリスクを軽減するために、エクスポート機能が無効になっています。

Q: AMS アカウントで VM Import/Export を使用するための前提条件または依存関係は何ですか？

- AWS 環境にインポートするには、サポートされているディスクイメージを指定する必要があります。詳細については、「VM Import/Export Requirements」を参照してください。
- VM Import/Export には AWS コンソールからアクセスできません。このサービスには AWS CLI、AWS Tools for PowerShell、、または AWS SDKs からアクセスする必要があります。または、変更タイプ ct-117rmp64d5mvb: Deployment | Advanced stack components | Identity and Access Management (IAM) | Create EC2 instance profile を送信して、インスタンスプロファイルをリクエストすることもできます。このインスタンスプロファイルにより、ツールはインスタンスからコマンドを実行できます。

カスタマーマネージドモード

AWS Managed Services (AMS) カスタマーマネージドモードは、柔軟で要件に適応できるガバナンスモデルを提供します。これは、AMS が動作できないサービスやアプリケーションのフォールバックオプションと考えることができます。AMS は、このモードで作成されたアカウントでホストされるインフラストラクチャを運用しません。ただし、このモードでは、一元化されたマルチアカウント管理を活用できます。このモードでは、次のマルチアカウントランディングゾーン機能を活用できます。

- 自動アカウントデプロイ
- ネットワークアカウントの Transit Gateway を介した接続
- AMS Config ルールライブラリ
- ログ記録アカウントにログのコピーを保存する
- セキュリティアカウントへのカスタマーマネージド Guard Duty アラートの集約
- 一括請求
- カスタムサービスコントロールポリシーの有効化。

例: AMS によって管理されるオペレーティングシステムではない Ubuntu Pro でワークロードを実行する場合は、カスタマーマネージドアカウントを使用してワークロードをホストできます。また、カスタマーマネージドアカウントを通じてワークロードを統合し、AWS 組織全体での共有を通じて利用可能なリザーブドインスタンス/共有プランの一括割引を利用することもできます。

カスタマーマネージドモードの開始方法

AMS カスタマーマネージドモードは、特別なマルチアカウントランディングゾーンアプリケーションアカウントを通じて使用できます。

カスタマーマネージドアプリケーションアカウントの作成方法などの詳細については、「カスタマーマネージドアプリケーションアカウント」を参照してください。

AMS と AWS Service Catalog

AWS Managed Services (AMS) のサービスカタログを使用すると、組織は AWS 情報テクノロジー (IT) サービスのカタログを作成および管理でき、IT 管理者は承認された製品のカタログを作成、管理、およびアカウントのエンドユーザーに配布できます。エンドユーザーは、パーソナライズされたサービスポータルで必要な製品にアクセスできます。管理者は、どのユーザーが各製品にアクセスできるかを制御して、組織のビジネスポリシーへの準拠を強制できます。管理者は、承認されたリソースをデプロイするためにエンドユーザーが Service Catalog への IAM アクセスのみを必要とするようにロールを設定することもできます。Service Catalog を使用すると、エンドユーザーは管理するカタログから必要な製品のみを見つけて起動できるため、組織は俊敏性とコスト削減の恩恵を受けることができます。

Service Catalog では、AMS マネージドアカウント (複数可) でリソースをプロビジョニングおよび更新するための AMS 変更リクエスト (RFC) プロセスの代わりに使用できます。AMS は、セキュリティ、コンプライアンス、プロビジョニング、可用性、パッチ、モニタリング、アラート、レポート、インシデント対応、コスト最適化など、Service Catalog を通じてプロビジョニングされたすべてのインフラストラクチャリソースに対して AWS を大規模に実行するために必要なすべてのインフラストラクチャオペレーションタスクを管理します。AMS マネージドアカウントで Service Catalog を使用すると、一般的にデプロイされる IT サービスを一元管理するためのメカニズムが提供され、ユーザーが必要とする承認済みの IT サービスのみをマネージド環境にすばやくデプロイしながら、一貫したガバナンスを実現できます。

Service Catalog の開始方法

AMS で Service Catalog の使用を開始するには、AMS コンソールからサービスリクエストを送信して、Service Catalog へのアクセスをリクエストします。リクエストを送信すると、3 つの IAM ロー

ルがアカウント (複数可) にデプロイされ、AMS (前Transform述) を呼び出す CloudFormation マクロを含む AMS マネージドスタックとともにデプロイされます。これにより、システムに製品を登録し、Service Catalog を介してプロビジョニングされたインフラストラクチャに対してオペレーションを実行できます。デプロイされた 3 つの IAM ロールには、IT 管理者が Service Catalog 管理者として製品を管理するためのロール、アプリケーション所有者とエンドユーザーが製品を設定、起動、管理するためのロール、および製品の起動または更新時に Service Catalog が使用するアクセス許可を定義する起動制約として使用されるロールが含まれます。

開始する前に AMS の Service Catalog

Service Catalog は、既存の AMS 変更リクエスト (RFC) プロセスを置き換えますか？

Service Catalog が有効になっているアカウントでは、事前定義された製品カタログを使用して AMS アカウントで IT サービスをプロビジョニングおよび更新する変更管理システムとして機能します。AMS はデフォルトのポートフォリオ/製品カタログを提供し、IT 管理者は独自の を作成および設定できます。Service Catalog は、Service Catalog を介してプロビジョニングされたスタックのみを承認します。同様に、Service Catalog を介してプロビジョニングされたサービスは AMS RFC プロセスを通じて変更できません。Service Catalog の外部で変更すると、承認された製品設定からスタックがドリフトするためです。

AMS コンソールでサービスカタログを通じてプロビジョニングされたスタックを確認できますか？

はい。AMS コンソールで、サービスカタログを通じてプロビジョニングされたすべてのスタックを表示できます。サービスカタログを介してプロビジョニングされたスタックは、スタック ID 「SC-」によって簡単に識別できます。スタックは AMS コンソールで表示できますが、AMS RFC プロセスを通じて更新することはできません。AMS 変更管理システム (RFCs) へのアクセスは、アクセスリクエスト、パッチオーケストレーション、バックアップ RFCs。

Service Catalog を使用してスタックをプロビジョニングまたは更新する場合、対応する RFC が AMS コンソールにありますか？

AMS コンソールに表示される唯一の RFC は、スタックが最初にプロビジョニングされたときにスタックを AMS に登録する RFC です。この RFC は、Service Catalog を介してスタックが起動されたときにトリガーされる AMS 検証プロセスによって自動的にファイルされます。その他のプロビジョニングと変更は Service Catalog で直接追跡され、Service Catalog コンソールで表示できます。さらに、Service Catalog のプロビジョニング済み製品プラン機能を使用して、製品のプロビジョニングまたは更新の前にリソースに加えられる変更のリストを表示できます。

AMS マネージドアカウントで製品をプロビジョニングするために、特定の操作を行う必要がありますか？

はい。AMS アカウントでプロビジョニングされるすべての Service Catalog 製品には、その製品を定義する CFN テンプレートにこの JSON 行が含まれている必要があります。

```
"Transform":{"Name":"AmsStackTransform","Parameters":{"StackId":
{"Ref":"AWS::StackId"}}}
```

この CloudFormation コードスニペットは、リソースを AMS マネージドアカウントでプロビジョニングするために必要な AMS 検証をトリガーします。このコード行を製品定義の一部として含めるのはお客様の責任です。含まれていない場合、プロビジョニングは失敗し、「製品の作成に失敗しました」というエラーメッセージが表示されます。このアカウントは AMS によって管理されます。AMS アカウントのすべての製品には、テンプレートに AMS `Transform`コードが必要です。」

起動時に AMS のお客様に利用できない、または制限されている Service Catalog 機能はありますか？

はい。AMS のお客様は、初回起動時に以下の SC 機能を使用できません。

- Service Catalog によるアカウントの作成
- Service Catalog を介してすべての AWS サービスを AMS マネージドアカウントで起動する機能。AWS サービスの可用性は、AMS がサポートするサービス (マネージド型およびセルフプロビジョニング型) に限定されます。AMS がサポートするサービスの詳細については、AMS サービスの説明を参照してください。
- Service Catalog IT サービスマネージャー (ITSM) コネクタは、AMS インシデントレポートやサービスリクエストと通信しません。
- Service Catalog のクイックスタートとリファレンスアーキテクチャを、変更なしで活用する機能。AMS アカウントの Service Catalog 製品には、次の JSON コード行が含まれている必要があることに注意してください。

  ```
  "Transform":{"Name":"AmsStackTransform","Parameters":{"StackId":
  {"Ref":"AWS::StackId"}}}
  ```

  CNF テンプレートの 。この行は一般的な AWS CloudFormation テンプレートの一部ではなく、明示的に追加する必要があることに注意してください。
- Terraform は現在、Service Catalog 製品のプロビジョニングのために AMS でサポートされていません。

- AWS CFN スタックセットは AMS ではサポートされていません。
- カスタム IAM ロールを作成することはできません。
- サービスアクションは以下に限定されます。
  - AWS-RebootRdsInstance
  - AWS-RestartEC2Instance
  - AWS-StartEC2Instance
  - AWS-StartRdsInstance
  - AWS-StopEC2Instance
  - AWS-StopRdsInstance
  - AWS-CreateImage
  - AWS-CreateRdsSnapshot
  - AWS-CreateSnapshot

> **Note**
>
> サービスアクションを作成するときは、実行ロールをエンドユーザーのアクセス許可、起動ロール、または選択したカスタム IAM ロールに設定できます。選択した実行ロールには、サービスアクションを実行するための十分なアクセス許可が必要であり、Service Catalog による引き受けを許可する TrustPolicy が必要です。そうしないと、サービスアクションは実行時に失敗します。サービスアクションとして使用する正しいアクセス許可と信頼ポリシーを持つ AWSManagedServicesServiceCatalogLaunchRole を使用することをお勧めします。

AMS RFC システムの使用にはまだ何が必要ですか？

一般提供 (GA) では、RFCS を使用して以下のアクションを実行する必要があります。

- パッチオーケストレーターの設定
- バックアップポリシーの設定
- インスタンスアクセスのリクエスト
- AMS ガイドラインの範囲外のセキュリティグループを作成して割り当てる。
- ワークロード取り込みの実行 (WIGS)
- 「IAM ロールの作成」

Service Catalog CLI を使用して AMS マネージドアカウントの Service Catalog にアクセスすることはできますか？

はい。Service Catalog APIsは CLI で使用および有効化できます。Service Catalog アーティファクトの管理から、それらのアーティファクトのプロビジョニングと終了までのアクションを使用できます。詳細については、AWS Service Catalog リソース」を参照するか、最新の AWS SDK または CLI をダウンロードしてください。

顧客の承認済み製品のカタログを作成、管理、配布するのは誰ですか？

お客様のカタログ管理者および/または IT 管理者、または割り当てられたリソースは、Service Catalog カタログおよび承認済み製品の管理を担当します。

AMS AMIs?

2020 年 3 月以降に販売された AMS AMIs は、AWS Service Catalog を通じてデプロイできます。

Service Catalog を使用して AMS に移行するにはどうすればよいですか？

Service Catalog を使用してワークロードを AMS に移行するには、まずワークロード取り込み (WIGs) プロセスに従って AMS に AMI を作成します。WIGS によって生成された AMI を使用して、Service Catalog で製品を作成します。これを行う方法については、AWS Service Catalog - 開始方法を参照してください。

AMS マルチアカウントランディングゾーン (MALZ) オンボーディング

MALZ ネットワークアーキテクチャ

マルチアカウントランディングゾーンのネットワークアーキテクチャについて

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

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

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

トピック

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

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

サービスリージョン

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

組織単位

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

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

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

- OU の高速化：

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

- アプリケーション > マネージド OU:

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

- アプリケーション > 開発 OU:

  AMS マネージドランディングゾーンのアプリケーション OU のこのサブ OU では、アカウントは、AMS 変更管理プロセス外で AWS リソースをプロビジョニングおよび更新するための昇格さ

れたアクセス許可を提供するデベロッパーモードアカウントです。この OU は、必要に応じて新しい子 OU の作成もサポートしています。

- カスタマーマネージド OU:

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

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

サービスコントロールポリシーと AWS Organization

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

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

単一の MALZ または複数の MALZsの選択

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

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

エンティティ	単一の AMS ランディングゾーン	複数の (2 つ以上の) ランディングゾーン
基本費用	低く、1 か月あたり約 3,000 USD で最適化されています。	より高い場合は、環境ごとに約 3,000 USD の追加コストが発生します。
請求	単一の請求/管理アカウントによる単一の請求。	マルチアカウントランディングゾーンごとに個別の請求書。現在、AWS Org は 1 回の請求でマルチ管理アカウントをサポートしていません。
既存のリザーブドインスタンス (RIsの移植性	低。AWS RIsは現在、複数の請求アカウント間で変換できません。マルチアカウントランディングゾーンの既存の RIs を再利用します。	下。RIs再利用し、すべてのマルチアカウントランディングゾーンに分散します。
製品階層化の割引	高 「ボリューム割引」を参照してください。	低。「ボリューム割引」を参照してください。
初期セットアップのオーバーヘッド (プロジェクト/移行タイムライン上)	低。Active Directory、ネットワーキング、およびシングルサインオン (SSO) 統合は 1 回のみです。	高 ランディングゾーンごとに Active Directory、ネットワーク統合、および SSO 統合を実行します。これにより、移行プロジェクトに遅延が発生する可能性があります。
一般的なサービスの設定可能性	労力が少ない。DNS、バックアップ、モニタリング、ログ記録などの共通/共有サービスを設定します。	高い労力。一般的なインフラストラクチャやサービスが置かれている場所に対処するには、追加の計画が必要です。各ランディングゾーンの複数のトランジットゲートウェイ (TGWs) を横断するトラフィックは、追加料金が発生する可能性があります。
スケーラビリティ	Medium。AMS には、マルチアカウントランディングゾーンあたり 150 個のアカウントという現在の実用的な制限	高 アカウントまたはアプリケーションの分離レベルを達成しながら、複数のマルチアカウントランディングゾー

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

エンティティ	単一の AMS ランディングゾーン	複数の (2 つ以上の) ランディングゾーン
アカウントの移行または移植性	はい。同じ AWS Organization 内で、ある OU から別の OU にアカウントを移動できます。	いいえ。AMS はランディングゾーン間、つまり AWS Organizations 間でのアカウントの移行をサポートしていません。ワークロードは、トランジットゲートウェイ (TGW) または VPC ピアリングを使用してランディングゾーン間で到達できます。
変更管理	Medium。TGW、Active Directory (AD)、アウトバウンド (Egress) などの一般的なコンポーネントに破壊的な変更を加えると、マルチアカウントランディングゾーン内のすべてのワークロードに影響を与える可能性があります。ただし、AMS が管理するコンポーネントへの変更は内部的にテストされ、ローリング更新でプッシュされます。	低。TGW、AD、アウトバウンド (エグレス) などの一般的なコンポーネントに破壊的な変更を加えると、その特定のマルチアカウントランディングゾーンのワークロードにのみ影響する可能性があります。
データおよびアクセスコントロール	(依存) Prod ワークロードと Non-Prod ワークロードの異なるオンプレミス ADs とネットワークに接続する場合は、コントロールが低くなります。SAML フェデレーション、TGW ドメイン、セキュリティグループ (SGsも、必要なコントロールを実装するのに役立ちます。	(依存) Prod ワークロードと Non-Prod ワークロードの異なるオンプレミス ADs とネットワークに接続する場合は、高い制御が可能です。厳格なコンプライアンス要件には、個別のランディングゾーンを使用します。

エンティティ	単一の AMS ランディングゾーン	複数の (2 つ以上の) ランディングゾーン
コンプライアンスとセキュリティ	(依存) マテリアルワークロードと非マテリアルワークロードを完全に分離するために厳格なコンプライアンスが必要な場合は、低。AMS 標準の予防的コントロールと検出的コントロールが導入されています。	(依存) 複数のマルチアカウントランディングゾーンが高いと、マテリアルワークロードと非マテリアルワークロードを完全に分離することで、厳格なコンプライアンス要件を満たすことができます。AMS 標準の予防的コントロールと検出的コントロールが導入されています。

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

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

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

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

A: はい。いつでも別のマルチアカウントランディングゾーンを設定できます。

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

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

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

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

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

さらに:

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

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

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

マルチアカウントランディングゾーンアカウント

トピック

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

管理アカウント

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

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

次の図は、管理アカウントに含まれるリソースの概要を示しています。

管理アカウントのリソース

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

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

ネットワークアカウント

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

ネットワークアカウントアーキテクチャ

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

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

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

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

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

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

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

Transit Gateway を使用した一元化されたエッジ接続

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

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

この設定には次のような利点があります。以下を実行できます。

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

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

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

DX または VPN をアカウント VPCsに接続する

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

ネットワークアカウントのリソース

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

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

AWS Network Manager

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

このリソースにアクセスするには、次のいずれかのロールを使用します。

- AWSManagedServicesCaseRole
- AWSManagedServicesReadOnlyRole
- AWSManagedServicesChangeManagementRole

エグレス VPC

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

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

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

マネージド型 Palo Alto Egress ファイアウォール

AMS は、マルチアカウントランディングゾーン環境内のすべてのネットワーク (パブリック向けサービスを除く) でインターネットバウンドアウトバウンドトラフィックフィルタリングを可能にする Managed Palo Alto Egress ファイアウォールソリューションを提供します。このソリューションは、業界をリードするファイアウォールテクノロジー (Palo Alto VM-300) と AMS のインフラストラクチャ管理機能を組み合わせて、準拠した運用環境内でインフラストラクチャをデプロイ、モニタリング、管理、スケーリング、復元します。Palo Alto Networks を含むサードパーティーは、ファイアウォールにアクセスできず、AMS エンジニアによってのみ管理されます。

トラフィックコントロール

マネージドアウトバウンドファイアウォールソリューションは、バックアップやパッチなどのサービスの AMS 必須ドメインと、定義されたドメインで構成されるドメイン許可リストを管理します。アウトバウンドインターネットトラフィックがファイアウォールにルーティングされると、セッション

が開かれ、トラフィックが評価され、許可されたドメインと一致する場合、トラフィックは送信先に転送されます。

アーキテクチャ

マネージドエグレスファイアウォールソリューションは、高可用性モデルに従います。このモデルでは、アベイラビリティーゾーン (AZs。このソリューションは、デフォルトの Egress VPC の IP スペースの一部を使用しますが、ファイアウォールの管理に必要な追加のリソース用に VPC 拡張機能 (/24) もプロビジョニングします。

ネットワークフロー

大まかに言うと、パブリックエグレストラフィックルーティングは、エグレス VPC からインターネットにトラフィックをルーティングする方法を除いて変わりません。

1. インターネット宛ての Egress トラフィックは、VPC ルートテーブルを介して Transit Gateway (TGW) に送信されます。
2. TGW は TGW ルートテーブルを介して送信 VPC にトラフィックをルーティングします
3. VPC は、プライベートサブネットルートテーブルを介してトラフィックをインターネットにルーティングします。
   a. デフォルトのマルチアカウントランディングゾーン環境では、インターネットトラフィックはネットワークアドレス変換 (NAT) ゲートウェイに直接送信されます。マネージドファイアウォールソリューションは、代わりにファイアウォールインターフェイスへのデフォルトルート (0.0.0.0/0) を指すようにプライベートサブネットルートテーブルを再設定します。

ファイアウォール自体には 3 つのインターフェイスが含まれています。

1. 信頼できるインターフェイス: 処理するトラフィックを受信するためのプライベートインターフェイス。
2. 信頼できないインターフェイス: インターネットにトラフィックを送信するパブリックインターフェイス。ファイアウォールは NAT を実行するため、外部サーバーはこれらのパブリック IP アドレスからのリクエストを受け入れます。
3. 管理インターフェイス: ファイアウォール API、更新、コンソールなどのプライベートインターフェイス。

すべてのルーティングを通じて、トラフィックは同じアベイラビリティーゾーン (AZ) 内に維持され、AZ 間のトラフィックが減少します。トラフィックは、フェイルオーバーが発生した場合にのみ AZs を通過します。

許可リストの変更

オンボーディング後、 という名前のデフォルトの許可リストams-allowlistが作成され、AMS が必要とするパブリックエンドポイントと、Windows および Linux ホストにパッチを適用するためのパブリックエンドポイントが含まれます。運用後、AMS コンソールの Management | Managed Firewall | Outbound (Palo Alto) カテゴリで RFC を作成して、許可リストを作成または削除したり、ドメインを変更したりできます。は変更ams-allowlistできないことに注意してください。RFC は完全な自動化で処理されます (手動ではありません) 。

カスタムセキュリティポリシー

セキュリティポリシーは、送信元と送信先のセキュリティゾーン、送信元と送信先の IP アドレス、サービスなどのトラフィック属性に基づいて、セッションをブロックするか許可するかを決定します。カスタムセキュリティポリシーは、完全に自動化された RFCs。セキュリティポリシーを作成または削除する CTsは、管理 | マネージドファイアウォール | アウトバウンド (Palo Alto) カテゴリにあり、既存のセキュリティポリシーを編集する CT は、デプロイ | マネージドファイアウォール | アウトバウンド (Palo Alto) カテゴリにあります。新しいセキュリティポリシーの作成、セキュリティポリシーの変更、またはセキュリティポリシーの削除を行うことができます。

> **Note**
>
> デフォルトのセキュリティポリシーは変更ams-allowlistできません

CloudWatch PA 出力ダッシュボード

CloudWatch には、パロアルト (PA) の集約ビューを提供する 2 つのダッシュボードがあります。AMS-MF-PA-Egress-Config-Dashboard には、PA 設定の概要、許可リストへのリンク、属性を含むすべてのセキュリティポリシーのリストが用意されています。AMS-MF-PA-Egress-Dashboard は、トラフィックログをフィルタリングするようにカスタマイズできます。たとえば、セキュリティポリシーのダッシュボードを作成するには、次のようなフィルターを使用して RFC を作成できます。

```
fields @timestamp, @message
| filter @logStream like /pa-traffic-logs/
| filter @message like /<Security Policy Name>/
```

```
| parse @message
 "*,*,*,
```

復元は、ホストがインスタンスを完全にリサイクルする必要がある場合にも発生する可能性があります。最新のバックアップの自動復元は、新しい EC2 インスタンスがプロビジョニングされたときに発生します。一般的に、ホストは定期的にリサイクルされず、重大な障害や必要な AMI スワップ用に予約されています。ホストのリサイクルは手動で開始され、リサイクルが発生する前に通知されます。

ファイアウォール設定バックアップを除き、特定の許可リストルールは個別にバックアップされます。バックアップは、定義された許可リストルールが変更されると自動的に作成されます。許可リストバックアップの復元は、必要に応じて AMS エンジニアが実行できます。

更新

AMS Managed Firewall Solution では、システムの改善、機能の追加、ファイアウォールオペレーティングシステム (OS) またはソフトウェアの更新を追加するために、時間の経過とともにさまざまな更新が必要です。

ほとんどの変更は、自動化インフラストラクチャの更新など、実行中の環境には影響しませんが、ファイアウォールインスタンスのローテーションや OS の更新など、その他の変更は中断を引き起こす可能性があります。更新によるサービス中断の可能性が評価されると、AMS はメンテナンスウィンドウに対応するためにお客様と調整します。

オペレーターアクセス

AMS オペレーターは ActiveDirectory 認証情報を使用して Palo Alto デバイスにログインし、オペレーション (パッチ適用、イベントへの応答など) を実行します。このソリューションは、標準の AMS Operator 認証ログと設定変更ログを保持して、Palo Alto ホストで実行されたアクションを追跡します。

デフォルトログ

デフォルトでは、ファイアウォールによって生成されたログは、各ファイアウォールのローカルストレージにあります。時間が経過すると、ローカルログはストレージ使用率に基づいて削除されます。AMS ソリューションは、マシンから CloudWatch Logs にログをリアルタイムで送信します。詳細については、「」を参照してくださいCloudWatch Logs の統合。

AMS エンジニアは、必要に応じてマシンから直接ログをクエリおよびエクスポートできます。さらに、ログは顧客所有の Panorama に配送できます。詳細については、「」を参照してくださいPanorama 統合。

ソリューションによって収集されたログは次のとおりです。

RFC ステータスコード

ログのタイプ	説明
トラフィック	各セッションの開始と終了のエントリを表示します。各エントリには、日付と時刻、送信元ゾーンと送信先ゾーン、アドレスとポート、アプリケーション名、フローに適用されるセキュリティルール名、ルールアクション (許可、拒否、またはドロップ) 、イングレスインターフェイスとエグレスインターフェイス、バイト数、セッション終了理由が含まれます。 Type 列は、エントリがセッションの開始または終了用か、セッションが拒否またはドロップされたかを示します。「drop」は、「any」アプリケーションをブロックしたセキュリティルールを示し、「deny」は、ルールが特定のアプリケーションを識別したことを示します。 ルールが特定のサービスのすべてのトラフィックを削除するなど、アプリケーションが特定される前にトラフィックがドロップされた場合、アプリケーションは「該当なし」として表示されます。
脅威	ファイアウォールによって生成された各セキュリティアラームのエントリを表示します。各エントリには、日付と時刻、脅威名または URL、送信元ゾーンと送信先ゾーン、アドレス、ポート、アプリケーション名、アラームアクション (許可またはブロック) と重要度が含まれます。 Type 列は、「ウイルス」や「スパイウェア」などの脅威のタイプを示します。Name 列は脅威の説明または URL、Category 列は脅威カテゴリ (「キーロガー」など) または URL カテゴリです。
URL フィルタリング	ウェブサイトへのアクセスと、ユーザーがウェブサイトに認証情報を送信できるかどうかを制御する URL フィルターのログを表示します。
設定	各設定変更のエントリを表示します。各エントリには、日付と時刻、管理者ユーザー名、変更元の IP アドレス、クライアントのタイプ (ウェブインターフェイスまたは CLI)、コマンド実行のタイプ、コマンドが成功したか失敗したか、設定パス、変更前後の値が含まれます。
システム	各システムイベントのエントリを表示します。各エントリには、日付と時刻、イベントの重要度、およびイベントの説明が含まれます。

ログのタイプ	説明
Alarms	アラームログには、システムによって生成されたアラームに関する詳細情報が記録されます。このログの情報は、アラームでも報告されます。「アラーム設定の定義」を参照してください。
認証	エンドユーザーが、認証ポリシールールによってアクセスが制御されるネットワークリソースにアクセスしようとしたときに発生する認証イベントに関する情報を表示します。ユーザーはこの情報を使用して、アクセスの問題をトラブルシューティングし、必要に応じてユーザー認証ポリシーを調整できます。相関オブジェクトと組み合わせて、ユーザーは認証ログを使用して、ブルートフォース攻撃などのユーザーネットワーク上の疑わしいアクティビティを特定することもできます。 オプションで、ユーザーは認証タイムアウトをログに記録するように認証ルールを設定できます。これらのタイムアウトは、ユーザーがリソースに対して一度だけ認証する必要があるが、繰り返しアクセスできる期間に関連しています。タイムアウトに関する情報を確認することで、ユーザーはタイムアウトを調整するかどうか、および調整方法を決定できます。
統合	最新のトラフィック、脅威、URL フィルタリング、WildFire 送信、データフィルタリングのログエントリを 1 つのビューに表示します。集合ログビューを使用すると、ユーザーはこれらのさまざまなタイプのログを一緒に調査およびフィルタリングできます (各ログセットを個別に検索するのではなく) 。または、ユーザーは表示するログタイプを選択できます。フィルターフィールドの左側にある矢印をクリックし、トラフィック、脅威、URL、データ、および/または山火事を選択して、選択したログタイプのみを表示できます。

イベント管理

AMS は、ファイアウォールの容量、ヘルスステータス、可用性を継続的にモニタリングします。ファイアウォールから生成されたメトリクスと AWS/AMS で生成されたメトリクスは、AMS オペレーションエンジニアが受信したアラームを作成するために使用されます。アラームは、問題を調査して解決します。現在のアラームは、次のケースを対象としています。

イベントアラーム：

- Firewall Dataplane CPU 使用率
  - CPU 使用率 - Dataplane CPU (トラフィックの処理)
- Firewall Dataplane パケット使用率が 80% を超えている
  - パケット使用率 - Dataplane (トラフィックの処理)
- Firewall Dataplane セッション使用率
- Firewall Dataplane セッションがアクティブ
- ファイアウォール CPU 使用率の集計
  - すべての CPU CPUs 使用率
- AZ によるフェイルオーバー
  - AZ でフェイルオーバーが発生した場合のアラーム
- 異常な Syslog ホスト
  - Syslog ホストがヘルスチェックに失敗する

管理アラーム :

- Health Check Monitor の失敗アラーム
  - ヘルスチェックワークフローが予期せず失敗した場合
  - これは、ファイアウォールのヘルスチェックが失敗した場合ではなく、ワークフロー自体用です。
- パスワードローテーション失敗アラーム
  - パスワードのローテーションが失敗した場合
  - API/サービスユーザーのパスワードは 90 日ごとにローテーションされます

メトリクス

すべてのメトリクスがキャプチャされ、ネットワークアカウントの CloudWatch に保存されます。これらは、ネットワークアカウントへのコンソールアクセスを取得し、CloudWatch コンソールに移動することで表示できます。個々のメトリクスは、メトリクスタブまたは選択したメトリクスの単一ペインダッシュボードビューで表示でき、集計されたメトリクスは、ダッシュボードタブに移動して AMS-MF-PA-Egress-Dashboard を選択することで表示できます。

カスタムメトリクス :

- ヘルスチェック

  - 名前空間: AMS/MF/PA/Egress
    - PARouteTableConnectionsByAZ
    - PAUnhealthyByInstance
    - PAUnhealthyAggregatedByAZ
    - PAHealthCheckLockState
- 生成されたファイアウォール
  - 名前空間: AMS/MF/PA/Egress/<instance-id>
    - DataPlaneCPUUtilizationPct
    - DataPlanePacketBuffferUtilization
    - panGPGatewayUtilizationPct
    - panSessionActive
    - panSessionUtilization

CloudWatch Logs の統合

CloudWatch Logs 統合は、ファイアウォールから CloudWatch Logs にログを転送します。これにより、ローカルストレージの使用率が原因でログが失われるリスクを軽減できます。ログは、ファイアウォールがログを生成するとリアルタイムで入力され、コンソールまたは API を介してオンデマンドで表示できます。

複雑なクエリは、ログ分析用に構築することも、CloudWatch Insights を使用して CSV にエクスポートすることもできます。さらに、カスタム AMS Managed Firewall CloudWatch ダッシュボードには、特定のトラフィックログクエリのクイックビューと、時間の経過に伴うトラフィックとポリシーヒットのグラフ視覚化も表示されます。CloudWatch ログを使用すると、AWS Kinesis などの他の AWS サービスとのネイティブ統合も可能になります。

> **Note**
>
> PA ログを既存のオンプレミスまたはサードパーティーの Syslog コレクターに直接転送することはできません。AMS Managed Firewall ソリューションは、PA マシンから AWS CloudWatch Logs にログをリアルタイムで送信します。CloudWatch Logs Insight 機能を使用して、アドホッククエリを実行できます。さらに、Palo Alto の Panorama 管理ソリューションにログを出荷できます。CloudWatch サブスクリプションフィルターを使用して、CloudWatch ログを他の送信先に転送することもできます。Panorama の詳細について

は、次のセクションを参照してください。Splunk の詳細については、「Splunk との統合」を参照してください。

Panorama 統合

AMS Managed Firewall は、オプションで既存の Panorama と統合できます。これにより、Panorama からファイアウォール設定を表示したり、ファイアウォールから Panorama にログを転送したりできます。Panorama と AMS Managed Firewall の統合は読み取り専用であり、Panorama からのファイアウォールの設定変更は許可されません。Panorama は完全に管理され、ユーザーによって設定されます。AMS は、それと通信するようにファイアウォールを設定する責任のみを担います。

ライセンス

AMS Managed Firewall の料金は、使用されるライセンスのタイプ、時間単位または持ち込みライセンス (BYOL)、アプライアンスが実行されるインスタンスサイズによって異なります。AWS Marketplace を通じて希望する Palo Alto ファイアウォールのインスタンスサイズとライセンスを注文する必要があります。

- Marketplace ライセンス: MALZ のネットワークアカウントから VM シリーズ次世代ファイアウォールバンドル 1 の利用規約を承諾します。
- BYOL ライセンス: MALZ のネットワークアカウントから VM-Series Next-Generation Firewall (BYOL) の利用規約に同意し、AMS にライセンスを購入した後に取得した「BYOL 認証コード」を共有します。

制限

現時点では、AMS は VM-300 シリーズまたは VM-500 シリーズファイアウォールをサポートしています。設定は、AWS EC2 インスタンスの VM シリーズモデル、

> **Note**
>
> AMS ソリューションは、AZ 内の各 PA インスタンスが尊重される AZ の出力トラフィックを処理するため、アクティブ/アクティブモードで実行されます。したがって、2 つの AZs では、各 PA インスタンスは最大 5 Gbps の出力トラフィックを処理し、2 つの AZs 全体で 10 Gbps のスループットを効果的に提供します。各 AZ のすべての制限に同じことが当てはまります。AMS ヘルスチェックが失敗した場合、不正な PA を持つ AZ から別の AZ にトラ

フィックを移行します。インスタンスの置き換え中、容量は残りの AZs制限に削減されます。
AMS は現在、AWS Marketplace で利用可能な他の Palo Alto バンドルをサポートしていません。たとえば、「VM シリーズ次世代ファイアウォールバンドル 2」をリクエストすることはできません。Palo Alto を使用する AMS Managed Firewall ソリューションは現在、Egress トラフィックフィルタリングサービスのみを提供しているため、高度な VM シリーズバンドルを使用しても、追加の機能や利点は提供されないことに注意してください。

オンボーディング要件

- AWS Marketplace の Palo Alto の VM シリーズ次世代ファイアウォールの利用規約を確認し、同意する必要があります。
- 使用するインスタンスサイズは、予想されるワークロードに基づいて確認する必要があります。
- マルチアカウントランディングゾーン環境またはオンプレミスのネットワークと競合しない /24 CIDR ブロックを指定する必要があります。Egress VPC と同じクラスである必要があります (ソリューションは /24 VPC 拡張を Egress VPC にプロビジョニングします) 。

料金

AMS Managed Firewall の基本インフラストラクチャのコストは、Palo Alto ファイアウォールをホストする EC2 インスタンス、ソフトウェアライセンス Palo Alto VM シリーズライセンス、CloudWatch Integrations の 3 つの主なドライバーに分かれています。

次の料金は、VM-300 シリーズファイアウォールに基づいています。

- EC2 インスタンス: Palo Alto ファイアウォールは、2～3 個の EC2 インスタンスの高可用性モデルで実行され、インスタンスは予想されるワークロードに基づいています。インスタンスのコストは、リージョンと AZs
  - 例: us-east-1、m5.xlarge、3AZs
    - 0.192 USD * 24 * 30 * 3 = 414.72 USD
  - https://aws.amazon.com/ec2/pricing/on-demand/
- Palo Alto ライセンス: Palo Alto VM-300 次世代ファイアウォールのソフトウェアライセンスコストは、AZ の数とインスタンスタイプによって異なります。
  - 例: us-east-1、m5.xlarge、3AZs
    - 0.87 USD * 24 * 30 * 3 = 1879.20 USD

    - https://aws.amazon.com/marketplace/pp/B083M7JPKB?ref_=srh_res_product_title#pdp-pricing
- CloudWatch Logs 統合: CloudWatch Logs 統合は、SysLog サーバー (EC2 - t3.medium)、NLB、CloudWatch Logs を使用します。サーバーのコストはリージョンと AZs の数に基づいており、NLB/CloudWatch ログのコストはトラフィック使用率によって異なります。
    - 例: us-east-1、t3.medium、3AZ
        - 0.0416 USD * 24 * 30 * 3 = 89.86 USD
    - https://aws.amazon.com/ec2/pricing/on-demand/
    - https://aws.amazon.com/cloudwatch/pricing/

境界 (DMZ) VPC

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

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

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

AWS Transit Gateway

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

このリソースを作成するには、次の入力を指定します。

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

共有サービスアカウント

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

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

- 共有サービス VPC CIDR 範囲： VPC を作成するときは、10.0.1.0/24 など、Classless Inter-Domain Routing (CIDR) ブロックの形式で VPC の IPv4 アドレスの範囲を指定する必要があります。これは VPC のプライマリ CIDR ブロックです。

  > **Note**
  >
  > AMS チームは /23 の範囲を推奨します。

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

- Trend Micro – エンドポイント保護セキュリティ (EPS): Trend Micro エンドポイント保護 (EPS) は、オペレーティングシステムのセキュリティのための AMS 内の主要なコンポーネントです。シ

ステムは、Deep Security Manager (DSM)、EC2 インスタンス、リレー EC2 インスタンス、およびすべてのデータプレーンとカスタマー EC2 インスタンス内に存在するエージェントで構成されます。

共有サービスアカウントEPSMarketplaceSubscriptionRoleで を引き受け、Trend Micro Deep Security (BYOL) AMI または Trend Micro Deep Security (Marketplace) のいずれかにサブスクライブする必要があります。

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

- リレーインスタンスタイプ: デフォルト値 - m5.large
- DSM インスタンスタイプ: デフォルト値 - m5.xlarge
- DB インスタンスサイズ: デフォルト値 - 200 GB
- RDS インスタンスタイプ: デフォルト値 - db.m5.large

- カスタマー踏み台: AMS 環境内の他のホストにアクセスするために、共有サービスアカウントで SSH または RDP 踏み台 (またはその両方) が提供されます。ユーザー (SSH/RDP) として AMS ネットワークにアクセスするには、「customer」踏み台をエントリポイントとして使用する必要があります。ネットワークパスはオンプレミスネットワークから発信され、DX/VPN を介してトランジットゲートウェイ (TGW) に移動し、共有サービス VPC にルーティングされます。踏み台にアクセスできるようになったら、アクセスリクエストが付与されていれば、AMS 環境内の他のホストにジャンプできます。
  - SSH 踏み台には次の入力が必要です。
    - SSH 踏み台に必要なインスタンス容量: デフォルト値 - 2。
    - SSH 踏み台最大インスタンス: デフォルト値 - 4。
    - SSH 踏み台最小インスタンス: デフォルト値 -2。
    - SSH 踏み台インスタンスタイプ: デフォルト値 - m5.large (t3.medium など、コストを節約するために変更できます) 。
    - SSH 踏み台入力 CIDRs: ネットワーク内のユーザーが SSH 踏み台にアクセスする IP アドレス範囲。
  - Windows RDP 踏み台には、次の入力が必要です。
    - RDP 踏み台インスタンスタイプ: デフォルト値 - t3.medium。
    - RDP 踏み台で必要な最小セッション数: デフォルト値 - 2。
    - RDP 最大セッション数: デフォルト値 -10。
    - RDP 踏み台設定タイプ: 次のいずれかの設定を選択できます。

  - SecureStandard = ユーザーは 1 つの踏み台を受け取り、1 人のユーザーだけが踏み台に接続できます。
  - SecureHA = ユーザーは 2 つの異なる AZ で 2 つの踏み台を受け取り、1 人のユーザーだけが踏み台に接続できます。
  - SharedStandard = ユーザーは に接続するための踏み台を 1 つ受け取り、2 人のユーザーは一度に同じ踏み台に接続できます。
  - SharedHA = ユーザーは 2 つの異なる AZ で 2 つの踏み台を受け取り、2 人のユーザーは一度に同じ踏み台に接続できます。
- お客様の RDP Ingress CIDRs: ネットワーク内のユーザーが RDP 踏み台にアクセスする IP アドレス範囲。

共有サービスの更新: マルチアカウントランディングゾーン

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

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

- コア OU の一部であるアカウント。

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

> **Note**
>
> AMS 演算子は、データプレーンの変更を実行するときに内部アラーム抑制変更タイプ (CT) を使用し、その CT の RFC が RFC リストに表示されます。これは、データプレーンのリリースがデプロイされると、さまざまなインフラストラクチャがシャットダウン、再起動、オフラインになるか、データプレーンのデプロイ中に無関係なアラームをトリガーする CPU

スパイクやその他のデプロイの影響が発生する可能性があるためです。デプロイが完了すると、すべてのインフラストラクチャが正常に実行されていることが確認され、アラームが再び有効になります。

ログアーカイブアカウント

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

セキュリティアカウント

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

アプリケーションアカウントタイプ

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

- AMS マネージドアプリケーションアカウント
- AMS Accelerate アカウント
- カスタマーマネージドアプリケーションアカウント

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

- ルート OU:

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

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

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

AMS マネージドアプリケーションアカウント

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

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

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

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

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

AMS Accelerate アカウント

AMS Accelerate は、ワークロードをサポートする AWS インフラストラクチャを運用できる AMS オペレーションプランです。モニタリングとアラート、インシデント管理、セキュリティ管理、バックアップ管理などの AMS Accelerate 運用サービスは、新しい移行、ダウンタイムの発生、AWS の使用方法の変更を必要とせずに利用できます。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、任意のアクセスと変更のメカニズムを使用します。

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

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

- 集中ログ記録、単一請求、セキュリティアカウントと SCPs の Config Aggregator など、マルチアカウントランディングゾーン (MALZ) コアアカウントの一部の機能は引き続き利用できます。
- AMS Accelerate は、EPS、アクセス管理、変更管理、プロビジョニングなどの一部の AMS Advanced サービスを提供していません。トランジットゲートウェイ (TGW) にアクセスして設定するには、次のステップに従うことをお勧めします。

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

Accelerate アカウントの作成

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

Accelerate アカウントへのアクセス

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

新しい Accelerate アカウントにアクセスするには：

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

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

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

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

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

Accelerate アカウントを Transit Gateway に追加するには、デプロイ | マネージドランディングゾーン | ネットワークアカウント | 静的ルート (ct-3r2ckznmt0a59) 変更タイプを使用して新しいルートをリクエストし、次の情報を含めます。

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

TGW ルートテーブルにルートを作成して、この VPC に接続します。

1. デフォルトでは、この VPC は MALZ ネットワーク内の他の VPCsと通信できません。
2. この Accelerate VPCs と通信する VPC をソリューションアーキテクトで決定します。
3. デプロイの送信 | マネージドランディングゾーン | ネットワークアカウント | 静的ルート (ct-3r2ckznmt0a59) 変更タイプを追加し、この情報を含めます。
   - ブラックホール: ルートのターゲットが使用できないことを示すために true。これは、静的ルートのトラフィックが Transit Gateway によってドロップされる場合に行います。指定した TGW アタッチメント ID にトラフィックをルーティングする場合は False。デフォルト値は false です。
   - DestinationCidrBlock: 送信先の一致に使用される IPV4 CIDR 範囲。ルーティングの決定は、最も具体的な一致に基づきます。例: 10.0.2.0/24。
   - TransitGatewayAttachmentId: ルートテーブルターゲットとして機能する TGW アタッチメント ID。ブラックホールが false の場合、このパラメータは必須です。それ以外の場合は、このパラメータを空白のままにします。例: tgw-attach-04eb40d1e14ec7272。
   - TransitGatewayRouteTableId: TGW ルートテーブルの ID。例: tgw-rtb-06ddc751c0c0c881c。

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

1. マルチアカウントランディングゾーンのネットワークアカウントで、Amazon VPC コンソールを開きます。
2. ナビゲーションペインで [Transit Gateways] を選択します。表示されるトランジットゲートウェイの TGW ID を記録します。

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

TGW アタッチメントをルートテーブルに関連付ける：

1. VPC を関連付ける TGW ルートテーブルを決定します。デプロイ | マネージドランディングゾーン | ネットワークアカウント | トランジットゲートウェイルートテーブル (ct-3dscwaeyi6cup) 変更タイプを使用して、Accelerate アカウント VPCs 用の新しいアプリケーションルートテーブルを作成することをお勧めします。
2. 管理 | マネージドランディングゾーン | ネットワークアカウント | ネットワークアカウントの TGW アタッチメント (ct-3nmh0qr338q6) RFC を関連付けて、VPC または TGW アタッチメントを選択したルートテーブルに関連付けます。

TGW ルートテーブルにルートを作成して、この VPC に接続します。

1. デフォルトでは、この VPC はマルチアカウントランディングゾーンネットワーク内の他の VPCs と通信できません。
2. この Accelerate アカウント VPCs と通信する VPC をソリューションアーキテクトで決定します。

3. デプロイの送信 | マネージドランディングゾーン | ネットワークアカウント | ネットワークアカウントに対して静的ルート (ct-3r2ckznmt0a59) RFC を追加して、必要な TGW ルートを作成します。

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

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

カスタマーマネージドアプリケーションアカウント

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

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

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

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

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

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

カスタマーマネージドアカウントへのアクセス

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

CMA にアクセスするには：

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

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

CMA と Transit Gateway の接続

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

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

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

- ブラックホール: ルートのターゲットが使用できないことを示すために true。これは、静的ルートのトラフィックが Transit Gateway によってドロップされる場合に行います。指定した TGW アタッチメント ID にトラフィックをルーティングする場合は False。デフォルト値は false です。
- DestinationCidrBlock: 送信先の一致に使用される IPV4 CIDR 範囲。ルーティングの決定は、最も具体的な一致に基づきます。例えば、`10.0.2.0/24` などです。

- TransitGatewayAttachmentId: ルートテーブルターゲットとして機能する TGW アタッチメント ID。ブラックホールが false の場合、このパラメータは必須です。それ以外の場合は、このパラメータを空白のままにします。例えば、`tgw-attach-04eb40d1e14ec7272` などです。
- TransitGatewayRouteTableId: TGW ルートテーブルの ID。例えば、`tgw-rtb-06ddc751c0c0c881c` などです。

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

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

TGW アタッチメントをルートテーブルに関連付ける :

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

TGW ルートテーブルにルートを作成して、この VPC に接続します。

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

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

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

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

カスタマーマネージドアカウントに関する運用上のヘルプの取得

AMS は、アカウントを AMS Accelerate にオンボーディングすることで、カスタマーマネージドアカウントにデプロイしたワークロードを運用するのに役立ちます。AMS Accelerate を使用すると、新しい移行を経験したり、ダウンタイムが発生したり、使用方法を変更したりすることなく、

モニタリングとアラート、インシデント管理、セキュリティ管理、バックアップ管理などの運用サービスからメリットを得ることができます AWS。AMS Accelerate は、定期的なパッチ適用を必要とする EC2-basedワークロード用のオプションのパッチアドオンも提供します。AMS Accelerate では、AMS Advanced カスタマーマネージドアカウントと同様に、すべての AWS サービスをネイティブに、または任意のツールで引き続き使用、設定、デプロイします。AMS は、チームのスケーリング、コストの最適化、セキュリティと効率の向上、回復力の向上に役立つ実証済みのプラクティスを適用しながら、任意のアクセスと変更のメカニズムを使用します。詳細については、 Accelerate サービスの説明を参照してください。

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

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

AMS Tools アカウント (ワークロードの移行)

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

ツールアカウントには以下が用意されています。

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

高レベルのアーキテクチャ図 :

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

> **Note**
>
> これは移行ハブであるため、2 つのアベイラビリティーゾーン (AZs) を使用することをお勧めします。
> デフォルトでは、AMS はすべてのアカウントに次の 2 つのセキュリティグループ (SGs) を作成します。これら 2 つの SGsが存在することを確認します。存在しない場合は、AMS チームで新しいサービスリクエストを開いてリクエストしてください。
>
> - SentinelDefaultSecurityGroupPrivateOnlyEgressAll
> - InitialGarden-SentinelDefaultSecurityGroupPrivateOnly
>
> CloudEndure レプリケーションインスタンスが、オンプレミスに戻るルートがあるプライベートサブネットに作成されていることを確認します。プライベートサブネットのルートテーブルに TGW へのデフォルトルートがあることを確認することができます。ただし、CloudEndure マシンのカットオーバーを実行すると、オンプレミスに戻るルートがない「分離された」プライベートサブネットに移動し、インターネットアウトバウンドトラフィックのみが許可されます。オンプレミスリソースへの潜在的な問題を回避するために、分離されたサブネットでカットオーバーが発生するようにすることが重要です。

前提条件:

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

AWS アプリケーション移行サービス (AWS MGN)

AWS Application Migration Service (AWS MGN) は、ツールアカウントのプロビジョニング中に自動的に作成される IAM `AWSManagedServicesMigrationRole` ロールを介して MALZ Tools アカウ

ントで使用できます。 AWS MGN を使用して、サポートされているバージョンの Windows および Linux オペレーティングシステムで実行されるアプリケーションとデータベースを移行できます。

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

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

MGN AWS 初期化のリクエスト

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

```
RFC Subject=Please initialize AWS MGN in this account
RFC Comment=Please click 'Get started' on the MGN welcome page here:

    https://console.aws.amazon.com/mgn/home?region=MALZ_PRIMARY_REGION#/welcome using
 all default values
    to 'Create template' and complete the initialization process.
```

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

新しい AMS Tools アカウントへのアクセスを有効にする

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

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

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

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

   - IAM ロール: `AWSManagedServicesMigrationRole`
   - IAM ユーザー: `customer_cloud_endure_user`

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

   AMS コンソールに移動し、次の RFCs。

   a. KMS キーを作成します。KMS キーの作成 (自動) または KMS キーの作成 (レビューが必要) を使用します。

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

   b. KMS キーを共有します。

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

最終的なアカウント設定の例：

AMS の事前承認された IAM CloudEndure ポリシーの例

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

AMS Tools アカウント接続とend-to-endテスト

1. まず、CloudEndure を設定し、AMS にレプリケートするサーバーに CloudEndure エージェントをインストールします。
2. CloudEndure でプロジェクトを作成します。
3. シークレットマネージャーを使用して、前提条件を実行したときに共有された AWS 認証情報を入力します。
4. レプリケーション設定：
   a. レプリケーションサーバーに適用するセキュリティグループを選択するオプションで、両方の AMS "Sentinel" セキュリティグループ (プライベートのみと EgressAll) を選択します。
   b. マシン (インスタンス) のカットオーバーオプションを定義します。詳細については、「ステップ 5」を参照してください。カットオーバー
   c. サブネット: プライベートサブネット。

5. セキュリティグループ：
   a. AMS "Sentinel" セキュリティグループ (プライベートのみと EgressAll) の両方を選択します。
   b. カットオーバーインスタンスは、AMS 管理の Active Directory (MAD) と AWS パブリックエンドポイントと通信する必要があります。
      i. Elastic IP: なし
      ii. パブリック IP: なし
      iii. IAM ロール: customer-mc-ec2-instance-profile
   c. 内部タグ付け規則に従ってタグを設定します。
6. CloudEndure エージェントをマシンにインストールし、EC2 コンソールの AMS アカウントに表示されるレプリケーションインスタンスを探します。

AMS 取り込みプロセス：

AMS Tools アカウントのハイジーン

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

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

- ロール
- ユーザーとアカウント

大規模な移行 - Migration Factory

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

MALZ: Core アカウントのオンボーディング

AWS マルチアカウントランディングゾーンコアアカウントへのオンボーディング時に実行する必要がある主要なタスクは次のとおりです。

トピック

- AMS で AWS マルチアカウントランディングゾーンコアアカウントを作成する
- AMS がアカウントにアクセスするための IAM ロールを作成する
- AMS のルートユーザーの多要素認証 (MFA) を使用して新しいアカウントを保護する
- Trend Micro Endpoint Protection (EPS) AWS Marketplace の にサブスクライブする
- ネットワークを設定する
- アクセス管理を設定する

オンボーディングに関する質問については、Cloud Architect にお問い合わせください。

AMS で AWS マルチアカウントランディングゾーンコアアカウントを作成する

AMS マルチアカウントランディングゾーンでは、AMS マルチアカウントランディングゾーン環境の管理アカウントとして機能する新しい Amazon Web Services (AWS) アカウントのプロビジョニングが必要です。を作成するには AWS アカウント、step-by-stepに従います。新しい Amazon Web Services アカウントを作成してアクティブ化する方法を教えてください。

簡単なステップは、アカウントの作成に移動し、今すぐサインアップをクリックし、開いたページで新しい の作成 AWS アカウントをクリックします。画面の指示に従ってください。これには、電話の受信と電話のキーパッドを使用した PIN の入力が含まれます。また、クレジットカードを入力する必要があります。AMS は、このアカウントを新しいマルチアカウントランディングゾーンの管理アカウントまたは支払者アカウントとして使用します。

Note

オンボーディングが完了したら、クレジットカードから請求書システムへの請求の移動について、クラウドサービス配信マネージャー (CSDM) に相談してください。以下の情報が必要です。

- 請求会社名
- 請求連絡先名
- 請求連絡先の電話番号
- 請求連絡先 E メール
- 請求アドレス

CSDM がこの更新に役立ちます。完了したら、支払い方法を変更するには、AWS 「支払い方法の管理」を参照してください。

Note

新しいアカウントを既存の管理アカウントまたは支払者アカウントにリンクしないでください。
アカウントが既存の の一部ではないことを確認します AWS Organizations。詳細については、「 とは」を参照してください AWS Organizations。

Important

潜在的なセキュリティインシデントへの対応を受け取れるように、E メールアドレス (個人の E メールアドレスではなくディストリビューションリスト) と電話番号がアカウントに関連付けられていることを確認することが非常に重要です。アカウントの電話番号と E メールアドレスは、アカウントのパスワードをリセットしないと変更できません。これは、AMS ルートアカウントにとって重要な作業です。これらの値を安定させるには、個人に関連付けられていない連絡先情報を選択することが重要であり、これは変更される可能性があります。グループを指す E メールエイリアスを選択します。電話番号を選択する場合と同じ方法に従います。グループを指す番号、または個人ではなく会社が所有する番号を指すことができる番号を選択します。

Core アカウントを AMS マルチアカウントランディングゾーンにオンボードするように求められる質問の詳細については、「」を参照してください付録: マルチアカウントランディングゾーン (MALZ) オンボーディングに関する考慮事項リスト。

AMS がアカウントにアクセスするための IAM ロールを作成する

新しい が正常に作成されたので AWS アカウント、プロセスの次のステップは、新しいアカウントへの AMS アクセスを許可して AMS 環境を作成および設定し、進行中の変更およびプロビジョニングリクエストを満たすことです。詳細については、「IAM ロールを使用して AWS アカウント間でアクセスを委任する」を参照してください。

AWS Identity and Access Management (IAM) は、ユーザーの AWS リソースへのアクセスを安全に制御するのに役立つウェブサービスです。IAM を使用して、 AWS リソースを使用できるユーザー (認証) 、使用できるリソース、および使用方法 (認可) を制御します。

AWS コンソールへの IAM アクセスをアクティブ化する

1. ルートアカウントの認証情報 (の作成に使用した E メールとパスワード) を使用して AWS マネジメントコンソールにサインインします AWS アカウント。他の IAM 認証情報でサインインしないでください。 AWS マネジメントコンソールのホームページが開きます。
2. 上部のナビゲーションバーで、アカウント名のドロップダウンメニューを開き、アカウントを選択します。請求のホームページが開きます。
3. 請求情報への IAM ユーザーおよびロールアクセスまで下にスクロールし、編集を選択します。Activate IAM アクセスエリアが開きます。
4. チェックボックスをオンにし、更新を選択します。これで、IAM ポリシーを使用して、ユーザーがアクセスできるページを制御できるようになります。

AMS が使用する IAM ロールを作成する

1. AMS がインフラストラクチャの作成に使用する IAM ロールを定義する JSON または YAML ファイルを取得します。次のいずれかを実行します:

   - AMS クラウドアーキテクト (CA) には、JSON または YAML ファイルが用意されています。
   - onboarding_iam_roles.zip をダウンロードし、次のいずれかを選択できます。
     - onboarding_role_admin.json (短いほど、完全な管理者アクセス権が付与されます)
     - onboarding_role_minimal.json (これより長く、最小特権を付与)

2. 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。

3. [Create Stack] (スタックの作成) を選択します。次のページが表示されます。

4. 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。

5. スタック名セクション**ams-onboarding-role**に「」と入力し、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。

6. 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。
7. スタックが正常に作成されたことを確認します。

AMS のルートユーザーの多要素認証 (MFA) を使用して新しいアカウントを保護する

このセクションは、機密性の高い AMS セキュリティ関連情報が含まれているため、編集されています。この情報は、AMS コンソールのドキュメントから入手できます。AWS Artifact にアクセスするには、CSDM に連絡して手順を確認するか、「AWS Artifact の開始方法」を参照してください。

Trend Micro Endpoint Protection (EPS) AWS Marketplace の にサブスクライブする

Trend Micro Endpoint Protection (EPS) は、オペレーティングシステムのセキュリティのための AMS 内のプライマリコンポーネントです。AMS ランディングゾーンの作成が開始されたら EPS をセットアップするには、共有サービスのコアアカウントにログインし、Trend Micro Deep Security AMI にサブスクライブする必要があります AWS Marketplace。CSDM または CA から通知されます。

1. のオンボーディングアンケートで指定したロールまたはユーザーを使用して AWS コンソールにログインします。 `CustomerEPSSubscriptionIAMRoleOrUser`
2. ロールの切り替え画面に移動します。

- アカウント: AMS によって提供される
- ロール: `EPSMarketplaceSubscriptionRole`
- 表示名: EPS サブスクリプションセッション

で Trend Micro Deep Security にサブスクライブするには AWS Marketplace、コンソールでロールを切り替えた後、次の手順に従います。

1. AWS Marketplace に移動します。
2. ニーズに合った AWS Marketplace 製品を検索する で、次のオプションを選択します。
   a. ベンダー: Trend Micro
   b. 料金プラン: ライセンスを持っている場合、またはホスト請求ごとに自分のライセンスを持ち込む
   c. 配信方法: Amazon マシンイメージ
3. 右側のパネルで「サブスクリプションに進む」をクリックします。
4. 利用規約を確認し、右上隅にある利用規約に同意するをクリックします。
5. アカウントからサインアウトし、手順が完了したことを Cloud Architect に確認します。

この時点で、AMS はインフラストラクチャを AMS 環境にデプロイし、ネットワークを接続してアクセスを設定すると、環境を使用できるようになります。

ネットワークを設定する

AMS 環境のネットワークは、主にネットワークコアアカウントで処理されます。

AWS Managed Services (AMS) のネットワークをセットアップするには、いくつかのプロセスを完了する必要があります。

- AMS 環境に IP スペースを割り当てる
- へのプライベートネットワーク接続の確立 AWS
- AMS オペレーションを許可するようにファイアウォールを設定する

AMS 環境に IP スペースを割り当てる

オンボーディングアンケートに記入しながら、AMS 環境の IP スペースを定義するために Cloud Architect と既に連携しているはずです。

AMS AWS での へのプライベートネットワーク接続の確立

AWS は、 AWS Direct Connect を介して VPN 接続と専用ラインを使用してプライベート接続を提供します。プライベート接続は、次の 2 つの方法で設定できます。

- Transit Gateway を使用した一元化された Edge 接続
- Direct Connect や VPN をアカウント VPCsに接続する

Transit Gateway を使用した一元化されたエッジ接続

AWS Transit Gateway は、Amazon Virtual Private Cloud (VPCs) とオンプレミスネットワークを単一のゲートウェイに接続できるサービスです。Transit Gateway を使用すると、既存のエッジ接続を統合し、単一の進入/退出ポイントを介してルーティングできます。詳細については、AWS 「Transit Gateway」を参照してください。

Direct Connect を Transit Gateway に接続する

既存の Direct Connect 接続を使用するか、既存の AWS アカウントの 1 つで新しい Direct Connect 接続を作成できます。Direct Connect 接続は、1 Gbps 以上で実行される専用接続またはホスト接続である必要があります。

> **Note**
>
> AWS サービスで Direct Connect を使用する方法については、AWS 「Direct Connect ロケーションの開始方法」を参照してください。

既存の Direct Connect 専用接続を使用するには、接続に 3 つ以上のトランジット仮想インターフェイスを作成することはできません。これは、 Direct Connect 専用接続には、接続あたり 4 つのトランジット仮想インターフェイスの制限があるためです。

Direct Connect の制限の詳細については、AWS 「Direct Connect の制限」を参照してください。

Direct Connect 接続が利用可能になると、次のようになります。

1. AMS は、ネットワークアカウントに Direct Connect Gateway を作成します。Direct Connect Gateway の自律システム番号 (ASN) と、Direct Connect Gateway からアドバタイズする必要があるプレフィックスを指定する必要があります。この ASN は Amazon ASN として使用されます。
2. 新しい Transit VIF を作成し、仮想インターフェイス所有者をネットワークアカウントとして設定します。
3. AMS はネットワークアカウントにログインし、接続提案を受け入れます。
4. AMS はトランジットゲートウェイを Direct Connect ゲートウェイに関連付けます。
5. AMS はアタッチメントをオンプレミス Transit Gateway ルーティングテーブルに関連付けます。

> **Note**
>
> Direct Connect ゲートウェイと Transit Gateway に提供される ASN は異なる必要があります。

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

VPN を Transit Gateway に接続する

VPN 接続を Transit Gateway にアタッチするには、カスタマーゲートウェイを指定する必要があります。カスタマーゲートウェイの要件の詳細については、Amazon VPC ネットワーク管理者ガイドの「カスタマーゲートウェイの要件」を参照してください。

BGP ASN 番号、静的パブリック IP アドレス、ルーティングオプション (静的または動的) を指定する必要があります。これらの詳細を指定すると、AMS は VPN アタッチメントを作成し、そのアタッチメントをオンプレミスの Transit Gateway ルーティングテーブルに関連付けます。

Transit Gateway アタッチメントの詳細については、「Transit Gateway VPN アタッチメント」を参照してください。

Direct Connect や VPN をアカウント VPCsに接続する

VPCs を Direct Connect または VPN に直接接続することもできます。トラフィックは、トランジットゲートウェイを経由することなくVPCs から Direct Connect または VPN に直接流れます。

> **Note**
>
> プライベート接続を確立するには、共有サービス VPC とアプリケーションアカウント VPCs を Direct Connect または VPN 接続に接続する必要があります。

Direct Connect AMS でのセットアップ

AMS 管理の VPC と内部ネットワークの間で通信 Direct Connect するように を設定します。

> **Note**
>
> AWS サービスで Direct Connect を使用する方法については、Direct Connect 「 ロケーションの開始方法」を参照してください。

Direct Connect 接続を設定するには、次の手順を実行します。

1. Amazon Web Services (AWS) にサインアップする
2. Direct Connect 接続リクエストを送信します。
3. Cross Connect を完了します。
4. （ オプション) で冗長接続を設定します Direct Connect。
5. AMS によって実行: 仮想インターフェイスを作成します。
6. AMS によって実行: ルーター設定をダウンロードします。
7. 仮想インターフェイスを確認します。

VPN のセットアップ

AMS が管理する VPC と内部ネットワーク間で通信するように VPN を設定するために AMS が実行する基本的なステップ。

> **Note**
>
> AWS サービスでの VPN の使用に関する全体的な理解を得るには、「What is AWS Site-to-Site VPN」と「Customer Gateway (VPN アプライアンス) 」を参照してください。

AWS VPN ユーザーガイドの開始方法と Site-to-Site VPN 接続のテストセクションに従って、次のステップを完了します。

1. AWS VPC で、カスタマーゲートウェイを作成します。
2. AWS VPC で、仮想プライベートゲートウェイを作成します。
3. AWS VPC で、ルートテーブルでルート伝播を有効にします。
4. AWS VPC で、セキュリティグループを更新してインバウンド SSH、RDP、ICMP アクセスを有効にします。
5. 内部ネットワークで、VPN 接続を作成し、カスタマーゲートウェイを設定します。
6. VPC と内部ネットワーク間の VPN 接続をテストします。

アクセス管理を設定する

AWS Managed Services (AMS) によって管理されるネットワークを使用すると、クラウドインフラストラクチャを管理するための AMS アクセスが付与されます。プライベートネットワークと AMS を安全に接続する方法を設定する必要があります。これはいくつかの決定から始まります。

- AMS API/CLI とコンソールアクセス: AMS CLI をインストールします (手順については、このドキュメントを参照してください) 。AMS 変更管理 API を使用して AMS に変更リクエストを行い、AMS SKMS API を使用して AMS マネージドリソースについて学習します。Active Directory フェデレーションサービス (AD FS) を使用すると、AMS コンソールにアクセスできます。
- ユーザーアクセス: AMS 側の AD (Directory Services 経由) と、ユーザーの管理に使用するディレクトリとの間に接続を確立する必要があります。
- インスタンスアクセス: インスタンスレベルのアクセスは、一方向の信頼設定を介して行われます。Directory Services は CORP AD の認証情報を信頼し、AMS 側のスタックが CORP 認証情報を使用したログインを許可できるようにします。

> **Note**
>
> AMS が信頼を設定する Active Directory (AD) は、AWS リソースへのアクセスを許可するユーザーのアカウントを持つディレクトリである必要があります。

Active Directory の信頼を確立する

信頼を設定するには、AMS でドメインコントローラーのローカルポリシー -> セキュリティオプション -> ネットワークアクセス: 匿名でアクセスできる名前付きパイプ、Netlogon パイプと lsarpc パイプを一覧表示する必要があります。これらのパイプはデフォルトで一覧表示されますが、セキュリティ上の懸念のために削除されることがあります。信頼が確立されたら、再度リストから削除できます。

条件付きフォワーダーを設定する

1. AD DNS Manager -> DNS ドメインで新しい条件付きフォワーダーを作成する： 指定されたドメイン名 AMS を使用します。たとえば、A523434123.amazonaws.com (オンボーディングアンケートで選択したドメイン名に変更します。
2. マスターサーバーの IP アドレスの下： AMS が提供する IP アドレスを追加します。両方のアドレスを検証して、接続の問題がないことを確認します。
3. この条件付きフォワーダーを Active Directory に保存し、次のようにレプリケートします。このドメイン内のすべての DNS サーバーを選択し、OK を押します。

AD 信頼を設定する

Microsoft AD の記事「このセクションで説明されている設定と選択肢を使用して、信頼の一方に対して一方向の受信フォレスト信頼を作成する」に従ってください。

1. Start -> Administrative Tools -> Active Directory Domains and Trusts ダイアログを開きます。信頼を確立するドメインのドメインノードを右クリックし、プロパティ -> Trusts -> New Trust をクリックして New Trust Wizard を開きます。信頼名に AMS から提供されたドメイン名を入力し、次へを押します。
2. Trust Type で、適切な信頼レベル (フォレストトラストなど) を選択します。PressNext。
3. 信頼の方向で、一方向: 受信を選択します。[次へ] を選択します。
4. Sides of Trust で、このドメインのみを選択します。[次へ] を選択します。
5. Trust Password に、選択したパスワードを入力します。[次へ] を選択します。
6. Trust Selections Completed と Trust Creation Complete の場合は、Next を押します。
7. 「受信信頼の確認」で「いいえ」を選択し、受信信頼を確認しません。[次へ] を選択します。
8. 「新しい信頼ウィザードの完了」で、「完了」を選択し、「OK」を選択して閉じます。
9. 信頼パスワードを入力します (セキュリティ上の理由から、CSDM の電話番号からお問い合わせください) 。AMS は信頼設定を完了します。

Active Directory のサイトとサービス

ログインのレイテンシーを減らすには、VPC CIDR 範囲を Active Directory のサイトとサービスに追加します (開始 -> 管理ツール -> Active Directory のサイトとサービス) 。AWS に最も近いドメインコントローラーを含む Active Directory サイトに VPC CIDR 範囲を追加します。

AMS 専用サイトの AD サイト名を CSDM に入力します。AMS は、AD の AMS 側のデフォルトサイトの名前を、指定された名前と一致するように変更します。

Active Directory 名のサフィックスルーティング

一方向フォレスト信頼が確立されたら、次の手順を実行してサフィックスルーティングを検証します。

1. 開始 > すべてのプログラム > 管理ツールで、Active Directory ドメインと信頼をクリックします。

   Active Directory ドメインと信頼コンソールが開きます。
2. 企業ドメインを右クリックし、プロパティをクリックします。

   そのドメインのプロパティダイアログが開きます。
3. Trusts タブをクリックします。

   Trusts ページが開きます。
4. Amazon ドメイン名をクリックし、プロパティをクリックします。

   Amazon ドメイン信頼のプロパティページが開きます。
5. Name Suffix Routing をクリックし、Refresh をクリックします。

   サービスプリンシパル名 (SPNs) が信頼を解決できるように、競合がないことを確認します。

AMS IAM ロールを使用して Active Directory をフェデレーションする

ディレクトリを AMS IAM ロールとフェデレーションする目的は、企業のユーザーが企業の認証情報を使用して AWS コンソールと AWS APIs、つまり AMS コンソールと APIs とやり取りできるようにすることです。

フェデレーションプロセスの例

この例では Active Directory フェデレーションサービス (AD FS) を使用していますが、AWS IAM フェデレーションをサポートするすべてのテクノロジーがサポートされています。AWS がサポートする IAM フェデレーションの詳細については、「IAM パートナーと ID プロバイダーとフェデレーション」を参照してください。CSDM は、AD チームや AMS との共同作業を含むこのプロセスを支援します。

API アクセスに SAML を統合する方法の詳細については、この AWS ブログ「SAML 2.0 と AD FS を使用したフェデレーティッド API と CLI アクセスの実装方法」を参照してください。

AMS CLI と SAML をインストールする例については、「付録: AD FS クレームルールと SAML 設定」を参照してください。

AMS コンソールへのフェデレーションの設定 (MALZ)

次の表に詳述されている IAM ロールと SAML ID プロバイダー (信頼されたエンティティ) は、AMS インフラストラクチャの一部としてプロビジョニングされています。これらのロールを使用すると、AMS コアアカウントを監査して表示できます。

ロール	アクセス許可
AWSManagedServicesReadOnlyRole	コアアカウントの AMS インフラストラクチャを表示できます。
AWSManagedServicesCaseRole	新しいアプリケーションアカウントのリソースを表示し、AMS インシデントとサービスリクエストをファイルできます。
AWSManagedServicesChangeManagementRole	コアアカウントの AMS インフラストラクチャを表示したり、AWS サポートチケットをファイリングしたり、いくつかの RFCsリクエストしたりできます。

異なるアカウントで使用可能なロールの完全なリストについては、「」を参照してくださいAMS の IAM ユーザーロール。

コンソールアクセスの確認

ADFS をセットアップし、認証に使用する AMS URL を取得したら、以下の手順に従います。

Active Directory フェデレーティッドサービス (ADFS) 設定では、以下のステップを実行できます。

1. ブラウザウィンドウを開き、アカウントのサインインページに移動します。アカウントの ADFS IdpInitiatedSignOn ページが開きます。
2. 次のいずれかのサイトにサインインの横にあるラジオボタンを選択します。サインインサイトのピックリストがアクティブになります。
3. signin.aws.amazon.com サイトを選択し、サインインをクリックします。認証情報を入力するためのオプションを開きます。
4. CORP 認証情報を入力し、サインインをクリックします。 AWS マネジメントコンソール が開きます。
5. AMS コンソールの URL をロケーションバーに貼り付け、Enter キーを押します。AMS コンソールが開きます。

API アクセスの検証

AMS は AWS API を使用します。AMS 固有のオペレーションについては、「AMS API リファレンス」を参照してください。

AWS には、Tools SDKs がいくつか用意されています。SDK を使用しない場合は、直接 API コールを実行できます。認証の詳細については、「AWS API リクエストの署名」を参照してください。SDK を使用していない場合、または直接 HTTP API リクエストを行う場合は、変更管理 (CM) および SKMS に AMS CLIs を使用できます。

AMS CLIs のインストール

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

1. AWS CLI をインストールするには、「AWS コマンドラインインターフェイスのインストール」を参照して、適切な手順に従ってください。このページの下部には、さまざまなインストーラー、Linux、MS Windows、macOS、仮想環境、バンドルインストーラー (Linux、macOS、または Unix) を使用する手順があることに注意してください。
2. インストール後、aws help を実行してインストールを確認します。
3. AWS CLI がインストールされたら、AMS CLI をインストールまたはアップグレードするには、AMS 配布用 zip ファイルをダウンロードして解凍します。AMS CLI の頒布可能ファイルには、AMS コンソールの左側のナビゲーションにあるドキュメントリンクからアクセスできます。または、クラウドサービス配信マネージャー (CSDM) に zip ファイルの送信を依頼してください。

4. オペレーティングシステムに応じて、 Managed Cloud Distributables -> CLI -> Windows または Managed Cloud Distributables -> CLI -> Linux / MacOS ディレクトリを開きます。
5. Windows の場合は、適切なインストーラを実行します (この方法は Windows 32 または 64 ビットシステムでのみ機能します)。
   - 32 ビット: ManagedCloudAPI_x86.msi
   - 64 ビット: ManagedCloudAPI_x64.msi
6. Mac/Linux の場合は、次のコマンドを実行して MC_CLI.sh という名前のファイルを実行します: sh MC_CLI.sh。amscm および amsskms ディレクトリとその内容は、MC_CLI.sh ファイルと同じディレクトリにある必要があります。
7. 企業の認証情報を AWS とのフェデレーション (AMS デフォルト設定) 経由で使用する場合は、フェデレーションサービスにアクセスできる認証情報管理ツールをインストールする必要があります。例えば、この AWS セキュリティブログ How to Implement Federated API and CLI Access Using SAML 2.0 and AD FS を使用して、認証情報管理ツールの設定に役立てることができます。
8. インストール後、 `aws amscm help`と `aws amsskms help` を実行してコマンドとオプションを表示します。

MALZ: アプリケーションアカウントのオンボーディング

新しいアプリケーションアカウントをリクエストする前に、コアアカウントでマルチアカウント AWS Managed Services (AMS) 環境を設定する必要があります。環境をセットアップした後に実行する必要がある手順は次のとおりです。

トピック

- 新しいアプリケーションアカウントのリクエスト
- AMS IAM ロールへのアクセスをフェデレーションするように Active Directory を設定する
- 新しいアプリケーションアカウントとのネットワークの設定
- アプリケーションアカウントで追加の VPCs を設定する

オンボーディングに関する質問については、クラウドサービスデリバリーマネージャー (CSDM) にお問い合わせください。「アプリケーションアカウント: AMS 管理、開発モード、カスタマー管理」も参照してください。モードの一般的な情報については、「AMS モード」を参照してくださいAWS Managed Services でのサービス管理。

アプリケーションアカウントのさまざまなモードの詳細については、「アプリケーションアカウント: AMS 管理、開発モード、カスタマー管理」を参照してください。モードの一般的な情報については、「AMS モード」を参照してください。

新しいアプリケーションアカウントのリクエスト

新しいアプリケーションアカウントをリクエストする前に、コアアカウントでマルチアカウント AWS Managed Services (AMS) 環境を設定する必要があります。コアアカウントでマルチアカウント環境を設定する方法については、「」を参照してくださいMALZ: Core アカウントのオンボーディング。

アプリケーションアカウントの初期 VPC には、次のいずれかの Amazon VPC タイプを選択できます。

- プライベート: この VPC にはインターネットゲートウェイがアタッチされていません。これは、インターネットとの間のアクセスを必要としないプライベートアプリケーションに適しています。
- パブリック: この VPC にはインターネットゲートウェイがアタッチされており、パブリックサブネットとプライベートサブネットがあります。これは、インターネットとの間のアクセスを必要とするパブリックアプリケーションに適しています。

Deployment | Managed Landing Zone | Management Account | Create application account (with VPC) (ct-1zdasmc2ewzrs) RFC を送信し、RFC に次の値を指定することで、新しいアプリケーションアカウントをリクエストできます。

- アカウント名: アカウントのカスタム名。アカウント名の最大長は 50 文字です。
- アカウント E メール: アカウントのディストリビューションリスト E メール。この E メール ID は、AWS アカウントの作成に使用されます。
- サポートレベル: AWS サポートレベル、プレミアムまたはプラス。
- VPC 名: VPC の名前。
- アベイラビリティーゾーン (AZs) の数: 2 または 3。
- VPC CIDR: VPC の CIDR ブロック。
- ルートタイプ: これは `routable`または のいずれかです`isolated`。 は、Transit Gateway (TGW) アプリケーションルートテーブルに関連付けられたアプリケーション VPCs がこの VPC に接続できる`Routable`ことを意味します。 は、TGW アプリケーションルートテーブルに関連付けられたアプリケーション VPCs がこの VPC に接続できない`Isolated`ことを意味します。デフォルトは `routable` です。

- トランジットゲートウェイアプリケーションルートテーブル: アプリケーションアカウント VPC を関連付ける必要があるトランジットゲートウェイルートテーブル。値を指定しない場合、デフォルト`defaultAppRouteDomain`が使用されます。つまり、このアカウントは同じルートテーブル内の他のすべてのアカウントと通信できます。
- AZ 1 のパブリックサブネットの PublicSubnetAZ<1-3>CIDRCIDR: アベイラビリティーゾーン 1 のパブリックサブネットの CIDR。
- AZ 1 のパブリックサブネットの PrivateSubnet<1-10>AZ*<I-3>*CIDRCIDR: アベイラビリティーゾーン 1 のパブリックサブネットの CIDR。

この時点で、AMS は指定された VPC 設定を使用して、新しいアプリケーションアカウントを AMS 管理アカウントにデプロイします。

AMS IAM ロールへのアクセスをフェデレーションするように Active Directory を設定する

ディレクトリを AMS IAM ロールとフェデレーションして、企業ユーザーが企業の認証情報を使用して AWS コンソールと AWS APIs、および AMS コンソールと AMS APIs とやり取りできるようにします。

フェデレーションプロセスの例

この例では、Active Directory フェデレーションサービス (ADFS) を使用します。ただし、AWS IAM フェデレーションをサポートするテクノロジーはすべてサポートされています。AWS がサポートする IAM フェデレーションの詳細については、「IAM パートナーと ID プロバイダーとフェデレーション」を参照してください。CSDM は、AD チームや AMS との共同作業を含むこのプロセスを支援します。

SAML を API アクセスに統合する方法の詳細については、AWS ブログ「How to Implement Federated API and CLI Access Using SAML 2.0 and AD FS」を参照してください。

AMS CLI と SAML をインストールする例については、AMS ユーザーガイドの「付録: AD FS クレームルールと SAML 設定」を参照してください。

AMS コンソールへのフェデレーションの設定

次の表に詳述されている IAM ロールと SAML ID プロバイダー (信頼されたエンティティ) は、新しいアプリケーションアカウントにプロビジョニングされます。これらのロールを使用すると、新しい

アプリケーションアカウントとファイル RFCs へのアクセス、S3 バケットへの書き込み、その他のアクションを実行できます。

ロール	アクセス許可
AWSManagedServicesReadOnlyRole	新しいアプリケーションアカウントのリソースを表示できます。
AWSManagedServicesCaseRole	新しいアプリケーションアカウントのリソースを表示し、AWS サポートチケットをファイルできます。
AWSManagedServicesChangeManagementRole	アプリケーションアカウントの AMS インフラストラクチャの表示、RFCsファイル作成、AWS サポートチケットのファイル作成、S3 バケットへの書き込み、Secrets Manager シークレットの管理、リザーブド Amazon Elastic Compute Cloud (Amazon EC2) インスタンスの管理を行うことができます。
AWSManagedServicesSecurityOpsRole	アプリケーションアカウントの AMS インフラストラクチャの表示、Secrets Manager シークレットの管理、ウェブアプリケーションファイアウォールルールの管理、証明書の管理、AWS サポートチケットのファイルを行うことができます。
AWSManagedServicesAdminRole	アプリケーションアカウントの AMS インフラストラクチャの表示、 Marketplace サブスクリプションの管理、Secrets Manager シークレットの管理、ウェブアプリケーションファイアウォールルールの管理、証明書の管理、RFCs の作成、リザーブド Amazon EC2 インスタンスの管理、S3 バケットへの書き込み、AWS サポートチケットのファイル作成、AWS Artifacts 契約の管理を行うことができます。

AMS へのフェデレーションリクエストの送信

これが最初のアカウントである場合は、CSDM (複数可) または Cloud Architect (複数可) と協力して、ID プロバイダーのメタデータ XML ファイルを提供します。

追加のアカウントまたは ID プロバイダーをオンボーディングしていて、管理アカウントまたは目的のアプリケーションアカウントにアクセスできる場合は、次の手順に従います。

1. AMS コンソールからサービスリクエストを作成します。

   > **Note**
   >
   > - アプリケーションアカウントの ID プロバイダーを作成する場合は、アプリケーションアカウント自体または管理アカウントからこのリクエストを送信します。
   > - AMS コアアカウントの ID プロバイダーを作成する場合は、管理アカウントからこのリクエストを送信します。
   > - 管理アカウントの ID プロバイダーを作成する場合は、管理アカウントからこのリクエストを送信するか、CSDM にお問い合わせください。

   サービスリクエストで、ID プロバイダーを追加するために必要な詳細を入力します。

   - 新しい ID プロバイダーが作成されるアカウントの AccountId。
   - 希望する ID プロバイダー名を指定しない場合、デフォルトは customer-saml になります。通常、これはフェデレーションプロバイダーで設定された設定と一致する必要があります。
   - 既存のアカウントの場合、新しい ID プロバイダーを既存のすべてのコンソールロールに伝達するか、新しい ID プロバイダーを信頼するロールのリストを提供するかを含めます。
   - フェデレーションエージェントからサービスリクエストにエクスポートされたメタデータ XML ファイルをファイルアタッチメントとしてアタッチします。
2. サービスリクエストを作成したのと同じアカウントから、以下の情報を含む CT-ID ct-1e1xtak34nx76 (管理 | その他 | その他 | 作成) を使用して新しい RFC を作成します。

   - タイトル：「Onboard SAML IDP <Name> for Account <AccountId>」。
   - ID プロバイダーが作成されるアカウントの AccountId。
   - ID プロバイダー名。

- 既存のアカウントの場合: ID プロバイダーを既存のすべてのコンソールロールに伝達するか、新しい ID プロバイダーを信頼するロールのリストに伝達するか。
- メタデータ XML ファイルがアタッチされているステップ 1 で作成されたサービスリクエストのケース ID。

コンソールアクセスの検証

AD FS でセットアップし、認証に使用する AMS URL を取得したら、次の手順を実行できます。

Active Directory フェデレーティッドサービス (AD FS) 設定では、以下のステップを実行できます。

1. ブラウザウィンドウを開き、アカウントのサインインページに移動します。アカウントの AD FS IdpInitiatedSignOn ページが開きます。
2. 次のいずれかのサイトにサインインの横にあるラジオボタンを選択します。サインインサイトリストがアクティブになります。
3. signin.aws.amazon.com サイトを選択し、サインインを選択します。認証情報を入力するためのオプションを開きます。
4. CORP 認証情報を入力し、サインインを選択します。AWS マネジメントコンソールが開きます。
5. AMS コンソールの URL をロケーションバーに貼り付け、Enter キーを押します。AMS コンソールが開きます。

API アクセスの検証

AMS は AWS API を使用します。AMS 固有のオペレーションについては、「AMS API リファレンス」を参照してください。

AWS には、Tools SDKs がいくつか用意されています。SDK を使用しない場合は、直接 API コールを実行できます。認証の詳細については、「AWS API リクエストの署名」を参照してください。SDK を使用していない場合、または直接 HTTP API リクエストを行う場合は、変更管理 (CM) および SKMS に AMS CLIs を使用できます。

新しいアプリケーションアカウントとのネットワークの設定

アプリケーションアカウントのネットワークの設定には、ファイアウォールルールの設定や、追加の Transit Gateway (TGW) ルートテーブルの設定が含まれます。

ファイアウォールのセットアップ

AMS 環境にデプロイされたアプリケーションを使用するには、いくつかのファイアウォールルールを作成する必要があります。インスタンスにアクセスするためにこれらのルールは必要ありません。踏み台をインスタンスにホップできます。

アプリケーションアクセスのファイアウォールルール

ファイアウォール経由のトラフィックについては、次のポートを開く必要があります。

- オンプレミスネットワークから新しいアプリケーション VPC CIDRs への進入と退出の両方の方向。
- 新しいアプリケーション VPC CIDRs からオンプレミスネットワークへの進入と退出の両方の方向 (クラウドアプリケーションがオンプレミスアプリケーションに連絡する必要がある場合) 。

[ポート]	[プロトコル]	サービス	開始/終了	送信元/送信元
80	TCP	HTTP ウェブアクセス	オンプレミスネットワーク	AMS アプリケーション VPC
443	TCP	HTTPS ウェブアクセス	オンプレミスネットワーク	AMS アプリケーション VPC

追加の Transit Gateway アプリケーションルートテーブルのセットアップ

AWS Managed Services (AMS) ネットワークは柔軟で、さまざまなネットワークユースケースをサポートしています。

- 同じアカウントのアプリケーション VPCs間の通信。
- 異なるアカウントのアプリケーション VPCs間の通信。
- 異なるアカウントのアプリケーション VPCs 間の分離。
- 同じアカウント内のアプリケーション VPCs 間の分離。

ネットワークに固有の/特別な要件がある場合は、AMS クラウドアーキテクトにお問い合わせください。AMS ネットワークアーキテクチャが要件を満たすための計画を立てます。

アプリケーションアカウント VPCs のネットワーク決定に基づいて、デプロイ | マネージドランディングゾーン | ネットワークアカウント | トランジットゲートウェイルートテーブルの作成 (ct-3dscwaeyi6cup) RFC を送信することで、複数の Transit Gateway (TGW) アプリケーションルートテーブルを作成できます。

変更タイプでは、 `TransitGatewayRouteTableName` (TGW ルートテーブルのわかりやすい名前) 、`TransitGatewayId`、および を指定する必要がありますTGWRouteTableType。

> **Note**
>
> TGWRouteTableType に createCustomRouteDomain が選択されている場合、作成されたルートテーブルは空です。デプロイ | マネージドランディングゾーン | ネットワークアカウント | 静的ルート (ct-3r2ckznmt0a59) 変更タイプを使用して RFC を提出する必要があります。

アプリケーションアカウントで追加の VPCs を設定する

デプロイ | マネージドランディングゾーン | アプリケーションアカウント | VPC (ct-1j3503fres5a5) RFC を作成することで、追加のアプリケーションアカウント VPC をリクエストできます。

これは、新しいアプリケーションアカウントの VPC を設定するのと同じ方法で機能します。詳細については、新しいアプリケーションアカウントのリクエスト を参照してください

付録: マルチアカウントランディングゾーン (MALZ) オンボーディングに関する考慮事項リスト

AMS マルチアカウントランディングゾーンのデプロイを計画する際に考慮すべき重要な考慮事項がいくつかあります。選択すると、必要なインフラストラクチャコンポーネントを決定するために必要な情報が AMS に提供されます。Cloud Architect (CA) は、この作業を支援するアンケートを提供します。

トピック

- AMS マルチアカウントランディングゾーンアカウント設定
- AMS マルチアカウントランディングゾーンモニタリングアラート
- ネットワーク構成

- Active Directory の設定
- Trend Micro Endpoint Protection (EPS)
- アクセス: 踏み台、SSH、RDP
- フェデレーション

> **Note**
>
> インスタンスタイプの詳細については、Amazon EC2 インスタンスタイプ」を参照してください。
> データベースインスタンスタイプの詳細については、「Amazon RDS インスタンスタイプ」を参照してください。
> Direct Connect が必要な場合は、「AMS シングルアカウントランディングゾーンオンボーディングガイド」を参照して Direct Connect 接続を作成します。

Cloud Service Delivery Manager (CSDM) からオンボーディングアンケートが届きます。このアンケートには、アカウントに必要な設定に関する質問が含まれています。先に進む前に、CSDM と協力してアンケートを完了してください。

AMS マルチアカウントランディングゾーンアカウント設定

- 新しいアカウント ID

  AMS マルチアカウントランディングゾーン用に作成した AWS アカウント ID。 AWS 組織の一部であってはなりません。
- サービスリージョン

  AMS マルチアカウントランディングゾーン環境がデプロイされるプライマリリージョン。
- 通知のコアアカウント E メール。 (これらはすべて同じドメインに存在する必要があります)。それぞれに E メールアドレスを指定します。
  - 共有サービスアカウント
  - ネットワークアカウント
  - アカウントのログ記録
  - セキュリティアカウント
- サービスタイプ、Premium または Plus

これにより、環境内の問題を解決するためのサービスレベルアグリーメント (SLAsが決まります。

AMS マルチアカウントランディングゾーンモニタリングアラート

AMS は、特定のモニタリングアラートに対して (AMS サービス通知を取得するのではなく) 直接アラートを受け取る方法を提供します。これにサインアップするには、Cloud Architect (CA) または Cloud Service Delivery Manager (CSDM) がこの情報を受信していることを確認します。

ダイレクトアラート E メール: AMS が特定のリソースベースのアラートを送信する E メールアドレスです。E メールに直接送信されるアラートの詳細については、AMS Advanced ユーザーガイドの「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。 AMS モニタリングの詳細については、「シングルアカウントランディングゾーン用 AMS ユーザーガイド」の「モニタリング管理」を参照してください。

ネットワーク構成

- トランジットゲートウェイ ASN 番号

  これはボーダーゲートウェイプロトコル (BGP) セッションの AWS 側の自律システム番号 (ASN) です。一意である必要があり、Direct Connect または VPN で使用されているものと同じにすることはできません。 16 ビット ASNs。
- AMS マルチアカウントランディングゾーンインフラストラクチャ VPC CIDR 範囲。

  これらの CIDR 範囲はオンプレミスネットワークと重複できません

  /22 CIDR 範囲を含めることも、各 VPC CIDR を個別に指定することもできます。これらの CIDR 範囲のみが許可されることに注意してください。
  - 10.0.0.0 – 10.255.255.255 (10/8 プレフィックス)
  - 172.16.0.0 – 172.31.255.255 (172.16/12 プレフィックス)
  - 192.168.0.0 – 192.168.255.255 (192.168/16 プレフィックス)

  IP 範囲 198.18.0.0/15 は使用できません (AWS Directory Service によって予約されています)。
  - コアインフラストラクチャ VPC CIDR 範囲 (/22 範囲を推奨)
  - ネットワーク VPC CIDR 範囲 (/24 範囲を推奨)
  - 共有サービス VPC CIDR 範囲 (/23 範囲を推奨)
  - DMZ VPC CIDR 範囲 (/25 範囲を推奨)

- VPN ECMP (有効または無効)

  [VPN ECMP サポート] で、VPN 接続間で Equal Cost Multipath (ECMP) ルーティングサポートが必要な場合は [enable (有効)] を選択します。接続が同じ CIDR をアドバタイズする場合、トラフィックは複数の接続間で均等に分散されます。

ネットワークアクセスコントロールリスト (NACL)

ネットワークアクセスコントロールリスト (NACL) は、1 つ以上のサブネットに出入りするトラフィックを制御するファイアウォールとして機能する VPC 用のオプションのセキュリティレイヤーです。セキュリティの追加レイヤーを VPC に追加するには、セキュリティグループと同様のルールを指定したネットワーク ACL をセットアップできます。セキュリティグループとネットワーク ACLs「セキュリティグループとネットワーク ACLs」を参照してください。

ただし、AMS マルチアカウントランディングゾーンでは、AMS がインフラストラクチャを効果的に管理およびモニタリングするために、NACLsされます。

- NACLsは、管理、ネットワーク、共有サービス、ログ記録、セキュリティのマルチアカウントランディングゾーンコアアカウントではサポートされていません。
- NACLs「拒否」リストとしてのみ使用される限り、マルチアカウントランディングゾーンのアプリケーションアカウントでサポートされます。さらに、AMS のモニタリングと管理オペレーションを確実にするように「すべて許可」を設定する必要があります。

大規模なマルチアカウント環境では、一元化されたエグレスファイアウォールなどの機能を活用して、AMS マルチアカウントランディングゾーンのアウトバウンドトラフィックや AWS Transit Gateway ルーティングテーブルを制御し、VPCs 間でネットワークトラフィックを分離することもできます。

Active Directory の設定

AMS マネージド Active Directory のドメイン FQDN

Trend Micro Endpoint Protection (EPS)

- EC2 インスタンスと Auto Scaling グループのインスタンスサイズ

  Trend Micro Endpoint Protection (EPS) は、オペレーティングシステムのセキュリティのための AMS 内のプライマリコンポーネントです。システムは、Deep Security Manager (DSM) EC2 イン

スタンス、リレー EC2 インスタンス、およびすべての AMS データプレーンと EC2 インスタンス内に存在するエージェントで構成されます。

- リレーインスタンスタイプ (AMS でサポートされる最小サイズは m5.large)
- DB インスタンスサイズ (200 GB を推奨)
- RDS インスタンスタイプ (db.m5.large または db.m5.xlarge のみ許可)

- DSM ライセンスタイプ (Marketplace または BYOL)

  ライセンスがすでにある場合は、BYOL (独自のライセンスを持つ) を選択します。AMS は、ライセンスに関する必要な情報を取得するためにお客様に連絡します。

- AWS Trend Micro Deep Security サブスクリプションの IAM ユーザーまたはロール Amazon リソースネーム (ARN) (ロール ARN: arn:aws:iam::*ACCOUNT_ID*:role/*ROLE_NAME*)

  アクセス AWS アカウント 可能な既存の のいずれかから、IAM ロール、ARN、または IAM ユーザー ARN を提供します。AMS は、AMS マルチアカウントランディングゾーン共有サービスアカウントに IAM ロールを作成し、共有サービスの IAM ロールの信頼で提供されるロールまたはユーザーを追加して、ユーザーが Trend Micro Deep Security をサブスクライブできるようにします AWS Marketplace。

アクセス: 踏み台、SSH、RDP

- SSH 踏み台の設定

  AMS は、AMS 環境のホストにアクセスするために、共有サービスアカウントに SSH 踏み台を提供します。SSH ユーザーとして AMS ネットワークにアクセスするには、SSH 踏み台をエントリポイントとして使用する必要があります。ネットワークパスはオンプレミスネットワークから発信され、DX/VPN を介してトランジットゲートウェイ (TGW) にルーティングされ、共有サービス VPC にルーティングされます。踏み台にアクセスできるようになったら、適切なアクセスリクエストが付与されていれば、AMS 環境内の他のホストにジャンプできます。

  - 必要なインスタンス数 (2 つ推奨)
  - 最大インスタンス (4 つの推奨)
  - 最小インスタンス (2 つの推奨)
  - インスタンスタイプ (m5.large を推奨)
  - イングレス CIDRs: ネットワーク内のユーザーが SSH 踏み台にアクセスする IP アドレス範囲 (ip 範囲 1、ip 範囲 2、ip 範囲 3 など)

- RDP 踏み台の設定

AMS は、オプションで AMS 環境のホストにアクセスするために、共有サービスアカウントに RDP 踏み台を提供します。RDP ユーザーとして AMS ネットワークにアクセスするには、エントリポイントとして RDP 踏み台を使用する必要があります。ネットワークパスはオンプレミスネットワークから発信され、DX/VPN を介して TGW に進み、共有サービス VPC にルーティングされます。踏み台にアクセスできるようになったら、適切なアクセスリクエストが付与されていれば、AMS 環境内の他のホストにジャンプできます。

- インスタンスタイプ (t3.medium を推奨)
- 希望する最小セッション数 (2 つ推奨)
- 希望する最大セッション数 (10 を推奨)

- RDP 踏み台設定タイプ、共有標準または共有 HA (デフォルトは共有標準)

  SecureStandard = ユーザーは 1 つの踏み台を受け取り、1 人のユーザーだけが踏み台に接続できます。

  SecureHA = ユーザーは 2 つの異なる AZ で 2 つの踏み台を受け取り、1 人のユーザーだけが踏み台に接続できます。

  SharedStandard = ユーザーは に接続するための踏み台を 1 つ受け取り、2 人のユーザーは一度に同じ踏み台に接続できます。

  SharedHA = ユーザーは 2 つの異なる AZ で 2 つの踏み台を受け取り、2 人のユーザーは一度に同じ踏み台に接続できます。

フェデレーション

ID プロバイダー (IDP) 名

デフォルトは `customer-saml` です。

AMS シングルアカウントランディングゾーン (SALZ) オンボーディング

AMS SALZ オンボーディングプロセス

AMS シングルアカウントランディングゾーン (SALZ) アカウントをオンボードするには、次の手順を実行する必要があります。

1. AMS がファイアウォールをホストするためのネットワークアカウントとして設定する新しい AWS アカウントを作成します。AWS 組織内に新しいアカウントがある場合は作成します。AMS は通常の AMS アカウントを作成する手順に従い、必要なすべての情報を収集する必要があります (CIDR、EPS ライセンス、ユーザーなど) 。注: /24 の CIDR 割り当ては適切です。
2. 送信トラフィックアカウントからインターネットゲートウェイ (IGWs) を削除するかどうかを指定します。
3. 承認されたドメインを決定します。AMS は、承認されたドメインリストを維持することで送信先フィルタリングを有効にします。リストは後で変更できます。
4. 予想されるスループットに基づいて、使用するインスタンスサイズを確認します。デフォルトでは、インスタンスは m4.xlarge インスタンスに作成され、ファイアウォールのスループットは 350Mbps であることがわかりました。AMS は、予想されるスループットが 1.25 Gbps である c4.8xLarge インスタンスにサイズを増やすことができます。
5. AMS とプライベートネットワーク間のネットワークを設定します。これには、複数のタスクを実行します。
    a. IP スペースを割り当てる
    b. AWS へのプライベートネットワーク接続を確立する
    c. ファイアウォールをセットアップする
    d. アクセス管理を設定する
    e. バックアップをスケジュールする
6. 作成したアカウントへのアクセスを AMS に提供します。
7. AMS サービスが正しく動作していることを確認します。

AMS は、最初のリクエスト日から 2 週間 (10 営業日) 以内にアカウントのアカウントビルドアウト (オンボーディング) を実行できます。フォローアップアクティビティは、AMS Planned Event Management (PEM) を使用して実行できます。

Note

- 米国東部 (バージニア)
- 米国西部 (北カリフォルニア)
- 米国西部 (オレゴン)
- 米国東部 (オハイオ)
- カナダ (中部)
- 南米 (サンパウロ)
- 欧州 (アイルランド)
- 欧州 (フランクフルト)
- 欧州 (ロンドン)
- 欧州西部 (パリ)
- アジアパシフィック (ムンバイ)
- アジアパシフィック (ソウル)
- アジアパシフィック (シンガポール)
- アジアパシフィック (シドニー)
- アジアパシフィック (東京)

新しいリージョンは頻繁に追加されます。最新のリストについては、「AWS リージョンとアベイラビリティーゾーン」を参照してください。

SALZ ネットワークアーキテクチャ

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

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

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

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

AMS シングルアカウントランディングゾーン共有サービス

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

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

  AMS アカウントに Active Directory を作成し、AMS ドメインを作成し、起動時にマネージドスタックをドメインに結合します。
- 管理ホスト = AMS 管理ホスト (プロビジョニングと一般的なタスクを自動化)

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

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

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

- 内部踏み台ホスト = お客様の踏み台

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

SALZ: AMS の新しい AWS アカウントを作成する

AWS Managed Services (AMS) の新しい AWS アカウントを作成する 5 つのステップは次のとおりです。

1. を作成する AWS アカウント
2. 一括請求を設定する – 新しいアカウントを支払いアカウントにリンクする
3. AMS アクセス AWS アカウント 用に を設定する
4. AMS のルートユーザーの多要素認証 (MFA) を使用して新しいアカウントを保護する
5. EPS AWS Marketplace の をサブスクライブする

ご質問がある場合は、カスタマーサービスデリバリーマネージャー (CSDM) にお問い合わせください。

を作成する AWS アカウント

AMS プログラムでは、新しい Amazon Web Services (AWS) アカウントのプロビジョニングが必要です。ステップバイステップの手順については、次の動画を参照してください。新しい Amazon Web Services アカウントを作成してアクティブ化する方法を教えてください。簡単なステップは次のとおりです。

にサインアップする AWS アカウント

がない場合は AWS アカウント、次の手順を実行して作成します。

にサインアップするには AWS アカウント

1. https://portal.aws.amazon.com/billing/signup を開きます。
2. オンラインの手順に従います。

   サインアップ手順の一環として、電話またはテキストメッセージを受け取り、電話キーパッドで検証コードを入力します。

   にサインアップすると AWS アカウント、 AWS アカウントのルートユーザー が作成されます。ルートユーザーには、アカウントのすべての AWS のサービス とリソースへのアクセス権があります。セキュリティベストプラクティスとして、ユーザーに管理アクセス権を割り当て、ルートユーザーアクセスが必要なタスクの実行にはルートユーザーのみを使用するようにしてください。

AWS サインアッププロセスが完了すると、 から確認メールが送信されます。https://aws.amazon.com/ の [マイアカウント] をクリックして、いつでもアカウントの現在のアクティビティを表示し、アカウントを管理することができます。

管理アクセスを持つユーザーを作成する

にサインアップしたら AWS アカウント、日常的なタスクにルートユーザーを使用しないように AWS アカウントのルートユーザー、 を保護し AWS IAM アイデンティティセンター、 を有効にして管理ユーザーを作成します。

を保護する AWS アカウントのルートユーザー

1. ルートユーザーを選択し、 AWS アカウント E メールアドレスを入力して、アカウント所有者AWS マネジメントコンソールとして にサインインします。次のページでパスワードを入力します。

   ルートユーザーを使用してサインインする方法については、AWS サインイン ユーザーガイドのルートユーザーとしてサインインするを参照してください。
2. ルートユーザーの多要素認証 (MFA) を有効にします。

   手順については、IAM ユーザーガイドの AWS アカウント 「ルートユーザー (コンソール) の仮想 MFA デバイスを有効にする」を参照してください。

管理アクセスを持つユーザーを作成する

1. IAM アイデンティティセンターを有効にします。

   手順については、「AWS IAM アイデンティティセンター ユーザーガイド」の「AWS IAM アイデンティティセンターの有効化」を参照してください。
2. IAM アイデンティティセンターで、ユーザーに管理アクセスを付与します。

   を ID ソース IAM アイデンティティセンターディレクトリ として使用する方法のチュートリアルについては、AWS IAM アイデンティティセンター 「 ユーザーガイド」の「デフォルトを使用してユーザーアクセスを設定する IAM アイデンティティセンターディレクトリ」を参照してください。

管理アクセス権を持つユーザーとしてサインインする

- IAM アイデンティティセンターのユーザーとしてサインインするには、IAM アイデンティティセンターのユーザーの作成時に E メールアドレスに送信されたサインイン URL を使用します。

  IAM Identity Center ユーザーを使用してサインインする方法については、AWS サインイン 「 ユーザーガイド」の AWS 「 アクセスポータルにサインインする」を参照してください。

追加のユーザーにアクセス権を割り当てる

1. IAM アイデンティティセンターで、最小特権のアクセス許可を適用するというベストプラクティスに従ったアクセス許可セットを作成します。

   手順については、「AWS IAM アイデンティティセンター ユーザーガイド」の「権限設定を作成する」を参照してください。
2. グループにユーザーを割り当て、そのグループにシングルサインオンアクセス権を割り当てます。

   手順については、「AWS IAM アイデンティティセンター ユーザーガイド」の「グループの結合」を参照してください。

> **Note**
>
> アカウントがすでにある場合は、AWS 料金ページに移動し、無料アカウントの作成をクリックします。少なくとも EC2 サービスにサインアップしてください。1 つのサービスにサ

インアップすると、 のすべてのサービスにアクセスできます AWS。料金は、使用するサービスの料金のみが請求されます。
一括請求の目的で新しいアカウントを支払いアカウントにリンクする場合は、プロンプトが表示されたら支払い方法の情報を入力する必要はありません。代わりに、画面にアクセスしてクレジットカード情報を入力したら、移動します。次のセクションで詳しく説明する一括請求/連結アカウントリクエストを送信するには、支払者アカウントに関連付けられた E メールアドレスが必要です。

Important

潜在的なセキュリティインシデントへの対応を受け取れるように、E メールアドレスと電話番号がアカウントに関連付けられていることを確認することが重要です。アカウントの電話番号と E メールアドレスは、アカウントのパスワードをリセットしないと変更できません。これは、AMS ルートアカウントにとって重要な作業です。これらの値を安定させるには、個人に関連付けられていない連絡先情報を選択することが重要であり、これは変更される可能性があります。グループを指す E メールエイリアスを選択します。電話番号を選択する場合と同じベストプラクティスに従います。グループを指す番号、または個人ではなく会社が所有する番号を指すことができる番号を選択します。

一括請求を設定する – 新しいアカウントを支払いアカウントにリンクする

新しい AMS 管理の AWS アカウント 請求書を既存の AWS Organizations 管理アカウントの支払いにロールする場合は、一括請求を設定し、アカウントをリンクする必要があります。これを行う方法の詳細については、「」を参照してください。

- およびマルチアカウント請求戦略の統合 AWS Organizations請求。 AWS
- を組織に招待 AWS アカウント する

Note

アカウントを AMS に引き渡す前に、これらのステップを実行できます。引き渡し後、組織に参加するステップ (上記で提供) は、変更管理プロセスを通じて実行できます。サポートが必要な場合は、クラウドサービスの配信マネージャー (CSDM) またはクラウドアーキテクト (CA) にお問い合わせください。

一括請求の管理を含む一般的な請求情報については、AWS「請求とは」を参照してください。アカウントがどのように連携できるかに関する一般的な AWS Organizations 情報については、「 とは AWS Organizations」を参照してください。 AWS Organizations 管理アカウントに関する規範的なガイダンスについては、「管理アカウント、信頼されたアクセス、委任された管理者」を参照してください。

AMS アクセス AWS アカウント 用に を設定する

上記の手順が完了すると、新しい が正常に保護 AWS アカウント され、関連するコストが適切に請求されます。このプロセスの最後のステップは、初期スタック設定と継続的な変更およびプロビジョニングリクエストを満たすために、AMS に新しいアカウントへのアクセスを許可することです。詳細については、「IAM ロールを使用した AWS アカウント間の委任アクセス」を参照してください。基本的な手順については、このセクションで説明します。

AWS ウェブサイトへのアクセスをアクティブ化する

IAM ユーザーにアカウントの請求情報とツールへのアクセスを許可するには、この機能を有効にする必要があります。

以下の手順に従ってください。

1. ルートアカウントの認証情報 (の作成に使用した E メールとパスワード) AWS マネジメントコンソール を使用して にサインインします AWS アカウント。IAM ユーザーの認証情報でサインインしないでください。

   AWS マネジメントコンソール ホームページが開きます。

2. 上部のナビゲーションバーで、アカウント名のドロップダウンメニューを開き、マイアカウントを選択します。

   請求のホームページが開きます。

3. 請求情報への IAM ユーザーアクセスエリアまで下にスクロールし、右側の編集をクリックします。##############################。

   アクティブ化 IAM アクセスエリアが開きます。

4. チェックボックスをオンにし、更新をクリックします。

   これで、IAM ポリシーを使用して、ユーザーがアクセスできるページを制御できるようになります。

でのこのプロセスの詳細については AWS、「アクセス許可の管理の概要」を参照してください。

AWS ウェブサイトにアクセスできる IAM ロールを作成する

AWS Identity and Access Management (IAM) は、ユーザーの AWS リソースへのアクセスを安全に制御するのに役立つウェブサービスです。IAM を使用して、 AWS リソースを使用できるユーザー (認証) 、使用できるリソース、および使用方法 (認可) を制御します。

1. IAM マネジメントコンソールに移動し、左側のナビゲーションペインのロールをクリックします。

   ロール管理ページが開き、IAM ロール、ロールの作成オプション、既存のロールのリストに関する情報が表示されます。

2. ロールの作成 をクリックします。

   ロールの作成 信頼されたエンティティのタイプを選択 ページが開きます。別の AWS アカウント をクリックすると、設定領域が下に表示されます。

   AMS から提供された AMS 信頼済みアカウント ID を入力します。
   必要外部 ID と必要 MFA オプションを選択解除したままにします。

3. [Next: Permissions (次の手順: アクセス許可)] をクリックします。

   ロールの作成 アクセス許可ポリシーのアタッチページが開き、新しいポリシーの作成、ページの更新、既存のポリシーの検索のオプションが表示されます。既存のポリシーのリストが表示されます。

4. AdministratorAccess ポリシーを選択し、次へ: 確認 をクリックします。

   ロールの作成レビューページが開きます。

5. 新しいロールに aws_managedservices_onboarding_role という名前を付け、ロールの説明に「AMS オンボーディングロール」と入力します。新しいロールの設定を確認し、問題がなければロールの作成をクリックします。

   ロール管理ページが開き、新しいロールが一覧表示されます。

EPS AWS Marketplace の をサブスクライブする

AMS エンドポイントセキュリティ (EPS) の最近の変更では、 を通じて TrendMicro Deep Security にサブスクライブ AWS Marketplace し、ソフトウェア条件に同意する必要があります。

TrendMicro には、保護されたインスタンス時間ごとと独自のライセンスの使用 (BYOL) の 2 つのライセンスモデルがあります。

- BYOL：
  1. 外部チャネルを通じて購入した独自のライセンスを使用します。
  2. EPS インフラストラクチャを構築するには、すべてのライセンスキーを AMS に提供する必要があります。すべてのモジュールをライセンスするアクティベーションコード、または特定のモジュールのセットをライセンスする個々のアクティベーションコードを指定できます。AMS は、指定したアクティベーションコードに対応するライセンスファイルのみを作成します。ライセンスのアクティベーションはオンボーディング中に行われるため、AMS リードエンジニアと CSDM の存在下で、その情報を共有できます。
  3. さらに、BYOL TrendMicro Market Place AMI サブスクリプションをサブスクライブする必要があります。「Trend Micro Deep Security (BYOL)」を参照してください。
- 保護されたインスタンス時間あたり：
  1. このサブスクリプションでは、以前に購入した Trend ライセンスは必要ありません。
  2. ただし、 Marketplace サブスクリプションをサブスクライブする必要があります。
  3. このモデルでは、ソフトウェアライセンス + EC2 インフラストラクチャの使用状況を含むトレンド使用量が自動的に計測されるため、AMS とのライセンスキー共有は必要ありません。「Trend Micro Deep Security」を参照してください。

Trend Micro にサブスクライブするには、次の手順に従います。

1. にログインします AWS アカウント。
2. Trend Micro Deep Security (BYOL または保護されたインスタンス時間ごと) の製品ページに移動します。
3. 右側のパネルで「サブスクリプションに進む」をクリックします。
4. 右上隅にある Accept Terms をクリックします。

Trend Micro Deep Security で IDS と IPS を有効にする

アカウントのデフォルト以外の機能である Trend Micro Intrusion Detection System (IDS) と Intrusion Protection Systems (IPS) を有効にするように AMS にリクエストできます。

これを行うには、更新リクエスト (管理 | その他 | その他 | 更新) を送信し、IDS および IPS 通知を受信する E メールアドレスのリストを含めます。これらのアドレスは、AMS が作成するアカウントの SNS トピックに追加されます。

> **Note**
>
> AMS は、他の AMS サービスを提供する能力を妨げる可能性のある Trend Micro サービスを追加することはできません。

次のステップ: AMS のルートユーザーの多要素認証 (MFA) を使用して新しいアカウントを保護する

AWS Marketplace for CentOS 7.6 をサブスクライブする

AMS は、CentOS 7 (x86_64) - と Centos.org が販売する更新 HVM を AMS AMI として提供するようになりました。この AMI を使用するには、無料 Cent OS ライセンスにオプトインし、すべての AMS アカウントでライセンスを受け入れる必要があります。

サブスクライブするには、「」に移動AWS Marketplaceし、オプトインの手順に従います。

この製品の使用に対してソフトウェア料金は発生しませんが、EC2 の使用を含むその他の AWS 料金は引き続きお客様の負担となります。これが「Bring Your Own License」製品である場合は、その製品を使用するには有効なソフトウェアライセンスが必要です。

このソフトウェアの情報は、CentOS 7 (x86_64) - with Updates HVM で確認できます。

AMS のルートユーザーの多要素認証 (MFA) を使用して新しいアカウントを保護する

このセクションは、機密性の高い AMS セキュリティ関連情報が含まれているため、編集されています。この情報は、AMS コンソールのドキュメントから入手できます。AWS Artifact にアクセスするには、CSDM に連絡して手順を確認するか、「AWS Artifact の開始方法」を参照してください。

SALZ: ネットワークの設定

AWS Managed Services (AMS) のネットワークをセットアップするには、いくつかのプロセスを完了する必要があります。

1. AMS 環境に IP スペースを割り当てる
2. AWS へのプライベートネットワーク接続を確立する
3. AMS オペレーションを許可するようにファイアウォールを設定する

AMS 環境に IP スペースを割り当てる

AMS は、推奨されるネットワーク割り当てとして /16 CIDR ブロックを使用して設計およびテストされました。AMS に接続された信頼されたネットワークは、AMS に割り当てられた CIDR ブロックと重複しない CIDR ブロックを使用することが重要です。これらのアドレスは、Virtual Private Cloud (VPC) とサブネットをセットアップするために必要です。AWS VPCs「Amazon VPC の制限」と「Amazon VPC に関するFAQs」を参照してください。

/16 CIDR ブロックは多くの IP アドレスのように見える場合がありますが、VPC は一度作成すると拡張できません。したがって、この割り当てにより、AMS マネージド VPC がかなりの期間機能できるようになります。CIDR ブロック内では、少なくとも 2 つのプライベートサブネットと 2 つのパブリックサブネットに IP アドレス範囲を割り当てる必要があります。

AWS は、ネイティブ AWS 仮想プライベートネットワーク (VPN) 機能を介して AMS 環境への接続を受け入れます。これを実現するには、AWS Direct Connect (DX)、ハードウェア VPN、またはソフトウェア VPN を使用します。AMS 側では、VPCs の仮想ゲートウェイ機能を使用します。

基本的な環境コンポーネント

ユーザーNetwork-to-Amazonオプション	
ハードウェア VPN	リモートネットワーク上のネットワーク機器から VPC に接続された AMS 管理のネットワーク機器へのハードウェア VPN 接続を確立します。
AWS Direct Connect (DX)	AWS Direct Connect を活用して、リモートネットワークから Amazon VPC へのプライ

ユーザーNetwork-to-Amazonオプション	
	ベートで論理的な (または VPN で使用する場合は暗号化された) 接続を確立します。
ソフトウェア VPN	リモートネットワーク上の機器から Amazon VPC 内で実行されているユーザー管理のソフトウェア VPN アプライアンスへの VPN 接続を確立します。

> **Note**
>
> AMS では、DX 接続への冗長プライベート VPN を推奨しています。カスタマーサービスデリバリーマネージャー (CSDM) は、アカウントのオンボーディング時にこの設定を支援します。

AWS へのプライベートネットワーク接続を確立する

企業の Active Directory に AMS を追加して、接続を確立します。プライベートネットワーク接続を介して管理アクションを実行したり、ユーザーアクセスを実行したりできます。AWS では、VPN 接続と 経由の専用回線の両方を提供しています Direct Connect。次の手順では、AMS を使用して接続手段のいずれか (または両方) を確立する方法について説明します。

VPN セットアップ

このセクションでは、AMS マネージド VPC と内部ネットワーク間で通信するように VPN を設定する基本的な手順について説明します。

> **Note**
>
> AWS のサービスでの VPN の使用に関する全体的な理解を得るには、「AWS Site-to-Site VPN とは」と「カスタマーゲートウェイ (VPN アプライアンス) について」を参照してください。

AWS VPN ユーザーガイドの開始方法と Site-to-Site VPN 接続のテストセクションに従って、次の手順を完了します。

- ステップ 1: AWS VPC でカスタマーゲートウェイを作成する
- ステップ 2: AWS VPC で仮想プライベートゲートウェイを作成する
- ステップ 3: AWS VPC で、ルートテーブルでルート伝播を有効にする
- ステップ 4: AWS VPC で、セキュリティグループを更新してインバウンド SSH、RDP、ICMP アクセスを有効にする
- ステップ 5: 内部ネットワークで VPN 接続を作成し、カスタマーゲートウェイを設定する
- ステップ 6: VPC と内部ネットワーク間の VPN 接続をテストする

Direct Connect セットアップ

このセクションでは、AMS マネージド VPC と内部ネットワーク間で通信するように Direct Connect (DX) を設定する基本的な手順について説明します。

> **Note**
>
> AWS のサービスで DX を使用する方法については、「Direct Connect ロケーションの開始方法」を参照してください。

DX 接続を設定するには、次のステップを完了する必要があります。

1. Amazon Web Services にサインアップする
2. AWS Direct Connect 接続リクエストを送信する
3. クロスコネクトを完了する
4. (オプション) AWS Direct Connect で冗長接続を設定する
5. AMS によって実行される: 仮想インターフェイスを作成する
6. AMS によって実行: ルーター設定のダウンロード
7. 仮想インターフェイスを検証する

ファイアウォールをセットアップする

このセクションは、機密性の高い AMS セキュリティ関連情報が含まれているため、編集されています。この情報は、AMS コンソールのドキュメントから入手できます。AWS Artifact にアクセスするには、CSDM に連絡して手順を確認するか、「AWS Artifact の開始方法」を参照してください。

アプリケーション移行/オンボーディング中の AMS 踏み台オプション

移行作業中に最高のエクスペリエンスを提供するために、AMS が現在活用できる可能性のあるオプションを以下に示します。

- オプション 1: 移行作業にのみ踏み台をバイパスする (一時的な対策として、セキュリティ上の目的でこれをサインオフする必要があります)。

  注: AMS が各リクエストを可視化できるように、監査機能は引き続き導入されます。
- オプション 2: 図に示すように、PuTTy など、任意のツールを使用した SSH トンネリング。

  このオプションでは、説明されている環境コンポーネントが既に存在している必要があります。

  AMS は追加の注意事項と手順を提供します。

PuTTy を使用した SSH トンネリングステップ :

PuTTY 内では、踏み台ホストのパブリック IP を使用して SSH セッションを作成し、AUTH セクションで PEM キーを指定してから、トンネルを作成します。トンネルの送信元ポートは未使用のローカルポート (5000 など) でなければならず、IP は送信先ホストの IP (到達しようとしている Windows ボックス) で、RDP ポート (3389) が追加されます。ボックスにログインするたびに設定を行う必要がないため、必ず設定を保存してください。踏み台ホストに接続し、ログインします。次に、localhost:5000 (または任意のポート) の RDP セッションを開始します。

1. 踏み台ホストのホスト名またはパブリック IP を設定する

2. SSH ->Auth で、プライベートキーファイルを .ppk 形式で設定します。

3. SSH ->Tunnels で、新しい転送ポートを追加します。送信元ポートは任意の未使用のポートで、送信先は踏み台ホストの背後にある送信先サーバーの IP で、RDP ポートが追加されている必要があります。

4. PuTTY 経由で踏み台ホストに接続し、ログインします。

5. localhost:5000 への RDP セッションを開始して、送信先サーバーに到達します。

SALZ: アクセス管理を設定する

AWS Managed Services (AMS) によって管理されるネットワークを使用すると、クラウドインフラストラクチャを管理するための AMS アクセスが付与されます。プライベートネットワークと AMS を安全に接続する方法を設定する必要があります。これは、提供するアクセスの種類に関するいくつかの決定から始まります。

- AMS API/CLI およびコンソールアクセスの場合: AMS CLI をインストールします (手順については、このドキュメントを参照してください) 。AMS 変更管理 API を使用して AMS への変更リクエストを行い、AMS SKMS API を使用して AMS マネージドリソースについて学習します。Active Directory フェデレーションサービス (AD FS) を使用すると、AMS コンソールにアクセスできます。

  > **Note**
  >
  > 独自の ITSM を設定する場合は、サービスリクエストとインシデントレポートに AWS サポート API (SAPI) を使用する必要があります。SAPI については、AWS 「 サポート API リファレンス」を参照してください。

- ユーザーアクセスの場合: Windows Active Directory (AD) を使用するユーザーを管理する場合でも、Linux/LDAP ソリューションを使用するユーザーを管理する場合でも、AMS 側 (Directory Services 経由) の AD と ディレクトリ間の接続を確立する必要があります。
- インスタンスアクセスの場合: インスタンスレベルのアクセスは、一方向のフォレスト信頼設定を介して行われます。Directory Services は CORP AD の認証情報を信頼し、AMS 側のスタックが CORP 認証情報を使用したログインを許可できるようにします。

  AMS が信頼を設定する Active Directory (AD) は、AWS リソースへのアクセスを許可するユーザーのアカウントを持つディレクトリである必要があります。

> **Important**
>
> フォレストの信頼を設定するには、AMS はドメインコントローラーのローカルポリシー -> セキュリティオプション -> ネットワークアクセス: 匿名でアクセスできる名前付きパイプ、Netlogon パイプと lsarpc パイプを一覧表示する必要があります。これらのパイプはデフォルトで一覧表示されますが、セキュリティ上の懸念のために削除されることがあります。信頼が確立されたら、再度リストから削除できます。

Active Directory (AD) 信頼を確立する

AWS Managed Services (AMS) アカウントの Active Directory (AD) 信頼を確立する前に、適切なファイアウォールポートが開いていることを確認してください。

AMS 管理の Active Directory と社内ディレクトリサービスからの信頼により、企業管理の認証情報を使用して AMS 管理のインスタンスにアクセスし、開発、テスト、または管理機能を実行できます。

信頼接続の作成は 2 つの部分からなる演習です。

まず、DNS クエリがどの DNS サーバーに移動するかを知るように、DNS 設定である条件付き転送を設定します。

次に、信頼を設定します。Active Directory (AD) コンストラクトは、あるドメインのユーザーからのアクセスが別のドメインのリソースを使用できるようにします。

条件付きフォワーダーを設定する

この Microsoft AD の記事「ドメイン名に条件付きフォワーダーを割り当てる」に従い、以下の設定と選択肢を使用します。

1. AD DNS Manager -> DNS ドメインで新しい条件付きフォワーダーを作成する： 指定されたドメイン名 AMS を使用します。例: *A523434123.amazonaws.com*。
2. マスターサーバーの IP アドレスの下： AMS が提供する IP アドレスを追加します。両方のアドレスを検証して、接続の問題がないことを確認します。
3. この条件付きフォワーダーを Active Directory に保存し、次のようにレプリケートします。このドメイン内のすべての DNS サーバーを選択し、OK を押します。

信頼を設定する

AWS Managed Services (AMS) アカウントの信頼を設定するには、この MicroSoft AD の記事「このセクションで説明されている設定と選択肢を使用して、信頼の片側に対して一方向、受信、フォレストの信頼を作成する」に従ってください。

1. Start -> Administrative Tools -> Active Directory Domains and Trusts ダイアログを開きます。信頼を確立するドメインのドメインノードを右クリックし、プロパティ -> Trusts -> New Trust をクリックして New Trust Wizard を開きます。信頼名に AMS から提供されたドメイン名を入力し、次へを押します。

2. Trust Type で、Forest Trust を選択します。[次へ] を選択します。
3. 信頼の方向で、一方向: 受信を選択します。[次へ] を選択します。
4. Sides of Trust で、このドメインのみを選択します。[次へ] を選択します。
5. Trust Password に、選択したパスワードを入力します。[次へ] を選択します。
6. Trust Selections Completed と Trust Creation Complete の場合は、Next を押します。
7. 「受信信頼の確認」で「いいえ」を選択し、受信信頼を確認しません。[次へ] を選択します。
8. 「新しい信頼ウィザードの完了」で、「完了」を選択し、「OK」を選択して閉じます。
9. 信頼パスワードを入力します (セキュリティ上の理由から、CSDM の電話番号からお問い合わせください) 。AMS は信頼設定を完了します。

Active Directory のサイトとサービス

ログインのレイテンシーを減らすには、VPC CIDR 範囲を Active Directory サイトとサービス (開始 -> 管理ツール -> Active Directory サイトとサービス) に追加します。AWS に最も近いドメインコントローラーを含む Active Directory サイトに VPC CIDR 範囲を追加します。

Active Directory 名のサフィックスルーティング

一方向フォレスト信頼が確立されたら、追加のステップを完了してください。

1. 開始 > すべてのプログラム > 管理ツールで、Active Directory ドメインと信頼をクリックします。

   Active Directory ドメインと信頼コンソールが開きます。
2. 企業ドメインを右クリックし、プロパティをクリックします。

   そのドメインのプロパティダイアログが開きます。
3. Trusts タブをクリックします。

   Trusts ページが開きます。
4. Amazon ドメイン名をクリックし、プロパティをクリックします。

   Amazon ドメイン信頼のプロパティページが開きます。
5. Name Suffix Routing をクリックし、Refresh をクリックします。

   これらのステップにより、サービスプリンシパル名 (SPNs) が信頼を解決できるようになります。

トラブルシューティング

問題が発生した場合に試すべきこと：

- AMS 管理の Active Directory アウトバウンドセキュリティグループは、CIDR ブロック (10.27.0.0/16 など) を介してドメインコントローラーに接続できる必要があります。
- AWS コンソールでドメインコントローラーからドメインコントローラーへのルートをトレースし、途中ですべてのセキュリティグループを確認します。
- Internet Control Message Protocol (ICMP) が許可されている場合は、AMS が管理する Active Directory ドメインコントローラーに ping を実行できることを確認してください。
- ドメインコントローラーが AWS Directory Services と通信できることを確認します。
- 条件付きフォワーダーが解決され、検証されていることを確認します。
- 新しい信頼ウィザードでフォレスト信頼が表示されない場合、条件付きフォワーダーが正しく動作していない可能性があります。
  - nslookup を使用して解決をテストする
  - ドメインコントローラーを再起動してみてください

AMS Managed Active Directory

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

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

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

注意:

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

  アクセスは次のようになります。

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

次のようになります。

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

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

   - アカウント情報
     - AMS 管理 AD: AWS アカウント number 用に AWS アカウント 作成された のアカウント ID
     - Managed AD をオンボードするリージョン： AWS リージョン
   - マネージド Active Directory 情報：
     - Microsoft AD Edition: Standard/Enterprise。AWS Microsoft AD (Standard Edition) には、1 GB のディレクトリオブジェクトストレージが含まれています。この容量は、ユーザー、グループ、コンピュータなど、最大 5,000 ユーザーまたは 30,000 ディレクトリオブジェクトをサポートできます。AWS Microsoft AD (Enterprise Edition) には 17 GB のディレクトリオブジェクトストレージが含まれており、最大 100,000 ユーザーまたは 500,000 オブジェクトをサポートできます。

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

- ドメイン FQDN: AMS Managed AD ドメインの FQDN。
- ドメイン NetBIOS 名: AMS Managed AD ドメインの NetBIOS 名。
- Managed AD 統合先の AMS 標準アカウントのアカウント番号 (AMS は AMS 標準アカウントの AD から Managed AD への一方向の信頼を設定します)
- Active Directory スキーマの変更が必要で、必要な場合はどのような変更が必要ですか？
- デフォルトでは、2 つのドメインコントローラーがプロビジョニングされます。さらに が必要ですか？ その場合は、必要な数と理由を教えてください。

- Managed Active Directory 情報のネットワーク：
  - ドメインコントローラーの Managed AD VPC CIDR (Managed AD ドメインコントローラーのプライベートサブネット範囲内の CIDR)。
    - ドメインコントローラーのサブネット CIDR 1: [CIDR、AMS Managed AD VPC CIDR の一部である必要があります〕
    - ドメインコントローラーのサブネット CIDR 2: [CIDR、AMS Managed AD VPC CIDR の一部である必要があります〕

    例:

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

    IP アドレスの競合を回避するには、指定する Managed AD VPC CIDR が、企業ネットワークで使用している他のプライベートサブネット CIDR と競合しないことを確認してください。
  - VPN テクノロジー (オプション): [Direct Connect/Direct Connect と VPN]
    - ゲートウェイの BGP 自律システム番号 (ASN): [お客様が用意した ASN]
    - ゲートウェイの外部インターフェイスのインターネットルーティング可能な IP アドレス。アドレスは静的である必要があります: [お客様提供の IP アドレス〕
    - VPN 接続に静的ルートが必要かどうか: [はい/いいえ〕

2. AMS は AD 環境の管理者アカウントのパスワードを提供し、AMS エンジニアが AD 環境にアクセスできなくなるようにパスワードをリセットするよう要求します。
3. 管理者アカウントのパスワードをリセットするには、Active Directory ユーザーとコンピュータ (ADUC) を使用して Active Directory 環境に接続します。ADUC およびその他のリモートサーバー管理ツール (RSAT) は、AMS 以外のインフラストラクチャでプロビジョニングされた管理ホスト

にインストールして実行する必要があります。Microsoft には、このような管理ホストを保護するためのベストプラクティスがあります。詳細については、「安全な管理ホストの実装」を参照してください。これらの管理ホストを使用して Active Directory 環境を管理します。

4. 日常業務では、AMS は、VPC 設定、AD バックアップ、AD 信頼の作成と削除など、 AWS Directory Service 側 AWS アカウント までの を管理します。AD 環境を使用および管理します。例えば、ユーザーの作成、グループの作成、グループポリシーの作成などです。

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

AMS AWS Identity and Access Management ロールを使用して Active Directory をフェデレーションする

ディレクトリを AMS IAM ロールとフェデレーションする目的は、企業のユーザーが企業の認証情報を使用して AWS マネジメントコンソール と AWS APIs、つまり AMS コンソールと APIs とやり取りできるようにすることです。

フェデレーションプロセスの例

この例では Active Directory フェデレーションサービス (AD AWS Identity and Access Management FS) を使用していますが、フェデレーションをサポートするすべてのテクノロジーがサポートされています。 AWS サポートされている IAM フェデレーションの詳細については、「IAM パートナーと ID プロバイダーとフェデレーション」を参照してください。CSDM は、AD チームや AMS との共同作業を含むこのプロセスを支援します。

API アクセスに SAML を統合する方法の詳細については、この AWS ブログ「How to Implement Federated API and CLI Access Using SAML 2.0 and AD FS」を参照してください。

> **Note**
>
> AMS CLI と SAML をインストールする例については、「」を参照してください付録: ActiveDirectory フェデレーションサービス (ADFS) クレームルールと SAML 設定。

AMS コンソールへのフェデレーションの設定 (SALZ)

次の表に詳述されている IAM ロールと SAML ID プロバイダー (信頼されたエンティティ) は、アカウントのオンボーディングの一部としてプロビジョニングされています。これらのロールを使用すると、RFCs、サービスリクエスト、インシデントレポートを送信およびモニタリングし、VPCsとスタックに関する情報を取得できます。

ロール	ID プロバイダー	アクセス許可
Customer_ReadOnly_Role	SAML	標準 AMS アカウントの場合。RFCs を送信して AMS が管理するインフラストラクチャを変更したり、サービスリクエストやインシデントを作成したりできます。
Customer_managed_ad_user_role	SAML	AMS Managed Active Directory アカウントの場合。AMS コンソールにログインして、サービスリクエストとインシデント (RFCsなし) を作成できます。

異なるアカウントで使用可能なロールの完全なリストについては、「」を参照してくださいAMS の IAM ユーザーロール。

オンボーディングチームのメンバーは、フェデレーションソリューションから事前設定された ID プロバイダーにメタデータファイルをアップロードします。Shibboleth や Active Directory フェデレーションサービスなどの SAML 互換 IdP (ID プロバイダー) 間の信頼を確立し、組織内のユーザーが AWS リソースにアクセスできるようにする場合は、SAML ID プロバイダーを使用します。IAM の SAML ID プロバイダーは、上記のロールを持つ IAM 信頼ポリシーのプリンシパルとして使用されます。

他のフェデレーションソリューションは AWS の統合手順を提供しますが、AMS には個別の手順があります。次のブログ記事「Windows Active Directory、AD FS、SAML 2.0 を使用した AWS へのフェデレーションの有効化」と以下の修正により、企業ユーザーは 1 つのブラウザから複数の AWS アカウントにアクセスできます。

ブログ投稿に従って証明書利用者の信頼を作成したら、次の方法でクレームルールを設定します。

- NameId: ブログ記事に従ってください。
- RoleSessionName: 次の値を使用します。
  - クレームルール名: RoleSessionName
  - 属性ストア: Active Directory
  - LDAP 属性: SAM-Account-Name
  - 送信クレームタイプ: https://aws.amazon.com/SAML/Attributes/RoleSessionName
- AD グループを取得する: ブログ記事に従ってください。
- ロールクレーム: ブログ記事に従いますが、カスタムルールには以下を使用します。

```
c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-([^d]{12})-"]
 => issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value =
 RegExReplace(c.Value, "AWS-([^d]{12})-",
 "arn:aws:iam::$1:saml-provider/customer-readonly-saml,arn:aws:iam::$1:role/"));
```

AD FS を使用する場合は、次の表に示す形式でロールごとに Active Directory セキュリティグループを作成する必要があります (customer_managed_ad_user_role は AMS Managed AD アカウント専用です)。

グループ	ロール
AWS-[AccountNo]-Customer_ReadOnly_Role	Customer_ReadOnly_Role
AWS-[AccountNo]-customer_managed_ad_user_role	Customer_managed_ad_user_role

詳細については、「認証レスポンスの SAML アサーションの設定」を参照してください。

> **Tip**
>
> トラブルシューティングに役立つように、ブラウザの SAML トレーサープラグインをダウンロードします。

AMS へのフェデレーションリクエストの送信

これが最初のアカウントである場合は、CSDM (複数可) または Cloud Architect (複数可) と協力して、ID プロバイダーのメタデータ XML ファイルを提供します。

追加のアカウントまたは ID プロバイダーをオンボーディングしていて、管理アカウントまたは目的のアプリケーションアカウントにアクセスできる場合は、次の手順に従います。

1. AMS コンソールからサービスリクエストを作成し、ID プロバイダーの追加に必要な詳細を指定します。
   - 新しい ID プロバイダーが作成されるアカウントの AccountId。
   - 希望する ID プロバイダー名を指定しない場合、デフォルトは customer-saml になります。通常、これはフェデレーションプロバイダーで設定された設定と一致する必要があります。
   - 既存のアカウントの場合、新しい ID プロバイダーを既存のすべてのコンソールロールに伝達するか、新しい ID プロバイダーを信頼するロールのリストを提供するかを含めます。
   - フェデレーションエージェントからサービスリクエストにエクスポートされたメタデータ XML ファイルをファイルアタッチメントとしてアタッチします。
2. サービスリクエストを作成したのと同じアカウントから、以下の情報を含む CT-ID ct-1e1xtak34nx76 (管理 | その他 | その他 | 作成) を使用して新しい RFC を作成します。
   - タイトル：「Onboard SAML IDP <Name> for Account <AccountId>」。
   - ID プロバイダーが作成されるアカウントの AccountId。
   - ID プロバイダー名。
   - 既存のアカウントの場合: ID プロバイダーを既存のすべてのコンソールロールに伝達するか、新しい ID プロバイダーを信頼するロールのリストに伝達するか。
   - メタデータ XML ファイルがアタッチされているステップ 1 で作成されたサービスリクエストのケース ID。

コンソールアクセスの確認

ADFS をセットアップし、認証に使用する AMS URL を取得したら、以下の手順に従います。

Active Directory フェデレーティッドサービス (ADFS) 設定では、以下のステップを実行できます。

1. ブラウザウィンドウを開き、アカウントのサインインページに移動します。アカウントの ADFS IdpInitiatedSignOn ページが開きます。

2. 次のいずれかのサイトにサインインの横にあるラジオボタンを選択します。サインインサイトのピックリストがアクティブになります。
3. signin.aws.amazon.com サイトを選択し、サインインをクリックします。認証情報を入力するためのオプションを開きます。
4. CORP 認証情報を入力し、サインインをクリックします。 AWS マネジメントコンソール が開きます。
5. AMS コンソールの URL をロケーションバーに貼り付け、Enter キーを押します。AMS コンソールが開きます。

API アクセスの検証

AMS は AWS API を使用します。AMS 固有のオペレーションについては、「AMS API リファレンス」を参照してください。

AWS には、Tools SDKs がいくつか用意されています。SDK を使用しない場合は、直接 API コールを実行できます。認証の詳細については、「AWS API リクエストの署名」を参照してください。SDK を使用していない場合、または直接 HTTP API リクエストを行う場合は、変更管理 (CM) および SKMS に AMS CLIs を使用できます。

AMS CLIs のインストール

SAML で使用する AWS Managed Services (AMS) CLI をインストールする例については、「」を参照してください付録: ActiveDirectory フェデレーションサービス (ADFS) クレームルールと SAML 設定。

一時的なアクセスが必要な場合は、AWS Managed Services (AMS) SDKs「一時的な AMS コンソールアクセス」を参照してください。

> **Note**
>
> この手順には管理者認証情報が必要です。

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

1. AWS CLI をインストールするには、「AWS コマンドラインインターフェイスのインストール」を参照して、適切な手順に従ってください。このページの下部には、さまざまなインストー

ラー、Linux、MS Windows、macOS、仮想環境、バンドルインストーラー (Linux、macOS、または Unix) を使用する手順があることに注意してください。

インストール後、 `aws help`を実行してインストールを確認します。

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

   次のいずれかを開きます。

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

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

   - 32 ビット: ManagedCloudAPI_x86.msi
   - 64 ビット: ManagedCloudAPI_x64.msi

   Mac/Linux の場合は、次のコマンドを実行して AWSManagedServices_InstallCLI.sh という名前のファイルを実行します。 `sh AWSManagedServices_InstallCLI.sh`amscm および amsskms ディレクトリとその内容は、AWSManagedServices_InstallCLI.sh ファイルと同じディレクトリにある必要があります。
4. 企業の認証情報を AWS とのフェデレーション (AMS デフォルト設定) で使用する場合は、フェデレーションサービスにアクセスできる認証情報管理ツールをインストールする必要があります。例えば、この AWS セキュリティブログ How to Implement Federated API and CLI Access Using SAML 2.0 and AD FS を使用して、認証情報管理ツールの設定に役立てることができます。
5. インストール後、 `aws amscm help`と `aws amsskms help` を実行してコマンドとオプションを表示します。

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

VPC レベルでの AMS バックアップのスケジュール

ターゲットインスタンスが割り当てられている VPC 内の AWS Managed Services (AMS) バックアップスケジューリングは、VPC 作成スキーマのデフォルトタグを使用してアカウントのオンボーディング中に作成されます。バックアップシステムは、その VPC タグに応じてスナップショットの実行をスケジュールします。スケジュールを変更するには、サービスリクエストを作成します。詳細については、「VPC タグとデフォルト」を参照してください。

バックアップのデフォルトについては、「AMS のデフォルトについて」を参照してください。

SALZ: デフォルト設定

AWS Managed Services (AMS) ネットワークは、ほとんどのサービスのデフォルトを使用して標準化された方法で設定されています。

このセクションでは、AMS がセキュリティ、アクセス、モニタリング、ログ記録、継続性、パッチ適用、管理に使用するデフォルト設定について説明します。

インフラストラクチャコストの例については、「基本コンポーネント」を参照してください。

ファイアウォールルールは で提供されます。 ファイアウォールをセットアップする

エンドポイントセキュリティ (EPS)

AMS Advanced 環境でプロビジョニングするリソースには、エンドポイントセキュリティ (EPS) モニタリングクライアントのインストールが自動的に含まれます。このプロセスにより、AMS

Advanced マネージドリソースが 24 時間 365 日モニタリングされ、サポートされます。さらに、AMS Advanced はすべてのエージェントアクティビティをモニタリングし、セキュリティイベントが検出されるとインシデントが作成されます。

> **Note**
>
> セキュリティインシデントはインシデントとして処理されます。詳細については、「インシデント対応」を参照してください。

エンドポイントセキュリティはマルウェア対策保護を提供します。具体的には、以下のアクションがサポートされています。

- EC2 インスタンスが EPS に登録される
- EC2 インスタンスが EPS から登録解除する
- EC2 インスタンスのマルウェア対策のリアルタイム保護
- EPS エージェントが開始したハートビート
- 隔離されたファイルの EPS 復元
- EPS イベント通知
- EPS レポート

AMS Advanced は、エンドポイントセキュリティ (EPS) に Trend Micro を使用します。これらはデフォルトの EPS 設定です。Trend Micro の詳細については、Trend Micro Deep Security ヘルプセンターを参照してください。Amazon 以外のリンクは予告なしに変更される可能性があります。

AMS Advanced マルチアカウントランディングゾーン (MALZ) のデフォルト設定については、以下のセクションで説明します。デフォルト以外の AMS マルチアカウントランディングゾーン EPS 設定については、「AMS Advanced マルチアカウントランディングゾーン EPS のデフォルト以外の設定」を参照してください。

> **Note**
>
> 独自の EPS を持ち込むことができます。「AMS bring your own EPS」を参照してください。

一般的な EPS 設定

エンドポイントセキュリティの一般的なネットワーク設定。

EPS のデフォルト

設定	デフォルト
ファイアウォールポート (インスタンスのセキュリティグループ)	EPS Deep Security Manager エージェント (DSMs) では、エージェント/リレーからマネージャーへの通信用にポート 4120 を、マネージャーコンソール用にポート 4119 を開く必要があります。EPS リレーでは、マネージャー/エージェントが通信を中継するためにポート 4122 が開いている必要があります。エージェントがすべてのリクエストを開始するため、カスタマーインスタンスのインバウンド通信に特定のポートを開くことはできません。
通信方向	エージェント/アプライアンスが開始されました
ハートビート間隔	10 分
アラートまでに見逃されたハートビートの数	2
サーバー時間間の最大許容ドリフト (差分)	無制限
非アクティブ (登録済みだがオンラインではない) 仮想マシンのオフラインエラーを発生させる	なし
デフォルトポリシー	基本ポリシー (次に説明)
同じホスト名の複数のコンピュータのアクティベーション	許可されます
保留中の更新のアラートが生成されます	7 日後
スケジュールの更新	AMS は、Trend Micro Deep Security Manager (DSM) / Deep Security Agent (DSA) ソフトウェ

設定	デフォルト
	ア更新の毎月のリリースサイクルを対象としています。ただし、AMS は更新の SLA を維持しません。更新は、デプロイ中に AMS 開発者チームによってフリート全体で実行されます。 DSA/DSA 更新は、AMS がデフォルトで 13 週間ローカルに保持する Trend Micro DSM システムイベントに記録されます。ベンダーのドキュメントについては、Trend Micro Deep Security ヘルプセンターの「システムイベント」を参照してください。ログは、Amazon CloudWatch のロググループ /aws/ams/eps/var/log/DSM.log にもエクスポートされます。
ソースの更新	Trend Micro Update Server (https://ipv6-iaus.trendmicro.com/iau_server.dll/)
イベントまたはログデータの削除	イベントとログは、7 日後に DSM データベースから削除されます。
エージェントソフトウェアバージョンが保持されている	最大 5 つ
最新のルール更新が保持されます	最大 10 個
ログストレージ	デフォルトでは、ログファイルは Amazon S3 に安全に保存されますが、監査およびコンプライアンス要件を満たすために Amazon Glacier にアーカイブすることもできます。

基本ポリシー

エンドポイントセキュリティの基本ポリシーのデフォルト設定。

EPS ベースポリシー

設定	デフォルト
有効なモジュール	マルウェア対策
無効なモジュール	ウェブ評価
	ファイアウォール
	侵入保護
	整合性モニタリング
	ログ検査
	アプリケーションコントロール

マルウェア対策

エンドポイントセキュリティのマルウェア対策設定。

EPS マルウェア対策のデフォルト

設定	デフォルト	注意
リアルタイムスキャン	すべてをスキャンする	疑わしいウイルスをすべて隔離します。IntelliTrap と Spyware/grayware Protection を有効にします。 スパイウェアとグレーウェアはアンチマルウェアをトリガーし、項目を隔離します。
	毎日/毎日 (24 時間)	

設定	デフォルト	注意
手動スキャン	すべてをスキャンする	リクエストする必要があり、デフォルトのリアルタイムスキャン設定に従います。
スケジュールされたスキャン	すべてをスキャンする	毎月最終日曜日の午前 6 時に を設定します。
スマート保護	無効	該当なし
隔離されたファイル	Trend Micro Deep Security Manager (DSM)	隔離用に予約された約 1GB のディスク。
スキャンの制限	Trend Micro DSM	すべてのサイズのファイルをスキャンします。
許可されたスパイウェアまたはグレーウェア	なし	該当なし
ローカルイベント通知	あり	該当なし

セキュリティグループ

AWS VPCs では、AWS セキュリティグループは仮想ファイアウォールとして機能し、1 つ以上のスタック (インスタンスまたは一連のインスタンス) のトラフィックを制御します。スタックを起動すると、スタックは 1 つ以上のセキュリティグループに関連付けられ、スタックに到達できるトラフィックが決まります。

- パブリックサブネット内のスタックの場合、デフォルトのセキュリティグループはすべての場所 (インターネット) からの HTTP (80) および HTTPS (443) からのトラフィックを受け入れます。スタックは、企業ネットワークからの内部 SSH および RDP トラフィック、および AWS 踏み台も受け入れます。これらのスタックは、任意のポートを介してインターネットに出力できます。ま

た、プライベートサブネットやパブリックサブネット内の他のスタックに出力することもできます。

- プライベートサブネット内のスタックは、プライベートサブネット内の他のスタックに出力でき、スタック内のインスタンスは、任意のプロトコルを介して相互に完全に通信できます。

> **Important**
>
> プライベートサブネット上のスタックのデフォルトのセキュリティグループでは、プライベートサブネット内のすべてのスタックが、そのプライベートサブネット内の他のスタックと通信できます。プライベートサブネット内のスタック間の通信を制限する場合は、制限を記述する新しいセキュリティグループを作成する必要があります。たとえば、そのプライベートサブネット内のスタックが特定のポート経由で特定のアプリケーションサーバーからのみ通信できるようにデータベースサーバーへの通信を制限する場合は、特別なセキュリティグループをリクエストします。これを行う方法については、このセクションで説明します。

デフォルトのセキュリティグループ

MALZ

次の表は、スタックのデフォルトのインバウンドセキュリティグループ (SG) 設定を示しています。SG はSentinelDefaultSecurityGroupPrivateOnly-vpc-ID」という名前で、*ID* は AMS マルチアカウントランディングゾーンアカウントの VPC ID です。すべてのトラフィックは、このセキュリティグループ経由でmc-initial-garden-SentinelDefaultSecurityGroupPrivateOnly」へのアウトバウンドが許可されます (スタックサブネット内のすべてのローカルトラフィックが許可されます) 。

すべてのトラフィックは、2 番目のセキュリティグループ SentinelDefaultSecurityGroupPrivateOnly」によって 0.0.0.0/0 へのアウトバウンドが許可されます。

> **Tip**
>
> EC2 create、OpenSearch create domain などの AMS 変更タイプのセキュリティグループを選択する場合は、ここで説明するデフォルトのセキュリティグループのいずれか、ま

たは作成したセキュリティグループを使用します。VPC あたりのセキュリティグループのリストは、AWS EC2 コンソールまたは VPC コンソールで確認できます。

内部 AMS 目的で使用される追加のデフォルトのセキュリティグループがあります。

AMS デフォルトセキュリティグループ (インバウンドトラフィック)

タイプ	プロトコル	ポート範囲	ソース
すべてのトラフィック	すべて	すべて	SentinelDefaultSecurityGroupPrivateOnly (同じセキュリティグループのメンバーへのアウトバウンドトラフィックを制限)
すべてのトラフィック	すべて	すべて	SentinelDefaultSecurityGroupPrivateOnlyEgressAll (アウトバウンドトラフィックを制限しません)
HTTP、HS、SSH、	TCP	80 / 443 (ソース 0.0.0.0/0) 踏み台からの SSH および RDP アクセスが許可されている	SentinelDefaultSecurityGroupPublic (アウトバウンドトラフィックを制限しません)
MALZ 踏み台：			
SSH	TCP	22	SharedServices VPC CIDR と DMZ VPC CIDR、およびお客様が用意したオンプレミス CIDRs
SSH	TCP	22	
RDP	TCP	3389	
RDP	TCP	3389	
SALZ 踏み台：			

タイプ	プロトコル	ポート範囲	ソース
SSH	TCP	22	mc-initial-garden-LinuxBastionSG
SSH	TCP	22	mc-initial-garden-LinuxBastionDMZSG
RDP	TCP	3389	mc-initial-garden-WindowsBastionSG
RDP	TCP	3389	mc-initial-garden-WindowsBastionDMZSG

SALZ

次の表は、スタックのデフォルトのインバウンドセキュリティグループ (SG) 設定を示しています。SG の名前はmc-initial-garden-SentinelDefaultSecurityGroupPrivateOnly-*ID*」で、*ID* は一意の識別子です。すべてのトラフィックは、このセキュリティグループ経由でmc-initial-garden-SentinelDefaultSecurityGroupPrivateOnly」へのアウトバウンドが許可されます (スタックサブネット内のすべてのローカルトラフィックが許可されます) 。

すべてのトラフィックは、2 番目のセキュリティグループmc-initial-garden-SentinelDefaultSecurityGroupPrivateOnlyEgressAll-0 へのアウトバウンドが許可されます。

> **Tip**
>
> EC2 create、OpenSearch create domain などの AMS 変更タイプのセキュリティグループを選択する場合は、ここで説明するデフォルトのセキュリティグループのいずれか、または作成したセキュリティグループを使用します。VPC あたりのセキュリティグループのリストは、AWS EC2 コンソールまたは VPC コンソールで確認できます。

内部 AMS 目的で使用される追加のデフォルトのセキュリティグループがあります。

AMS デフォルトセキュリティグループ (インバウンドトラフィック)

タイプ	プロトコル	ポート範囲	ソース
すべてのトラフィック	すべて	すべて	SentinelDefaultSecurityGroupPrivateOnly (同じセキュリティグループのメンバーへのアウトバウンドトラフィックを制限)
すべてのトラフィック	すべて	すべて	SentinelDefaultSecurityGroupPrivateOnlyEgressAll (アウトバウンドトラフィックを制限しません)
HTTP、HS、SSH、	TCP	80 / 443 (ソース 0.0.0.0/0) 踏み台からの SSH および RDP アクセスが許可されている	SentinelDefaultSecurityGroupPublic (アウトバウンドトラフィックを制限しません)
MALZ 踏み台：			
SSH	TCP	22	SharedServices VPC CIDR と DMZ VPC CIDR、およびお客様が用意したオンプレミス CIDRs
SSH	TCP	22	
RDP	TCP	3389	
RDP	TCP	3389	
SALZ 踏み台：			
SSH	TCP	22	mc-initial-garden-LinuxBastionSG
SSH	TCP	22	mc-initial-garden-LinuxBastionDMZSG
RDP	TCP	3389	mc-initial-garden-WindowsBastionSG

タイプ	プロトコル	ポート範囲	ソース
RDP	TCP	3389	mc-initial-garden-WindowsBastionDMZSG

セキュリティグループの作成、変更、または削除

カスタムセキュリティグループをリクエストできます。デフォルトのセキュリティグループがアプリケーションまたは組織のニーズを満たさない場合は、新しいセキュリティグループを変更または作成できます。このようなリクエストは承認が必要と見なされ、AMS オペレーションチームによってレビューされます。

スタックと VPCs の外部でセキュリティグループを作成するには、`Deployment | Advanced stack components | Security group | Create (review required)`変更タイプ (ct-1oxx2g2d7hc90) を使用して RFC を送信します。

Active Directory (AD) セキュリティグループの変更には、次の変更タイプを使用します。

- ユーザーを追加するには: 管理を使用して RFC を送信する | Directory Service | ユーザーとグループ | ユーザーをグループに追加する [ct-24pi85mjtza8k]
- ユーザーを削除するには: Management | Directory Service | Users and groups | Remove user from group [ct-2019s9y3nfml4] を使用して RFC を送信します。

> **Note**
>
> 「レビュー必須」CT を使用する場合、AMS では ASAP スケジューリングオプション (コンソールで ASAP を選択し、API/CLI で開始時刻と終了時刻を空白のままにしておく) を使用することをお勧めします。これらの CTs では、AMS オペレーターが RFC を調べる必要があり、承認して実行する前にお客様と通信する必要があるためです。これらの RFCsスケジュールする場合は、少なくとも 24 時間かかります。スケジュールされた開始時刻より前に承認が行われない場合、RFC は自動的に拒否されます。

セキュリティグループの検索

スタックまたはインスタンスにアタッチされているセキュリティグループを検索するには、EC2 コンソールを使用します。スタックまたはインスタンスを見つけたら、そのスタックまたはインスタンスにアタッチされているすべてのセキュリティグループを確認できます。

コマンドラインでセキュリティグループを検索し、出力をフィルタリングする方法については、「」を参照してくださいdescribe-security-groups。

EC2 IAM インスタンスプロファイル

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

MALZ

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

ポリシーの説明

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

プロファイル	ポリシー
customer-mc-ec2-instance-profile-s3	AMSInstanceProfileBYOEPSPolicy : Ec2 インスタンスが AMS Bring Your Own EPS を使用できるようにします。
	AMSInstanceProfileLoggingPolicy : Ec2 インスタンスが S3 と CloudWatch にログをプッシュできるようにします。
	AMSInstanceProfileManagementPolicy : Ec2 インスタンスが Active Directory の結合などの起動アクションを実行できるようにします。
	AMSInstanceProfileMonitoringPolicy : Ec2 インスタンスが AMS モニタリングサービスに結果をレポートできるようにします。
	AMSInstanceProfilePatchPolicy : Ec2 インスタンスがパッチを受信できるようにします。
	AMSInstanceProfileS3WritePolicy : Ec2 インスタンスがお客様の S3 バケットを読み書きできるようにします。

SALZ

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

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

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

EC2 のデフォルトの IAM インスタンスプロファイルのアクセス許可

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

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

CW = CloudWatch。ARN = Amazon リソースネーム。* = ワイルドカード (任意) 。			
ポリシーステートメント	効果	アクション	説明とリソース (ARN)
S3 での SSM アクセス	許可	GetObject、 PutObject、 AbortMultipartUpload、 ListMultipartUploadPorts、 ListBucketMultipartUploads	EC2 の SSM が、 でオブジェクトを取得および更新し、 でマルチパートオブジェクトのアップロードを中止して、マルチパートアップロードに使用できるポートとバケットを一覧表示できるようにしますaws:s3:::mc-*-internal-*/aws/ssm* 。
Amazon EC2 Simple Storage Service (S3)			
S3 でオブジェクトを取得する	許可	Get リスト	EC2 アプリケーションがアカウントの S3 バケット内のオブジェクトを取得して一覧表示できるようにします。
お客様が暗号化したログ S3 アクセス	許可	PutObject	EC2 アプリケーションが でオブジェクトを更新することを許可する aws:s3:::mc-*-logs-*/encrypted/app/*
パッチデータプットオブジェクト S3	許可	PutObject	EC2 アプリケーションが でパッチ適用データを S3 バケットにアップロードできるようにします aws:s3:::awsms-a*-patch-data-*

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

CW = CloudWatch。ARN = Amazon リソースネーム。* = ワイルドカード (任意) 。			
ポリシーステートメント	効果	アクション	説明とリソース (ARN)
明示的に拒否リストバケット S3	拒否	ListBucket	暗号化、監査ログ、またはリザーブド (mc) オブジェクトの一覧表示を禁止します。 `aws:s3:::mc-*-logs-*`
AWS Secrets Manager Amazon EC2 の			
Trend Cloud One Secrets アクセス	許可	GetSecretValue	Amazon EC2 が Trend Cloud One 移行のシークレットにアクセスできるようにします。 `aws:secretsmanager:*:*:secret:/ams/eps/cloud-one-agent-tenant-id*` , `arn:aws:secretsmanager:*:*:secret:/ams/eps/cloud-one-agent-activation-token*` , `aws:secretsmanager:*:*:secret:/ams/eps/cloud-one-agent-tenant-id*` , `aws:secretsmanager:*:*:secret:/ams/eps/cloud-one-agent-tenant-guid*`
AWS Key Management Service Amazon EC2 の			

CW = CloudWatch。ARN = Amazon リソースネーム。* = ワイルドカード (任意) 。			
ポリシーステートメント	効果	アクション	説明とリソース (ARN)
Trend Cloud One 復号キー	許可	Decrypt	Amazon EC2 がエイリアス名 / ams/eps/cloudone-migration で AWS KMS キーを復号できるようにする `arn:aws:kms:*:*:alias/ams/eps/cloudone-migration`

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

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

モニタリングされたメトリクスのデフォルト

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。変更管理変更リクエスト (RFC) を使用してデフォルトを変更できます。

> **Note**
>
> CloudWatch は、2016 年 11 月 1 日にメトリクスの保持期間の延長を開始しました。詳細については、CloudWatch の制限」を参照してください。

ベースラインモニタリングからのアラート

サービス	セキュリティアラート	アラート名とトリガー条件	注意
スター付き (*) アラートの場合、AMS は影響を事前に評価し、可能な場合は修復します。修復が不可能な場合は、AMS がインシデントを作成します。自動化によって問題が修正されない場合、AMS はインシデントケースを通知し、AMS エンジニアが対応します。さらに、これらのアラートは E メールに直接送信できます (Direct-Customer-Alerts SNS トピックにオプトインしている場合)。			
Application Load Balancer (ALB) インスタンス	なし	RejectedConnectionCount sum > 0 for 1 min, 5 consecutive times。	CloudWatch アラームは、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を示します。
Application Load Balancer (ALB) ターゲット	なし	TargetConnectionErrorCount sum > 0 for 1 min, 5 consecutive times。	ロードバランサーと登録されたインスタンス間の接続数が正常に確立されなかった場合の CloudWatch アラーム。
Amazon EC2 インスタンス – Windows	なし	SecureChannelFailure 過去 15 個のデータポイントのうち 10 個が > 0.0。	Windows インスタンスの CloudWatch アラームは、チャネル接続の保護が失敗したときに警告します。
Aurora インスタンス	なし	CPUUtilization > 5 分間 85%、2 回連続。	CloudWatch アラーム。

サービス	セキュリティアラート	アラート名とトリガー条件	注意
AWS Backup	あり	DeleteRecoveryPoint 予期しない IAM ロールプリンシパルまたは IAM ユーザープリンシパルが AWS Backup 復旧ポイントを削除しました。	CloudWatch イベント。バックアップ復旧ポイントが削除されたときに発行されます。
AWS Outposts	あり	AMSOutpostsInstanceFamilyCapacityAvailability InstanceFamilyCapacityAvailability = 5 分間 80%、連続 12 回。	リソースのインスタンスファミリー容量の可用性に関する CloudWatch AWS Outposts アラーム。
		AMSOutpostsInstanceTypeCapacityAvailability TypeCapacityAvailability = 5 分間 80%、連続 12 回。	リソースのインスタンスタイプのキャパシティーの可用性に関する CloudWatch AWS Outposts アラーム。
		AMSOutpostsConnectedStatusConnectedStatus < 1 を 5 分間、1 回連続。	AWS Outposts サービスリンク接続の CloudWatch アラーム。1 カウント未満で障害が発生します。
		AMSOutpostsCapacityExceptionCapacityExceptions 0 は 5 分間、1 回連続。	AWS Outpostsリソースのインスタンス起動の容量不足エラーに関する CloudWatch アラーム .

サービス	セキュリティアラート	アラート名とトリガー条件	注意
EC2 インスタンス - すべての OSs	なし	CPUUtilization* >= 5 分間 95%、連続 6 回。	CloudWatch アラーム。CPU 使用率が高いことは、デッドロック、無限ループ、悪意のある攻撃、その他の異常など、アプリケーションの状態の変化を示す指標です。
		StatusCheckFailed > 0 を 5 分間、連続 3 回。	CloudWatch アラーム。
		ルートボリュームの使用状況 >= 5 分間 95%、連続 6 回。	
		非ルートボリュームの使用 > 5 分間 85%、2 回連続。 デフォルトでは無効になっています。詳細については、「」を参照してくださいhttps://docs.aws.amazon.com/managedservices/latest/ctref/management-monitoring-cloudwatch-enable-non-root-volumes-monitoring.html#management-monitoring-cloudwatch-enable-non-root-volumes-monitoring-info。	

サービス	セキュリティアラート	アラート名とトリガー条件	注意
		メモリ無料* MemoryFree < 5%、5 分間、6 回連続。	
	あり	EPS マルウェア インスタンスでマルウェアが見つかりました。	CloudWatch イベント。
Amazon EC2 インスタンス - Linux	なし	ルートボリューム Inode の使用 平均 >= 5 分間 95%、連続 6 回。	CloudWatch アラーム。Linux インスタンスにのみ適用されます。
		スワップ無料* メモリスワップ < 5% を 5 分間、連続 6 回。	
ElastiCache クラスター	なし	CurrConnections = 65000	このアラームは、ElastiCache ホストの最大接続制限を AMS に通知します。 CloudWatch アラーム。このしきい値を更新する場合は、AMS サポートにお問い合わせください。

サービス	セキュリティアラート	アラート名とトリガー条件	注意
ElastiCache ノード	なし	CPUUtilization Average > 15 分間の事前定義された値、2 回連続。	CloudWatch アラーム。デフォルトは 90 です。Redis の場合は、インスタンスタイプに基づいて次のいずれかの値を使用します。 • cache.t1.micro: 90% • cache.m1.small: 90% • cache.m1.medium: 90% • cache.m1.large: 45% • cache.m1.xlarge: 22.5% • cache.m2.xlarge: 45% • cache.m2.4xlarge: 11.25% • cache.c1.xlarge: 11.25% • cache.t2.micro: 90% • cache.t2.small: 90% • cache.t2.medium: 45% • cache.m3.medium: 90% • cache.m3.large: 45% • cache.m3.xlarge: 22.5% • cache.m3.2xlarge: 11.25% • cache.r3.large: 45% • cache.r3.xlarge: 22.5% • cache.r3.2xlarge: 11.25% • cache.r3.4xlarge: 5.625%

サービス	セキュリティアラート	アラート名とトリガー条件	注意
			• cache.r3.8xlarge: 2.8125%
ElastiCache ノード - memcached	なし	SwapUsage 最大 > 50,000,000 バイト、5 分間、5 回連続。	CloudWatch アラーム。memcached にのみ適用されます。
OpenSearch クラスター	なし	ClusterStatus.red maximum は >= 1 で 1 分間、連続 1 回です。 AMS は、このアラートがトリガーされたときに、運用への影響を軽減するために積極的なアクションを実行します。	CloudWatch アラーム。少なくとも 1 つのプライマリシャードとそのレプリカがノードに割り当てられていません。詳細については、「Red Cluster Status」を参照してください。
OpenSearch ドメイン	なし	KMSKeyError >= 1 を 1 分間、連続 1 回。	CloudWatch アラーム。ドメインに保存されているデータを暗号化する KMS 暗号化キーが無効になっています。通常のオペレーションを復元するために、再度有効にしてください。詳細については、OpenSearch Service 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	セキュリティアラート	アラート名とトリガー条件	注意
		ClusterStatus.yellow 最大は >= 1 で 1 分間、連続 1 回 AMS は、このアラートがトリガーされたときに、運用への影響を軽減するために積極的なアクションを実行します。	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。
		FreeStorageSpace 最小は <= 20480 で 1 分間、連続 1 回 AMS は、このアラートがトリガーされたときに、運用への影響を軽減するために積極的なアクションを実行します。	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スペースがない」を参照してください。
		ClusterIndexWritesBlocked >= 1 を 5 分間、1 回連続 AMS は、このアラートがトリガーされたときに、運用への影響を軽減するために積極的なアクションを実行します。	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	セキュリティアラート	アラート名とトリガー条件	注意
		ノード 最小は < x で 1 日間、連続 1 回 AMS は、このアラートがトリガーされたときに、運用への影響を軽減するために積極的なアクションを実行します。	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。
		CPUUtilization 平均は 15 分間で >= 80%、連続 3 回 AMS は、このアラートがトリガーされたときに、運用への影響を軽減するために積極的なアクションを実行します。	100% の CPU 使用率が一般的ですが、持続的な高い平均は問題です。より大規模なインスタンスタイプを使用するか、インスタンスを追加することを検討してください。

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

サービス	セキュリティアラート	アラート名とトリガー条件	注意
		MasterJVMMemoryPressure 最大は >= 80% で 15 分間、1 回連続 AMS は、このアラートがトリガーされたときに、運用への影響を軽減するために積極的なアクションを実行します。	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ブルー/グリーンデプロイにおける役割により、専用マスターノードの平均 CPU 使用率はデータノードよりも低くなります。
OpenSearch インスタンス	なし	AutomatedSnapshotFailure maximum は >= 1 で 1 分間、連続 1 回です。	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。「赤クラスターのステータス」を参照してください。
Elastic Load Balancing インスタンス	なし	SurgeQueueLength > 100 を 1 分間、連続 15 回。	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。
		HTTPCode_ELB_5XX_Count sum > 0 for 5 min, 3 consecutive times。	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。

サービス	セキュリティアラート	アラート名とトリガー条件	注意
		SpilloverCount > 1 を 1 分間、連続 15 回。	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。
GuardDuty サービス	あり	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。 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は、GuardDuty アクティブ検出結果タイプにあります。
ヘルス	可変	AWS Health Dashboard	AMS でサポートされているベースラインサービスに関連して AWS Health Dashboard（ AWS Health) イベントのステータスが変更されると、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。
AWS Managed Microsoft AD	なし	Active Directory のステータス AWS Managed Microsoft AD インスタンスはアクティブなステータスイベントを送信します。	サービスイベント。イベント後にディレクトリが正常に動作している場合に出力されます。

サービス	セキュリティアラート	アラート名とトリガー条件	注意
		ディレクトリの障害ステータス AWS Managed Microsoft AD インスタンスは障害が発生したディレクトリステータスイベントを送信します。	サービスイベント。ディレクトリがパフォーマンス低下状態で実行されている場合に出力されます。1 つまたは複数の問題が検出され、すべてのディレクトリのオペレーションが最適に動作しているとは限りません。
		操作できないディレクトリのステータス AWS Managed Microsoft AD インスタンスは、動作不能なステータスイベントを送信します。	サービスイベント。ディレクトリが機能していない場合に発行されます。すべてのディレクトリエンドポイントが問題を報告しています。
		ディレクトリステータスの削除 AWS Managed Microsoft AD インスタンスは、ディレクトリステータスの削除イベントを送信します。	サービスイベント。ディレクトリが現在削除されているときに発行されます。
		失敗したディレクトリのステータス AWS Managed Microsoft AD インスタンスは失敗したステータスイベントを送信します。	サービスイベント。ディレクトリを作成できなかったときに出力されます。

サービス	セキュリティアラート	アラート名とトリガー条件	注意
		RestoreFailed ディレクトリのステータス AWS Managed Microsoft AD インスタンスは、復元に失敗したディレクトリステータスイベントを送信します。	サービスイベント。スナップショットからディレクトリを復元できませんでした。
Amazon RDS インスタンス	なし	DB インスタンスに割り当てられたストレージが使い果たされると、低ストレージアラートがトリガーされます。	RDS-EVENT-0007 の詳細については、「Amazon RDS イベント通知の使用」を参照してください。
		DB インスタンスが失敗する DB インスタンスは、互換性のない設定または基本的なストレージの問題により失敗しました。DB インスタンスのポイントインタイムの復元をスタートします。	サービスイベント。RDS-EVENT-0031、Amazon RDS イベントカテゴリとイベントメッセージ。
		フェイルオーバーが試行されない Amazon RDS はリクエストされたフェイルオーバーを実行できません。これは、DB インスタンスでフェイルオーバーが最近発生したためです。	サービスイベント。RDS-EVENT-0034、Amazon RDS イベントカテゴリとイベントメッセージ。

サービス	セキュリティアラート	アラート名とトリガー条件	注意
		DB インスタンスの無効なパラメータ 例えば、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、お客様のアクションはメモリパラメータを変更して DB インスタンスを再起動することです。	サービスイベント。RDS-EVENT-0035、Amazon RDS イベントカテゴリとイベントメッセージ。
		無効なサブネット IDsインスタンス 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、Amazon RDS イベントカテゴリとイベントメッセージ。
		DB インスタンスのリードレプリカエラー 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。	サービスイベント。RDS-EVENT-0045、Amazon RDS イベントカテゴリとイベントメッセージ。

サービス	セキュリティアラート	アラート名とトリガー条件	注意
		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 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、Amazon RDS イベントカテゴリとイベントメッセージ。
		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 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、Amazon RDS イベントカテゴリとイベントメッセージ。
		DB インスタンス復旧の開始 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、Amazon RDS イベントカテゴリとイベントメッセージ。

サービス	セキュリティアラート	アラート名とトリガー条件	注意
		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。
		無効なアクセス許可復旧 S3 バケット 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、Amazon RDS イベントカテゴリとイベントメッセージ。
		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。
		DB インスタンスが割り当てられたストレージの 90% 以上を消費した場合の低ストレージアラート	RDS-EVENT-0089 の詳細については、「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。
		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。	RDS-EVENT-0143 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	セキュリティアラート	アラート名とトリガー条件	注意
		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。
		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。
		このイベントは、RDS インスタンスストレージの自動スケー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。
		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。
		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。

サービス	セキュリティアラート	アラート名とトリガー条件	注意
		サブネットに十分な IP アドレスがないため、RDS はプロキシの容量をプロビジョニングできませんでした。	RDS-EVENT-0243 の詳細については、「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。
		AWS アカウントのストレージが、許可されたストレージクォータを超えています。	RDS-EVENT-0254 の詳細については、「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。
		CPUUtilization 平均 CPU 使用率 > 90%、15 分間、2 回連続。	CloudWatch アラーム。
		DiskQueueDepth 合計は 1 分間 > 75 で、連続して 15 回です。	
		FreeStorageSpace 平均 < 1,073,741,824 バイト、5 分間、2 回連続。	
		SwapUsage 平均 >= 5 分間 104,857,600 バイト、連続 2 回。	

サービス	セキュリティアラート	アラート名とトリガー条件	注意
Amazon Redshift クラスター	なし	RedshiftClusterStatus メンテナンスモードでない場合のクラスターの状態 < 1 を 5 分間。	1 は正常なクラスターを表します。
Amazon Macie	あり	新しく生成されたアラートと既存のアラートの更新。 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 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。

ログの保持とローテーションのデフォルト

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

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

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

監査およびセキュリティ上の理由から無期限に保持される口グを除き、すべての AWS CloudTrail 口グの口グ保持の変更をリクエストできます。

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

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

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

継続性管理のデフォルト

このセクションでは、AMS 継続性管理のデフォルトについて説明します。AMS バックアップの詳細については、「AMS ユーザーガイド継続性管理」の章を参照してください。

バックアップ設定はオンボーディング時に行われます。これらは、デフォルトの (推奨) バックアップ設定です。

VPC タグとデフォルト

AMS バックアップに関する最新情報については、「継続性管理」を参照してください。

> **Important**
>
> デフォルトでは、EC2 スタックのバックアップは無効になっています (バックアップ = False)。作成時に EC2 インスタンスのバックアップを有効にするには、RFC (CT ct-14027q0sjyt1h) を介して EC2 スタックをリクエスト`Key: Backup, Value: True`するときにタグを追加します。インスタンスの作成後に タグを追加する場合は、 Management | Advanced stack components | EC2 instance stack | Update CT (ct-38s4s4tm4ic4u) を使用して RFC を送信します。

EC2 インスタンスのタグとデフォルト

EC2 スタックバックアップタグは、スタックにアタッチされた EBS ボリュームのスナップショットが必要かどうかを指定します。

タグ `Key: Backup`

タグ `Value: True, False`

デフォルトでは、 値は`False`バックアップタグは存在せず、スタックにはスケジュールされたバックアップがありません。

タグを Key: Backupに変更Value: Trueしてバックアップを有効にします。バックアップは、VPC バックアップタグで設定されたスケジュールで実行されます。

> **Note**
>
> タグ値 (値のみ) の大文字と小文字は区別されないため、True/true または False/false はすべて許容されます。

RDS インスタンスのバックアップとデフォルト

Amazon Relational Database Service (RDS) のデフォルト値は、スタックテンプレートで定義されます。

```
Backup: Yes

Backup Window: 22:00-23:00 (RDS local time zone)

Retention Period: 7 (7 snapshots stored)
```

パッチ適用のデフォルト

このセクションでは、AMS パッチ適用のデフォルトについて説明します。AMS パッチ適用の詳細については、AMS ユーザーガイドのパッチ管理の章を参照してください。

AMS はパッチが適用された AMIs毎月リリースします。新しいスタックリクエストはすべて最新の AMS AMI で設定する必要があります。

> **Important**
>
> タグベースのパッチ適用である AMS Patch Orchestrator は、AWS Systems Manager (SSM) 機能を使用して、インスタンスにタグを付けるか、AMS 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します。詳細については、「パッチオーケストレーター: タグベースのパッチ適用モデル」を参照してください。

AMS 標準、アカウントベース、パッチ適用: インプレースパッチを受け取るスタックを持つアカウントごとに、該当するパッチの通知が「パッチ火曜日」の直後に送信されます。通知には、すべてのスタックと適用可能なパッチのリスト、および推奨されるパッチウィンドウが含まれます。重要なパッチの場合、ウィンドウは 10 日以上前に設定されず、標準パッチの場合は 14 日以上前に設定されま

せん。通知に返信しない場合、パッチ適用は行われません。特定のパッチを除外する場合は、通知に返信するか、サービスリクエストを送信します。パッチ適用に同意して返信しても、特に別のスケジュールをリクエストしない場合、受信した通知の説明に従ってパッチが適用されます。

> **Note**
>
> パッチサービス通知は、アカウントの連絡先に送信される E メールであり、AWS サポートコンソールへのリンクが含まれています。AWS サポートコンソール、または通知がサービス通知として表示される AMS サービスリクエストページから返信できます。

AMS 標準パッチ適用プロセスの時点で、AMS は以下を実行します。

1. 提案されたパッチウィンドウの 14 日前にパッチ適用サービス通知が送信されます。パッチ適用サービス通知は、アカウントに登録されている連絡先 E メールアドレスに E メールで送信されます。
2. パッチ適用通知で提供されたスタックのリストに基づいて、スタック内で到達可能なすべての EC2 インスタンスを識別します。この場合、「Reachable」とは、「RunningEC2 状態にあり、EC2 Run Command エージェントが完全に動作するインスタンスを意味します。
3. AMS は、十分な数の EC2 インスタンスが同時に実行され (`healthy-host-threshold` 設定で設定) 、スタックが正常なままになるようにパッチを適用します。
4. すべての EC2 インスタンスのパッチ適用オペレーションが完了すると、AMS はパッチ適用ステータスとして成功、部分成功、失敗の RFC を更新します。Success 以外のステータスの場合、オペレータがパッチ適用結果をフォローアップし、修正アクションを実行するためのチケットが作成されます。

AMS サービスの検証 (SALZ)

AWS Managed Services (AMS) サービスが正常に動作していることを検証するには、この章でいくつかの演習について説明します。

AMS アカウント設定の検索

AMS RFCs の作成、スケジュールの設定、通知の受信者の決定に使用されるアカウント設定。

一部の設定はオンボーディング中に作成され、変更するにはサービスリクエストが必要です。これらのアカウントの詳細は、AMS と通信するときに使用するため、書き留めておきます。

- 認証情報: AMS ユーザー名またはパスワードを取得する必要がある場合は、ローカル IT 管理者にお問い合わせください。--AMS は社内の Active Directory を使用します。
- Cloud Service Delivery Manager (CSDM): このユーザーは AMS との連絡係であり、サービスの質問に回答できます。このユーザーの連絡先情報はオンボーディング時に提供され、AMS を操作する組織内のすべてのユーザーが利用できるようにする必要があります。このユーザーから AMS サービスに関する月次レポートを受け取ることを期待できます。
- コンソールアクセス: アカウント専用に設定された URL で AMS コンソールにアクセスします。URL は CSDM から取得できます。
- AMS CLI: AMS CLI は、AMS コンソール開発者のリソースページ、または CSDM から取得した頒布可能パッケージから取得できます。頒布可能パッケージを入手したら、「AMS CLI のインストールまたはアップグレード」で説明されているステップに従います。
- メンテナンスウィンドウ: EC2 インスタンスのパッチ適用がいつ行われるかは、メンテナンスウィンドウによって決まります。AWS Managed Servicesメンテナンスウィンドウ (またはメンテナンスウィンドウ) は、AWS Managed Services (AMS) のメンテナンスアクティビティを実行し、毎月第 2 木曜日の太平洋標準時の午後 3 時から午後 4 時まで繰り返します。AMS は、48 時間前に通知することでメンテナンスウィンドウを変更する場合があります。オンボーディング時に別のウィンドウを選択している可能性があります。選択したメンテナンスウィンドウの記録を保持します。
- モニタリング: AMS はデフォルトで一連の CloudWatch メトリクスを提供しますが、追加のメトリクスをリクエストすることもできます。その場合は、記録しておきます。
- ログ: デフォルトでは、ログは ams-a-*ACCOUNT_ID*-log-management-*REGION* に保存されます。*REGION* はログが生成されたリージョンです。
- 緩和策: リソースに対するマルウェア攻撃が特定された場合、AMS はオンボーディング時に選択した緩和アクションを記録します。たとえば、特定のユーザーに連絡します。AMS を操作する組織内のすべてのユーザーがこの情報を利用できるようにします。
- リージョン: AMS コンソールの VPC の詳細ページを確認できます。AMS SKMS CLI をインストールした後にこのコマンドを実行することもできます (このコマンドは SAML プロファイルを使用し、認証方法が異なる場合は を削除します)。

```
aws --profile saml amsskms get-vpc --vpc-id VPC_ID
```

Important

Note

AMS API/CLI (amscm および amsskms) エンドポイントは、AWS N. Virginia リージョン にありますus-east-1。認証の設定方法や、アカウントとリソースがどの AWS リージョンにあるかによっては、コマンドの発行--region us-east-1時に追加する必要がある場合があります。認証方法である場合は--profile saml、 を追加する必要がある場合もあります。

AMS で FQDNs を検索する

AWS Managed Services (AMS) アクセス変更タイプ (CTs) には、AMS が信頼するドメインの完全修飾ドメイン名または FQDN が の形式で必要ですC844273800838.amazonaws.com。FQDN AWS を検出するには、次のいずれかを実行します。

- AWS コンソール: ディレクトリ名列の AWS Directory Service コンソールを確認します。
- CLI: ドメインにログインしている間は、次のコマンドを使用します。

  Windows (ユーザーと FQDN を返します):

```
whoami /upn
```

  または (DC+DC+DC=FQDN)

```
whoami /fqdn
```

  Linux:

```
hostname --fqdn
```

Note

AMS API/CLI (amscm および amsskms) エンドポイントは、AWS N. Virginia リージョン にありますus-east-1。認証の設定方法や、アカウントとリソースがどの AWS リージョンに

あるかによっては、コマンドの発行--region us-east-1時に追加する必要がある場合があります。認証方法である場合は--profile saml、 を追加する必要がある場合もあります。

AMS でアベイラビリティーゾーン (AZs) を検索する

アベイラビリティーゾーン: すべてのアカウントに少なくとも 2 つのアベイラビリティーゾーンがあります。アベイラビリティーゾーン名を正確に検索するには、まず関連するサブネット ID を知る必要があります。

- AMS コンソール: ナビゲーションペインで VPCsをクリックし、必要に応じて関連する VPC をクリックします。VPCs の詳細ページで、サブネットのテーブルで関連するサブネットを選択し、関連するアベイラビリティーゾーンの名前を含むサブネットの詳細ページを開きます。
- AMS SKMS API/CLI:

```
aws amsskms list-subnet-summaries --output table
```

```
aws amsskms get-subnet --subnet-id SUBNET_ID
```

Note

AMS API/CLI (amscm および amsskms) エンドポイントは、AWS N. Virginia リージョン にありますus-east-1。認証の設定方法、およびアカウントとリソースがどの AWS リージョンにあるかによっては、コマンドの発行--region us-east-1時に追加する必要がある場合があります。認証方法である場合は--profile saml、 を追加する必要がある場合もあります。

AMS で SNS トピックを検索する

SNS トピックは、さまざまな状況で通知されるユーザーを決定します。AMS は、AMI 通知 (SNS を使用した AMS AMI 通知を参照) 、CloudWatch アラーム、EC2 リソース (AMS によって生成されたアラートの受信を参照) などの SNS https://docs.aws.amazon.com/managedservices/latest/userguide/sent-alert-views.htmlトピックを提供します。 CloudWatch EC2 既存の SNS トピックを検出するには：

- AWS コンソール: SNS コンソールを使用して、すべてのトピック、アプリケーション、サブスクリプション、およびメッセージのグラフを表示します。また、トピックを作成、削除、サブスクライブ、公開します。
- API/CLI (AMS アカウントにログインする場合、 には AWS CLI が必要です) 。

  SNS トピックを一覧表示します。

```
aws sns list-topics
```

  SNS サブスクリプションを一覧表示します。

```
aws sns list-subscriptions
```

> **Note**
>
> AMS API/CLI (amscm および amsskms) エンドポイントは、AWS N. Virginia リージョン にありますus-east-1。認証の設定方法や、アカウントとリソースがどの AWS リージョンにあるかによっては、コマンドの発行--region us-east-1時に追加する必要がある場合があります。認証方法である場合は--profile saml、 を追加する必要がある場合もあります。

AMS でバックアップ設定を検索する

バックアップとスナップショットは、ネイティブAWS Backupサービスを通じて AMS によって管理されます。

設定は AWS Backup 計画を通じて管理されます。タグ付けされたリソースをバックアップスケジュールと保持ポリシーに関連付ける複数の AWS Backup プランを持つことができます。AMS アカウント AWS Backup 設定を確認するには、https://console.aws.amazon.com/backup コンソールを使用するか、バックアップコマンドの AWS CLI コマンドリファレンスを使用します。

AMS と の詳細については AWS Backup、「継続性管理」を参照してください。

インスタンス ID または IP アドレスの検索

インスタンスにログインするには、インスタンスの IP アドレスが必要です。

- インスタンスへのアクセスをリクエストする、インスタンスにログインする、または AMI を作成するには、インスタンス ID が必要です。EC2 インスタンス (スタンドアロンインスタンスまたはスタックの一部) またはデータベースインスタンスの場合は、いくつかの異なる方法で ID を見つけることができます。

  - ASG スタック内のインスタンスの AMS コンソール: スタックを作成した RFC の RFC 詳細ページを確認します。実行出力セクションには、ASG スタックのスタック ID が表示され、EC2 コンソールの Auto Scaling Groups ページに移動してそのスタック ID を検索し、そのスタックのインスタンスを検索できます。インスタンスを見つけたら、そのインスタンスを選択すると、IP アドレスなどの詳細を含むエリアがページの下部に表示されます。
  - スタンドアロン EC2 またはデータベース (DB) インスタンスの AMS コンソール: EC2 スタックまたは DB インスタンスを作成した RFC の RFC 詳細ページを確認します。実行出力セクションには、インスタンス ID と IP アドレスが表示されます。
  - AWS EC2 コンソール：

    1. ナビゲーションペインで、[インスタンス] を選択します。インスタンスページが開きます。
    2. ID が必要なインスタンスをクリックします。インスタンスの詳細ページが開き、ID と IP アドレスが表示されます。

  - AWS データベースコンソール：

    1. ホームページで、DB インスタンスを選択します。インスタンスページが開きます。
    2. ID が必要な DB インスタンスをフィルタリングします。インスタンスの詳細ページが開き、ID が表示されます。

  - AMS CLI/API。

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

> **Note**
>
> AMS API/CLI (amscm および amsskms) エンドポイントは、AWS N. Virginia リージョン にありますus-east-1。認証の設定方法や、アカウントとリソースが存在する AWS リージョンによっては、コマンドの発行--region us-east-1時に追加が必要になる場合があります。認証方法である場合は--profile saml、 を追加する必要がある場合もあります。

次のコマンドを実行して、スタック実行出力の詳細を取得します。

```
aws amsskms get-stack --stack-id STACK_ID
```

出力は次のようになります。InstanceId は下部の の下に表示されます Outputs (値は例です)。

```
{
    "Stack": {
        "StackId": "stack-7fa52bd5eb8240123",
        "Status": {
            "Id": "CreateCompleted",
            "Name": "CreateCompleted"
        },
        "VpcId": "vpc-01234567890abcdef",
        "Description": "Amazon",
        "Parameters": [
            {
                "Value": "sg-01234567890abcdef,sg-01234567890abcdef",
                "Key": "SecurityGroups"
            },
            {
                "Value": "subnet-01234567890abcdef",
                "Key": "InstanceSubnetId"
            },
            {
                "Value": "t2.large",
                "Key": "InstanceType"
            },
            {
```

```
                "Value": "ami-01234567890abcdef",
                "Key": "InstanceAmiId"
            }
        ],
        "Tags": [],
        "Outputs": [
            {
                "Value": "i-0b22a22eec53b9321",
                "Key": "InstanceId"
            },
            {
                "Value": "10.0.5.000",
                "Key": "InstancePrivateIP"
            }
        ],
        "StackTemplateId": "stm-s6xvs000000000000",
        "CreatedTime": "1486584508416",
        "Name": "Amazon"
    }
}
```

DNS フレンドリ踏み台名

MALZ

マルチアカウントランディングゾーン (MALZ) の場合、AMS マネージド Active Directory の FQDN の踏み台に DNS レコードが作成されます。AMS は、必要に応じて Linux と Windows の踏み台を置き換えます。例えば、デプロイする必要がある新しい踏み台 AMI がある場合、踏み台 DNS レコードは新しい有効な踏み台を指すように動的に更新されます。

1. SSH (Linux) 踏み台にアクセスするには、次のような DNS レコードを使用します。
   `sshbastion(1-4).Your_Domain.com`

   たとえば、ドメインが の場合`Your_Domain`：

   - `sshbastion1.Your_Domain.com`
   - `sshbastion2.Your_Domain.com`
   - `sshbastion3.Your_Domain.com`
   - `sshbastion4.Your_Domain.com`

2. RDP (Windows) 踏み台にアクセスするには、 のような DNS レコードを使用しますrdp-*Username*.*Your_Domain*.com。

   たとえば、ユーザー名が alex、test、demo、または でbob、ドメインが の場合*Your_Domain*.com：

   - rdp-alex.*Your_Domain*.com
   - rdp-test.*Your_Domain*.com
   - rdp-demo.*Your_Domain*.com
   - rdp-bob.*Your_Domain*.com

SALZ

シングルアカウントランディングゾーン (SALZ) は、必要に応じて Linux と Windows の踏み台を置き換えます。例えば、デプロイする必要がある新しい踏み台 AMI がある場合、踏み台 DNS レコードは新しい有効な踏み台を指すように動的に更新されます。

1. SSH (Linux) 踏み台にアクセスするには、次のような DNS レコードを使用します。sshbastion*(1-4)*.A*AccountNumber*.amazonaws.com.

   たとえば、 123456789012はアカウント番号です。

   - sshbastion1.A123456789012.amazonaws.com
   - sshbastion2.A123456789012.amazonaws.com
   - sshbastion3.A123456789012.amazonaws.com
   - sshbastion4.A123456789012.amazonaws.com

2. RDP (Windows) 踏み台にアクセスするには、 のような DNS レコードを使用しますrdpbastion*(1-4)*.A*ACCOUNT_NUMBER*.amazonaws.com。

   たとえば、 123456789012はアカウント番号です。

   - rdpbastion1.A123456789012.amazonaws.com
   - rdpbastion2.A123456789012.amazonaws.com
   - rdpbastion3.A123456789012.amazonaws.com
   - rdpbastion4.A123456789012.amazonaws.com

踏み台 IP アドレスの検索

AMS のお客様は、DNS フレンドリ踏み台名前述の または踏み台 IP アドレスのいずれかの SSH および RDP 踏み台を使用できます。

アカウントの踏み台 IP アドレス、SSH、RDP を見つけるには：

1. マルチアカウントランディングゾーンのみ: 共有サービスアカウントにログインします。
2. EC2 コンソールを開き、インスタンスの実行を選択します。

   インスタンスページが開きます。
3. 上部のフィルターボックスに、ssh-bastion または rdp-bastion を入力します。

   上部のフィルターボックスに、customer-ssh または customer-rdp を入力します。

   アカウントの SSH および/または RDP 踏み台が表示されます。

   SSH 踏み台に加えて、リストに AMS 境界ネットワーク踏み台が表示される場合がありますが、これは利用できません。
4. SSH または RDP 踏み台を選択します。Windows コンピュータを使用していて、Linux インスタンスにログインする場合は、SSH 踏み台を使用します。Windows インスタンスにログインする場合は、RDP 踏み台を使用します。Linux OS で Windows インスタンスにログインする場合は、RDP トンネルを介して SSH 踏み台を使用します (これにより Windows デスクトップにアクセスできます) 。Linux OS から Linux インスタンスにアクセスするには、SSH 踏み台を使用します。

EC2 インスタンス: の作成

AMS コンソールまたは API/CLI を使用して、追加のボリュームを持つ Amazon EC2 と Amazon EC2 を作成できます。

スタックの作成

コンソールを使用した EC2 インスタンスの作成

AMS コンソールでこの変更タイプを以下に示します。

仕組み：

1. RFC の作成ページに移動します。AMS コンソールの左側のナビゲーションペインでRFCs をクリックして RFCsリストページを開き、RFC の作成をクリックします。
2. デフォルトの変更タイプ参照ビューで一般的な変更タイプ (CT) を選択するか、カテゴリ別選択ビューで CT を選択します。
   - 変更タイプ別に参照: クイック作成エリアで一般的な CT をクリックすると、すぐに RFC の実行ページを開くことができます。クイック作成で古い CT バージョンを選択することはできません。

     CTs をソートするには、カードビューまたはテーブルビューですべての変更タイプエリアを使用します。どちらのビューでも、CT を選択し、RFC の作成をクリックして RFC の実行ページを開きます。必要に応じて、RFC の作成ボタンの横に古いバージョンで作成オプションが表示されます。
   - カテゴリ別に選択: カテゴリ、サブカテゴリ、項目、オペレーションを選択すると、CT 詳細ボックスが開き、必要に応じて古いバージョンで作成するオプションが表示されます。RFC の作成をクリックして、RFC の実行ページを開きます。
3. RFC の実行ページで、CT 名エリアを開き、CT の詳細ボックスを表示します。件名は必須です (変更タイプの参照ビューで CT を選択した場合は入力されます) 。追加設定エリアを開き、RFC に関する情報を追加します。

   実行設定領域で、使用可能なドロップダウンリストを使用するか、必要なパラメータの値を入力します。オプションの実行パラメータを設定するには、追加設定エリアを開きます。
4. 完了したら、実行 をクリックします。エラーがない場合、RFC が正常に作成されたページに、送信された RFC の詳細と最初の実行出力が表示されます。
5. Run parameters 領域を開き、送信した設定を確認します。ページを更新して RFC 実行ステータスを更新します。必要に応じて、RFC をキャンセルするか、ページ上部のオプションを使用してコピーを作成します。

CLI を使用した EC2 インスタンスの作成

仕組み：

1. インライン作成 (すべての RFC と実行パラメータを含む`create-rfc`コマンドを発行) またはテンプレート作成 (2 つの JSON ファイルを作成します。1 つは RFC パラメータ用、もう 1 つは実行パラメータ用) のいずれかを使用し、2 つのファイルを入力として`create-rfc`コマンドを発行します。どちらの方法もここで説明します。

2. 返された RFC ID を使用して RFC: `aws amscm submit-rfc --rfc-id ID` コマンドを送信します。

   RFC: `aws amscm get-rfc --rfc-id ID` コマンドをモニタリングします。

変更タイプのバージョンを確認するには、次のコマンドを使用します。

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> 変更タイプのスキーマの一部であるかどうかにかかわらず、任意の RFC で任意のCreateRfcパラメータを使用できます。たとえば、RFC ステータスが変更されたときに通知を受け取るには、リクエストの RFC パラメータ部分 (実行パラメータではなく) `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"`にこの行を追加します。すべての CreateRfc パラメータのリストについては、AMS 変更管理 API リファレンスを参照してください。

インライン作成：

インラインで指定された実行パラメータ (インラインで実行パラメータを指定する場合は引用符をエスケープ) を指定して create RFC コマンドを発行し、返された RFC ID を送信します。たとえば、コンテンツを次のような内容に置き換えることができます。

```
aws amscm create-rfc --change-type-id "ct-14027q0sjyt1h" --change-type-version "4.0"
 --title "EC2-Create-RFC" --execution-parameters "{\"Description\": \"Create a new
 EC2 Instance stack\",\"VpcId\": \"vpc-0a60eb65b4EXAMPLE\",\"Name\": \"My-EC2\",
\"TimeoutInMinutes\": 60,\"Parameters\": {\"InstanceAmiId\": \"ami-1234567890EXAMPLE\",
\"InstanceDetailedMonitoring\": false,\"InstanceEBSOptimized\": false,\"InstanceProfile
\": \"customer-mc-ec2-instance-profile\",\"InstanceRootVolumeIops\": 3000,
\"InstanceRootVolumeType\": \"gp3\",\"InstanceType\": \"t2.large\",\"InstanceUserData
\": \"\",\"InstanceSubnetId\": \"subnet-0bb1c79de3EXAMPLE\",\"EnforceIMDSV2\":
 \"false\"}}"
```

テンプレートの作成：

1. この変更タイプの実行パラメータを JSON ファイルに出力します。この例では CreateEC2Params.json:

```
aws amscm get-change-type-version --change-type-id "ct-14027q0sjyt1h" --query
 "ChangeTypeVersion.ExecutionInputSchema" --output text > CreateEC2Params.json
```

2. CreateEC2Params ファイルを変更して保存します。たとえば、コンテンツを次のような内容に置き換えることができます。

```
{
  "Description": "Create a new EC2 Instance stack",
  "VpcId": "vpc-0a60eb65b4EXAMPLE",
  "Name": "My-EC2",
  "TimeoutInMinutes": 60,
  "Parameters": {
    "InstanceAmiId": "ami-1234567890EXAMPLE",
    "InstanceDetailedMonitoring": false,
    "InstanceEBSOptimized": false,
    "InstanceProfile": "customer-mc-ec2-instance-profile",
    "InstanceRootVolumeIops": 3000,
    "InstanceRootVolumeType": "gp3",
    "InstanceType": "t2.large",
    "InstanceUserData": "",
    "InstanceSubnetId": "subnet-0bb1c79de3EXAMPLE",
    "EnforceIMDSV2": "false"
  }
}
```

3. RFC テンプレートを現在のフォルダ内のファイルに出力します。この例では CreateEC2Rfc.json:

```
aws amscm create-rfc --generate-cli-skeleton > CreateEC2Rfc.json
```

4. CreateEC2Rfc.json ファイルを変更して保存します。たとえば、コンテンツを次のような内容に置き換えることができます。

```
{
"ChangeTypeVersion":    "4.0",
"ChangeTypeId":         "ct-14027q0sjyt1h",
"Title":                "EC2-Create-RFC"
}
```

5. CreateEC2Rfc ファイルと CreateEC2Params ファイルを指定して、RFC を作成します。

```
aws amscm create-rfc --cli-input-json file://CreateEC2Rfc.json  --execution-
parameters file://CreateEC2Params.json
```

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

ヒント

> **セキュリティグループ**
>
> この変更タイプのバージョン 3.0 以降、独自のセキュリティグループを指定した場合、AMS はデフォルトの AMS セキュリティグループをアタッチしません。リクエストで独自のセキュリティグループを指定しない場合、AMS は AMS のデフォルトのセキュリティグループをアタッチします。以前のバージョンでは、独自のセキュリティグループを指定したかどうかにかかわらず、AMS はデフォルトのセキュリティグループをアタッチしました。
> 現在、カスタムセキュリティグループを指定する場合は、アカウントのデフォルトの AMS セキュリティグループの IDs `mc-initial-garden-SG-name`と も指定する必要がありますmc-initial-garden-SG-name。

> **インスタンスタイプ**
>
> AMS では、t2.micro/t3.micro および t2.nano/t3.nano タイプは推奨されません。これらはより小さなインスタンスタイプであり、アプリケーションと AMS ツールのパフォーマンスを低下させる可能性があります。EC2 インスタンスには、アプリケーションのワークロードに加えて、EPS、SSM、Cloudwatch などの AMS ツールをサポートするのに十分な容量が必要です。詳細については、「アプリケーションに適した EC2 インスタンスタイプの選択」を参照してください。

追加ボリュームで EC2 スタックを作成するには、EC2 スタック | 作成 (追加ボリュームあり) 」を参照してください。

最大 50 個のタグを追加できますが、追加設定ビューを有効にする必要があります。

必要に応じて、EC2 インスタンススタックの作成が失敗する」を参照してください。

スタックを作成する (ボリュームを追加)

コンソールを使用した EC2 インスタンスと追加のボリュームの作成

AMS コンソールでこの変更タイプを以下に示します。

仕組み :

1. RFC の作成ページに移動します。AMS コンソールの左側のナビゲーションペインでRFCs をクリックして RFCsリストページを開き、RFC の作成をクリックします。
2. デフォルトの変更タイプ参照ビューで一般的な変更タイプ (CT) を選択するか、カテゴリ別選択ビューで CT を選択します。
   - 変更タイプ別に参照: クイック作成エリアで一般的な CT をクリックすると、すぐに RFC の実行ページを開くことができます。クイック作成で古い CT バージョンを選択することはできません。

     CTs をソートするには、カードビューまたはテーブルビューですべての変更タイプエリアを使用します。どちらのビューでも、CT を選択し、RFC の作成をクリックして RFC の実行ページを開きます。必要に応じて、RFC の作成ボタンの横に古いバージョンで作成オプションが表示されます。
   - カテゴリ別に選択: カテゴリ、サブカテゴリ、項目、オペレーションを選択すると、CT 詳細ボックスが開き、必要に応じて古いバージョンで作成するオプションが表示されます。RFC の作成をクリックして、RFC の実行ページを開きます。
3. RFC の実行ページで、CT 名エリアを開き、CT の詳細ボックスを表示します。件名は必須です (変更タイプの参照ビューで CT を選択した場合は入力されます) 。追加設定エリアを開き、RFC に関する情報を追加します。

   実行設定領域で、使用可能なドロップダウンリストを使用するか、必要なパラメータの値を入力します。オプションの実行パラメータを設定するには、追加設定エリアを開きます。
4. 完了したら、実行 をクリックします。エラーがない場合、RFC が正常に作成されたページに、送信された RFC の詳細と最初の実行出力が表示されます。
5. Run parameters 領域を開き、送信した設定を確認します。ページを更新して RFC 実行ステータスを更新します。必要に応じて、RFC をキャンセルするか、ページ上部のオプションを使用してコピーを作成します。

CLI を使用した EC2 インスタンスと追加のボリュームの作成

仕組み：

1. インライン作成 (すべての RFC と実行パラメータを含むcreate-rfcコマンドを発行) またはテンプレート作成 (2 つの JSON ファイルを作成します。1 つは RFC パラメータ用、もう 1 つは実行パラメータ用) のいずれかを使用し、2 つのファイルを入力としてcreate-rfcコマンドを発行します。どちらの方法もここで説明します。
2. 返された RFC ID を使用して RFC: `aws amscm submit-rfc --rfc-id ID` コマンドを送信します。

   RFC: `aws amscm get-rfc --rfc-id ID` コマンドをモニタリングします。

変更タイプのバージョンを確認するには、次のコマンドを使用します。

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> 変更タイプのスキーマの一部であるかどうかにかかわらず、任意の RFC で任意のCreateRfcパラメータを使用できます。たとえば、RFC ステータスが変更されたときに通知を受け取るには、リクエストの RFC パラメータ部分 (実行パラメータではなく) `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"`にこの行を追加します。すべての CreateRfc パラメータのリストについては、AMS 変更管理 API リファレンスを参照してください。

インライン作成：

インラインで指定された実行パラメータ (インラインで実行パラメータを指定する場合は引用符をエスケープ) を指定して create RFC コマンドを発行し、返された RFC ID を送信します (例は必須パラメータのみを示しています) 。たとえば、コンテンツを次のような内容に置き換えることができます。

```
aws amscm create-rfc --change-type-id "ct-1aqsjf86w6vxg" --change-type-version "4.0"
 --title "EC2-Create-A-V-QC" --execution-parameters "{\"Description\":\"My EC2 stack
 with addl vol\",\"VpcId\":\"VPC_ID\",\"Name\":\"My Stack\",\"StackTemplateId\":
```

```
\"stm-nn8v8ffhcal611bmo\",\"TimeoutInMinutes\":60,\"Parameters\":{\"InstanceAmiId\":
\"AMI_ID\",\"InstanceSubnetId\":\"SUBNET_ID\"}}
```

テンプレートの作成：

1. この変更タイプの実行パラメータを CreateEC2AVParams.json.

```
aws amscm get-change-type-version --change-type-id "ct-1aqsjf86w6vxg" --query
 "ChangeTypeVersion.ExecutionInputSchema" --output text > CreateEC2AVParams.json
```

2. CreateEC2AVParams ファイルを変更して保存します (例はほとんどのパラメータを示しています) 。たとえば、コンテンツを次のような内容に置き換えることができます。

```
{
"Description":      "EC2-Create-1-Addl-Volumes",
"VpcId":            "VPC_ID",
"StackTemplateId":  "stm-nn8v8ffhcal611bmo",
"Name":             "My-EC2-1-Addl-Volume",
"TimeoutInMinutes": 60,
"Parameters":   {
    "InstanceAmiId":    "AMI_ID",
    "InstanceSecurityGroupIds": "SECURITY_GROUP_ID",
    "InstanceCoreCount": 1,
    "InstanceThreadsPerCore": 2,
    "InstanceDetailedMonitoring": "true",
    "InstanceEBSOptimized": "false",
    "InstanceProfile": "customer-mc-ec2-instance-profile",
    "InstanceRootVolumeIops": 100,
    "InstanceRootVolumeName": "/dev/xvda",
    "InstanceRootVolumeSize": 50,
    "InstanceRootVolumeType": "io1",
    "RootVolumeKmsKeyId": "default",
    "InstancePrivateStaticIp": "10.27.0.100",
    "InstanceSecondaryPrivateIpAddressCount": 0,
    "InstanceTerminationProtection": "false",
    "InstanceType": "t3.large",
    "CreditSpecification": "unlimited",
    "InstanceUserData": "echo $",
    "Volume1Encrypted": "true",
    "Volume1Iops":      "IOPS"
    "Volume1KmsKeyId":  "KMS_MASTER_KEY_ID",
    "Volume1Name":      "xvdh"
    "Volume1Size":      "2 GiB",
```

```
    "Volume1Snapshot":  "SNAPSHOT_ID",
    "Volume1Type":      "iol",
    "InstanceSubnetId": "SUBNET_ID"
    }
}
```

3. RFC テンプレートを現在のフォルダ内のファイルに出力します。この例では CreateEC2AVRfc.json:

```
aws amscm create-rfc --generate-cli-skeleton > CreateEC2AVRfc.json
```

4. CreateEC2AVRfc.json ファイルを変更して保存します。たとえば、コンテンツを次のような内容に置き換えることができます。

```
{
"ChangeTypeVersion":    "4.0",
"ChangeTypeId":         "ct-1aqsjf86w6vxg",
"Title":                "EC2-Create-1-Addl-Volume-RFC"
}
```

5. CreateEC2AVRfc ファイルと CreateEC2AVParams ファイルを指定して、RFC を作成します。

```
aws amscm create-rfc --cli-input-json file://CreateEC2AVRfc.json  --execution-
parameters file://CreateEC2AVParams.json
```

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

ヒント

> **Important**
>
> この変更タイプには、別の StackTemplateId (stm-nn8v8ffhcal611bmo) を使用する新しいバージョン v 4.0 があります。これは、コマンドラインでこの変更タイプを使用して RFC を送信する場合に重要です。新しいバージョンでは、2 つの新しいパラメータ (RootVolumeKmsKeyId と CreditSpecification) が導入され、1 つの既存のパラメータ (InstanceType) のデフォルトが変更されました。

インスタンスタイプ

- コアまたはスレッドの数を指定する場合は、両方の値を指定する必要があります。パラメータ InstanceCoreCountと を使用しますInstanceThreadsPerCore。コア/スレッドの有効な組み合わせを確認するには、「インスタンスタイプ ごとの CPU コアと CPU コアあたりのスレッド」を参照してください。
- AMS では、t2.micro/t3.micro または t2.nano/t3.nano インスタンスタイプは推奨されません。これらは小さすぎて、ビジネスワークロードに加えて EPS、SSM、Cloudwatch などの AMS ツールをサポートできません。詳細については、「アプリケーションに適した EC2 インスタンスタイプの選択」を参照してください。
- バージョン 4.0 では、デフォルトのタイプが t2.large から t3.large に引き上げられました。T3 インスタンスは、デフォルトで「無制限のクレジット」で起動します。インスタンスがすべての CPU クレジットを消費しても、CPU スロットリングは発生しません。代わりに、T2 インスタンスを選択し、CreditSpecification 無制限オプションを使用できます。
- サイズのレコメンデーションを含む Amazon EC2 の詳細については、「Amazon Elastic Compute Cloud ドキュメント」を参照してください。

作成後に EC2 スタックを追加ボリュームで更新するには、EC2 インススタック: 更新 (追加ボリュームあり) 」を参照してください。

アクセス、リクエスト

管理者アクセスをリクエストする

コンソールを使用した管理者アクセスのリクエスト

AMS コンソールでこの変更タイプを以下に示します。

仕組み：

1. RFC の作成ページに移動します。AMS コンソールの左側のナビゲーションペインでRFCs をクリックして RFCsリストページを開き、RFC の作成をクリックします。
2. デフォルトの Browse change types ビューで一般的な変更タイプ (CT) を選択するか、Choose by category ビューで CT を選択します。

- 変更タイプ別に参照: クイック作成エリアで一般的な CT をクリックすると、すぐに RFC の実行ページを開くことができます。クイック作成で古い CT バージョンを選択することはできません。

  CTs をソートするには、カードビューまたはテーブルビューですべての変更タイプ領域を使用します。どちらのビューでも、CT を選択し、RFC の作成をクリックして RFC の実行ページを開きます。必要に応じて、RFC の作成ボタンの横に古いバージョンで作成オプションが表示されます。
- カテゴリ別に選択: カテゴリ、サブカテゴリ、項目、オペレーションを選択すると、CT 詳細ボックスが開き、必要に応じて古いバージョンで作成するオプションが表示されます。RFC の作成をクリックして、RFC の実行ページを開きます。

3. RFC の実行ページで、CT 名エリアを開き、CT の詳細ボックスを表示します。件名は必須です (変更タイプの参照ビューで CT を選択した場合は入力されます) 。追加設定領域を開き、RFC に関する情報を追加します。

   実行設定領域で、使用可能なドロップダウンリストを使用するか、必要なパラメータの値を入力します。オプションの実行パラメータを設定するには、追加設定エリアを開きます。
4. 完了したら、実行 をクリックします。エラーがない場合、RFC が正常に作成されたページに、送信された RFC の詳細と最初の実行出力が表示されます。
5. Run parameters エリアを開き、送信した設定を確認します。ページを更新して RFC 実行ステータスを更新します。必要に応じて、RFC をキャンセルするか、ページ上部のオプションを使用してコピーを作成します。

CLI を使用した管理者アクセスのリクエスト

仕組み：

1. インライン作成 (すべての RFC と実行パラメータを含む`create-rfc`コマンドを発行) またはテンプレート作成 (2 つの JSON ファイルを作成し、1 つは RFC パラメータ用、もう 1 つは実行パラメータ用) のいずれかを使用し、2 つのファイルを入力として`create-rfc`コマンドを発行します。どちらの方法もここで説明します。
2. 返された RFC ID を使用して RFC: `aws amscm submit-rfc --rfc-id` *`ID`* コマンドを送信します。

   RFC: `aws amscm get-rfc --rfc-id` *`ID`* コマンドをモニタリングします。

変更タイプのバージョンを確認するには、次のコマンドを使用します。

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> 変更タイプのスキーマの一部であるかどうかにかかわらず、任意の RFC で任意のCreateRfcパラメータを使用できます。たとえば、RFC ステータスが変更されたときに通知を受け取るには、リクエストの RFC パラメータ部分 (実行パラメータではなく) --notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"にこの行を追加します。すべての CreateRfc パラメータのリストについては、AMS 変更管理 API リファレンスを参照してください。

インライン作成：

インラインで指定された実行パラメータ (インラインで実行パラメータを指定する場合は引用符をエスケープ) を指定して create RFC コマンドを発行し、返された RFC ID を送信します。たとえば、コンテンツを次のような内容に置き換えることができます。

```
aws --profile saml amscm create-rfc --change-type-id "ct-1dmlg9g1l91h6" --change-type-
version "3.0" --title "Stack-Admin-Access-QC" --execution-parameters "{\"DomainFQDN
\":\"TEST.com\",\"StackIds\":[\"stack-01234567890abcdef\"],\"TimeRequestedInHours\":1,
\"Usernames\":[\"TEST\"],\"VpcId\":\"VPC_ID\"}"
```

テンプレートの作成：

1. この変更タイプの実行パラメータ JSON スキーマをファイルに出力します。この例では GrantAdminAccessParams.json:

   ```
   aws amscm get-change-type-version --change-type-id "ct-1dmlg9g1l91h6"
    --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
    GrantAdminAccessParams.json
   ```

   GrantAdminAccessParams ファイルを変更して保存します。たとえば、コンテンツを次のような内容に置き換えることができます。

   ```
   {
   ```

```
"DomainFQDN":           "mycorpdomain.acme.com",
"StackIds":             [STACK_ID, STACK_ID],
"TimeRequestedInHours": 12,
"Username":             ["USERNAME", "USERNAME"],
"VpcId":                "VPC_ID"
}
```

TimeRequestedInHours オプションはデフォルトで 1 時間であることに注意してください。最大 12 時間リクエストできます。

2. RFC テンプレートを現在のフォルダ内のファイルに出力します。この例では GrantAdminAccessRfc.json:

```
aws amscm create-rfc --generate-cli-skeleton > GrantAdminAccessRfc.json
```

3. GrantAdminAccessRfc.json ファイルを変更して保存します。たとえば、コンテンツを次のような内容に置き換えることができます。

```
{
"ChangeTypeId":         "ct-1dmlg9g1l91h6",
"ChangeTypeVersion":    "3.0",
"Title":                "Request-Admin-Access-to-EC2-RFC"
}
```

4. RFC を作成し、GrantAdminAccessRfc ファイルと GrantAdminAcessParams ファイルを指定します。

```
aws amscm create-rfc --cli-input-json file://GrantAdminAccessRfc.json --execution-
parameters file://GrantAdminAccessParams.json
```

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

踏み台を介してインスタンスにログインするには、次の手順「インスタンスアクセスの例」に従います。

ヒント

> **Note**
>
> アクセスリクエストの更新は、有効期限が切れる前に送信できます。詳細については、「スタック管理者アクセス | 更新」を参照してください。
> ASG の一部であるインスタンスにログインするには、関連するすべてのインスタンスにアクセスできる ASG スタックへのアクセスをリクエストします。

ReadOnly アクセスのリクエストの例については、ReadOnly access: requesting」を参照してください。

ReadOnly アクセスをリクエストする

コンソールを使用した ReadOnly アクセスのリクエスト

AMS コンソールでこの変更タイプを以下に示します。

仕組み：

1. RFC の作成ページに移動します。AMS コンソールの左側のナビゲーションペインでRFCs をクリックして RFCsリストページを開き、RFC の作成をクリックします。
2. デフォルトの変更タイプ参照ビューで一般的な変更タイプ (CT) を選択するか、カテゴリ別選択ビューで CT を選択します。
   - 変更タイプ別に参照: クイック作成エリアで一般的な CT をクリックすると、すぐに RFC の実行ページを開くことができます。クイック作成で古い CT バージョンを選択することはできません。

     CTs をソートするには、カードビューまたはテーブルビューですべての変更タイプエリアを使用します。どちらのビューでも、CT を選択し、RFC の作成をクリックして RFC の実行ページを開きます。必要に応じて、RFC の作成ボタンの横に古いバージョンで作成オプションが表示されます。
   - カテゴリ別に選択: カテゴリ、サブカテゴリ、項目、オペレーションを選択すると、CT 詳細ボックスが開き、必要に応じて古いバージョンで作成するオプションが表示されます。RFC の作成をクリックして、RFC の実行ページを開きます。

3. RFC の実行ページで、CT 名エリアを開き、CT の詳細ボックスを表示します。件名は必須です (変更タイプの参照ビューで CT を選択した場合は入力されます) 。追加設定エリアを開き、RFC に関する情報を追加します。

   実行設定領域で、使用可能なドロップダウンリストを使用するか、必要なパラメータの値を入力します。オプションの実行パラメータを設定するには、追加設定エリアを開きます。

4. 完了したら、実行 をクリックします。エラーがない場合、RFC が正常に作成されたページに、送信された RFC の詳細と最初の実行出力が表示されます。

5. Run parameters エリアを開き、送信した設定を確認します。ページを更新して RFC 実行ステータスを更新します。必要に応じて、RFC をキャンセルするか、ページ上部のオプションを使用してコピーを作成します。

CLI を使用した ReadOnly アクセスのリクエスト

仕組み：

1. インライン作成 (すべての RFC と実行パラメータを含むcreate-rfcコマンドを発行) またはテンプレート作成 (2 つの JSON ファイルを作成し、1 つは RFC パラメータ用、もう 1 つは実行パラメータ用) のいずれかを使用し、2 つのファイルを入力としてcreate-rfcコマンドを発行します。どちらの方法もここで説明します。

2. 返された RFC ID を使用して RFC: `aws amscm submit-rfc --rfc-id` *`ID`* コマンドを送信します。

   RFC: `aws amscm get-rfc --rfc-id` *`ID`* コマンドをモニタリングします。

変更タイプのバージョンを確認するには、次のコマンドを使用します。

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> 変更タイプのスキーマの一部であるかどうかにかかわらず、任意の RFC で任意のCreateRfcパラメータを使用できます。たとえば、RFC ステータスが変更されたときに通知を受け取るには、リクエストの RFC パラメータ部分 (実行パラメータではなく) `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com`

\"]}}"にこの行を追加します。すべての CreateRfc パラメータのリストについては、AMS 変更管理 API リファレンスを参照してください。

インライン作成：

インラインで指定された実行パラメータ (インラインで実行パラメータを指定する場合は引用符を エスケープ) を指定して create RFC コマンドを発行し、返された RFC ID を送信します。たとえば、コンテンツを次のような内容に置き換えることができます。

```
aws --profile saml amscm create-rfc --change-type-id "ct-199h35t7uz6jl" --change-type-
version "3.0" --title "Stack-RO-Access-QC" --execution-parameters "{\"DomainFQDN\":
\"TEST.com\",\"StackIds\":[\"stack-01234567890abcdef\"],\"TimeRequestedInHours\":1,
\"Usernames\":[\"TEST\"],\"VpcId\":\"VPC_ID\"}"
```

テンプレートの作成：

1. この変更タイプの実行パラメータ JSON スキーマをファイルに出力します。この例では GrantReadOnlyAccessParams.json:

   ```
   aws amscm get-change-type-version --change-type-id "ct-199h35t7uz6jl"
    --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
    GrantReadOnlyAccessParams.json
   ```

   GrantReadOnlyAccessParams ファイルを変更して保存します。たとえば、コンテンツを次のような内容に置き換えることができます。

   ```
   {
   "DomainFQDN":           "mycorpdomain.acme.com",
   "StackIds":             [STACK_ID, STACK_ID],
   "TimeRequestedInHours": 12,
   "Usernames":             ["USERNAME", "USERNAME"],
   "VpcId":                "VPC_ID"
   }
   ```

   TimeRequestedInHours オプションはデフォルトで 1 時間であることに注意してください。最大 12 時間リクエストできます。

2. RFC テンプレートを現在のフォルダ内のファイルに出力します。この例では GrantReadOnlyAccessRfc.json:

```
aws amscm create-rfc --generate-cli-skeleton > GrantReadOnlyAccessRfc.json
```

3. GrantReadOnlyAccessRfc.json ファイルを変更して保存します。たとえば、コンテンツを次のような内容に置き換えることができます。

```
{
"ChangeTypeId":          "ct-199h35t7uz6jl",
"ChangeTypeVersion":     "3.0",
"Title":                 "Request-ReadOnly-Access-to-EC2-RFC"
}
```

4. RFC を作成し、GrantReadOnlyAccessRfc ファイルと GrantReadOnlyAcessParams ファイルを指定します。

```
aws amscm create-rfc --cli-input-json file://GrantReadOnlyAccessRfc.json --
execution-parameters file://GrantReadOnlyAccessParams.json
```

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

踏み台を介してインスタンスにログインするには、次の手順「インスタンスアクセスの例」に従います。

ヒント

> **Note**
>
> アクセスリクエストの更新は、有効期限が切れる前に送信できます。詳細については、「Stack Read-Only Access | Update」を参照してください。
> EC2 Auto Scaling グループ (ASG) の一部であるインスタンスにログインするには、関連するすべてのインスタンスにアクセスできる ASG スタックへのアクセスをリクエストします。

管理者アクセスをリクエストするチュートリアルについては、「管理者アクセス: リクエスト」を参照してください。

その他 | その他の RFC、作成 (CLI)

この例では、 Management | Other | Other | Create CT (ct-1e1xtak34nx76) を使用して、使用可能な CTs がアドレス指定しない変更をリクエストする方法を示します。

この CT は、目的の変更タイプが見つからない場合に使用します。ただし、既存の CT でパラメータを指定するかどうか不明な場合は、サービスリクエストを送信してヘルプを求めることをお勧めします。サービスリクエストの送信については、「サービスリクエストの例」を参照してください。

このタイプの RFC は承認が必要です。つまり、実装する前に AMS 承認が必要です。RFC を送信すると、AMS オペレーターから連絡があり、デプロイするスタックについて説明します。

> **Note**
>
> 「レビュー必須」CT を使用する場合、AMS では ASAP スケジューリングオプション (コンソールで ASAP を選択し、API/CLI で開始時刻と終了時刻を空白のままにしておく) を使用することをお勧めします。これらの CTs では、AMS オペレータが RFC を調べ、承認して実行する前にお客様と通信する必要があるためです。これらの RFCsスケジュールする場合は、少なくとも 24 時間かかります。スケジュールされた開始時刻より前に承認が行われない場合、RFC は自動的に拒否されます。

必須データ：

- `Comment`: RFC の用途。
- `ChangeTypeId` および `ChangeTypeVersion`: その他を使用する | 新しいリソースをリクエストするには (`ct-1e1xtak34nx76`) を作成し、その他 | 更新 (`ct-0xdawir96cy7k`) を使用して既存のリソースを変更します。どちらも ですv1。

オプションデータ: `Priority`: 使用できる値は、`High`、`Medium`、または ですLow。

インライン作成：

- インラインで指定された実行パラメータ (インラインで実行パラメータを指定する場合は引用符をエスケープ) を使用して、create RFC コマンドを発行します。この例では、その他 | 作成を使用します。

```
aws amscm create-rfc --change-type-id "ct-1e1xtak34nx76" --change-type-version "1.0"
 --title "TITLE" --execution-parameters "{\"Comment\": \"What you want created\"}"
```

- RFC の作成オペレーションで返された RFC ID を使用して RFC を送信します。送信されるまで、RFC は Editing状態のままであり、 に対して動作しません。

```
aws amscm submit-rfc --rfc-id RFC_ID
```

- RFC ステータスをモニタリングし、実行出力を表示します。

```
aws amscm get-rfc --rfc-id RFC_ID
```

テンプレートの作成：

1. 実行パラメータの JSON ファイルを作成して保存します。例では OtherParams.json という名前を付け、オプションのPriorityパラメータを含めます。

```
{
"Comment":          "What you want created",
"Priority":         "Medium"
}
```

2. RFC パラメータの JSON ファイルを作成して保存します。例名は OtherRfc.json.

```
{
"ChangeTypeId":         "ct-1e1xtak34nx76",
"ChangeTypeVersion":    "1.0",
"Title":                "TITLE"
}
```

3. RFC を作成し、OtherRfc ファイルと OtherParams ファイルを指定します。

```
aws amscm create-rfc --cli-input-json file://OtherRfc.json  --execution-parameters
 file://OtherParams.json
```

レスポンスで新しい RFC の RfcId を受け取ります。例:

```
{
"RfcId": "RFC-ID"
```

```
}
```

4. RFC を送信します。

```
aws amscm submit-rfc --rfc-id RFC-ID
```

エラーが報告されない場合、オペレーションは成功しました。

5. リクエストのステータスをモニタリングし、実行出力を表示するには：

```
aws amscm get-rfc --rfc-id RFC-ID
```

スタック: 削除、再起動、開始、停止

AMS コンソールまたは API/CLI を使用して、AMS スタックを削除、再起動、開始、または停止できます。

スタックの削除

コンソールを使用したスタックの削除

AMS コンソールでのこの変更タイプのスクリーンショット：

仕組み：

1. RFC の作成ページに移動します。AMS コンソールの左側のナビゲーションペインでRFCs をクリックして RFCsリストページを開き、RFC の作成をクリックします。
2. デフォルトの変更タイプ参照ビューで一般的な変更タイプ (CT) を選択するか、カテゴリ別選択ビューで CT を選択します。
   - 変更タイプ別に参照: クイック作成エリアで一般的な CT をクリックすると、すぐに RFC の実行ページを開くことができます。クイック作成で古い CT バージョンを選択することはできません。

     CTs をソートするには、カードビューまたはテーブルビューですべての変更タイプエリアを使用します。どちらのビューでも、CT を選択し、RFC の作成をクリックして RFC の実行ページを開きます。必要に応じて、RFC の作成ボタンの横に古いバージョンで作成オプションが表示されます。

- カテゴリ別に選択: カテゴリ、サブカテゴリ、項目、オペレーションを選択すると、CT 詳細ボックスが開き、必要に応じて古いバージョンで作成するオプションが表示されます。RFC の作成をクリックして、RFC の実行ページを開きます。

3. RFC の実行ページで、CT 名エリアを開き、CT の詳細ボックスを表示します。件名は必須です (変更タイプの参照ビューで CT を選択した場合は入力されます) 。追加設定エリアを開き、RFC に関する情報を追加します。

   実行設定領域で、使用可能なドロップダウンリストを使用するか、必要なパラメータの値を入力します。オプションの実行パラメータを設定するには、追加設定エリアを開きます。
4. 完了したら、実行 をクリックします。エラーがない場合、RFC が正常に作成されたページに、送信された RFC の詳細と最初の実行出力が表示されます。
5. Run parameters 領域を開き、送信した設定を確認します。ページを更新して RFC 実行ステータスを更新します。必要に応じて、RFC をキャンセルするか、ページ上部のオプションを使用してコピーを作成します。

CLI を使用したスタックの削除

仕組み：

1. インライン作成 (すべての RFC と実行パラメータを含むcreate-rfcコマンドを発行) またはテンプレート作成 (2 つの JSON ファイルを作成します。1 つは RFC パラメータ用、もう 1 つは実行パラメータ用) のいずれかを使用し、2 つのファイルを入力としてcreate-rfcコマンドを発行します。どちらの方法もここで説明します。
2. 返された RFC ID を使用して RFC: `aws amscm submit-rfc --rfc-id` *`ID`* コマンドを送信します。

   RFC: `aws amscm get-rfc --rfc-id` *`ID`* コマンドをモニタリングします。

変更タイプのバージョンを確認するには、次のコマンドを使用します。

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> 変更タイプのスキーマの一部であるかどうかにかかわらず、任意の RFC で任意のCreateRfcパラメータを使用できます。たとえば、RFC ステータスが変更されたとき

に通知を受け取るには、リクエストの RFC パラメータ部分 (実行パラメータではなく) --notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"にこの行を追加します。すべての CreateRfc パラメータのリストについては、AMS 変更管理 API リファレンスを参照してください。

インライン作成：

インラインで指定された実行パラメータ (インラインで実行パラメータを指定する場合は引用符を エスケープ) を指定して create RFC コマンドを発行し、返された RFC ID を送信します。たとえば、コンテンツを次のような内容に置き換えることができます。

```
aws amscm create-rfc --change-type-id "ct-0q0bic0ywqk6c" --change-type-version "1.0" --
title "Delete My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

テンプレートの作成：

1. RFC テンプレートを現在のフォルダ内のファイルに出力します。この例では DeleteStackRfc.json:

   ```
   aws amscm create-rfc --generate-cli-skeleton > DeleteStackRfc.json
   ```

2. DeleteStackRfc.json ファイルを変更して保存します。

   ExecutionParameters JSON 拡張機能の内部引用符は、バックスラッシュ (\) で エスケープする必要があります。開始時刻と終了時刻のない例：

   ```
   {
   "ChangeTypeVersion":    "1.0",
   "ChangeTypeId":         "ct-0q0bic0ywqk6c",
   "Title":                "Delete-My-Stack-RFC"
   "ExecutionParameters":  "{
           \"StackId\":\"STACK_ID\"}"
   }
   ```

3. RFC を作成します。

   ```
   aws amscm create-rfc --cli-input-json file://DeleteStackRfc.json
   ```

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

ヒント

> **Note**
>
> S3 バケットを削除する場合は、まずオブジェクトを空にする必要があります。

> **Important**
>
> スタックを削除すると、望ましくない予期しない結果が生じる可能性があります。重要な注意事項については、「RFC Troubleshooting section RFCs for Delete Stack」を参照してください。

スタックを再起動する

コンソールを使用したスタックの再起動

AMS コンソールでのこの変更タイプのスクリーンショット：

仕組み：

1. RFC の作成ページに移動します。AMS コンソールの左側のナビゲーションペインでRFCs をクリックして RFCsリストページを開き、RFC の作成をクリックします。
2. デフォルトの変更タイプ参照ビューで一般的な変更タイプ (CT) を選択するか、カテゴリ別選択ビューで CT を選択します。
   - 変更タイプ別に参照: クイック作成エリアで一般的な CT をクリックすると、すぐに RFC の実行ページを開くことができます。クイック作成で古い CT バージョンを選択することはできません。

     CTs をソートするには、カードビューまたはテーブルビューですべての変更タイプ領域を使用します。どちらのビューでも、CT を選択し、RFC の作成をクリックして RFC の実行ページを開きます。必要に応じて、RFC の作成ボタンの横に古いバージョンで作成オプションが表示されます。

- カテゴリ別に選択: カテゴリ、サブカテゴリ、項目、オペレーションを選択すると、CT 詳細ボックスが開き、必要に応じて古いバージョンで作成するオプションが表示されます。RFC の作成をクリックして、RFC の実行ページを開きます。

3. RFC の実行ページで、CT 名エリアを開き、CT の詳細ボックスを表示します。件名は必須です (変更タイプの参照ビューで CT を選択した場合は入力されます) 。追加設定エリアを開き、RFC に関する情報を追加します。

   実行設定領域で、使用可能なドロップダウンリストを使用するか、必要なパラメータの値を入力します。オプションの実行パラメータを設定するには、追加設定エリアを開きます。
4. 完了したら、実行 をクリックします。エラーがない場合、RFC が正常に作成されたページに、送信された RFC の詳細と最初の実行出力が表示されます。
5. Run parameters エリアを開き、送信した設定を確認します。ページを更新して RFC 実行ステータスを更新します。必要に応じて、RFC をキャンセルするか、ページ上部のオプションを使用してコピーを作成します。

CLI を使用したスタックの再起動

仕組み：

1. インライン作成 (すべての RFC と実行パラメータを含むcreate-rfcコマンドを発行) またはテンプレート作成 (2 つの JSON ファイルを作成します。1 つは RFC パラメータ用、もう 1 つは実行パラメータ用) のいずれかを使用し、2 つのファイルを入力としてcreate-rfcコマンドを発行します。どちらの方法もここで説明します。
2. 返された RFC ID を使用して RFC: `aws amscm submit-rfc --rfc-id` *`ID`* コマンドを送信します。

   RFC: `aws amscm get-rfc --rfc-id` *`ID`* コマンドをモニタリングします。

変更タイプのバージョンを確認するには、次のコマンドを使用します。

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> 変更タイプのスキーマの一部であるかどうかにかかわらず、任意の RFC で任意のCreateRfcパラメータを使用できます。たとえば、RFC ステータスが変更されたとき

に通知を受け取るには、リクエストの RFC パラメータ部分 (実行パラメータではなく) --notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"にこの行を追加します。すべての CreateRfc パラメータのリストについては、AMS 変更管理 API リファレンスを参照してください。

インライン作成：

インラインで指定された実行パラメータ (インラインで実行パラメータを指定する場合は引用符をエスケープ) を指定して create RFC コマンドを発行し、返された RFC ID を送信します。たとえば、コンテンツを次のような内容に置き換えることができます。

```
aws amscm create-rfc --change-type-id "ct-02u0hoaa9grat" --change-type-version "1.0" --title "Reboot My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

テンプレートの作成：

1. RFC テンプレートを現在のフォルダ内のファイルに出力します。この例では、RebootStackRfc.json. インスタンスを停止 (再起動または開始) するための実行パラメータは 1 つしかないため、実行パラメータはスキーマ JSON ファイル自体に含めることができ、個別の実行パラメータ JSON ファイルを作成する必要はありません。

   ```
   aws amscm create-rfc --generate-cli-skeleton > StopInstanceRfc.json
   ```

2. RebootStackRfc.json ファイルを変更して保存します。

   JSON 拡張機能の内部引用符は、バックスラッシュ (\) ExecutionParameters でエスケープする必要があります。例:

   ```
   {
   "ChangeTypeId":          "ct-02u0hoaa9grat",
   "Title":                 "Reboot-My-EC2-RFC",
   "TimeoutInMinutes":      60,
   "ExecutionParameters":   "{
           \"StackId\":\"STACK_ID\"
       }"
   }
   ```

3. RFC を作成します。

```
aws amscm create-rfc --cli-input-json file://RebootStackRfc.json
```

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

ヒント

Application Load Balancer の詳細については、「Application Load Balancer」を参照してください。

スタックの開始

コンソールでスタックを開始する

AMS コンソールでのこの変更タイプのスクリーンショット：

仕組み：

1. RFC の作成ページに移動します。AMS コンソールの左側のナビゲーションペインでRFCs をクリックして RFCsリストページを開き、RFC の作成をクリックします。
2. デフォルトの変更タイプ参照ビューで一般的な変更タイプ (CT) を選択するか、カテゴリ別選択ビューで CT を選択します。
   - 変更タイプ別に参照: クイック作成エリアで一般的な CT をクリックすると、すぐに RFC の実行ページを開くことができます。クイック作成で古い CT バージョンを選択することはできません。

     CTs をソートするには、カードビューまたはテーブルビューですべての変更タイプ領域を使用します。どちらのビューでも、CT を選択し、RFC の作成をクリックして RFC の実行ページを開きます。必要に応じて、RFC の作成ボタンの横に古いバージョンで作成オプションが表示されます。
   - カテゴリ別に選択: カテゴリ、サブカテゴリ、項目、オペレーションを選択すると、CT 詳細ボックスが開き、必要に応じて古いバージョンで作成するオプションが表示されます。RFC の作成をクリックして、RFC の実行ページを開きます。
3. RFC の実行ページで、CT 名エリアを開き、CT の詳細ボックスを表示します。件名は必須です (変更タイプの参照ビューで CT を選択した場合は入力されます) 。追加設定エリアを開き、RFC に関する情報を追加します。

実行設定領域で、使用可能なドロップダウンリストを使用するか、必要なパラメータの値を入力します。オプションの実行パラメータを設定するには、追加設定エリアを開きます。

4. 完了したら、実行 をクリックします。エラーがない場合、RFC が正常に作成されたページに、送信された RFC の詳細と最初の実行出力が表示されます。
5. Run parameters 領域を開き、送信した設定を確認します。ページを更新して RFC 実行ステータスを更新します。必要に応じて、RFC をキャンセルするか、ページ上部のオプションを使用してコピーを作成します。

CLI でスタックを開始する

仕組み：

1. インライン作成 (すべての RFC と実行パラメータを含むcreate-rfcコマンドを発行) またはテンプレート作成 (2 つの JSON ファイルを作成し、1 つは RFC パラメータ用、もう 1 つは実行パラメータ用) のいずれかを使用し、2 つのファイルを入力としてcreate-rfcコマンドを発行します。どちらの方法もここで説明します。
2. 返された RFC ID を使用して RFC: `aws amscm submit-rfc --rfc-id ID` コマンドを送信します。

   RFC: `aws amscm get-rfc --rfc-id ID` コマンドをモニタリングします。

変更タイプのバージョンを確認するには、次のコマンドを使用します。

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> 変更タイプのスキーマの一部であるかどうかにかかわらず、任意の RFC で任意のCreateRfcパラメータを使用できます。たとえば、RFC ステータスが変更されたときに通知を受け取るには、リクエストの RFC パラメータ部分 (実行パラメータではなく) `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"`にこの行を追加します。すべての CreateRfc パラメータのリストについては、AMS 変更管理 API リファレンスを参照してください。

インライン作成：

インラインで指定された実行パラメータ (インラインで実行パラメータを指定する場合は引用符を エスケープ) を指定して create RFC コマンドを発行し、返された RFC ID を送信します。たとえば、コンテンツを次のような内容に置き換えることができます。

```
aws amscm create-rfc --change-type-id "ct-1h5xgl9cr4bzy" --change-type-version "1.0" --
title "Start My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

テンプレートの作成：

1. RFC テンプレートを現在のフォルダ内のファイルに出力します。この例で は、StartInstanceRfc.json. スタックを開始するための実行パラメータは 1 つしかないため、実行パラメータはスキーマ JSON ファイル自体に含めることができ、個別の実行パラメータ JSON ファイルを作成する必要はありません。

   ```
   aws amscm create-rfc --generate-cli-skeleton > StartStackRfc.json
   ```

2. StartStackRfc.json ファイルを変更して保存します。たとえば、コンテンツを次のような内容に置き換えることができます。

   ```
   {
   "ChangeTypeId":          "ct-1h5xgl9cr4bzy",
   "Title":                 "Start-My-EC2-RFC",
   "TimeoutInMinutes":      60,
   "ExecutionParameters":   "{
           \"StackId\":\"STACK_ID\"
       }"
   }
   ```

3. RFC を作成します。

   ```
   aws amscm create-rfc --cli-input-json file://StartStackRfc.json
   ```

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

ヒント

Application Load Balancer の詳細については、「Application Load Balancer」を参照してください。

スタックを停止する

コンソールを使用したスタックの停止

AMS コンソールでのこの変更タイプのスクリーンショット：

仕組み：

1. RFC の作成ページに移動します。AMS コンソールの左側のナビゲーションペインでRFCs をクリックして RFCsリストページを開き、RFC の作成をクリックします。
2. デフォルトの変更タイプ参照ビューで一般的な変更タイプ (CT) を選択するか、カテゴリ別選択ビューで CT を選択します。
   - 変更タイプ別に参照: クイック作成エリアで一般的な CT をクリックすると、すぐに RFC の実行ページを開くことができます。クイック作成で古い CT バージョンを選択することはできません。

     CTsソートするには、カードビューまたはテーブルビューですべての変更タイプ領域を使用します。どちらのビューでも、CT を選択し、RFC の作成をクリックして RFC の実行ページを開きます。必要に応じて、RFC の作成ボタンの横に古いバージョンで作成オプションが表示されます。
   - カテゴリ別に選択: カテゴリ、サブカテゴリ、項目、オペレーションを選択すると、CT 詳細ボックスが開き、必要に応じて古いバージョンで作成するオプションが表示されます。RFC の作成をクリックして、RFC の実行ページを開きます。
3. RFC の実行ページで、CT 名エリアを開き、CT の詳細ボックスを表示します。件名は必須です (変更タイプの参照ビューで CT を選択した場合は入力されます) 。追加設定エリアを開き、RFC に関する情報を追加します。

   実行設定領域で、使用可能なドロップダウンリストを使用するか、必要なパラメータの値を入力します。オプションの実行パラメータを設定するには、追加の設定領域を開きます。
4. 完了したら、実行 をクリックします。エラーがない場合、RFC が正常に作成されたページに、送信された RFC の詳細と最初の実行出力が表示されます。
5. Run parameters 領域を開き、送信した設定を確認します。ページを更新して RFC 実行ステータスを更新します。必要に応じて、RFC をキャンセルするか、ページ上部のオプションを使用してコピーを作成します。

CLI を使用したスタックの停止

仕組み：

1. インライン作成 (すべての RFC と実行パラメータを含むcreate-rfcコマンドを発行) またはテンプレート作成 (2 つの JSON ファイルを作成し、1 つは RFC パラメータ用、もう 1 つは実行パラメータ用) のいずれかを使用し、2 つのファイルを入力としてcreate-rfcコマンドを発行します。どちらの方法もここで説明します。
2. 返された RFC ID を使用して RFC: `aws amscm submit-rfc --rfc-id ID` コマンドを送信します。

   RFC: `aws amscm get-rfc --rfc-id ID` コマンドをモニタリングします。

変更タイプのバージョンを確認するには、次のコマンドを使用します。

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> 変更タイプのスキーマの一部であるかどうかにかかわらず、任意の RFC で任意のCreateRfcパラメータを使用できます。たとえば、RFC ステータスが変更されたときに通知を受け取るには、リクエストの RFC パラメータ部分 (実行パラメータではなく) `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"`にこの行を追加します。すべての CreateRfc パラメータのリストについては、AMS 変更管理 API リファレンスを参照してください。

インライン作成：

インラインで指定された実行パラメータ (インラインで実行パラメータを指定する場合は引用符をエスケープ) を指定して create RFC コマンドを発行し、返された RFC ID を送信します。たとえば、コンテンツを次のような内容に置き換えることができます。

```
aws amscm create-rfc --change-type-id "ct-3dgbnh6gpst4d" --change-type-version "1.0" --
title "Stop My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

テンプレートの作成：

1. RFC テンプレートを現在のフォルダ内のファイルに出力します。この例では、StopStackRfc.json. インスタンスを停止 (再起動または開始) するための実行パラメータは 1 つしかないため、実行パラメータはスキーマ JSON ファイル自体に含めることができ、個別の実行パラメータ JSON ファイルを作成する必要はありません。

```
aws amscm create-rfc --generate-cli-skeleton > StopStackRfc.json
```

2. StopStackRfc.json ファイルを変更して保存します。たとえば、コンテンツを次のような内容に置き換えることができます。

```
{
"ChangeTypeId":          "ct-3dgbnh6gpst4d",
"Title":                 "Stop-My-EC2-RFC",
"TimeoutInMinutes":      60,
"ExecutionParameters":   "{
        \"StackId\":\"STACK_ID\"
    }"
}
```

3. RFC を作成します。

```
aws amscm create-rfc --cli-input-json file://StopInstanceRfc.json
```

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

ヒント

AMS Resource Scheduler を使用して再起動をスケジュールしない限り、停止したインスタンスは停止したままになります。

必要に応じて、EC2 インスタンススタックの停止が失敗する」を参照してください。

アクセスの例

これらの例は、RFC を通じてアクセス権が付与されたら、踏み台を介してインスタンスにログインする方法を示しています。アクセス許可の取得の詳細については、「アクセスリクエスト」を参照してください。

> **Note**
>
> Auto Scaling グループを介して作成された EC2 インスタンスには、入出力をサイクルする IP アドレスがあり、EC2 コンソールを使用してその IP アドレスを見つける必要があります。

必要なデータ：

- 踏み台 DNS フレンドリ名または IP アドレス: 「」で説明されているように DNS フレンドリ名を使用するDNS フレンドリ踏み台名か、「」で説明されているように踏み台 IP アドレスを見つけます踏み台 IP アドレスの検索。
- ユーザー名 (username@customerdomain.com など) とパスワード: アカウントの認証情報。
- スタック IP アドレス: これを取得するには、ログインするスタックの AMS コンソールスタックページを確認し、アカウントの EC2 コンソールでそのスタック ID をフィルタリングします。単一の EC2 インスタンスの場合は、AMS SKMS コマンドを使用することもできます。AMS SKMS API リファレンスの場合は、AWS Artifact コンソールのレポートタブを参照してください。スタック ID を見つけるには、AMS SKMS API リファレンスの場合は、AWS Artifact コンソールのレポートタブを参照してください。スタック IP アドレスを見つけるには、 を参照してください。

必要に応じて踏み台 IP アドレス SSH または RDP にアクセスし、次のいずれかの手順を使用してログインします。

Linux コンピュータから Linux インスタンスへ

SSH を使用して SSH 踏み台に接続し、次に Linux インスタンスに接続します。

MALZ

フレンドリ踏み台名の詳細については、「DNS 踏み台」を参照してください。

Linux インスタンスに接続するには、まず SSH 踏み台に接続する必要があります。

1. シェルウィンドウを開き、次のように入力します。

```
ssh Domain_FQDN\\Username@SSH_bastion_name
    or SSH_bastion_IP
```

Domain_FQDN が「corp.domain.com」、アカウント番号が「123456789123」、Your_Domain が「amazonaws.com」、踏み台「4」、ユーザー名が JoeSmith」の場合、次のようになります。

```
ssh corp.domain.com\\JoeSmith sshbastion4.A123456789123.amazonaws.com
```

2. 会社の Active Directory 認証情報を使用してログインします。
3. Bash プロンプトが表示されたら、インスタンスに SSH インし、次のように入力します。

```
ssh Domain_FQDN\\Username@Instance_IP
```

または、Login フラグ (-l) を使用できます。

```
ssh -l Domain_FQDN\\Username@Instance_IP
```

SALZ

フレンドリ踏み台名の詳細については、「DNS 踏み台」を参照してください。

Linux インスタンスに接続するには、まず SSH 踏み台に接続する必要があります。

1. シェルウィンドウを開き、次のように入力します。

```
ssh DOMAIN_FQDN\\USERNAME@SSH_BASTION_name
    or SSH_BASTION_IP
```

アカウント番号が 123456789123 で、踏み台 4 を選択し、ユーザー名が JoeSmith の場合、次のようになります。

```
ssh corp.domain.com\\JoeSmith sshbastion1.A123456789123.amazonaws.com
```

2. 会社の Active Directory 認証情報を使用してログインします。
3. Bash プロンプトが表示されたら、インスタンスに SSH インし、次のように入力します。

```
ssh DOMAIN_FQDN\\USERNAME@INSTANCE_IP
```

または、Login フラグ (-l) を使用できます。

```
ssh -l DOMAIN_FQDN\\USERNAME@INSTANCE_IP
```

Linux コンピュータから Windows インスタンスへ

SSH トンネルと RDP クライアントを使用して、Linux コンピュータから Windows インスタンスに接続します。

MALZ

この手順では、Linux 用のリモートデスクトップ接続クライアントが必要です。この例では、Microsoft リモートデスクトップ (Windows リモートデスクトップサービスに接続するためのオープンソースの UNIX クライアント) を使用します。Rdesktop は代替手段です。

> **Note**
>
> Windows インスタンスへのログイン方法は、使用しているリモートデスクトップクライアントによって異なる場合があります。

まず SSH トンネルを確立してからログインします。

フレンドリ踏み台名の詳細については、「」を参照してくださいDNS フレンドリ踏み台名。

開始する前に:

- 接続するインスタンスへのアクセスをリクエストします。詳細については、「アクセスリクエスト」を参照してください。
- 接続するわかりやすい DNS SSH 踏み台名を選択します。次に例を示します。

  ```
  sshbastion(1-4).Your_Domain
  ```

  Domain_FQDN が「corp.domain.com」で、AMS が管理する Your_Domain が「amazonaws.com」で、踏み台「4」を選択し、ユーザー名がJoeSmith」の場合、次のようになります。

  ```
  ssh corp.domain.com\\JoeSmith sshbastion4.amazonaws.com
  ```

- 接続するインスタンスの IP アドレスを見つけます。詳細については、「インスタンス ID または IP アドレスの検索」を参照してください。

1. Linux デスクトップから Windows インスタンスへの SSH トンネル経由で RDP を設定します。正しい値でsshコマンドを発行するには、いくつかの方法があります。

   - Linux シェルで変数を設定し、SSH 接続コマンドを入力します。

     ```
     BASTION="sshbastion(1-4).Your_Domain""
     WINDOWS="Windows_Instance_Private_IP"
     AD="AD_Account_Number"
     USER="AD_Username"
     ssh -L 3389:$WINDOWS:3389 A$AD\\\\$USER@$BASTION
     ```

     たとえば、次の値を使用する場合です。

     BASTION="sshbastion4.A123456789123.amazonaws.com"

     WINDOWS="172.16.3.254"

     AD="ACORP_example"

     USER="john.doe"

   - 変数値を ssh コマンドに直接追加します。

   いずれの場合も、レンダリングされたリクエストは次のようになります (変数値の同じセットを想定) 。

   ```
   ssh -L 3389:172.16.3.254:3389 ACORP_example\\\\john.doe@myamsadomain.com
   ```

2. どちらか: リモートデスクトップクライアントを開き、ループバックアドレスとポート 127.0.0.1:3389 を入力し、接続を開きます。

   または、新しい Linux デスクトップシェルから Windows インスタンスにログインします。RDesktop を使用する場合、コマンドは次のようになります。

   ```
   rdesktop 127.0.0.1:3389
   ```

Windows インスタンスのリモートデスクトップウィンドウが Linux デスクトップに表示されます。

> **Tip**
>
> リモートデスクトップセッションの開始に失敗した場合、SSH 踏み台からの Windows インスタンスへのネットワーク接続が、ステップ 1 のシェルからのポート 3389 で許可されていることを確認します (`private_ip_address_of_windows_instance`適切に置き換えてください)。
>
> ```
> nc private_ip_address_of_windows_instance 3389 -v -z
> ```
>
> 成功：
>
> ```
> nc 172.16.0.83 3389 -v -z
>         Connection to 172.16.0.83 3389 port [tcp/ms-wbt-server] succeeded
>         netstat -anvp | grep 3389
>         tcp    0     0 172.16.0.253:48079 172.16.3.254:3389 ESTABLISHED
> ```

SALZ

シングルアカウントランディングゾーンのこの手順では、Linux 用のリモートデスクトップ接続クライアントが必要です。この例では、Microsoft リモートデスクトップ (Windows リモートデスクトップサービスに接続するためのオープンソースの UNIX クライアント) を使用します。Rdesktop は代替手段です。

> **Note**
>
> Windows インスタンスへのログイン方法は、使用しているリモートデスクトップクライアントによって異なる場合があります。

まず SSH トンネルを確立してからログインします。

フレンドリ踏み台名の詳細については、「」を参照してくださいDNS フレンドリ踏み台名。

開始する前に:

- 接続するインスタンスへのアクセスをリクエストします。詳細については、「アクセスリクエスト」を参照してください。
- 接続するわかりやすい DNS SSH 踏み台名を選択します。次に例を示します。

```
sshbastion(1-4).AAMSAccountNumber.amazonaws.com
```

アカウント番号が 123456789123 で、踏み台 4 を選択した場合、次のようになります。

```
sshbastion4.A123456789123.amazonaws.com
```

- 接続するインスタンスの IP アドレスを見つけます。詳細については、「インスタンス ID または IP アドレスの検索」を参照してください。

1. Linux デスクトップから Windows インスタンスへの SSH トンネル経由で RDP を設定します。正しい値でsshコマンドを発行するには、いくつかの方法があります。

   - Linux シェルで変数を設定し、SSH 接続コマンドを入力します。

   ```
   BASTION="sshbastion(1-4).AAMSAccountNumber.amazonaws.com"
   WINDOWS="WINDOWS_INSTANCE_PRIVATE_IP"
   AD="AD_ACCOUNT_NUMBER"
   USER="AD_USERNAME"
   ssh -L 3389:$WINDOWS:3389 A$AD\\\\$USER@$BASTION
   ```

   たとえば、次の値を使用する場合です。

   ```
   BASTION="sshbastion4.A123456789123.amazonaws.com"

   WINDOWS="172.16.3.254"

   AD="ACORP_example"

   USER="john.doe"
   ```

   - 変数値を ssh コマンドに直接追加します。

   いずれの場合も、レンダリングされたリクエストは次のようになります (変数値の同じセットを想定) 。

```
ssh -L 3389:172.16.3.254:3389 ACORP_example\\\
\john.doe@sshbastion4.A123456789123.amazonaws.com
```

2. どちらか: リモートデスクトップクライアントを開き、ループバックアドレスとポート 127.0.0.1:3389 を入力し、接続を開きます。

   または、新しい Linux デスクトップシェルから Windows インスタンスにログインします。RDesktop を使用する場合、コマンドは次のようになります。

   ```
   rdesktop 127.0.0.1:3389
   ```

   Windows インスタンスのリモートデスクトップウィンドウが Linux デスクトップに表示されます。

   > **Tip**
   >
   > リモートデスクトップセッションの開始に失敗した場合、SSH 踏み台からの Windows インスタンスへのネットワーク接続が、ステップ 1 のシェルからのポート 3389 で許可されていることを確認します (private_ip_address_of_windows_instance適切に置き換えてください)。
   >
   > ```
   > nc private_ip_address_of_windows_instance 3389 -v -z
   > ```
   >
   > 成功：
   >
   > ```
   > nc 172.16.0.83 3389 -v -z
   >         Connection to 172.16.0.83 3389 port [tcp/ms-wbt-server] succeeded
   >         netstat -anvp | grep 3389
   >         tcp    0     0 172.16.0.253:48079 172.16.3.254:3389 ESTABLISHED
   > ```

Windows コンピュータから Windows インスタンスへ

Windows リモートデスクトップ接続クライアントを使用して、Windows コンピュータから Windows インスタンスに接続します。

MALZ

フレンドリ踏み台名の詳細については、「」を参照してくださいDNS フレンドリ踏み台名。

1. 標準の Windows プログラムであるリモートデスクトップ接続プログラムを開き、ホスト名フィールドに Windows 踏み台の名前を入力します。

2. [接続] を選択します。リモートデスクトップ接続は、踏み台への RDP 接続を試みます。

   成功すると、認証情報ダイアログボックスが開きます。アクセスを取得するには、Windows インスタンスと同様に、会社の Active Directory 認証情報を使用します。

3. 踏み台でリモートデスクトップ接続プログラムを開き、接続する Windows インスタンスの IP アドレス (10.0.0.100 など) を入力し、接続を選択します。Windows インスタンスに接続する前に、会社の Active Directory 認証情報が再度必要です。

SALZ

フレンドリ踏み台名の詳細については、「」を参照してくださいDNS フレンドリ踏み台名。

1. 標準の Windows プログラムであるリモートデスクトップ接続プログラムを開き、ホスト名フィールドに Windows 踏み台の名前を入力します。たとえば、 です。アカウント番号が 123456789123 でrdpbastion*(1-4)*.A*AMSAccountNumber*.amazonaws.com、踏み台 4、 を選択した場合、このようになりますrdpbastion4.A123456789123.amazonaws.com。

2. [接続] を選択します。リモートデスクトップ接続は、踏み台への RDP 接続を試みます。

   成功すると、認証情報ダイアログボックスが開きます。アクセスを取得するには、Windows インスタンスと同様に、会社の Active Directory 認証情報を使用します。

3. 踏み台でリモートデスクトップ接続プログラムを開き、接続する Windows インスタンスの IP アドレス (10.0.0.100 など) を入力し、接続を選択します。Windows インスタンスに接続する前に、会社の Active Directory 認証情報が再度必要です。

Windows コンピュータから Linux インスタンスへ

Windows 環境から SSH 踏み台に RDP するには、次の手順に従います。

MALZ

開始する前に:

- 接続するインスタンスへのアクセスをリクエストします。詳細については、「アクセスリクエスト」を参照してください。
- 接続するわかりやすい DNS SSH 踏み台名を選択します。次に例を示します。

```
sshbastion(1-4).YOUR_DOMAIN
```

YOUR_DOMAIN が myamsaddomain.com" で、踏み台 4 を選択した場合、次のようになります。

```
sshbastion4.myamsaddomain.com
```

- 接続するインスタンスの IP アドレスを見つけます。詳細については、「インスタンス ID または IP アドレスの検索」を参照してください。

Windows マシンから Linux インスタンスに接続するには、まず SSH 踏み台に接続する必要があります。

ネイティブ Windows OpenSSH クライアントを使用するか、ローカルマシンに PuTTY をインストールします。OpenSSH の詳細については、「Windows での OpenSSH」を参照してください。

1. ネイティブ Windows を使用するかPuTTY を開き、SSH 踏み台ホスト名または SSH 踏み台 IP アドレスを入力します。たとえば、10.65.2.214 (22 は SSH に使用されるポートで、デフォルトで設定されます) です。
2. OpenSSH または PuTTY は踏み台への SSH 接続を試み、シェルウィンドウを開きます。
3. RDP ホストと同じように、会社の Active Directory 認証情報を使用してアクセスします。
4. Bash プロンプトが表示されたら、インスタンスに SSH します。次のとおりに入力します。

```
ssh DOMAIN_FQDN\USERNAME@INSTANCE_IP
```

SALZ

開始する前に:

- 接続先のインスタンスへのアクセスをリクエストします。詳細については、「アクセスリクエスト」を参照してください。
- 接続するわかりやすい DNS SSH 踏み台名を選択します。次に例を示します。

```
sshbastion(1-4).AAMSAccountNumber.amazonaws.com
```

アカウント番号が 123456789123 で、踏み台 4 を選択した場合、次のようになります。

```
sshbastion4.A123456789123.amazonaws.com
```

- 接続するインスタンスの IP アドレスを見つけます。詳細については、「インスタンス ID または IP アドレスの検索」を参照してください。

Windows マシンから Linux インスタンスに接続するには、まず SSH 踏み台に接続する必要があります。

ネイティブ Windows OpenSSH クライアントを使用するか、ローカルマシンに PuTTY をインストールします。OpenSSH の詳細については、「Windows での OpenSSH」を参照してください。

1. ネイティブ Windows を使用するかPuTTY を開き、SSH 踏み台ホスト名または SSH 踏み台 IP アドレスを入力します。たとえば、10.65.2.214 (22 は SSH に使用されるポートで、デフォルトで設定されます) です。
2. OpenSSH または PuTTY は踏み台への SSH 接続を試み、シェルウィンドウを開きます。
3. RDP ホストと同じように、会社の Active Directory 認証情報を使用してアクセスします。
4. Bash プロンプトが表示されたら、インスタンスに SSH します。次のとおりに入力します。

```
ssh DOMAIN_FQDN\USERNAME@INSTANCE_IP
```

インシデントの報告

AMS コンソールを使用してインシデントを報告します。新しい問題や質問ごとに新しいインシデントを作成することが重要です。古い問い合わせに関連するケースを開くときは、以前のやり取りを参照できるように、関連するケース番号を含めると便利です。

> **Note**
>
> ケースコレスポンデンスが元の問題から逸脱した場合、AMS オペレーターから新しいインシデントの報告を求められることがあります。

AMS コンソールを使用してインシデントを報告するには：

1. 左側のナビゲーションから、Incidents を選択します。

   インシデントリストが開きます。

   インシデントリストが空の場合、フィルターをクリアオプションはフィルターを Any ステータスにリセットします。

   電話またはチャットを使用する場合は、サポートセンターでインシデントの作成をクリックして、サポートセンターコンソールでインシデントの作成ページを開き、AMS サービスタイプが自動的に入力されます。

   > **Important**
   >
   > - 応答を改善するために、 で開始された通話 サポート が記録されます。通話が切断された場合は、サポートセンターのケースを通じてコールバックする必要があります。コールバックするメカニズム AWS はありません。
   > - 電話とチャットのサポートは、RFC やセキュリティの問題ではなく、サポートケース、インシデント、サービスリクエストに役立つように設計されています。
   > - RFC の問題については、関連する RFC の詳細ページの対応オプションを使用して、AMS エンジニアに連絡してください。
   > - セキュリティ上の問題については、優先度の高い (P1 または P2) サポートケースを作成します。ライブチャット機能は、セキュリティイベント用ではありません。

2. 既存のインシデントを検索する場合は、ドロップダウンリストからインシデントステータスフィルターを選択します。

	• まだ解決されていないすべてのインシデント。 • まだ割り当てられていない新しいインシデント。 • 割り当てられたインシデント。 • 再開したインシデント。 • 割り当てられた複雑なインシデント。 • 次のステップの前にフィードバックが必要なインシデント。 • 最近情報を送信したインシデント。 • が終了したインシデント。 • アカウント内のすべてのインシデント。

3. [作成] を選択します。

   インシデントの作成ページが開きます。

4. 優先度を選択します。

   - 低: AWS/AMS リソースに関連するビジネスサービスまたはアプリケーションの重要ではない機能が影響を受けます。
   - 中: AWS/AMS リソースに関連するビジネスサービスまたはアプリケーションが中程度の影響を受け、機能が低下しています。
   - 高: ビジネスに大きな影響を与えます。 AWS/AMS リソースに関連するアプリケーションの重要な機能は利用できません。本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。

5. カテゴリを選択します。

> **Note**
>
> インシデント機能をテストする場合は、インシデントタイトルにアクションなしフラグ (AMSTestNoOpsActionRequired) を追加します。

6. 次の情報を入力します。

   - 件名: インシデントレポートのわかりやすいタイトル。
   - CC E メール: インシデントレポートと解決策について通知するユーザーの E メールアドレスのリスト。
   - 詳細: インシデントの包括的な説明、影響を受けるシステム、および解決の期待される結果。事前設定された質問に回答するか、それらを削除して関連情報を入力します。

   添付ファイルを追加するには、添付ファイルの追加を選択し、必要な添付ファイルを参照し、開くをクリックします。添付ファイルを削除するには、削除アイコン をクリックします 。

7. [Submit] を選択してください。

   詳細ページが開き、タイプ、件名、作成済み、ID、ステータスなどのインシデントに関する情報と、作成したリクエストの説明を含む通信エリアが表示されます。

   返信をクリックしてコレスポン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します。

   インシデントが解決されたら、Close Case をクリックします。

   1 ページに収まるよりも多くのコレスポンデンスがある場合は、「Load More」をクリックします。

   コミュニケーションを評価することを忘れないでください。

   インシデントがインシデントリストページに表示されます。

サービスリクエストの作成

AWS Managed Services (AMS) コンソールを使用してサービスリクエストを作成するには：

1. 左側のナビゲーションから、サービスリクエストを選択します。

   サービスリクエストリストが開きます。

   サービスリクエストリストが空の場合、フィルターをクリアオプションはフィルターを Any ステータスにリセットします。

   電話またはチャットを使用する場合は、サポートセンターでサービスリクエストの作成をクリックして、サポートセンターコンソールでサービスリクエストの作成ページを開き、AMS サービスタイプが自動的に入力されます。

   > **Note**
   >
   > 応答を改善するために、 サポート センターで開始された通話が記録されます。通話が切断された場合は、サポートセンターのケースを通じてコールバックする必要があります。コールバックするメカニズム AWS はありません。

   > **Important**
   >
   > 電話とチャットのサポートは、サポートケース、インシデント、サービスリクエストに役立つように設計されています。RFC の問題については、関連する RFC の詳細ページの対応オプションを使用して、AMS エンジニアに連絡してください。

2. 既存のサービスリクエストを検索する場合は、ドロップダウンリストからサービスリクエストのステータスフィルターを選択します。

	• まだ解決されていないすべてのサービスリクエスト。 • まだ割り当てられていない新しいサービスリクエスト。 • 割り当てられたサービスリクエスト。 • 再開したサービスリクエスト。 • 割り当てられた複雑なサービスリクエスト。

	• 次のステップの前にフィードバックが必要なサービスリクエスト。 • 最近情報を送信したサービスリクエスト。 • が終了したサービスリクエスト。 • アカウント内のすべてのサービスリクエスト。

3. [作成] を選択します。

   サービスリクエストの作成ページが開きます。

4. カテゴリを選択します。

   > **Note**
   >
   > サービスリクエスト機能をテストする場合は、サービスリクエストのタイトルにアクションなしフラグ `AMSTestNoOpsActionRequired.` を追加します。

5. 次の情報を入力します。

   - 件名: これにより、リストページのサービスリクエストの詳細へのリンクが作成されます。
   - CC E メール: これらの E メールは、デフォルトの E メール連絡先に加えて通信を受信します。
   - 詳細: できるだけ多くの情報をここに入力します。

   添付ファイルを追加するには、添付ファイルの追加を選択し、必要な添付ファイルを参照し、開くをクリックします。添付ファイルを削除するには、削除アイコン をクリックします

   。

6. [Submit] を選択してください。

   詳細ページが開き、タイプ、件名、作成済み、ID、ステータスなどのサービスリクエストに関する情報と、作成したリクエストの説明を含む通信エリアが表示されます。

   さらに、サービスリクエストがサービスリクエストリストページに表示されます。これは、アラートがあるが、AMS からまだ聞こえていない場合に使用します。

返信をクリックしてコレスポンデンスエリアを開き、追加の詳細またはステータスの更新を指定します。

サービスリクエストが解決されたら、ケースの解決をクリックします。

Load More をクリックして、最初のページに収まらない追加のコレスポンデンスを表示します。

コミュニケーションを評価することを忘れないでください。

請求関連のクエリの場合は、AMS コンソールの Other Category、AMS CM API `ChangeTypeId` `ct-1e1xtak34nx76`の 、または AWS サポート API `IssueType=AMS`の を使用します。

オンボーディング後のステップ

AMS アカウントに登録したので、AMS ドキュメントをさらにお読みください。以下のドキュメントを参照してください。

- HA 2 層スタック CT を使用して完全に機能する WordPress スタックを作成するためのチュートリアルでは、完全な AMS エクスペリエンスを提供します。
- AMS ユーザーガイド: AMS ユーザーガイドでは、AMS の機能について説明し、主要な用語、オペレーション、インターフェイスを一覧表示し、一般的な AMS マネージドインフラストラクチャアーキテクチャの概要を示します。さらに、アクセス管理の詳細と AMS のデフォルトも指定されます。また、AMS 変更管理システムの使用方法の詳細な説明と、いくつかのウォークスルーについても説明します。その他の管理の概念についても説明します。
- AMS API リファレンス: この API リファレンスでは、リクエスト、レスポンス、例など、すべての API コールについて説明します。
- AMS アプリケーションガイド: AMS アプリケーションガイドでは、アプリケーションを AMS にデプロイおよび保守するためのさまざまなオプションと方法について説明します。

チュートリアル

以下のチュートリアルでは、 CLI と コンソールを使用して、高可用性 (アドバンスト) CT (ct-06mjngx5flwto) で 2 層スタックを作成する手順について詳しく説明します。Linux Auto Scaling グループ (ASG) をデプロイするためのチュートリアルと Windows ASG をデプロイするためのチュートリアルが用意されています。

ChangeTypeId を含むすべての CT オプションの説明は、AMS 変更タイプリファレンスで確認できます。

CLI チュートリアル: 高可用性 2 層スタック (Linux/RHEL)

このセクションでは、AMS CLI を使用して高可用性 (HA) 2 層スタックを AMS 環境にデプロイする方法について説明します。

> **Note**
>
> このデプロイのチュートリアルは、AMZN Linux および RHEL 環境でテストされています。

タスクと必要な RFCs の概要：

1. インフラストラクチャの作成 (HA 2 層スタック)
2. CodeDeploy アプリケーション用の S3 バケットを作成する
3. WordPress アプリケーションバンドルを作成し、S3 バケットにアップロードする
4. CodeDeploy を使用してアプリケーションをデプロイする
5. WordPress サイトにアクセスしてログインし、デプロイを検証します。

開始する前に

Deployment | Advanced Stack Components | High Availability Two Tier Stack Advanced | Create CT は、Auto Scaling グループ、ロードバランサー、データベース、CodeDeploy アプリケーション名とデプロイグループ (アプリケーションと同じ名前) を作成します。CodeDeploy の詳細については、CodeDeploy とは」を参照してください。

このチュートリアルでは、UserData を含む高可用性 2 層スタック (アドバンスト) RFC を使用し、CodeDeploy がデプロイできる WordPress バンドルを作成する方法について説明します。

この例`UserData`に示す は、http://169.254.169.254/latest/meta-data/ で利用可能な EC2 インスタンスメタデータサービスをクエリすることで、実行中のインスタンス内からインスタンス ID、リージョンなどのインスタンスメタデータを取得します。ユーザーデータスクリプトのこの行: は`REGION=$(curl 169.254.169.254/latest/meta-data/placement/availability-zone/ | sed 's/[a-z]$//')`、メタデータサービスからサポートされているリージョンの $REGION 変数にアベイラビリティーゾーン名を取得し、それを使用して CodeDeploy エージェン

トをダウンロードする S3 バケットの URL を完了します。169.254.169.254 IP は VPC 内でのみルーティング可能です (すべての VPCsはサービスをクエリできます) 。サービスの詳細については、「インスタンスメタデータとユーザーデータ」を参照してください。また、UserData として入力されたスクリプトは「ルート」ユーザーとして実行され、「sudo」コマンドを使用する必要はありません。

このチュートリアルでは、以下のパラメータをデフォルト値 (表示) のままにします。

- Auto Scaling グループ: `Cooldown=300, DesiredCapacity=2, EBSOptimized=false, HealthCheckGracePeriod=600, IAMInstanceProfile=customer-mc-ec2-instance-profile, InstanceDetailedMonitoring=true, InstanceRootVolumeIops=0, InstanceRootVolumeType=standard, InstanceType=m3.medium, MaxInstances=2, MinInstances=2, ScaleDownPolicyCooldown=300, ScaleDownPolicyEvaluationPeriods=4, ScaleDownPolicyPeriod=60, ScaleDownPolicyScalingAdjustment=-1, ScaleDownPolicyStatistic=Average, ScaleDownPolicyThreshold=35, ScaleMetricName=CPUUtilization, ScaleUpPolicyCooldown=60, ScaleUpPolicyEvaluationPeriods=2, ScaleUpPolicyPeriod=60, ScaleUpPolicyScalingAdjustment=2, ScaleUpPolicyStatistic=Average, ScaleUpPolicyThreshold=75`。
- Load Balancer: `HealthCheckInterval=30, HealthCheckTimeout=5`。
- データベース: `BackupRetentionPeriod=7, Backups=true, InstanceType=db.m3.medium, IOPS=0, MultiAZ=true, PreferredBackupWindow=22:00-23:00, PreferredMaintenanceWindow=wed:03:32-wed:04:02, StorageEncrypted=false, StorageEncryptionKey="", StorageType=gp2`。
- アプリケーション: `DeploymentConfigName=CodeDeployDefault.OneAtATime`。
- S3 バケット: `AccessControl=Private`。

その他の設定：

`RequestedStartTime` RFC をスケジュール`RequestedEndTime`する場合は、 を使用して正しい UTC 時間Time.isを決定できます。提供された例は、適切に調整する必要があります。開始時刻が経過すると、RFC は続行できません。または、これらの値をオフのままにして、承認が渡されるとすぐに実行される ASAP RFC を作成することもできます。

> **Note**
>
> 以下に示すものとは異なる設定を選択できるパラメータが多数あります。この例に示すこれらのパラメータの値はテスト済みですが、適切ではない可能性があります。

インフラストラクチャを作成する

開始する前に次のデータを収集すると、デプロイがより速くなります。

必須データにはスタックがあります。

- AutoScalingGroup:
  - `UserData`: この値は、このチュートリアルで提供されています。これには、CodeDeploy のリソースをセットアップし、CodeDeploy エージェントを起動するためのコマンドが含まれています。
  - `AMI-ID`: この値は、Auto Scaling グループ (ASG) がスピンアップする EC2 インスタンスの種類を決定します。アカウントで「customer-」で始まり、目的のオペレーティングシステムの AMI を選択してください。AMS SKMS API リファレンスで AMI IDs を検索するには、AWS Artifact コンソールのレポートタブを参照してください。 オペレーション (CLI: list-amis) または AMS コンソール VPCs -> VPCsの詳細ページ。このチュートリアルは、Linux AMI を使用するように設定された ASGs を対象としています。
- データベース:
  - これらのパラメータ 、`DBEngine`、 は、例に示す値がテスト済みですが`EngineVersion`、状況に応じて設定`LicenseModel`する必要があります。
  - これらのパラメータ 、`RDSSubnetIds`、`DBNameMasterUsername`、`MasterUserPassword`は、アプリケーションバンドルをデプロイするときに必要です。RDSSubnetIds には、2 つのプライベートサブネットを使用します。
- LoadBalancer:
  - これらのパラメータ 、`DBEngine`、 は、例に示す値がテスト済みですが`EngineVersion`、状況に応じて設定`LicenseModel`する必要があります。
  - `ELBSubnetIds`: 2 つのパブリックサブネットを使用します。
- アプリケーション: `ApplicationName`値は CodeDeploy アプリケーション名と CodeDeploy デプロイグループ名を設定します。これを使用してアプリケーションをデプロイします。アカウント内で一意である必要があります。アカウントで CodeDeploy 名を確認するには、CodeDeploy コン

ソール」を参照してください。この例では「WordPress」を使用していますが、その値を使用する場合は、まだ使用されていないことを確認してください。

この手順では、高可用性 2 層スタック (アドバンスト) CT (ct-06mjngx5flwto) と Create S3 storage CT (ct-1a68ck03fn98r) を使用します。認証されたアカウントから、コマンドラインで以下のステップに従います。

1. インフラストラクチャスタックを起動します。

   a. HA 2 層スタック CT の実行パラメータ JSON スキーマを、CreateStackParams.json.

```
aws amscm get-change-type-version --change-type-id "ct-06mjngx5flwto"
 --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
 CreateStackParams.json
```

   b. スキーマを変更します。必要に応じて##を置き換えます。たとえば、ASG が作成する EC2 インスタンスに必要な OS を使用します。後でアプリケーションのデプロイに使用するApplicationNameため、 を記録します。最大 50 個のタグを追加できます。

```
{
"Description":      "HA two tier stack for WordPress",
"Name":             "WordPressStack",
"TimeoutInMinutes":  360,
"Tags": [
        {
            "Key": "ApplicationName",
            "Value": "WordPress"
        }
    ],
"AutoScalingGroup": {
            "AmiId":    "AMI-ID",
            "UserData": "#!/bin/bash \n
            REGION=$(curl 169.254.169.254/latest/meta-data/placement/
availability-zone/ | sed 's/[a-z]$//') \n
            yum -y install ruby httpd \n
            chkconfig httpd on \n
            service httpd start \n
            touch /var/www/html/status \n
            cd /tmp \n
            curl -O https://aws-codedeploy-$REGION.s3.amazonaws.com/latest/
install \n
```

```
            chmod +x ./install \n
            ./install auto \n
            chkconfig codedeploy-agent on \n
            service codedeploy-agent start"
    },
    "LoadBalancer": {
        "Public":               true,
        "HealthCheckTarget":    "HTTP:80/status"
    },
    "Database":     {
        "DBEngine":             "MySQL",
        "DBName":               "wordpress",
        "EngineVersion":        "8.0.16 ",
        "LicenseModel":         "general-public-license",
        "MasterUsername":       "admin",
        "MasterUserPassword":   "p4ssw0rd"
    },
    "Application":  {
    "ApplicationName":  "WordPress"
        }
}
```

c. CreateStackRfc.CreateStackRfc.json:

```
aws amscm create-rfc --generate-cli-skeleton > CreateStackRfc.json
```

d. RFC テンプレートを次のように変更して保存します。内容を削除して置き換えることができます。RequestedStartTime と RequestedEndTimeはオプションになりました。これらを除外すると、承認されるとすぐに実行される ASAP RFC が作成されます (通常は自動的に実行されます) 。スケジュールされた RFC を送信するには、これらの値を追加します。

```
{
"ChangeTypeVersion":    "3.0",
"ChangeTypeId":         "ct-06mjngx5flwto",
"Title":                "HA-Stack-For-WP-RFC"
}
```

e. CreateStackRfc.json ファイルと CreateStackParams.json 実行パラメータファイルを指定して、RFC を作成します。

```
aws amscm create-rfc --cli-input-json file://CreateStackRfc.json --execution-
parameters file://CreateStackParams.json
```

レスポンスで RFC ID を受け取ります。後続のステップの ID を保存します。

f. RFC を送信します。

```
aws amscm submit-rfc --rfc-id  RFC_ID
```

RFC が成功した場合、出力は受信されません。

g. RFC ステータスを確認するには、 を実行します。

```
aws amscm get-rfc --rfc-id RFC_ID
```

RFC ID をメモしておきます。

2. S3 バケットを起動する

開始する前に次のデータを収集すると、デプロイがより速くなります。

必須データ S3 バケット：

- VPC-ID: この値により、S3 バケットの場所が決まります。以前に使用したものと同じ VPC ID を使用します。
- BucketName: この値は S3 バケット名を設定します。これを使用してアプリケーションバンドルをアップロードします。アカウントのリージョン全体で一意である必要があり、大文字を含めることはできません。BucketName の一部としてアカウント ID を含めることは必須ではありませんが、後でバケットを識別しやすくなります。アカウントに存在する S3 バケット名を確認するには、アカウントの Amazon S3 コンソールに移動します。

a. S3 ストレージ作成 CT の実行パラメータ JSON スキーマを CreateS3StoreParams.json.

```
aws amscm get-change-type-version --change-type-id "ct-1a68ck03fn98r"
 --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
 CreateS3StoreParams.json
```

b. スキーマを次のように変更し、コンテンツを削除して置き換えることができます。*VPC_ID* を適切に置き換えます。この例の値はテスト済みですが、適切ではない可能性があります。

> **Tip**
>
> はアカウントのリージョン全体で一意BucketNameである必要があり、大文字を含めることはできません。BucketName の一部としてアカウント ID を含めることは必須ではありませんが、後でバケットを識別しやすくなります。アカウントに存在する S3 バケット名を確認するには、アカウントの Amazon S3 コンソールに移動します。

```
{
"Description":      "S3BucketForWordPressBundle",
"VpcId":            "VPC_ID",
"StackTemplateId":  "stm-s2b72beb000000000",
"Name":             "S3BucketForWP",
"TimeoutInMinutes":  60,
"Parameters":   {
    "AccessControl":    "Private",
    "BucketName":       "ACCOUNT_ID-BUCKET_NAME"
    }
}
```

c. CreateRfc の JSON テンプレートを、CreateS3StoreRfc.json:

```
aws amscm create-rfc --generate-cli-skeleton > CreateS3StoreRfc.json
```

d. CreateS3StoreRfc.json ファイルを変更して保存し、コンテンツを削除して置き換えることができます。RequestedStartTime と RequestedEndTimeはオプションになりました。これらを除外すると、承認されるとすぐに実行される ASAP RFC が作成されます (通常は自動的に実行されます) 。スケジュールされた RFC を送信するには、これらの値を追加します。

```
{
"ChangeTypeVersion":    "1.0",
"ChangeTypeId":         "ct-1a68ck03fn98r",
"Title":                "S3-Stack-For-WP-RFC"
}
```

e. CreateS3StoreRfc.json ファイルと CreateS3StoreParams.json 実行パラメータファイルを指定して、RFC を作成します。

```
aws amscm create-rfc --cli-input-json file://CreateS3StoreRfc.json  --
execution-parameters file://CreateS3StoreParams.json
```

レスポンスで新しい RFC の RfcId を受け取ります。後続のステップの ID を保存します。

f. RFC を送信します。

```
aws amscm submit-rfc --rfc-id RFC_ID
```

RFC が成功した場合、出力は受信されません。

g. RFC ステータスを確認するには、 を実行します。

```
aws amscm get-rfc --rfc-id RFC_ID
```

アプリケーションの作成、アップロード、デプロイ

まず、WordPress アプリケーションバンドルを作成し、CodeDeploy CT を使用してアプリケーションを作成してデプロイします。 CTs

1. WordPress をダウンロードし、ファイルを抽出して ./scripts ディレクトリを作成します。

   Linux コマンド：

   ```
   wget https://github.com/WordPress/WordPress/archive/master.zip
   ```

   Windows: ブラウザウィンドウhttps://github.com/WordPress/WordPress/archive/master.zipに貼り付け、zip ファイルをダウンロードします。

   パッケージをアセンブルする一時ディレクトリを作成します。

   Linux:

   ```
   mkdir /tmp/WordPress
   ```

   Windows: WordPress」ディレクトリを作成します。後でディレクトリパスを使用します。

2. WordPress ソースをWordPress」ディレクトリに抽出し、./scripts ディレクトリを作成します。

   Linux:

```
unzip master.zip -d /tmp/WordPress_Temp
cp -paf /tmp/WordPress_Temp/WordPress-master/* /tmp/WordPress
rm -rf /tmp/WordPress_Temp
rm -f master
cd /tmp/WordPress
mkdir scripts
```

Windows: 作成したWordPress」ディレクトリに移動し、そこに「scripts」ディレクトリを作成します。

Windows 環境の場合は、スクリプトファイルのブレークタイプを Unix (LF) に設定してください。Notepad ++ では、これはウィンドウの右下にあるオプションです。

3. WordPress ディレクトリに CodeDeploy appspec.yml ファイルを作成します (例をコピーする場合は、インデントと各スペース数を確認します) 。重要: WordPress ファイル (この場合は WordPress ディレクトリ) を目的の宛先 (/var/www/html/WordPress) にコピーするための WordPress 「ソース」パスが正しいことを確認します。この例では、appspec.yml ファイルは WordPress ファイルを含む ディレクトリにあるため、「/」のみが必要です。また、Auto Scaling グループに RHEL AMI を使用した場合でも、「os: linux」行はそのままにしておきます。appspec.yml ファイルの例：

```
version: 0.0
os: linux
files:
  - source: /
    destination: /var/www/html/WordPress
hooks:
  BeforeInstall:
    - location: scripts/install_dependencies.sh
      timeout: 300
      runas: root
  AfterInstall:
    - location: scripts/config_wordpress.sh
      timeout: 300
      runas: root
  ApplicationStart:
    - location: scripts/start_server.sh
      timeout: 300
      runas: root
  ApplicationStop:
    - location: scripts/stop_server.sh
```

```
      timeout: 300
      runas: root
```

4. WordPress ./scripts ディレクトリに bash ファイルスクリプトを作成します。

   まず、次の内容config_wordpress.shで を作成します (必要に応じて、wp-config.php ファイルを直接編集できます) 。

> **Note**
>
> *DBName* を HA スタック RFC で指定された値 (例:) に置き換えますwordpress。
> *DB_MasterUsername* を HA スタック RFC で指定されたMasterUsername値 (などadmin) に置き換えます。
> *DB_MasterUserPassword* を HA スタック RFC で指定されたMasterUserPassword値 (例:) に置き換えますp4ssw0rd。
> *DB_ENDPOINT* を HA スタック RFC の実行出力のエンドポイント DNS 名 (例:) に置き換えますsrt1cz23n45sfg.clgvd67uvydk.us-east-1.rds.amazonaws.com。これは、GetRfc オペレーション (CLI: get-rfc --rfc-id RFC_ID) または以前に送信した HA スタック RFC の AMS コンソール RFC の詳細ページで確認できます。

```
#!/bin/bash
chmod -R 755 /var/www/html/WordPress
cp /var/www/html/WordPress/wp-config-sample.php /var/www/html/WordPress/wp-
config.php
cd /var/www/html/WordPress
sed -i "s/database_name_here/DBName/g" wp-config.php
sed -i "s/username_here/DB_MasterUsername/g" wp-config.php
sed -i "s/password_here/DB_MasterUserPassword/g" wp-config.php
sed -i "s/localhost/DB_ENDPOINT/g" wp-config.php
```

5. 同じディレクトリに、次の内容install_dependencies.shで を作成します。

```
#!/bin/bash
yum install -y php
yum install -y php-mysql
yum install -y mysql
service httpd restart
```

> **Note**
>
> HTTPS は、ヘルスチェックを最初から機能させるために、起動時にユーザーデータの一部としてインストールされます。

6. 同じディレクトリに、次の内容`start_server.sh`で を作成します。

   - Amazon Linux インスタンスの場合は、以下を使用します。

   ```
   #!/bin/bash
   service httpd start
   ```

   - RHEL インスタンスの場合は、以下を使用します (追加のコマンドは、SELINUX が WordPress を受け入れることを許可するポリシーです) 。

   ```
   #!/bin/bash
   setsebool -P  httpd_can_network_connect_db 1
   setsebool -P  httpd_can_network_connect 1
   chcon -t httpd_sys_rw_content_t /var/www/html/WordPress/wp-content -R
   restorecon -Rv /var/www/html
   service httpd start
   ```

7. 同じディレクトリに、次の内容`stop_server.sh`で を作成します。

   ```
   #!/bin/bash
   service httpd stop
   ```

8. zip バンドルを作成します。

   Linux:

   ```
   $ cd /tmp/WordPress
   $ zip -r wordpress.zip .
   ```

   Windows: WordPress」ディレクトリに移動し、すべてのファイルを選択して zip ファイルを作成します。必ず wordpress.zip という名前を付けます。

1. アプリケーションバンドルを S3 バケットにアップロードします。

スタックのデプロイを続行するには、バンドルを設定する必要があります。

作成した S3 バケットインスタンスに自動的にアクセスできます。踏み台または S3 コンソールからアクセスし、WordPress バンドルをdrag-and-dropでアップロードするか、zip ファイルを参照して選択できます。

シェルウィンドウで次のコマンドを使用することもできます。zip ファイルへの正しいパスがあることを確認してください。

```
aws s3 cp wordpress.zip s3://BUCKET_NAME/
```

2. WordPress アプリケーションバンドルをデプロイします。

開始する前に次のデータを収集すると、デプロイがより速くなります。

必須データ：

- VPC-ID: この値により、S3 バケットの場所が決まります。以前に使用したものと同じ VPC ID を使用します。
- CodeDeployApplicationName および CodeDeployApplicationName: HA 2-Tier スタック RFC で使用したApplicationName値は、CodeDeployApplicationName と CodeDeployDeploymentGroupName を設定します。この例では「WordPress」を使用していますが、別の値を使用した可能性があります。
- S3Location: にはS3Bucket、BucketName以前に作成した を使用します。S3BundleType と S3Keyは、S3 ストアに配置したバンドルのものです。

a. CodeDeploy アプリケーションデプロイ CT の実行パラメータ JSON スキーマを DeployCDAppParams.json.

```
aws amscm get-change-type-version --change-type-id "ct-2edc3sd1sqmrb"
 --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
 DeployCDAppParams.json
```

b. スキーマを次のように変更し、 として保存します。コンテンツを削除して置き換えることができます。

```
{
"Description":                          "DeployWPCDApp",
"VpcId":                                "VPC_ID",
```

```
"Name":                                "WordPressCDAppDeploy",
"TimeoutInMinutes":                    60,
"Parameters":   {
    "CodeDeployApplicationName":                "WordPress",
    "CodeDeployDeploymentGroupName":            "WordPress",
    "CodeDeployIgnoreApplicationStopFailures":   false,
    "CodeDeployRevision": {
      "RevisionType": "S3",
      "S3Location": {
        "S3Bucket":     "BUCKET_NAME",
        "S3BundleType": "zip",
        "S3Key":        "wordpress.zip" }
        }
    }
}
```

c. CreateRfc の JSON テンプレートを、現在のフォルダの DeployCDAppRfc.json:

```
aws amscm create-rfc --generate-cli-skeleton > DeployCDAppRfc.json
```

d. DeployCDAppRfc.json ファイルを変更して保存し、コンテンツを削除して置き換えることができます。RequestedStartTime と RequestedEndTimeはオプションになりました。これらを除外すると、承認されるとすぐに実行される ASAP RFC が作成されます (通常は自動的に実行されます) 。スケジュールされた RFC を送信するには、これらの値を追加します。

```
{
"ChangeTypeVersion":    "1.0",
"ChangeTypeId":         "ct-2edc3sd1sqmrb",
"Title":                "CD-Deploy-For-WP-RFC"
}
```

e. DeployCDAppRfc ファイルと DeployCDAppParams 実行パラメータファイルを指定して、RFC を作成します。

```
aws amscm create-rfc --cli-input-json file://DeployCDAppRfc.json  --execution-
parameters file://DeployCDAppParams.json
```

レスポンスで新しい RFC の RfcId を受け取ります。後続のステップの ID を保存します。

f. RFC を送信します。

```
aws amscm submit-rfc --rfc-id RFC_ID
```

RFC が成功した場合、出力は受信されません。

g. RFC ステータスを確認するには、 を実行します。

```
aws amscm get-rfc --rfc-id RFC_ID
```

アプリケーションのデプロイを検証する

WordPress デプロイパス: /WordPress を使用して、以前に作成したロードバランサーのエンドポイント (ELB CName) WordPress に移動します。例：

```
http://stack-ID-FOR-ELB.us-east-1.elb.amazonaws.com/WordPress
```

アプリケーションのデプロイをティアダウンする

チュートリアルが終了したら、リソースに対して課金されないようにデプロイを破棄します。

以下は、一般的なスタック削除オペレーションです。HA 2-Tierスタックの場合は 1 回、S3 バケットスタックの場合は 1 回、2 回送信します。最後のフォローアップとして、S3 バケットのすべてのスナップショット (サービスリクエストに S3 バケットスタック ID を含める) を削除するサービスリクエストを送信します。これらは 10 日後に自動的に削除されますが、早期に削除すると多少のコストを節約できます。

このチュートリアルでは、AMS コンソールを使用して S3 スタックを削除する例を示します。この手順は、AMS コンソールを使用してスタックを削除する場合に適用されます。

> **Note**
>
> S3 バケットを削除する場合は、まずオブジェクトを空にする必要があります。

必須データ：

- `StackId`: 使用するスタック。これは、左側のナビゲーションのリンクから入手できる AMS コンソールスタックページから確認できます。AMS SKMS API/CLI を使用して、AMS SKMS API リファレンスについては、AWS Artifact Console のレポートタブを参照してください。 オペレーション (`list-stack-summaries` CLI の)。

- このウォークスルーの変更タイプ ID は でct-0q0bic0ywqk6c、バージョンは「1.0」です。最新バージョンを確認するには、次のコマンドを実行します。

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=ct-0q0bic0ywqk6c
```

インライン作成：

- インラインで指定された実行パラメータ (インラインで実行パラメータを指定する場合は引用符をエスケープ) を使用して、create RFC コマンドを発行します。E

```
aws amscm create-rfc --change-type-id "ct-0q0bic0ywqk6c" --change-type-version "1.0"
 --title "Delete My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

- RFC の作成オペレーションで返された RFC ID を使用して RFC を送信します。送信されるまで、RFC は Editing状態のままで、 に対して動作しません。

```
aws amscm submit-rfc --rfc-id RFC_ID
```

- RFC ステータスをモニタリングし、実行出力を表示します。

```
aws amscm get-rfc --rfc-id RFC_ID
```

テンプレートの作成：

1. RFC テンプレートを現在のフォルダ内のファイルに出力します。例名は DeleteStackRfc.json:

   ```
   aws amscm create-rfc --generate-cli-skeleton > DeleteStackRfc.json
   ```

2. DeleteStackRfc.json ファイルを変更して保存します。スタックの削除には実行パラメータが 1 つしかないため、実行パラメータは DeleteStackRfc.json ファイル自体に含めることができます (実行パラメータを使用して別の JSON ファイルを作成する必要はありません)。

   ExecutionParameters JSON 拡張機能の内部引用符は、バックスラッシュ (\) で エスケープする必要があります。開始時刻と終了時刻のない例：

   ```
   {
   "ChangeTypeVersion":    "1.0",
   ```

```
"ChangeTypeId":          "ct-0q0bic0ywqk6c",
"Title":                 "Delete-My-Stack-RFC"
"ExecutionParameters":   "{
        \"StackId\":\"STACK_ID\"}"
}
```

3. RFC を作成します。

```
aws amscm create-rfc --cli-input-json file://DeleteStackRfc.json
```

レスポンスで新しい RFC の RfcId を受け取ります。例:

```
{
"RfcId": "daaa1867-ffc5-1473-192a-842f6b326102"
}
```

後続のステップの ID を保存します。

4. RFC を送信します。

```
aws amscm submit-rfc --rfc-id RFC_ID
```

RFC が成功した場合、コマンドラインに確認は送信されません。

5. リクエストのステータスをモニタリングし、実行出力を表示するには：

```
aws amscm get-rfc --rfc-id RFC_ID --query "Rfc.
{Status:Status.Name,Exec:ExecutionOutput}" --output table
```

コンソールチュートリアル: 高可用性 2 層スタック (Linux/RHEL)

このセクションでは、AMS コンソールを使用して高可用性 (HA) WordPress サイトを AMS 環境にデプロイする方法について説明します。

> **Note**
>
> このデプロイのチュートリアルは、AMZN Linux および RHEL 環境でテストされています。

タスクと必要な RFCs の概要：

1. インフラストラクチャの作成 (HA 2 層スタック)
2. CodeDeploy アプリケーション用の S3 バケットを作成する
3. WordPress アプリケーションバンドルを作成し、S3 バケットにアップロードする
4. CodeDeploy を使用してアプリケーションをデプロイする
5. WordPress サイトにアクセスしてログインし、デプロイを検証します。
6. デプロイをティアダウンする

ChangeTypeId を含むすべての CT オプションの説明は、AMS 変更タイプリファレンスで確認できます。

開始する前に

Deployment | Advanced Stack Components | High Availability Two Tier Stack | Create CT は、Auto Scaling グループ、ロードバランサー、データベース、CodeDeploy アプリケーション名とデプロイグループ (アプリケーションと同じ名前) を作成します。CodeDeploy の詳細については、CodeDeploy とは」を参照してください。

このチュートリアルでは、CodeDeploy がデプロイできる WordPress バンドルの作成方法`UserData`を含む高可用性 2 層スタック RFC を使用します。

この例`UserData`に示す は、http://169.254.169.254/latest/meta-data/ で利用可能な EC2 インスタンスメタデータサービスをクエリすることで、実行中のインスタンス内からインスタンス ID、リージョンなどのインスタンスメタデータを取得します。ユーザーデータスクリプトのこの行: は`REGION=$(curl 169.254.169.254/latest/meta-data/placement/availability-zone/ | sed 's/[a-z]$//')`、メタデータサービスからサポートされているリージョンの $REGION 変数にアベイラビリティーゾーン名を取得し、それを使用して CodeDeploy エージェントをダウンロードする S3 バケットの URL を完了します。169.254.169.254 IP は VPC 内でのみルーティング可能です (すべての VPCsはサービスをクエリできます) 。サービスの詳細については、「インスタンスメタデータとユーザーデータ」を参照してください。また、UserData として入力されたスクリプトは「ルート」ユーザーとして実行され、「sudo」コマンドを使用する必要はありません。

このチュートリアルでは、次のパラメータをデフォルト値 (表示) のままにします。

- Auto Scaling グループ: `Cooldown=300, DesiredCapacity=2, EBSOptimized=false, HealthCheckGracePeriod=600, IAMInstanceProfile=customer-mc-ec2-instance-profile, InstanceDetailedMonitoring=true, InstanceRootVolumeIops=0,`

InstanceRootVolumeType=standard, InstanceType=m3.medium, MaxInstances=2, MinInstances=2, ScaleDownPolicyCooldown=300, ScaleDownPolicyEvaluationPeriods=4, ScaleDownPolicyPeriod=60, ScaleDownPolicyScalingAdjustment=-1, ScaleDownPolicyStatistic=Average, ScaleDownPolicyThreshold=35, ScaleMetricName=CPUUtilization, ScaleUpPolicyCooldown=60, ScaleUpPolicyEvaluationPeriods=2, ScaleUpPolicyPeriod=60, ScaleUpPolicyScalingAdjustment=2, ScaleUpPolicyStatistic=Average, ScaleUpPolicyThreshold=75。

- Load Balancer: HealthCheckInterval=30, HealthCheckTimeout=5。
- データベース: BackupRetentionPeriod=7, Backups=true, InstanceType=db.m3.medium, IOPS=0, MultiAZ=true, PreferredBackupWindow=22:00-23:00, PreferredMaintenanceWindow=wed:03:32-wed:04:02, StorageEncrypted=false, StorageEncryptionKey="", StorageType=gp2。
- アプリケーション: DeploymentConfigName=CodeDeployDefault.OneAtATime。

変数パラメータ：

コンソールには開始時刻の ASAP オプションが用意されており、このチュートリアルではそれを使用することをお勧めします。ASAP では、承認に合格するとすぐに RFC が実行されます。

> **Note**
>
> 以下に示すものとは異なる設定を選択できるパラメータが多数あります。この例に示すパラメータの値はテスト済みですが、適切ではない可能性があります。必須の値のみが例に表示されます。#######フォントの値は、アカウント固有の値として変更する必要があります。

インフラストラクチャを作成する

この手順では、高可用性 2 層スタック CT の後に S3 ストレージ CT を作成します。

開始する前に次のデータを収集すると、デプロイがより速くなります。

必須データのスタック：

- AutoScalingGroup：

  - UserData: この値は、このチュートリアルで提供されています。これには、CodeDeploy のリソースをセットアップし、CodeDeploy エージェントを起動するためのコマンドが含まれています。
  - AMI-ID: この値は、Auto Scaling グループ (ASG) がスピンアップする EC2 インスタンスのオペレーティングシステムを決定します。アカウントで「customer-」で始まり、目的のオペレーティングシステムの AMI を選択します。AMS コンソール VPCs -> VPCsの詳細ページで AMI IDs を検索します。このチュートリアルは、Amazon Linux または RHEL AMI を使用するように設定された ASGs を対象としています。
- データベース：
  - これらのパラメータ DBEngine、EngineVersion、LicenseModel は、例に示す値がテスト済みですが、状況に応じて設定する必要があります。このチュートリアルでは、それぞれ *MySQL*、*8.0.16*、 *general-public-license* の値を使用します。
  - これらのパラメータ、DBName、MasterUserPassword、MasterUsername は、アプリケーションバンドルをデプロイするときに必要です。このチュートリアルでは、*wordpressDB*、*p4ssw0rd*、*admin* の各値を使用します。DBName には英数字のみを含めることができます。
  - RDS DB の MasterUsername を入力すると、クリアテキストで表示されるため、できるだけ早くデータベースにログインし、パスワードを変更してセキュリティを確保します。
  - RDSSubnetIds には、2 つのプライベートサブネットを使用します。それぞれの後に「Enter」を押すたびに 1 つずつ入力します。AMS SKMS API リファレンスでサブネット IDs を検索するには、AWS Artifact コンソールのレポートタブを参照してください。 オペレーション (CLI: list-subnet-summaries) または AMS コンソール VPCs-> VPC の詳細ページ。
- LoadBalancer：
  - チュートリアルではパブリック ELB サブネットを使用するため、このパラメータ Public を true に設定します。
  - ELBSubnetIds: 2 つのパブリックサブネットを使用します。それぞれの後に「Enter」を押すたびに 1 つずつ入力します。AMS SKMS API リファレンスでサブネット IDs を検索するには、AWS Artifact コンソールのレポートタブを参照してください。 オペレーション (CLI: list-subnet-summaries) または AMS コンソール VPCs-> VPC の詳細ページ。
- アプリケーション: ApplicationName 値は、CodeDeploy アプリケーション名と CodeDeploy デプロイグループ名を設定します。これを使用してアプリケーションをデプロイします。アカウント内で一意である必要があります。アカウントで CodeDeploy 名を確認するには、CodeDeploy コンソールを参照してください。この例では *WordPress* を使用していますが、その値を使用する場合は、まだ使用されていないことを確認してください。

1. 高可用性スタックを起動します。

   a. RFC の作成ページで、リストから「デプロイ」、「サブカテゴリ標準スタック」、「高可用性 2 層スタック」、「Create」を選択します。

   b. 重要: Advanced を選択し、図のように値を設定します。

      星付き (*) オプションの値を入力するだけで、テストされた値は例に示されています。不要な空のオプションは空白のままにすることができます。

   c. RFC の説明セクションの場合：

```
Subject: WP-HA-2-Tier-RFC
```

   d. リソース情報セクションで、AutoScalingGroup、 Database、LoadBalancer、Application、および Tags のパラメータを設定します。

      また、AppName」タグキーの目的は、EC2 コンソールで ASG インスタンスを簡単に検索できるようにすることです。このタグキー「Name」または他の任意のキー名を呼び出すことができます。最大 50 個のタグを追加できます。

```
UserData:
    #!/bin/bash
    REGION=$(curl 169.254.169.254/latest/meta-data/placement/availability-zone/
 | sed 's/[a-z]$//')
    yum -y install ruby httpd
    chkconfig httpd on
    service httpd start
    touch /var/www/html/status
    cd /tmp
    curl -O https://aws-codedeploy-$REGION.s3.amazonaws.com/latest/install
    chmod +x ./install
    ./install auto
    chkconfig codedeploy-agent on
    service codedeploy-agent start
AmiId:              AMI-ID
Description:        WP-HA-2-Tier-Stack

Database:
    LicenseModel:    general-public-license (USE RADIO BUTTON)
    EngineVersion:   8.0.16
    DBEngine:        MySQL
```

```
    RDSSubnetIds:     PRIVATE_AZ1 PRIVATE_AZ2 (ENTER ONE AT A TIME PRESSING
 "ENTER" AFTER EACH)
    MasterUserPassword:  p4ssw0rd
    MasterUsername:      admin
    DBName:              wordpressDB

LoadBalancer:
    Public:              true (USE RADIO BUTTON)
    ELBSubnetIds:        PUBLIC_AZ1 PUBLIC_AZ2

Application:
    ApplicationName:     WordPress

Tags:
    Name:                WP-Rhel-Stack
```

e. 完了したら、送信 をクリックします。

2. 作成したデータベースにログインし、パスワードを変更します。
3. S3 バケットスタックを起動します。

   開始する前に次のデータを収集すると、デプロイがより速くなります。

   必須データ S3 バケット：

   - VPC-ID: この値により、S3 バケットの場所が決まります。AMS SKMS API リファレンスで VPC IDs を検索するには、AWS Artifact コンソールのレポートタブを参照してください。 オペレーション (CLI: list-vpc-summaries) または AMS コンソール VPCsページ。
   - BucketName: この値は S3 バケット名を設定します。これを使用してアプリケーションバンドルをアップロードします。アカウントのリージョン全体で一意である必要があり、大文字を含めることはできません。BucketName の一部としてアカウント ID を含めることは必須ではありませんが、後でバケットを識別しやすくなります。アカウントに存在する S3 バケット名を確認するには、アカウントの Amazon S3 コンソールに移動します。

   a. RFC の作成ページで、RFC CT ピックリストから、カテゴリデプロイ、サブカテゴリアドバンストスタックコンポーネント、項目 S3 ストレージ、およびオペレーションの作成を選択します。

   b. デフォルトの基本オプションを保持し、図のように値を設定します。

```
Subject:              S3-Bucket-WP-HA-RFC
```

```
Description:          S3BucketForWordPressBundles
BucketName:           ACCOUNT_ID-BUCKET_NAME
AccessControl:        Private
VpcId:                VPC_ID
Name:                 S3-Bucket-WP-HA-Stack
TimeoutInMinutes:     60
```

c. 完了したら送信をクリックします。この変更タイプでデプロイされたバケットは、アカウント全体への完全な読み取り/書き込みアクセスを許可します。

アプリケーションの作成、アップロード、デプロイ

まず、WordPress アプリケーションバンドルを作成し、CodeDeploy CT を使用してアプリケーションを作成してデプロイします。 CTs

1. WordPress をダウンロードし、ファイルを抽出して ./scripts ディレクトリを作成します。

   Linux コマンド：

   ```
   wget https://github.com/WordPress/WordPress/archive/master.zip
   ```

   Windows: ブラウザウィンドウhttps://github.com/WordPress/WordPress/archive/master.zipに貼り付け、zip ファイルをダウンロードします。

   パッケージをアセンブルする一時ディレクトリを作成します。

   Linux:

   ```
   mkdir /tmp/WordPress
   ```

   Windows: WordPress」ディレクトリを作成します。後でディレクトリパスを使用します。

2. WordPress ソースをWordPress」ディレクトリに抽出し、./scripts ディレクトリを作成します。

   Linux:

   ```
   unzip master.zip -d /tmp/WordPress_Temp
   cp -paf /tmp/WordPress_Temp/WordPress-master/* /tmp/WordPress
   rm -rf /tmp/WordPress_Temp
   rm -f master
   cd /tmp/WordPress
   ```

```
mkdir scripts
```

Windows: 作成したWordPress」ディレクトリに移動し、そこに「scripts」ディレクトリを作成します。

Windows 環境の場合は、スクリプトファイルのブレークタイプを Unix (LF) に設定してください。Notepad ++ では、これはウィンドウの右下にあるオプションです。

3. WordPress ディレクトリに CodeDeploy appspec.yml ファイルを作成します (例をコピーする場合は、インデントを確認し、各スペース数を確認します) 。重要: WordPress ファイル (この場合は WordPress ディレクトリ) を目的の宛先 (/var/www/html/WordPress) にコピーするには、 WordPress 「ソース」パスが正しいことを確認してください。この例では、appspec.yml ファイルは WordPress ファイルを含む ディレクトリにあるため、「/」のみが必要です。また、Auto Scaling グループに RHEL AMI を使用した場合でも、「os: linux」行はそのままにしておきます。appspec.yml ファイルの例 :

```
version: 0.0
os: linux
files:
  - source: /
    destination: /var/www/html/WordPress
hooks:
  BeforeInstall:
    - location: scripts/install_dependencies.sh
      timeout: 300
      runas: root
  AfterInstall:
    - location: scripts/config_wordpress.sh
      timeout: 300
      runas: root
  ApplicationStart:
    - location: scripts/start_server.sh
      timeout: 300
      runas: root
  ApplicationStop:
    - location: scripts/stop_server.sh
      timeout: 300
      runas: root
```

4. WordPress ./scripts ディレクトリに bash ファイルスクリプトを作成します。

まず、次の内容config_wordpress.shで を作成します (必要に応じて、wp-config.php ファイルを直接編集できます) 。

> **Note**
>
> *DBName* を HA スタック RFC で指定された値 (例:) に置き換えますwordpress。
> *DB_MasterUsername* を HA スタック RFC で指定されたMasterUsername値 (などadmin) に置き換えます。
> *DB_MasterUserPassword* を HA スタック RFC で指定されたMasterUserPassword値 (例:) に置き換えますp4ssw0rd。
> *DB_ENDPOINT* を HA スタック RFC の実行出力のエンドポイント DNS 名 (例:) に置き換えますsrt1cz23n45sfg.clgvd67uvydk.us-east-1.rds.amazonaws.com。これは、GetRfc オペレーション (CLI: get-rfc --rfc-id RFC_ID) または以前に送信した HA スタック RFC の AMS コンソール RFC の詳細ページで確認できます。

```
#!/bin/bash
chmod -R 755 /var/www/html/WordPress
cp /var/www/html/WordPress/wp-config-sample.php /var/www/html/WordPress/wp-
config.php
cd /var/www/html/WordPress
sed -i "s/database_name_here/DBName/g" wp-config.php
sed -i "s/username_here/DB_MasterUsername/g" wp-config.php
sed -i "s/password_here/DB_MasterUserPassword/g" wp-config.php
sed -i "s/localhost/DB_ENDPOINT/g" wp-config.php
```

5. 同じディレクトリに、次の内容install_dependencies.shで を作成します。

```
#!/bin/bash
yum install -y php
yum install -y php-mysql
yum install -y mysql
service httpd restart
```

> **Note**
>
> HTTPS は、ヘルスチェックを最初から機能させるために、起動時にユーザーデータの一部としてインストールされます。

6. 同じディレクトリに、次の内容`start_server.sh`で を作成します。

   - Amazon Linux インスタンスの場合は、以下を使用します。

   ```
   #!/bin/bash
   service httpd start
   ```

   - RHEL インスタンスの場合は、以下を使用します (追加のコマンドは、SELINUX が WordPress を受け入れることを許可するポリシーです) 。

   ```
   #!/bin/bash
   setsebool -P  httpd_can_network_connect_db 1
   setsebool -P  httpd_can_network_connect 1
   chcon -t httpd_sys_rw_content_t /var/www/html/WordPress/wp-content -R
   restorecon -Rv /var/www/html
   service httpd start
   ```

7. 同じディレクトリに、次の内容`stop_server.sh`で を作成します。

   ```
   #!/bin/bash
   service httpd stop
   ```

8. zip バンドルを作成します。

   Linux:

   ```
   $ cd /tmp/WordPress
   $ zip -r wordpress.zip .
   ```

   Windows: WordPress」ディレクトリに移動し、すべてのファイルを選択して zip ファイルを作成します。必ず wordpress.zip という名前を付けます。

1. アプリケーションバンドルを S3 バケットにアップロードする

スタックのデプロイを続行するには、パッケージが設定されている必要があります。

作成した S3 バケットインスタンスに自動的にアクセスできます。踏み台 (「インスタンスへのアクセス」を参照) または S3 コンソールからアクセスし、drag-and-dropで CodeDeploy パッケージをアップロードするか、 ファイルを参照して選択します。

シェルウィンドウで次のコマンドを使用することもできます。zip ファイルへの正しいパスがあることを確認してください。

```
aws s3 cp wordpress/wordpress.zip s3://BUCKET_NAME/
```

2. WordPress CodeDeploy アプリケーションバンドルをデプロイする

必須データコードアプリケーションのデプロイ：

- CodeDeployApplicationName: CodeDeploy アプリケーションに付けた名前。
- CodeDeployGroupName: CodeDeploy アプリケーションとグループはどちらも HA スタック RFC で CodeDeploy アプリケーションに付けた名前から作成されたため、これは CodeDeployApplicationName と同じ名前です。
- S3Bucket: S3 バケットに付けた名前。
- S3BundleType と S3Key: これらはデプロイした WordPress アプリケーションバンドルの一部です。
- VpcId: 関連する VPC。

a. RFC の作成ページで、RFC CT ピックリストから、カテゴリデプロイ、サブカテゴリアプリケーション、項目 CodeDeploy アプリケーション、およびオペレーションデプロイを選択します。
b. デフォルトの基本オプションを保持し、図のように値を設定します。

> **Note**
> 以前に作成した CodeDeploy アプリケーション、CodeDeploy デプロイグループ、S3 バケット、バンドルを参照してください。

```
Subject:                                WP-CD-Deploy-RFC
Description:                            DeployWordPress
```

```
S3Bucket:                                BUCKET_NAME
S3Key:                                   wordpress.zip
S3BundleType:                            zip
CodeDeployApplicationName:               WordPress
CodeDeployDeploymentGroupName:           WordPress
CodeDeployIgnoreApplicationStopFailures: false
RevisionType:                            S3



VpcId:                                   VPC_ID
Name:                                    WP-CD-Deploy-Op
TimeoutInMinutes:                        60
```

c. 完了したら送信をクリックします。

アプリケーションのデプロイを検証する

WordPress デプロイパス: /WordPress を使用して、以前に作成したロードバランサーのエンドポイント (LoadBalancerCName) WordPress に移動します。例:

```
http://stack-ID-FOR-ELB.us-east-1.elb.amazonaws.com/WordPress
```

次のようなページが表示されます。

高可用性デプロイのティアダウン

デプロイを破棄するには、HA 2 階層スタックと S3 バケットに対して Delete Stack CT を送信し、RDS スナップショットの削除をリクエストできます (10 日後に自動的に削除されますが、その間は少額のコストがかかります)。HA スタックと S3 バケットのスタック IDs を収集し、以下の手順に従います。「スタック | 削除」を参照してください。

付録: SALZ オンボーディングアンケート

トピック

- デプロイの概要
- 環境アーキテクチャに関する考慮事項
- 単一アカウントランディングゾーンのモニタリングアラート

- メンテナンスウィンドウ
- 次のステップ

これは、アカウントをオンボーディングする前に考慮すべき情報の一部です。

デプロイの概要

デプロイの説明。例:

- このアカウントは、 (製品アプリケーションのデプロイではなく) Line-of-Business アプリケーションのデプロイ用です。
- デプロイには、アカウントのパブリックサブネットまたは DMZ サブネット内の自動スケーリングされた ARP (認証されたリバースプロキシ) が含まれます。
- ウェブサーバーとアプリケーションサーバーは、アカウントのプライベートサブネット内にデプロイされます。
- RDS (Amazon Relational Database Service) インスタンスもアカウントのプライベートサブネット内にデプロイされます。
- サーバー (ARP、ウェブ、アプリケーション、データベース、ロードバランサーなど) は、個別のセキュリティグループに分割されます。
- アカウントには、AZs) にまたがる HA (高可用性) 設計が必要です。

環境アーキテクチャに関する考慮事項

環境とアーキテクチャの設定方法については、次の基準を考慮してください。

- 仮想データセンターは企業ネットワークに接続されますか？
  - 既存の AWS DirectConnect サービスをお持ちですか、それとも新しい DirectConnect サービスが必要ですか？
  - 既存の VPN 接続があるか、新しい VPN サービスが必要ですか？
- 割り当てることができる内部アドレスの CIDR ブロック範囲は何ですか? (/16 推奨、企業ネットワーク範囲と重複してはいけません)
- 仮想データセンターにはインターネットアクセスが必要ですか？
- どのリージョン (複数可) を使用する予定ですか？ (シドニー/北 バージニア/ダブリン)
- 他のすべてのサブネットに接続しているアプリケーションをホストするために、共有サービスサブネットが必要ですか？

- 個別のサブネットとしてホストする組織部門は何ですか。それぞれについて：
  - 他のサブネットにはどのような接続が必要ですか？
  - サブネットにはインターネットアクセスが必要ですか？
  - そのサブネットにアプリケーションデプロイの制限はありますか？
  - そのサブネットに特定のネットワーク要件はありますか？
- 個別の開発環境やテスト環境が必要ですか？（いつでもアクセスできるように重複する共有サービスが含まれます）
- スナップショットのバックアップ要件は何ですか？
- 保持する既存のメンテナンスプロセスまたはパッチウィンドウ (複数可) はありますか？
- ドメイン登録の要件は何ですか？
- シングルサインオン要件はありますか? (AD、LDAP など）
- 予想される全体的なオペレーティングシステムと予想される容量要件は何ですか？

単一アカウントランディングゾーンのモニタリングアラート

AMS は、特定のモニタリングアラートに対して (AMS サービス通知を取得するのではなく) 直接アラートを受け取る方法を提供します。これにサインアップするには、Cloud Architect (CA または Cloud Service Delivery Manager (CSDM) がこの情報を受信していることを確認します。

ダイレクトアラート E メール: AMS が特定のリソースベースのアラートを送信する E メールアドレスです。E メールに直接送信されるアラートの詳細については、「シングルアカウントランディングゾーン用 AMS ユーザーガイド」の「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。AMS モニタリングの詳細については、「シングルアカウントランディングゾーン用 AMS ユーザーガイド」の「モニタリング管理」を参照してください。

メンテナンスウィンドウ

さまざまなアプリケーションのニーズ、異なるストレス期間 AWS リージョン、および異なるストレス期間を考慮したメンテナンスウィンドウを作成する必要があります。メンテナンスウィンドウは、AMS がパッチを適用する時刻です。次にいくつかのガイドラインを示します。

- ユーザーへの影響を制限するには、環境 AWS リージョン がデプロイされている に従ってメンテナンスウィンドウを計画します。
- 通常の営業時間外と、本番サーバーで予想されるトラフィックが最も少ない時間帯をスケジュールします。

- 通常、インフラストラクチャスタックには毎月の更新が必要です。
- メンテナンスウィンドウを少なくとも 300 分間スケジュールします。オペレーティングシステムのパッチ適用には 60～90 分、インフラストラクチャスタックのパッチ適用には 180～300 分かかります。

次のステップ

AMS オンボーディングチームは、アカウントを AMS にオンボーディングするすべてのステップを支援します。これらはオンボーディング要件です。

- AMS AWS アカウント に使用する新しい をプロビジョニングし、 AWS アカウント ID を指定します。
- 希望するレベルのサポートにサインアップします。
- クロスアカウント IAM ロールを作成して、AMS プロビジョニングアカウントにアクセス権を付与し、ロール名を AMS に提供します。
- アカウント 753102745277 を信頼されたエンティティとして追加します。

付録: ActiveDirectory フェデレーションサービス (ADFS) クレームルールと SAML 設定

AD FS をインストールして設定する方法のstep-by-stepについては、「Windows Active Directory、ADFS、および SAML 2.0 を使用した AWS へのフェデレーションの有効化」を参照してください。

ADFS クレームルールの設定

ADFS 実装が既にある場合は、以下を設定します。

- 信頼する側の信頼
- クレームルール

証明書利用者の信頼とクレームルールのステップは、Windows Active Directory、AD FS、および SAML 2.0 ブログを使用して AWS へのフェデレーションを有効にするから実行します。

- クレームルール：
  - Nameid: ブログ投稿ごとの設定
  - RoleSessionName: 次のように設定します
    - クレームルール名: **RoleSessionName**
    - 属性ストア: **Active Directory**
    - LDAP 属性: **SAM-Account-Name**
    - 送信クレームタイプ: **https://aws.amazon.com/SAML/Attributes/RoleSessionName**
    - AD グループの取得: ブログ投稿ごとの設定
    - ロールクレーム: 次のように を設定します。

```
c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-([^d]{12})-"]
```

```
=> issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value =
 RegExReplace(c.Value, "AWS-([^d]{12})-", "arn:aws:iam::$1:saml-provider/
customer-readonly-saml,arn:aws:iam::$1:role/"));
```

ウェブコンソール

〔*ADFS-FQDN]* を ADFS 実装の FQDN に置き換えることで、AWS ウェブコンソールにアクセスできます。

https://*[ADFS-FQDN]*/adfs/ls/IdpInitiatedSignOn.aspx

IT 部門は、グループポリシーを介して上記のリンクをユーザー母集団にデプロイできます。

SAML による API および CLI アクセス

SAML を使用して API および CLI アクセスを設定する方法。

Python パッケージは、以下のブログ記事から入手できます。

- NTLM: SAML 2.0 と AD FS を使用してフェデレーティッド API と CLI アクセスを実装する方法
- フォーム: SAML 2.0 を使用してフェデレーティッド API/CLI アクセスの一般的なソリューションを実装する方法
- PowerShell: Windows PowerShell を使用して AWS へのフェデレーティッド API アクセスをセットアップする方法

スクリプト設定

1. Notepad++ を使用して、デフォルトのリージョンを正しいリージョンに変更する
2. Notepad++ を使用して、テスト環境と開発環境の SSL 検証を無効にする
3. Notepad++ を使用して idpentryurl を設定する

```
https://[ADFS-FDQN]/adfs/ls/IdpInitiatedSignOn.aspx?
loginToRp=urn:amazon:webservices
```

Windows 設定

以下に、Python パッケージの手順を示します。生成された認証情報は 1 時間有効です。

1. Python をダウンロードしてインストールする (2.7.11)
2. AWS CLI ツールをダウンロードしてインストールする
3. AMS CLI をインストールします。

a. Cloud Service Delivery Manager (CSDM) が提供する AMS 頒布可能ファイルをダウンロードして解凍します。

   いくつかのディレクトリとファイルが利用可能になりました。

b. オペレーティングシステムに応じて、 Managed Cloud Distributables -> CLI -> Windows または Managed Cloud Distributables -> CLI -> Linux / MacOS ディレクトリを開きます。

   Windows の場合は、適切なインストーラを実行します (この方法は Windows 32 または 64 ビットシステムでのみ機能します) 。

   - 32 ビット: ManagedCloudAPI_x86.msi
   - 64 ビット: ManagedCloudAPI_x64.msi

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

c. 企業の認証情報を AWS とのフェデレーション (AMS デフォルト設定) 経由で使用する場合は、フェデレーションサービスにアクセスできる認証情報管理ツールをインストールする必要があります。例えば、この AWS セキュリティブログの How to Implement Federated API and CLI Access Using SAML 2.0 and AD FS を使用して、認証情報管理ツールの設定に役立てることができます。

d. インストール後、 `aws amscm help`と `aws amsskms help` を実行してコマンドとオプションを表示します。

4. 必要な SAML スクリプトをダウンロードする

   c:\aws\scripts にダウンロードする

5. PIP のダウンロード

   c:\aws\downloads にダウンロードする

6. PowerShell を使用して PIP をインストールする

   <pythondir>.\python.exe c:\aws\downloads\get-pip.py

7. PowerShell を使用して boto モジュールをインストールする

   <pythondir\scripts>pip install boto

8. PowerShell を使用してリクエストモジュールをインストールする

<pythondir\scripts>pip インストールリクエスト

9. PowerShell を使用してリクエストセキュリティモジュールをインストールする

   <pythondir\scripts>pip インストールリクエスト〔セキュリティ〕

10. PowerShell を使用して beautifulsoup モジュールをインストールする

    <pythondir\scripts>pip install beautifulsoup4

11. PowerShell を使用して、ユーザープロファイルに .aws というフォルダを作成します (%userprofile%\.aws)。

    mkdir .aws

12. PowerShell を使用して、.aws フォルダに認証情報ファイルを作成します。

    New-Item 認証情報 - タイプファイル –force

    認証情報ファイルにはファイル拡張子を付けることはできません

    ファイル名はすべて小文字で、名前認証情報が必要です

13. メモ帳を使用して認証情報ファイルを開き、正しいリージョンを指定して次のデータに貼り付けます。

```
[default]
output = json
region = us-east-1
aws_access_key_id =
aws_secret_access_key =
```

14. PowerShell を使用した SAML スクリプトとログオン

    <pythondir>.\python.exe c:\aws\scripts\samlapi.py

    ユーザー名: [USERNAME]@upn

    引き受けるロールを選択する

Linux 設定

生成された認証情報は 1 時間有効です。

1. WinSCP を使用して SAML スクリプトを転送する
2. WinSCP を使用してルート CA 証明書を転送する (テストと開発には無視)
3. 信頼できるルート証明書に ROOT CA を追加する (テストと開発には無視)

   $ openssl x509 -inform der -in [certname].cer -out certificate.pem (テストと開発には無視)

   certificate.pem の内容を /etc/ssl/certs/ca-bundle.crt ファイルの末尾に追加する ((テスト開発では無視)
4. home/ec2-user 5 に .aws フォルダを作成する

```
[default]
output = json
region = us-east-1
aws_access_key_id =
aws_secret_access_key =
```

5. WinSCP を使用して認証情報ファイルを .aws フォルダに転送する
6. boto モジュールをインストールする

   $ sudo pip install boto
7. リクエストモジュールをインストールする

   $ sudo pip インストールリクエスト
8. beautifulsoup モジュールをインストールする

   $ sudo pip install beautifulsoup4
9. スクリプトを home/ec2-user にコピーする

   必要なアクセス許可を設定する

   スクリプトを実行する: samlapi.py

ドキュメント履歴

次の表は、AMS の前回のリリース以降のドキュメントの重要な変更点を示しています。

- API バージョン: 2019-05-21
- ドキュメントの最終更新日: 2025 年 9 月 23 日

変更	説明	日付
AWS Managed Services の SageMaker AI でのエンドポイントの自動スケーリングに関する FAQ セクションの変更タイプを更新しました	AMS SSP を使用して、AMS アカウントに Amazon SageMaker AI をプロビジョニングします。 管理を使用して RFC を送信する | 高度なスタックコンポーネント | Identity and Access Management (IAM) | エンティティまたはポリシー (レビューが必要) の変更タイプ (ct-27tuth19k52b4) を更新して、自動スケーリングのアクセス許可を一時的または永続的に昇格させます。これは、自動スケーリングには CloudWatch サービスへの許可付きアクセスが必要なためです。	2025 年 9 月 25 日
正確な変更タイプのリファレンス	セキュリティグループを作成、変更、または削除します。 ユーザーを追加するには: Management | Directory Service | Users and groups | Add user to group [ct-24pi85mjtza8k] を使用して RFC を送信し、ユーザーを削除するには: Management | Directory Service | Users and groups | Remove user from group [ct-2019s9y3nfml4] を使用して RFC を送信します。	2025 年 8 月 8 日
TOC リンクの削除	TOC AWS 用語集リンクを削除しました。	2025 年 8 月 8 日

変更	説明	日付
処方ガイダンスのリンクを追加しました	一括請求を設定する – 新しいアカウントを支払いアカウントにリンクする.	2025 年 5 月 8 日
への IAM アクセスをアクティブ化する手順を更新しましたAWS マネジメントコンソール	への IAM アクセスをアクティブ化する手順を明確にしましたAWS マネジメントコンソール。	AWS コンソールへの IAM アクセスをアクティブ化する
Direct Connect 専用接続で許可されるトランジット仮想インターフェイスの数を更新しました	Direct Connect 専用接続では、接続あたり 4 つのトランジット仮想インターフェイスに制限されるようになりました。	Direct Connect を Transit Gateway に接続する
文言を改善します。	AMS のモニタリングと管理オペレーションを確実にするために、「Deny」リストとしてのみ使用される「Allow All」を含める必要があることを指定しました。	ネットワーク構成
AMS CLI の使用に関する追加情報。	「一部の CLI コマンドには `--region`オプションが必要になる場合があることに注意してください」	AMS CLIs のインストール
更新: 一貫性と読みやすさに関する章見出し、一部のトピックサブセクションをより適切なセクションに移動	「変更管理の変更」は「変更管理」の新しい見出しです。	変更管理モード
更新された内容	以前は「変更管理モード」または「標準 CM モード」と呼ばれていた AMS モードは、「RFC モード」と呼ばれるようになりました。モードセクションが展開されました。	RFC モード.

変更	説明	日付
更新された内容	以前は「変更管理モード」または「標準 CM モード」と呼ばれていた AMS モードは、「RFC モード」と呼ばれるようになりました。モードセクションが短縮され、モードに関する AMS アドバンストユーザーガイドセクションへのリンクが追加されました。	AMS モード.
MALZ: ネットワークアーキテクチャ図を更新	ネットワークアカウントアーキテクチャm	2022 年 6 月 16 日
トピックリストを以下の段落に移動	AWS Managed Servicesオンボーディングの概要	2022 年 6 月 16 日
コンテンツの更新、包括的な言語イニシアチブ	「マスターアカウント」ではなく「管理アカウント」。	AMS の IAM ユーザーロール、「ポリシーの例」セクション
更新されたコンテンツ、ツールアカウントのロール名	ロール名 CustomerMigrationAccessRole を AWSManagedServicesMigrationRole に更新しました。	AWS アプリケーション移行サービス (AWS MGN)
SALZ: 継続性管理のデフォルト	リンクを更新し、 から古い情報を削除 VPC タグとデフォルト	2022 年 2 月 28 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。