aws

ユーザーガイド

AWS Systems Manager

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Systems Manager: ユーザーガイド

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標およびトレードドレスは、Amazon のものではない製品またはサービスと関連付けてはならず、また、お客様に混乱を招くような形や Amazon の信用を傷つけたり失わせたりする形で使用することはできません。Amazon が所有していない他のすべての商標は、それぞれの所有者の所有物であり、Amazon と提携、接続、または後援されている場合とされていない場合があります。

Table of Contents

AWS Systems Manager とは 1
Systems Manager が業務にもたらす利点 2
Systems Manager はどのようなユーザーにお勧めか 2
Systems Manager の主な機能とは 3
サポートされている AWS リージョン 3
Systems Manager へのアクセス 4
Systems Manager サービス名履歴 5
サポートされているオペレーティングシステムとマシンタイプ 6
System Manager でサポートされているオペレーティングシステム 6
ハイブリッドおよびマルチクラウド環境でサポートされるマシンタイプ 13
統合コンソールとは 14
AWS Systems Manager のマネージドノードのセットアップ 16
Systems Manager を利用した EC2 インスタンスの管理 16
Systems Manager に必要なインスタンスのアクセス許可を設定する 17
Systems Manager のために VPC エンドポイントを使用して EC2 インスタンスのセキュリティを強化する 29
Systems Manager を利用したハイブリッド環境およびマルチクラウド環境でのノードの管理 33
ハイブリッドおよびマルチクラウド環境で Systems Manager に必要な IAM サービスロールを作成する 36
ハイブリッドアクティベーションを作成して、Systems Manager にノードを登録する 44
ハイブリッド Linux ノードで SSM Agent をインストールする 51
ハイブリッド Windows Server ノードに SSM Agent をインストールする 58
Systems Manager を利用したエッジデバイスの管理 62
エッジデバイス用の IAM サービスロールを作成 64
AWS IoT Greengrass のためにエッジデバイスを設定する 70
AWS IoT Greengrass トークン交換ロールを更新して SSM Agent をエッジデバイスにインストールします。 70
Systems Manager 用の AWS Organizations 委任された管理者の作成 71
Change Manager での委任された管理者の使用 71
Explorer での委任された管理者の使用 72
OpsCenter での委任された管理者の使用 72
Quick Setup での委任された管理者の使用 73
一般的なセットアップ 73

AWS アカウントへのサインアップ ... 73
管理アクセスを持つユーザーを作成する ... 74
AWS Systems Manager を設定する ... 76
Systems Manager コンソールアクセスのセットアップ ... 76
Systems Manager オンボーディングポリシー ... 76
AWS Systems Manager コンソールオペレーターのポリシー ... 82
AWS Systems Manager コンソールオペレーターの読み取り専用ポリシー ... 86
組織用の Systems Manager 統合コンソールのセットアップ ... 88
前提条件 ... 89
統合コンソールリソース ... 89
統合コンソールをセットアップする ... 92
単一のアカウントとリージョン用の Systems Manager 統合コンソールのセットアップ ... 94
統合コンソールリソース ... 94
統合コンソールをセットアップする ... 96
Systems Manager 統合コンソールの無効化 ... 97
ノード管理タスクの実行 ... 99
ノードインサイトの確認 ... 99
ウィジェットの追加または削除 ... 102
ウィジェットの再配置 ... 103
ノードの探索 ... 104
コンソールフィルターを使用したノードの探索 ... 104
Amazon Q でテキストプロンプトを使用したノードの探索 ... 110
個々のノードの詳細の表示およびノードに対するアクションの実行 ... 116
マネージドノードレポートのダウンロードまたはエクスポート ... 118
ノードレポートのコンテンツと外観の管理 ... 122
Systems Manager を使用したジャストインタイムノードアクセス ... 123
Systems Manager でジャストインタイムアクセスをセットアップする ... 125
ジャストインタイムノードアクセスセッションを開始する ... 171
ジャストインタイムアクセスリクエストを管理する ... 173
Session Manager からジャストインタイムノードアクセスに移行する ... 174
Systems Manager でジャストインタイムアクセスを無効にする ... 179
よくある質問 ... 179
診断と修復 ... 181
失敗したデプロイの診断と修復 ... 183
ドリフトした設定の診断と修復 ... 184
アンマネージド Amazon EC2 インスタンスの診断と修復 ... 185

ランブックアクションの修復の影響タイプ 192
修復の実行履歴の詳細の表示 195
Systems Manager 設定の調整 196
アカウントセットアップ設定 196
組織のセットアップの設定 196
[診断および修復] の設定 197
Systems Manager での Amazon S3 バケットとバケットポリシーの使用 199
AWS Systems Manager ツールの使用方法 208
ノードツール 208
変更管理ツール 210
アプリケーションツール 212
運用ツール 213
Systems Manager を使用したノードタスクの実行 214
前提条件 214
SSM Agent がプリインストールされた AMI を使用してインスタンスを起動する 214
Systems Manager を使用してマネージドインスタンスに接続する 215
インスタンスのクリーンアップ 216
ノードツール 216
コンプライアンス 217
Distributor 236
Fleet Manager 293
ハイブリッドアクティベーション 381
インベントリ 383
Patch Manager 478
Run Command 794
Session Manager 861
State Manager 1012
変更管理ツール 1112
オートメーション 1113
Change Calendar 1585
Change Manager 1605
ドキュメント 1690
Maintenance Windows 1825
Quick Setup 1958
アプリケーションツール 212
AWS AppConfig 2008

Application Manager 2009
Parameter Store 2056
運用ツール 2212
Incident Manager 2213
Explorer 2213
OpsCenter 2252
CloudWatch ダッシュボード 2338
「SSM Agent」 の使用 2339
SSM Agent に関する技術的な詳細を知る 2340
SSM Agent バージョン 3.2.x.x 認証情報の動作 2340
SSM Agent 認証情報の優先順位 2340
連邦情報処理規格 (FIPS) での使用のための SSM Agent の設定 2342
ローカル ssm-user アカウントについて 2344
SSM Agentと Instance Metadata Service (IMDS) 2345
SSM Agent を最新の状態に維持 2345
SSM Agent インストールディレクトリが変更、移動、削除されていないことの確認 2346
AWS リージョン による SSM Agent のローリング更新 2346
SSM Agent と AWS マネージド S3 バケットとの通信 2347
SSM Agent がプリインストールされている AMIs を見つける 2355
SSM Agent のステータスを確認する 2356
Linux 用 EC2 インスタンスで SSM Agent を使用する 2361
SSM Agent の署名の確認 2361
Linux 用 EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする 2376
Linux ノードでプロキシを使用するための SSM Agent の設定 2436
macOS 用 EC2 インスタンスで SSM Agent を使用する 2441
macOS 用の EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする 2442
Windows Server 用 EC2 インスタンスで SSM Agent を使用する 2444
Windows Server 用の EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする 2445
SSM Agent が Windows Server インスタンス用にプロキシを使用するように設定する 2448
SSM Agent ステータスの確認とエージェントの起動 2452
SSM Agent バージョン番号の確認 2454
SSM Agent ログの表示 2459
SSM Agentデバッグログの有効化 2460

SSM Agent を介してルートレベルコマンドへのアクセスを制限する 2462
SSM Agent への更新の自動化 2463
SSM Agent の自動更新 2465
SSM Agent 通知にサブスクライブする 2466
SSM Agent のトラブルシューティング 2467
SSM Agent が最新ではない 2468
SSM Agent ログファイルを使用して問題をトラブルシューティングする 2468
エージェントログファイルがローテーションしない (Windows) 2469
SSM エンドポイントに接続できない 2469
VPC 設定を検証する 2470
VPC DNS 関連の属性を検証する 2471
エンドポイントセキュリティグループでイングレスルールを検証する 2471
ssm-cli を使用してマネージドノードの可用性をトラブルシューティングする 2472
セキュリティ 2473
データ保護 2474
データ暗号化 2475
インターネットトラフィックのプライバシー 2478
アイデンティティ/アクセス管理 2478
対象者 2478
アイデンティティを使用した認証 2479
ポリシーを使用したアクセス権の管理 2482
AWS Systems Manager と IAM の連携方法 2486
アイデンティティベースポリシーの例 2497
AWS マネージドポリシー 2508
トラブルシューティング 2563
サービスリンクロールの使用 2565
インベントリおよび Explorer データロール 2566
OpsCenter および Explorer のアカウント検出ロール 2569
OpsData および OpsItems 作成ロール 2572
オペレーションインサイト作成ロール 2576
Quick Setup デプロイヘルスチェックロール 2580
OpsData サービスロールをエクスポートする 2583
ジャストインタイムノードアクセスサービスロール 2585
ジャストインタイムノードアクセスリクエスト通知サービスロール 2589
ログ記録とモニタリング 2593
コンプライアンス検証 2596

耐障害性 ... 2597
インフラストラクチャセキュリティ ... 2597
設定と脆弱性の分析 ... 2597
セキュリティに関するベストプラクティス ... 2598
Systems Manager の予防的セキュリティのベストプラクティス ... 2598
Systems Manager のモニタリングと監査のベストプラクティス ... 2602
コードの例 ... 2605
基本 ... 2612
こんにちは、Systems Manager ... 2616
基本を学ぶ ... 2620
アクション ... 2672
ログ記録とモニタリング ... 2952
モニタリングツール ... 2953
統合された CloudWatch Logs へのノードログの送信 (CloudWatch エージェント) ... 2953
Windows Server ノードのログ収集を CloudWatch エージェントに移行する ... 2955
CloudWatch エージェントの設定を Parameter Store に保存する ... 2965
SSM Agent でのログ収集へのロールバック ... 2966
CloudWatch Logs に SSM Agent ログを送信する ... 2970
変更リクエストイベントのモニタリング ... 2973
オートメーションのモニタリング ... 2976
オートメーションメトリクス ... 2976
Amazon CloudWatch を使用した Run Command メトリクスのモニタリング ... 2977
Systems Manager Run Command のメトリクスとディメンション ... 2978
AWS Systems Manager による AWS CloudTrail API コールのログ記録 ... 2979
CloudTrail の Systems Manager データイベント ... 2980
CloudTrail の Systems Manager 管理イベント ... 2982
Systems Manager のイベント例 ... 2982
CloudWatch Logs を使用した自動アクション出力のログ記録 ... 2988
Run Command の Amazon CloudWatch Logs の設定 ... 2992
コマンド送信時に CloudWatch Logs を指定する ... 2993
CloudWatch Logs でのコマンド出力の表示 ... 2994
Amazon EventBridge を使用してモニタリングする ... 2994
Systems Manager イベント用の EventBridge を設定する ... 2996
Systems Manager 用の Amazon EventBridge イベントの例 ... 2999
サンプルシナリオ: Amazon EventBridge ルールのSystems Manager ターゲット ... 3014
Amazon SNS 通知を使用した Systems Manager のステータス変更のモニタリング ... 3016

AWS Systems Manager の Amazon SNS 通知の設定 ... 3017
AWS Systems Manager の Amazon SNS 通知の例 ... 3028
Run Command を使用してステータス通知を返すコマンドを送信する ... 3030
メンテナンスウィンドウを使用して、ステータス通知を返すコマンドを送信する ... 3033
製品およびサービスの統合 ... 3039
AWS のサービス との統合 ... 3039
コンピューティング ... 3039
IoT ... 3042
[Storage (ストレージ)] ... 3043
開発者用ツール ... 3044
セキュリティ、アイデンティティ、およびコンプライアンス ... 3045
暗号化と PKI ... 3048
マネジメントとガバナンス ... 3048
ネットワークとコンテンツ配信 ... 3054
分析 ... 3055
アプリケーション統合 ... 3057
AWS Management Console ... 3058
Amazon S3 からのスクリプトの実行 ... 3058
Parameter Store パラメータからの AWS Secrets Manager シークレットの参照 ... 3063
Parameter Store SecureString パラメータの AWS KMS 暗号化 ... 3069
Amazon Elastic Kubernetes Service で AWS Secrets Manager シークレットを使用する ... 3082
AWS Lambda 関数での Parameter Store パラメーターの使用 ... 3102
その他の製品やサービスとの統合 ... 3125
GitHub からのスクリプトの実行 ... 3129
Systems Manager Compliance で Chef InSpec プロファイルを使用する ... 3137
ServiceNow との統合 ... 3143
AWS Systems Manager リファレンス ... 3144
AWS SDK の操作 ... 3145
パッチ適用オペレーション用の Amazon S3 バケット ... 3146
パッチ適用オペレーション用の SSM Command ドキュメントが含まれるバケット (Linux および Windows Server) ... 3147
パッチ適用オペレーション用の SSM Command ドキュメントが含まれるバケット (macOS) ... 3150
AWS が管理するパッチベースラインのスナップショットが含まれるバケット ... 3153
Systems Manager 用の EventBridge イベントパターンとタイプ ... 3156
イベントタイプ: オートメーション ... 3157

イベントタイプ: Change Calendar 3158
イベントタイプ: Change Manager 3158
イベントタイプ: 設定コンプライアンス 3158
イベントタイプ: インベントリ 3159
イベントタイプ: メンテナンスウィンドウ 3160
イベントタイプ: OpsCenter 3162
イベントタイプ: Parameter Store 3163
イベントタイプ: Run Command 3163
イベントタイプ: State Manager 3164
cron 式または rate 式 3165
cron 式または rate 式に関する一般情報 3165
関連付けのための cron および rate 式 3170
メンテナンスウィンドウの関連付けに使用する cron 式および rate 式 3173
ec2messages、ssmmessages およびその他の API オペレーション 3175
エージェント関連の API オペレーション (ssmmessages および ec2messages エンドポイント) 3176
ssm:* 名前空間インスタンス関連の API オペレーション 3178
ssm:* 名前空間の他の API オペレーション 3180
Systems Manager の日付および時刻の文字列のフォーマット 3180
Systems Manager の日付と時刻文字列を書式設定する 3181
Systems Manager のカスタム日付と時刻文字列を作成する 3181
ユースケースとベストプラクティス 3184
Systems Manager リソースとアーティファクトの削除 3187
State Manager または Maintenance Windows の選択 3192
State Manager および Maintenance Windows: 主要なユースケース 3192
関連情報 3199
ドキュメント履歴 3201
2018 年 6 月以前のアップデート 3411
ドキュメントの表記規則 3430

AWS Systems Manager とは

AWS Systems Manager では、オンプレミスでもマルチクラウド環境でも、AWS 内のノードを広範囲にわたって一元的に表示、管理、および運用できます。統合コンソールエクスペリエンスのリリースにより、Systems Manager では AWS アカウントと AWS リージョン全体にわたってよく使用するノードタスクを完了できるさまざまなツールが統合されています。

Systems Manager を使用するには、ノードを管理する必要があります。つまり、SSM Agent がマシンにインストールされ、Systems Manager サービスと通信できる必要があります。ノードが管理対象としてレポートされていない理由を特定できるように、Systems Manager にはワンクリックエージェント問題診断および修復ランブックが用意されており、定義したスケジュールに従ってこれを自動的に実行するように設定できます。この機能により、ネットワークの設定ミスなど、ノードが Systems Manager に接続できない理由を特定できます。この機能には、ネットワークの問題のほか、ノードをマネージドノードとして設定することを阻害しているその他の問題を修復するのに適したお勧めのランブックも用意されています。

統合コンソールエクスペリエンスには、ノードの概要を把握できるダッシュボードも用意されています。古くなったオペレーティングシステム (OS) ソフトウェアを実行しているノードなど、さらに具体的なノードインサイトをドリルダウンできます。また、フィルターを使用して OS、OS のバージョン、AWS リージョン、AWS アカウント、SSM Agent のバージョンといったインスタンスメタデータに基づいてきめ細かなビューを表示することもできます。こうしたフィルターにより、組織全体にわたって特定のアカウントレベルやアプリケーションレベルで関連情報を取得できます。

トピック

- Systems Manager が業務にもたらす利点
- Systems Manager はどのようなユーザーにお勧めか
- Systems Manager の主な機能とは
- サポートされている AWS リージョン
- Systems Manager へのアクセス
- Systems Manager サービス名履歴
- サポートされているオペレーティングシステムとマシンタイプ
- 統合コンソールとは

Systems Manager が業務にもたらす利点

Systems Manager には、次のような利点があります。

- インフラストラクチャ全体にわたって可視性を強化

  Systems Manager では、組織のアカウントとリージョン全体のノードを一元的に表示できます。ID、名前、OS の詳細、インストールされたエージェントといったインスタンス情報にすばやくアクセスできます。Amazon Q Developer を使用して自然言語でインスタンスメタデータにクエリを実行し、問題を特定して迅速に対策を講じることができます。

- 自動化で業務効率が向上

  よく使用する運用タスクを自動化して、システムを保守するために必要な時間と労力を削減できます。Systems Manager では、サーバーにログインしなくても、広範囲にわたってノードをリモートから安全確実に管理できます。踏み台ホスト、SSH、リモート PowerShell を使用する必要がなくなりました。Systems Manager では、レジストリの編集、ユーザー管理、ソフトウェアやパッチのインストールなど、ノードグループ全体でよく使用する管理タスクも簡単に自動化できます。

- あらゆる環境で広範囲にわたってノード管理を簡素化

  Systems Manager では、AWS、オンプレミス、マルチクラウド環境全体にわたってノードを管理できます。SSM Agent の問題を特定してワンクリックランブックで修復する自動診断をスケジュールします。ノードをマネージドノードとして設定したら、セキュリティパッチを適用する、ログ記録セッションを開始する、リモートからコマンドを実行するといった重要な運用タスクを実行できます。

Systems Manager はどのようなユーザーにお勧めか

Systems Manager は、IT オペレーションマネージャーとオペレーター、DevOps エンジニア、セキュリティマネージャー、コンプライアンスマネージャー、IT 担当取締役、CIO によって使用されています。大まかに言うと、Systems Manager は次のような組織に適しています。

- 広範囲にわたってノードの管理とセキュリティを改善したい組織。
- インフラストラクチャを管理するときに可視性と運用の俊敏性を高めたい組織。
- 広範囲にわたって業務効率を高めたい組織。

Systems Manager の主な機能とは

Systems Manager の主な機能は、統合コンソールと Systems Manager が提供する個々のツールとの間で共有されるため、ノードを大規模に管理できます。

統合コンソール

統合コンソールでは、ノードの閲覧や管理を一元的に行うことができます。このコンソールでは Systems Manager のさまざまなツールを活用できるほか、以下の機能を利用できます。

- ノードの一元的なビュー
- ノードの詳細なインサイト
- ノードによく見られる問題の自動診断と修復

統合コンソールの詳細については、「統合コンソールとは」を参照してください。

ツール

ツールには、Systems Manager の個々の機能のほか、Run Command、Session Manager、Automation、Parameter Store などがあります。Systems Manager ツールでは、次のことを実行できます。

- 広範囲にわたってノードにパッチを適用する
- インバウンドポートを開かずにノードに安全に接続する
- ノードで遠隔的にコマンドを実行する
- アプリケーションが参照するデータを安全に保存する
- 一般的なシステム管理タスクを自動化する

Systems Manager ツールの詳細については、「AWS Systems Manager ツールの使用方法」を参照してください。

サポートされている AWS リージョン

Systems Manager ツールをサポートしている AWS リージョンの一覧については、「Amazon Web Services 全般のリファレンス」の「Systems Manager のサービスエンドポイント」を参照してください。

2024 年 11 月 21 日にリリースされた Systems Manager 統合コンソールは、次の AWS リージョンで利用できます。

- US East (N. Virginia) Region
- US East (Ohio) Region
- 米国西部 (北カリフォルニア) リージョン
- 米国西部 (オレゴン) リージョン
- カナダ (中部) リージョン
- 南米 (サンパウロ) リージョン
- アジアパシフィック (ムンバイ) リージョン
- アジアパシフィック (東京) リージョン
- Asia Pacific (Seoul) Region
- アジアパシフィック (シンガポール) リージョン
- アジアパシフィック (シドニー) リージョン
- 欧州 (フランクフルト) リージョン
- 欧州 (ストックホルム) リージョン
- 欧州 (アイルランド) リージョン
- 欧州 (ロンドン) リージョン
- 欧州(パリ)リージョン

Systems Manager へのアクセス

Systems Manager は、次のいずれかの方法で使用できます。

Systems Manager コンソール

Systems Manager コンソールは、Systems Manager にアクセスして使用するための、ブラウザベースのインターフェイスです。

AWS IoT Greengrass V2 コンソール

Greengrass コンソールの AWS IoT Greengrass 用に設定されたエッジデバイスを確認と管理できます。

AWS コマンドラインツール

AWS コマンドラインツールを使用して、システムのコマンドラインでコマンドを発行することで、Systems Manager および他の AWS タスクを実行できます。これらのツールは Linux、macOS、および Windows でサポートされています。AWS Command Line Interface (AWS CLI) を使用した方が、コンソールを使用するよりも高速で便利です。コマンドラインツールは、AWS のタスクを実行するスクリプトを作成する場合に便利です。

AWS には、AWS Command Line Interface と AWS Tools for Windows PowerShell という 2 セットのコマンドラインツールが用意されています。AWS CLI のインストールおよび使用の方法については、「AWS Command Line Interface ユーザーガイド」を参照してください。Tools for Windows PowerShell のインストールおよび使用の方法については、AWS Tools for Windows PowerShellユーザーガイドを参照してください。

> **Note**
>
> Windows Server インスタンスでは、特定の SSM ドキュメント (例: レガシー Windows PowerShell 3.0 ドキュメント) を実行するには、`AWS-ApplyPatchBaseline` 以降が必要です。Windows Server インスタンスが Windows Management Framework 3.0 以降を実行中であることを確認します。このフレームワークには、Windows PowerShell が含まれます。

AWS SDK

AWS には、さまざまなプログラミング言語およびプラットフォーム (Java、Python、Ruby、.NET、iOS、Android、および など) のライブラリとサンプルコードで構成されたソフトウェア開発キット (SDK) が用意されています。SDK は、Systems Manager へのアクセス権をプログラムによって許可するのに役立ちます。ダウンロードやインストールなどの方法を含む AWS SDK の詳細については、「Tools for Amazon Web Services」(Amazon Web Services 用のツール) を参照してください。

Systems Manager サービス名履歴

AWS Systems Manager (Systems Manager) の以前の名称は 「Amazon Simple Systems Manager (SSM)」 および 「Amazon EC2 Systems Manager (SSM)」 でした。サービスの元の省略名「SSM」は、他のいくつかのサービスコンソールを含むさまざまな AWS リソースにまだ反映されています。例:

- Systems Manager Agent: SSM Agent
- Systems Manager パラメータ： SSM パラメータ
- Systems Manager サービスのエンドポイント: `ssm.region.amazonaws.com`
- AWS CloudFormation リソースタイプ: `AWS::SSM::Document`
- AWS Config ルール識別子: `EC2_INSTANCE_MANAGED_BY_SSM`
- AWS Command Line Interface (AWS CLI) コマンド: `aws ssm describe-patch-baselines`
- AWS Identity and Access Management (IAM) 管理ポリシー名: `AmazonSSMReadOnlyAccess`
- Systems Manager リソース ARN: `arn:aws:ssm:region:account-id:patchbaseline/pb-07d8884178EXAMPLE`

サポートされているオペレーティングシステムとマシンタイプ

Systems Manager を使用する前に、オペレーティングシステム (OS)、OS バージョン、およびマシンタイプがマネージドノードとしてサポートされていることを確認してください。

トピック

- System Manager でサポートされているオペレーティングシステム
- ハイブリッドおよびマルチクラウド環境でサポートされるマシンタイプ

System Manager でサポートされているオペレーティングシステム

次のセクションでは、Systems Manager がサポートする OS と OS のバージョンを表示します。

> **Note**
>
> Systems Manager で AWS IoT Greengrass コアデバイスを管理と設定する場合、それらのデバイスは AWS IoT Greengrass の要件を満たす必要があります。詳細については、AWS IoT Greengrass Version 2 デベロッパーガイドの「AWS IoT Greengrass コアデバイスの設定」を参照してください。
>
> AWS IoT と非 AWS エッジデバイスを管理と設定する場合、それらのデバイスはここに記載されている要件を満たし、Systems Manager のオンプレミスマネージドノードとして設定されている必要があります。詳細については、「Systems Manager を利用したエッジデバイスの管理」を参照してください。

> **Important**
>
> Systems Manager のツールの 1 つである Patch Manager は、このトピックに記載されているすべての OS バージョンをサポートしていない場合があります。Patch Manager でサポートされているバージョンの詳細なリストについては、「Patch Manager の前提条件」を参照してください。

オペレーティングシステムタイプ

- リナックス
- macOS (Amazon EC2 インスタンスのみ)
- Raspberry Pi OS (旧称 Raspbian)
- Windows Server

OS プラットフォームを選択すると、サポートされているメジャーバージョンとマイナーバージョンが表示されます。

リナックス

AlmaLinux

バージョン	x86	x86_64	ARM64
8.3 ~ 8.10		✓	✓
9.x		✓	✓

Amazon Linux 1

バージョン	x86	x86_64	ARM64
2012.03 ~ 2018.03	✓	✓	

> **Note**
>
> バージョン 2015.03 以降では、Amazon Linux 1 は、x86_64 バージョンでのみリリースされています。

Amazon Linux 1 は、2020 年 12 月 31 日に標準サポートが終了し、2023 年 12 月 31 日に廃止されました。これは、「AWS ニュースブログ」の「Amazon Linux AMI 廃止に関するアップデート」でお知らせしています。AWS では、このオペレーティングシステム向けの Amazon Machine Images (AMIs) の提供を終了しました。ただし、AWS Systems Manager では、既存の Amazon Linux 1 インスタンスは引き続きサポートします。

Amazon Linux 2

バージョン	x86	x86_64	ARM64
2.0 および以降のすべてのバージョン		✓	✓

Amazon Linux 2023

バージョン	x86	x86_64	ARM64
2023.0.20230315.0 以降のすべてのバージョン		✓	✓

Bottlerocket

バージョン	x86_64	ARM64
1.0.0 以降のすべてのバージョン	✓	✓

CentOS

バージョン	x86	x86_64	ARM64
6.x[1]	✓	✓	
7.1 および 7.x 以降のバージョン		✓	✓

バージョン	x86	x86_64	ARM64
8.x		✓	✓

[1] これらのバージョンを使用するには、3.0.x バージョンの SSM Agent を使用する必要があります。使用可能な最新の 3.0.x バージョンの SSM Agent を使用することをお勧めします。それ以降の SSM Agent バージョン (3.1 以降) はサポートされていません。

CentOS Stream

バージョン	x86	x86_64	ARM64
8		✓	✓
9		✓	✓

Debian サーバー

バージョン	x86	x86_64	ARM64
Jessie (8)		✓	
Stretch (9)		✓	✓
Buster (10)		✓	✓
Bullseye (11)		✓	✓
Bookworm (12)		✓	✓

Oracle Linux

バージョン	x86	x86_64	ARM64
7.5 ~ 7.8		✓	
8.x		✓	
9.x		✓	

Red Hat Enterprise Linux (RHEL)

バージョン	x86	x86_64	ARM64
6.x[1]	✓	✓	
7.0 ~ 7.5		✓	
7.6 ~ 8.x		✓	✓
9.x		✓	✓

[1] これらのバージョンを使用するには、3.0.x バージョンの SSM Agent を使用する必要があります。使用可能な最新の 3.0.x バージョンの SSM Agent を使用することをお勧めします。それ以降の SSM Agent バージョン (3.1 以降) はサポートされていません。

Rocky Linux

バージョン	x86	x86_64	ARM64
8.x		✓	✓
9.x		✓	✓

SUSE Linux Enterprise Server (SLES)

バージョン	x86	x86_64	ARM64
12 および 12.x 以降のバージョン		✓	
15.x		✓	✓

Ubuntu Server

バージョン	x86	x86_64	ARM64
12.04 LTS および 14.04 LTS	✓	✓	

バージョン	x86	x86_64	ARM64
16.04 LTS および 18.04 LTS		✓	✓
20.04 LTS および 20.10 STR		✓	✓
22.04 LTS		✓	✓
23.04、23.10		✓	✓
24.04 LTS		✓	✓
24.10		✓	✓

macOS (Amazon EC2 インスタンスのみ)

バージョン	x86	x86_64	Mac with Apple silicon
10.14.x (Mojave)		✓	
10.15.x (Catalina)		✓	
11.x (Big Sur)		✓	✓
12.x (Monterey)		✓	✓
13.x (Ventura)		✓	✓
14.x (Sonoma)		✓	✓
15.x (Sequoia)		✓	✓

> **Note**
>
> すべての AWS リージョン において macOS はサポートされていません。macOS についての Amazon EC2 のサポートの詳細については、「Amazon EC2 ユーザーガイド」の「Amazon EC2 Mac インスタンス」を参照してください。

Raspberry Pi OS (旧称 Raspbian)

バージョン	ARM32
8 (Jessie)	✓
9 (Stretch)	✓

詳細情報

- AWS Systems Manager を使用した Raspberry Pi デバイスの管理

Windows Server

SSM Agent では、Windows Server インスタンスで特定の AWS Systems Manager ドキュメント (SSM ドキュメント) (レガシー `AWS-ApplyPatchBaseline` ドキュメントなど) を実行する場合、Windows PowerShell 3.0 以降が必要です。Windows Server インスタンスが Windows Management Framework 3.0 以降を実行中であることを確認します。このフレームワークには、Windows PowerShell が含まれます。詳細については、「Windows Management Framework 3.0」を参照してください。

バージョン	x86	x86_64	ARM64
2008[1]	✓	✓	
2008 R2[1]		✓	
2012 および 2012 R2[2]		✓	
2016		✓	

バージョン	x86	x86_64	ARM64
2019		✓	
2022		✓	
2025		✓	

[1] Windows Server 2008 および 2008 R2 サポート: 2020 年 1 月 14 日以降、Windows Server 2008 は Microsoft の機能更新プログラムまたはセキュリティ更新プログラムでサポートされなくなりました。Windows Server 2008 および 2008 R2 のレガシー Amazon Machine Images (AMIs) には、依然としてバージョン 2 の SSM Agent がプリインストールされていますが、Systems Manager は 2008 バージョンを正式にサポートしなくなり、これらのバージョンの Windows Server のエージェントを更新しなくなりました。さらに、SSM Agent のバージョン 3 は、Windows Server 2008 および 2008 R2 のいずれのオペレーションとも互換性がない場合があります。Windows Server 2008 バージョンで正式にサポートされている最後の SSM Agent のバージョンは 2.3.1644.0 です。

[2] Windows Server 2012 および 2012 R2 サポート: Windows Server 2012 および 2012 R2 は 2023 年 10 月 10 日にサポートが終了しました。これらのバージョンで SSM Agent を使用する場合、Microsoft の拡張セキュリティ更新プログラム (ESU) を使用することをお勧めします。詳細については、Microsoft ウェブサイトの「Windows Server 2012 および 2012 R2 のサポート終了」を参照してください。

ハイブリッドおよびマルチクラウド環境でサポートされるマシンタイプ

Systems Manager は、マネージドノードとしてさまざまなマシンタイプをサポートしています。マネージドノードとは、Systems Manager と提携するように設定された任意のマシンのことです。

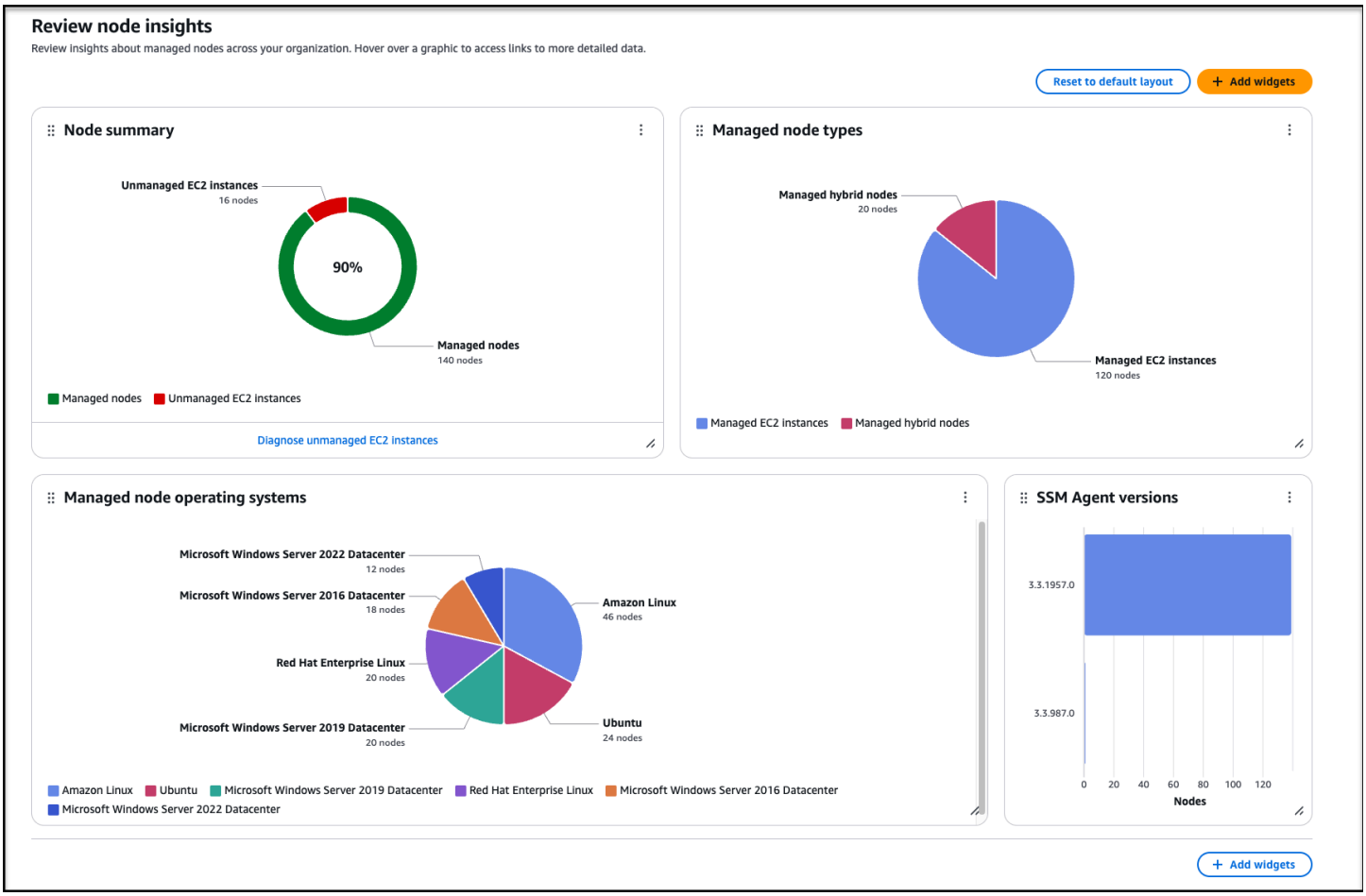
本ユーザーガイドでは、ハイブリッドおよびマルチクラウドという用語を、以下のマシンタイプの任意の組み合わせを含む環境を指すために使用しています。

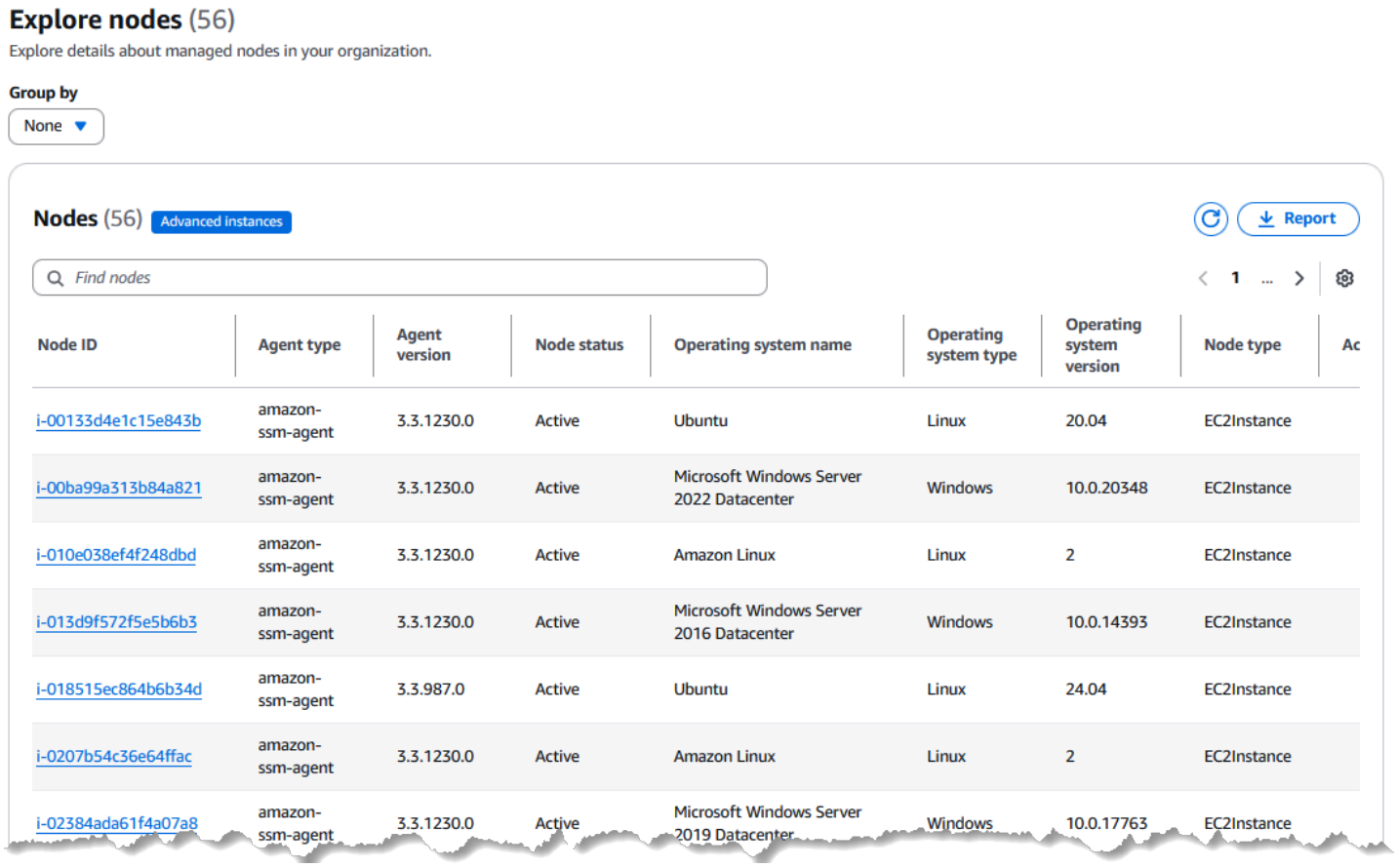
- Amazon Elastic Compute Cloud (Amazon EC2) インスタンス
- 自社構築サーバー (オンプレミスサーバー)
- AWS IoT Greengrass コアデバイス
- AWS IoT および非 AWS エッジデバイス
- 他のクラウド環境内の VM を含む仮想マシン (VM)

ハイブリッドおよびマルチクラウド環境の AWS サポートについては、「AWS ハイブリッドおよびマルチクラウドのソリューション」を参照してください。

統合コンソールとは

Systems Manager の統合コンソールとは、さまざまなツールを組み合わせた統合エクスペリエンスであり、AWS Organizations 組織内の複数の AWS アカウントと AWS リージョンで、または単一のアカウントとリージョンを横断して共通するノードタスクを実行できます。ノードには、マルチクラウド環境で実行される EC2 インスタンス、ハイブリッドサーバー、サーバーがあります。この統合コンソールでは、ノードに関する詳細なインサイトを得ることができます。ノードのレポートを生成したり、Systems Manager が管理する場合のようにノードが報告することを妨げている一般的な問題 (接続の問題など) を診断して修復したりすることができます。ノードの概要に加え、ソフトウェアインベントリやパッチ適用のステータスなど、ノードに関する特定の詳細を閲覧できます。





組織内の複数のアカウントとリージョンにノードがある場合でも、単一のアカウントとリージョンにノードがある場合でも、統合コンソールを使用することをお勧めします。Systems Manager は、統合コンソールのさらに多くのノードタスクを実行するために継続的に機能を追加しています。現在、統合コンソールを使用して実行できるノードタスクについては、「AWS Systems Manager を使用したノード管理タスクの実行」を参照してください。

次のトピックに進み、Systems Manager が管理するノードを設定します。Systems Manager のノードの設定方法については、「AWS Systems Manager のマネージドノードのセットアップ」を参照してください。ノードを設定すると、Systems Manager と統合コンソールを設定できるようになります。Systems Manager の設定の詳細については、「AWS Systems Manager を設定する」を参照してください。

AWS Systems Manager のマネージドノードのセットアップ

このセクションのタスクを完了して、AWS Systems Manager ツール用にロール、ユーザーアカウント、許可、初期リソースをセットアップおよび設定します。このセクションで説明するタスクは、通常、AWS アカウント およびシステム管理者によって実行されます。これらのステップが完了したら、組織内のユーザーは Systems Manager を使用してマネージドノードを設定、管理、アクセスします。マネージドノードは、ハイブリッドおよびマルチクラウド環境内の Systems Manager 用に設定されたあらゆるマシンです。

> **Note**
>
> Amazon EC2 インスタンスと独自のコンピューティングリソースの両方をハイブリッドおよびマルチクラウド環境で使用する場合は、Systems Manager を利用した EC2 インスタンスの管理 のステップに従います。そのトピックは、EC2 インスタンスおよび非 EC2 マシン用の Systems Manager セットアップを完了するための最適な順序でステップを説明します。

他の AWS のサービス を既に使用している場合は、これらの手順の一部は完了しています。ただし、他の手順は Systems Manager に固有です。そのため、このセクション全体を確認の上、Systems Manager のすべてのツールを使用できる状態であることを確認します。

トピック

- Systems Manager を利用した EC2 インスタンスの管理
- Systems Manager を利用したハイブリッド環境およびマルチクラウド環境でのノードの管理
- Systems Manager を利用したエッジデバイスの管理
- Systems Manager 用の AWS Organizations 委任された管理者の作成
- AWS Systems Manager の一般的なセットアップ

Systems Manager を利用した EC2 インスタンスの管理

このセクションのタスクを完了して、AWS Systems Manager 用にロール、許可、初期リソースを設定します。このセクションで説明するタスクは、通常、AWS アカウント およびシステム管理者によって実行されます。これらのステップが完了すると、組織内のユーザーは Systems Manager を使用して、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを設定、管理、アクセスできます。

> **Note**
>
> Systems Manager を使用してオンプレミスマシンを管理および設定する場合は、「Systems Manager を利用したハイブリッド環境およびマルチクラウド環境でのノードの管理」のセットアップ手順に従います。Amazon EC2 インスタンスと非 EC2 インスタンスの両方をハイブリッドおよびマルチクラウド環境で使用する場合は、まずこのステップに従います。このセクションでは、Systems Manager オペレーションで使用するロール、ユーザー、アクセス許可、初期リソースを推奨される順序で設定するための手順を説明します。

他の AWS のサービス を既に使用している場合は、これらの手順の一部は完了しています。ただし、他の手順は Systems Manager に固有です。そのため、このセクション全体を確認の上、Systems Manager のすべてのツールを使用できる状態であることを確認します。

内容

- Systems Manager に必要なインスタンスのアクセス許可を設定する
- Systems Manager のために VPC エンドポイントを使用して EC2 インスタンスのセキュリティを強化する

Systems Manager に必要なインスタンスのアクセス許可を設定する

デフォルトでは、AWS Systems Manager にはインスタンスでアクションを実行する権限がありません。インスタンスのアクセス許可は、AWS Identity and Access Management (IAM) ロールを使用してアカウントレベルで付与するか、またはインスタンスプロファイルを使用してインスタンスレベルで付与することができます。可能であれば、デフォルトのホスト管理設定を使用してアカウントレベルでアクセスを付与することをお勧めします。

> **Note**
>
> このステップをスキップして、統合コンソールをセットアップするときに Systems Manager が自動的に必要なアクセス許可をインスタンスに適用するようにすることもできます。詳細については、「AWS Systems Manager を設定する」を参照してください。

EC2 インスタンスのアクセス許可の推奨設定

デフォルトのホスト管理設定では、Systems Manager が Amazon EC2 インスタンスを自動的に管理することができます。この設定をオンにすると、SSM Agent バージョン 3.2.582.0 以降がインストールされている AWS リージョン および AWS アカウント で、インスタンスメタデータサービスバージョン 2 (IMDSv2) を使用しているすべてのインスタンスが、自動的にマネージドインスタンスになります。デフォルトのホスト管理設定は、インスタンスメタデータサービスバージョン 1 をサポートしていません。IMDSv2 への移行の詳細については、「Amazon EC2 ユーザーガイド」の「インスタンスメタデータサービスバージョン 2 の使用への移行」を参照してください。インスタンスにインストールされている SSM Agent のバージョンを確認する方法については、「SSM Agent バージョン番号の確認」を参照してください。SSM Agent の更新方法については、「SSM Agent の自動更新」を参照してください。マネージドインスタンスには、次のような利点があります。

- Session Manager を使用して安全にインスタンスに接続する。
- Patch Manager を使用して自動パッチスキャンを実行する。
- Systems Manager インベントリを使用して、インスタンスに関する詳細情報を表示する。
- Fleet Manager を使用してインスタンスを追跡、管理する。
- SSM Agent を自動的に最新の状態に保つ。

Fleet Manager、Inventory、Patch Manager、Session Manager は AWS Systems Manager のツールです。

デフォルトのホスト管理設定では、インスタンスプロファイルを使用せずにインスタンスを管理でき、Systems Manager にリージョンとアカウント内のすべてのインスタンスを管理するアクセス許可が付与されていることを確認できます。付与されたアクセス許可がユースケースに十分でない場合は、デフォルトのホスト管理設定で作成されたデフォルトの IAM ロールにポリシーを追加することもできます。また、デフォルトの IAM ロールで提供されるすべての機能の一部に対してのみアクセス許可が必要な場合は、独自のカスタムロールとポリシーを作成できます。デフォルトのホスト管理設定で選択した IAM ロールに加えられた変更は、リージョンとアカウントのすべてのマネージド Amazon EC2 インスタンスに適用されます。デフォルトのホスト管理設定で使用するポリシーの詳細については、「AWS マネージドポリシー: AmazonSSMManagedEC2InstanceDefaultPolicy」を参照してください。デフォルトのホスト管理設定に関する詳細については、「Default Host Management Configuration を使用した EC2 インスタンスの自動管理」を参照してください。

Important

デフォルトのホスト管理設定を使用して登録されたインスタンスは、登録情報を `/lib/amazon/ssm` または `C:\ProgramData\Amazon` ディレクトリへローカルに保存します。これらのディレクトリやファイルを削除すると、インスタンスはデフォルトのホスト管理設定を使用して Systems Manager に接続するために必要な認証情報を取得できなくなります。このような場合は、インスタンスプロファイルを使用してインスタンスに必要なアクセス許可を付与するか、インスタンスを再作成する必要があります。

Note

この手順を実行できるのは、管理者のみです。ユーザー個人がデフォルトのホスト管理設定を設定または変更できるようにする場合は、最小特権アクセス許可を実装してください。デフォルトのホスト管理設定は、Amazon EC2 インスタンスを自動的に管理したい AWS リージョン でオンにする必要があります。

デフォルトのホスト管理設定を有効にするには

デフォルトのホスト管理設定は、Fleet Manager コンソールからオンにできます。AWS Management Console または任意のコマンドラインツールを使用してこの手順を正常に完了するには、API オペレーション (GetServiceSetting、ResetServiceSetting、UpdateServiceSetting) のアクセス許可が必要です。さらに、`AWSSystemsManagerDefaultEC2InstanceManagementRole` IAM ロールの `iam:PassRole` アクセス許可を付与する権限が必要です。以下は、ポリシーの例です。各##############をユーザー自身の情報に置き換えます。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "ssm:GetServiceSetting",
    "ssm:ResetServiceSetting",
    "ssm:UpdateServiceSetting"
   ],
   "Resource": "arn:aws:ssm:region:account-id:servicesetting/ssm/managed-instance/
default-ec2-instance-management-role"
```

```
  },
  {
   "Effect": "Allow",
   "Action": [
    "iam:PassRole"
   ],
   "Resource": "arn:aws:iam::account-id:role/service-role/
AWSSystemsManagerDefaultEC2InstanceManagementRole",
   "Condition": {
    "StringEquals": {
     "iam:PassedToService": [
      "ssm.amazonaws.com"
     ]
    }
   }
  }
 ]
}
```

開始する前に、Amazon EC2 インスタンスにインスタンスプロファイルが添付されている場合は、`ssm:UpdateInstanceInformation` オペレーションを許可する権限をすべて削除してください。SSM Agent は、デフォルトのホスト管理設定のアクセス許可を使用する前に、インスタンスプロファイルのアクセス許可を使用しようとします。インスタンスプロファイルで `ssm:UpdateInstanceInformation` オペレーションを許可すると、インスタンスはデフォルトのホスト管理設定のアクセス許可を使用しません。

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. [アカウント管理] ドロップダウンの一覧で [デフォルトのホスト管理設定] をクリックします。
4. [デフォルトのホスト管理設定を有効にする] をオンにします。
5. インスタンスの Systems Manager ツールを有効にするために使用する IAM ロールを選択します。デフォルトのホスト管理設定で提供されるデフォルトのロールを使用することをお勧めします。このロールには、Systems Manager を使用して Amazon EC2 インスタンスを管理するために必要となる最小限のアクセス許可のセットが含まれています。カスタムロールを使用する場合は、ロールの信頼ポリシーで Systems Manager を信頼できるエンティティとして許可する必要があります。
6. [設定] をクリックして、セットアップを完了します。

デフォルトのホスト管理設定をオンにした後、選択したロールの認証情報をインスタンスが使用できるようになるまでに 30 分かかる場合があります。デフォルトのホスト管理設定は、Amazon EC2 インスタンスを自動的に管理したい各リージョンで有効にする必要があります。

EC2 インスタンスのアクセス許可の代替設定

AWS Identity and Access Management (IAM) インスタンスプロファイルを使用すると、アクセス許可を個々のインスタンスレベルで付与することができます。インスタンスプロファイルは、起動時に IAM ロール情報を Amazon Elastic Compute Cloud (Amazon EC2) インスタンスに渡すコンテナです。Systems Manager のインスタンスプロファイルを作成するには、必要なアクセス許可を定義する 1 つ以上の IAM ポリシーを、新しいロールか、作成済みのロールにアタッチします。

> **Note**
>
> AWS Systems Manager のツールである Quick Setup を使用すると、AWS アカウントのあらゆるインスタンスでインスタンスプロファイルをすばやく設定できます。Quick Setup では、IAM サービスロール (またはロールの継承) を作成します。これにより、Systems Manager はユーザーに代わってインスタンスで安全にコマンドを実行できます。Quick Setup を使用すると、このステップ (ステップ 3) とステップ 4 をスキップできます。詳細については、「AWS Systems Manager Quick Setup」を参照してください。

IAM インスタンスプロファイルの作成に関する次の詳細情報に注意してください。

- Systems Manager のハイブリッドおよびマルチクラウド環境で非 EC2 を設定する場合、インスタンスプロファイルを作成する必要はありません。代わりに、IAM サービス ロールを使用するようにサーバーと VM を設定します。詳細については、「ハイブリッドおよびマルチクラウド環境で Systems Manager に必要な IAM サービスロールを作成する」を参照してください。
- IAM インスタンスプロファイルを変更した場合、インスタンスの認証情報が更新されるまでに時間がかかることがあります。更新されるまで、SSM Agent はリクエストを処理しません。更新プロセスを高速化するには、SSM Agent を再起動するか、インスタンスを再起動します。

インスタンスプロファイルに新しいロールを作成するか、既存のロールに必要なアクセス許可を追加するかに応じて、以下のいずれかの手順を実行します。

Systems Manager マネージドインスタンスのインスタンスプロファイルを作成するには (コンソール)

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. ナビゲーションペインで ロール を選択してから、ロールを作成する を選択します。
3. [Trusted entity type] (信頼できるエンティティタイプ) で、[AWS のサービス] を選択します。
4. [Use case] (ユースケース) で [EC2] を選択し、[Next] (次へ) を選択します。
5. [アクセス許可を追加] ページで、以下を実行します。

   - [Search] (検索) フィールドを使用して、[AmazonSSMManagedInstanceCore] ポリシーを検索します。次の図に示すように、名前の横にあるチェックボックスをオンにします。

   他のポリシーを検索しても、コンソールでは選択内容が保持されます。

   - 以前の手順 (オプション) S3 バケットへのアクセスのカスタムポリシーを作成する でカスタムの S3 バケットポリシーを作成した場合は、それを検索してその名前の横にあるチェックボックスをオンにします。
   - AWS Directory Service によって管理されている Active Directory にインスタンスを結合する場合は、[AmazonSSMDirectoryServiceAccess] を検索し、その名前の横にあるチェックボックスをオンにします。
   - EventBridge または CloudWatch Logs を使用して、インスタンスを管理またはモニタリングする場合は、[CloudWatchAgentServerPolicy] を検索し、その名前の横にあるチェックボックスをオンにします。

6. [Next] を選択します。
7. [Role name] (ロール名) に、新しいインスタンスプロファイルの名前 (**SSMInstanceProfile** など) を入力します。

> **Note**
>
> ロール名を書き留めます。このロール名は、Systems Manager を使用して管理するインスタンスを新しく作成する際に選択します。

8. (オプション) [Description] (説明) にある、このインスタンスプロファイルの説明を更新します。
9. (オプション) [Tags] (タグ) で、1 つ以上のタグキーと値のペアを追加し、このロールのアクセスを整理、追跡、制御して、[Create role] (ロールの作成) を選択します。ロールページが再度表示されます。

Systems Manager のインスタンスプロファイルのアクセス許可を既存のロールに追加するには (コンソール)

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. ナビゲーションペインで、[ロール] を選択して、Systems Manager オペレーションのためにインスタンスプロファイルに関連付ける既存のロールを選択します。
3. [Permissions] (アクセス許可) タブで、[Add permissions, Attach policies] (アクセス許可の追加、ポリシーのアタッチ) をクリックします。
4. [Attach Policy] (ポリシーのアタッチ) ページで、次の操作を実行します。
   - [Search] (検索) フィールドを使用して、[AmazonSSMManagedInstanceCore] ポリシーを検索します。名前の横にあるチェックボックスを選択します。
   - カスタムの S3 バケットポリシーを作成した場合は、その名前の横にあるチェックボックスをオンにします。インスタンスプロファイルのカスタム S3 バケットポリシーについては、「(オプション) S3 バケットへのアクセスのカスタムポリシーを作成する」を参照してください。
   - AWS Directory Service によって管理されている Active Directory にインスタンスを結合する場合は、[AmazonSSMDirectoryServiceAccess] を検索し、その名前の横にあるチェックボックスをオンにします。
   - EventBridge または CloudWatch Logs を使用して、インスタンスを管理またはモニタリングする場合は、[CloudWatchAgentServerPolicy] を検索し、その名前の横にあるチェックボックスをオンにします。
5. [ポリシーのアタッチ] を選択します。

信頼できるエンティティを含むように、またはさらにアクセスを制限するようにロールを更新する方法については、IAM ユーザーガイドの「ロールの修正」を参照してください。

(オプション) S3 バケットへのアクセスのカスタムポリシーを作成する

Amazon S3 アクセス用のカスタムポリシーは、VPC エンドポイントを使用している場合、または Systems Manager オペレーションに独自の S3 バケットを使用している場合にのみ作成する必要があります。このポリシーは、デフォルトのホスト管理設定で作成されたデフォルトの IAM ロール、または前の手順で作成したインスタンスプロファイルにアタッチできます。

以下のポリシーでアクセスを付与する AWS マネージドの S3 バケットの詳細については、「SSM Agent と AWS マネージド S3 バケットとの通信」を参照してください。

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. ナビゲーションペインで ポリシーを選択してから ポリシーの作成を選択します。
3. [JSON] タブを選択し、デフォルトのテキストを次に置き換えます。

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

  1                                                                    {
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": [
                "arn:aws:s3:::aws-ssm-region/*",
                "arn:aws:s3:::aws-windows-downloads-region/*",
                "arn:aws:s3:::amazon-ssm-region/*",
                "arn:aws:s3:::amazon-ssm-packages-region/*",
                "arn:aws:s3:::region-birdwatcher-prod/*",
                "arn:aws:s3:::aws-ssm-distributor-file-region/*",
                "arn:aws:s3:::aws-ssm-document-attachments-region/*",
                "arn:aws:s3:::patch-baseline-snapshot-region/*"
            ]
        },

  2                                                                    {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
```

```
 "s3:PutObjectAcl", 3

 "s3:GetEncryptionConfiguration" 4
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket/*",
                "arn:aws:s3:::amzn-s3-demo-
bucket" 5
            ]
        }
    ]
}
```

[1] 最初の Statement エレメントは、VPC エンドポイントを使用する場合にのみ必要です。

[2] 2 番目の Statement エレメントは、Systems Manager オペレーションで使用するために作成した S3 バケットを使用する場合にのみ必要です。

[3] PutObjectAcl アクセスコントロールリストは、他のアカウントで S3 バケットへのクロスアカウントアクセスをサポートする場合にのみ必要です。

[4] S3 バケットが暗号化を使用するように設定されている場合、GetEncryptionConfiguration エレメントが必要です。

[5] S3 バケットが暗号化を使用するように設定されている場合、S3 バケットのルート (例: arn:aws:s3:::amzn-s3-demo-bucket) が [リソース] セクションに表示されている必要があります。ユーザー、グループ、またはロールに、ルートバケットへのアクセスを設定する必要があります。

4. オペレーションで VPC エンドポイントを使用する場合は、以下の操作を行います。

   最初の Statement エレメントで、*region* の各プレースホルダーを、このポリシーが使用される AWS リージョン の識別子に置き換えます。例えば、米国東部 (オハイオ) リージョンの場合は、us-east-2 を使用します。サポートされている *region* 値の一覧については、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」にある Region 列を参照してください。

> **Important**
>
> このポリシーの特定のリージョンの代わりにワイルドカード文字 (*) を使用しないことをお勧めします。たとえば、`arn:aws:s3:::aws-ssm-us-east-2/*` を使用して、`arn:aws:s3:::aws-ssm-*/*` は使用しないでください。ワイルドカードを使用すると、アクセスを付与する S3 バケットへのアクセス権が付与される場合があります。複数のリージョンでインスタンスプロファイルを使用する場合は、各リージョンの最初の `Statement` エレメントを繰り返すことをお勧めします。

-または-

オペレーションで VPC エンドポイントを使用しない場合は、最初の `Statement` エレメントは削除することができます。

5. Systems Manager オペレーションで独自の S3 バケットを使用する場合は、以下の操作を行います。

   2 つめの `Statement` エレメントで、*amzn-s3-demo-bucket* をアカウント内の S3 バケットの名前に置き換えます。このバケットは、Systems Manager のオペレーションに使用します。バケットのオブジェクトにアクセス許可を付与します。この際、`"arn:aws:s3:::my-bucket-name/*"` をリソースとして使用します。バケット、またはバケットのオブジェクトに許可を付与する方法については、Amazon Simple Storage Service ユーザーガイドのトピック「Amazon S3 アクション」および AWS ブログ記事「IAM ポリシーとバケットポリシーと ACL!」を参照してください。Oh, My! (Controlling Access to S3 Resources)。

   > **Note**
   >
   > 複数のバケットを使用する場合は、それぞれの ARN を入力します。バケットのアクセス許可については、次の例を参照してください。
   >
   > ```
   > "Resource": [
   > "arn:aws:s3:::amzn-s3-demo-bucket1/*",
   > "arn:aws:s3:::amzn-s3-demo-bucket2/*"
   >              ]
   > ```

   -または-

Systems Manager オペレーションで独自の S3 バケットを使用していない場合は、2 つめの `Statement` エレメントは削除できます。

6. [Next: Tags] (次へ: タグ) を選択します。
7. (オプション) [Add tag] (タグを追加) を選択してタグを追加し、ポリシーの優先タグを入力します。
8. [次へ: レビュー] を選択します。
9. [Name] (名前) に、このポリシーを識別するための名前 (**`SSMInstanceProfileS3Policy`** など) を入力します。
10. [Create policy] を選択します。

マネージドインスタンスのポリシーに関するその他の考慮事項

このセクションでは、デフォルトのホスト管理設定で作成されたデフォルトの IAM ロール、または AWS Systems Manager のインスタンスプロファイルに追加できるポリシーについて説明します。インスタンスと Systems Manager API 間における通信の許可を付与する場合、システムのニーズとセキュリティ要件を反映したカスタムポリシーを作成することをお勧めします。オペレーションプランによっては、他の 1 つまたは複数のポリシーに設定されているアクセス許可が必要になる場合があります。

ポリシー: **`AmazonSSMDirectoryServiceAccess`**

Windows Server の Amazon EC2 インスタンスを Microsoft AD ディレクトリに結合する場合にのみ必要です。

AWS 管理ポリシーでは、マネージドインスタンスによるドメインの結合リクエストに対して、SSM Agent による AWS Directory Service へのアクセスをお客様の代わりに許可します。詳細については、 AWS Directory Service 管理ガイドの 「Windows EC2 インスタンスにシームレスに参加する」を参照してください。

ポリシー: **`CloudWatchAgentServerPolicy`**

メトリクスを読み取り、インスタンスにデータのログを記録して Amazon CloudWatch に書き込むために、インスタンスに CloudWatch をインストールして実行する場合にのみ必要です。これらは、AWS リソースの問題や変更をモニタリング、分析、および迅速に対応するのに役立ちます。

このポリシーは、Amazon EventBridge や Amazon CloudWatch Logs などの機能を使用する場合にのみ、デフォルトのホスト管理設定やインスタンスプロファイルで作成されたデフォルトの

IAM ロールで必要になります。(例えば、特定の CloudWatch Logs ログストリームへの書き込みアクセスを制限する、より制限の厳しいポリシーを作成することもできます)。

> **Note**
>
> EventBridge および CloudWatch Logs 機能の使用はオプションです。ただし、使用することにした場合は、Systems Manager の設定プロセスの最初にそれらを設定することをお勧めします。詳細については、Amazon EventBridge ユーザーガイドおよび Amazon CloudWatch Logs ユーザーガイドを参照してください。

追加の Systems Manager ツールのアクセス許可を含む IAM ポリシーを作成するには、次のリソースを参照してください。

- IAM ポリシーを使用して Parameter Store パラメータへのアクセスを制限する
- オートメーションの設定
- ステップ 2: Session Manager のインスタンスのアクセス権限の確認または追加

インスタンスに Systems Manager インスタンスプロファイルを添付する (コンソール)

次の手順は、Amazon EC2 コンソールを使用して、IAM インスタンスプロファイルを Amazon EC2 インスタンスにアタッチする方法を示します。

1. AWS Management Console にサインインし、Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
2. ナビゲーションペインで、[Instances] の下にある [Instances] を選択します。
3. リストから EC2 インスタンスに移動して選択します。
4. [アクション] メニューで、[セキュリティ]、[IAM ロールの変更] の順に選択します。
5. [IAM ロール] で、EC2 インスタンスのアクセス許可の代替設定 の手順に従って作成したインスタンスプロファイルを選択します。
6. [Update IAM role] (IAM ロールの更新) を選択します。

インスタンスへの IAM ロールのアタッチの詳細については、選択したオペレーティングシステムのタイプに応じて、次のいずれかを選択してください。

- 「Amazon EC2 ユーザーガイド」の「IAM ロールをインスタンスにアタッチする」
- 「Amazon EC2 ユーザーガイド」の「IAM ロールをインスタンスにアタッチする」

「Systems Manager のために VPC エンドポイントを使用して EC2 インスタンスのセキュリティを強化する」に進みます。

Systems Manager のために VPC エンドポイントを使用して EC2 インスタンスのセキュリティを強化する

Amazon Virtual Private Cloud (Amazon VPC) でインターフェイス VPC エンドポイントを使用するように AWS Systems Manager を設定することで、マネージドノード (ハイブリッドおよびマルチクラウド環境の非 EC2 マシンを含む) のセキュリティ体制を向上させることができます。インターフェイス VPC エンドポイント (インターフェイスエンドポイント) を使用すると、AWS PrivateLink によって提供されるサービスに接続できます。AWS PrivateLink は、プライベート IP アドレスを使用して Amazon Elastic Compute Cloud (Amazon EC2) および Systems Manager API にプライベートアクセスできるようにするテクノロジーです。

AWS PrivateLink は、マネージドインスタンス、Systems Manager、および Amazon EC2 間のすべてのネットワークトラフィックを Amazon ネットワークに制限します。つまり、マネージドインスタンスはインターネットにアクセスできません。また AWS PrivateLink を使用する場合、インターネットゲートウェイ、NAT デバイス、仮想プライベートゲートウェイは必要はありません。

AWS PrivateLink の設定は要件ではありませんが、推奨されます。AWS PrivateLink および VPC エンドポイントの詳細については、「AWS PrivateLink と VPC エンドポイント」を参照してください。

> **Note**
>
> VPC エンドポイントを使用する代わりに、マネージドインスタンスでアウトバウンドのインターネットアクセスを許可します。この場合、マネージドインスタンスは、以下のエンドポイントへの HTTPS (ポート 443) アウトバウンドトラフィックも許可する必要があります。
>
> - `ssm.region.amazonaws.com`
> - `ssmmessages.region.amazonaws.com`
> - `ec2messages.region.amazonaws.com`
>
> SSM Agent は、クラウド内の Systems Manager サービスへのすべての接続を開始します。このため、Systems Manager のインスタンスへのインバウンドトラフィックを許可するようにファイアウォールを設定する必要はありません。

これらのエンドポイントへの呼び出しの詳細については、「リファレンス: ec2messages、ssmmessages およびその他の API オペレーション」を参照してください。

Amazon VPC について

Amazon Virtual Private Cloud (Amazon VPC) を使用すると、AWS クラウド 内の論理的に分離された独自の領域に仮想プライベートクラウド (VPC) と呼ばれる仮想ネットワークを定義できます。AWS のリソース (インスタンスなど) を VPC 内部で起動できます。VPC は、お客様自身のデータセンターで運用されている従来のネットワークによく似ていますが、 のスケーラブルなインフラストラクチャを使用できるというメリットがありますAWS お客様の VPC はお客様が設定できます。IP アドレスレンジの選択、サブネットの作成、ルートテーブル、ネットワークゲートウェイ、セキュリティの設定ができます。VPC のインスタンスをインターネットに接続できます。VPC を自社のデータセンターに接続し、AWS クラウド をデータセンターの拡張部分として使用できます。各サブネットでのリソースの保護には、セキュリティグループ、ネットワークアクセスコントロールリストなど、複数のセキュリティレイヤーを使用できます。詳細については、Amazon VPC ユーザーガイドを参照してください。

トピック

- VPC エンドポイントの制約と制限
- Systems Manager 用の VPC エンドポイントを作成する
- インターフェイス VPC エンドポイントポリシーの作成

VPC エンドポイントの制約と制限

Systems Manager の VPC エンドポイントを設定する前に、以下の制約と制限に注意してください。

VPC ピアリング接続

VPC インターフェイスのエンドポイントには、リージョン内およびリージョン間 VPC ピア接続の両方を介してアクセスできます。VPC インターフェイスエンドポイントの VPC ピア接続リクエストの詳細については、Amazon Virtual Private Cloud ユーザーガイドの「VPC ピア接続 (クォータ)」を参照してください。

VPC ゲートウェイエンドポイントの接続を、VPC の外に延長することはできません。VPC 内の VPC ピア接続の反対側のリソースは、ゲートウェイエンドポイントを使用してゲートウェイエンドポイントサービス内のリソースと通信することはできません。VPC ゲートウェイエンドポイントの

VPC ピア接続リクエストの詳細については、Amazon Virtual Private Cloud ユーザーガイドの「VPC エンドポイント (クォータ)」を参照してください。

着信接続

VPC エンドポイントにアタッチされたセキュリティグループでは、マネージドインスタンスのプライベートサブネットから、ポート 443 で着信接続を許可する必要があります。着信接続が許可されていない場合、マネージドインスタンスは SSM および EC2 エンドポイントに接続できません。

DNS 解決

カスタム DNS サーバーを使用する場合は、`amazonaws.com` ドメインへのすべてのクエリの条件付きフォワーダーを VPC の Amazon DNS サーバーに追加する必要があります。

S3 バケット

VPC エンドポイントポリシーは、少なくとも SSM Agent と AWS マネージド S3 バケットとの通信にリストされている Amazon S3 バケットへのアクセスを許可する必要があります。

> **Note**
>
> オンプレミスのファイアウォールを使用していて Patch Manager を使用する場合は、そのファイアウォールでパッチベースラインのエンドポイントへの適切なアクセスを許可する必要もあります。

Amazon CloudWatch Logs

インスタンスがインターネットにアクセスすることを許可しない場合、CloudWatch Logs にログを送信する機能を使用するには、CloudWatch Logs の VPC エンドポイントを作成します。CloudWatch Logs のエンドポイントの作成の詳細については、Amazon CloudWatch Logs ユーザーガイドの「CloudWatch Logs 用の VPC エンドポイントの作成」を参照してください。

ハイブリッドおよびマルチクラウド環境の DNS

ハイブリッドおよびマルチクラウド環境で AWS PrivateLink エンドポイントと連携するように DNS を設定する方法については、「Amazon VPC ユーザーガイド」の「インターフェイスエンドポイントのプライベート DNS」を参照してください。独自の DNS を使用する場合には、Route 53 リゾルバーを使用できます。詳細については、「Amazon Route 53 デベロッパーガイド」の「VPC とネットワーク間の DNS クエリの解決」を参照してください。

Systems Manager 用の VPC エンドポイントを作成する

以下の情報を使用して、AWS Systems Manager の VPC インターフェイスエンドポイントを作成します このトピックは、Amazon VPC ユーザーガイドの手順にリンクしています。

> **Note**
>
> *region* は、米国東部 (オハイオ) リージョンの us-east-2 のように、AWS Systems Manager でサポートされている AWS リージョン の識別子を表します。サポートされている *region* 値の一覧については、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」にある Region 列を参照してください。

「インターフェイスエンドポイントの作成」の手順に従って、以下のインターフェイスエンドポイントを作成します。

- **com.amazonaws.*region*.ssm** — Systems Manager サービスのエンドポイント。
- **com.amazonaws.*region*.ec2messages** — Systems Manager は、このエンドポイントを使用して SSM Agent から Systems Manager サービスへの呼び出しを行います。SSM Agent のバージョン 3.3.40.0 以降、Systems Manager は、使用可能な場合には ec2messages:* エンドポイント (Amazon Message Delivery Service) の代わりに ssmmessages:* エンドポイント (Amazon Message Gateway Service) を使用するようになりました。
- **com.amazonaws.*region*.ec2** — Systems Manager を使用して VSS 対応のスナップショットを作成する場合は、EC2 サービスへのエンドポイントがあることを確認します。EC2 エンドポイントが定義されていない場合、アタッチした Amazon EBS ボリュームを列挙する呼び出しは失敗し、Systems Manager コマンドが失敗します。
- **com.amazonaws.*region*.s3** – Systems Manager は、このエンドポイントを使用して SSM Agent を更新します。また、Systems Manager は、バケットに保存されているスクリプトや他のファイルを取得したり、出力ログをバケットにアップロードしたりすることをユーザーがオプションで選択した場合にも、このエンドポイントを使用します。インスタンスに関連付けられたセキュリティグループでアウトバウンドトラフィックが制限されている場合は、Amazon S3 のプレフィックス一覧へのトラフィックを可能にするルールを追加する必要があります。詳細については、AWS PrivateLink ガイドの「セキュリティグループの変更」を参照してください。
- **com.amazonaws.*region*.ssmmessages** – このエンドポイントは、Run Command のために、および Session Manager を使用してセキュアなデータチャネル経由でインスタンスに接続している場合に、SSM Agent が Systems Manager サービスと通信する上で必要です。詳細について

は、AWS Systems Manager Session Managerおよびリファレンス: ec2messages、ssmmessages およびその他の API オペレーションを参照してください。

- (オプション) **com.amazonaws.*region*.kms** – Session Manager または Parameter Store パラメータのために AWS Key Management Service (AWS KMS) 暗号化を使用する場合は、このエンドポイントを作成します。
- (オプション) **com.amazonaws.*region*.logs** – Session Manager、Run Command、または SSM Agent ログのために Amazon CloudWatch Logs (CloudWatch Logs) を使用する場合は、このエンドポイントを作成します。

SSM Agent がアクセスできる必要がある AWS マネージド S3 バケットについては、「SSM Agent と AWS マネージド S3 バケットとの通信」を参照してください。Systems Manager のオペレーションで仮想プライベートクラウド (VPC) エンドポイントを使用している場合は、Systems Manager の EC2 インスタンスプロファイル、またはハイブリッドおよびマルチクラウド環境の非 EC2 ノードのサービスロールで、明示的な許可を付与する必要があります。

インターフェイス VPC エンドポイントポリシーの作成

AWS Systems Manager には VPC インターフェイスエンドポイントのポリシーを作成することができます。このポリシーでは、以下の内容を指定できます。

- アクションを実行できるプリンシパル
- 実行可能なアクション
- 自身に対してアクションを実行できたリソース

詳細については、Amazon VPC ユーザーガイドの「VPC エンドポイントによるサービスへのアクセスのコントロール」を参照してください。

Systems Manager を利用したハイブリッド環境およびマルチクラウド環境でのノードの管理

AWS Systems Manager を使用して、Amazon Elastic Compute Cloud (EC2) インスタンスと多数の非 EC2 マシンタイプの両方を管理できます。このセクションでは、ハイブリッドおよびマルチクラウド環境で Systems Manager を使用して非 EC2 マシンを管理するために、アカウントおよびシステム管理者が実行する設定タスクについて説明します。これらのステップが完了したら、AWS アカウント 管理者から許可が付与されたユーザーは、Systems Manager を使用して組織の非 EC2 サーバーを設定と管理できます。

Systems Manager で使用するように設定されたマシンはすべて、マネージドノードと呼ばれます。

> **Note**
>
> - 非 EC2 マシンと同じハイブリッドアクティベーション手順を使用して、エッジデバイスをマネージドノードとして登録できます。これらのエッジデバイスのタイプには、AWS IoT デバイスと AWS IoT デバイス以外のデバイスの両方が含まれます。これらのエッジデバイスのタイプを設定するには、このセクションで説明されている手順を実行します。
>
> Systems Manager は AWS IoT Greengrass コアソフトウェアを使用するエッジデバイスもサポートします。AWS IoT Greengrass コアデバイスの設定プロセスおよび要件は、AWS IoT および AWS エッジデバイス以外のエッジデバイスのものとは異なります。Systems Manager で使用する AWS IoT Greengrass デバイスの登録については、「Systems Manager を利用したエッジデバイスの管理」を参照してください。
> - 非 EC2 macOS マシンは、Systems Manager のハイブリッドおよびマルチクラウド環境ではサポートされていません。

Systems Manager を使用して Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理する場合、または Amazon EC2 インスタンスと非 EC2 マシンの両方をハイブリッドおよびマルチクラウド環境で使用する場合は、最初に Systems Manager を利用した EC2 インスタンスの管理 の手順に従います。

Systems Manager 向けにハイブリッドおよびマルチクラウド環境を設定すると以下のことを行うことができます。

- 同じツールやスクリプトを使用して 1 か所からハイブリッドおよびマルチクラウドのワークロードをリモートで管理できる一貫したセキュアな方法が作成されます。
- AWS Identity and Access Management (IAM) を使ってマシンに実行できるアクションのアクセス制御を一元化します。
- AWS CloudTrail に記録されている API のアクティビティを確認することで、マシンで実行されるオペレーションを一元的に監査できます。

  CloudTrail を使用して Systems Manager のアクションをモニタリングする方法については、「AWS Systems Manager による AWS CloudTrail API コールのログ記録」を参照してください。
- モニタリングを一元化するには、サービス実行の成功に関する通知を送信するように Amazon EventBridge と Amazon Simple Notification Service (Amazon SNS) を設定します。

EventBridge を使用して Systems Manager イベントをモニタリングする方法については、「Amazon EventBridge を使用して Systems Manager イベントをモニタリングする」を参照してください。

マネージドノードについて

このセクションで説明している Systems Manager 用の非 EC2 マシンの設定を完了したら、ハイブリッドアクティベーションマシンは AWS Management Console にリストされてマネージドノードとして表示されます。コンソールでは、ハイブリッドアクティベーションマネージドノードの ID は、「mi-」のプレフィックスにより Amazon EC2 インスタンスと区別されます。Amazon EC2 インスタンス ID は、プレフィックス「i-」を使用します。

マネージドノードとは、Systems Manager 用に設定されたあらゆるマシンのことです。以前は、マネージドノードはすべてマネージドインスタンスと呼ばれていました。現在、インスタンスとは EC2 インスタンスのみを指します。deregister-managed-instance コマンドは、この用語変更の前に命名されました。

詳細については、「マネージドノードの使用」を参照してください。

インスタンスの階層について

Systems Manager はハイブリッドおよびマルチクラウド環境内の非 EC2 マネージドノード用にスタンダードインスタンス層とアドバンストインスタンス層を提供します。スタンダードインスタンス層により、AWS アカウント ごと、AWS リージョン ごとに最大 1,000 のハイブリッドアクティベーションマシンを登録できます。1 つのアカウントとリージョンに 1,000 を超える非 EC2 マシンを登録する必要がある場合は、アドバンストインスタンス層を使用します。アドバンストインスタンスは、AWS Systems Manager Session Manager を使用して非 EC2 マシンに接続することも可能にします。Session Manager はマネージドノードにインタラクティブシェルアクセスを実現します。

詳細については、「インスタンス層の設定」を参照してください。

トピック

- ハイブリッドおよびマルチクラウド環境で Systems Manager に必要な IAM サービスロールを作成する
- ハイブリッドアクティベーションを作成して、Systems Manager にノードを登録する
- ハイブリッド Linux ノードで SSM Agent をインストールする
- ハイブリッド Windows Server ノードに SSM Agent をインストールする

ハイブリッドおよびマルチクラウド環境で Systems Manager に必要な IAM サービスロールを作成する

ハイブリッドおよびマルチクラウド環境の非 EC2 (Amazon Elastic Compute Cloud) マシンでは、AWS Systems Manager サービスと通信するために AWS Identity and Access Management (IAM) サービスロールが必要です。ロールは、Systems Manager サービスに AWS Security Token Service (AWS STS) `AssumeRole` の信頼を付与します。AWS アカウント ごとにハイブリッドおよびマルチクラウド環境用にサービスロールを一度のみ作成する必要があります。ただし、ハイブリッドおよびマルチクラウド環境のマシンに異なる許可が必要な場合、異なるハイブリッドアクティベーションに対して複数のサービスロールを作成することもできます。

以下の手順は、Systems Manager コンソールまたはお好みのコマンドラインツールを使用して、必要なサービスロールを作成する方法を説明します。

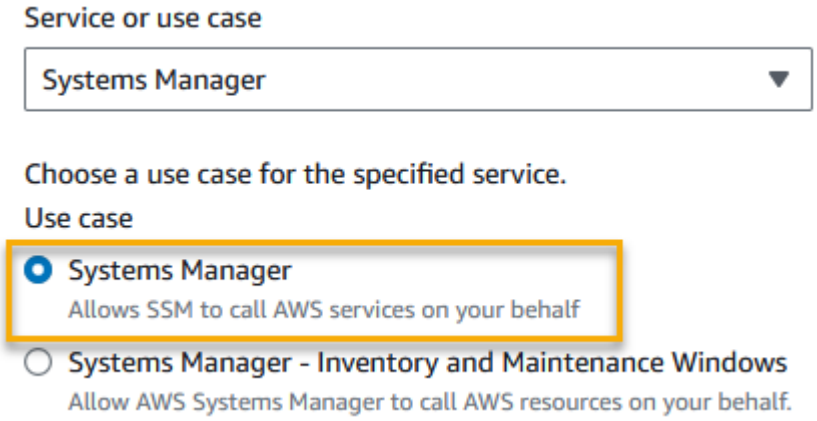
AWS Management Console を使用して Systems Manager ハイブリッドアクティベーション用の IAM サービスロールを作成する

ハイブリッドアクティベーションのサービスロールを作成するために、以下の手順にしたがいます。この手順では、Systems Manager の主要機能で `AmazonSSMManagedInstanceCore` ポリシーを使用します。ユースケースによっては、オンプレミスマシンが他の Systems Manager ツールまたは AWS のサービスにアクセスできるようにするため、サービスロールにポリシーを追加する必要がある場合があります。例えば、必要な AWS マネージド型 Amazon Simple Storage Service (Amazon S3) バケットにアクセスがなければ、Patch Manager パッチ運用オペレーションが失敗します。

サービスロールを作成するには (コンソール)

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. ナビゲーションペインで ロール を選択してから、ロールを作成する を選択します。
3. [Select trusted entity] (信頼できるエンティティを選択) で、次のように選択します。
    1. 信頼できるエンティティタイプ で、AWS のサービス を選択します。
    2. [その他の AWS のサービス のユースケース] で、[Systems Manager] を選択します。
    3. [Systems Manager] を選択します。

        次の画像は、Systems Manager オプションの場所を示しています。



4. [Next] を選択します。
5. [アクセス許可を追加] ページで、以下を実行します。

   - [Search] (検索) フィールドを使用して、[AmazonSSMManagedInstanceCore] ポリシーを検索します。次の図に示すように、名前の横にあるチェックボックスをオンにします。

   > **Note**
   >
   > 他のポリシーを検索しても、コンソールでは選択内容が保持されます。

   - 手順 (オプション) S3 バケットへのアクセスのカスタムポリシーを作成する でカスタムの S3 バケットポリシーを作成した場合は、それを検索してその名前の横にあるチェックボックスをオンにします。
   - AWS Directory Service によって管理されている Active Directory に、EC2 以外のマシンを結合する場合は、AmazonSSMDirectoryServiceAccess を検索し、その名前の横にあるチェックボックスをオンにします。
   - EventBridge または CloudWatch Logs を使用して、マネージドノードを管理またはモニタリングする場合は、[CloudWatchAgentServerPolicy] を検索し、その名前の横にあるチェックボックスをオンにします。

6. [Next] を選択します。

7. [ロール名] で、**SSMServerRole** などの新しい IAM サーバーロールの名前を入力します。

> **Note**
>
> ロール名を書き留めます。このロール名は、Systems Manager を使用して管理するマシンを新しく登録する際に選択します。

8. (オプション) [Description] (説明) で、この IAM サーバーロールの説明を更新します。
9. (オプション) [Tags] (タグ)で、タグとキーの値のペアを 1 つまたは複数追加して、このロールのアクセスを整理、追跡、または制御します。
10. [ロールの作成] を選択します。ロールページが再度表示されます。

AWS CLI を使用して Systems Manager ハイブリッドアクティベーション用の IAM サービスロールを作成する

ハイブリッドアクティベーションのサービスロールを作成するために、以下の手順にしたがいます。この手順では、Systems Manager の主要機能で `AmazonSSMManagedInstanceCore` ポリシーを使用します。ユースケースによっては、ハイブリッドおよびマルチクラウド環境の EC2 以外のマシンのサービスロールにポリシーをさらに追加して、他のツールや AWS のサービスにアクセスできるようにする必要がある場合があります。

S3 バケットのポリシーの要件

次のいずれかのケースに当てはまる場合は、この手順を実行する前に Amazon Simple Storage Service (Amazon S3) バケット用のカスタム IAM アクセス許可ポリシーを作成する必要があります。

- ケース 1 — VPC エンドポイントを使用して、サポートされている AWS のサービス、および AWS PrivateLink を搭載した VPC エンドポイントサービスに VPC をプライベート接続している。
- ケース 2 — Run Command コマンドや Session Manager セッションの出力を S3 バケットに保存するなど、作成する Amazon S3 バケットを Systems Manager オペレーションの一環として使用する。先に進む前に、「インスタンスプロファイル用のカスタム S3 バケットポリシーを作成する」の手順に従います。そのトピックの S3 バケットポリシーに関する情報は、サービスロールにも適用されます。

AWS CLI

ハイブリッドおよびマルチクラウド環境に IAM サービスロールを作成するには (AWS CLI)

1. まだ AWS Command Line Interface (AWS CLI) をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」を参照してください。

2. ローカルマシンで以下の信頼ポリシーを使用して、SSMService-Trust.json のような名前でテキストファイルを作成します。ファイル保存時に、必ずファイル拡張子 (.json) を付けます。ハイブリッドアクティベーションを作成した際の ARN 内の AWS アカウント と AWS リージョン を必ず指定してください。アカウント ID とリージョンの *placeholder values* をユーザーの情報に置き換えます。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"",
         "Effect":"Allow",
         "Principal":{
            "Service":"ssm.amazonaws.com"
         },
         "Action":"sts:AssumeRole",
         "Condition":{
            "StringEquals":{
               "aws:SourceAccount":"123456789012"
            },
            "ArnEquals":{
               "aws:SourceArn":"arn:aws:ssm:us-east-2:123456789012:*"
            }
         }
      }
   ]
}
```

3. AWS CLI を開き、JSON ファイルを作成したディレクトリで create-role コマンドを実行してサービスロールを作成します。この例では、SSMServiceRole という名前のロールが作成されます。別の名前を選択することもできます。

Linux & macOS

```
aws iam create-role \
    --role-name SSMServiceRole \
    --assume-role-policy-document file://SSMService-Trust.json
```

Windows

```
aws iam create-role ^
    --role-name SSMServiceRole ^
    --assume-role-policy-document file://SSMService-Trust.json
```

4. 以下のように attach-role-policy を実行して、先ほど作成したサービスロールでセッショントークンを作成できるようにします。セッショントークンは、Systems Manager を使用してコマンドを実行するためのアクセス許可をマネージドノードに付与します。

> **Note**
>
> ハイブリッドおよびマルチクラウド環境のマネージドノードのサービスプロファイルに追加するポリシーは、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのインスタンスプロファイルの作成に使用されるものと同じです。以下のコマンドで使用する AWS ポリシーの詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」を参照してください。

(必須) 次のコマンドを使用して、マネージドノードで AWS Systems Manager サービスの主要機能を使用できるようにします。

Linux & macOS

```
aws iam attach-role-policy \
    --role-name SSMServiceRole \
    --policy-arn arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore
```

Windows

```
aws iam attach-role-policy ^
    --role-name SSMServiceRole ^
```

```
    --policy-arn arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore
```

サービスロールのカスタム S3 バケットポリシーを作成した場合は、次のコマンドを実行して、ポリシーで指定したバケットに AWS Systems Manager Agent (SSM Agent) がアクセスできるようにします。*account-id* と *amzn-s3-demo-bucket* は、お使いの AWS アカウント ID とバケット名に置き換えてください。

Linux & macOS

```
aws iam attach-role-policy \
    --role-name SSMServiceRole \
    --policy-arn arn:aws:iam::account-id:policy/amzn-s3-demo-bucket
```

Windows

```
aws iam attach-role-policy ^
    --role-name SSMServiceRole ^
    --policy-arn arn:aws:iam::account-id:policy/amzn-s3-demo-bucket
```

(オプション) 次のコマンドを実行して、マネージドノードによるドメインへの結合リクエストに対して、SSM Agent がユーザーの代わりに AWS Directory Service にアクセスできるようにします。ノードを Microsoft AD ディレクトリに統合する場合のみ、サービスロールにこのポリシーが必要です。

Linux & macOS

```
aws iam attach-role-policy \
    --role-name SSMServiceRole \
    --policy-arn arn:aws:iam::aws:policy/AmazonSSMDirectoryServiceAccess
```

Windows

```
aws iam attach-role-policy ^
    --role-name SSMServiceRole ^
    --policy-arn arn:aws:iam::aws:policy/AmazonSSMDirectoryServiceAccess
```

(オプション) 次のコマンドを実行して、CloudWatch エージェントがマネージドノードで実行できるようにします。このコマンドを使用すると、ノードの情報を読み込んで CloudWatch に書き込みを行うことができます。サービスプロファイルには、Amazon EventBridge や Amazon CloudWatch Logs などのサービスを利用する場合にのみ、このポリシーが必要です。

```
aws iam attach-role-policy \
    --role-name SSMServiceRole \
    --policy-arn arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy
```

Tools for PowerShell

ハイブリッドおよびマルチクラウド環境に IAM サービスロールを作成するには (AWS Tools for Windows PowerShell)

1. AWS Tools for PowerShell (Tools for Windows PowerShell) をインストールして設定します (まだインストールしていない場合)。

   詳細については、「AWS Tools for PowerShell のインストール」を参照してください。

2. ローカルマシンで以下の信頼ポリシーを使用して、SSMService-Trust.json のような名前でテキストファイルを作成します。ファイル保存時に、必ずファイル拡張子 (.json) を付けます。ハイブリッドアクティベーションを作成した際の ARN 内の AWS アカウント と AWS リージョン を必ず指定してください。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"",
         "Effect":"Allow",
         "Principal":{
            "Service":"ssm.amazonaws.com"
         },
         "Action":"sts:AssumeRole",
         "Condition":{
            "StringEquals":{
               "aws:SourceAccount":"123456789012"
            },
```

```
            "ArnEquals":{
               "aws:SourceArn":"arn:aws:ssm:region:123456789012:*"
            }
         }
      }
   ]
}
```

3. PowerShell を管理モードで開き、JSON ファイルを作成したディレクトリで以下のように New-IAMRole を実行してサービスロールを作成します。この例では、SSMServiceRole という名前のロールが作成されます。別の名前を選択することもできます。

```
New-IAMRole `
    -RoleName SSMServiceRole `
    -AssumeRolePolicyDocument (Get-Content -raw SSMService-Trust.json)
```

4. 以下のように、Register-IAMRolePolicy を使用して、作成したサービスロールでセッショントークンを作成できます。セッショントークンは、Systems Manager を使用してコマンドを実行するためのアクセス許可をマネージドノードに付与します。

> **Note**
>
> ハイブリッドおよびマルチクラウド環境のマネージドノードのサービスプロファイルに追加するポリシーは、EC2 インスタンスのインスタンスプロファイルの作成に使用されるものと同じです。以下のコマンドで使用する AWS ポリシーの詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」を参照してください。

(必須) 次のコマンドを使用して、マネージドノードで AWS Systems Manager サービスの主要機能を使用できるようにします。

```
Register-IAMRolePolicy `
    -RoleName SSMServiceRole `
    -PolicyArn arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore
```

サービスロールのカスタム S3 バケットポリシーを作成した場合は、次のコマンドを実行し、ポリシーで指定したバケットに SSM Agent がアクセスできるようにします。*account-*

id および *my-bucket-policy-name* を AWS アカウント ID およびバケット名に置き換えます。

```
Register-IAMRolePolicy `
    -RoleName SSMServiceRole `
    -PolicyArn arn:aws:iam::account-id:policy/my-bucket-policy-name
```

(オプション) 次のコマンドを実行して、マネージドノードによるドメインへの結合リクエストに対して、SSM Agent がユーザーの代わりに AWS Directory Service にアクセスできるようにします。ノードを Microsoft AD ディレクトリに統合する場合のみ、サーバーロールにこのポリシーが必要です。

```
Register-IAMRolePolicy `
    -RoleName SSMServiceRole `
    -PolicyArn arn:aws:iam::aws:policy/AmazonSSMDirectoryServiceAccess
```

(オプション) 次のコマンドを実行して、CloudWatch エージェントがマネージドノードで実行できるようにします。このコマンドを使用すると、ノードの情報を読み込んで CloudWatch に書き込みを行うことができます。サービスプロファイルには、Amazon EventBridge や Amazon CloudWatch Logs などのサービスを利用する場合にのみ、このポリシーが必要です。

```
Register-IAMRolePolicy `
    -RoleName SSMServiceRole `
    -PolicyArn arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy
```

「ハイブリッドアクティベーションを作成して、Systems Manager にノードを登録する」に進みます。

ハイブリッドアクティベーションを作成して、Systems Manager にノードを登録する

Amazon Elastic Compute Cloud (EC2) インスタンス以外のマシンをハイブリッドおよびマルチクラウド環境のマネージドノードとしてセットアップするには、ハイブリッドアクティベーションを作成して適用します。アクティベーションが正常に完了すると、コンソールページの上部にアクティベーションコードとアクティベーション ID が直ちに表示されます。ハイブリッドおよびマルチクラウド環境で非 EC2 マシンに AWS Systems Manager SSM Agent をインストールする際に、このコードと

ID の組み合わせを指定します。このコードと ID を使用することで、マネージドノードから Systems Manager サービスに安全にアクセスできます。

> **Important**
>
> アクティベーションの作成方法に応じて、Systems Manager はすぐにアクティベーションコードと ID をコンソールまたはコマンドウィンドウに返します。この情報をコピーして、安全な場所に保管します。コンソールから離れたり、コマンドウィンドウを閉じたりすると、この情報は失われる可能性があります。紛失した場合は、新しいアクティベーションを作成する必要があります。

アクティベーションの有効期限について

アクティベーションの有効期限は、オンプレミスのマシンを Systems Manager で登録できる時間帯です。アクティベーションの有効期限が切れても、Systems Manager に前もって登録したサーバーまたは VM に影響はありません。アクティベーションが期限切れになると、その特定のアクティベーションを使用して、複数のサーバーまたは VM を Systems Manager に登録することはできません。新しいものを作成する必要があるだけです。

前もって登録したすべてのオンプレミスサーバーおよび VM は、明示的に登録を解除するまで、Systems Manager のマネージドノードとして登録されたままになります。EC2 以外のマネージドノードの登録は以下の方法で解除できます。

- Systems Manager コンソールの Fleet Manager でマネージドノードタブを使用する
- AWS CLI コマンド deregister-managed-instance を実行する
- API アクション DeregisterManagedInstance を使用する

詳細については、以下の各トピックを参照してください。

- マネージドノードの登録解除と再登録 (Linux)
- マネージドノードの登録解除と再登録 (Windows Server)

マネージドノードについて

マネージドノードは AWS Systems Manager 用に設定されたすべてのマシンを指します。AWS Systems Manager は、Amazon Elastic Compute Cloud (Amazon EC2) インスタンス、エッジデバイス、オンプレミスサーバー、または VM (他のクラウド環境にある VM を含む) をサポートしていま

す。以前は、マネージドノードはすべてマネージドインスタンスと呼ばれていました。現在、インスタンスとは EC2 インスタンスのみを指します。deregister-managed-instance コマンドは、この用語変更の前に命名されました。

アクティベーションタグについて

AWS Command Line Interface (AWS CLI) または AWS Tools for Windows PowerShell を使用してアクティベーションを作成する場合は、タグを指定できます。タグは、リソースに割り当てるオプションのメタデータです。タグを使用すると、目的、所有者、環境などのさまざまな方法でリソースを分類できます。ここでは、米国東部 (オハイオ) のローカル Linux マシンで実行する、オプションのタグを含む AWS CLI サンプルコマンドを示します。

```
aws ssm create-activation \
  --default-instance-name MyWebServers \
  --description "Activation for Finance department webservers" \
  --iam-role service-role/AmazonEC2RunCommandRoleForManagedInstances \
  --registration-limit 10 \
  --region us-east-2 \
  --tags "Key=Department,Value=Finance"
```

アクティベーションの作成時にタグを指定すると、それらのタグはアクティブ化する際に自動的にマネージドノードに割り当てられます。

既存のアクティベーションにタグを追加したり、既存のアクティベーションからタグを削除したりすることはできません。アクティベーションを使用してオンプレミスサーバーと VM に自動的にタグを割り当てない場合は、後でタグを追加できます。具体的には、オンプレミスサーバーと VM が初めて Systems Manager に接続した後にタグを付けることができます。接続すると、マネージドノード ID が割り当てられ、先頭に「mi-」が付いた ID で Systems Manager コンソールに表示されます。

> **Note**
>
> Systems Manager コンソールを使用してアクティベーションを作成した場合、アクティベーションにタグを割り当てることはできません。AWS CLI または Tools for Windows PowerShell のいずれかを使用してアクティベーションを作成する必要があります。

Systems Manager を使用してオンプレミスサーバーや仮想マシン (VM) を管理する必要がなくなった場合は、登録解除できます。詳細については、ハイブリッドおよびマルチクラウド環境でのマネージドノードの登録解除 を参照してください。

トピック

- AWS Management Console を使用して、Systems Manager でマネージドノードを登録するためのアクティベーションを作成します。
- コマンドラインを使用して、Systems Manager でマネージドノードを登録するためのアクティベーションを作成する

AWS Management Console を使用して、Systems Manager でマネージドノードを登録するためのアクティベーションを作成します。

マネージドノードのアクティベーションを作成するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで [ハイブリッドアクティベーション] を選択します。
3. [Create activation] を選択します。

   -または-

   現在の AWS リージョン で [Hybrid Activations] (ハイブリッドアクティベーション) に初めてアクセスしている場合は、[Create an Activation] (アクティベーションの作成) を選択します。
4. (オプション) [Activation description] (アクティベーションの説明) フィールドに、このアクティベーションの説明を入力します。多数のサーバーや VM を有効化する場合は、説明を入力することをお勧めします。
5. [Instance limit] (インスタンス制限) で、このアクティベーションの一環として AWS に登録するノードの合計数を指定します。デフォルト値は 1 インスタンスです。
6. [IAM role name] (IAM ロール) で、サーバーや VM とクラウド内の AWS Systems Manager との通信を可能にするサービスロールオプションを選択します。

   - オプション 1: AWS が提供するロールと管理ポリシーを使用するには、[Use the default role created by the system] (システムによって作成されたデフォルトのロールを使用する) を選択します。
   - オプション 2: 前に作成したオプションのカスタムロールを使用するには、[Select an existing custom IAM role that has the required permissions] (必要な許可を持つ既存のカスタム IAM ロールを選択する) を選択します。このロールには、`"Service": "ssm.amazonaws.com"` を指定する信頼関係ポリシーが必要です。IAM ロールが信頼関係ポリシーでこの原則を指定しない場合、次のエラーが発生します。

```
An error occurred (ValidationException) when calling the CreateActivation
                                    operation: Not existing role:
 arn:aws:iam::<accountid>:role/SSMRole
```

このロールの作成に関する詳細については、「ハイブリッドおよびマルチクラウド環境で Systems Manager に必要な IAM サービスロールを作成する」を参照してください。

7. [Activation expiry date] (アクティベーションの有効期限日) で、アクティベーションの有効期限日を指定します。有効期限は将来の日付で、30 日以内でなければなりません。デフォルト値は 24 時間です。

> **Note**
>
> 有効期限日後にマネージドノードを追加で登録するには、新しいアクティベーションを作成する必要があります。有効期限日は、登録済みで実行中のインスタンスには影響しません。

8. (オプション) [Default instance name] (デフォルトのインスタンス名) フィールドで、このアクティベーションに関連付けられているすべてのマネージドノードに表示する識別名の値を指定します。
9. [Create activation] を選択します。Systems Manager は、すぐにアクティベーションコードと ID をコンソールに返します。

コマンドラインを使用して、Systems Manager でマネージドノードを登録するためのアクティベーションを作成する

次の手順では、AWS Command Line Interface (AWS CLI) (Linux または Windows Server の場合) または AWS Tools for PowerShell を使用して、マネージドノードのアクティベーションを作成する方法について説明します。

アクティベーションを作成するには

1. まだ AWS CLI または AWS Tools for PowerShell をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」および「AWS Tools for PowerShell のインストール」を参照してください。

2. アクティベーションを作成するには、次のコマンドを実行します。

> **Note**
>
> - 次のコマンドで、*[Region]* (リージョン) をユーザー自身の情報に置き換えます。サポートされている *region* 値の一覧については、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」にある Region 列を参照してください。
> - *iam-role* パラメータに指定するロールには、"Service": "ssm.amazonaws.com" を指定する信頼関係ポリシーが必要です。AWS Identity and Access Management (IAM) ロールが信頼関係ポリシーでこの原則を指定しない場合、次のエラーが発生します。
>
>   ```
>   An error occurred (ValidationException) when calling the CreateActivation
>                                           operation: Not existing role:
>    arn:aws:iam::<accountid>:role/SSMRole
>   ```
>
>   このロールの作成に関する詳細については、「ハイブリッドおよびマルチクラウド環境で Systems Manager に必要な IAM サービスロールを作成する」を参照してください。
> - --expiration-date の場合、アクティベーションコードの有効期限が切れるときの日付を、"2021-07-07T00:00:00" などのタイムスタンプ形式で指定します。日付は 30 日を上限に事前に指定できます。有効期限を指定しない場合、アクティベーションコードは 24 時間で有効期限が切れます。

Linux & macOS

```
aws ssm create-activation \
    --default-instance-name name \
    --iam-role iam-service-role-name \
    --registration-limit number-of-managed-instances \
    --region region \
    --expiration-date "timestamp" \\
    --tags "Key=key-name-1,Value=key-value-1" "Key=key-name-2,Value=key-value-2"
```

Windows

```
aws ssm create-activation ^
    --default-instance-name name ^
    --iam-role iam-service-role-name ^
    --registration-limit number-of-managed-instances ^
    --region region ^
    --expiration-date "timestamp" ^
    --tags "Key=key-name-1,Value=key-value-1" "Key=key-name-2,Value=key-value-2"
```

PowerShell

```
New-SSMActivation -DefaultInstanceName name `
    -IamRole iam-service-role-name `
    -RegistrationLimit number-of-managed-instances `
    -Region region `
    -ExpirationDate "timestamp" `
    -Tag @{"Key"="key-name-1";"Value"="key-value-1"},@{"Key"="key-
name-2";"Value"="key-value-2"}
```

以下はその例です。

Linux & macOS

```
aws ssm create-activation \
    --default-instance-name MyWebServers \
    --iam-role service-role/AmazonEC2RunCommandRoleForManagedInstances \
    --registration-limit 10 \
    --region us-east-2 \
    --expiration-date "2021-07-07T00:00:00" \
    --tags "Key=Environment,Value=Production" "Key=Department,Value=Finance"
```

Windows

```
aws ssm create-activation ^
    --default-instance-name MyWebServers ^
    --iam-role service-role/AmazonEC2RunCommandRoleForManagedInstances ^
    --registration-limit 10 ^
    --region us-east-2 ^
    --expiration-date "2021-07-07T00:00:00" ^
```

```
    --tags "Key=Environment,Value=Production" "Key=Department,Value=Finance"
```

PowerShell

```
New-SSMActivation -DefaultInstanceName MyWebServers `
    -IamRole service-role/AmazonEC2RunCommandRoleForManagedInstances `
    -RegistrationLimit 10 `
    -Region us-east-2 `
    -ExpirationDate "2021-07-07T00:00:00" `
    -Tag
 @{"Key"="Environment";"Value"="Production"},@{"Key"="Department";"Value"="Finance"}
```

アクティベーションが正常に完了するとすぐに、システムからアクティベーションコードとアクティベーション ID が返ります。

ハイブリッド Linux ノードで SSM Agent をインストールする

このトピックでは、ハイブリッドおよびマルチクラウド環境で非 EC2 (Amazon Elastic Compute Cloud) Linux マシンに AWS Systems Manager SSM Agent をインストールする方法について説明します。Linux の EC2 インスタンスへの SSM Agent のインストールの詳細については、「Linux 用 EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする」を参照してください。

開始する前に、「ハイブリッドアクティベーションを作成して、Systems Manager にノードを登録する」の説明に従って、ハイブリッドアクティベーションプロセス中に生成されたアクティベーションコードとアクティベーション ID を見つけます。このコードと ID を次の手順で指定します。

ハイブリッドおよびマルチクラウド環境の非 EC2 マシンに SSM Agent をインストールするには

1. ハイブリッドおよびマルチクラウド環境のサーバーまたは VM にログオンします。
2. HTTP または HTTPS プロキシを使用する場合は、現在のシェルセッションで `http_proxy` または `https_proxy` の環境変数を設定する必要があります。プロキシを使用していない場合は、この手順を省略できます。

   HTTP プロキシサーバーの場合は、コマンドラインで次のコマンドを入力します。

```
export http_proxy=http://hostname:port
export https_proxy=http://hostname:port
```

HTTPS プロキシサーバの場合は、コマンドラインで次のコマンドを入力します。

```
export http_proxy=http://hostname:port
export https_proxy=https://hostname:port
```

3. SSH に以下のコマンドブロックをコピーアンドペーストします。プレースホルダー値を、ハイブリッドアクティベーションプロセス中に生成されたアクティベーションコードとアクティベーション ID、および SSM Agent のダウンロード元の AWS リージョン の識別子に置き換えて、Enter を押します。

> **Important**
>
> 次の重要な詳細に留意してください。
>
> - EC2 以外のインストールに ssm-setup-cli を使用すると、Systems Manager のインストールと設定のセキュリティを最大化できます。
> - root ユーザーの場合は sudo が必要ありません。
> - ハイブリッドアクティベーションを作成したのと同じ AWS リージョン から ssm-setup-cli をダウンロードします。
> - ssm-setup-cli で、エージェントのダウンロード元を判断する manifest-url オプションがサポートされました。ご自身の組織で必要とされている場合を除き、このオプションには値を指定しないでください。
> - インスタンスを登録するときは、ssm-setup-cli 用として指定されたダウンロードリンクのみを使用します。ssm-setup-cli を今後の使用のために個別に保管しないでください。
> - ここに記載されているスクリプトを使用して、ssm-setup-cli の署名を検証できます。

region は、米国東部 (オハイオ) リージョンの us-east-2 のように、AWS Systems Manager でサポートされている AWS リージョン の識別子を表します。サポートされている *region* 値の一覧については、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」にある Region 列を参照してください。

さらに、ssm-setup-cli には次のオプションが含まれます。

- version – 有効な値は latest および stable です。

- downgrade - SSM Agent を以前のバージョンにダウングレードすることを許可します。エージェントの以前のバージョンをインストールするため true を指定します。
- skip-signature-validation - エージェントをダウンロードおよびインストールする間の署名検証をスキップします。

RHEL、 6.x、および CentOS 6.x

```
mkdir /tmp/ssm
curl https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/3.0.1479.0/linux_amd64/
amazon-ssm-agent.rpm -o /tmp/ssm/amazon-ssm-agent.rpm
sudo yum install -y /tmp/ssm/amazon-ssm-agent.rpm
sudo stop amazon-ssm-agent
sudo -E amazon-ssm-agent -register -code "activation-code" -id "activation-id" -region
 "region"
sudo start amazon-ssm-agent
```

Amazon Linux 1

```
mkdir /tmp/ssm
curl https://amazon-ssm-region.s3.region.amazonaws.com/latest/linux_amd64/ssm-setup-cli
 -o /tmp/ssm/ssm-setup-cli
sudo chmod +x /tmp/ssm/ssm-setup-cli
sudo /tmp/ssm/ssm-setup-cli -register -activation-code "activation-code" -id
 "activation-id" -region "region"
```

Amazon Linux 2、RHEL 7.x、Oracle Linux、CentOS 7.x、および SLES

```
mkdir /tmp/ssm
curl https://amazon-ssm-region.s3.region.amazonaws.com/latest/linux_amd64/ssm-setup-cli
 -o /tmp/ssm/ssm-setup-cli
sudo chmod +x /tmp/ssm/ssm-setup-cli
sudo /tmp/ssm/ssm-setup-cli -register -activation-code "activation-code" -activation-id
 "activation-id" -region "region"
```

RHEL 8.x および CentOS 8.x

```
mkdir /tmp/ssm
curl https://amazon-ssm-region.s3.region.amazonaws.com/latest/linux_amd64/ssm-setup-cli
 -o /tmp/ssm/ssm-setup-cli
sudo chmod +x /tmp/ssm/ssm-setup-cli
```

```
sudo /tmp/ssm/ssm-setup-cli -register -activation-code "activation-code" -activation-id
 "activation-id" -region "region"
```

Debian Server

```
mkdir /tmp/ssm
curl https://amazon-ssm-region.s3.region.amazonaws.com/latest/debian_amd64/ssm-setup-
cli -o /tmp/ssm/ssm-setup-cli
sudo chmod +x /tmp/ssm/ssm-setup-cli
sudo /tmp/ssm/ssm-setup-cli -register -activation-code "activation-code" -activation-id
 "activation-id" -region "region"
```

Raspberry Pi OS (旧称 Raspbian)

```
mkdir /tmp/ssm
curl https://amazon-ssm-region.s3.region.amazonaws.com/latest/debian_arm/ssm-setup-cli
 -o /tmp/ssm/ssm-setup-cli
sudo chmod +x /tmp/ssm/ssm-setup-cli
sudo /tmp/ssm/ssm-setup-cli -register -activation-code "activation-code" -activation-id
 "activation-id" -region "region"
```

Ubuntu Server

- .deb パッケージを使用

  ```
  mkdir /tmp/ssm
  curl https://amazon-ssm-region.s3.region.amazonaws.com/latest/debian_amd64/ssm-setup-
  cli -o /tmp/ssm/ssm-setup-cli
  sudo chmod +x /tmp/ssm/ssm-setup-cli
  sudo /tmp/ssm/ssm-setup-cli -register -activation-code "activation-code" -activation-
  id "activation-id" -region "region"
  ```

- スナップパッケージを使用

  ダウンロードの URL を指定する必要はありません。snap コマンドでは、エージェントが Snap アプリストア https://snapcraft.io から自動的にダウンロードされます。

  Ubuntu Server 20.10 STR および 20.04、18.04、16.04 LTS の場合、SSM Agent インストーラファイル (エージェントバイナリや設定ファイルなど) は /snap/amazon-ssm-agent/current/ ディレクトリに保存されます。このディレクトリで設定ファイルに変更を加えた場合、これらのファイルを /snap ディレクトリから /etc/amazon/ssm/ ディレクトリにコピーす

る必要があります。ログファイルおよびライブラリファイルは変更されていません (/var/lib/amazon/ssm、/var/log/amazon/ssm)。

```
sudo snap install amazon-ssm-agent --classic
sudo systemctl stop snap.amazon-ssm-agent.amazon-ssm-agent.service
sudo /snap/amazon-ssm-agent/current/amazon-ssm-agent -register -code "activation-code" -id "activation-id" -region "region"
sudo systemctl start snap.amazon-ssm-agent.amazon-ssm-agent.service
```

> **Important**
>
> Snap ストアの候補チャンネルには、安定したチャンネルではなく、SSM Agent の最新バージョンが含まれています。候補チャンネルの SSM Agent バージョン情報を追跡する場合は、Ubuntu Server 18.04 および 16.04 LTS 64 ビットマネージドノードで次のコマンドを実行します。
>
> ```
> sudo snap switch --channel=candidate amazon-ssm-agent
> ```

このコマンドでは、ハイブリッドおよびマルチクラウド環境のハイブリッドアクティベーションマシンに SSM Agent をダウンロードしてインストールします。コマンドは、SSM Agent を停止してから、マシンを Systems Manager サービスに登録します。これで、マシンはマネージドノードになりました。Systems Manager 用に設定されている Amazon EC2 インスタンスも、マネージドノードです。ただし、Systems Manager コンソールでは、ハイブリッドアクティベーションノードは、プレフィックス「mi-」が付いている Amazon EC2 インスタンスとは区別されます。

「ハイブリッド Windows Server ノードに SSM Agent をインストールする」に進んでください。

プライベートキーの自動ローテーションを設定する

セキュリティポスチャを強化するには、ハイブリッドおよびマルチクラウド環境のプライベートキーを自動的にローテーションするように AWS Systems Manager エージェント (SSM Agent) を設定できます。SSM Agent バージョン 3.0.1031.0 以降を使用すると、この機能にアクセスできます。次の手順に従ってこの機能を有効にします。

ハイブリッドおよびマルチクラウド環境のプライベートキーをローテーションするように SSM Agent を設定するには

1. Linux マシンでは /etc/amazon/ssm/、Windows マシンでは C:\Program Files\Amazon\SSM に移動します。
2. amazon-ssm-agent.json.template の内容を amazon-ssm-agent.json という名前の新ファイルにコピーします。amazon-ssm-agent.json.template と同じディレクトリに amazon-ssm-agent.json を保存します。
3. Profile、KeyAutoRotateDays を探す プライベートキーの自動ローテーション間隔の日数を入力します。
4. SSM Agent を再起動します。

設定を変更するたびに、SSM Agent を再起動します。

同じ手順を使用して、SSM Agent の他の機能をカスタマイズできます。使用可能な設定プロパティとそのデフォルト値の最新リストについては、「Config Property Definitions (設定プロパティの定義)」を参照してください。

マネージドノードの登録解除と再登録 (Linux)

ハイブリッドアクティベーションマネージドノードの登録を解除するには、AWS CLI または Tools for Windows PowerShell のいずれかから DeregisterManagedInstance API オペレーションを呼び出します。以下に CLI コマンドの例を示します。

```
aws ssm deregister-managed-instance --instance-id "mi-1234567890"
```

エージェントの残りの登録情報を削除するには、amazon-ssm-agent.json ファイル内の IdentityConsumptionOrder キーを削除します。インストールのタイプに応じて、次のいずれかのコマンドを実行します。

Snap パッケージを使用して SSM Agent がインストールされた Ubuntu Server ノードの場合:

```
sudo /snap/amazon-ssm-agent/current/amazon-ssm-agent -register -clear
```

それ以外の Linux インストールの場合:

```
amazon-ssm-agent -register -clear
```

非 EC2 Linux マシンでマネージノードを再登録するには

マシンは、登録解除した後に再登録できます。ただし、マシンを登録するために以前使用したものとは異なる、アクティベーションコードとアクティベーション ID を使用する必要があります。

1. マシンへ接続します。
2. 以下のコマンドを実行してください。必ずプレースホルダー値の代わりに、マネージドノードのアクティベーションの作成時に生成されたアクティベーションコードとアクティベーション ID、および SSM Agent のダウンロード元のリージョンの識別子を入力します。

```
echo "yes" | sudo /tmp/ssm/ssm-setup-cli -register -activation-code "activation-code" -activation-id "activation-id" -region "region
```

非 EC2 Linux マシンでの SSM Agent のインストールに関するトラブルシューティング

次の情報は、ハイブリッドおよびマルチクラウド環境でハイブリッドアクティベーション Linux マシンに SSM Agent をインストールする際の問題のトラブルシューティングに役立ちます。

DeliveryTimedOut エラーの発生

問題: ある AWS アカウント のマシンを別の AWS アカウント のマネージドノードとして設定している際に、ターゲットマシンに SSM Agent をインストールするコマンドを実行した後に `DeliveryTimedOut` が表示されます。

解決方法: `DeliveryTimedOut` がこのシナリオで予想される応答コードです。ターゲットノードに SSM Agent をインストールするコマンドによって、ソースノードのノード ID が変更されます。ノード ID が変更されたため、ソースノードは、実行中にコマンドが失敗したこと、完了したこと、またはタイムアウトしたことをターゲットノードに返信できません。

ノードの関連付けをロードできない

問題: インストールコマンドを実行した後、SSM Agent エラーログに次のエラーが表示されます。

```
Unable to load instance associations, unable to retrieve
associations unable to retrieve associations error occurred in
RequestManagedInstanceRoleToken: MachineFingerprintDoesNotMatch:
Fingerprint doesn't match
```

このエラーは、再起動後にマシン ID が持続しない場合に表示されます。

解決方法: この問題を解決するには、次のコマンドを実行します。このコマンドは、再起動後もマシン ID を強制的に保持します。

```
umount /etc/machine-id
systemd-machine-id-setup
```

ハイブリッド Windows Server ノードに SSM Agent をインストールする

このトピックでは、ハイブリッドおよびマルチクラウド環境の Windows Server マシンに AWS Systems Manager SSM Agent をインストールする方法について説明します。Windows Server の EC2 インスタンス SSM Agent へのインストールの詳細については、「Windows Server 用の EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする」を参照してください。

開始する前に、「ハイブリッドアクティベーションを作成して、Systems Manager にノードを登録する」の説明に従って、ハイブリッドアクティベーションプロセス中に生成されたアクティベーションコードとアクティベーション ID を見つけます。このコードと ID を次の手順で指定します。

ハイブリッドおよびマルチクラウド環境の非 EC2 Windows Server マシンに SSM Agent をインストールするには

1. ハイブリッドおよびマルチクラウド環境のサーバーまたは VM にログオンします。
2. HTTP または HTTPS プロキシを使用する場合は、現在のシェルセッションで `http_proxy` または `https_proxy` の環境変数を設定する必要があります。プロキシを使用していない場合は、この手順を省略できます。

   HTTP プロキシサーバーの場合は、次の変数を設定します。

   ```
   http_proxy=http://hostname:port
   https_proxy=http://hostname:port
   ```

   HTTPS プロキシサーバーの場合は、次の変数を設定します。

   ```
   http_proxy=http://hostname:port
   https_proxy=https://hostname:port
   ```
3. 昇格された (管理者) モードで Windows PowerShell を開きます。
4. Windows PowerShell に以下のコマンドブロックを貼り付けます。各##############をユーザー自身の情報に置き換えます。例えば、ハイブリッドのアクティベーションの作成時に生成さ

れたアクティベーションコードとアクティベーション ID、および SSM Agent のダウンロード元の AWS リージョン の識別子です。

> **Important**
>
> 次の重要な詳細に留意してください。
>
> - EC2 以外のインストールに `ssm-setup-cli` を使用すると、Systems Manager のインストールと設定のセキュリティを最大化できます。
> - `ssm-setup-cli` で、エージェントのダウンロード元を判断する `manifest-url` オプションがサポートされました。ご自身の組織で必要とされている場合を除き、このオプションには値を指定しないでください。
> - ここに記載されているスクリプトを使用して、`ssm-setup-cli` の署名を検証できます。
> - インスタンスを登録するときは、`ssm-setup-cli` 用として指定されたダウンロードリンクのみを使用します。`ssm-setup-cli` を今後の使用のために個別に保管しないでください。

`region` は、米国東部 (オハイオ) リージョンの `us-east-2` のように、AWS Systems Manager でサポートされている AWS リージョン の識別子を表します。サポートされている *`region`* 値の一覧については、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」にある Region 列を参照してください。

さらに、`ssm-setup-cli` には次のオプションが含まれます。

- `version` – 有効な値は `latest` および `stable` です。
- `downgrade` - エージェントを以前のバージョンに戻します。
- `skip-signature-validation` - エージェントをダウンロードおよびインストールする間の署名検証をスキップします。

64-bit

```
[System.Net.ServicePointManager]::SecurityProtocol = 'TLS12'
$code = "activation-code"
$id = "activation-id"
$region = "us-east-1"
```

```
$dir = $env:TEMP + "\ssm"
New-Item -ItemType directory -Path $dir -Force
cd $dir
(New-Object System.Net.WebClient).DownloadFile("https://amazon-ssm-$region.s3.
$region.amazonaws.com/latest/windows_amd64/ssm-setup-cli.exe", $dir + "\ssm-
setup-cli.exe")
./ssm-setup-cli.exe -register -activation-code="$code" -activation-id="$id" -
region="$region"
Get-Content ($env:ProgramData + "\Amazon\SSM\InstanceData\registration")
Get-Service -Name "AmazonSSMAgent"
```

32-bit

```
"[System.Net.ServicePointManager]::SecurityProtocol = 'TLS12'"
$code = "activation-code"
$id = "activation-id"
$region = "us-east-1"
$dir = $env:TEMP + "\ssm"
New-Item -ItemType directory -Path $dir -Force
cd $dir
(New-Object System.Net.WebClient).DownloadFile("https://amazon-ssm-$region.s3.
$region.amazonaws.com/latest/windows_386/ssm-setup-cli.exe", $dir + "\ssm-setup-
cli.exe")
./ssm-setup-cli.exe -register -activation-code="$code" -activation-id="$id" -
region="$region"
Get-Content ($env:ProgramData + "\Amazon\SSM\InstanceData\registration")
Get-Service -Name "AmazonSSMAgent"
```

5. Enter キーを押します。

> **Note**
>
> コマンドが失敗した場合は、AWS Tools for PowerShell の最新バージョンを実行していることを確認します。

コマンドが以下の操作を行います。

- SSM Agent をマシンにダウンロードしてインストールします。
- マシンを Systems Manager サービスに登録します。
- リクエストに対して次のようなレスポンスを返します。

```
    Directory: C:\Users\ADMINI~1\AppData\Local\Temp\2


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----       07/07/2018   8:07 PM                ssm
{"ManagedInstanceID":"mi-008d36be46EXAMPLE","Region":"us-east-2"}

Status      : Running
Name        : AmazonSSMAgent
DisplayName : Amazon SSM Agent
```

これで、マシンはマネージドノードになりました。これらのマネージドノードは、「mi-」というプレフィックスで識別されます。Fleet Manager の [マネージドノード] ページにマネージドノードを表示するには、AWS CLI コマンド describe-instance-information、または API コマンド DescribeInstanceInformation を使用します。

プライベートキーの自動ローテーションを設定する

セキュリティポスチャを強化するには、AWS Systems Manager エージェント (SSM Agent) を設定して、ハイブリッドまたはマルチクラウド環境用のプライベートキーを自動的にローテーションさせます。SSM Agent バージョン 3.0.1031.0 以降を使用すると、この機能にアクセスできます。次の手順に従ってこの機能を有効にします。

ハイブリッドおよびマルチクラウド環境のプライベートキーをローテーションするように SSM Agent を設定するには

1. Linux マシンでは `/etc/amazon/ssm/`、Windows Server マシンでは `C:\Program Files\Amazon\SSM` に移動します。
2. `amazon-ssm-agent.json.template` の内容を `amazon-ssm-agent.json` という名前の新ファイルにコピーします。`amazon-ssm-agent.json.template` と同じディレクトリに `amazon-ssm-agent.json` を保存します。
3. `Profile`、`KeyAutoRotateDays` を探す プライベートキーの自動ローテーション間隔の日数を入力します。
4. SSM Agent を再起動します。

設定を変更するたびに、SSM Agent を再起動します。

同じ手順を使用して、SSM Agent の他の機能をカスタマイズできます。使用可能な設定プロパティとそのデフォルト値の最新リストについては、「Config Property Definitions (設定プロパティの定義)」を参照してください。

マネージドノードの登録解除と再登録 (Windows Server)

マネージドノードの登録を解除するには、AWS CLI または Tools for Windows PowerShell のいずれかから DeregisterManagedInstance API オペレーションを呼び出します。以下に CLI コマンドの例を示します。

```
aws ssm deregister-managed-instance --instance-id "mi-1234567890"
```

エージェントの残りの登録情報を削除するには、`amazon-ssm-agent.json` ファイル内の `IdentityConsumptionOrder` キーを削除します。次に、以下のコマンドを実行します。

```
amazon-ssm-agent -register -clear
```

Windows Server ハイブリッドマシンでマネージドノードを再登録するには

マシンは、登録解除した後に再登録できます。ただし、マシンを登録するために以前使用したものとは異なる、アクティベーションコードとアクティベーション ID を使用する必要があります。

1. マシンへ接続します。
2. 以下のコマンドを実行してください。必ずプレースホルダー値の代わりに、ハイブリッドのアクティベーションの作成時に生成されたアクティベーションコードとアクティベーション ID、および SSM Agent のダウンロード元のリージョンの識別子を入力します。

```
'yes' | & Start-Process ./ssm-setup-cli.exe -ArgumentList @("-register", "-
activation-code=$code", "-activation-id=$id", "-region=$region") -Wait
Get-Content ($env:ProgramData + "\Amazon\SSM\InstanceData\registration")
Get-Service -Name "AmazonSSMAgent"
```

Systems Manager を利用したエッジデバイスの管理

このセクションでは、アカウント管理者とシステム管理者が AWS IoT Greengrass コアデバイスの設定と管理を有効にするために実行する設定タスクについて説明します。これらのタスクを完了すると、AWS アカウント 管理者によって権限が付与されたユーザーは AWS Systems Manager を使って組織の AWS IoT Greengrass コアデバイスを設定と管理することができます。

> **Note**
>
> - AWS IoT Greengrass 用の SSM Agent は macOS と Windows 10 にサポートされていません。Systems Manager のツールを使用して、これらのオペレーティングシステムを使用するエッジデバイスの管理と設定を行うことはできません。
> - Systems Manager は、AWS IoT Greengrass コアデバイスとして設定されていないエッジデバイスもサポートしています。Systems Manager を使用して AWS IoT コアデバイスおよび非 AWS エッジデバイスを管理する場合、ハイブリッドアクティベーションを使用して設定する必要があります。詳細については、「Systems Manager を利用したハイブリッド環境およびマルチクラウド環境でのノードの管理」を参照してください。
> - Session Manager と Microsoft アプリケーションパッチをエッジデバイスと使用する場合、アドバンストインスタンス層を有効にする必要があります。詳細については、「アドバンストインスタンス層を有効にするには」を参照してください。

[開始する前に]

エッジデバイスが以下の要件を満たしていることを確認します。

- エッジデバイスを AWS IoT Greengrass コアデバイスとして設定する場合、要件を満たしている必要があります。詳細については、AWS IoT Greengrass Version 2 デベロッパーガイドの「AWS IoT Greengrass コアデバイスの設定」を参照してください。
- エッジデバイスは AWS Systems Manager エージェント (SSM Agent) と互換性がなければなりません。詳細については、「System Manager でサポートされているオペレーティングシステム」を参照してください。
- エッジデバイスはクラウド内の Systems Manager サービスと通信できる必要があります。Systems Manager は切断されたエッジデバイスをサポートしていません。

エッジデバイスのセットアップについて

Systems Manager 用に AWS IoT Greengrass デバイスの設定には以下のプロセスが含まれます。

> **Note**
>
> エッジデバイスからの SSM Agent のアンインストールの詳細については、AWS IoT Greengrass Version 2 デベロッパーガイドの「Uninstall the AWS Systems Manager Agent」を参照してください。

エッジデバイス用の IAM サービスロールを作成

AWS IoT Greengrass コアデバイスは AWS Systems Manager と通信するため、AWS Identity and Access Management (IAM) サービスロールが必要となります。ロールは、Systems Manager サービスに AWS Security Token Service (AWS STS) AssumeRole の信頼を付与します。サービスロールの作成は AWS アカウント ごとに一度のみ行う必要があります。AWS IoT Greengrass デバイスに SSM Agent のコンポーネントを設定と展開する際、このロールは `RegistrationRole` のパラメータに指定します。ハイブリッドおよびマルチクラウド環境用に非 EC2 ノードをセットアップするときにこのロールを既に作成している場合は、この手順をスキップできます。

> **Note**
>
> エッジデバイスで Systems Manager を社内または組織内で使用するユーザーは、Systems Manager API を呼び出すために IAM で許可を付与する必要があります。

S3 バケットのポリシーの要件

次のいずれかのケースに当てはまる場合は、この手順を実行する前に Amazon Simple Storage Service (Amazon S3) バケット用のカスタム IAM アクセス許可ポリシーを作成する必要があります。

- ケース 1: VPC エンドポイントを使用して、サポートされている AWS のサービス、および AWS PrivateLink を搭載した VPC エンドポイントサービスに VPC をプライベート接続しています。
- ケース 2: Systems Manager オペレーションの一環として作成した S3 バケットを使用します (例: Run Command コマンドまたは、Session Manager セッションの出力を S3 バケットに保存)。先に進む前に、「インスタンスプロファイル用のカスタム S3 バケットポリシーを作成する」の手順に従います。そのトピックの S3 バケットポリシーに関する情報は、サービスロールにも適用されます。

> **Note**
>
> デバイスがファイアウォールで保護され、かつ Patch Manager を使用する場合、ファイアウォールはパッチベースラインのエンドポイント `arn:aws:s3:::patch-baseline-snapshot-region/*` へアクセスを許可する必要があります。
> *region* は、米国東部 (オハイオ) リージョンの `us-east-2` のように、AWS Systems Manager でサポートされている AWS リージョン の識別子を表します。サポートされている *region* 値の一覧については、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」にある Region 列を参照してください。

AWS CLI

AWS IoT Greengrass 環境用 (AWS CLI) に IAM サービスロールを作成する方法

1. まだ AWS Command Line Interface (AWS CLI) をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」を参照してください。

2. ローカルマシンで以下の信頼ポリシーを使用して、`SSMService-Trust.json` のような名前でテキストファイルを作成します。ファイル保存時に、必ずファイル拡張子 (`.json`) を付けます。

   > **Note**
   >
   > 名前をメモします。SSM Agent を AWS IoT Greengrass コアデバイスに展開する際にそれを指定します。

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Principal": {
            "Service": "ssm.amazonaws.com"
        },
        "Action": "sts:AssumeRole"
```

```
    }
}
```

3. AWS CLI を開き、JSON ファイルを作成したディレクトリで create-role コマンドを実行してサービスロールを作成します。各##############をユーザー自身の情報に置き換えます。

   Linux と macOS

   ```
   aws iam create-role \
       --role-name SSMServiceRole \
       --assume-role-policy-document file://SSMService-Trust.json
   ```

   Windows

   ```
   aws iam create-role ^
       --role-name SSMServiceRole ^
       --assume-role-policy-document file://SSMService-Trust.json
   ```

4. 以下のように attach-role-policy を実行して、先ほど作成したサービスロールでセッショントークンを作成できるようにします。セッショントークンは、Systems Manager を使用してコマンドを実行するため、エッジデバイスに許可を付与します。

   > **Note**
   >
   > エッジデバイスに対してサービスプロファイル用に追加するポリシーは、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのインスタンスプロファイルの作成に使用されるものと同じポリシーです。次のコマンドで使用する IAM ポリシーの詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」を参照してください。

   (必須) 以下のコマンドを実行して、エッジデバイスが AWS Systems Manager サービスの主要機能を使用できるようにします。

   Linux と macOS

   ```
   aws iam attach-role-policy \
       --role-name SSMServiceRole \
   ```

```
    --policy-arn arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore
```

Windows

```
aws iam attach-role-policy ^
    --role-name SSMServiceRole ^
    --policy-arn arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore
```

サービスロールのカスタム S3 バケットポリシーを作成した場合は、次のコマンドを実行して、ポリシーで指定したバケットに AWS Systems Manager Agent (SSM Agent) がアクセスできるようにします。*account_ID* と *my_bucket_policy_name* をユーザーの AWS アカウント ID とバケット名に置き換えます。

Linux と macOS

```
aws iam attach-role-policy \
    --role-name SSMServiceRole \
    --policy-arn arn:aws:iam::account_ID:policy/my_bucket_policy_name
```

Windows

```
aws iam attach-role-policy ^
    --role-name SSMServiceRole ^
    --policy-arn arn:aws:iam::account_id:policy/my_bucket_policy_name
```

(選択可) 以下のコマンドを実行して、エッジデバイスからドメインの統合するリクエストのため、ユーザーに代わって SSM Agent が AWS Directory Service にアクセスできるようにします。エッジデバイスを Microsoft AD ディレクトリに統合する場合のみ、サービスロールはこのポリシーが必要です。

Linux と macOS

```
aws iam attach-role-policy \
    --role-name SSMServiceRole \
    --policy-arn arn:aws:iam::aws:policy/AmazonSSMDirectoryServiceAccess
```

Windows

```
aws iam attach-role-policy ^
```

```
    --role-name SSMServiceRole ^
    --policy-arn arn:aws:iam::aws:policy/AmazonSSMDirectoryServiceAccess
```

(選択可) 以下のコマンドを実行して、CloudWatch エージェントがエッジデバイスの実行できるようにします。このコマンドはデバイスの情報を読み込んでCloudWatch に書き込むことを可能にします。サービスロールは、Amazon EventBridge や Amazon CloudWatch Logs などのサービスを利用する場合にのみ、このポリシーが必要です。

```
aws iam attach-role-policy \
    --role-name SSMServiceRole \
    --policy-arn arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy
```

Tools for PowerShell

AWS IoT Greengrass 環境用 (AWS Tools for Windows PowerShell) に IAM サービスロールを作成する方法

1. AWS Tools for PowerShell (Tools for Windows PowerShell) をインストールして設定します (まだインストールしていない場合)。

   詳細については、「AWS Tools for PowerShell のインストール」を参照してください。

2. ローカルマシンで以下の信頼ポリシーを使用して、SSMService-Trust.json のような名前でテキストファイルを作成します。ファイル保存時に、必ずファイル拡張子 (.json) を付けます。

   > **Note**
   >
   > 名前をメモします。SSM Agent を AWS IoT Greengrass コアデバイスに展開する際にそれを指定します。

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Principal": {
            "Service": "ssm.amazonaws.com"
        },
```

```
        "Action": "sts:AssumeRole"
    }
}
```

3. PowerShell を管理モードで開き、JSON ファイルを作成したディレクトリで以下のように New-IAMRole を実行してサービスロールを作成します。

```
New-IAMRole `
    -RoleName SSMServiceRole `
    -AssumeRolePolicyDocument (Get-Content -raw SSMService-Trust.json)
```

4. 以下のように、Register-IAMRolePolicy を使用して、作成したサービスロールでセッショントークンを作成できます。セッショントークンは、Systems Manager を使用してコマンドを実行するため、エッジデバイスに許可を付与します。

> **Note**
>
> AWS IoT Greengrass 環境内でエッジデバイスに対してサービスロール用に追加するポリシーは、EC2 インスタンスのインスタンスプロファイルの作成に使用されるものと同じポリシーです。以下のコマンドで使用する AWS ポリシーの詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」を参照してください。

(必須) 以下のコマンドを実行して、エッジデバイスが AWS Systems Manager サービスの主要機能を使用できるようにします。

```
Register-IAMRolePolicy `
    -RoleName SSMServiceRole `
    -PolicyArn arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore
```

サービスロールのカスタム S3 バケットポリシーを作成した場合は、次のコマンドを実行し、ポリシーで指定したバケットに SSM Agent がアクセスできるようにします。*account_ID* と *my_bucket_policy_name* をユーザーの AWS アカウント ID とバケット名に置き換えます。

```
Register-IAMRolePolicy `
    -RoleName SSMServiceRole `
    -PolicyArn arn:aws:iam::account_ID:policy/my_bucket_policy_name
```

(選択可) 以下のコマンドを実行して、エッジデバイスからドメインの統合するリクエストのため、ユーザーに代わって SSM Agent が AWS Directory Service にアクセスできるようにします。エッジデバイスを Microsoft AD ディレクトリに統合する場合のみ、サービスロールはこのポリシーが必要です。

```
Register-IAMRolePolicy `
    -RoleName SSMServiceRole `
    -PolicyArn arn:aws:iam::aws:policy/AmazonSSMDirectoryServiceAccess
```

(選択可) 以下のコマンドを実行して、CloudWatch エージェントがエッジデバイスの実行できるようにします。このコマンドはデバイスの情報を読み込んでCloudWatch に書き込むことを可能にします。サービスロールは、Amazon EventBridge や Amazon CloudWatch Logs などのサービスを利用する場合にのみ、このポリシーが必要です。

```
Register-IAMRolePolicy `
    -RoleName SSMServiceRole `
    -PolicyArn arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy
```

AWS IoT Greengrass のためにエッジデバイスを設定する

エッジデバイスを AWS IoT Greengrass コアデバイスとしてセットアップします。セットアッププロセスは、サポートされたオペレーティングシステムとシステム要件の確認、並びにデバイス上に AWS IoT Greengrass コアソフトウェアのインストールと設定が含まれます。詳細については、AWS IoT Greengrass Version 2 デベロッパーガイドの「AWS IoT Greengrass コアデバイスの設定」を参照してください。

AWS IoT Greengrass トークン交換ロールを更新して SSM Agent をエッジデバイスにインストールします。

Systems Manager用の AWS IoT Greengrass コアデバイスのセットアップと設定における最終ステップでは、AWS IoT Greengrass AWS Identity and Access Management (IAM) デバイスサービスロール (トークン交換ロール) と AWS Systems Manager エージェント (SSM Agent) を AWS IoT Greengrass デバイスにデプロイする必要があります。これらのプロセスの詳細については、AWS IoT Greengrass Version 2 デベロッパーガイドの「AWS Systems Manager エージェントのインストール」を参照してください。

デバイスに SSM Agent を展開したら、AWS IoT Greengrass はデバイスを自動的に Systems Manager に登録します。追加登録は必要ありません。Systems Manager のツールを使って、AWS IoT Greengrass デバイスへのアクセスやその管理、設定を行うことができます。

> **Note**
>
> エッジデバイスはクラウド内の Systems Manager サービスと通信できる必要があります。Systems Manager は切断されたエッジデバイスをサポートしていません。

Systems Manager 用の AWS Organizations 委任された管理者の作成

AWS Organizations で組織をセットアップする際には、すべての AWS のサービス に対してすべての管理タスクを実行する管理アカウントを割り当てます。管理アカウントユーザーは、Systems Manager が Change Manager、Explorer、および OpsCenter の管理タスクを実行するための委任管理者アカウントのみを割り当てることができます。AWS Organizations は、組織を作成し、これらの AWS アカウント を一元管理するために割り当てるために使用できるアカウント管理サービスです。AWS Organizations の詳細については、「AWS Organizations ユーザーガイド」の「AWS Organizations」を参照してください。

AWS Systems Manager のツールである Change Manager、Explorer、および OpsCenter を AWS Organizations と連携させて、組織のすべてのメンバーアカウントでタスクを実行できます。Systems Manager のすべてのツールに対して、委任管理者を 1 人だけ割り当てることができます。委任管理者アカウントは、割当先の組織のメンバーである必要があります。

トピック

- Change Manager での委任された管理者の使用
- Explorer での委任された管理者の使用
- OpsCenter での委任された管理者の使用
- Quick Setup での委任された管理者の使用

Change Manager での委任された管理者の使用

Change Manager は、アプリケーションの設定やインフラストラクチャに対する運用上の変更を要求、承認、実装、レポート作成するためのエンタープライズ変更管理フレームワークです。

組織全体で Change Manager を使用する場合は、委任管理者アカウントを割り当てて、すべてのメンバーアカウントの変更テンプレート、承認、およびレポートを管理します。Quick Setup の使用により、組織での使用向けに Change Manager をセットアップして委任された管理者アカウントを選することができます。Change Manager を単一の AWS アカウント のみで使用する場合、委任管理者アカウントは必要ありません。

デフォルトでは、Change Manager には委任管理者アカウントのすべての変更関連タスクが表示されます。組織の Change Manager をセットアップする時に委任管理者を設定する手順については、「組織の Change Manager の設定 (管理アカウント)」を参照してください。

> **Important**
>
> 組織全体で Change Manager を使用する場合は、常に委任管理者アカウントから変更を行うことをお勧めします。組織内の他のアカウントから変更を行うことはできますが、それらの変更は、委任管理者アカウントで報告されず、表示することもできません。

Explorer での委任された管理者の使用

Explorer はカスタマイズ可能なオペレーションダッシュボードであり、AWS リージョン 全体の AWS アカウント のオペレーションデータ (OpsData) の集約ビューをレポートします。

Systems Manager の委任管理者アカウントを設定して、AWS Organizations とのリソースデータ同期を使用して、複数のリージョンとアカウントから Explorer データを集約できます。委任管理者は、AWS Management Console、AWS Command Line Interface (AWS CLI)、または AWS Tools for Windows PowerShell を使用し Explorer データを検索、フィルタリング、および集約できます。

Explorer 用に委任管理者アカウントを使用する場合、各 AWS アカウント へマルチアカウントおよびリージョンのリソースデータの同期を作成または削除できる管理者の数を制限します。

Explorer を使用することにより、組織内のすべての AWS アカウント 間でオペレーションデータを同期できます。Explorer から委任管理者を割り当てる方法については、「Explorer のための委任された管理者の設定」を参照してください。

OpsCenter での委任された管理者の使用

OpsCenter は、オペレーションエンジニアや IT プロフェッショナルは AWS リソースに関連する運用上の作業項目 (OpsItems) の表示、調査、解決を一元管理できます。OpsCenter を使用して複数の

アカウント間で OpsItems を一元管理する場合は、AWS Organizations で組織をセットアップする必要があります。

OpsCenter の Quick Setup を使用すると、委任された管理者アカウントを割り当て、OpsItems を一元管理するように OpsCenter を設定できます。詳細については、「(オプション) Quick Setup を使用して、複数のアカウント間で OpsItems を管理するように OpsCenter を設定」を参照してください。

Quick Setup での委任された管理者の使用

Quick Setup は Systems Manager のツールであり、推奨されるベストプラクティスに従って、よく使用する AWS サービスと機能をすばやく設定できます。Quick Setup 用に委任管理者アカウントを設定することで、AWS Organizations を使用してアカウントとリージョン全体にわたって設定をデプロイおよび管理できます。Quick Setup の委任管理者は、組織の設定マネージャーリソースを作成、更新、表示、および削除できます。Systems Manager は、統合コンソールエクスペリエンスのセットアッププロセスの一環として Quick Setup の委任管理者を登録します。詳細については、「組織用の Systems Manager 統合コンソールのセットアップ」を参照してください。

AWS Systems Manager の一般的なセットアップ

まだ作成していない場合は、AWS アカウント にサインアップして管理者ユーザーを作成します。

AWS アカウントへのサインアップ

AWS アカウント がない場合は、以下のステップを実行して作成します。

AWS アカウントにサインアップするには

1. https://portal.aws.amazon.com/billing/signup を開きます。
2. オンラインの手順に従います。

   サインアップ手順の一環として、通話呼び出しを受け取り、電話キーパッドで検証コードを入力するように求められます。

   AWS アカウント にサインアップすると、AWS アカウントのルートユーザー が作成されます。ルートユーザーには、アカウントのすべての AWS のサービスとリソースへのアクセス権があります。セキュリティのベストプラクティスとして、ユーザーに管理アクセスを割り当て、ルートユーザーのみを使用してルートユーザーアクセスが必要なタスクを実行してください。

サインアップ処理が完了すると、AWS からユーザーに確認メールが送信されます。https://aws.amazon.com/ の [マイアカウント] をクリックして、いつでもアカウントの現在のアクティビティを表示し、アカウントを管理することができます。

管理アクセスを持つユーザーを作成する

AWS アカウント にサインアップしたら、AWS アカウントのルートユーザー をセキュリティで保護し、AWS IAM Identity Center を有効にして、管理ユーザーを作成します。これにより、日常的なタスクにルートユーザーを使用しないようにします。

AWS アカウントのルートユーザーをセキュリティで保護する

1. [ルートユーザー] を選択し、AWS アカウント のメールアドレスを入力して、アカウント所有者として AWS Management Console にサインインします。次のページでパスワードを入力します。

   ルートユーザーを使用してサインインする方法については、AWS サインイン ユーザーガイドのルートユーザーとしてサインインするを参照してください。
2. ルートユーザーの多要素認証 (MFA) を有効にします。

   手順については、「IAM ユーザーガイド」で AWS アカウントのルートユーザーの仮想 MFA デバイスを有効にする方法 (コンソール) を確認してください。

管理アクセスを持つユーザーを作成する

1. IAM アイデンティティセンターを有効にします。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「AWS IAM Identity Center の有効化」を参照してください。
2. IAM アイデンティティセンターで、ユーザーに管理アクセスを付与します。

   IAM アイデンティティセンターディレクトリ をアイデンティティソースとして使用するチュートリアルについては、「AWS IAM Identity Center ユーザーガイド」の「 Configure user access with the default IAM アイデンティティセンターディレクトリ」を参照してください。

管理アクセス権を持つユーザーとしてサインインする

- IAM アイデンティティセンターのユーザーとしてサインインするには、IAM アイデンティティセンターのユーザーの作成時に E メールアドレスに送信されたサインイン URL を使用します。

IAM アイデンティティセンターユーザーを使用してサインインする方法については、「AWS サインイン User Guide」の「Signing in to the AWS access portal」を参照してください。

追加のユーザーにアクセス権を割り当てる

1. IAM アイデンティティセンターで、最小特権のアクセス許可を適用するというベストプラクティスに従ったアクセス許可セットを作成します。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」を参照してください。
2. グループにユーザーを割り当て、そのグループにシングルサインオンアクセス権を割り当てます。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「グループの結合」を参照してください。

AWS Systems Manager を設定する

以下のトピックでは、AWS Organizations 組織またはシングル AWS アカウントのために統一された AWS Systems Manager コンソールをセットアップする方法について説明します。

トピック

- Systems Manager コンソールアクセスのセットアップ
- 組織用の Systems Manager 統合コンソールのセットアップ
- 単一のアカウントとリージョン用の Systems Manager 統合コンソールのセットアップ
- Systems Manager 統合コンソールの無効化

Systems Manager コンソールアクセスのセットアップ

AWS Management Consoleで AWS Systems Manager を使用するには、適切なアクセス許可が設定されている必要があります。

AWS Identity and Access Management ポリシーを作成して IAM ID にアタッチする方法の詳細については、「IAM ユーザーガイド」の「Create IAM policies」を参照してください。

Systems Manager オンボーディングポリシー

以下の例に示すような IAM ポリシーを作成して、IAM ID にアタッチできます。このポリシーは、Systems Manager をオンボーディングおよび設定するためのフルアクセスを許可します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `ssm-quicksetup` – プリンシパルがすべての AWS Systems Manager Quick Setup アクションにアクセスすることを許可します。
- `ssm` – プリンシパルが Systems Manager Automation と Resource Explorer にアクセスすることを許可します。
- `organizations` – プリンシパルが AWS Organizations で組織の構造を読み取り、組織として Systems Manager にオンボーディングするときに委任管理者を管理することを許可します。
- `cloudformation` – プリンシパルが Quick Setup スタックを管理することを許可します。

- iam – プリンシパルが Systems Manager のオンボーディングに必要な IAM ロールとポリシーを管理することを許可します。

```
{
   "Version": "2012-10-17",
   "Statement": [
     {
       "Sid": "QuickSetupActions",
       "Effect": "Allow",
       "Action": [
         "ssm-quicksetup:*"
       ],
       "Resource": "*"
     },

     {
       "Sid": "SsmReadOnly",
       "Effect": "Allow",
       "Action": [
         "ssm:DescribeAutomationExecutions",
         "ssm:GetAutomationExecution",
         "ssm:ListAssociations",
         "ssm:DescribeAssociation",
         "ssm:ListDocuments",
         "ssm:ListResourceDataSync",
         "ssm:DescribePatchBaselines",
         "ssm:GetPatchBaseline",
         "ssm:DescribeMaintenanceWindows",
         "ssm:DescribeMaintenanceWindowTasks"
       ],
       "Resource": "*"
     },
     {
       "Sid": "SsmDocument",
       "Effect": "Allow",
       "Action": [
         "ssm:GetDocument",
         "ssm:DescribeDocument"
       ],
       "Resource": [
         "arn:aws:ssm:*:*:document/AWSQuickSetupType-*",
         "arn:aws:ssm:*:*:document/AWS-EnableExplorer"
```

```
        ]
      },
      {
        "Sid": "SsmEnableExplorer",
        "Effect": "Allow",
        "Action": "ssm:StartAutomationExecution",
        "Resource": "arn:aws:ssm:*:*:automation-definition/AWS-EnableExplorer:*"
      },
      {
        "Sid": "SsmExplorerRds",
        "Effect": "Allow",
        "Action": [
          "ssm:GetOpsSummary",
          "ssm:CreateResourceDataSync",
          "ssm:UpdateResourceDataSync"
        ],
        "Resource": "arn:aws:ssm:*:*:resource-data-sync/AWS-QuickSetup-*"
      },
      {
        "Sid": "OrgsReadOnly",
        "Effect": "Allow",
        "Action": [
          "organizations:DescribeAccount",
          "organizations:DescribeOrganization",
          "organizations:ListDelegatedAdministrators",
          "organizations:ListRoots",
          "organizations:ListParents",
          "organizations:ListOrganizationalUnitsForParent",
          "organizations:DescribeOrganizationalUnit",
          "organizations:ListAWSServiceAccessForOrganization"
        ],
        "Resource": "*"
      },
      {
        "Sid": "OrgsAdministration",
        "Effect": "Allow",
        "Action": [
          "organizations:EnableAWSServiceAccess",
          "organizations:RegisterDelegatedAdministrator",
          "organizations:DeregisterDelegatedAdministrator"
        ],
        "Resource": "*",
        "Condition": {
          "StringEquals": {
```

```
            "organizations:ServicePrincipal": [
              "ssm.amazonaws.com",
              "ssm-quicksetup.amazonaws.com",
              "member.org.stacksets.cloudformation.amazonaws.com",
              "resource-explorer-2.amazonaws.com"
            ]
          }
        }
      },
      {
        "Sid": "CfnReadOnly",
        "Effect": "Allow",
        "Action": [
          "cloudformation:ListStacks",
          "cloudformation:DescribeStacks",
          "cloudformation:ListStackSets",
          "cloudformation:DescribeOrganizationsAccess"
        ],
        "Resource": "*"
      },
      {
        "Sid": "OrgCfnAccess",
        "Effect": "Allow",
        "Action": [
          "cloudformation:ActivateOrganizationsAccess"
        ],
        "Resource": "*"
      },
      {
        "Sid": "CfnStackActions",
        "Effect": "Allow",
        "Action": [
          "cloudformation:CreateStack",
          "cloudformation:DeleteStack",
          "cloudformation:DescribeStackResources",
          "cloudformation:DescribeStackEvents",
          "cloudformation:GetTemplate",
          "cloudformation:RollbackStack",
          "cloudformation:TagResource",
          "cloudformation:UntagResource",
          "cloudformation:UpdateStack"
        ],
        "Resource": [
          "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-*",
```

```
        "arn:aws:cloudformation:*:*:stack/AWS-QuickSetup-*",
        "arn:aws:cloudformation:*:*:type/resource/*"
      ]
    },
    {
      "Sid": "CfnStackSetActions",
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStackInstances",
        "cloudformation:CreateStackSet",
        "cloudformation:DeleteStackInstances",
        "cloudformation:DeleteStackSet",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DetectStackSetDrift",
        "cloudformation:ListStackInstanceResourceDrifts",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults",
        "cloudformation:TagResource",
        "cloudformation:UntagResource",
        "cloudformation:UpdateStackSet"
      ],
      "Resource": [
        "arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-*",
        "arn:aws:cloudformation:*:*:type/resource/*",
        "arn:aws:cloudformation:*:*:stackset-target/AWS-QuickSetup-*:*"
      ]
    },
    {
      "Sid": "ValidationReadonlyActions",
      "Effect": "Allow",
      "Action": [
        "iam:ListRoles",
        "iam:GetRole"
      ],
      "Resource": "*"
    },
    {
      "Sid": "IamRolesMgmt",
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
```

```
        "iam:DeleteRole",
        "iam:GetRole",
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy",
        "iam:GetRolePolicy",
        "iam:ListRolePolicies"
      ],
      "Resource": [
        "arn:aws:iam::*:role/AWS-QuickSetup-*",
        "arn:aws:iam::*:role/service-role/AWS-QuickSetup-*"
      ]
    },
    {
      "Sid": "IamPassRole",
      "Effect": "Allow",
      "Action": [
        "iam:PassRole"
      ],
      "Resource": [
        "arn:aws:iam::*:role/AWS-QuickSetup-*",
        "arn:aws:iam::*:role/service-role/AWS-QuickSetup-*"
      ],
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": [
            "ssm.amazonaws.com",
            "ssm-quicksetup.amazonaws.com",
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "IamRolesPoliciesMgmt",
      "Effect": "Allow",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
      ],
      "Resource": [
        "arn:aws:iam::*:role/AWS-QuickSetup-*",
        "arn:aws:iam::*:role/service-role/AWS-QuickSetup-*"
      ],
      "Condition": {
```

```
          "ArnEquals": {
            "iam:PolicyARN": [
              "arn:aws:iam::aws:policy/AWSSystemsManagerEnableExplorerExecutionPolicy",
              "arn:aws:iam::aws:policy/AWSQuickSetupSSMDeploymentRolePolicy"
            ]
          }
        }
      },
      {
        "Sid": "CfnStackSetsSLR",
        "Effect": "Allow",
        "Action": [
          "iam:CreateServiceLinkedRole"
        ],
        "Resource": [
          "arn:aws:iam::*:role/aws-service-role/stacksets.cloudformation.amazonaws.com/
AWSServiceRoleForCloudFormationStackSetsOrgAdmin",
          "arn:aws:iam::*:role/aws-service-role/ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM",
          "arn:aws:iam::*:role/aws-service-role/accountdiscovery.ssm.amazonaws.com/
AWSServiceRoleForAmazonSSM_AccountDiscovery",
          "arn:aws:iam::*:role/aws-service-role/ssm-quicksetup.amazonaws.com/
AWSServiceRoleForSSMQuickSetup",
          "arn:aws:iam::*:role/aws-service-role/resource-explorer-2.amazonaws.com/
AWSServiceRoleForResourceExplorer"
        ]
      }
    ]
 }
```

AWS Systems Manager コンソールオペレーターのポリシー

以下の例に示すような IAM ポリシーを作成して、IAM ID にアタッチできます。このポリシーは、Systems Manager を運用するためのフルアクセスを許可し、診断と修復のために Automation ドキュメントを実行することを Systems Manager に許可します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `ssm` – プリンシパルがすべての Systems Manager API にアクセスすることを許可します。
- `ssm-quicksetup` – プリンシパルが自身の Quick Setup 設定を管理することを許可します。

- ec2 – 有効になっている AWS リージョンと Amazon EC2 インスタンスのステータスを判断することを Systems Manager に許可します。
- cloudformation – プリンシパルが自身の Quick Setup スタックを読み取ることを許可します。
- organizations – プリンシパルが AWS Organizations で組織の構造を読み取り、組織として Systems Manager にオンボーディングするときに委任管理者を管理することを許可します。
- s3 – プリンシパルが Systems Manager のオンボーディングプロセス時に作成された Amazon S3 バケット内のオブジェクトを診断のためにリストおよび取得することを許可します。
- iam:PassRole – プリンシパルが Automation を実行してアンマネージドノードの診断と修復を行うときに、引き受けられるロールを Systems Manager に渡すことを許可します。
- iam:GetRole – プリンシパルが Systems Manager での作業時に Quick Setup ロールの特定のロール情報を取得することを許可します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:*",
        "ssm-quicksetup:*"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowEC2DescribeActions",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CfnAccess",
      "Effect": "Allow",
      "Action": [
        "cloudformation:ListStacks",
        "cloudformation:ListStackSets",
```

```
        "cloudformation:ListStackInstances",
        "cloudformation:ListStackSetOperations",
        "cloudformation:ListStackSetOperationResults",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackSet",
        "cloudformation:DescribeStackSetOperation",
        "cloudformation:DescribeOrganizationsAccess",
        "cloudformation:DescribeStackInstance",
        "cloudformation:DetectStackSetDrift",
        "cloudformation:ListStackInstanceResourceDrifts"
      ],
      "Resource": "*"
    },
    {
      "Sid": "OrgsReadOnly",
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListRoots",
        "organizations:ListParents",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowKMSOperations",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "arn:aws:kms:*:*:key/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/SystemsManagerManaged": "true"
        },
        "ArnLike": {
          "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::do-not-delete-ssm-
diagnosis-*"
        },
```

```
        "StringLike": {
          "kms:ViaService": "s3.*.amazonaws.com"
        },
        "Bool": {
          "aws:ViaAWSService": "true"
        }
      }
    },
    {
      "Sid": "AllowReadS3BucketFromOrganization",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": "arn:aws:s3:::do-not-delete-ssm-diagnosis*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceOrgId": "${aws:PrincipalOrgId}"
        }
      }
    },
    {
      "Sid": "AllowReadS3BucketFromSingleAccount",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": "arn:aws:s3:::do-not-delete-ssm-diagnosis*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": [
        "arn:aws:iam::*:role/AWS-SSM-DiagnosisAdminRole*",
        "arn:aws:iam::*:role/AWS-SSM-DiagnosisExecutionRole*",
        "arn:aws:iam::*:role/AWS-SSM-RemediationAdminRole*",
        "arn:aws:iam::*:role/AWS-SSM-RemediationExecutionRole*"
```

```
      ],
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "ssm.amazonaws.com"
        }
      }
    },
    {
      "Sid": "IamReadOnly",
      "Effect": "Allow",
      "Action": "iam:GetRole",
      "Resource": [
        "arn:aws:iam::*:role/AWS-QuickSetup-*",
        "arn:aws:iam::*:role/service-role/AWS-QuickSetup-*"
      ]
    }
  ]
}
```

AWS Systems Manager コンソールオペレーターの読み取り専用ポリシー

以下の例に示すような IAM ポリシーを作成して、IAM ID にアタッチできます。この管理ポリシーは、Systems Manager を使用するための読み取り専用アクセスを許可します。

- `ssm` – プリンシパルが Systems Manager 読み取り専用 API にアクセスすることを許可します。
- `ssm-quicksetup` – プリンシパルが Quick Setup 設定を読み取ることを許可します。
- `cloudformation` – プリンシパルが自身の Quick Setup スタックを読み取ることを許可します。
- `iam:GetRole` – プリンシパルが Systems Manager の使用時に Quick Setup ロールの特定のロール情報を取得することを許可します。
- `ec2:DescribeRegions` – 有効になっている AWS リージョンを判断することを Systems Manager に許可します。
- `organizations` – プリンシパルが組織として Systems Manager にオンボーディングするときに AWS Organizations で組織の構造を読み取ることを許可します。
- `s3` – プリンシパルが Systems Manager のオンボーディングプロセス時に作成された Amazon S3 バケット内のオブジェクトをリストおよび取得することを許可します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:Describe*",
        "ssm:Get*",
        "ssm:List*",
        "ssm-quicksetup:List*",
        "ssm-quicksetup:Get*",
        "cloudformation:Describe*",
        "cloudformation:Get*",
        "cloudformation:List*",
        "iam:GetRole",
        "ec2:DescribeRegions",
        "organizations:Describe*",
        "organizations:List*"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowKMSOperations",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:*:*:key/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/SystemsManagerManaged": "true"
        },
        "ArnLike": {
          "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::do-not-delete-ssm-
diagnosis-*"
        },
        "StringLike": {
          "kms:ViaService": "s3.*.amazonaws.com"
        },
        "Bool": {
          "aws:ViaAWSService": "true"
        }
      }
```

```
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": "arn:aws:s3:::do-not-delete-ssm-diagnosis*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceOrgId": "${aws:PrincipalOrgId}"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": "arn:aws:s3:::do-not-delete-ssm-diagnosis*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

組織用の Systems Manager 統合コンソールのセットアップ

Systems Manager 統合コンソールエクスペリエンスのセットアッププロセスは、AWS Management Consoleから数回クリックするだけで完了します。AWS Organizations 組織用に Systems Manager をセットアップするには、組織の管理アカウントと、委任管理者として使用する組織内の別のアカウントにアクセスできる必要があります。管理アカウントへのアクセスが必要になるのは、Systems Manager を有効または無効にする場合だけです。ノードの管理には、委任管理者アカウントを使用します。

前提条件

Systems Manager は、組織全体にわたってノードを管理する場合、さまざまな依存サービスを使用して統合コンソールの機能をセットアップおよび強化します。このため、Systems Manager では信頼できるアクセスを有効にし、以下のサービス用に委任管理者アカウントを登録する必要があります。

- AWS CloudFormation – Systems Manager に必要なリソースをアカウントにデプロイします。
- AWS Resource Explorer – アカウント内の EC2 インスタンスを検索およびフィルタリングします。
- AWS Systems Manager Explorer – アカウント内の Systems Manager 用にデプロイされたリソースの正常性をモニタリングしてトラブルシューティングします。
- AWS Systems Manager Quick Setup – Systems Manager に必要な Quick Setup 設定をアカウントにデプロイします。

作業を開始する前に、こうした依存サービスに対して委任管理者のクォータをまだ超えていないことを確認してください。超えていた場合、Systems Manager を有効にするために必要な委任管理者アカウントを登録することはできません。組織用に Systems Manager を有効にすると、組織内のすべてのアカウントが対象になります。現時点では、セットアッププロセスからアカウントを除外するためのプロビジョニングはありません。Systems Manager を有効にするときに、どの AWS リージョンを含めるかを選択できます。Systems Manager 統合コンソールを現在サポートしているリージョンのみを選択できます。コンソールエクスペリエンスを利用できるリージョンの詳細については、「サポートされている AWS リージョン」を参照してください。

統合コンソールリソース

Systems Manager 統合コンソールのセットアッププロセスでは、多くの前提条件タスクが自動的に完了します。設定する機能によっては、デフォルトのホスト管理設定を有効にして必要な IAM アクセス許可をノードに付与するといったことが必要になります。以下は、統合コンソール用に Systems Manager によって作成されたリソースの詳細なリストです。設定する機能によっては、一部のリソースが作成されないことがあります。

AWS Resource Explorer マネージドビュー

- `AWSManagedViewForSSM` – Systems Manager が組織の Resource Explorer によってインデックス付けされたリソース情報にアクセスできるようにします。これらのマネージドビューは、Systems Manager のみが更新または削除できます。つまり、マネージドビューを削除した

り、Resource Explorer をオフにしたりする場合は、統合コンソールを無効にする必要があります。統合コンソールを無効にする方法の詳細については、「Systems Manager 統合コンソールの無効化」を参照してください。マネージドビューの詳細については、Resource Explorer ユーザーガイドの「AWS マネージドビュー」を参照してください。

> **Note**
>
> ホームリージョンとは異なるリージョンに Resource Explorer 用のアグリゲーターインデックスを作成した場合は、Systems Manager により現在のインデックスが降格します。その後、Systems Manager によりホームリージョン内のローカルインデックスが新しいアグリゲーターインデックスとして昇格します。それまでの間、ホームリージョンのノードのみが表示されます。このプロセスが完了するまで最大 24 時間かかる場合があります。

IAM ロール

- `RoleForOnboardingAutomation` – Systems Manager に、セットアッププロセス中にリソースを管理することを許可します。ポリシーの詳細については、「AWSQuickSetupSSMManageResourcesExecutionPolicy」を参照してください。
- `RoleForLifecycleManagement` – Lambda に、セットアッププロセスで作成されたリソースの、ライフサイクルの管理を許可します。ポリシーの詳細については、「AWSQuickSetupSSMLifecycleManagementExecutionPolicy」を参照してください。
- `RoleForAutomation` – Systems Manager Automation がランブックを実行するために引き受けるサービスロールです。詳細については、「コンソールを使用して Automation 用のサービスロールを作成する」を参照してください。
- `AWSSSMDiagnosisAdminRole` – 診断ランブックを使用するオートメーションを開始するときに使用する管理者ロールです。ポリシーの詳細については、「AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy」、「AWS-SSM-Automation-DiagnosisBucketPolicy」、「AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy」を参照してください。
- `AWSSSMDiagnosisExecutionRole` – 診断ランブック用のオートメーションの実行ロールです。ポリシーの詳細については、「AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy」と「AWS-SSM-Automation-DiagnosisBucketPolicy」を参照してください。
- `AWSSSMRemediationAdminRole` – 修復ランブックを使用するオートメーションを開始するときに使用する管理者ロールです。ポリシーの詳細については、「AWS-SSM-RemediationAutomation-AdministrationRolePolicy」、「AWS-SSM-

Automation-DiagnosisBucketPolicy」、「AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy」を参照してください。

- AWSSSMRemediationExecutionRole – 修復ランブック用のオートメーション実行ロールです。ポリシーの詳細については、「AWS-SSM-RemediationAutomation-ExecutionRolePolicy」と「AWS-SSM-Automation-DiagnosisBucketPolicy」を参照してください。
- ManagedInstanceCrossAccountManagementRole – Systems Manager に、アカウント間でマネージドノード情報を収集することを許可します。

State Manager 関連付け

- EnableDHMCAssociation – 毎日実行され、デフォルトのホスト管理設定が有効になっていることを確認します。
- SystemAssociationForEnablingExplorer – 毎日実行され、Explorer が有効になっていることを確認します。Explorer はマネージドノードから得られたデータの同期に使用されます。
- EnableAREXAssociation – 毎日実行され、AWS Resource Explorer が有効になっていることを確認します。Resource Explorer は、組織のどの Amazon EC2 インスタンスが Systems Manager によって管理されていないかを判断するために使用されます。
- SSMAgentUpdateAssociation – 14 日ごとに実行され、利用可能な最新バージョンの SSM Agent がマネージドノードにインストールされていることを確認します。
- SystemAssociationForInventoryCollection – 12 時間ごとに実行され、マネージドノードからインベントリデータを収集します。

S3 バケット

- DiagnosisBucket – 診断ランブックの実行により収集されたデータを保存します。

Lambda 関数

- SSMLifecycleOperatorLambda – プリンシパルがすべての AWS Systems Manager Quick Setup アクションにアクセスすることを許可します。
- SSMLifecycleResource – セットアッププロセスにより作成されたリソースの、ライフサイクルの管理に役立つカスタムリソースです。

また、セットアッププロセスが完了したら、[診断および修復] ノードタスクを選択して、Systems Manager の管理対象であると報告されていないノードに自動的に修正を適用できます。例え

ば、Systems Manager エンドポイントへのネットワーク接続などの問題を特定できます。詳細については、「診断と修復」を参照してください。

統合コンソールをセットアップする

組織用に Systems Manager をセットアップするには

1. 組織の管理アカウントにログインします。
2. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
3. 委任管理者として登録するアカウントの ID を入力します。
4. 委任管理者アカウントが正常に登録されたら、先ほど登録した委任管理者アカウントにログインし、Systems Manager コンソールに戻って Systems Manager のセットアップを終了します。
5. [Systems Manager を有効にする] を選択します。
6. [ホームリージョン] セクションで、Systems Manager が集約したノードデータの保存先となるリージョンを決定します。デフォルトでは、現在使用しているリージョンが Systems Manager によって選択されます。別のホームリージョンを選択するには、Systems Manager をセットアップする前に、使用するリージョンにコンソールを変更します。ノードデータが組織アカウントとリージョン全体にレプリケートされて、ホームリージョンに保存されます。Systems Manager のセットアップ後に、選択したリージョンを変更することはできません。別のリージョンを組織のホームリージョンとして使用するには、統合コンソールを無効にしてから再度セットアッププロセスを完了する必要があります。組織で IAM アイデンティティセンターを使用している場合は、IAM アイデンティティセンターをセットアップしたのと同じリージョンをホームリージョンとして選択する必要があります。
7. [リージョン] セクションで、Systems Manager を有効にするリージョンを選択します。
8. [機能の設定] セクションで、設定に対して有効にするオプションを選択します。

   デフォルトのホスト管理設定 (DHMC) を有効にする

   Systems Manager で DHMC を設定できるようにします。この機能により、Systems Manager は IAM ロールを使用して、アカウントとリージョン内のすべての Amazon EC2 インスタンスに Systems Manager で管理するために必要なアクセス許可を付与できるようになります。また、ドリフトの修復頻度を指定することもできます。設定のドリフトは、設定で行った選択と競合するサービスや機能に対し、ユーザーが変更を加えるたびに発生します。Systems Manager は、設定のドリフトがないかチェックし、もしあれば指定した頻度に基づいて修復を試みます。1～31 日の値を指定する必要があります。リージョンに DHMC を既に設定していても、以前に選択した IAM ロールが Systems Manager によって変更される

ことはありません。DHMC の詳細については、「Default Host Management Configuration を使用した EC2 インスタンスの自動管理」を参照してください。

DHMC により、AWS Identity and Access Management (IAM) インスタンスプロファイルを手動で作成しなくても Amazon EC2 インスタンスを管理できます。EC2 インスタンスに必要なアクセス許可を Systems Manager で管理できるように、このオプションを選択することをお勧めします。

インベントリメタデータの収集を有効にする

Systems Manager でノードから以下のタイプのメタデータを収集するように設定できます。

- AWS コンポーネント – EC2 ドライバー、エージェント、バージョンなど。
- アプリケーション – アプリケーション名、発行元、バージョンなど。
- ノードの詳細 – システム名、オペレーティングシステム (OS) 名、OS バージョン、最終起動、DNS、ドメイン、ワークグループ、OS アーキテクチャなど。
- ネットワーク設定 – IP アドレス、MAC アドレス、DNS、ゲートウェイ、サブネットマスクなど。
- サービス – 名前、表示名、ステータス、依存サービス、サービスタイプ、スタートタイプなど (Windows Server ノードのみ)。
- Windows ロール – 名前、表示名、パス、特徴タイプ、インストールされている状態など (Windows Server ノードのみ)。
- Windows 更新 – Hotfix ID、インストール者、インストール日など (Windows Server ノードのみ)。

インベントリを収集する頻度を指定します。1 ~ 744 時間の値を指定する必要があります。AWS Systems Manager のツールである Inventory の詳細については、「AWS Systems Manager インベントリ」を参照してください。

Systems Manager (SSM) エージェントの自動更新を有効にする

Systems Manager は、指定した頻度でエージェントの新しいバージョンをチェックできるようになります。頻度の値は 1 ~ 31 日で指定する必要があります。新しいバージョンがある場合、Systems Manager はのマネージドノード上エージェントを最新のリリースバージョンに自動的に更新します。Systems Manager は、エージェントがまだ存在しないインスタンスにエージェントをインストールしません。どの AMIs に SSM Agent がプリインストールされているかについては、「SSM Agent がプリインストールされている AMIs を見つける」を参照してください。

ノードが常に最新バージョンの SSM Agent を実行できるように、このオプションを選択することをお勧めします。エージェントを手動でインストールする方法など SSM Agent の詳細については、「「SSM Agent」 の使用」を参照してください。

9. [Submit] を選択してください。

組織の規模によっては、Systems Manager 統合コンソールエクスペリエンスをセットアップするまでに長い時間がかかる場合があります。

単一のアカウントとリージョン用の Systems Manager 統合コンソールのセットアップ

単一の AWS アカウントアカウントと AWS リージョンリージョン用に Systems Manager 統合コンソールエクスペリエンスをセットアップする場合、Organizations を使用したり、委任管理者アカウントを登録したりする必要はありません。Systems Manager コンソールエクスペリエンスのセットアッププロセスでは、自動的に多くの前提条件タスクが完了します。設定する機能によっては、デフォルトのホスト管理設定を有効にして必要な IAM アクセス許可をノードに付与するといったことが必要になります。以下は、統合コンソール用に Systems Manager によって作成されたリソースの詳細なリストです。

統合コンソールリソース

設定する機能によっては、一部のリソースが作成されないことがあります。

IAM ロール

- `RoleForOnboardingAutomation` – Systems Manager に、セットアッププロセス中にリソースを管理することを許可します。ポリシーの詳細については、「AWSQuickSetupSSMManageResourcesExecutionPolicy」を参照してください。
- `RoleForLifecycleManagement` – Lambda に、セットアッププロセスで作成されたリソースの、ライフサイクルの管理を許可します。ポリシーの詳細については、「AWSQuickSetupSSMLifecycleManagementExecutionPolicy」を参照してください。
- `RoleForAutomation` – Systems Manager Automation がランブックを実行するために引き受けるサービスロールです。詳細については、「コンソールを使用して Automation 用のサービスロールを作成する」を参照してください。
- `AWSSSMDiagnosisAdminRole` – 診断ランブック用のオートメーションの実行ロールです。ポリシーの詳細については、「AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy」、

「AWS-SSM-Automation-DiagnosisBucketPolicy」、「AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy」を参照してください。

- AWSSSMRemediationAdminRole – 修復ランブック用のオートメーション実行ロールです。ポリシーの詳細については、「AWS-SSM-RemediationAutomation-AdministrationRolePolicy」、「AWS-SSM-Automation-DiagnosisBucketPolicy」、「AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy」を参照してください。
- ManagedInstanceCrossAccountManagementRole – Systems Manager に、アカウント間でマネージドノード情報を収集することを許可します。

State Manager 関連付け

- EnableDHMCAssociation – 毎日実行され、デフォルトのホスト管理設定が有効になっていることを確認します。
- SystemAssociationForEnablingExplorer – 毎日実行され、Explorer が有効になっていることを確認します。Explorer はマネージドノードから得られたデータの同期に使用されます。
- EnableAREXAssociation – 毎日実行され、AWS Resource Explorer が有効になっていることを確認します。Resource Explorer は、組織のどの Amazon EC2 インスタンスが Systems Manager によって管理されていないかを判断するために使用されます。
- SSMAgentUpdateAssociation – 14 日ごとに実行され、利用可能な最新バージョンの SSM Agent がマネージドノードにインストールされていることを確認します。
- SystemAssociationForInventoryCollection – 12 時間ごとに実行され、マネージドノードからインベントリデータを収集します。

S3 バケット

- DiagnosisBucket – 診断ランブックの実行により収集されたデータを保存します。

Lambda 関数

- SSMLifecycleOperatorLambda – プリンシパルがすべての AWS Systems Manager Quick Setup アクションにアクセスすることを許可します。
- SSMLifecycleResource – セットアッププロセスにより作成されたリソースの、ライフサイクルの管理に役立つカスタムリソースです。

また、セットアッププロセスが完了したら、[診断および修復] ノードタスクを選択して、Systems Manager の管理対象であると報告されていないノードに自動的に修正を適用できます。例えば、Systems Manager エンドポイントへのネットワーク接続などの問題を特定できます。

統合コンソールをセットアップする

単一のアカウントとリージョン用に Systems Manager をセットアップするには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. [Systems Manager を有効にする] を選択します。
3. [機能の設定] セクションで、設定に対して有効にするオプションを選択します。

デフォルトのホスト管理設定 (DHMC) を有効にする

Systems Manager で DHMC を設定できるようにします。この機能により、Systems Manager は IAM ロールを使用して、アカウントとリージョン内のすべての Amazon EC2 インスタンスに Systems Manager で管理するために必要なアクセス許可を付与できるようになります。また、ドリフトの修復頻度を指定することもできます。設定のドリフトは、設定で行った選択と競合するサービスや機能に対し、ユーザーが変更を加えるたびに発生します。Systems Manager は、設定のドリフトがないかチェックし、もしあれば指定した頻度に基づいて修復を試みます。1 ~ 31 日の値を指定する必要があります。リージョンに DHMC を既に設定していても、以前に選択した IAM ロールが Systems Manager によって変更されることはありません。DHMC の詳細については、「Default Host Management Configuration を使用した EC2 インスタンスの自動管理」を参照してください。

DHMC により、AWS Identity and Access Management (IAM) インスタンスプロファイルを手動で作成しなくても Amazon EC2 インスタンスを管理できます。EC2 インスタンスに必要なアクセス許可を Systems Manager で管理できるように、このオプションを選択することをお勧めします。

インベントリメタデータの収集を有効にする

Systems Manager でノードから以下のタイプのメタデータを収集するように設定できます。

- AWS コンポーネント – EC2 ドライバー、エージェント、バージョンなど。
- アプリケーション – アプリケーション名、発行元、バージョンなど。

- ノードの詳細 – システム名、オペレーティングシステム (OS) 名、OS バージョン、最終起動、DNS、ドメイン、ワークグループ、OS アーキテクチャなど。
- ネットワーク設定 – IP アドレス、MAC アドレス、DNS、ゲートウェイ、サブネットマスクなど。
- サービス – 名前、表示名、ステータス、依存サービス、サービスタイプ、スタートタイプなど (Windows Server ノードのみ)。
- Windows ロール – 名前、表示名、パス、特徴タイプ、インストールされている状態など (Windows Server ノードのみ)。
- Windows 更新 – Hotfix ID、インストール者、インストール日など (Windows Server ノードのみ)。

インベントリを収集する頻度を指定します。1 ~ 744 時間の値を指定する必要があります。AWS Systems Manager のツールである Inventory の詳細については、「AWS Systems Manager インベントリ」を参照してください。

Systems Manager (SSM) エージェントの自動更新を有効にする

Systems Manager は、指定した頻度でエージェントの新しいバージョンをチェックできるようになります。頻度の値は 1 ~ 31 日で指定する必要があります。新しいバージョンがある場合、Systems Manager はのマネージドノード上エージェントを最新のリリースバージョンに自動的に更新します。Systems Manager は、エージェントがまだ存在しないインスタンスにエージェントをインストールしません。どの AMIs に SSM Agent がプリインストールされているかについては、「SSM Agent がプリインストールされている AMIs を見つける」を参照してください。

ノードが常に最新バージョンの SSM Agent を実行できるように、このオプションを選択することをお勧めします。エージェントを手動でインストールする方法など SSM Agent の詳細については、「「SSM Agent」 の使用」を参照してください。

4. [Submit] を選択します。

Systems Manager 統合コンソールの無効化

組織で Systems Manager 統合コンソールを無効にするには、Systems Manager の委任管理者として登録したアカウントにアクセスする必要があります。組織の委任管理者アカウントにログインしたら、統合コンソールの [設定] セクションで組織のセットアップを無効にできます。組織の統合コンソールのセットアップを無効にすると、Systems Manager が Resource Explorer のマネージドビューを含め、セットアッププロセス時に作成されたリソースを削除します。組織のセットアップを

無効にしても、信頼できるアクセスが取り消されたり、依存サービスの委任管理者アカウントの登録が解除されたりすることはありません。以下の手順では、統合コンソールのセットアップを無効にする方法について説明します。

Systems Manager 統合コンソールのセットアップを無効にするには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインの [設定] を選択します。
3. [無効化] を選択します。組織のセットアップを無効にしてもよいか確認する必要があります。このアクションにより、統合コンソール用に作成されたリソースが削除され、元に戻すことはできません。

統合コンソールのセットアップを無効にしたいのに Systems Manager の委任管理者アカウントにアクセスできない場合は、組織の管理アカウントからアクセスすることもできます。AWS CLI や SDK を使用して、`DeleteConfigurationManager` API オペレーションを呼び出してアカウントの組織セットアップの `ManagerArn` 値を渡します。統合コンソールのセットアップに使用されるマネージャー ARN の形式は、以下のとおりです。

`arn:aws:ssm-quicksetup:`*`account-id`*`:configuration-manager/`*`configuration-manager-id`*.

> **Note**
>
> *`configuration-manager-id`* の値がわからない場合は、`ListConfigurationManagers` API アクションを呼び出し、`AWSQuickSetupType-SSM` タイプを使用して結果をフィルタリングします。

AWS Systems Manager を使用したノード管理タスクの実行

以下のトピックでは、統合 AWS Systems Manager コンソールを使用して AWS Organizations 組織とシングル AWS アカウントに対する一般的なノードタスクを完了する方法について説明します。

トピック

- ノードインサイトの確認
- ノードの探索
- Systems Manager を使用したジャストインタイムノードアクセス
- 診断と修復
- Systems Manager 設定の調整

ノードインサイトの確認

Systems Manager の統合コンソールを使用することで、組織またはアカウント内のマネージドノードおよびアンマネージド EC2 インスタンスの全体的なステータスに関するインサイトを得ることができます。

Systems Manager は、マネージドノードと、Systems Manager によってまだ管理されていない EC2 インスタンスに関する視覚的な概要を提供します。(マネージドノードとは、ハイブリッドおよびマルチクラウド環境において Systems Manager で使用するように設定された任意のマシンです。サポートされているマシンタイプの詳細については、「ハイブリッドおよびマルチクラウド環境でサポートされるマシンタイプ」を参照してください。)

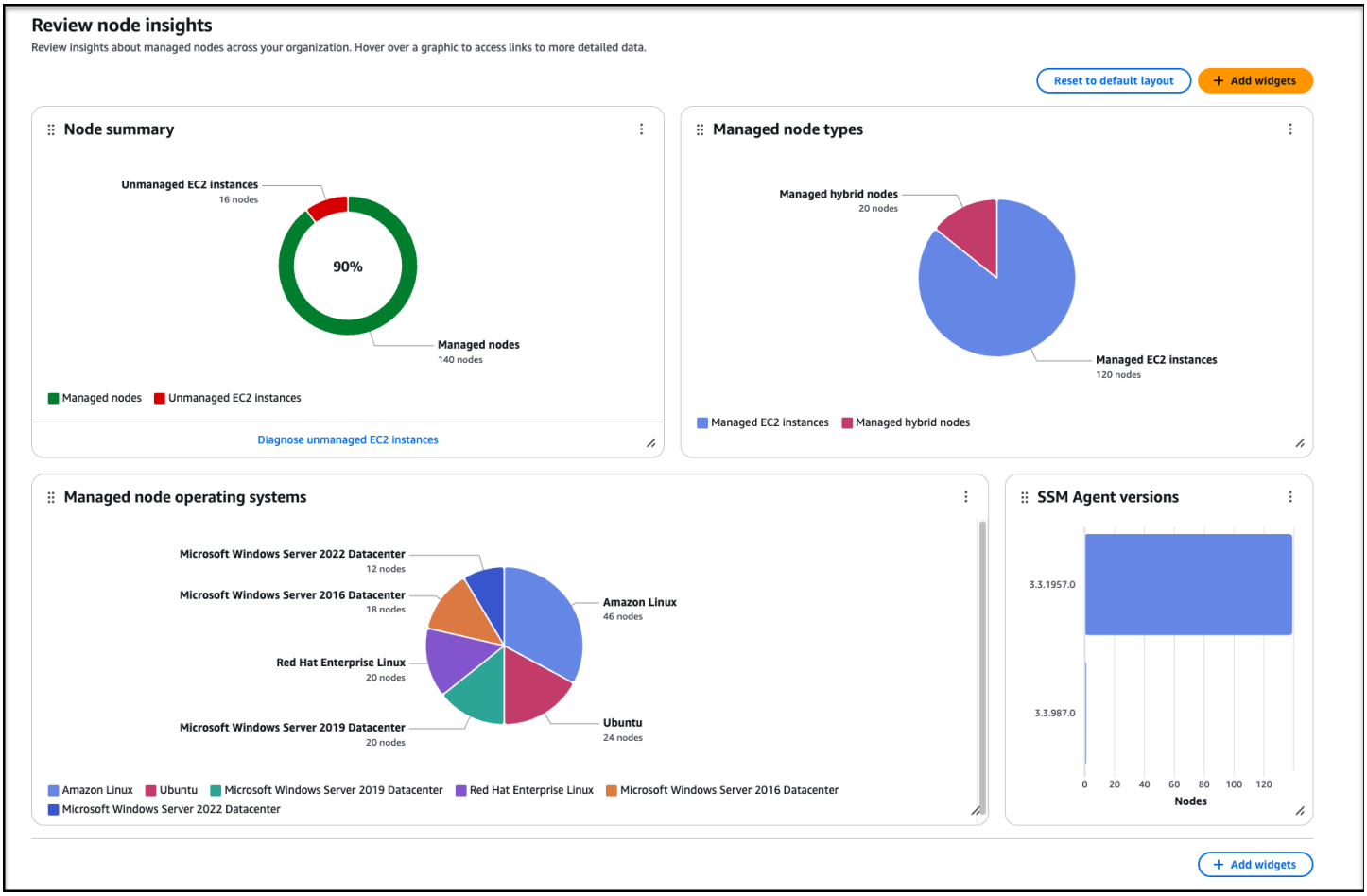
この概要は、ウィジェットと呼ばれる個別のレポートボックスを通じて提供されます。ウィジェットには、インタラクティブな円グラフやその他のグラフィックが備わっています。

[開始する前に]

ノードインサイトを確認するには、まず組織またはアカウントを Systems Manager 統合コンソールにオンボーディングする必要があります。詳細については、「AWS Systems Manager を設定する」を参照してください。

オンボーディング後、Systems Manager コンソールを開き、[ノードインサイトの確認] を選択します。

次の図は、[ノードインサイトの確認] ページで使用できるウィジェットと呼ばれる個別のレポートボックスを示しています。



この表示では、以下の情報を提供するウィジェットがサポートされています。

ノードの概要

組織またはアカウント内で現在マネージドノードではない EC2 インスタンスの数と、組織またはアカウントのフリートに含まれるマネージドノードの数を示します。

アンマネージドインスタンスとは

マネージド EC2 インスタンスを停止すると、Systems Manager コンソールで「アンマネージド」としてレポートされます。これは、SSM Agent がサービスへのアクティブな接続を持っていないため、想定される動作です。

> **Note**
>
> これは、AWS Config がインスタンスをアンマネージドとして定義する方法とは異なります。インスタンスが現在停止している場合、AWS Config は、インスタンスの SSM

Agent と Systems Manager サービスとの間で「ハートビート」接続が最後に確立されたときのインスタンスのステータスを報告します。

インスタンスが再起動すると、Systems Manager サービスに自動的に再接続され、統合コンソールのステータスは 5 分以内に「マネージド」に復元されます。手動による介入は必要なく、インスタンスのすべての Systems Manager 設定は停止/開始サイクルの間も保持されます。

ただし、インスタンスが起動から数分後に「マネージド」としてまだ報告されていない場合、インスタンスは Systems Manager 管理用に正しく設定されていない可能性があります。この場合、診断を実行して、インスタンスがアンマネージド状態のままである理由を特定することをお勧めします。詳細については、「Systems Manager でのアンマネージド Amazon EC2 インスタンスの診断と修復」を参照してください。

診断スキャンで問題を特定できない場合は、次のトピックを参照して、SSM Agent、AWS Identity and Access Management (IAM) ロール、および Systems Manager の前提条件の要件がすべて満たされていることを確認します。

- SSM Agent のトラブルシューティング
- Systems Manager に必要なインスタンスのアクセス許可を設定する
- マネージドノードの可用性のトラブルシューティング

マネージドノードのタイプ

フリート内のマネージドノードのうち、EC2 インスタンスの数および他のサーバータイプの数を示します。他のサーバータイプには、自社設備内のサーバー (オンプレミスサーバー)、AWS IoT Greengrass コアデバイス、AWS IoT および非 AWS エッジデバイス、仮想マシン (VM) などがあります。仮想マシンには、他のクラウド環境の VM も含まれます。[ノードタイプ] グラフィックにカーソルを合わせると、[ノードの探索] ページの詳細情報へのリンクにアクセスできます。

ハイブリッド環境およびマルチクラウド環境での AWS のサポートの詳細については、「ハイブリッドおよびマルチクラウド向けの AWS ソリューション」を参照してください。

「SSM Agent バージョン」

フリートにおける AWS Systems Manager エージェント (SSM Agent) のインストールに関する情報を提供します。SSM Agent は、マネージドノードで実行される Amazon ソフトウェアです。SSM Agent により、Systems Manager はこれらのリソースを更新、管理、および設定できるようになります。エージェントは AWS クラウド 上の Systems Manager サービスからのリクエストを処理し、リクエストに指定されたとおりにそれらを実行します。

フリート内のマネージドノードについて、このウィジェットは、フリート内の SSM Agent のバージョンを最新のものから順に報告します。SSM Agent バージョンのグラフィックにカーソルを合わせると、[ノードの探索] ページの詳細情報へのリンクにアクセスできます。

SSM Agent の詳細については、「「SSM Agent」 の使用」を参照してください。

マネージドノードのオペレーティングシステム

フリート内のマネージドノードにおける各オペレーティングシステムの割合の内訳を提供します。オペレーティングシステム別のマネージドノードのグラフィックにカーソルを合わせると、[ノードの探索] ページの詳細情報へのリンクにアクセスできます。

[ノードインサイトの確認] ページでウィジェットのレイアウトをカスタマイズするには、ドラッグアンドドロップ機能を使用したり、表示するウィジェットの削除や追加を行ったりします。

以下のトピックの情報は、Systems Manager のノードインサイトのウィジェットを操作するのに役立ちます。

トピック

- [ノードインサイトの確認] ページのウィジェットの追加または削除
- [ノードインサイトの確認] ページのウィジェットの再配置

[ノードインサイトの確認] ページのウィジェットの追加または削除

ウィジェットを追加および削除することで、Systems Manager の [ノードインサイトの確認] ページでレイアウトをカスタマイズできます。

> **Note**
>
> デフォルトでは、このページには使用可能なすべてのウィジェットが表示されます。

[ノードインサイトの確認] ページのウィジェットを追加または削除する手順

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. 左のナビゲーションで、[ノードインサイトの確認] を選択します。
3. 表示からウィジェットを削除するには、次の手順を実行します。

a. ウィジェットのメニューから [その他]
( )
を選択します。

b. [Remove widget] (ウィジェットの削除) を選択します。

4. 表示にウィジェットを追加するには、次の手順を実行します。

a. ウィジェットの追加 を選択します。

b. [ウィジェットの追加] ペインで、表示に追加するウィジェットのドラッグハンドル
( )
をクリックして長押しします。

c. ウィジェットをドラッグして、メインペインにドロップします。

[ノードインサイトの確認] ページのウィジェットの再配置

ウィジェットを再配置することで、[ノードインサイトの確認] ページのレイアウトをカスタマイズできます。

[ノードインサイトの確認] ページでウィジェットを再配置する手順

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[ノードインサイトの確認] を選択します。
3. ウィジェットのレイアウトをカスタマイズするには、移動するウィジェットを選択します。ウィジェットのドラッグハンドル
( )
をクリックしたまま、新しい場所までドラッグします。
4. 再配置するウィジェットごとにこのプロセスを繰り返します。

新しいレイアウトが気に入らない場合は、[デフォルトレイアウトにリセット] を選択すると、すべてのウィジェットが元の場所に戻ります。

ノードの探索

Systems Manager で [ノードの探索] ページを使用すると、フィルターに指定した条件に従って組織またはアカウント内のマネージドノードの詳細を確認できます。また、AWS 生成 AI ソリューションである Amazon Q Developer (Amazon Q) と Systems Manager との統合により、テキストプロンプトを使用して検索することもできます。

[開始する前に]

[ノードの探索] 機能を使用するには、まず組織またはアカウントを Systems Manager の統合コンソールにオンボーディングする必要があります。詳細については、「組織用の Systems Manager 統合コンソールのセットアップ」を参照してください。

オンボーディング後、Systems Manager コンソールを開き、[ノードの探索] を選択します。

> **Note**
>
> ホームリージョンとは異なるリージョンに Resource Explorer 用のアグリゲーターインデックスを作成した場合は、Systems Manager により現在のインデックスが降格します。その後、Systems Manager によりホームリージョン内のローカルインデックスが新しいアグリゲーターインデックスとして昇格します。それまでの間、ホームリージョンのノードのみが表示されます。このプロセスが完了するまで最大 24 時間かかる場合があります。

トピック

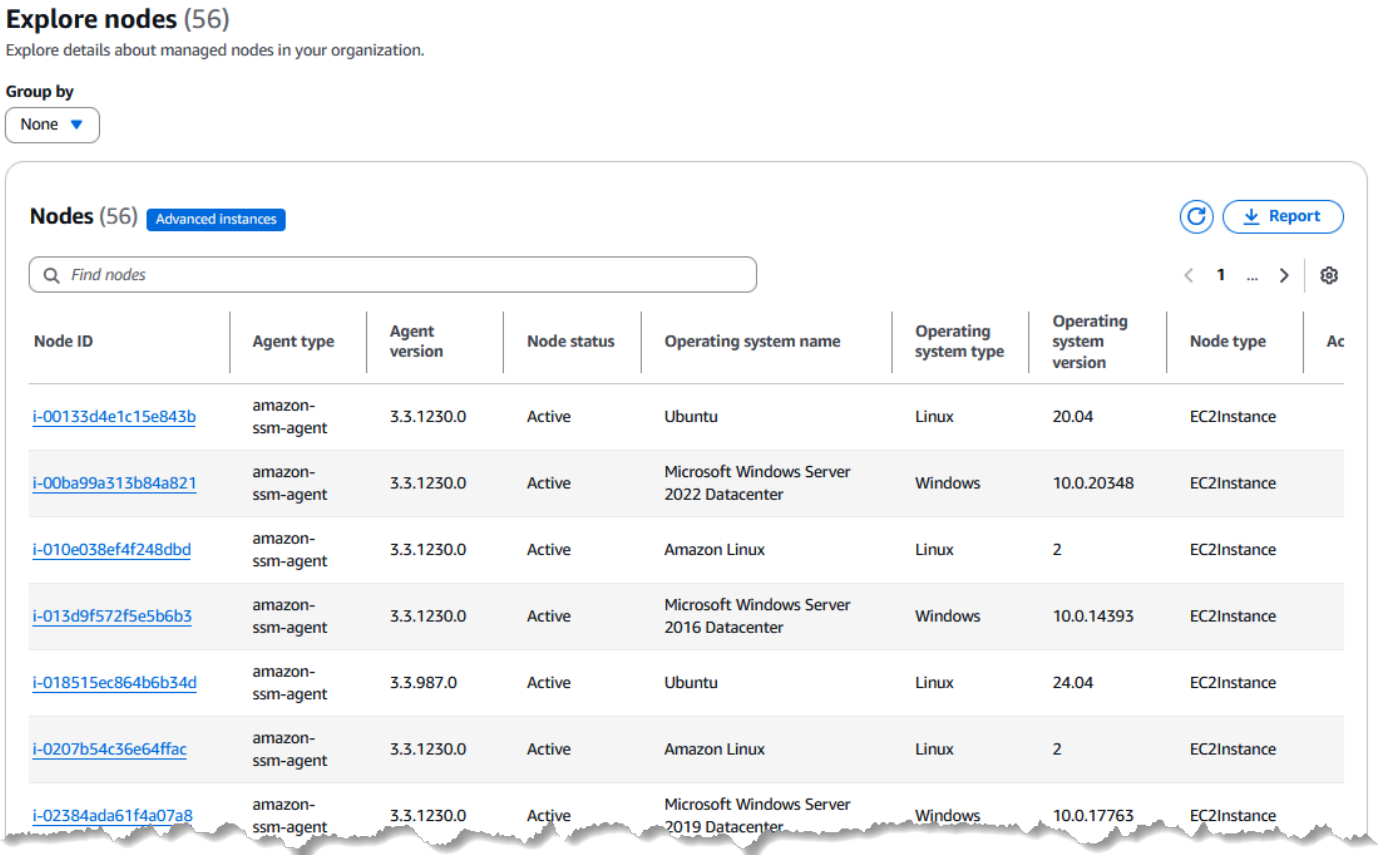
- コンソールフィルターを使用したノードの探索
- Amazon Q でテキストプロンプトを使用したノードの探索
- 個々のノードの詳細の表示およびノードに対するアクションの実行
- マネージドノードレポートのダウンロードまたはエクスポート
- ノードレポートのコンテンツと外観の管理

コンソールフィルターを使用したノードの探索

Systems Manager コンソールでは、以下のビューに従ってマネージドノードをグループ化できます。

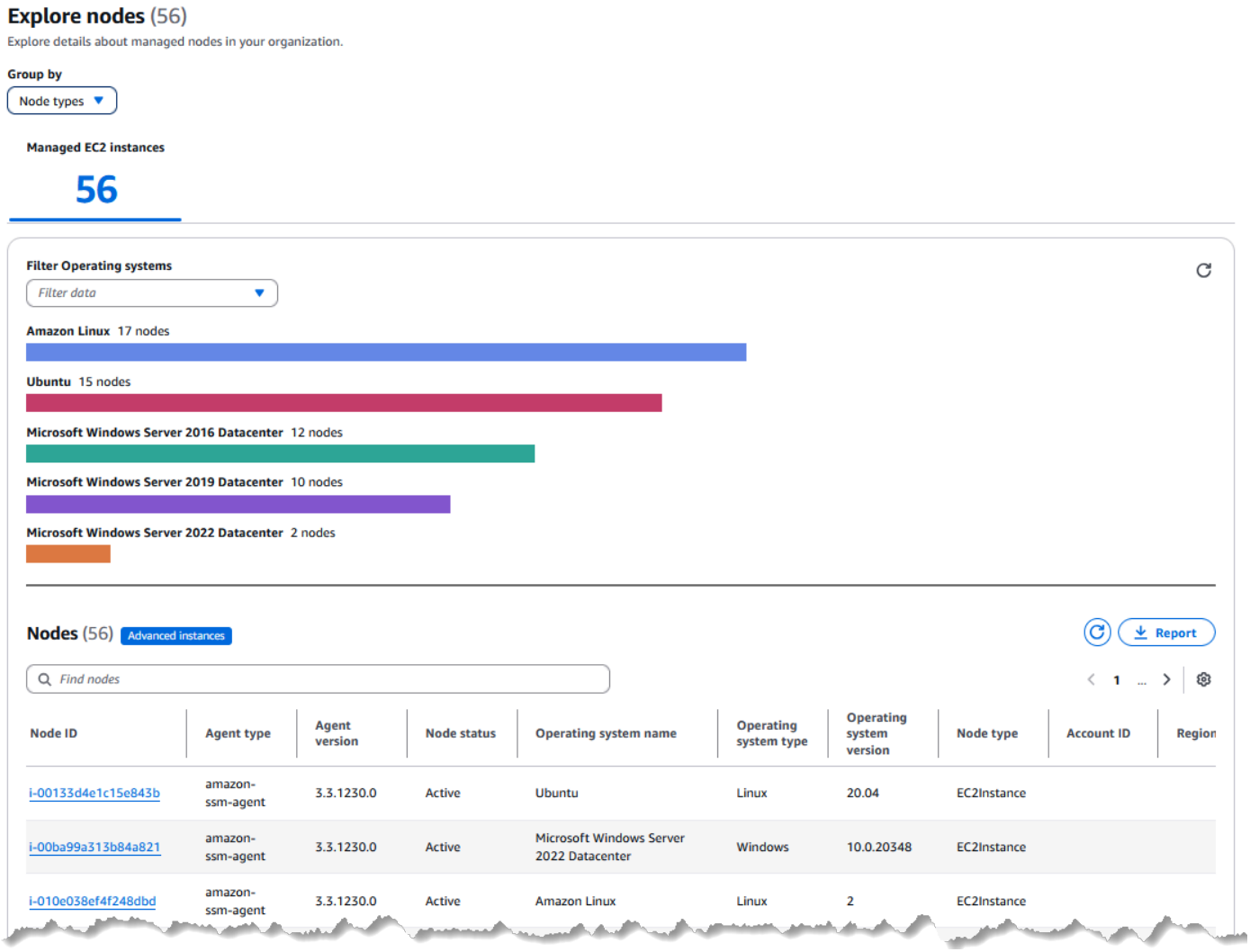
All nodes (No filter)

組織またはアカウント内のすべてのマネージドノードをリストします。



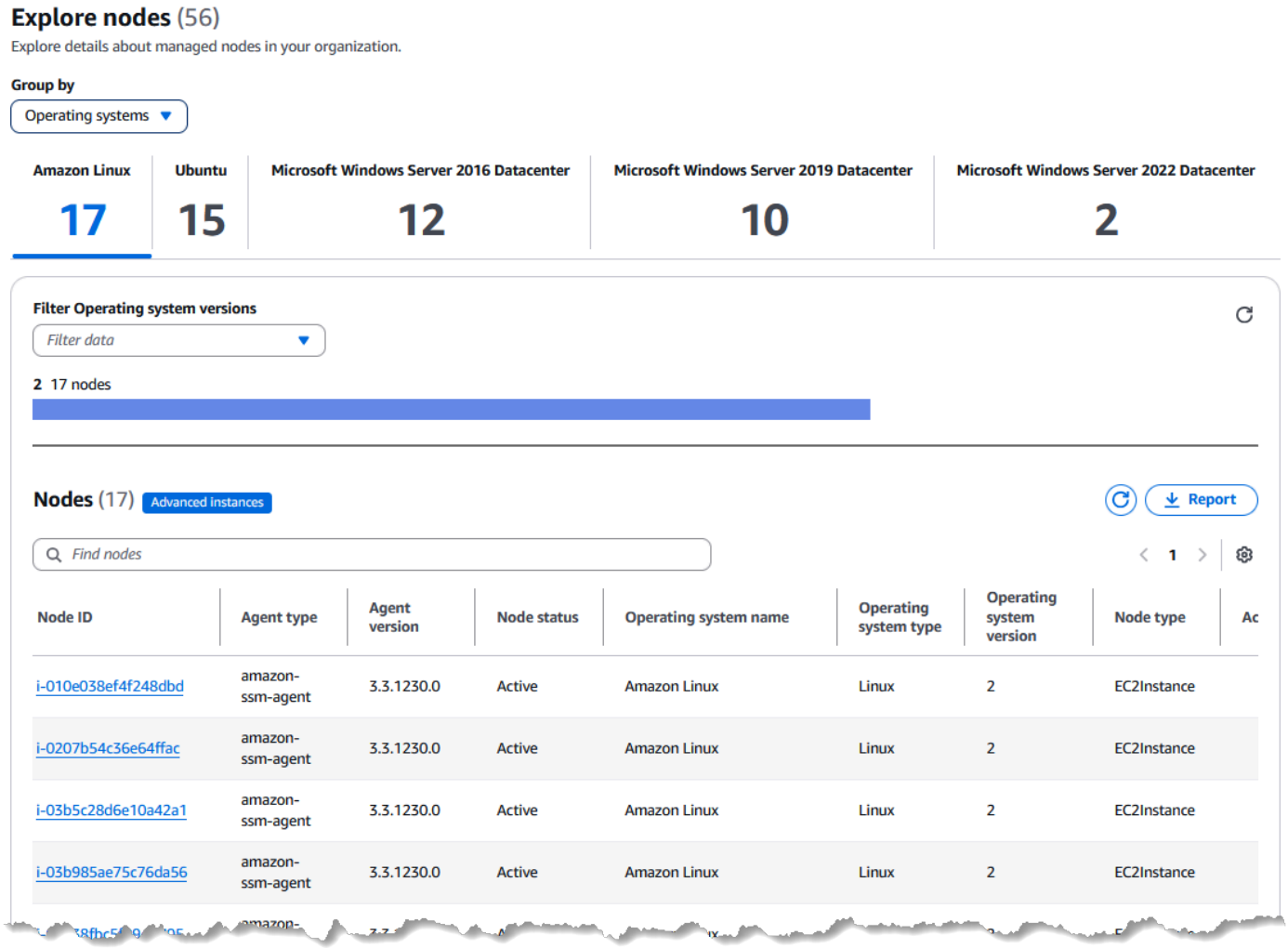
Node types

Amazon Elastic Compute Cloud (Amazon EC2) インスタンスとその他のマシンタイプのデータがタブに分かれて表示されます。こうしたマシンタイプには自社構築サーバー (オンプレミスサーバー)、AWS IoT Greengrass コアデバイス、AWS IoT デバイス、非 AWS エッジデバイス、他のクラウド環境の VM も含めた仮想マシン (VM) などがあります。



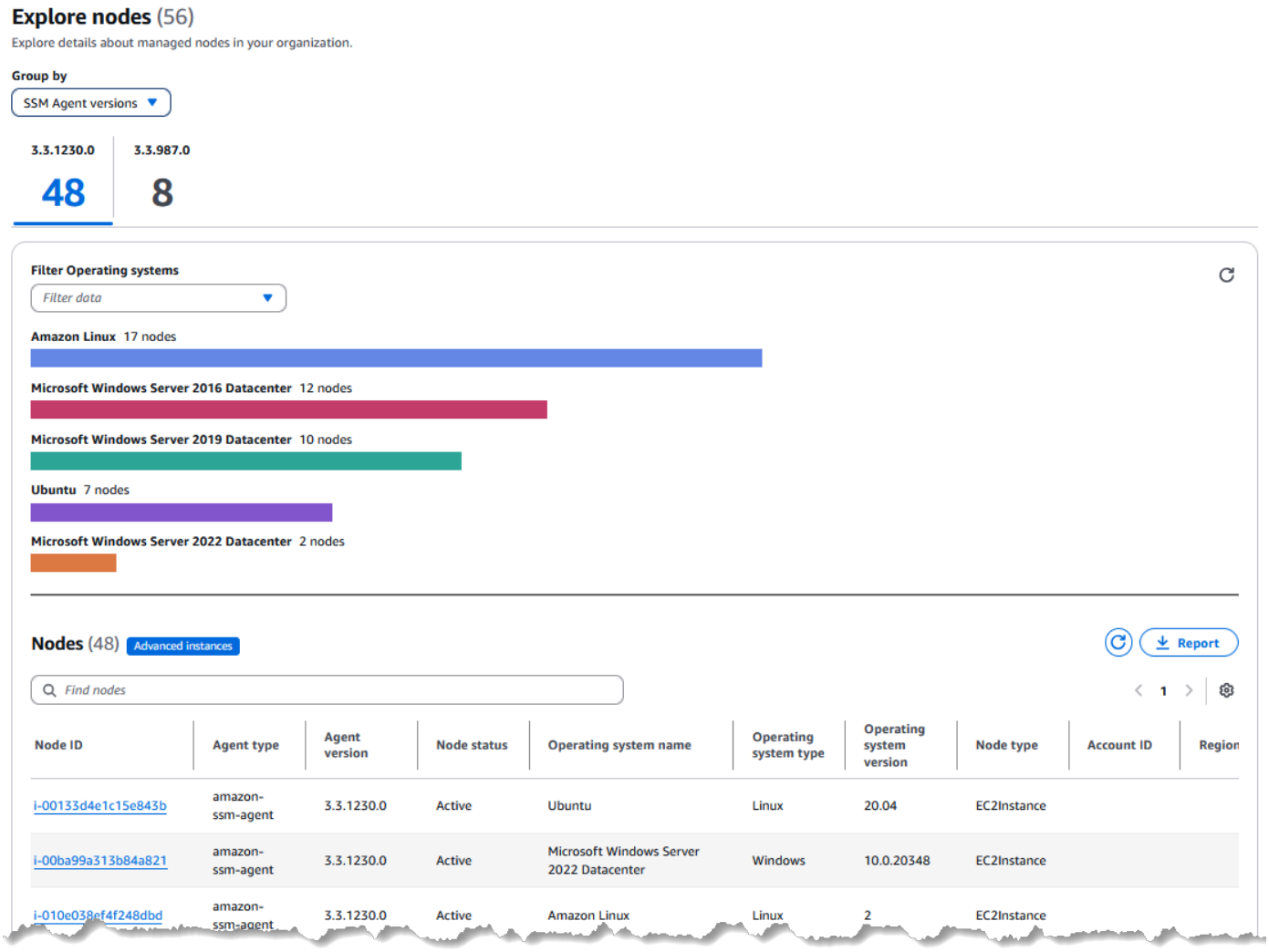
Operating systems

Amazon Linux や Microsoft Windows Server 2022 Datacenter など、組織またはアカウント内のオペレーティングシステムタイプごとにタブが表示されます。各タブでは、Amazon Linux 2 や Amazon Linux 2023 など特定のバージョンのオペレーティングシステムのみを選択して、さらにリストをフィルタリングできます。



SSM Agent versions

フリート内のマネージドノードにインストールされている SSM Agent のバージョンごとにタブが表示されます。各タブでは、Amazon Linux や Amazon Windows Server 2022 Datacenter など特定のオペレーティングシステムのみを選択して、さらにリストをフィルタリングできます。



またこれらのビューごとに、ノードステータス、AWS アカウント ID、組織単位 ID など特定のプロパティのノードのみを表示するように選択することで、レポートされるノードのリストをさらに絞り込むことができます。

使用可能なデータ列のうちどれを [ノードの探索] ページに表示するかを選択することで、レポート表示をカスタマイズできます。また、CSV 形式または JSON 形式でレポートをダウンロードしたり、レポートを CSV 形式で Amazon S3 にエクスポートしたりすることもできます。

トピック

- マネージドノードの概要のフィルタービューの選択

マネージドノードの概要のフィルタービューの選択

Systems Manager の [ノードの探索] ページでは、使用可能なさまざまなフィルタービューに応じて、フリートに関する集約データを表示できます。

マネージドノードの概要のフィルタービューを選択する手順

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[ノードの探索] を選択します。
3. [フィルタービュー] で、いずれかのフィルターオプションを選択し、必要に応じてレポートをさらに絞り込みます。

   - [マネージドノード] – 検索 ( ) ボックスで、プロパティと区切り記号を選択できます (`Node type = Managed EC2 instances` など)。
   - [オペレーティングシステム] – [オペレーティングシステムバージョンをフィルタリング] リストで、OS バージョン番号を選択できます。検索 ( ) ボックスで、プロパティと区切り文字を選択できます (`Node type = Managed EC2 instances` など)。
   - [SSM Agent のバージョン] – [オペレーティングシステムをフィルタリング] リストで、OS 名を選択できます。検索 ( ) ボックスで、プロパティと区切り文字を選択できます (`Node type = Managed EC2 instances` など)。
   - [ノードタイプ] – [オペレーティングシステムをフィルタリング] リストで、OS 名を選択できます。検索 ( ) ボックスで、プロパティと区切り文字を選択できます (`Node type = Managed EC2 instances` など)。

オプションでリストをフィルタリングした後、[ノード ID] 列で ID を選択することで、特定のマネージドノードの詳細を表示できます。その詳細ビューから、ノードに対してさまざまなアクションを実行できます。

Amazon Q でテキストプロンプトを使用したノードの探索

Amazon Q Developer と Systems Manager との統合により、テキストプロンプトを使用して、マネージドノードについて生成 AI が作成した情報を表示できます。

Amazon Q Developer は、AWS アプリケーションの理解、構築、拡張、運用を支援する生成 AI 搭載の会話型アシスタントです。AWS での構築を加速するために、過不足がなく、実用的で参考になる回答が生成されるよう、Amazon Q を支えるモデルを高品質の AWS コンテンツで強化しています。詳細については、「Amazon Q Developer ユーザーガイド」の「What is Amazon Q Developer?」を参照してください。

Systems Manager と Amazon Q との統合により、複数の AWS アカウントとリージョン全体にわたって大規模な分散環境をすばやく可視化して制御できます。自然言語クエリを使用してノードデータをすばやく検索し、問題を特定して迅速に対策を講じることができます。

ユーザーがマネージドノードまたはマネージドインスタンスについて自然言語で質問すると、Amazon Q は Systems Manager `ListNodes` アクションを使用し、ユーザーが入力したテキストに基づいてフィルターを作成して結果を取得します。

例えば、Amazon Q に以下のプロンプトを与えたとします。

`List my managed nodes running Red Hat Enterprise Linux 9.2`

Amazon Q は、リクエストに含めるフィルターを判断して、以下のようなクエリを実行します。

```
aws ssm list-nodes \
    --filters Key=PlatformName,Values='Red Hat Enterprise Linux',Type=Equal
 Key=PlatformVersion,Values=9.2,Type=Equal
```

次に、Amazon Q はアカウント内の Red Hat Enterprise Linux インスタンスに関するレポートを生成して、インスタンスの数、その ID とリージョンなどの情報をリストします。

また、各インスタンスの詳細を JSON 形式のサマリーで表示できるほか、Systems Manager の [ノードの探索] ページに EC2 インスタンスまたはマネージドノードのリスト全体を表示するためのリンクを開くことができます。[ノードの探索] には、プロンプトに含めたフィルター条件に一致する結果が表示されます。それを基に、「ノードの探索」で説明しているようにリクエストのフィルターを変更したり絞り込んだりできます。

トピック

- Amazon Q にフリートについてたずねる的確なプロンプトの作成方法

- Amazon Q を使用したマネージドノードの探索

Amazon Q にフリートについてたずねる的確なプロンプトの作成方法

Amazon Q に与える質問 (プロンプト) の質を上げれば、得られる結果の質も向上します。

クエリプロンプトのヒント

Amazon Q にフリートについてクエリする場合は、以下のヒントに留意してください。

1. 結果の精度を高めるには、プロンプトで単に「ノード」や「インスタンス」を使用するのではなく「マネージドノード」や「マネージドインスタンス」という語句を使用します。
2. AWS Organizations に設定されているように、組織に含まれる複数のアカウントを対象に結果をクエリするには、指定されたホームリージョンの委任管理者アカウントにログインする必要があります。
3. 委任管理者アカウントでは、組織全体にわたるノードとインスタンスについてたずねていることを Amazon Q が理解できる用語を使用します。特に、「組織内で」や「123456789012 というアカウントで」といった用語を使用すると効果的です。

トピック

- Amazon Q へのサンプルの質問
- プロンプトでサポートされているオペレーティングシステムの名前とバージョン

Amazon Q へのサンプルの質問

以下の表にサンプルの質問を挙げて、Amazon Q でよりよい結果を得るためのクエリの作成方法を示します。

ListNodes コマンドの実行時に Amazon Q が適用するフィルターの例も示します。これらは、プロンプトの内容から生成されます。

自然言語によるサンプルの質問	Amazon Q が適用したフィルター
Show me my Windows managed nodes.	`PlatformType = Windows`
List my managed instances in account 123456789012.	`AccountId = 123456789012`

自然言語によるサンプルの質問	Amazon Q が適用したフィルター
Show me all managed nodes running Amazon Linux 1 across my organization.	`PlatformName = Amazon Linux` `PlatformVersion = 1`
Show me all managed instances running Microsoft Windows Server 2019 Datacenter in my organization.	`PlatformName = Microsoft Windows Server 2019 Datacenter`
Can you show me all managed nodes with SSM Agent version 3.3.1142.0?	`AgentType = amazon-ssm-agent` `AgentVersion = 3.3.1142.0`

List all Amazon Linux 2 managed instances in account 123456789012 that have SSM Agent version 3.3.1230.0.	`PlatformName = Amazon Linux`
	`PlatformVersion = 2`
	`AccountId = 123456789012`
	`AgentType = amazon-ssm-agent`
	`AgentVersion = 3.3.1230.0`

What Microsoft Windows Server 2008 R2 Enterprise managed nodes are running in the eu-central-1 region across my entire organization?	`PlatformName = Microsoft Windows Server 2008 R2 Enterprise` `Region = eu-central-1`

Show me all managed instances running CentOS Linux 7 in ou-d6ty-gxdma6vm.	`PlatformName = CentOS Linux`
	`PlatformVersion = 7`
	`OrganizationalUnitId = ou-d6ty-gxdma6vm`

What Ubuntu managed instances are in account 123456789012?	`PlatformName = Ubuntu` `AccountId = 123456789012`
List my Linux managed instances.	`PlatformType = Linux`

自然言語によるサンプルの質問	Amazon Q が適用したフィルター
Find my macOS managed nodes.	`PlatformType = macOS`
Show me all Amazon Linux managed nodes in my org.	`PlatformName = Amazon Linux`
List managed nodes running Amazon Linux 2 .	`PlatformName = Amazon Linux` `PlatformVersion = 2`

List the managed nodes with Ubuntu 16.04 in account 123456789012.	`PlatformName = Ubuntu`
	`PlatformVersion = 16.04`
	`AccountId = 123456789012`

Find all managed nodes that have an SSM Agent version that is not 3.3.987.0.	`AgentType = amazon-ssm-agent` `AgentVersion != 3.3.987.0`
List all managed instances that are not running a Linux operating system.	`PlatformType != Linux`

プロンプトでサポートされているオペレーティングシステムの名前とバージョン

Amazon Q にアカウント内のマネージドノードについてたずねるときは、オペレーティングシステムの名前を Systems Manager でのラベルのとおりに指定すると効果的です。また、バージョン番号を指定して結果をさらに絞り込むこともできます。例えば、以下の表に示すように、**macOS 14.5**、**Microsoft Windows Server 2019 Datacenter**、**AlmaLinux 9.2 through 9.4** といった名前を具体的に挙げて結果を求めることができます。

以下のリストは網羅的なものではなく、例として挙げているにすぎません。

macOS

プラットフォーム名	バージョン番号
macOS	11.6.7、11.7.10、12.6.6、12.7.6、13.2、13.4、13.7、14.1、14.5、14.6.1、15.0

Windows

リリース	バージョン番号
Microsoft Windows Server 2008 Enterprise	6.0.6003
Microsoft Windows Server 2008 R2 Datacenter	6.1.7601
Microsoft Windows Server 2008 R2 Enterprise	6.1.7601
Microsoft Windows Server 2008 R2 Standard	6.1.7601
Microsoft Windows Server 2012 R2 Datacenter	6.3.9600
Microsoft Windows Server 2012 R2 Standard	6.3.9600
Microsoft Windows Server 2012 Standard	6.2.9200
Microsoft Windows Server 2016 Datacenter	該当なし
Microsoft Windows Server 2016 Standard	10.0.14393
Microsoft Windows Server 2019 Datacenter	該当なし
Microsoft Windows Server 2019 Standard	該当なし
Microsoft Windows Server 2022 Datacenter	該当なし
Microsoft Windows Server 2022 Standard	10.0.20348

Linux

プラットフォーム名	バージョン番号
AlmaLinux	8.10、9.2、9.3、9.4
Amazon Linux 2	2.0 以降
Amazon Linux 2023	2,023.0.20230315.0 以降
Amazon Linux	2015.03、2015.09、2016.03、2016.09、2017.03、2017.09、2018.03
Bottlerocket	1.14.3、1.16.1、1.18.0、1.19.1、1.19.2、1.19.5、1.20.0、1.20.1、1.20.2、1.20.3、1.20.5、1.21.1、1.23.0、1.24.0、1.24.1、1.25.0、1.26.1、
CentOS	6.7、6.8、6.9 (Final)、6.10、6.10 (Final)
CentOS Linux	7、7.2.1511、7.2.1511 (Core)、7.3.1611、7.3.1611 (Core)、7.4.1708、7.5.1804、7.5.1804 (Core)、7.6.1810、7.7.1908、7.8.2003、7.9.2009、7.9.2009 (Core)、8.2.2004、8.5.2111
CentOS Stream	8、9
Debian GNU/Linux	8 ~ 12
Oracle Linux Server	7.8、8.2、8.3、8.8、8.9、8.10、9.4
Red Hat Enterprise Linux	8.2、8.3、8.4、8.5、8.6、8.7、8.8、8.9、8.10、9.2、9.3、9.4
Red Hat Enterprise Linux サーバー	6.9 (Santiago)、6.10 (Santiago)、7.3、7.6、7.7、7.8、7.9
Rocky Linux	8.6、8.7、8.8、8.9、8.10、9.1、9.2、9.3、9.4
SLES	12.4、15、15.1、15.2、15.3、15.4、15.5

プラットフォーム名	バージョン番号
Ubuntu	14.04、16.04、18.04、20.04、22.04、24.04

Amazon Q を使用したマネージドノードの探索

Systems Manager と Amazon Q Developer の統合により、Amazon Q インターフェイスが使用可能な AWS Management Consoleの任意の場所から、フリート内のマネージドノードについて質問できます。

Amazon Q の操作方法の詳細については、「Amazon Q Developer ユーザーガイド」の「Chatting with Amazon Q Developer about AWS」を参照してください。

Amazon Q を使用してマネージドノードを探索する手順

1. AWS Management Consoleの任意の場所から、Amazon Q アイコン
   ( )
   を選択します。
2. Amazon Q ペインの下部にあるプロンプトフィールドで、アカウントまたは組織内のマネージドノードについて質問します。

   > **Tip**
   >
   > 効果的なプロンプトの作成方法に関するヒントは、「Amazon Q にフリートについてたずねる的確なプロンプトの作成方法」の情報を参照してください。

3. 特定のノードに関する情報を調査するか、[AWS Systems Manager コンソールを開く] を選択して探索を続行します。

個々のノードの詳細の表示およびノードに対するアクションの実行

Systems Manager の [ノードの探索] ページのリストから個々のノードを選択して、マシンに関する包括的な詳細を表示したり、ノードに対してさまざまなアクションを実行したりできます。詳細ページの [一般] ページには、ノードに関する包括的な情報が表示されます。

個々のノードの詳細を表示し、ノードに対してアクションを実行する手順

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[ノードの探索] を選択します。
3. (オプション)「マネージドノードの概要のフィルタービューの選択」の手順に従って、組織またはアカウントに表示されるマネージドノードのリストを絞り込みます。
4. [ノード ID] 列で、ノードのリンクされた ID を選択します。
5. ノードの詳細を表示するには、左側のナビゲーションの [プロパティ] リストで、詳細を表示するプロパティを選択します。

   - [タグ] – ノードに適用されているタグのリストを表示します。タグを追加または削除することもできます。
   - [インベントリ] – インベントリタイプ ([AWS:Application] や [AWS:Network] など) を選択して、ノードのインベントリの詳細を表示します。
   - [関連付け] – ノードに適用されているすべての State Manager 関連付けに関する詳細 (ステータスや関連付けられている SSM ドキュメント名など) を表示します。
   - [パッチ] – ノードのパッチとパッチステータスに関する概要情報を表示します。
   - [設定コンプライアンス] — ノードのコンプライアンスの詳細 (コンプライアンスステータスやコンプライアンス問題の重要度など) を表示します。
6. ノードに対してアクションを実行するには、[ノードアクション] メニューで次のオプションを使用します。

   > **Note**
   >
   > これらのアクションは、現在作業している AWS アカウントおよびリージョンのマネージドノードに対してのみ使用できます。他のアカウントまたはリージョンのマネージドノードの場合は、そのノードに対するアクセス権を持っていれば、代わりに [プロパティ] リストにアクセスできます。

   - [接続、ターミナルセッションを開始する] — AWS Systems Manager Session Manager を使用してノードに接続します。
   - ツール

- [ファイルシステムを表示] – ノードのディレクトリ構造のコンテンツを参照します。ディレクトリを追加、名前変更、削除します。ファイルを切り取り/コピーして貼り付けます。
- [パフォーマンスカウンタを表示] – ノードに関するパフォーマンス情報 (CPU 使用率、ネットワークトラフィック、その他の使用率タイプなど) を表示します。
- [プロセスを管理] – ノードのリソース使用状況に関する情報を表示します。ノード上でプロセスを開始または停止します。
- [ユーザーとグループを管理] – ノード上のユーザーアカウントおよびユーザーグループを表示、追加、または削除します。
- [実行コマンドを実行] – AWS Systems Manager Run Commandを使用してノードの設定を管理します。Run Command は Systems Manager ドキュメントを使用して、アプリケーションの更新、Linux シェルスクリプトや Windows PowerShell コマンドの実行など、オンデマンドの変更を実行します。
- [パッチノード] – AWS Systems Manager Patch Manager の [今すぐパッチ適用] 機能を使用して、コンソールからノードに対するオンデマンドパッチ適用オペレーションを実行します。

> **Note**
>
> 上記のタスクは、左側のナビゲーションにある [ツール] メニューから開始することもできます。

- ノード設定
  - [タグの追加] — ノードに追加のタグキーと値のペアを適用します。
  - [ノードユーザーパスワードのリセット] – ノード上の指定されたユーザー用に新しいパスワードを設定します。
  - [IAM ロールを変更] – ノードに関連付けられている IAM ロールを変更します。ノードにアタッチする新しい IAM ロールを作成します。

マネージドノードレポートのダウンロードまたはエクスポート

Systems Manager の [ノードの探索] 機能を使用して、Systems Manager コンソールで、AWS 組織またはアカウント内のマネージドノードのフィルタリングされた/フィルタリングされていないリストを表示できます。データをオフラインで表示したり、別のアプリケーションで処理したりする場合は、レポートを CSV ファイルまたは JSON ファイルとして保存できます。

レポートのサイズに応じて、レポートをローカルマシンにダウンロードするか、Amazon S3 バケットにエクスポートするかを求められます。S3 バケットに保存されるレポートは CSV 形式のみです。

マネージドノードレポートをダウンロードまたはエクスポートする手順

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[ノードの探索] を選択します。
3. (オプション)「マネージドノードの概要のフィルタービューの選択」の手順に従って、組織またはアカウントに表示されるマネージドノードのリストを絞り込みます。
4. [レポート]
   (⬇)
   を選択します。
5. [レポートのダウンロード] ダイアログボックスが表示された場合は、以下の手順を実行します。

   a. [ファイル名] にファイルの名前を入力します。レポートの範囲を表す名前 (`all-organization-nodes` や `ec2-instances-out-of-date-agent` など) を指定することをお勧めします。

   b. [含まれる列] で、すべての使用可能なノード詳細の列を含めるか、現在の表示用に選択した列のみを含めるかを指定します。

   > **Tip**
   > レポート表示の列の管理については、「ノードレポートのコンテンツと外観の管理」を参照してください。

   c. [ファイル形式] で、ファイルの使用方法に応じて [CSV] または [JSON] を選択します。

   d. CSV ファイルに列見出し行を含める場合は、[スプレッドシートの見出し] で [列名の行を含める] を選択します。

   e. [ダウンロード] を選択します。

   レポートは、ブラウザの設定に応じて、デフォルトのダウンロード場所に保存されます。
6. [Amazon S3 にエクスポート] ダイアログボックスが表示された場合は、以下の手順を実行します。

   a. [S3 URI] に、レポートのエクスポート先のバケットの URI を入力します。

> **Tip**
>
> Amazon S3 コンソールでバケットのリストを表示するには、[表示] を選択します。アカウント内のバケットのリストから選択するには、[S3 を参照] を選択します。

b. [承認方法] で、レポートをバケットにエクスポートするためのアクセス許可の付与に使用するサービスロールを指定します。

Systems Manager にロールを作成させることを選択した場合は、Systems Manager によって、オペレーションに必要なすべてのアクセス許可と信頼ステートメントが提供されます。

独自のロールを使用または作成する場合は、そのロールに必要なアクセス許可と信頼ステートメントを含める必要があります。このロールの作成の詳細については、「診断レポートを S3 にエクスポートするカスタムサービスロールの作成」を参照してください。

c. [Submit] を選択します。

診断レポートを S3 にエクスポートするカスタムサービスロールの作成

Systems Manager の [ノードの探索] ページで、AWS 組織やアカウントのマネージドノードのフィルタリングされた/フィルタリングされていないリストを表示している場合、そのリストをレポートとして CSV ファイル形式で Amazon S3 バケットにエクスポートできます。

そのためには、オペレーションに必要なアクセス許可と信頼ポリシーを持つサービスロールを指定する必要があります。レポートのダウンロードプロセス中に Systems Manager によって自動的にロールが作成されるようにすることもできます。オプションで、ユーザー自身がロールおよびそのロールに必要なポリシーを作成することもできます。

診断レポートを S3 にエクスポートするカスタムサービスロールを作成する手順

1. 「IAM ユーザーガイド」の「JSON エディターを使用したポリシーの作成」の手順を実行します。

   - ポリシーコンテンツとして以下を使用します。その際に、*#########*は独自の情報に置き換えてください。

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

```
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::s3-bucket-name/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "account-id"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketAcl",
        "s3:ListBucket",
        "s3:PutLifecycleConfiguration",
        "s3:GetLifecycleConfiguration"
      ],
      "Resource": "arn:aws:s3:::s3-bucket-name",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "account-id"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ssm:ListNodes"
      ],
      "Resource": "*"
    }
  ]
}
```

- 次のステップで簡単にわかるように、ポリシーに名前を付けます。

2. 「IAM ユーザーガイド」の「カスタム信頼ポリシーを使用した IAM ロールの作成 (コンソール)」の手順を実行します。

- ステップ 4 では、次の信頼ポリシーを入力します。その際に、*#########*は独自の情報に置き換えてください。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SSMAssumeRole",
      "Effect": "Allow",
      "Principal": {
        "Service": "ssm.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "account-id"
        }
      }
    }
  ]
}
```

3. ステップ 10 では、[ステップ 2: アクセス許可を追加する] を選択し、前のステップで作成したポリシーの名前を選択します。

ロールを作成すると、「マネージドノードレポートのダウンロードまたはエクスポート」の手順を実行する際にそのロールを選択できるようになります。

ノードレポートのコンテンツと外観の管理

Systems Manager の [ノードの探索] 機能を使用して、Systems Manager コンソールで、AWS 組織またはアカウント内のマネージドノードのフィルタリングされた/フィルタリングされていないリストを表示できます。ノードのリストに含めるフィールドとして、[ノード ID]、[オペレーティングシステム名]、[リージョン] など、多数のフィールドから選択できます。また、リストやレポートの列の順序を変更したり、コンソールでのリストの表示方法を変更したりすることもできます。

ノードレポートのコンテンツと外観を管理する手順

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。

2. ナビゲーションペインで、[ノードの探索] を選択します。
3. [ノード] 領域で、設定の歯車アイコン
   ( )
   を選択します。
4. [設定] ダイアログボックスで、以下の操作を実行します。
   a. [ページサイズ] で、各コンソールビュー表示に含める行数 (10、25、または 50) を選択します。
   b. [改行] でボックスを選択すると、セルのすべてのコンテンツが使用可能な列幅で表示されます。
   c. [ストライプ行] でボックスを選択すると、背景が透明な行と網掛けの行が交互に表示されます。
   d. [表示するコンテンツを選択] で、以下の操作を実行します。
      - リスト表示とレポートの個々の列のオン/オフを設定します。
      - 列の順序を変更するには、列名のドラッグハンドル
        ( )
        をクリックしたまま、リスト内で上下にドラッグします。
5. [確認] を選択してください。

Systems Manager を使用したジャストインタイムノードアクセス

Systems Manager では、ジャストインタイムアクセスをサポートすることで、ノードのセキュリティを強化できます。ジャストインタイムノードアクセスを使用すると、ユーザーがノードへの期限付きの一時的なアクセスをリクエストできるようになり、アクセスが本当に必要な場合にのみリクエストを承認できます。そのため、IAM ポリシーで管理するノードへの長期的なアクセスを付与する必要がなくなります。また、Systems Manager では Windows Server ノードへの RDP セッションを記録できるので、コンプライアンス要件を満たす、根本原因を分析するといったことができるようになります。ジャストインタイムノードアクセスを使用するには、Systems Manager 統合コンソールをセットアップする必要があります。

ジャストインタイムノードアクセスを使用するときは、許可したユーザーのみがノードへのアクセスリクエストを送信できるようにきめ細かく IAM ポリシーを作成します。次に、承認ポリシーを作成して、ノードへの接続に必要な承認を定義します。ジャストインタイムノードアクセス用のポリシーには、自動承認ポリシーと手動承認ポリシーがあります。自動承認ポリシーでは、ユーザーが自動的

に接続できるノードを定義します。手動承認ポリシーでは、指定したノードにアクセスするために必要な手動承認の数とレベルを定義します。このほか、アクセス拒否ポリシーも作成できます。アクセス拒否ポリシーを使用すると、指定したノードへのアクセスリクエストの自動承認を明示的に防ぐことができます。アクセス拒否ポリシーは、AWS Organizations 組織内のすべてのアカウントに適用されます。自動承認ポリシーと手動承認ポリシーは、作成元の AWS アカウントと AWS リージョンにのみ適用されます。

ノードに接続しようとすると、ユーザーはノードにアクセスする理由を入力するように求められます。次に、承認ポリシーが評価されます。ポリシーに応じて、ユーザーがターゲットノードに自動的に接続するか、Systems Manager がリクエスタに代わって手動承認リクエストを自動的に作成します。その後、ノードに適用される手動承認ポリシーに定められた承認者にアクセスリクエストに関する通知が届き、承認者はリクエストを承認または拒否できます。承認者とリクエスタへの通知には E メールを使用できるほか、チャットアプリケーションを Slack や Microsoft Teams と統合していれば Amazon Q Developer からも行えます。Systems Manager がリクエストされたノードへのアクセスを許可するのは、指定された承認者から必要なすべての承認が得られたときだけです。必要なすべての承認が得られたら、ユーザーは承認ポリシーに指定されているアクセス時間帯が終了するまで必要な数だけノードへのセッションを開始できます。Systems Manager は、ジャストインタイムノードアクセスセッションを自動的には終了しません。セッション設定で最大セッション期間とアイドルセッションタイムアウトの値を指定するのがベストプラクティスです。これらの値を設定すると、ユーザーは承認されたアクセス時間帯を超えてノードに接続したままにすることができなくなります。

重要度の高いデータがあるノードは保護し、重要度の低いノードは介入なしでユーザーの接続を許可するように、承認ポリシーをいくつか組み合わせて使用することをお勧めします。例えば、データベースノードへのアクセスリクエストには手動承認を義務づけ、永続的でないプレゼンテーション層のノードへのセッションは自動承認します。

Systems Manager は、IAM Identity Center または IAM とフェデレートされたユーザーに対してジャストインタイムノードアクセスをサポートしています。アクセスリクエストを送信するときに、フェデレーションユーザーはターゲットノード、およびノードへの接続が必要な理由を指定します。Systems Manager は、組織の承認ポリシーに定義されているパラメータとユーザーの ID を比較します。自動承認ポリシーの条件が満たされるか、承認者が手動で承認を与えると、リクエスタはターゲットノードに接続できます。ユーザーが承認されたノードへの接続を試みると、Systems Manager は一時的なトークンを作成し、それを使用してセッションを確立します。

Systems Manager サービスがアクセスリクエストの認証とセッションの確立を担当するため、IAM ポリシーを使用してノードへのアクセスを管理する必要はありません。Systems Manager ではジャストインタイムノードアクセスを使用することで、Zero Standing Privileges に近いアプローチを

取ることができます。ユーザーにノードへの永続的なアクセス許可を与えてセッションの開始を許可するのではなく、アクセスリクエストの作成を許可するだけでよくなります。コンプライアンス要件の遵守を支援するため、Systems Manager はすべてのアクセスリクエストを 1 年間保持します。Systems Manager はこのほか、ジャストインタイムノードアクセスに関する EventBridge イベントを発行して、アクセスリクエストの失敗に備え、手動承認のアクセスリクエストのステータスを更新できるようにします。詳細については、「Amazon EventBridge を使用して Systems Manager イベントをモニタリングする」を参照してください。

トピック

- Systems Manager でジャストインタイムアクセスをセットアップする
- ジャストインタイムノードアクセスセッションを開始する
- ジャストインタイムアクセスリクエストを管理する
- Session Manager からジャストインタイムノードアクセスに移行する
- Systems Manager でジャストインタイムアクセスを無効にする
- ジャストインタイムノードアクセスに関するよくある質問

Systems Manager でジャストインタイムアクセスをセットアップする

Systems Manager でジャストインタイムノードアクセスをセットアップするには、複数のステップが必要です。まず、ジャストインタイムノードアクセスをセットアップするターゲットを選択します。ターゲットは、AWS Organizations 組織単位 (OU) と AWS リージョンで構成されています。デフォルトでは、Systems Manager 統合コンソールをセットアップするときに選択したのと同じターゲットがジャストインタイムノードアクセスにも選択されます。ジャストインタイムノードアクセスは、同じすべてのターゲットにセットアップすることも、Systems Manager 統合コンソールをセットアップするときに指定したターゲットのサブセットにセットアップすることもできます。Systems Manager 統合コンソールをセットアップするときに選択されなかったターゲットを新たに追加する機能はサポートされていません。

次に、承認ポリシーを作成して、どのようなときにノード接続に手動承認が必要になるのか、どのようなときにノード接続を自動的に承認するのかを決定します。承認ポリシーは、組織内の各アカウントで管理されます。また、委任された管理者アカウントからのポリシーを共有して、特定のノードへの接続の自動承認を明示的に拒否することもできます。

> **Note**
>
> ジャストインタイムノードアクセスをセットアップしても、Session Manager に対して設定した既存の IAM ポリシーや設定には影響しません。ユーザーがノードへの接続を試みたときにジャストインタイムノードアクセスのみが使用されるようにするには、IAM ポリシーに規定された `StartSession` などの Session Manager アクションに対するアクセス許可を削除する必要があります。ジャストインタイムノードアクセスをセットアップしたら、Session Manager に対するアクセス許可を削除する前に、ユーザーとノードのサブセットで承認ポリシーをテストして、ポリシーが想定通りに機能していることを確認することをお勧めします。

以下の IAM ポリシーは、ユーザーが Systems Manager でノードへのジャストインタイムノードアクセスリクエストを作成することを管理および許可するために必要なアクセス許可の概要を示しています。Systems Manager でジャストインタイムノードアクセスを使用するために必要なアクセス許可が付与されていることを確認したら、セットアッププロセスを続行できます。各#############をユーザー自身の情報に置き換えます。

ジャストインタイムノードアクセスを有効にするための IAM ポリシー

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "QuickSetupConfigurationManagers",
            "Effect": "Allow",
            "Action": [
                "ssm-quicksetup:CreateConfigurationManager",
                "ssm-quicksetup:DeleteConfigurationManager",
                "ssm-quicksetup:GetConfiguration",
                "ssm-quicksetup:GetConfigurationManager",
                "ssm-quicksetup:GetServiceSettings",
                "ssm-quicksetup:ListConfigurationManagers",
                "ssm-quicksetup:ListConfigurations",
                "ssm-quicksetup:ListQuickSetupTypes",
                "ssm-quicksetup:ListTagsForResource",
                "ssm-quicksetup:TagResource",
                "ssm-quicksetup:UntagResource",
                "ssm-quicksetup:UpdateConfigurationDefinition",
                "ssm-quicksetup:UpdateConfigurationManager",
                "ssm-quicksetup:UpdateServiceSettings"
```

```
            ],
            "Resource": "*"
        },
        {
            "Sid": "QuickSetupDeployments",
            "Effect": "Allow",
            "Action": [
                "cloudformation:DescribeStackSetOperation",
                "cloudformation:ListStacks",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackResources",
                "cloudformation:ListStackSetOperations",
                "cloudformation:ListStackInstances",
                "cloudformation:DescribeStackSet",
                "cloudformation:ListStackSets",
                "cloudformation:DescribeStackInstance",
                "cloudformation:DescribeOrganizationsAccess",
                "cloudformation:ActivateOrganizationsAccess",
                "cloudformation:GetTemplate",
                "cloudformation:ListStackSetOperationResults",
                "cloudformation:DescribeStackEvents",
                "cloudformation:UntagResource",
                "ssm:DescribeAutomationExecutions",
                "ssm:GetAutomationExecution",
                "ssm:ListAssociations",
                "ssm:DescribeAssociation",
                "ssm:GetDocument",
                "ssm:ListDocuments",
                "ssm:DescribeDocument",
                "ssm:GetOpsSummary",
                "organizations:DeregisterDelegatedAdministrator",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListRoots",
                "organizations:ListParents",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:DescribeOrganizationalUnit",
                "organizations:ListAWSServiceAccessForOrganization",
                "iam:ListRoles",
                "iam:ListRolePolicies",
                "iam:GetRole",
                "iam:CreatePolicy",
                "cloudformation:TagResource"
```

```
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:RollbackStack",
                "cloudformation:CreateStack",
                "cloudformation:UpdateStack",
                "cloudformation:DeleteStack"
            ],
            "Resource": [
                "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-JITNA*",
                "arn:aws:cloudformation:*:*:stack/AWS-QuickSetup-*",
                "arn:aws:cloudformation:*:*:type/resource/*",
                "arn:aws:cloudformation:*:*:stack/StackSet-SSMQuickSetup"
            ]
        },
        {
            "Sid": "StackSetOperations",
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStackSet",
                "cloudformation:UpdateStackSet",
                "cloudformation:DeleteStackSet",
                "cloudformation:DeleteStackInstances",
                "cloudformation:CreateStackInstances",
                "cloudformation:StopStackSetOperation"
            ],
            "Resource": [
                "arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-JITNA*",
                "arn:aws:cloudformation:*:*:type/resource/*",
                "arn:aws:cloudformation:*:*:stackset-target/AWS-QuickSetup-JITNA*:*"
            ]
        },
        {
            "Sid": "IamRolesMgmt",
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:GetRole",
                "iam:AttachRolePolicy",
                "iam:PutRolePolicy",
```

```
                "iam:DetachRolePolicy",
                "iam:GetRolePolicy",
                "iam:ListRolePolicies"
            ],
            "Resource": [
                "arn:aws:iam::*:role/AWS-QuickSetup-JITNA*",
                "arn:aws:iam::*:role/service-role/AWS-QuickSetup-JITNA*"
            ]
        },
        {
            "Sid": "IamPassRole",
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/AWS-QuickSetup-JITNA*",
                "arn:aws:iam::*:role/service-role/AWS-QuickSetup-JITNA*"
            ],
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "ssm.amazonaws.com",
                        "ssm-quicksetup.amazonaws.com",
                        "cloudformation.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "SSMAutomationExecution",
            "Effect": "Allow",
            "Action": "ssm:StartAutomationExecution",
            "Resource": "arn:aws:ssm:region:account id:automation-definition/AWS-
EnableExplorer:*"
        },
        {
            "Sid": "SSMAssociationPermissions",
            "Effect": "Allow",
            "Action": [
            "ssm:DeleteAssociation",
            "ssm:CreateAssociation",
            "ssm:StartAssociationsOnce"
            ],
```

```
            "Resource": "arn:aws:ssm:region:account id:association/*"
        },
        {
            "Sid": "SSMResourceDataSync",
            "Effect": "Allow",
            "Action": [
                "ssm:CreateResourceDataSync",
                "ssm:UpdateResourceDataSync"
            ],
            "Resource": "arn:aws:ssm:region:account-id:resource-data-sync/AWS-
QuickSetup-*"
        },
        {
            "Sid": "ListResourceDataSync",
            "Effect": "Allow",
            "Action": [
                "ssm:ListResourceDataSync"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateServiceLinkedRoles",
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": [
                        "accountdiscovery.ssm.amazonaws.com",
                        "ssm.amazonaws.com",
                        "ssm-quicksetup.amazonaws.com",
                        "stacksets.cloudformation.amazonaws.com"
                    ]
                }
            },
            "Resource": "*"
        },
        {
            "Sid": "CreateStackSetsServiceLinkedRole",
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
```

```
            "Resource": "arn:aws:iam::*:role/aws-service-role/
stacksets.cloudformation.amazonaws.com/
AWSServiceRoleForCloudFormationStackSetsOrgAdmin"
        },
        {
            "Sid": "AllowSsmJitnaPoliciesCrudOperations",
            "Effect": "Allow",
            "Action": [
                "ssm:CreateDocument",
                "ssm:UpdateDocument",
                "ssm:UpdateDocumentDefaultVersion",
                "ssm:GetDocument",
                "ssm:DescribeDocument",
                "ssm:DeleteDocument"
            ],
            "Resource": [
                "arn:aws:ssm:region:account id:document/SSM-
JustInTimeAccessDenyAccessOrgPolicy"
            ],
            "Condition": {
                "StringEquals": {
                    "ssm:DocumentType": [
                        "AutoApprovalPolicy"
                    ]
                }
            }
        },
        {
            "Sid": "AllowAccessRequestOpsItemOperations",
            "Effect": "Allow",
            "Action": [
                "ssm:GetOpsItem",
                "ssm:DescribeOpsItems",
                "ssm:GetOpsSummary",
                "ssm:DeleteOpsItem",
                "ssm:ListOpsItemEvents"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IdentityCenterPermissions",
            "Effect": "Allow",
            "Action": [
                "sso:DescribeRegisteredRegions",
```

```
                "sso:ListDirectoryAssociations",
                "identitystore:GetUserId",
                "identitystore:DescribeUser",
                "identitystore:DescribeGroup",
                "identitystore:ListGroupMembershipsForMember"
            ],
            "Resource": "*"
        }
    ]
}
```

ジャストインタイムノードアクセスを設定するための IAM ポリシー

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSsmJitnaPoliciesCrudOperations",
            "Effect": "Allow",
            "Action": [
                "ssm:CreateDocument",
                "ssm:UpdateDocument",
                "ssm:UpdateDocumentDefaultVersion",
                "ssm:GetDocument",
                "ssm:DescribeDocument",
                "ssm:DeleteDocument"
            ],
            "Resource": [
                "arn:aws:ssm:region:account id:document/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ssm:DocumentType": [
                        "ManualApprovalPolicy",
                        "AutoApprovalPolicy"
                    ]
                }
            }
        },
        {
            "Sid": "AllowSsmJitnaPoliciesListOperations",
            "Effect": "Allow",
            "Action": [
```

```
                "ssm:ListDocuments",
                "ssm:ListDocumentVersions"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::account id:role/SSM-JustInTimeAccessTokenRole",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "justintimeaccess.ssm.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "AllowAccessRequestOpsItemOperations",
            "Effect": "Allow",
            "Action": [
                "ssm:GetOpsItem",
                "ssm:DescribeOpsItems",
                "ssm:GetOpsSummary",
                "ssm:DeleteOpsItem",
                "ssm:ListOpsItemEvents"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowSessionManagerPreferencesOperation",
            "Effect": "Allow",
            "Action": [
                "ssm:CreateDocument",
                "ssm:GetDocument",
                "ssm:DescribeDocument",
                "ssm:UpdateDocument",
                "ssm:DeleteDocument"
            ],
            "Resource": "arn:aws:ssm:region:account id:document/SSM-
SessionManagerRunShell",
            "Condition": {
                "StringEquals": {
                    "ssm:DocumentType": "Session"
```

```
                }
            }
        },
        {
            "Sid": "AllowSessionManagerOperations",
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeSessions",
                "ssm:GetConnectionStatus",
                "ssm:TerminateSession"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowRDPConnectionRecordingOperations",
            "Effect": "Allow",
            "Action": [
                "ssm-guiconnect:UpdateConnectionRecordingPreferences",
                "ssm-guiconnect:GetConnectionRecordingPreferences",
                "ssm-guiconnect:DeleteConnectionRecordingPreferences"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowRDPConnectionRecordingKmsOperation",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant"
            ],
            "Resource": "arn:aws:kms:region:account id:key/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged": "true"
                },
                "StringLike": {
                    "kms:ViaService": "ssm-guiconnect.*.amazonaws.com"
                },
                "Bool": {
                    "aws:ViaAWSService": "true"
                }
            }
        },
        {
            "Sid": "AllowFleetManagerOperations",
```

```
            "Effect": "Allow",
            "Action": [
                "ssm-guiconnect:GetConnection",
                "ssm-guiconnect:ListConnections"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SNSTopicManagement",
            "Effect": "Allow",
            "Action": [
                "sns:CreateTopic",
                "sns:SetTopicAttributes"
            ],
            "Resource": [
                "arn:aws:sns:region:account id:SSM-JITNA*"
            ]
        },
        {
            "Sid": "SNSListTopics",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Sid": "EventBridgeRuleManagement",
            "Effect": "Allow",
            "Action": [
                "events:PutRule",
                "events:PutTargets"
            ],
            "Resource": [
                "arn:aws:events:region:account id:rule/SSM-JITNA*"
            ]
        },
        {
            "Sid": "ChatbotSlackManagement",
            "Effect": "Allow",
            "Action": [
                "chatbot:CreateSlackChannelConfiguration",
                "chatbot:UpdateSlackChannelConfiguration",
                "chatbot:DescribeSlackChannelConfigurations",
```

```
                "chatbot:DescribeSlackWorkspaces",
                "chatbot:DeleteSlackChannelConfiguration",
                "chatbot:RedeemSlackOauthCode",
                "chatbot:DeleteSlackWorkspaceAuthorization",
                "chatbot:GetSlackOauthParameters"

            ],
            "Resource": "*"
        },
        {
            "Sid": "ChatbotTeamsManagement",
            "Effect": "Allow",
            "Action": [
                "chatbot:ListMicrosoftTeamsChannelConfigurations",
                "chatbot:CreateMicrosoftTeamsChannelConfiguration",
                "chatbot:UpdateMicrosoftTeamsChannelConfiguration",
                "chatbot:ListMicrosoftTeamsConfiguredTeams",
                "chatbot:DeleteMicrosoftTeamsChannelConfiguration",
                "chatbot:RedeemMicrosoftTeamsOauthCode",
                "chatbot:DeleteMicrosoftTeamsConfiguredTeam",
                "chatbot:GetMicrosoftTeamsOauthParameters",
                "chatbot:TagResource"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SSMEmailSettings",
            "Effect": "Allow",
            "Action": [
                "ssm:UpdateServiceSetting",
                "ssm:GetServiceSetting"
            ],
            "Resource": [
                "arn:aws:ssm:region:account id:servicesetting/ssm/access-request/email-
role-mapping",
                "arn:aws:ssm:region:account id:servicesetting/ssm/access-request/
enabled-email-notifications"
            ]
        },
        {
            "Sid": "AllowViewingJitnaCloudWatchMetrics",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:GetMetricData",
```

```
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:ListMetrics"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/SSM/JustInTimeAccess"
                }
            }
        },
        {
            "Sid": "QuickSetupConfigurationManagers",
            "Effect": "Allow",
            "Action": [
                "ssm-quicksetup:ListConfigurationManagers",
                "ssm-quicksetup:ListConfigurations",
                "ssm-quicksetup:ListQuickSetupTypes",
                "ssm-quicksetup:GetConfiguration",
                "ssm-quicksetup:GetConfigurationManager"
            ],
            "Resource": "*"
        },
        {
            "Sid": "QuickSetupDeployments",
            "Effect": "Allow",
            "Action": [
                "cloudformation:ListStacks",
                "cloudformation:DescribeStacks",
                "organizations:DescribeOrganization",
                "organizations:ListDelegatedAdministrators"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ManualPolicy",
            "Effect": "Allow",
            "Action": [
                "sso:DescribeRegisteredRegions",
                "ssm:GetServiceSetting",
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
```

```
            "Sid": "SessionPreference",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowIamListForKMS",
            "Effect": "Allow",
            "Action": [
                "iam:ListUsers"
            ],
            "Resource": "arn:aws:iam::account id:user/*"
        },
        {
            "Sid": "KMSPermission",
            "Effect": "Allow",
            "Action": [
                "kms:TagResource",
                "kms:ListAliases",
                "kms:CreateAlias"
            ],
            "Resource": "*"
        },
        {
            "Sid": "KMSCreateKey",
            "Effect": "Allow",
            "Action": [
                "kms:CreateKey"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged": "true"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "SystemsManagerJustInTimeNodeAccessManaged"
                    ]
                }
            }
        },
        {
```

```
            "Sid": "AllowIamRoleForChatbotAction",
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "arn:aws:iam::account id:role/role name",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "chatbot.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid": "AllowIamServiceRoleForChat",
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::account id:role/aws-service-role/
management.chatbot.amazonaws.com/AWSServiceRoleForAWSChatbot"
        },
        {
            "Sid": "CloudWatchLogs",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups"
            ],
            "Resource": "arn:aws:logs:*:account id:log-group::log-stream:"
        },
        {
            "Sid": "IdentityStorePermissions",
            "Effect": "Allow",
            "Action": [
                "sso:ListDirectoryAssociations",
                "identitystore:GetUserId",
                "sso-directory:SearchUsers",
                "sso-directory:SearchGroups",
                "identitystore:DescribeGroup",
                "identitystore:DescribeUser"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

アクセスリクエスト承認者用の IAM ポリシー

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAccessRequestDescriptions",
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeOpsItems",
                "ssm:GetOpsSummary",
                "ssm:ListOpsItemEvents"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowGetSpecificAccessRequest",
            "Effect": "Allow",
            "Action": [
                "ssm:GetOpsItem"
            ],
            "Resource": "arn:aws:ssm:region:account id:opsitem/*"
        },
        {
            "Sid": "AllowApprovalRejectionSignal",
            "Effect": "Allow",
            "Action": [
                "ssm:SendAutomationSignal"
            ],
            "Resource": "arn:aws:ssm:*:*:automation-execution/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged": "true"
                }
            }
        },
        {
            "Sid": "QuickSetupConfigurationManagers",
            "Effect": "Allow",
            "Action": [
```

```
                "ssm-quicksetup:ListConfigurationManagers",
                "ssm-quicksetup:ListConfigurations",
                "ssm-quicksetup:GetConfigurationManager",
                "ssm-quicksetup:ListQuickSetupTypes",
                "ssm-quicksetup:GetConfiguration"
            ],
            "Resource": "*"
        },
        {
            "Sid": "QuickSetupDeployments",
            "Effect": "Allow",
            "Action": [
                "cloudformation:ListStacks",
                "cloudformation:DescribeStacks",
                "organizations:DescribeOrganization",
                "organizations:ListDelegatedAdministrators"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowSsmJitnaPoliciesCrudOperations",
            "Effect": "Allow",
            "Action": [
                "ssm:GetDocument",
                "ssm:DescribeDocument"
            ],
            "Resource": [
                "arn:aws:ssm:region:account id:document/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ssm:DocumentType": [
                        "ManualApprovalPolicy",
                        "AutoApprovalPolicy"
                    ]
                }
            }
        },
        {
            "Sid": "AllowSsmJitnaPoliciesListOperations",
            "Effect": "Allow",
            "Action": [
                "ssm:ListDocuments",
                "ssm:ListDocumentVersions"
```

```
            ],
            "Resource": "*"
        },
        {
            "Sid": "IDCPermissions",
            "Effect": "Allow",
            "Action": [
                "sso:DescribeRegisteredRegions",
                "sso:ListDirectoryAssociations",
                "identitystore:GetUserId",
                "identitystore:DescribeUser",
                "identitystore:DescribeGroup",
                "identitystore:ListGroupMembershipsForMember"
            ],
            "Resource": "*"
        }
    ]
}
```

ジャストインタイムノードアクセスユーザー用の IAM ポリシー

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "AllowJITNAOperations",
            "Effect": "Allow",
            "Action": [
                "ssm:StartAccessRequest",
                "ssm:GetAccessToken"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowOpsItemCreationAndRetrieval",
            "Effect": "Allow",
            "Action": [
                "ssm:CreateOpsItem",
                "ssm:GetOpsItem"
            ],
            "Resource": "arn:aws:ssm:*:*:opsitem/*"
        },
        {
            "Sid": "AllowListAccessRequests",
```

```
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeOpsItems",
                "ssm:GetOpsSummary",
                "ssm:ListOpsItemEvents",
                "ssm:DescribeSessions"
            ],
            "Resource": "*"
        },
        {
            "Sid": "RequestManualApprovals",
            "Action": "ssm:StartAutomationExecution",
            "Effect": "Allow",
            "Resource": "arn:aws:ssm:*:*:document/*",
            "Condition": {
                "StringEquals": {
                    "ssm:DocumentType": "ManualApprovalPolicy"
                }

            }
        },
        {
            "Sid": "StartManualApprovalsAutomationExecution",
            "Effect": "Allow",
            "Action": "ssm:StartAutomationExecution",
            "Resource": "arn:aws:ssm:*:*:automation-execution/*"
        },
        {
            "Sid": "AllowManualApprovalAutomationExecutionTagging",
            "Effect": "Allow",
            "Action": [
                "ssm:AddTagsToResource"
            ],
            "Resource": [
                "arn:aws:ssm:*:*:automation-execution/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/SystemsManagerJustInTimeNodeAccessManaged": "true"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "SystemsManagerJustInTimeNodeAccessManaged"
                    ]
```

```
                }
            }
        },
        {
            "Sid": "CancelAccessRequestManualApproval",
            "Effect": "Allow",
            "Action": "ssm:StopAutomationExecution",
            "Resource": "arn:aws:ssm:*:*:automation-execution/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/SystemsManagerJustInTimeNodeAccessManaged": "true"
                }
            }
        },
        {
            "Sid": "DescribeEC2Instances",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeTags",
                "ec2:GetPasswordData"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowListSSMManagedNodesAndTags",
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeInstanceInformation",
                "ssm:ListTagsForResource"
            ],
            "Resource": "*"
        },
        {
            "Sid": "QuickSetupConfigurationManagers",
            "Effect": "Allow",
            "Action": [
                "ssm-quicksetup:ListConfigurationManagers",
                "ssm-quicksetup:GetConfigurationManager",
                "ssm-quicksetup:ListConfigurations",
                "ssm-quicksetup:ListQuickSetupTypes",
                "ssm-quicksetup:GetConfiguration"
            ],
            "Resource": "*"
```

```
        },
        {
            "Sid": "AllowSessionManagerOperations",
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeSessions",
                "ssm:GetConnectionStatus"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowRDPOperations",
            "Effect": "Allow",
            "Action": [
                "ssm-guiconnect:ListConnections",
                "ssm:GetConnectionStatus"
            ],
            "Resource": "*"
        },
        {
            "Sid": "QuickSetupDeployments",
            "Effect": "Allow",
            "Action": [
                "cloudformation:ListStacks",
                "cloudformation:DescribeStacks",
                "organizations:DescribeOrganization",
                "organizations:ListDelegatedAdministrators"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowSsmJitnaPoliciesReadOnly",
            "Effect": "Allow",
            "Action": [
                "ssm:GetDocument",
                "ssm:DescribeDocument"
            ],
            "Resource": [
                "arn:aws:ssm:*:account id:document/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ssm:DocumentType": [
                        "ManualApprovalPolicy",
```

```
                        "AutoApprovalPolicy"
                    ]
                }
            }
        },
        {
            "Sid": "AllowSsmJitnaPoliciesListOperations",
            "Effect": "Allow",
            "Action": [
                "ssm:ListDocuments",
                "ssm:ListDocumentVersions"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ExploreNodes",
            "Effect": "Allow",
            "Action": [
                "ssm:ListNodesSummary",
                "ssm:ListNodes",
                "ssm:DescribeInstanceProperties"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IdentityStorePermissions",
            "Effect": "Allow",
            "Action": [
                "sso:DescribeRegisteredRegions",
                "sso:ListDirectoryAssociations",
                "identitystore:GetUserId",
                "identitystore:DescribeUser",
                "identitystore:DescribeGroup"
            ],
            "Resource": "*"
        }
    ]
}
```

> **Note**
>
> 承認ポリシーを作成、更新、または削除する API オペレーションへのアクセスを制限するには、AutoApprovalPolicy と ManualApprovalPolicy のドキュメントタイ

プに対して ssm:DocumentType 条件キーを使用します。StartAccessRequest と GetAccessToken のどちらの API オペレーションも、以下のグローバルコンテキストキーをサポートしません。

- aws:ViaAwsService
- aws:MultiFactorAuthPresent
- aws:SourceVpce
- aws:UserAgent

Systems Manager の条件コンテキストキーの詳細については、「サービス許可リファレンス」の「Condition keys for AWS Systems Manager」を参照してください。

以下の手順では、ジャストインタイムノードアクセスの最初のセットアップステップを完了する方法について説明します。

ジャストインタイムノードアクセスをセットアップするには

1. 組織用の Systems Manager 委任管理者アカウントにログインします。
2. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
3. ナビゲーションペインで、[ジャストインタイムノードアクセス] を選択します。
4. [新しいエクスペリエンスを有効にする] を選択します。
5. ジャストインタイムノードアクセスを有効にするリージョンを選択します。デフォルトでは、Systems Manager 統合コンソールをセットアップするときに選択したのと同じリージョンがジャストインタイムノードアクセスにも選択されます。Systems Manager 統合コンソールをセットアップするときに選択されなかったリージョンを新たに選択する機能はサポートされていません。
6. [ジャストインタイムノードアクセスを有効にする] を選択します。

この機能を有効にしてから 30 日間、ジャストインタイムノードアクセスは無料で使用できます。30 日間のトライアル期間が過ぎると、ジャストインタイムノードアクセスの使用には料金がかかります。詳細については、AWS Systems Manager 料金を参照してください。

ノードの承認ポリシーを作成する

承認ポリシーでは、ユーザーがノードにアクセスするために必要な承認を定義します。ジャストインタイムノードアクセスでは、IAM ポリシーを通じたノードへの長期的なアクセス許可が不要になるため、ノードへのアクセスを許可する承認ポリシーを作成する必要があります。ノードに適用される承認ポリシーがない場合、ユーザーはノードへのアクセスをリクエストできません。

ジャストインタイムノードアクセスには、3 つのポリシータイプがあります。このポリシータイプは、自動承認、アクセス拒否、および手動承認です。

ジャストインタイムノードアクセスポリシータイプ

- 自動承認ポリシーでは、ユーザーが自動的に接続できるノードを定義します。
- 手動承認ポリシーでは、指定したノードにアクセスするために必要な手動承認の数とレベルを定義します。
- アクセス拒否ポリシーを使用すると、指定したノードへのアクセスリクエストの自動承認を明示的に防ぐことができます。

アクセス拒否ポリシーは、AWS Organizations 組織内のすべてのアカウントに適用されます。例えば、`Production` キーでタグ付けされたノードに対して、`Intern` グループの自動承認を明示的に拒否できます。自動承認ポリシーと手動承認ポリシーは、作成元の AWS アカウントと AWS リージョンにのみ適用されます。組織内の各メンバーアカウントが、独自の承認ポリシーを管理します。承認ポリシーは次の順序で評価されます。

1. アクセス拒否
2. 自動承認
3. 手動

組織ごとに 1 つのアクセス拒否ポリシー、アカウントとリージョンごとに 1 つの自動承認ポリシーのみを持つことができますが、アカウントには複数の手動承認ポリシーがある可能性があります。手動承認ポリシーを評価する場合、ジャストインタイムノードアクセスでは、ノードのより具体的なポリシーが常に優先されます。手動承認ポリシーは次の順序で評価されます。

1. タグの具体的なターゲット
2. すべてのノードのターゲット

例えば、Demo キーでタグ付けされたノードがあるとします。同じアカウントに、すべてのノードをターゲットとする手動承認ポリシーがあり、1 つのレベルからの 1 つの承認が必要です。また、Demo キーでタグ付けされたノードには、2 つのレベルからの 2 つの承認を必要とする手動承認ポリシーもあります。Systems Manager は、Demo タグをターゲットとするポリシーをノードに適用します。このポリシーが、すべてのノードをターゲットとするポリシーよりも具体的であるためです。これにより、アカウント内のすべてのノードの一般的なポリシーを作成し、ユーザーがアクセスリクエストを送信できるようにしながら、必要に応じてより詳細なポリシーを作成できます。

組織によっては、ノードに複数のタグが適用される場合があります。このシナリオでは、ノードに複数の手動承認ポリシーが適用されると、アクセスリクエストは失敗します。例えば、ノードに Production および Database キーがタグ付けされているとします。同じアカウントに、Production キーでタグ付けされたノードに適用される手動承認ポリシーと、Database キーでタグ付けされたノードに適用される別の手動承認ポリシーがあります。その結果、両方のキーでタグ付けされたノードで競合が発生し、アクセスリクエストが失敗します。Systems Manager は、失敗したリクエストにユーザーをリダイレクトします。ここでは、競合しているポリシーとタグの詳細を表示して、必要なアクセス許可がある場合は必要な調整を行うことができます。そうでない場合は、ポリシーを変更するために必要なアクセス許可を持つ組織内の同僚に通知できます。アクセスリクエストの失敗につながるポリシーの競合は EventBridge イベントを出力するため、独自のレスポンスワークフローを柔軟に構築できます。さらに、Systems Manager はアクセスリクエストの失敗につながるポリシーの競合に関する E メール通知を指定された受信者に送信します。ポリシーの競合用の E メール通知の設定の詳細については、「ジャストインタイムアクセスリクエストに関する通知を設定する」を参照してください。

アクセス拒否ポリシーでは、Cedar ポリシー言語を使用して、ユーザーが組織内で明示的に自動的に接続できないノードを定義します。このポリシーは、組織の委任管理者アカウントから作成および共有されます。アクセス拒否ポリシーは、すべての自動承認ポリシーよりも優先されます。組織ごとに 1 つのアクセス拒否ポリシーのみを持つことができます。

自動承認ポリシーでは、Cedar ポリシー言語を使用して、手動承認なしで指定されたノードに自動的に接続できるユーザーを定義します。自動的に承認されるアクセスリクエストのアクセス期間は 1 時間です。この値は変更できません。アカウントとリージョンごとに 1 つの自動承認ポリシーのみを持つことができます。

手動承認ポリシーでは、アクセス期間、必要な承認レベル数、レベルごとに必要な承認者の数、ジャストインタイムアクセスリクエストを承認できるノードを指定します。手動承認ポリシーのアクセス期間は 1～336 時間である必要があります。複数の承認レベルを指定した場合、アクセスリクエストの承認では一度に 1 つずつレベルが処理されます。つまり、承認プロセスが後続のレベルに移行する前に、1 つのレベルに必要なすべての承認が提供される必要があります。手動承認ポリシーで複

数のタグを指定した場合、and ステートメントではなく or ステートメントとして評価されます。例えば、タグ Application、Web、および Test を含む手動承認ポリシーを作成した場合、これらのキーのいずれかでタグ付けされたすべてのノードにポリシーが適用されます。3 つすべてのキーでタグ付けされたノードにのみポリシーが適用されるわけではありません。

手動ポリシーと自動承認ポリシーを組み合わせて使用して、より重要なデータがあるノードを保護しながら、重要度の低いノードにユーザーが介入なしで接続できるようにすることをお勧めします。例えば、データベースノードへのアクセスリクエストには手動承認を義務づけ、永続的でないプレゼンテーション層のノードへのセッションは自動承認します。

次の手順では、ジャストインタイムノードアクセス用の承認ポリシーを作成する方法について説明します。

トピック

- ジャストインタイムノードアクセス用の手動承認ポリシーを作成する
- 自動承認ポリシーとアクセス拒否ポリシーのステートメントの構造とビルトイン演算子
- ジャストインタイムノードアクセスの自動承認ポリシーを作成する
- ジャストインタイムノードアクセス用のアクセス拒否ポリシーを作成する
- Amazon Q を使用してジャストインタイムノードアクセスの承認ポリシーを作成する

ジャストインタイムノードアクセス用の手動承認ポリシーを作成する

以下の手順では、手動承認ポリシーを作成する方法について説明します。Systems Manager では、AWS アカウントと AWS リージョンごとに手動承認ポリシーを最大 50 個作成できます。

手動承認ポリシーを作成するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[ノードアクセスを管理] を選択します。
3. [手動承認ポリシーの作成] ステップの [ポリシーの詳細] セクションで、承認ポリシーの名前と説明を入力します。
4. [アクセス期間] の値を入力します。これは、アクセスリクエストの承認後にユーザーがノードへのセッションを開始できる最大時間です。1 ~ 336 の値で時間を指定する必要があります。
5. [ノードターゲット] セクションで、ポリシーを適用するノードに関連付けられたタグキーと値のペアを入力します。ポリシーに指定されているタグのいずれもノードに関連付けられていない場合、ポリシーはノードに適用されません。

6. [アクセスリクエスト承認者] セクションで、ポリシー内のノードターゲットへのアクセスリクエストを承認できるようにするユーザーまたはグループを入力します。アクセスリクエスト承認者にできるのは、IAM Identity Center ユーザーとグループ、または IAM ユーザーです。レベルごとに最大 5 人の承認者と、最大 5 レベルの承認者を指定できます。
7. [手動承認ポリシーの作成] を選択します。

自動承認ポリシーとアクセス拒否ポリシーのステートメントの構造とビルトイン演算子

次の表は、自動承認ポリシーとアクセス拒否ポリシーの構造を示しています。

コンポーネント	構文
effect	`permit | forbid`
scope	`(principal, action, resource)`
条件句	`when { principal or resource has attribute name };`

ポリシーの構成要素

自動承認ポリシーまたはアクセス拒否ポリシーには、次のコンポーネントが含まれます。

- 効果 - アクセスの `permit` (許可) または `forbid` (拒否)。
- スコープ - 効果を適用するプリンシパル、アクション、リソース。特定のプリンシパル、アクション、リソースを指定しないでおくと、Cedar のスコープを未定義のままにすることができます。この場合、ポリシーはすべてのプリンシパル、アクション、リソースに適用されます。ジャストインタイムノードアクセスの場合、`action` は常に `AWS::SSM::Action::"getTokenForInstanceAccess"` です。
- 条件句 - 効果が適用されるコンテキスト。

コメント

ポリシーにコメントを含めることができます。コメントは、`//` で始まり改行文字で終わる行として定義されます。

以下の例は、ポリシー内のコメントを示しています。

```
// Allows users in the Engineering group from the Platform org to automatically connect
 to nodes tagged with Engineering and Production keys.
permit (
    principal in AWS::IdentityStore::Group::"d4q81745-r081-7079-d789-14da1EXAMPLE",
    action == AWS::SSM::Action::"getTokenForInstanceAccess",
    resource
)
when {
    principal has organization && resource.hasTag("Engineering") &&
 resource.hasTag("Production") && principal.organization == "Platform"
};
```

複数の句

&& 演算子を使用すると、1 つのポリシーステートメントに複数の条件句を含めることができます。

```
// Allow access if node has tag where the tag key is Environment
// & tag value is Development

permit(principal, action == AWS::SSM::getTokenForInstanceAccess, resource)
when {
    resource.hasTag("Environment") &&
    resource.getTag("Environment") == "Development"
};
```

予約文字

次の例は、コンテキストのプロパティでポリシー言語の予約文字である：(セミコロン) が使用されている場合のポリシーの記述方法を示しています。

```
permit (
    principal,
    action == AWS::SSM::Action::"getTokenForInstanceAccess",
    resource
)
when {
    principal has employeeNumber && principal.employeeNumber like "E-1*" &&
 resource.hasTag("Purpose") && resource.getTag("Purpose") == "Testing"
}
```

その他の例については、「ポリシーステートメントの例」を参照してください。

ジャストインタイムノードアクセスのスキーマ

以下は、ジャストインタイムノードアクセス用の Cedar スキーマです。

```
namespace AWS::EC2 {
    entity Instance tags String;
}


namespace AWS::IdentityStore {
    entity Group;

    entity User in [Group] {
    employeeNumber?: String,
    costCenter?: String,
    organization?: String,
    division?: String,
    };

}


namespace AWS::IAM {

    entity Role;

    type AuthorizationContext = {
        principalTags: PrincipalTags,
    };

    entity PrincipalTags tags String;
}

namespace AWS::SSM {

    entity ManagedInstance tags String;

    action "getTokenForInstanceAccess" appliesTo {
    principal: [AWS::IdentityStore::User],
    resource: [AWS::EC2::Instance, AWS::SSM::ManagedInstance],
    context: {
        "iam": AWS::IAM::AuthorizationContext
```

```
        }
    };
}
```

ビルトイン演算子

さまざまな条件を使用して自動承認ポリシーまたはアクセス拒否ポリシーのコンテキストを作成する場合は、&& 演算子を使用して追加条件を指定できます。ポリシー条件にさらに表現力を加えるために使用できるビルトイン演算子は他にも多数あります。参照用にすべてのビルトイン演算子を下表に示します。

演算子	タイプとオーバーロード	説明
!	Boolean → Boolean	論理否定。
==	any → any	等価。タイプが一致しなくても、いずれかのタイプの引数で機能します。異なるタイプの値が互いに等しくなることはありません。
!=	any → any	不等価。等価の正反対 (上記参照)。
<	(long, long) → Boolean	Long integer less-than.
<=	(long, long) → Boolean	Long integer less-than-or-equal-to.
>	(long, long) → Boolean	Long integer greater-than.
>=	(long, long) → Boolean	Long integer greater-than-or-equal-to.
in	(entity, entity) → Boolean	階層メンバーシップ (再帰形：A の A は常にトゥルー)。
	(entity, set(entity)) → Boolean	階層メンバーシップ：(A and B) || (A in C) || であれば A in [B, C, ...] はトゥルー... セット

演算子	タイプとオーバーロード	説明
		に non-entity が含まれている場合はエラーになります。
&&	(Boolean, Boolean) → Boolean	Logical and (short-circuiting).
||	(Boolean, Boolean) → Boolean	Logical or (short-circuiting).
.exists()	entity → Boolean	Entity existence.
has	(entity, attribute) → Boolean	中置演算子。`e has f` レコードまたはエンティティに e 属性 f へのバインディングがあるかどうかをテストします。e が存在しないか、e が存在しても属性 f を持たない場合は `false` を返します。属性は識別子または文字列リテラルとして表現できます。
like	(string, string) → Boolean	中置演算子。`t like p` テキスト t がパターン p と一致するかどうかを確認します。パターンには、0 個以上の文字と一致するワイルドカード文字 * が含まれる場合があります。t のリテラルスター文字と一致させるには、p で特殊なエスケープ文字シーケンス * を使用できます。
.hasTag()	(entity, string) → Boolean	エンティティに指定されたタグが適用されているかどうかを確認します。
.getTag()	(entity, string) → Boolean	指定されたタグキーの値を返します。

演算子	タイプとオーバーロード	説明
.contains()	(set, any) → Boolean	メンバーシップ (B が A の要素かどうか) を設定します。
.containsAll()	(set, set) → Boolean	セット A にセット B のすべての要素が含まれているかどうかをテストします。
.containsAny()	(set, set) → Boolean	セット A にセット B の要素のいずれかが含まれているかどうかをテストします。

ポリシーステートメントの例

ポリシーステートメントの例を以下に示します。

```
// Users assuming IAM roles with a principal tag of "Elevated" can automatically access
 nodes tagged with the "Environment" key when the value equals "prod"
permit(principal, action == AWS::SSM::getTokenForInstanceAccess, resource)
when {
    // Verify IAM role principal tag
    context.iam.principalTags.getTag("AccessLevel") == "Elevated" &&

    // Verify the node has a tag with "Environment" tag key and a tag value of "prod"
    resource.hasTag("Environment") &&
    resource.getTag("Environment") == "prod"
};
```

```
// Identity Center users in the "Contractor" division can automatically access nodes
 tagged with the "Environment" key when the value equals "dev"
permit(principal, action == AWS::SSM::getTokenForInstanceAccess, resource)
when {
    // Verify that the user is part of the "Contractor" division
    principal.division == "Contractor" &&

    // Verify the node has a tag with "Environment" tag key and a tag value of "dev"
    resource.hasTag("Environment") &&
    resource.getTag("Environment") == "dev"
```

```
};
```

```
// Identity Center users in a specified group can automatically access nodes tagged
 with the "Environment" key when the value equals "Production"
permit(principal in AWS::IdentityStore::Group::"d4q81745-r081-7079-d789-14da1EXAMPLE",
    action == AWS::SSM::getTokenForInstanceAccess,
    resource)
when {
    resource.hasTag("Environment") &&
    resource.getTag("Environment") == "Production"
};
```

ジャストインタイムノードアクセスの自動承認ポリシーを作成する

自動承認ポリシーでは、Cedar ポリシー言語を使用して、どのユーザーが指定されたノードに手動承認なしで自動的に接続できるかを定義します。自動承認ポリシーには、principal と resource を指定する permit ステートメントがいくつか含まれています。各ステートメントには、自動承認の条件を定義する when 句があります。

次に、自動承認ポリシーの例を示します。

```
permit (
    principal in AWS::IdentityStore::Group::"e8c17310-e011-7089-d989-10da1EXAMPLE",
    action == AWS::SSM::Action::"getTokenForInstanceAccess",
    resource
)
when {
    principal has costCenter && resource.hasTag("CostCenter") && principal.costCenter
 == resource.getTag("CostCenter")
};

permit (
    principal in AWS::IdentityStore::Group::"d4q81745-r081-7079-d789-14da1EXAMPLE",
    action == AWS::SSM::Action::"getTokenForInstanceAccess",
    resource
)
when {
    principal has organization && resource.hasTag("Engineering") &&
 resource.hasTag("Production") && principal.organization == "Platform"
};
```

```
permit (
    principal,
    action == AWS::SSM::Action::"getTokenForInstanceAccess",
    resource
)
when {
    principal has employeeNumber && principal.employeeNumber like "E-1*" &&
 resource.hasTag("Purpose") && resource.getTag("Purpose") == "Testing"
};
```

以下の手順では、ジャストインタイムノードアクセス用に自動承認ポリシーを作成する方法について説明します。自動的に承認されるアクセスリクエストのアクセス期間は 1 時間です。この値は変更できません。AWS アカウントと AWS リージョンごとに自動承認ポリシーを 1 つのみ設定できます。ポリシーステートメントを作成する方法の詳細については、「自動承認ポリシーとアクセス拒否ポリシーのステートメントの構造とビルトイン演算子」を参照してください。

自動承認ポリシーを作成するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[ノードアクセスを管理] を選択します。
3. [承認ポリシー] タブで、[自動承認ポリシーを作成] を選択します。
4. [ポリシーステートメント] セクションに自動承認ポリシー用のポリシーステートメントを入力します。あらかじめ用意されている [サンプルステートメント] を使用すると、ポリシーを簡単に作成できます。
5. [自動承認ポリシーを作成] を選択します。

ジャストインタイムノードアクセス用のアクセス拒否ポリシーを作成する

アクセス拒否ポリシーでは、Cedar ポリシー言語を使用して、ユーザーが手動承認なしでどのノードに自動的には接続できないかを定義します。アクセス拒否ポリシーには、`principal` と `resource` を指定する `forbid` ステートメントがいくつか含まれています。各ステートメントには、自動承認を明示的に拒否する条件を定義する `when` 句があります。

次に、アクセス拒否ポリシーの例を示します。

```
forbid (
    principal in AWS::IdentityStore::Group::"e8c17310-e011-7089-d989-10da1EXAMPLE",
    action == AWS::SSM::Action::"getTokenForInstanceAccess",
```

```
    resource
)
when {
    resource.hasTag("Environment") && resource.getTag("Environment") == "Production"
};

forbid (
    principal,
    action == AWS::SSM::Action::"getTokenForInstanceAccess",
    resource
)
when {
    principal has division && principal.division != "Finance" &&
 resource.hasTag("DataClassification") && resource.getTag("DataClassification") ==
 "Financial"
};


forbid (
    principal,
    action == AWS::SSM::Action::"getTokenForInstanceAccess",
    resource
)
when {

    principal has employeeNumber && principal.employeeNumber like "TEMP-*" &&
 resource.hasTag("Criticality") && resource.getTag("Criticality") == "High"
};
```

以下の手順では、ジャストインタイムノードアクセス用にアクセス拒否ポリシーを作成する方法について説明します。ポリシーステートメントを作成する方法の詳細については、「自動承認ポリシーとアクセス拒否ポリシーのステートメントの構造とビルトイン演算子」を参照してください。

> **Note**
>
> 以下の情報に注意してください。
>
> - アクセス拒否ポリシーを作成するには、AWS 管理アカウントまたは委任管理者アカウントにログインしている必要があります。AWS Organizations 組織は、アクセス拒否ポリシーを 1 つのみ設定できます。
> - ジャストインタイムノードアクセスは AWS Resource Access Manager (AWS RAM) を使用して、拒否アクセスポリシーを組織内のメンバーアカウントと共有します。拒否アクセ

スポリシーを組織内のメンバーアカウントと共有する場合は、組織の管理アカウントからリソース共有を有効にする必要があります。詳細については、「AWS RAM ユーザーガイド」の「AWS Organizations 内でリソース共有を有効にする」を参照してください。

アクセス拒否ポリシーを作成するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[ノードアクセスを管理] を選択します。
3. [承認ポリシー] タブで、[アクセス拒否ポリシーを作成] を選択します。
4. [ポリシーステートメント] セクションにアクセス拒否ポリシー用のポリシーステートメントを入力します。あらかじめ用意されている [サンプルステートメント] を使用すると、ポリシーを簡単に作成できます。
5. [アクセス拒否ポリシーを作成] を選択します。

Amazon Q を使用してジャストインタイムノードアクセスの承認ポリシーを作成する

コマンドライン用の Amazon Q Developer を使用すると、ソフトウェア開発のさまざまな側面でガイダンスとサポートが提供されます。ジャストインタイムノードアクセスの場合、Amazon Q は、ポリシーのコードの生成および更新や、ポリシーステートメントの分析などにより、承認ポリシーを作成する際に役立ちます。以下の情報は、コマンドライン用の Amazon Q を使用して承認ポリシーを作成する方法を示しています。

ユースケースの特定

承認ポリシーを作成する最初のステップは、ユースケースを明確に定義することです。例えば、組織で `Environment:Testing` タグを持つノードへのアクセスリクエストを自動的に承認できます。また、従業員 ID が `TEMP` で始まる場合に、`Environment:Production` タグを持つノードへの自動承認を明示的に拒否することもできます。`Tier:Database` タグを持つノードについて、2 つのレベルの手動承認を必要とすることもできます。

特定のシナリオで、あるポリシーまたは条件を別のポリシーまたは条件よりも優先できます。そのため、ユースケースと設定に最適なステートメントを決定するために必要なポリシーの動作を明確に定義することをお勧めします。

開発環境をセットアップする

承認ポリシーを作成するコマンドライン用の Amazon Q をインストールします。コマンドライン用の Amazon Q のインストールについては、「Amazon Q Developer ユーザーガイド」の「Installing Amazon Q for command line」を参照してください。

また、AWS ドキュメントの MCP サーバーをインストールすることをお勧めします。この MCP サーバーは、コマンドライン用の Amazon Q を最新のドキュメントリソースに接続します。コマンドライン用の Amazon Q との MCP の使用の詳細については、「Amazon Q Developer ユーザーガイド」の「Using MCP with Amazon Q Developer」を参照してください。

AWS ドキュメント MCP サーバーの詳細については、「AWS Documentation MCP Server」を参照してください。

まだ AWS CLI をインストールして設定していない場合は、インストールして設定します。詳細については、「AWS CLI の最新バージョンのインストールまたは更新」を参照してください。

承認ポリシーの内容を開発する

ユースケースを特定して環境をセットアップしたら、ポリシーの内容を開発できます。主にユースケースと設定によって、使用する承認ポリシーとステートメントのタイプが決まります。

特定のポリシーの使用方法が不明な場合や、ポリシーのスキーマに関する詳細情報が必要な場合は、「ノードの承認ポリシーを作成する」および以降のトピックを参照してください。これらのトピックでは、ポリシーの評価方法を詳しく説明し、実用的なステートメントの例を示しています。

以下の手順は、コマンドライン用の Amazon Q を使用して承認ポリシーを作成する方法を示しています。

> **Note**
>
> Amazon Q Developer は生成 AI を使用します。レスポンスの検証が必要になる場合があります。「AWS 責任ある AI ポリシー」を参照してください。

コマンドライン用の Amazon Q を使用して承認ポリシーを作成するには

1. ターミナルを開き、Amazon Q とのセッションを開始します。

```
$ q chat
```

2. プロンプトを入力し、作成するポリシーステートメントの種類を記述します。例えば、承認ポリシーの前述のシナリオを使用して、次のプロンプトを入力できます。

```
Create a Cedar policy statement that allows a principal to use the
 “getTokenForInstanceAccess" action for a resource
that has a tag key “Environment” and tag value of “Testing”. Use the following
 example statement for reference to verify the syntax.

permit (
    principal in AWS::IdentityStore::Group::"e8c17310-e011-7089-d989-10da1EXAMPLE",
    action == AWS::SSM::Action::"getTokenForInstanceAccess",
    resource
)
when {
    principal has organization && resource.hasTag("Engineering") &&
 resource.hasTag("Production") && principal.organization == "Platform"
};

The Cedar policy statement you create must be valid. Validate the Cedar statement
 using the AWS documentation provided for just-in-time node access policy statement
 structure and make sure you abide by the schema.
```

3. このプロンプト例を入力すると、次のように出力されます。

```
Based on the AWS documentation for Cedar policy statements and the examples
 provided, I'll create a valid Cedar policy
statement that allows a principal to use the "getTokenForInstanceAccess" action for
 resources with the tag key "Environment" and tag value "Testing".

Here's the Cedar policy statement:

permit (
    principal,
    action == AWS::SSM::Action::"getTokenForInstanceAccess",
    resource
)
when {
    resource.hasTag("Environment") &&
    resource.getTag("Environment") == "Testing"
};


This policy statement:
```

```
1. Uses the permit effect to allow access
2. Applies to any principal (since no specific principal is defined)
3. Specifically targets the "getTokenForInstanceAccess" action
4. Applies to resources that have a tag with key "Environment" and value "Testing"
5. Uses the proper syntax for the condition clause with the hasTag() and getTag()
 operators

The statement follows the Cedar policy language structure as documented in the AWS
 Systems Manager documentation for just-in-time node access policies.
```

4. ポリシーステートメントを新しい Cedar ファイルに貼り付けて、構文を検証します。Cedar プレイグラウンドを使用してステートメントを検証することもできます。
5. ステートメントを検証したら、Cedar ファイルを保存します。
6. ターミナルから次の AWS CLI コマンドを実行して、ポリシーの内容を使用して SSM ドキュメントを作成します。本番環境で承認ポリシーを使用する前に、AWS アカウントおよび AWS リージョンの ID とノードのサブセットを使用して承認ポリシーをテストします。

> **Note**
>
> 自動承認ポリシーの場合、ドキュメント名は SSM-JustInTimeAccessAutoApprovalPolicy である必要があります。AWS アカウントおよび AWS リージョンごとに 1 つの自動承認ポリシーのみが存在できます。アクセス拒否ポリシーの場合、ドキュメント名は SSM-JustInTimeAccessDenyAccessOrgPolicy である必要があります。AWS Organizations 組織ごとに 1 つのアクセス拒否ポリシーのみが存在できます。このポリシーは、Systems Manager の委任管理者アカウントで作成する必要があります。手動承認ポリシーの命名に関する制約は、他の SSM ドキュメントと同じです。詳細については、「CreateDocument」を参照してください。

Linux & macOS

```
aws ssm create-document \
    --content file://path/to/file/policyContent.cedar \
    --name "SSM-JustInTimeAccessAutoApprovalPolicy" \
    --document-type "AutoApproval"
```

Windows

```
aws ssm create-document ^
    --content file://C:\path\to\file\policyContent.cedar ^
    --name "SSM-JustInTimeAccessAutoApprovalPolicy" ^
    --document-type "AutoApproval"
```

PowerShell

```
$cedar = Get-Content -Path "C:\path\to\file\policyContent.cedar" | Out-String
New-SSMDocument `
    -Content $cedar `
    -Name "SSM-JustInTimeAccessAutoApprovalPolicy" `
    -DocumentType "AutoApproval"
```

ジャストインタイムノードアクセスセッション設定を更新する

ジャストインタイムノードアクセスでは、組織内の AWS アカウントと AWS リージョンごとにセッション記録とログ記録の全般的な設定を指定できます。あるいは、AWS CloudFormation StackSets を使用して複数のアカウントとリージョンに 1 つのセッション設定ドキュメントを作成することで、セッション設定の一貫性を保つことができます。セッション設定ドキュメントのスキーマについては、「セッションドキュメントスキーマ」を参照してください。

ログ記録の用途には、Amazon CloudWatch Logs でストリーミングオプションを使用することをお勧めします。この機能により、セッションデータログの連続ストリームを CloudWatch Logs に送信できます。セッションデータのストリーミングには、ユーザーがセッションで実行したコマンド、コマンドを実行したユーザーの ID、セッションデータが CloudWatch Logs にストリーミングされた時のタイムスタンプなど、重要な詳細情報が含まれます。セッションデータをストリーミングする場合、ログは JSON 形式で、既存のログソリューションとの統合に役立ちます。

Systems Manager は、ジャストインタイムノードアクセスセッションを自動的には終了しません。最大セッション期間設定とアイドルセッションタイムアウト設定に値を指定するのがベストプラクティスです。これらの設定を使用すると、ユーザーがアクセスリクエストで承認された時間枠よりも長くノードに接続したままにするのを防ぐことができます。以下の手順では、ジャストインタイムノードアクセスのセッション設定を更新する方法について説明します。

セッション設定を更新するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインの [設定] を選択します。
3. [ジャストインタイムノードアクセス] タブを選択します。
4. [セッション設定] セクションで、[編集] を選択します。
5. 必要に応じて全般的な設定とログ記録の設定を更新し、[保存] を選択します。

ジャストインタイムアクセスリクエストに関する通知を設定する

ユーザーがジャストインタイムノードアクセスリクエストを作成したら、承認者とリクエスタの E メールアドレスまたはチャットクライアントに通知を送信するように、Systems Manager を設定できます。通知にはリクエスタが指定したアクセスリクエストの理由、AWS アカウント、AWS リージョン、リクエストのステータス、ターゲットノードの ID が含まれています。現在、チャットアプリケーションに Amazon Q Developer が統合されたことで、Systems Manager は Slack クライアントと Microsoft Teams クライアントをサポートしています。チャットクライアントで通知を使用するときに、アクセスリクエスト承認者はアクセスリクエストと直接対話できます。このため、アクセスリクエストを操作するためにコンソールにログインする必要がなくなります。

現在 IAM ロールを使用して組織内のユーザー ID を管理している場合は、通知の送信先となる承認者またはリクエスタの E メールアドレスを、関連付けられたロールに手動で関連付ける必要があります。そうしないと、E メールで目的の受信者に通知できません。以下の手順では、ジャストインタイムノードアクセスリクエストに関する通知を設定する方法について説明します。

ジャストインタイムノードアクセスの通知を受け取れるようにチャットクライアントを設定するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインの [設定] を選択します。
3. [ジャストインタイムノードアクセス] タブを選択します。
4. [チャット] セクションで、[新しいクライアントを設定] を選択します。
5. [クライアントタイプを選択] ドロップダウンで、設定するチャットクライアントのタイプを選択し、[次へ] を選択します。
6. チャットアプリケーションの Amazon Q Developer からチャットクライアントへのアクセスを許可するように求められます。[許可] を選択します。

7. [チャネルを設定] セクションで、チャットクライアントチャネルに関する情報を入力し、受け取る通知のタイプを選択します。
8. [チャネルを設定] を選択します。

ジャストインタイムノードアクセスの通知を受け取れるように E メール通知を設定するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインの [設定] を選択します。
3. [ジャストインタイムノードアクセス] タブを選択します。
4. [E メール] セクションで、[編集] を選択します。
5. [E メールの追加] を選択し、E メールアドレスを手動で関連付ける IAM ロールを選択します。
6. [E メールアドレス] フィールドに E メールアドレスを入力します。指定した IAM ロールによる承認が必要なアクセスリクエストが作成されるたびに、そのロールに関連付けた E メールアドレスに通知が届きます。
7. [E メールアドレスの追加] を選択します。

RDP 接続を記録する

ジャストインタイムノードアクセスには、Windows Server ノードへの RDP 接続を記録する機能があります。RDP 接続を記録するには、S3 バケットおよび AWS Key Management Service (AWS KMS) カスタマーマネージドキーが必要です。AWS KMS key は、記録対象のデータが生成されて Systems Manager リソースに保存される際に一時的に暗号化するために使用されます。カスタマーマネージドキーは、暗号化と復号を主な用途とする対称キーでなければなりません。組織で 1 つのマルチリージョンキーを使用することもできれば、ジャストインタイムノードアクセスを有効にしたリージョンごとにカスタマーマネージドキーを作成しなければならないこともあります。

記録を保存する S3 バケットで KMS 暗号化を有効にしている場合は、バケット暗号化に使用されるカスタマーマネージドキーへのアクセスを `ssm-guiconnect` サービスプリンシパルに提供する必要があります。このカスタマーマネージドキーは、記録設定で指定したものとは異なる場合があります。これには、接続を確立するために必要な `kms:CreateGrant` アクセス許可を含める必要があります。

RDP 記録用の S3 バケット暗号化の設定

接続記録は、RDP 記録を有効にするときに指定した S3 バケットに保存されます。

S3 バケット (SSE-KMS) のデフォルトの暗号化メカニズムとして KMS キーを使用する場合は、ssm-guiconnect サービスプリンシパルにキーに対する kms:GenerateDataKey アクションへのアクセスを許可する必要があります。S3 バケットで SSE-KMS 暗号化を使用する場合は、カスタマーマネージドキーを使用することをお勧めします。お勧めする理由は、カスタマーマネージドキーの関連付けられたキーポリシーを更新できるためです。AWS マネージドキー のキーポリシーを更新することはできません。

以下は、S3 ストレージの KMS キーへの ssm-guiconnect サービスアクセスを許可するために使用できるポリシーの例です。カスタマーマネージドキーの更新については、「AWS Key Management Service デベロッパーガイド」の「キーポリシーの変更」を参照してください。

```
{
    "Sid": "Allow the GUI Connect service principal to access S3",
    "Effect": "Allow",
    "Principal": {
        "Service": "ssm-guiconnect.amazonaws.com"
    },
    "Action": [
        "kms:GenerateDataKey*"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:ViaService": "s3.us-east-1.amazonaws.com"
        }
    }
}
```

RDP 接続を記録するように IAM アクセス許可を設定する

ジャストインタイムノードアクセスに IAM アクセス許可が必要になるほか、実行する必要があるタスクに基づいて、使用するユーザーやロールに対して以下のアクセス許可を付与する必要があります。

接続を記録するように設定するためのアクセス許可

RDP 接続を記録するように設定するには、以下のアクセス許可が必要です。

- ssm-guiconnect:UpdateConnectionRecordingPreferences
- ssm-guiconnect:GetConnectionRecordingPreferences
- ssm-guiconnect:DeleteConnectionRecordingPreferences

- kms:CreateGrant

接続を開始するためのアクセス許可

ジャストインタイムノードアクセスとの RDP 接続を確立するには、以下のアクセス許可が必要です。

- ssm-guiconnect:CancelConnection
- ssm-guiconnect:GetConnection
- ssm-guiconnect:StartConnection
- kms:CreateGrant

[開始する前に]

接続の記録を保存するには、まず S3 バケットを作成し、以下のバケットポリシーを追加する必要があります。各###############をユーザー自身の情報に置き換えます。

(バケットポリシーの追加方法の詳細については、「Amazon Simple Storage Service ユーザーガイド」の「Amazon S3 コンソールを使用したバケットポリシーの追加」を参照してください。)

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ConnectionRecording",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "ssm-guiconnect.amazonaws.com"
                ]
            },
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::bucket name",
                "arn:aws:s3:::bucket name/*"
            ],
            "Condition":{
            "StringEquals":{
                "aws:SourceAccount":"123456789012"
                }
```

```
            }
        }
    ]
}
```

RDP 接続記録の有効化と設定

以下の手順では、RDP 接続の記録を有効にして設定する方法について説明します。

RDP 接続記録を有効化および設定するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインの [設定] を選択します。
3. [ジャストインタイムノードアクセス] タブを選択します。
4. [RDP 記録] セクションで、[RDP 記録を有効にする] を選択します。
5. セッション記録のアップロード先となる S3 バケットを選択します。
6. 記録対象のデータが生成されて Systems Manager リソースに保存される際に、データの一時的な暗号化に使用するカスタマーマネージドキーを選択します。(これは、バケットの暗号化に使用するものとは異なるカスタマーマネージドキーにすることができます。)
7. [保存] を選択します。

RDP 接続の記録ステータス値

RPD 接続記録の有効なステータス値は次のとおりです。

- `Recording` - 接続は記録中です。
- `Processing` - 接続が終了した後、動画が処理されています。
- `Finished` - 正常な終了状態: 接続録画の動画が正常に処理され、指定されたバケットにアップロードされました。
- `Failed` - 失敗した終了状態。接続は正常に記録されませんでした。
- `ProcessingError` - 動画処理中に 1 つ以上の中間障害/エラーが発生しました。考えられる原因には、記録の保存用に指定された S3 バケットの設定ミスによるサービス依存関係の問題やアクセス許可の不足などがあります。記録がこの状態にある場合、サービスは処理を試行し続けます。

> **Note**
>
> `ProcessingError` は、接続の確立後に S3 バケットにオブジェクトをアップロードするアクセス許可が `ssm-guiconnect` サービスプリンシパルに付与されていない可能性があります。もう 1 つの考えられる原因は、S3 バケット暗号化に使用される KMS キーに対する KMS アクセス許可がないことです。

ターゲットを変更する

ジャストインタイムノードアクセスを設定するときに、ジャストインタイムノードアクセスをセットアップするターゲットを選択します。ターゲットは、AWS Organizations 組織単位 (OU) と AWS リージョンで構成されています。デフォルトでは、Systems Manager 統合コンソールをセットアップするときに選択したのと同じターゲットがジャストインタイムノードアクセスにも選択されます。ジャストインタイムノードアクセスは、同じすべてのターゲットにセットアップすることも、Systems Manager 統合コンソールをセットアップするときに指定したターゲットのサブセットにセットアップすることもできます。Systems Manager 統合コンソールをセットアップするときに選択されなかったターゲットを新たに追加する機能はサポートされていません。ジャストインタイムノードアクセスをセットアップした後で選択したターゲットを変更できます。

以下の手順では、ジャストインタイムノードアクセスのターゲットを変更する方法について説明します。

ターゲットを変更するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインの [設定] を選択します。
3. [ジャストインタイムノードアクセス] タブを選択します。
4. [ターゲット] セクションで、[編集] を選択します。
5. ジャストインタイムノードアクセスを使用する [組織単位] と [リージョン] を選択します。
6. [保存] を選択します。

ID プロバイダーを変更する

デフォルトでは、ジャストインタイムノードアクセスでは ID プロバイダーに IAM が使用されます。ジャストインタイムノードアクセスを有効にした後に、組織で統合コンソールを使用しているお客様

は、IAM アイデンティティセンターを使用するようにこの設定を変更できます。単一のアカウントとリージョン用に設定する場合、ジャストインタイムノードアクセスでは、ID プロバイダーとして IAM アイデンティティセンターはサポートされていません。

次の手順では、ジャストインタイムノードアクセスの ID プロバイダーを変更する方法について説明します。

ID プロバイダーを変更するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインの [設定] を選択します。
3. [ジャストインタイムノードアクセス] タブを選択します。
4. [ユーザー ID] セクションで、[編集] を選択します。
5. [AWS IAM アイデンティティセンター] を選択します。
6. [保存] を選択します。

ジャストインタイムノードアクセスセッションを開始する

ジャストインタイムノードアクセスを有効にしてセットアップし、セッションと通知の設定を行ったら、ユーザーがジャストインタイムノードアクセスセッションを開始する準備は完了です。Systems Manager コンソールから、または Session Manager プラグインを使用して AWS Command Line Interface から、ジャストインタイムノードアクセスを使用してセッションを開始できます。ジャストインタイムノードアクセスセッションは、同じアカウントとリージョン内のノード上で開始できます。以下の手順では、ジャストインタイムノードアクセスでセッションを開始する方法について説明します。

> **Note**
>
> ユーザーが以前に Session Manager を使用してノードに接続していた場合、ジャストインタイムノードアクセスを使用してセッションを開始するには、IAM ポリシーから Session Manager アクセス許可 (例えば `ssm:StartSession`) を削除する必要があります。そうしないと、ノードに接続するときにユーザーは引き続き Session Manager を使用します。

コンソールを使用してジャストインタイムノードアクセスでセッションを開始するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで [ノードを詳しく見る] を選択します。
3. 接続するノードを選択します。
4. [アクション] ドロップダウンで、[接続] を選択します。

組織の承認ポリシーがノードへの自動接続を許可していない場合は、アクセスリクエストを送信するように求められます。必要事項を入力してアクセスリクエストを送信し、必要なすべての承認が得られたら、ノードへのセッションを開始できるようになります。

AWS CLI を使用してジャストインタイムノードアクセスでセッションを開始するには

1. 次のコマンドを実行して、アクセスリクエストワークフローを開始します。*########*は自分の情報に置き換えてください。

   ```
   aws ssm start-access-request \
       --targets  Key=InstanceIds,Values=i-02573cafcfEXAMPLE
       --reason "Troubleshooting networking performance issue"
   ```

   組織の承認ポリシーに応じて、ノードに自動的に接続されるか、手動承認プロセスが開始されます。リクエストに手動承認が必要な場合は、レスポンスで返されたアクセスリクエストの ID を書き留めます。
2. 必要なすべての承認が得られるまで待機します。
3. 必要なすべての承認が得られたら、以下のコマンドを実行して一時的な認証情報が含まれているアクセストークンを取得します。*#########*を、ユーザー自身の情報に置き換えます。

   ```
   aws ssm get-access-token \
       --access-request-id oi-12345abcdef
   ```

   レスポンスで返されたアクセストークンを書き留めます。
4. 次のコマンドを実行して、AWS CLI で一時的な認証情報を使用します。*########*は自分の情報に置き換えてください。

   ```
   export AWS_SESSION_TOKEN=AQoDYXdzEJr...<remainder of session token>
   ```

5. 次のコマンドを実行して、ノードへのセッションを開始します。########は自分の情報に置き換えてください。

```
aws ssm start-session \
    --target i-02573cafcfEXAMPLE
```

ジャストインタイムアクセスリクエストを管理する

組織全体にわたって可視性を高めるために、Systems Manager は組織用の委任管理者アカウントにアクセスリクエストをレプリケートします。コンプライアンス要件の遵守を支援するため、Systems Manager はすべてのアクセスリクエストを 1 年間保持します。以下のトピックでは、ジャストインタイムノードアクセスリクエストを管理する方法について説明します。この情報は、アクセスリクエスト承認者を対象としています。作業を始める前に、IAM ポリシーをレビューし、ジャストインタイムノードアクセスを管理するために必要なアクセス許可が付与されていることを確認しておくことをお勧めします。詳細については、「Systems Manager でジャストインタイムアクセスをセットアップする」を参照してください。

トピック

- ジャストインタイムノードアクセスリクエストを承認および拒否する

ジャストインタイムノードアクセスリクエストを承認および拒否する

アクセスリクエスト承認者は、統合 Systems Manager コンソールまたは任意のコマンドラインツールを使用して、ジャストインタイムノードアクセスリクエストを承認または拒否できます。この情報は、アクセスリクエスト承認者を対象としています。アクセスリクエストを承認または拒否するために必要なアクセス許可がない場合は、管理者にお問い合わせください。次の手順では、ジャストインタイムノードアクセスリクエストを承認または拒否する方法について説明します。

コンソールを使用してジャストインタイムノードアクセスリクエストを承認または拒否するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[ノードアクセスを管理] を選択します。
3. [アクセスリクエスト] タブを選択します。
4. [自分のためのリクエスト] トグルを選択します。
5. 承認または拒否するアクセスリクエストの横にあるチェックボックスをオンにします。

6. [承認] または [拒否] を選択します。

アクセスリクエストを承認した後に、[取り消し] を選択して、いつでも承認を取り消すことができます。

コマンドラインを使用してジャストインタイムノードアクセスリクエストを承認または拒否するには

1. 通知のアクセスリクエスト ID を書き留めます。例えば、*oi-12345abcdef* などです。
2. 次のコマンドを実行して、アクセスリクエストの承認ワークフローの詳細を返します。*placeholder values* を自身の情報に置き換えていることを確認します。

```
aws ssm get-ops-item \
    --ops-item-id oi-12345abcdef
```

   OperationalData の /aws/accessrequest フィールドの automationExecutionId 値を書き留めます。例えば、*9231944f-61c6-40be-8bce-8ee2bEXAMPLE* などです。
3. 次のコマンドを実行して、アクセスリクエストを承認または拒否します。Approve シグナルタイプを使用してリクエストを承認し、Deny を使用してリクエストを拒否します。*placeholder values* を自身の情報に置き換えていることを確認します。

```
aws ssm send-automation-signal \
    --automation-execution-id 9231944f-61c6-40be-8bce-8ee2bEXAMPLE \
    --signal-type "Approve"
```

Session Manager からジャストインタイムノードアクセスに移行する

ジャストインタイムノードアクセスを有効にしても、Systems Manager が Session Manager の既存のリソースに変更を加えることはありません。そのため、既存の環境に混乱が生じることはなく、ユーザーは承認ポリシーを作成し検証しているときでも引き続きセッションを開始できるようになります。承認ポリシーをテストする準備ができたら、ジャストインタイムノードアクセスへの移行を完了できるように既存の IAM ポリシーを変更する必要があります。例えば、ID へのジャストインタイムノードアクセスに必要なアクセス許可を追加する、Session Manager への StartSession API オペレーション用のアクセス許可を削除するといったことです。AWS アカウントと AWS リージョンの ID とノードのサブセットで承認ポリシーをテストすることをお勧めします。

ジャストインタイムノードアクセスに必要なアクセス許可の詳細については、「Systems Manager でジャストインタイムアクセスをセットアップする」を参照してください。

ID の IAM アクセス許可の変更に関する詳細については、「IAM ユーザーガイド」の「IAM アイデンティティ許可の追加と削除」を参照してください。

ここでは、Session Manager からジャストインタイムノードアクセスに移行する方法について詳しく説明します。

Session Manager からジャストインタイムノードアクセスに移行するには、運用に混乱を招くことなくスムーズに移行できるように入念に計画を立ててテストする必要があります。以降のセクションでは、このプロセスを完了する方法について説明します。

前提条件

作業を開始する前に、次のタスクが完了していることを確認してください。

- Systems Manager 統合コンソールをセットアップする。
- 自分のアカウントに IAM ポリシーを変更するアクセス許可が付与されていることを確認する。
- 現時点で Session Manager アクセス許可を付与しているすべての IAM ポリシーとロールを特定する。
- セッション設定や口グ記録設定など現在の Session Manager 設定を文書化する。

評価

以下のタスクを完了することで、現在の環境を評価し、承認に必要な作業を明らかにします。

1. ノードのインベントリを作成する - ユーザーが現在 Session Manager を介してアクセスしているすべてのノードを特定します。
2. ユーザーアクセスパターンを特定する - どのユーザーやロールがどのノードにどのような状況でアクセスする必要があるかを文書化します。
3. 承認ワークフローをマッピングする - さまざまなタイプのノードに対するアクセスリクエストを誰が承認すべきかを決定します。
4. タグ付け戦略をレビューする - 計画した承認ポリシーをサポートするようにノードが適切にタグ付けされていることを確認します。
5. 既存の IAM ポリシーを監査する - Session Manager アクセス許可が含まれているすべてのポリシーを特定する。

計画

段階的戦略

Session Manager からジャストインタイムノードアクセスに移行するときは、以下のような段階的アプローチを使用することをお勧めします。

1. フェーズ 1: セットアップと設定 - 既存の Session Manager アクセス許可を変更することなくジャストインタイムノードアクセスを有効にします。
2. フェーズ 2: ポリシー策定 - ノードの承認ポリシーを作成し、テストします。
3. フェーズ 3: パイロット移行 - 重要でないノードとユーザーやロールからなる小さなグループを Session Manager からジャストインタイムノードアクセスに変更します。
4. フェーズ 4: 完全移行 - 残りのノードとユーザーやロールを徐々に移行します。

タイムラインの考慮事項

Session Manager からジャストインタイムノードアクセスに移行するタイムラインを作成するときは、以下の要因を考慮します。

- 新しい承認ワークフローに合わせてユーザーをトレーニングし調整する時間を確保する。
- 運用アクティビティの少ない時間帯に移行をスケジュールする。
- トラブルシューティングと調整のバッファ時間を含める。
- 両方のシステムが稼働する並列オペレーションの期間を計画する。

実装手順

フェーズ 1: セットアップと設定

1. Systems Manager コンソールでジャストインタイムノードアクセスを有効にします。詳細なステップについては、「Systems Manager でジャストインタイムアクセスをセットアップする」を参照してください。
2. 現在の Session Manager 設定に合わせてジャストインタイムノードアクセスのセッション設定を行います。詳細については、「ジャストインタイムノードアクセスセッション設定を更新する」を参照してください。
3. アクセスリクエストの通知設定をセットアップします。詳細については、「ジャストインタイムアクセスリクエストに関する通知を設定する」を参照してください。

4. Windows Server ノードへの RDP 接続を使用する場合は、RDP 記録を設定します。詳細については、「RDP 接続を記録する」を参照してください。

フェーズ 2: ポリシー策定

1. ジャストインタイムノードアクセスの管理者とユーザーを対象とした IAM ポリシーを作成します。
2. セキュリティ要件およびユースケースに基づいて承認ポリシーを策定します。
3. 非本番環境でポリシーをテストして、想定通りに機能することを確認します。

フェーズ 3: パイロット移行

1. ユーザーと重要でないノードからなる小さなグループをパイロットとして選択します。
2. パイロットユーザー用にジャストインタイムノードアクセス許可を含めた新しい IAM ポリシーを作成します。
3. パイロットユーザーの IAM ポリシーから Session Manager アクセス許可 (`ssm:StartSession`) を削除します。
4. 新しいアクセスリクエストワークフローでパイロットユーザーをトレーニングします。
5. 問題がないかパイロットをモニタリングし、フィードバックを収集します。
6. パイロットの結果に基づいてポリシーと手順を調整します。

パイロットユーザー向けに IAM ポリシーを変更する例

Session Manager アクセス許可がある元のポリシー:

```
{
                    "Version": "2012-10-17",
                    "Statement": [
                        {
                            "Effect": "Allow",
                            "Action": [
                                "ssm:StartSession",
                                "ssm:ResumeSession",
                                "ssm:TerminateSession"
                            ],
                            "Resource": "*"
                        }
```

```
                    ]
                }
```

ジャストインタイムノードアクセスに合わせてポリシーを変更:

```
{
                    "Version": "2012-10-17",
                    "Statement": [
                        {
                            "Effect": "Allow",
                            "Action": [
                                "ssm:StartAccessRequest",
                                "ssm:GetAccessToken",
                                "ssm:ResumeSession",
                                "ssm:TerminateSession"
                            ],
                            "Resource": "*"
                        }
                    ]
                }
```

フェーズ 4: 完全移行

残りのユーザーとノードを一括して移行するスケジュールを策定します。

テスト方法

移行プロセス全体を通して、以下のテストを実施します。

- ポリシーの検証 - 承認ポリシーが目的のノードとユーザーに適切に適用されていることを検証します。
- アクセスリクエストワークフロー - 自動承認と手動承認の両方のシナリオで、アクセスリクエストからセッション確立までのワークフロー全体をテストします。
- 通知 - 設定されたチャネル (E メール、Slack、Microsoft Teams) を介して承認者が通知を受け取ることを検証します。
- ログ記録とモニタリング - セッションログとアクセスリクエストが適切にキャプチャされて保存されることを検証します。

移行を正常に完了するためのベストプラクティス

- 早めに頻繁に伝える - ジャストインタイムノードアクセスの移行タイムラインと利点についてユーザーに周知します。
- 重要でないシステムから開始する - 本番環境に移行する前に開発環境またはテスト環境で移行を開始します。
- 何事も文書化する - 承認ポリシー、IAM ポリシーの変更、構成設定を詳細に記録します。
- モニタリングして調整する - アクセスリクエストと承認ワークフローを継続的にモニタリングし、必要に応じてポリシーを調整します。
- ガバナンスを確立する - 承認ポリシーを定期的にレビューし、環境の変化に応じて更新するためのプロセスを作成します。

Systems Manager でジャストインタイムアクセスを無効にする

以下の手順では、ジャストインタイムノードアクセスを無効にする方法について説明します。ジャストインタイムノードアクセスを無効にすると、他の接続方法を既に実装している場合を除き、組織内のユーザーはノードに接続できなくなる可能性があります。

ジャストインタイムノードアクセスを無効にするには

1. 組織用の Systems Manager 委任管理者アカウントにログインします。
2. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
3. ナビゲーションペインの [設定] を選択します。
4. [ジャストインタイムノードアクセス] タブで、[無効] を選択します。

ジャストインタイムノードアクセスに関するよくある質問

Session Manager からジャストインタイムノードアクセスに移行するにはどうすればよいですか?

統合コンソールを設定してジャストインタイムノードアクセスを有効にした後に、既存の IAM ポリシーを変更してジャストインタイムノードアクセスへの移行を完了する必要があります。これには、ジャストインタイムノードアクセスに必要なアクセス許可の追加や、Session Manager 用の `StartSession` API オペレーションのアクセス許可の削除が含まれます。ジャストインタイムノー

ドアクセス用の IAM ポリシーの詳細については、「Systems Manager でジャストインタイムアクセスをセットアップする」を参照してください。

ジャストインタイムノードアクセスを使用するように統合コンソールを設定する必要がありますか?

はい。統合コンソールの設定は、ジャストインタイムノードアクセスの前提条件です。ただし、統合コンソールを設定してジャストインタイムノードアクセスを有効にした後は、ノードに接続する方法がいくつかあります。例えば、Amazon EC2 コンソールと AWS CLI からジャストインタイムノードアクセスセッションを開始できます。統合コンソールの設定の詳細については、「組織用の Systems Manager 統合コンソールのセットアップ」を参照してください。

ジャストインタイムノードアクセスに関連するコストはありますか?

Systems Manager では、ジャストインタイムノードアクセス用の 30 日間の無料トライアルが提供されます。トライアル後、ジャストインタイムノードアクセスにはコストが発生します。詳細については、AWS Systems Manager の料金を参照してください。

ジャストインタイムノードアクセスの承認ポリシーの優先順位はどのようになっていますか?

承認ポリシーは次の順序で評価されます。

1. アクセス拒否
2. 自動承認
3. 手動

手動承認ポリシーはどのように評価されますか?

ジャストインタイムノードアクセスでは、ノードのより具体的なポリシーが常に優先されます。手動承認ポリシーは次の順序で評価されます。

1. タグの具体的なターゲット
2. すべてのノードのターゲット

ノードに適用される承認ポリシーがない場合はどのようになりますか?

ジャストインタイムノードアクセスを使用してノードに接続するには、ノードに承認ポリシーを適用する必要があります。ノードに適用される承認ポリシーがない場合、ユーザーはノードへのアクセスをリクエストできません。

複数の承認ポリシーでタグをターゲットにできますか?

タグは、承認ポリシーで 1 回のみターゲットにできます。

タグが重複した結果、複数の手動承認ポリシーがノードに適用された場合はどのようになりますか?

ノードに複数の手動承認ポリシーが適用されると、競合が発生し、ユーザーはノードへのアクセスをリクエストできません。ケースによってはインスタンスに複数のタグがある場合もあるため、手動承認ポリシーを作成するときはこの点に注意してください。

ジャストインタイムノードアクセスを使用して、アカウントとリージョンをまたいだノードでアクセスをリクエストし、セッションを開始することはできますか?

ジャストインタイムノードアクセスでは、リクエスタと同じアカウントとリージョンのノードでの、アクセスのリクエストとセッションの開始がサポートされています。

ジャストインタイムノードアクセスを使用して、ハイブリッドアクティベーションに登録されたノードでアクセスをリクエストし、セッションを開始することはできますか?

はい。ジャストインタイムノードアクセスでは、ハイブリッドアクティベーションに登録されたノードでの、アクセスのリクエストとセッションの開始がサポートされています。ノードは、リクエスタと同じアカウントとリージョンに登録する必要があります。

診断と修復

Systems Manager の統合コンソールを使用すると、単一の診断オペレーションでフリート全体の問題を特定できます。組織の場合、単一のオートメーションオペレーションを使用して、すべてのターゲットまたは選択したターゲットのみに対して修復を試みることができます。組織の場合、委任されたアカウント管理者として、すべてのアカウントおよびリージョンにわたってターゲットを選択でき

ます。単一のアカウントで作業している場合は、一度に 1 つのリージョンのターゲットを選択できます。

Systems Manager は、複数のタイプのデプロイ障害やドリフトした設定を診断することができ、それらをユーザーが修復するのに役立ちます。また、Systems Manager は、アカウント内または組織内の Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのうち、マネージドノードとして扱うことができないインスタンスを特定することもできます。EC2 インスタンス診断プロセスでは、仮想プライベートクラウド (VPC)、ドメインネームサービス (DNS) 設定、または Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループの設定ミスに関連する問題を特定できます。

> **Note**
>
> Systems Manager は、ハイブリッドおよびマルチクラウド環境において、EC2 インスタンスとその他のマシンタイプの両方をマネージドノードとしてサポートします。マネージドノードになるには、そのマシンに AWS Systems Manager Agent (SSM Agent) がインストールされており、Systems Manager がそのマシン上でアクションを実行するアクセス許可を持っている必要があります。
> EC2 インスタンスの場合、このアクセス許可は、AWS Identity and Access Management (IAM) ロールを使用してアカウントレベルで付与するか、またはインスタンスプロファイルを使用してインスタンスレベルで付与することができます。詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」を参照してください。
> 非 EC2 マシンの場合、このアクセス許可は IAM サービスロールを使用して付与されます。詳細については、「ハイブリッドおよびマルチクラウド環境で Systems Manager に必要な IAM サービスロールを作成する」を参照してください。

[開始する前に]

[診断および修復] 機能を使用してアンマネージド EC2 インスタンスを検出するには、まず、組織またはアカウントを Systems Manager の統合コンソールにオンボーディングする必要があります。このプロセス中に、これらのオペレーションに必要な IAM ロールとマネージドポリシーを作成するオプションを選択する必要があります。詳細については、「組織用の Systems Manager 統合コンソールのセットアップ」を参照してください。

以下のトピックは、一般的なタイプのデプロイ障害、ドリフトした設定、およびアンマネージド EC2 インスタンスを特定して修正するのに役立ちます。

トピック

- 失敗したデプロイの診断と修復
- ドリフトした設定の診断と修復
- Systems Manager でのアンマネージド Amazon EC2 インスタンスの診断と修復
- ランブックアクションの修復の影響タイプ
- Systems Manager での修復実行の進行状況と履歴の表示

失敗したデプロイの診断と修復

Systems Manager は、次のタイプの失敗したデプロイを診断することができ、ユーザーによる修復を支援します。

- 組織メンバーアカウントのコアセットアップ
- 委任管理者アカウントのコアセットアップ
- アカウントのコアセットアップ

次の手順を使用して、これらのタイプの問題の修復を試みます。

失敗したデプロイを診断および修復する手順

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[診断および修復] を選択します。
3. [デプロイ関連] タブを選択します。
4. [失敗したデプロイ] セクションで、失敗したデプロイの検出結果のリストを確認します。
5. [セットアップ手順] 列で、検出結果の名前を選択して、問題に関する追加の詳細を確認します。例: 組織メンバーアカウントのコアセットアップ。
6. その失敗したデプロイの詳細ページで、アカウントのリストと、各アカウント内でデプロイの失敗が発生したリージョンの数を確認できます。
7. アカウント ID を選択すると、そのアカウントにおける失敗の理由に関する情報が表示されます。
8. [失敗したリージョン] 領域で、[ステータスの理由] として提供された情報を調べます。この情報には、デプロイが失敗した理由が示されており、必要な設定変更についてのインサイトが得られる場合があります。
9. 設定を変更せずにデプロイを再試行する場合は、[再デプロイ] を選択します。

ドリフトした設定の診断と修復

Systems Manager は、次のタイプのドリフトした設定を診断することができ、ユーザーによる修復を支援します。

- 組織メンバーアカウントのコアセットアップ
- 委任管理者アカウントのコアセットアップ
- アカウントのコアセットアップ

次の手順を使用して、これらのタイプのドリフトした設定の修復を試みます。

ドリフトした設定を診断および修復する手順

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[診断および修復] を選択します。
3. [デプロイ関連] タブを選択します。
4. [ドリフトしたデプロイ] セクションで、失敗したデプロイの検出結果のリストを確認します。

   -または-

   新しい診断を実行するには、[ドリフトの検出] を選択します。
5. [セットアップ手順] 列で、検出結果の名前を選択して、問題に関する追加の詳細を確認します。例: 組織メンバーアカウントのコアセットアップ。
6. その失敗したデプロイの詳細ページで、アカウントのリストと、各アカウント内で設定ドリフトが発生したリージョンの数を確認できます。
7. アカウント ID を選択すると、そのアカウントにおける設定ドリフトの理由に関する情報が表示されます。
8. [ドリフトされたリソース] 領域で、[リソース] 列にドリフトが発生したリソースの名前が報告されます。[ドリフトタイプ] 列には、リソースが変更されたか削除されたかが報告されます。
9. 目的の設定を再デプロイするには、[再デプロイ] を選択します。

Systems Manager でのアンマネージド Amazon EC2 インスタンスの診断と修復

Systems Manager を使用して Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理するのを支援するために、Systems Manager の統合コンソールを使用して次のことができます。

1. 手動による、またはスケジュールされた診断プロセスを実行して、現在 Systems Manager によって管理されていない、アカウントまたは組織内の EC2 インスタンスを特定します。
2. Systems Manager がインスタンスの管理を引き継ぐのを妨げているネットワークまたはその他の問題を特定します。
3. オートメーション実行を実行して問題を自動的に修復するか、手動で問題に対処するのに役立つ情報にアクセスします。

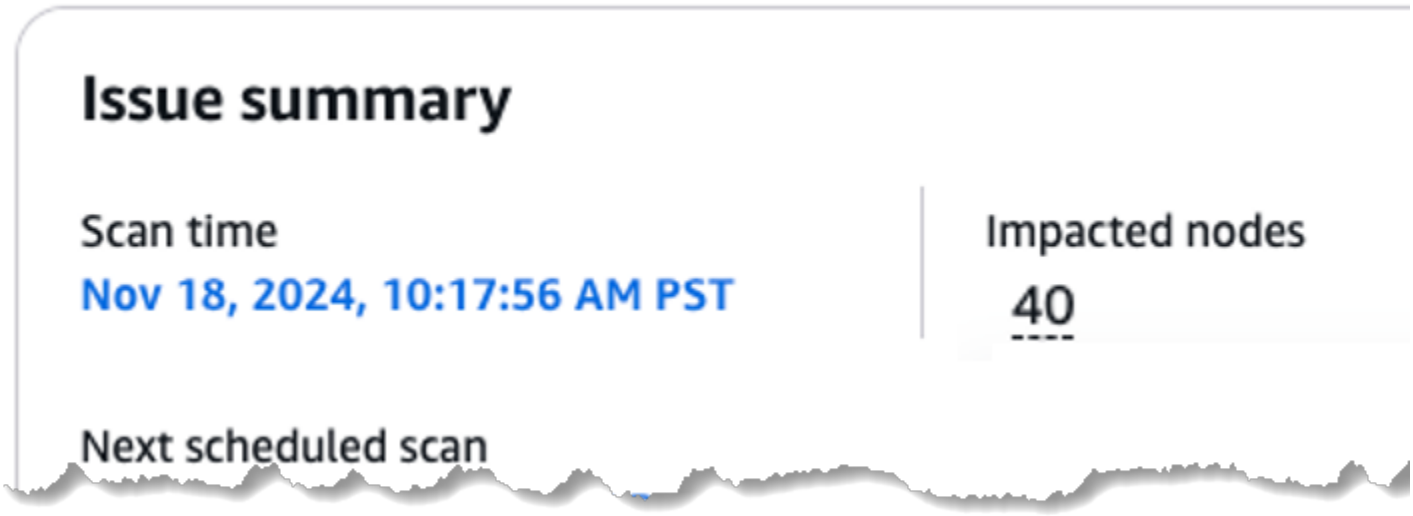
以下のトピックの情報を使用して、Systems Manager が EC2 インスタンスを管理することを妨げている問題を診断および修復できます。

Systems Manager が「アンマネージド EC2 インスタンスの問題」リストで影響を受けるノードをカウントする方法

[アンマネージド EC2 インスタンスの問題] タブでアンマネージドとして報告されたノードの数は、診断スキャン時に以下のいずれかのステータス値を持っていたインスタンスの総数を表します。

- `Running`
- `Stopped`
- `Stopping`

この数は、[問題の概要] 領域で [影響を受けるノード] として報告されます。次の図で、現在 Systems Manager によって管理されていない、影響を受けるノードの数は `40` です。



[ノードインサイトの確認] ページのアンマネージド EC2 インスタンスのレポートとは異なり、このEC2 インスタンスの数は動的ではありません。これは、最後に報告された診断スキャン時 ([スキャン時刻] の値として示されている) における検出結果を表しています。そのため、この報告された影響を受けるノードの数を最新の状態に保つために、アンマネージド EC2 インスタンスの診断スキャンを定期的に実行することをお勧めします。

[ノードのインサイトを確認] ページでのアンマネージドインスタンス数の詳細については、「ノードインサイトの確認」トピックの「アンマネージドインスタンスとは」を参照してください。

トピック

- 診断可能なアンマネージド EC2 インスタンスの問題のカテゴリ
- アンマネージド EC2 インスタンスに対する診断およびオプションの修復の実行
- アンマネージド EC2 インスタンスの定期スキャンのスケジュール

診断可能なアンマネージド EC2 インスタンスの問題のカテゴリ

このトピックでは、ユーザーが診断と修復を行う際に Systems Manager が支援できる EC2 管理の問題の主要なカテゴリと、各カテゴリの具体的な問題についてリストします。一部の問題については、Systems Manager が問題を特定することはできるが、自動修復を行うことはできない場合があるので注意してください。そのような場合、Systems Manager のコンソールで、問題を手動で解決するのに役立つ情報が提供されます。

診断プロセスでは、EC2 インスタンスが属する仮想プライベートクラウド (VPC) に応じて、各グループの EC2 インスタンスを一度に検査します。

問題タイプ

- 問題カテゴリ: セキュリティグループ設定と HTTPS 通信
- 問題カテゴリ: DNS または DNS ホスト名の設定
- 問題カテゴリ: VPC エンドポイント設定

問題カテゴリ: セキュリティグループ設定と HTTPS 通信

診断オペレーションによって、SSM Agent が HTTPS 経由で Systems Manager サービスと通信できないことが検出される場合があります。そのような場合は、オートメーションランブックを実行することを選択できます。これにより、インスタンスにアタッチされているセキュリティグループの更新が試行されます。

> **Note**
>
> 場合によっては、Systems Manager がこれらの問題を自動的に修復できないことがありますが、影響を受けたセキュリティグループを手動で編集することは可能です。

サポートされている問題タイプ

- インスタンスセキュリティグループ: ポート 443 でのアウトバウンドトラフィックは許可されません
- **ssm** VPC エンドポイントのセキュリティグループ: ポート 443 でのインバウンドトラフィックは許可されません
- **ssmmessages** VPC エンドポイントのセキュリティグループ: ポート 443 でのインバウンドトラフィックは許可されません
- **ec2messages** VPC エンドポイントのセキュリティグループ: ポート 443 でのインバウンドトラフィックは許可されません

詳細については、トピック「SSM Agent のトラブルシューティング」の「エンドポイントセキュリティグループでイングレスルールを検証する」を参照してください。

問題カテゴリ: DNS または DNS ホスト名の設定

診断オペレーションによって、ドメインネームシステム (DNS) または DNS ホスト名が VPC に対して適切に設定されていないことが検出される場合があります。そのような場合は、オー

トメーションランブックを実行することを選択できます。これにより、影響を受けた VPC の enableDnsSupport 属性および enableDnsHostnames 属性の有効化が試行されます。

サポートされている問題タイプ

- VPC では DNS サポートは無効化されています。
- VPC では DNS ホスト名は無効化されています。

詳細については、トピック「SSM Agent のトラブルシューティング」の「VPC DNS 関連の属性を検証する」を参照してください。

問題カテゴリ: VPC エンドポイント設定

診断オペレーションによって、VPC エンドポイントが VPC に対して適切に設定されていないことが検出される場合があります。

SSM Agent に必要な VPC エンドポイントが存在しない場合、Systems Manager はオートメーションランブックを実行して VPC エンドポイントを作成し、それを関連する各リージョンアベイラビリティーゾーン (AZ) 内の 1 つのサブネットに関連付けようとします。VPC に必要なエンドポイントは存在するが、問題が見つかったサブネットに関連付けられていない場合、ランブックはその VPC エンドポイントを影響を受けたサブネットに関連付けます。

> **Note**
>
> Systems Manager は、誤って設定された VPC エンドポイントのすべての問題の修復をサポートしているわけではありません。そのような場合、Systems Manager は、オートメーションランブックを実行する代わりに、ユーザーに対して手動修復手順を提供します。

サポートされている問題タイプ

- PrivateLink 用の ssm.*region*.amazonaws.com エンドポイントが見つかりませんでした。
- PrivateLink 用の ssmmessages.*region*.amazonaws.com エンドポイントが見つかりませんでした。
- PrivateLink 用の ec2messages.*region*.amazonaws.com エンドポイントが見つかりませんでした。

診断可能な問題タイプ

Systems Manager は、以下の問題タイプを診断できますが、現在、これらの問題の修復に使用できるランブックはありません。これらの問題について、設定を手動で編集することは可能です。

- インスタンスのサブネットが ssm.*region*.amazonaws.com エンドポイントにアタッチされていません。
- インスタンスのサブネットが ssmmessages.*region*.amazonaws.com エンドポイントにアタッチされていません。
- インスタンスのサブネットが ec2messages.*region*.amazonaws.com エンドポイントにアタッチされていません。

詳細については、トピック「SSM Agent のトラブルシューティング」の「VPC 設定を検証する」を参照してください。

アンマネージド EC2 インスタンスに対する診断およびオプションの修復の実行

Systems Manager が EC2 インスタンスを管理するのを妨げている可能性があるネットワーク関連および VPC 関連の問題を診断するには、次の手順を使用します。

診断オペレーションでは、以下のタイプの問題を検出してグループ化できます。

- [ネットワーク設定の問題] — EC2 インスタンスがクラウド内の Systems Manager サービスと通信するのを妨げている可能性があるネットワーク問題のタイプ。これらの問題では、修復オペレーションを使用できる場合があります。ネットワーク設定の問題の詳細については、「診断可能なアンマネージド EC2 インスタンスの問題のカテゴリ」を参照してください。
- [未確認の問題] — EC2 インスタンスがクラウド内の Systems Manager サービスと通信できない理由を診断オペレーションによって判断できなかった場合の検出結果のリスト。

アンマネージド EC2 インスタンスに対して診断および修復を実行する手順

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[診断および修復] を選択します。
3. [アンマネージド EC2 インスタンスの問題] タブを選択します。
4. [問題の概要] セクションで [新しい診断の実行] を選択します。

   -または-

アンマネージド EC2 の問題を初めて診断する場合は、[アンマネージド EC2 インスタンスの診断] セクションで [実行] を選択します。

> **Tip**
>
> 診断の実行中に [進行状況を表示] または [実行を表示] を選択すると、実行の現在の状態をモニタリングできます。詳細については、「Systems Manager での修復実行の進行状況と履歴の表示」を参照してください。

5. 診断が完了したら、次の操作を実行します。

   - [未確認の問題] セクションで報告された問題については、[詳細] リンクを選択すると問題の解決方法を確認できます。
   - [ネットワーク設定の問題] セクションで報告された問題については、次のステップに進みます。

6. 検出結果タイプのリスト内で、特定の問題に対応する [推奨事項] 列のリンク ([2 つの推奨事項] など) を選択します。

7. 開いた [推奨事項] ペインで、使用可能な緩和策から選択します。

   - [詳細] — 問題を手動で解決する方法に関する情報を含むトピックを開きます。
   - [ランブックの表示] – EC2 インスタンスの問題を解決するために実行できるオートメーションランブックに関する情報と、ランブックが実行するアクションのプレビューを生成するためのオプションを含むペインを開きます。次のステップに進みます。

8. ランブックペインで、次の操作を実行します。

   a. [ドキュメントの説明] で、コンテンツを確認します。コンテンツには、ランブックがアンマネージド EC2 インスタンスの問題を修復するために実行できるアクションの概要が示されています。[ステップを表示] を選択して、ランブックで実行される個々のアクションをプレビューします。

   b. [ターゲット] で、以下の作業を行います。

      - 組織の修復を管理している場合は、[アカウント] で、このランブックがすべてのアカウントをターゲットにするか、選択したアカウントのサブセットのみをターゲットにするかを指定します。

- [リージョン] で、このランブックがアカウントまたは組織内のすべての AWS リージョンをターゲットにするか、選択したリージョンのサブセットのみをターゲットにするかを指定します。

c. [ランブックのプレビュー] で、情報を慎重に確認します。この情報は、ランブックの実行を選択した場合の範囲と影響について説明しています。

> **Note**
>
> ランブックの実行を選択すると、料金が発生します。続行するかどうかを決定する前に、プレビュー情報を注意深く確認してください。

[ランブックのプレビュー] のコンテンツでは、次の情報が提供されます。

- ランブックオペレーションが実行されるリージョンの数。
- (組織のみ) オペレーションを実行する組織単位 (OU) の数。
- 実行されるアクションのタイプと、各アクションの実行回数。

  アクションタイプには以下のものがあります。

  - 変異: ランブックステップは、リソースの作成、変更、または削除を行うアクションを通じて、ターゲットに変更を加えます。
  - 非変異: ランブックステップは、リソースに関するデータを取得しますが、データに変更を加えることはありません。このカテゴリには通常、`Describe*`、`List*`、`Get*`、および同様の読み取り専用 API アクションが含まれます。
  - 未確定: 未確定ステップは、AWS Lambda、AWS Step Functions、または AWS Systems Manager Run Command など、他のオーケストレーションサービスによって処理される実行を呼び出します。未確定ステップは、サードパーティー API を呼び出すこともあります。Systems Manager Automation は、オーケストレーションプロセスやサードパーティー API の実行結果を認識できないため、それらのステップの結果は未確定になります。

d. この時点で、次のいずれかのアクションを選択できます。

- 停止して、ランブックを実行しない。
- [実行] を選択して、既に選択したオプションを使用してランブックを実行する。

オペレーションを実行することを選択した場合は、[進行状況を表示] または [実行を表示] を選択すると、実行の現在の状態をモニタリングできます。詳細については、「Systems Manager での修復実行の進行状況と履歴の表示」を参照してください。

アンマネージド EC2 インスタンスの定期スキャンのスケジュール

さまざまな設定の問題によって Systems Manager が管理できない、アカウントまたは組織内の Amazon EC2 インスタンスに対して、オンデマンドスキャンを実行できます。定期的なスケジュールに従って自動的に実行されるように、このスキャンをスケジュールすることもできます。

アンマネージド EC2 インスタンスの定期スキャンをスケジュールする手順

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[診断および修復] を選択します。
3. [アンマネージド EC2 インスタンスの問題] タブを選択します。
4. [アンマネージド EC2 インスタンスの診断] セクションで、[定期診断のスケジュール] をオンにします。
5. [診断頻度] で、診断を 1 日に 1 回実行するか、週に 1 回実行するかを選択します。
6. (オプション) [開始時刻] に、診断を開始する時刻を 24 時間形式で入力します。例えば、午後 8:15 の場合は **`20:15`** と入力します。

   入力する時刻は、現在のローカルタイムゾーンの時刻です。

   時刻を指定しない場合、診断スキャンは即時に実行されます。Systems Manager は、今後のスキャンも現在時刻に実行されるようにスケジュールします。時刻を指定すると、Systems Manager は指定された時刻まで待ってから診断スキャンを実行します。
7. [実行] を選択してください。診断は即時に実行されますが、指定したスケジュールでも実行されます。

ランブックアクションの修復の影響タイプ

Systems Manager は、特定のタイプの失敗したデプロイやドリフトした構成、および Systems Manager が EC2 インスタンスを管理するのを妨げている特定のタイプの設定の問題を検出する診断オペレーションを実行できます。診断の結果には、問題の解決を試みるために実行できるオートメー

ションランブックの推奨事項が含まれる場合があります。これらの診断オペレーションの詳細については、次のトピックを参照してください。

- 失敗したデプロイの診断と修復
- ドリフトした設定の診断と修復
- Systems Manager でのアンマネージド Amazon EC2 インスタンスの診断と修復

Systems Manager は、影響を受けるリソースでオートメーションランブックを実行することで修正できる可能性のある問題を特定すると、実行プレビューを提供します。実行プレビューでは、ランブックの実行によってターゲットにどのようなタイプの変更が加えられるかについての情報が提供されます。この情報には、診断によって特定された 3 つのタイプの変更それぞれの数が含まれます。

これらの変更タイプは以下のとおりです。

- `Mutating`: ランブックステップは、リソースの作成、変更、または削除を行うアクションを通じて、ターゲットに変更を加えます。
- `Non-Mutating`: ランブックステップは、リソースに関するデータを取得しますが、データに変更を加えることはありません。このカテゴリには通常、`Describe*`、`List*`、`Get*`、および同様の読み取り専用 API アクションが含まれます。
- `Undetermined`: 未確定ステップは、AWS Lambda、AWS Step Functions、または AWS Systems Manager のツールである Run Command など、他のオーケストレーションサービスによって処理される実行を呼び出します。また、未確定ステップは、サードパーティー API を呼び出したり、Python や PowerShell スクリプトを実行したりする場合もあります。Systems Manager Automation は、オーケストレーションプロセスまたはサードパーティー API 実行の結果を検出できないため、それらを評価することができません。これらのステップの結果は、手動で確認して、その影響を判断する必要があります。

  サポートされているオートメーションアクションの影響タイプについては、次の表を参照してください。

サポートされている修復アクションの影響タイプ

この表は、修復ランブックに含めることができるさまざまなアクションの影響タイプ (変異、非変異、未確定) を示しています。

アクション[1]	影響タイプ
aws:approve	非変異
aws:assertAwsResourceProperty	非変異
aws:branch	非変異
aws:changeInstanceState	変異
aws:copyImage	変異
aws:createImage	変異
aws:createStack	変異
aws:createTags	変異
aws:deleteImage	変異
aws:deleteStack	変異
aws:executeAutomation	未定
aws:executeAwsApi	未定
aws:executeScript	未定
aws:executeStateMachine	未定
aws:invokeLambdaFunction	未定
aws:invokeWebhook	未定
aws:loop	可変。ループに含まれるアクションによって異なります。
aws:pause	非変異
aws:runCommand	未定
aws:runInstances	変異

アクション[1]	影響タイプ
aws:sleep	非変異
aws:updateVariable	変異
aws:waitForAwsResourceProperty	非変異

[1] オートメーションアクションの詳細については、「Systems Manager Automation アクションのリファレンス」を参照してください。

Systems Manager での修復実行の進行状況と履歴の表示

Systems Manager の [診断および修復] 機能を使用して実行された、すべての進行中および完了済みの修復オペレーションのリストを表示できます。

実行履歴リストのデータによって、以下のタイプの情報が報告されます。

- 実行のタイプ: `Diagnosis` または `Remediation`。
- 実行ステータス: `Success` や `Failed` など。
- 実行の開始時刻と終了時刻。

修復の実行の進行状況と履歴を表示する手順

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[診断および修復] を選択します。
3. [実行の表示] を選択します。

> **Tip**
> 実行が進行中の場合は、[進行状況を表示] を選択して [実行履歴] ページを開くこともできます。

4. (オプション) 検索
   (🔍)
   ボックスに、**EC2** や **VPC** など、実行リストを絞り込むのに役立つフレーズを入力します。

5. (オプション) 実行に関する詳細を表示するには、[実行名] 列で [AWS-DiagnoseUnmanagedEC2NetworkIssues] などのオペレーション名を選択します。

   詳細ペインでは、オペレーション中に試行されたすべてのステップ、および実行におけるすべての入力と出力に関する情報を確認できます。

Systems Manager 設定の調整

Systems Manager 統合コンソールで [設定] ページのオプションを使用して、各種機能を有効にして設定できます。表示されるオプションは、ログインに使用しているアカウントと、Systems Manager を既にセットアップしているかどうかによって異なります。

> **Note**
>
> [設定] ページのオプションが Systems Manager のツール (これまで機能と呼ばれていたもの) に影響を与えることはありません。

アカウントセットアップ設定

Systems Manager が有効になっている場合に、Organizations のメンバーでないアカウントでログインするか、委任管理者が Organizations アカウントを Systems Manager に追加していないと、[アカウント設定] ページに [Systems Manager を無効にする] オプションが表示されます。Systems Manager を無効にすると、Systems Manager に統合コンソールが表示されなくなります。Systems Manager ツールはいずれも引き続き機能します。

組織のセットアップの設定

[組織のセットアップ] タブの [ホームリージョン] セクションに、セットアップ時にホームリージョンとして選択された AWS リージョンが表示されます。AWS Organizations を使用するマルチアカウントとマルチリージョンの環境で、Systems Manager がすべてのアカウントとリージョンからホームリージョンにノードデータを自動的に集約します。このようにデータを集約すると、アカウントとリージョン全体のノードデータを 1 か所に表示できます。

> **Note**
>
> ホームリージョンを変更する場合は、Systems Manager をいったん無効にしてから再度有効にする必要があります。Systems Manager を無効にするには、[無効化] を選択します。

[組織のセットアップ] セクションに、セットアップ時に選択した AWS 組織単位と AWS リージョンが表示されます。Systems Manager にノードデータを表示する組織単位とリージョンを変更するには、[編集] を選択します。組織に Systems Manager をセットアップする方法の詳細については、「AWS Systems Manager を設定する」を参照してください。

[診断および修復] の設定

[診断および修復] の設定によって、Systems Manager でノードを自動的にスキャンしてノードが Systems Manager と通信できるようにするかどうかが決まります。この機能を有効にすると、定義したスケジュールに従って機能が自動的に実行されます。これにより、Systems Manager に接続できないノードとその理由を特定できます。この機能には、ネットワークの問題のほか、ノードをマネージドノードとして設定することを阻害しているその他の問題を修復するのに適したお勧めのランブックも用意されています。

定期診断スキャンのスケジューリング

Systems Manager は、複数のタイプのデプロイ障害やドリフトした設定を診断することができ、それらをユーザーが修復するのに役立ちます。また、Systems Manager は、アカウント内または組織内の Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのうち、マネージドノードとして扱うことができないインスタンスを特定することもできます。EC2 インスタンス診断プロセスでは、仮想プライベートクラウド (VPC)、ドメインネームサービス (DNS) 設定、または Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループの設定ミスに関連する問題を特定できます。

[定期診断のスケジューリング] 機能を使用して定期診断スキャンを自動化することで、Systems Manager に接続できないノードを特定するタスクを簡単に実行できます。このスキャンにより、Systems Manager に接続できないノードとその理由を特定できます。ノードの定期診断スキャンを有効にして設定するには、以下の手順に従います。

定期診断スキャンをスケジューリングするには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[設定]、[診断および修復] タブの順に選択します。
3. [定期診断のスケジューリング] オプションを有効にします。
4. [スキャン期間] でスキャンの実行頻度を選択します。
5. (オプション) [開始時刻] に、診断を開始する時刻を 24 時間形式で入力します。例えば、午後 8:15 の場合は **`20:15`** と入力します。

入力する時刻は、現在のローカルタイムゾーンの時刻です。

時刻を指定しない場合、診断スキャンは即時に実行されます。Systems Manager は、今後のスキャンも現在時刻に実行されるようにスケジュールします。時刻を指定すると、Systems Manager は指定された時刻まで待ってから診断スキャンを実行します。

6. [Save] を選択します。
7. スキャンが完了したら、左側のナビゲーションで [診断および修復] を選択して詳細を表示します。

[診断および修復] 機能の詳細については、「診断と修復」を参照してください。

S3 バケット暗号化の更新

Systems Manager をオンボーディングすると、AWS Organizations セットアップ用の委任管理者アカウントに Quick Setup によって Amazon Simple Storage Service (Amazon S3) バケットが作成されます。シングルアカウントセットアップの場合、バケットはセットアップされるアカウントに保存されます。このバケットは、診断スキャン中に生成されたメタデータを保存するために使用されます。

Systems Manager の統合コンソールのセットアップ方法については、「AWS Systems Manager を設定する」を参照してください。

デフォルトでは、バケット内のデータは AWS がユーザーに代わって所有および管理する AWS Key Management Service (AWS KMS) キーを使用して暗号化されます。

これとは別の AWS KMS キーをバケットの暗号化に使用することもできます。例えば、カスタマーマネージドキー (CMK) を使用して、AWS KMS keysによるサーバー側の暗号化 (SSE-KMS) を使用するという方法があります。詳細については、Systems Manager での Amazon S3 バケットとバケットポリシーの使用 を参照してください。

S3 バケットの暗号化に別の AWS KMS キーを使用するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[設定]、[診断および修復] タブの順に選択します。
3. [S3 バケットの暗号化の更新] 領域で、[編集] を選択します。
4. [暗号化設定のカスタマイズ (高度)] チェックボックスを選択します。

5. [AWS KMS キーの選択] でそのキーの Amazon リソースネーム (ARN) を選択または入力します。

> **Tip**
>
> 新しいキーを作成するには、[AWS KMS キーを作成] を選択します。

6. [Save] を選択します。

Systems Manager での Amazon S3 バケットとバケットポリシーの使用

AWS Systems Manager のオンボーディングプロセス時に、Quick Setup によって組織セットアップ用に Amazon Simple Storage Service (Amazon S3) バケットが委任管理者アカウントに作成されます。シングルアカウントセットアップの場合、バケットはセットアップされるアカウントに保存されます。

Systems Manager を使用してフリートで診断オペレーションを実行することで、デプロイが失敗して設定がドリフトした原因を特定できます。Systems Manager では、設定の問題のために Systems Manager がアカウントや組織の EC2 インスタンスを管理できないケースも検出できます。こうした診断オペレーションの結果は、この Amazon S3 バケットに保存され、暗号化方法と S3 バケットポリシーの両方で保護されます。このバケットにデータを出力する診断オペレーションについては、「診断と修復」を参照してください。

バケット暗号化方法の変更

デフォルトでは、S3 バケットは Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3) を使用します。

「S3 リソースを暗号化するための AWS KMS カスタマーマネージドキーへの変更」で説明しているように、Amazon S3 マネージドキーの代わりにカスタマーマネージドキー (CMK) を使用して、AWS KMS keys (SSE-KMS) でサーバー側の暗号化を使用することもできます。

バケットポリシーの内容

バケットポリシーを使用すると、組織内のメンバーアカウントが互いに検出することを防ぐことができます。バケットに対する読み取りおよび書き込み許可は、Systems Manager に対して作成された診断および修復ロールにのみ許可されます。こうしたシステム生成のポリシーの内容については、「Systems Manager 統合コンソールの S3 バケットポリシー」を参照してください。

> **Warning**
>
> デフォルトのバケットポリシーを変更すると、組織内のメンバーアカウントが相互に発見したり、他のアカウントのインスタンスの診断出力を読み取ったりできるようになる可能性があります。このポリシーを変更する場合は、細心の注意を払うことをお勧めします。

トピック

- S3 リソースを暗号化するための AWS KMS カスタマーマネージドキーへの変更
- Systems Manager 統合コンソールの S3 バケットポリシー

S3 リソースを暗号化するための AWS KMS カスタマーマネージドキーへの変更

Systems Manager の統合コンソールのオンボーディングプロセス中に、Quick Setup は委任管理者アカウントに Amazon Simple Storage Service (Amazon S3) バケットを作成します。このバケットは、修復ランブックの実行中に生成された診断出力データを保存するために使用されます。デフォルトでは、このバケットは Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3) を使用します。

これらのポリシーのコンテンツについては、「Systems Manager 統合コンソールの S3 バケットポリシー」を参照してください。

ただし、AWS KMS keyの代わりにカスタマーマネージドキー (CMK) を使用して、AWS KMS keys によるサーバー側の暗号化 (SSE-KMS) を使用することもできます。

CMK を使用するように Systems Manager を設定するには、以下のタスクを実行します。

タスク 1: 既存の CMK にタグを追加する

AWS Systems Manager は、次のキーと値のペアでタグ付けされている場合にのみ CMK を使用します。

- キー: `SystemsManagerManaged`
- 値: `true`

次の手順を使用して、CMK で S3 バケットを暗号化するためのアクセス権を付与します。

既存の CMK にタグを追加する手順

1. AWS KMS コンソール (https://console.aws.amazon.com/kms) を開きます。
2. 左のナビゲーションで、[カスタマーマネージドキー] を選択します。
3. AWS Systems Manager で使用する AWS KMS keyを選択します。
4. [タグ] タブを選択し、次に [編集] を選択します。
5. [タグを追加] を選択します。
6. 以下の操作を実行します。
   a. [Tag key (タグキー)] に、**SystemsManagerManaged** と入力します。
   b. [タグ値] に **true** と入力します。
7. [保存] を選択します。

タスク 2: 既存の CMK キーポリシーを変更する

次の手順を使用して、AWS Systems Manager のロールがユーザーの代わりに S3 バケットを暗号化できるように、CMK の KMS キーポリシーを更新します。

既存の CMK キーポリシーを変更する手順

1. AWS KMS コンソール (https://console.aws.amazon.com/kms) を開きます。
2. 左のナビゲーションで、[カスタマーマネージドキー] を選択します。
3. AWS Systems Manager で使用する AWS KMS keyを選択します。
4. アクセスポリシー タブで 編集 を選択します。
5. 次の JSON ステートメントを `Statement` フィールドに追加し、*`#########`*を独自の情報に置き換えます。

   AWS Systems Manager にオンボーディングされている組織内のすべての AWS アカウント ID を、`Principal` フィールドに追加する必要があります。

   Amazon S3 コンソールで正しいバケット名を見つけるには、委任管理者アカウントで、`do-not-delete-ssm-`*`operational-account-id`*`-`*`home-region`*`-`*`disambiguator`* の形式のバケットを探します。

```
{
     "Sid": "EncryptionForSystemsManagerS3Bucket",
```

```
        "Effect": "Allow",
        "Principal": {
            "AWS": [
                "account-id-1",
                "account-id-2",
                ...
            ]
        },
        "Action": ["kms:Decrypt", "kms:GenerateDataKey"],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-bucket"
            },
            "StringLike": {
                "kms:ViaService": "s3.*.amazonaws.com"
            },
            "ArnLike": {
                "aws:PrincipalArn": "arn:aws:iam::*:role/AWS-SSM-*"
            }
        }
    }
```

> **Tip**
>
> または、aws:PrincipalOrgID 条件キーを使用して CMK キーポリシーを更新することにより、AWS Systems Manager に CMK へのアクセスを許可することもできます。

タスク 3: Systems Manager 設定で CMK を指定する

上記の 2 つのタスクを完了したら、次の手順を使用して S3 バケットの暗号化を変更します。この変更により、関連付けられた Quick Setup 設定プロセスで、Systems Manager が CMK を受け入れるためのアクセス許可を追加できるようになります。

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで [設定] を選択します。
3. [診断および修復] タブの [S3 バケットの暗号化の更新] セクションで、[編集] を選択します。
4. [暗号化設定のカスタマイズ (高度)] チェックボックスを選択します。

5. 検索
   (🔍)
   ボックスで、既存のキーの ID を選択するか、既存のキーの ARN を貼り付けます。
6. [保存] を選択します。

Systems Manager 統合コンソールの S3 バケットポリシー

このトピックでは、組織または単一アカウントを Systems Manager 統合コンソールにオンボーディングする際に Systems Manager によって作成される Amazon S3 バケットポリシーについて説明します。

> ⚠ Warning
>
> デフォルトのバケットポリシーを変更すると、組織内のメンバーアカウントが相互に発見したり、他のアカウントのインスタンスの診断出力を読み取ったりできるようになる可能性があります。このポリシーを変更する場合は、細心の注意を払うことをお勧めします。

組織の Amazon S3 バケットポリシー

診断バケットは、組織を Systems Manager にオンボーディングする際に、次のデフォルトのバケットポリシーを使用して作成されます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyHTTPRequests",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ],
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            }
```

```
        },
        {
            "Sid": "DenyNonSigV4Requests",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "s3:SignatureVersion": "AWS4-HMAC-SHA256"
                }
            }
        },
        {
            "Sid": "AllowAccessLog",
            "Effect": "Allow",
            "Principal": {
                "Service": "logging.s3.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/access-logs/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "operational-account-id"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:::amzn-s3-demo-bucket"
                }
            }
        },
        {
            "Sid": "AllowCrossAccountRead",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/actions/*/
${aws:PrincipalAccount}/*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "organization-id"
                }
```

```
            }
        },
        {
            "Sid": "AllowCrossAccountWrite",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "s3:PutObject",
                "s3:DeleteObject"
            ],
            "Resource": "arn:aws:s3:::bucket-name/actions/*/${aws:PrincipalAccount}/*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "organization-id"
                },
                "ArnLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::*:role/AWS-SSM-
DiagnosisExecutionRole-operational-account-id-home-region",
                        "arn:aws:iam::*:role/AWS-SSM-DiagnosisAdminRole-operational-
account-id-home-region",
                        "arn:aws:iam::*:role/AWS-SSM-
RemediationExecutionRole-operational-account-id-home-region",
                        "arn:aws:iam::*:role/AWS-SSM-RemediationAdminRole-operational-
account-id-home-region"
                    ]
                }
            }
        },
        {
            "Sid": "AllowCrossAccountListUnderAccountOwnPrefix",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "organization-id"
                },
                "StringLike": {
                    "s3:prefix": "*/${aws:PrincipalAccount}/*"
                }
            }
        },
```

```
        {
            "Sid": "AllowCrossAccountGetConfigWithinOrganization",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetEncryptionConfiguration",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "organization-id"
                }
            }
        }
    ]
}
```

単一アカウントの Amazon S3 バケットポリシー

診断バケットは、単一アカウントを Systems Manager にオンボーディングする際に、次のデフォルトのバケットポリシーを使用して作成されます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyHTTPRequests",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket",
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {
        "Bool": {
          "aws:SecureTransport": "false"
        }
      }
    },
    {
      "Sid": "DenyNonSigV4Requests",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
```

```
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket",
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "s3:SignatureVersion": "AWS4-HMAC-SHA256"
        }
      }
    }
  ]
}
```

AWS Systems Manager ツールの使用方法

Systems Manager のツールには以下の 4 つのカテゴリがあります。以下のドキュメントでは、AWS Systems Manager のさまざまなツールと、そのセットアップおよび使用方法について説明します。各カテゴリのタブをクリックすると、各ツールの詳細が表示されます。

ノードツール

マネージドノードとは、ハイブリッドおよびマルチクラウド環境で Systems Manager で使用するように設定された任意のマシンです。

Compliance

マネージドノードのフリートをスキャンし、パッチコンプライアンスと設定の整合性を検出するには、Compliance を使用します。複数の AWS アカウント と AWS リージョン からデータを収集して集計し、それに準拠していない特定のリソースにドリルダウンすることができます。デフォルトで、設定コンプライアンスは Patch Manager のパッチ適用、および State Manager の関連付けに関する現在のコンプライアンスデータを表示します。サービスをカスタマイズし、IT またはビジネスの要件に基づいて独自のコンプライアンスタイプを作成することもできます。

ディストリビューター

Distributor により、デプロイパッケージを作成してマネージドノードに展開します。Distributor で、自分のソフトウェアをパッケージ化または AWS を提供するエージェントソフトウェアパッケージ (AmazonCloudWatchAgent など) を探して Systems Manager のマネージドノードにインストールすることができます。初めてパッケージをインストールした後、Distributor を使用して新しいパッケージバージョンのアンインストールと再インストールするか、新しいまたは変更されたファイルを追加するインプレース更新を実行できます。Distributor はソフトウェアパッケージなどのリソースを Systems Manager のマネージドノードに発行します。

Fleet Manager

Fleet Manager は、統合されたユーザーインターフェイス (UI) エクスペリエンスであり、ノードをリモートから管理することに役たちます。Fleet Manager で 1 つのコンソールからフリート全体の正常性とパフォーマンスステータスを確認できます。個別のデバイスとインスタンスからデータを収集して、コンソールから一般的なトラブルシューティングと管理タスクを実行することもできます。これには、ディレクトリとファイルの内容の表示、Windows レジストリ管理、オペレーティングシステムのユーザー管理などが含まれます。

Hybrid Activations

ハイブリッドおよびマルチクラウド環境の非 EC2 マシンをマネージドノードとしてセットアップするには、ハイブリッドアクティベーションを作成します。アクティベーションが完了したら、アクティベーションコードと ID を受け取ります。このコードと ID の組み合わせは Amazon Elastic Compute Cloud (Amazon EC2) のアクセス ID とシークレット キーのように機能し、マネージドインスタンスから Systems Manager サービスへの安全なアクセスを可能になります。

Systems Manager を使用してエッジデバイスを管理する場合、エッジデバイス用のアクティベーションを作成することもできます。

Inventory

インベントリは、マネージドノードからのソフトウェアインベントリの収集プロセスを自動化します。インベントリでアプリケーション、ファイル、コンポーネント、パッチなどに関するメタデータを収集できます。

Patch Manager

Patch Manager を使用して、セキュリティ関連とその他のアップデートの両方でマネージドノードにパッチ適用するプロセスを自動化します。Patch Manager を使用すると、オペレーティングシステムとアプリケーションの両方にパッチを適用することができます。(Windows Server では、アプリケーションのサポートは、Microsoft がリリースしたアプリケーションの更新に制限されています)。

このツールはマネージドノードをスキャンして欠落パッチを確認し、タグを使用して個別またはマネージドノードの大グループに欠落パッチを適用することを実現します。Patch Manager はパッチベースラインを使用し、リリースから数日以内にパッチを自動承認するルールと、承認済と拒否済みパッチのリストが含まれています。Systems Manager のメンテナンスウィンドウタスクとしてパッチを実行するようスケジュールすることにより、セキュリティパッチを定期的にインストールでき、またはいつでもオンデマンドでマネージドノードにパッチを適用できます。

Linux オペレーティングシステムの場合、パッチベースラインの一部として、パッチ適用オペレーションに使用するレポジトリを定義できます。これにより、マネージドノードで設定されたレポジトリとは関係なく、信頼されたレポジトリからのみ更新プログラムがインストールされることを保証します。Linux の場合、オペレーティングシステムのセキュリティ更新として分類されているものだけでなく、マネージドノードでどのようなパッケージでも更新する機能があります。任意の S3 バケットに送信されるパッチレポートを生成することもできます。1 つのマネージドノードの場合、レポートはマシンに適用されたすべてのパッチ詳細が含まれます。すべての

マネージドノードに関するレポートでは、欠けているパッチの数についての概要のみが提供されます。

Run Command

Run Command を使用すると、マネージドノードの設定を、安全にリモートで大規模に管理することができます。Run Command を使用して、数十または数百台のマネージドノードのターゲットセットに対して、アプリケーションの更新、または Linux シェルスクリプトと Windows PowerShell コマンドの実行といった変更をオンデマンドで行います。

セッションマネージャー

Session Manager により、インタラクティブなブラウザ ベースのワンクリックシェルまたは AWS CLI を介して、エッジデバイスと Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを管理できます。Session Manager は、インバウンドポートを開いたり、踏み台ホストを維持したり、SSH キーを管理したりする必要がなく、安全で監査可能なエッジデバイスとインスタンスの管理を実現します。同時に Session Manager では、エッジデバイスとインスタンスへ制御されたアクセス、厳格なセキュリティプラクティス、エッジデバイスとインスタンスへのアクセス詳細を含む完全に監査可能なログを必要とする企業ポリシーの遵守を可能にしつつ、エンドユーザーに対しては、エッジデバイスと EC2 インスタンスへのワンクリックによる簡単なクロスプラットフォームアクセスを提供します。Session Manager を使用する場合、アドバンストインスタンス層を有効にする必要があります。詳細については、「アドバンストインスタンス層を有効にするには」を参照してください。

ステートマネージャー

マネージドノードを定義された状態に維持するためのプロセスを自動化するには、State Manager を使用します。State Manager を使用してマネージドノードがスタートアップ時に特定のソフトウェアでブートストラップされ、Windows ドメイン (Windows Server ノードのみ) に結合され、または特定のソフトウェア更新でパッチが適用されることを保証します。

変更管理ツール

Automation

メンテナンスとデプロイでの一般的なタスクを自動化するには、オートメーションを使用します。オートメーションを使用すると、Amazon Machine Images (AMIs) の作成と更新、ドライバーとエージェントの更新プログラムの適用、Windows Server インスタンスでのパスワードのリセット、Linux インスタンスでの SSH キーのリセット、OS パッチまたはアプリケーション更新プログラムの適用が可能になります。

Change Calendar

Change Calendar では、(Systems Manager Automation ランブックなどで) 指定したアクションを AWS アカウント で実行できる、または実行できない日時の範囲を設定できます。Change Calendar では、これらの範囲をイベントと呼びます。Change Calendar エントリを作成すると、ChangeCalendar タイプの Systems Manager ドキュメントが作成されます。Change Calendar では、ドキュメントに iCalendar 2.0 データがプレーンテキスト形式で保存されます。Change Calendar エントリに追加したイベントは、ドキュメントの一部になります。Change Calendar インターフェイスでイベントを手動で追加したり、.ics ファイルを使用して、サポートされているサードパーティーのカレンダーからイベントをインポートしたりできます。

Change Manager

Change Manager は、アプリケーションの設定やインフラストラクチャに対する運用上の変更を要求、承認、実装、レポート作成するためのエンタープライズ変更管理フレームワークです。AWS Organizations を使用すると、単一の委任された管理者アカウントから、複数の AWS リージョン の複数の AWS アカウント にまたがる変更を管理できます。または、ローカルアカウントを使用して、単一の AWS アカウント の変更を管理できます。AWSリソースとオンプレミスリソースの両方に対する変更を管理する場合に Change Manager を使用します。

Documents

Systems Manager ドキュメント (SSM ドキュメント) は、Systems Manager が実行する操作を定義します。SSM ドキュメントタイプには、State Manager と Run Command で使用される Command ドキュメントや、Systems Manager Automation で使用される Automation ランブックなどがあります。Systems Manager には、実行時にパラメータを指定して使用できる事前設定済みのドキュメントが 数十件含まれています。ドキュメントは JSON や YAML で表すことができ、ユーザーが指定するパラメータおよびステップが含まれます。

メンテナンスウィンドウ

Maintenance Windows を使用して、ビジネスクリティカルなオペレーションを中断することなく、パッチや更新プログラムのインストールなどの管理タスクを実行するように、マネージドインスタンスの定期的なスケジュールを設定します。

Quick Setup

Quick Setup により、頻繁に使用する AWS のサービスと機能を、推奨されるベストプラクティスを使用して設定できます。AWS Organizations との統合により、個々の AWS アカウント で、または複数の AWS アカウント と AWS リージョン にまたがって Quick Setup を使用で

きます。Quick Setup は、一般的なタスクや推奨されるタスクを自動化することで、Systems Manager などのサービスのセットアップを簡素化します。これらのタスクには、例えば、必須の AWS Identity and Access Management (IAM) インスタンスプロファイルロールの作成、定期的なパッチスキャンやインベントリ収集などの運用上のベストプラクティスの設定が含まれます。

アプリケーションツール

AppConfig

AppConfig は、アプリケーション設定や機能フラグを作成、管理、デプロイする際に有用です。AppConfig では、あらゆる規模のアプリケーションへの管理型デプロイがサポートされています。AppConfig は、Amazon EC2 インスタンス、AWS Lambda コンテナ、モバイルアプリケーション、エッジデバイスでホストされているアプリケーションで使用できます。アプリケーション設定のデプロイ時のエラーを防ぐため、AppConfig にはバリデータが含まれています。バリデータは構文チェックまたはセマンティックチェックを実施して、デプロイする設定が意図したとおりに動作することを確認します。AppConfig は設定のデプロイ中、アプリケーションをモニタリングしてデプロイが正常に実施されたことを確認します。システムでエラーが発生した場合、またはデプロイによってアラームが呼び出された場合、AppConfig は変更をロールバックして、アプリケーションユーザーへの影響を最小限に抑えます。

Application Manager

Application Manager は、DevOps エンジニアがアプリケーションとクラスターのコンテキストで AWS リソースの問題を調査および修正する際に役立ちます。Application Manager では、アプリケーションはユニットとして動作する AWS リソースの論理グループです。この論理グループは、アプリケーションのさまざまなバージョン、オペレーターの所有権の境界、デベロッパー環境などを表すことができます。Application Manager は Amazon Elastic Kubernetes Service (Amazon EKS) クラスターと Amazon Elastic Container Service (Amazon ECS) クラスターの両方を含むコンテナクラスターをサポートしています。Application Manager は複数の AWS のサービスや Systems Manager ツールの運用情報を単一の AWS Management Consoleに集約します。

パラメータストア

Parameter Store は、設定データ管理と機密管理のための安全な階層型ストレージを提供します。パスワード、データベース文字列、Amazon Elastic Compute Cloud (Amazon EC2)、Amazon Machine Image (AMI) ID、ライセンスコードなどのデータをパラメータ値として保存できます。値はプレーンテキストまたは暗号化されたデータとして保存できます。次に、パラメータの作成時に指定した一意の名前を使用して値を参照できます。

運用ツール

CloudWatch Dashboards

Amazon CloudWatch ダッシュボードは、CloudWatch コンソールにあるカスタマイズ可能なページであり、ダッシュボードを使用すれば、異なるリージョンにまたがっているリソースでも、1 つのビューでモニタリングできます。CloudWatch ダッシュボードを使用して、AWS リソースのメトリクスおよびアラームをカスタマイズした状態で表示することができます。

Explorer

Explorer は、AWS リソースに関する情報の報告に使用するカスタマイズ可能なオペレーションダッシュボードです。Explorer には、AWS アカウント および AWS リージョン 全体のオペレーションデータ (OpsData) の集約的なビューが表示されます。Explorer では、OpsData に Amazon EC2 インスタンス、パッチコンプライアンスの詳細、および運用作業項目 (OpsItems) に関するメタデータが含まれています。Explorer では、OpsItems が事業部門またはアプリケーション全体にどのように分散されているか、それらが時間の経過とともにどのような傾向を示すか、およびカテゴリによってどのように異なるかに関するコンテキストが提供されます。Explorer で情報をグループ化およびフィルタリングすると、自身に関連する項目や、アクションが必要な項目に注目することができます。優先度の高い問題を特定したら、Systems Manager のツールである OpsCenter を使用して Automation ランブックを実行し、問題を解決できます。

Incident Manager

Incident Manager は、AWS がホストするアプリケーションに影響を与えるインシデントを、ユーザーが緩和したりそのようなインシデントから復旧したりできるように設計された、インシデントマネジメントコンソールです。

Incident Manager は、影響をレスポンダーに通知し、関連するトラブルシューティングデータを強調表示し、サービスをバックアップして実行するためのコラボレーションツールを提供することで、インシデントの解決を向上させます。また、Incident Manager は応答計画を自動化して、応答者チームのエスカレーションも可能にします。

OpsCenter

OpsCenter は、オペレーションエンジニアや IT プロフェッショナルが AWS リソースに関連する運用作業項目 (OpsItems) を表示、調査、解決できる一元的な場所を提供します。OpsCenter は、AWS リソースに影響を与える問題の解決までの平均時間を、短縮する目的で設計されています。この Systems Manager ツールでは、各 OpsItem、関連のある OpsItems、および関連リソースに関する状況に応じた調査データを提供しながら、サービス間で OpsItems を集約および標準化します。また、OpsCenter では、問題の解決に使用できる Systems Manager Automation

ランブックも提供しています。検索可能なカスタムデータを OpsItem ごとに指定することができます。OpsItems について自動的に生成された概要レポートは、ステータスとソース別に表示することもできます。

Systems Manager を使用したノードタスクの実行

このチュートリアルにより、AWS Systems Manager の使用を開始できます。Systems Manager によって管理される Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを起動する方法と、マネージドインスタンスに接続する方法について説明します。

Systems Manager は複数のツールのコレクションであるため、1 つのチュートリアルやウォークスルーでサービス全体を紹介することはできません。このチュートリアルでは、いくつかのツールの概要について説明します。

前提条件

開始する前に、Systems Manager を利用した EC2 インスタンスの管理 の手順を完了するようにしてください。

SSM Agent がプリインストールされた AMI を使用してインスタンスを起動する

以下の手順で説明しているように、AWS Management Console を使用して Amazon EC2 インスタンスを起動できます。このチュートリアルは、初めてのマネージドインスタンスをすばやく起動するように想定されています。そのため、すべての可能なオプションを網羅してはいません。

インスタンスを起動するには

1. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
2. EC2 コンソールダッシュボードから、[Launch instance] (インスタンスを起動する) ボックス内で [Launch instance] (インスタンスを起動する) を選び、表示されるオプションから [Launch instance] (インスタンスを起動する) を選びます。
3. [名前とタグ] の [名前] には、インスタンス用のわかりやすい名前を入力します。
4. [アプリケーションと OS イメージ (Amazon マシンイメージ)] で、次の操作を行います。

    a. [Quick Start] タブを選択してから、Amazon Linux を選択します。これが、インスタンスのオペレーティングシステム (OS) です。

    b. [Amazon マシンイメージ (AMI)] で、Amazon Linux 2 の HVM バージョンを選択します。

5. [インスタンスタイプ] の [インスタンスタイプ] リストから、インスタンスのハードウェア構成を選択します。`t2.micro` インスタンスタイプを選択します。デフォルトではこれが選択されています。`t2.micro` インスタンスタイプは AWS 無料利用枠の対象です。`t2.micro` を利用できない AWS リージョン では、無料利用枠で `t3.micro` インスタンスを使用できます。詳細については、AWS 無料利用枠を参照してください。
6. [キーペア (ログイン)] の [キーペア名] で、キーペアを選択します。
7. [ネットワーク設定] で、[編集] を選択します。[セキュリティグループ名] に、ウィザードで作成して選択したセキュリティグループが表示されます。このセキュリティグループを使用するか、次のステップを使用して前に作成したセキュリティグループを選択できます。

   a. [Select existing security group] (既存のセキュリティグループを選択) を選択します。
   b. [Common security groups] (共通セキュリティグループ) から、既存のセキュリティグループのリストからセキュリティグループを選択します。
8. デフォルトのホスト管理設定を使用していない場合は [高度な詳細] セクションを展開し、[IAM インスタンスプロファイル] では、Systems Manager に必要なインスタンスのアクセス許可を設定する でセットアップ時に作成したインスタンスプロファイルを選択します。
9. インスタンスの他の構成設定については、デフォルトの選択のままにします。
10. [概要] ペインで、インスタンス設定の概要を確認します。準備ができたら、[インスタンスの起動] を選択します。
11. 確認ページに、インスタンスが起動中であることが表示されます。[View all instances] (すべてのインスタンスの表示) を選択して確認ページを閉じ、コンソールに戻ります。
12. インスタンス画面で、起動のステータスを確認できます。インスタンスの起動には短時間かかります。
13. インスタンスがマネージドとして表示され、接続できるようになるまでに数分かかる場合があります。インスタンスがステータスチェックに合格したことを確認するには、情報を [ステータスチェック] 列に表示します。

Systems Manager を使用してマネージドインスタンスに接続する

マネージドインスタンスに接続するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. 接続するインスタンスの横にあるボタンを選択します。

4. [ノードアクション] メニューで、[ターミナルセッションの開始] を選択します。
5. [Connect] (接続) を選択します。

インスタンスのクリーンアップ

このチュートリアル用に作成したマネージドインスタンスの操作が完了したら、終了します。インスタンスを終了すると、インスタンスは実質的に削除されます。

インスタンスを終了するには

1. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
2. ナビゲーションペインで、[インスタンス] を選択します。インスタンスの一覧で、インスタンスを選択してください。
3. [Instance state (インスタンスの状態)]、[Terminate instance (インスタンスの終了)] の順に選択してください。
4. 確認を求めるメッセージが表示されたら、[Terminate (終了)] を選択してください。

   Amazon EC2 によって、インスタンスがシャットダウンおよび終了します。インスタンスの終了後、インスタンスはしばらくの間コンソールに表示されたままになりますが、エントリは自動的に削除されます。終了したインスタンスを自分でコンソールディスプレイから削除することはできません。

AWS Systems Manager ノードツール

AWS Systems Manager は、マネージドノードにアクセスし、管理および設定するために次のツールを提供します。マネージドノードは、ハイブリッドおよびマルチクラウド環境内の Systems Manager 用に設定されたあらゆるマシンです。

トピック

- AWS Systems Manager のコンプライアンス
- AWS Systems Manager Distributor
- AWS Systems Manager Fleet Manager
- AWS Systems Manager ハイブリッドアクティベーション
- AWS Systems Manager インベントリ
- AWS Systems Manager Patch Manager

- AWS Systems Manager Run Command
- AWS Systems Manager Session Manager
- AWS Systems Manager State Manager

AWS Systems Manager のコンプライアンス

AWS Systems Manager のツールである Compliance を使ってマネージドノードのフリートをスキャンし、パッチコンプライアンスと設定の不整合を調べるために使用できます。複数の AWS アカウント とリージョンからデータを収集して集計し、それに準拠していない特定のリソースにドリルダウンすることができます。デフォルトで、Compliance は Patch Manager のパッチ適用、および State Manager の関連付けに関する現在のコンプライアンスデータを表示します (Patch Manager と State Manager は AWS Systems Manager のツールです)。コンプライアンスの使用を開始するには、Systems Manager コンソールを開きます。ナビゲーションペインで、[コンプライアンス] を選択します。

Patch Manager からパッチコンプライアンスデータを AWS Security Hub に送信できます Security Hub では、高優先度のセキュリティアラートとコンプライアンス状況を包括的に確認できます。また、フリートのパッチ適用状況も監視できます。詳細については、「Patch Managerと AWS Security Hub の統合」を参照してください。

コンプライアンスには、さらに次のような利点と特徴があります。

- AWS Config を使用して、Patch Managerによるパッチの適用のデータやState Managerによる関連付けに関するコンプライアンスの履歴や変更の追跡を表示できます。
- Compliance をカスタマイズして、IT またはビジネスの要件に基づいた独自のコンプライアンスタイプを作成できます。
- AWS Systems Manager のツールである Run Command、State Manager、または Amazon EventBridge を使用して、問題を修復します。
- Amazon Athena と Amazon QuickSight にデータを移植して、フリート全体のレポートを生成します。

EventBridge のサポート

この Systems Manager ツールは、Amazon EventBridge ルールのイベントタイプとしてサポートされています。詳細については、「Amazon EventBridge を使用して Systems Manager イベントをモ

ニタリングする」および「リファレンス: Systems Manager 用の Amazon EventBridge イベントパターンとタイプ」を参照してください。

Chef InSpec の統合

Systems Manager は、Chef InSpec と統合します。InSpec は、オープンソースのランタイムフレームワークであり、人間が読み取れるプロファイルを GitHub または Amazon Simple Storage Service (Amazon S3) で作成できます。その後、Systems Manager を使用してコンプライアンススキャンを実行し、準拠または非準拠のマネージドノードを表示できます。詳細については、「Systems Manager Compliance で Chef InSpec プロファイルを使用する」を参照してください。

料金

設定コンプライアンスは、追加料金なしで提供されています。お客様は、使用した AWS リソースに対してのみ料金を支払います。

内容

- 設定コンプライアンスの使用開始方法
- Compliance のアクセス許可の設定
- Compliance のためのリソースデータ同期の作成
- コンプライアンスの詳細について
- Compliance のためのリソースデータ同期の削除
- EventBridge を使用してコンプライアンス問題を修復する
- AWS CLI を使用してカスタムコンプライアンスメタデータを割り当てる

設定コンプライアンスの使用開始方法

AWS Systems Manager のツールである Compliance の使用を開始するには、以下のタスクを完了してください。

タスク	詳細情報
Compliance では、Patch Manager のパッチデータと State Manager の関連付けを使用できます。(Patch Manager と State Manager は AWS Systems Manager のツールです。) Compliance は、Systems Manager を使用して	組織用の Systems Manager 統合コンソールのセットアップ

タスク	詳細情報
管理されるマネージドノードのカスタムコンプライアンスタイプでも機能します。ハイブリッドおよびマルチクラウド環境で、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスと非 EC2 マシンのセットアップ要件を完了していることを確認します。	
マネージドノードで使用される AWS Identity and Access Management (IAM) ロールを更新して、Compliance のアクセス許可を制限します。	Compliance のアクセス許可の設定
パッチのコンプライアンスをモニタリングする場合は、Patch Manager を設定していることを確認します。設定コンプライアンスでパッチのコンプライアンスデータを表示するには、その前に Patch Manager を使用してパッチ適用操作を実行しておく必要があります。	AWS Systems Manager Patch Manager
関連付けのコンプライアンスをモニタリングする場合は、State Manager の関連付けを作成したことを確認します。設定コンプライアンスで関連付けのコンプライアンスデータを表示するには、その前に関連付けを作成しておく必要があります。	AWS Systems Manager State Manager
(オプション) コンプライアンス履歴および変更の追跡が表示されるようにシステムを設定します。	コンプライアンスの設定履歴と変更の追跡の表示
(オプション) カスタムコンプライアンスタイプを作成します。	AWS CLI を使用してカスタムコンプライアンスメタデータを割り当てる

タスク	詳細情報
(オプション) リソースデータ同期を作成して、ターゲットの Amazon Simple Storage Service (Amazon S3) バケット内のすべてのコンプライアンスデータを集計します。	Compliance のためのリソースデータ同期の作成

Compliance のアクセス許可の設定

セキュリティのベストプラクティスとして、マネージドノードで使用される AWS Identity and Access Management (IAM) ロールを以下のアクセス許可で更新して、ノードが PutComplianceItems API アクションを使用する機能を制限することをお勧めします。この API アクションは、Amazon EC2 インスタンスやマネージドノードなど、指定されたリソースにコンプライアンスタイプやその他のコンプライアンスの詳細を登録します。

ノードが Amazon EC2 インスタンスの場合は、インスタンスで使用される IAM インスタンスプロファイルを次のアクセス許可で更新する必要があります。Systems Manager によって管理される EC2 インスタンスのインスタンスプロファイルの詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」を参照してください。他のタイプのマネージドノードでは、ノードで使用される IAM ロールを次のアクセス許可で更新します。詳細については、「IAM ユーザーガイド」の「ロールに対するアクセス許可を更新する」を参照してください。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:PutComplianceItems"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:SourceInstanceARN": "${ec2:SourceInstanceARN}"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                "ssm:PutComplianceItems"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ssm:SourceInstanceARN": "${ssm:SourceInstanceARN}"
                }
            }
        }
    ]
}
```

Compliance のためのリソースデータ同期の作成

AWS Systems Manager のリソースデータ同期機能を使用して、すべてのマネージドノードからターゲットの Amazon Simple Storage Service (Amazon S3) バケットにコンプライアンスデータを送信できます。同期を作成するときは、複数の AWS アカウント、AWS リージョン およびオンプレミスのハイブリッドおよびマルチクラウド環境からのマネージドノードを指定できます。その後、リソースデータの同期により、新しいコンプライアンスデータが収集されると一元化されたデータが自動的に更新されます。ターゲット S3 バケットに保存されたすべてのコンプライアンスデータに対して、Amazon Athena や Amazon QuickSight などのサービスを使用して集計データのクエリや分析ができます。Compliance のためのリソースデータ同期の設定は、1 回限りの操作です。

次の手順に従って、AWS Management Console を使用して Compliance のためのリソースデータ同期の作成を行います。

リソースデータの同期用に S3 バケットを作成して設定するには (コンソール)

1. Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 集計されたコンプライアンスデータを保存するバケットを作成します。詳細については、Amazon Simple Storage Service ユーザーガイドの「バケットの作成」を参照してください。バケット名とそれを作成した AWS リージョン を書き留めます。
3. バケットを開き、[Permissions (アクセス許可)] タブ、[Bucket Policy (バケットポリシー)] の順に選択します。
4. 次のバケットポリシーをコピーし、ポリシーエディタに貼り付けます。amzn-s3-demo-bucket と *Account-ID* を、作成した S3 バケットの名前と有効な AWS アカウント ID に置き換えます。任意で、*Bucket-Prefix* を Amazon S3 プレフィックス (サブディレクトリ) に置き換えます。プレフィックスを作成しなかった場合は、*Bucket-Prefix*/ をこのポリシーの ARN から削除します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SSMBucketPermissionsCheck",
            "Effect": "Allow",
            "Principal": {
                "Service": "ssm.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
        },
        {
            "Sid": " SSMBucketDelivery",
            "Effect": "Allow",
            "Principal": {
                "Service": "ssm.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket/Bucket-Prefix/*/
accountid=Account_ID_number/*"],
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control"
                }
            }
        }
    ]
}
```

リソースデータの同期を作成するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. [アカウント管理]、[リソースデータの同期] の順に選択し、[リソースデータの同期の作成] を選択します。
4. [Sync name] フィールドに、同期設定の名前を入力します。

5. [Bucket name] フィールドに、この手順の最初で作成した Amazon S3 バケットの名前を入力します。
6. (オプション) [Bucket prefix] フィールドに、S3 バケットのプレフィックス (サブディレクトリ) の名前を入力します。
7. 作成した S3 バケットが現在の AWS リージョン にある場合は、[バケットリージョン] フィールドで [このリージョン] を選択します。バケットが他の AWS リージョン にある場合は、[Another region(別のリージョン)] を選択して、リージョンの名前を入力します。

> **Note**
>
> 同期とターゲット S3 バケットが異なるリージョンにある場合は、データ転送料金が発生する場合があります。詳細については、Amazon S3 の料金 を参照してください。

8. [Create] (作成) を選択します。

コンプライアンスの詳細について

AWS Systems Manager のツールである Compliance は、Patch Manager パッチ適用のステータスと State Manager の関連付けに関するデータを収集して報告します。(Patch Manager と State Manager も AWS Systems Manager のツールです。) Compliance では、マネージドノードに対して指定したカスタムコンプライアンスタイプについてもレポートします。このセクションでは、各コンプライアンスタイプに関する詳細および Systems Manager のコンプライアンスデータを表示する方法について説明します。このセクションでは、コンプライアンス履歴および変更の追跡を表示する方法についても説明します。

> **Note**
>
> Systems Manager は、Chef InSpec と統合します。InSpec は、オープンソースのランタイムフレームワークであり、人間が読み取れるプロファイルを GitHub または Amazon Simple Storage Service (Amazon S3) で作成できます。その後、Systems Manager を使用してコンプライアンススキャンを実行し、準拠または非準拠のインスタンスを表示できます。詳細については、「Systems Manager Compliance で Chef InSpec プロファイルを使用する」を参照してください。

パッチコンプライアンスについて

Patch Manager を使用してインスタンスにパッチをインストールすると、コンソールでも、AWS Command Line Interface (AWS CLI) コマンドまたは対応する Systems Manager API オペレーションへのレスポンスでも、コンプライアンスステータス情報をすぐに表示できるようになります。

パッチのコンプライアンスステータス値については、「パッチコンプライアンス状態の値」を参照してください。

State Manager 関連付けのコンプライアンスについて

State Manager の関連付けを 1 つまたは複数作成すると、コンソールでも、 AWS CLI コマンドまたは対応する Systems Manager API オペレーションへのレスポンスでも、コンプライアンスステータス情報をすぐに表示できるようになります。関連付けについては、設定コンプライアンスが `Compliant` または `Non-compliant` のステータス、および `Critical` または `Medium` などの関連付けに割り当てられた重大度レベルを表示します。

カスタムコンプライアンスについて

マネージドノードにコンプライアンスメタデータを割り当てることができます。このメタデータは、次にコンプライアンスの報告の目的で、他のコンプライアンスデータと集計できます。たとえば、ビジネスでソフトウェア X のバージョン 2.0、3.0、および 4.0 をマネージドノードで実行しているとします。会社はバージョン 4.0 で標準化したいと考えています。つまり、バージョン 2.0 と 3.0 を実行しているインスタンスは非準拠です。PutComplianceItems API オペレーションを使用して、古いバージョンのソフトウェア X を実行しているマネージドノードを明示的に確認できます。AWS CLI、AWS Tools for Windows PowerShell、または SDK のみを使用して、コンプライアンスのメタデータを割り当てることができます。次の CLI サンプルコマンドは、マネージドインスタンスにコンプライアンスメタデータを割り当て、必要な形式 `Custom:` でコンプライアンスタイプを指定します。各*##########*をユーザー自身の情報に置き換えます。

Linux & macOS

```
aws ssm put-compliance-items \
    --resource-id i-1234567890abcdef0 \
    --resource-type ManagedInstance \
    --compliance-type Custom:SoftwareXCheck \
    --execution-summary ExecutionTime=AnyStringToDenoteTimeOrDate \
    --items
 Id=Version2.0,Title=SoftwareXVersion,Severity=CRITICAL,Status=NON_COMPLIANT
```

Windows

```
aws ssm put-compliance-items ^
    --resource-id i-1234567890abcdef0 ^
    --resource-type ManagedInstance ^
    --compliance-type Custom:SoftwareXCheck ^
    --execution-summary ExecutionTime=AnyStringToDenoteTimeOrDate ^
    --items
 Id=Version2.0,Title=SoftwareXVersion,Severity=CRITICAL,Status=NON_COMPLIANT
```

> **Note**
>
> ResourceType パラメータは ManagedInstance のみをサポートしています。マネージド AWS IoT Greengrass コアデバイスにカスタムコンプライアンスを追加する場合は、ManagedInstance の ResourceType を指定する必要があります。

次に、コンプライアンスマネージャーは、準拠しているマネージドノードと準拠していないマネージドノードに関する概要を表示するか、レポートを作成できます。マネージドノードには最大 10 個の異なるカスタムコンプライアンスタイプを割り当てることができます。

カスタムコンプライアンスタイプの作成と、コンプライアンスデータの表示の例については、「AWS CLI を使用してカスタムコンプライアンスメタデータを割り当てる」を参照してください。

現在のコンプライアンスデータの表示

このセクションでは、Systems Manager コンソールおよび AWS CLI を使用してコンプライアンスデータを表示する方法について説明します。パッチおよび関連付けのコンプライアンス履歴および変更の追跡を表示する方法については、「コンプライアンスの設定履歴と変更の追跡の表示」を参照してください。

トピック

- 現在のコンプライアンスデータの表示 (コンソール)
- 現在のコンプライアンスデータの表示 (AWS CLI)

現在のコンプライアンスデータの表示 (コンソール)

Systems Manager コンソールでコンプライアンスデータを表示するには、以下の手順に従います。

Systems Manager コンソールで現在のコンプライアンスレポートを表示するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[コンプライアンス] を選択します。
3. [Compliance dashboard filtering] (コンプライアンスダッシュボードのフィルタリング) セクションで、コンプライアンスデータをフィルタリングするオプションを選択します。[Compliance resources summary] (コンプライアンスリソースの概要) セクションに、選択したフィルタに基づくコンプライアンスデータの数が表示されます。
4. リソースにドリルダウンして詳細を表示するには、[Details overview for resources] (リソースの詳細概要) エリアをクリックし、マネージドノードの ID を選択します。
5. [Instance ID] (インスタンス ID) または [Name] (名前) の詳細ページで [Configuration compliance] (設定コンプライアンス) タブを選択し、マネージドノードの詳細な設定コンプライアンスレポートを表示します。

> **Note**
>
> コンプライアンスの問題の修正については、「EventBridge を使用してコンプライアンス問題を修復する」を参照してください。

現在のコンプライアンスデータの表示 (AWS CLI)

次の AWS CLI コマンドを使用して、パッチ適用、関連付け、およびカスタムコンプライアンスタイプのコンプライアンスデータの概要を AWS CLI に表示できます。

list-compliance-summaries

指定したフィルタに従って、準拠しているパッチステータスと準拠していないパッチステータスの集計カウントを返します。(API: ListComplianceSummaries)

list-resource-compliance-summaries

リソースレベルの集計カウントを返します。概要には、指定したフィルタ基準に従って、準拠しているステータスと準拠していないステータス、およびコンプライアンス項目の重大度のカウントに関する情報が含まれます。(API: ListResourceComplianceSummaries)

次の AWS CLI コマンドを使用すると、パッチ適用に対する追加のコンプライアンスデータを表示できます。

describe-patch-group-state

パッチグループの集計されたパッチコンプライアンス状態の概要を返します。(API: DescribePatchGroupState)

describe-instance-patch-states-for-patch-group

指定したパッチグループのインスタンスに関するパッチ状態の概要を返します。(API: DescribeInstancePatchStatesForPatchGroup)

> **Note**
>
> AWS CLI を使用してパッチ適用を設定する方法およびパッチコンプライアンスの詳細を表示する方法については、「チュートリアル: AWS CLI を使用してサーバー環境にパッチを適用する」を参照してください。

コンプライアンスの設定履歴と変更の追跡の表示

Systems Manager Compliance では、マネージドノードに対する現在のパッチ適用と関連付けに関するコンプライアンスデータが表示されます。AWS Config を使用して、パッチ適用と関連付けのコンプライアンス履歴と変更の追跡を表示できます。AWS Config は、AWS アカウント の AWS リソースの設定の詳細な表示を提供します。これには、リソース間の関係と設定の履歴が含まれるため、時間の経過と共に設定と関係がどのように変わるかを確認できます。パッチ適用および関連付けのコンプライアンス履歴および変更の追跡を表示するには、AWS Config で以下のリソースを有効にしておく必要があります。

- `SSM:PatchCompliance`
- `SSM:AssociationCompliance`

AWS Config でこれらの特定のリソースを選択および設定する方法については、AWS Config デベロッパーガイドの「AWS Configで記録するリソースの選択」を参照してください。

> **Note**
>
> AWS Config の料金については、「料金」を参照してください。

Compliance のためのリソースデータ同期の削除

AWS Systems Manager コンプライアンスを使用してコンプライアンスデータを表示する必要がなくなった場合は、コンプライアンスデータ収集に使用するリソースデータ同期を削除することもお勧めします。

コンプライアンスリソースデータ同期を削除するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. [Account management (アカウント管理)] で [Resource data sync (リソースデータ同期)] を選択します。
4. リストで同期を選択します。

   > **Important**
   >
   > 必ずコンプライアンスで使用する同期を選択してください。Systems Manager では、複数のツールに対するリソースデータ同期がサポートされています。間違った同期を選択すると、Systems Manager Explorer、または Systems Manager Inventory のデータ集約が中断する可能性があります。

5. [削除] を選択します。
6. データが保存されている Amazon Simple Storage Service (Amazon S3) バケットを削除します。S3 バケットを削除する方法の詳細については、「バケットの削除」を参照してください。

EventBridge を使用してコンプライアンス問題を修復する

AWS Systems Manager のツールである Run Command を使用すると、パッチおよび関連付けのコンプライアンスの問題を迅速に修復できます。インスタンスまたは AWS IoT Greengrass コアデバイス ID またはタグのどちらかをターゲットに設定して、`AWS-RunPatchBaseline` ドキュメントまたは `AWS-RefreshAssociation` ドキュメントを実行できます。関連付けの更新またはパッチベー

スラインの再実行で、コンプライアンスの問題を解決できない場合は、関連付け、パッチベースライン、またはインスタンス設定を調査して、Run Command オペレーションで問題が解決しなかった理由を把握する必要があります。

パッチ適用の詳細については、「AWS Systems Manager Patch Manager」および「パッチ適用のための SSM コマンドドキュメント: AWS-RunPatchBaseline」を参照してください。

関連付けの詳細については、「Systems Manager の関連付けの使用」を参照してください。

コマンドの実行の詳細については、「AWS Systems Manager Run Command」を参照してください。

EventBridge イベントのターゲットとして設定コンプライアンスを指定する

Systems Manager Compliance のイベントに応じてアクションを実行するよう Amazon EventBridge を設定することもできます。例えば、1 つ以上のマネージドノードが、重要なパッチ更新のインストールまたはアンチウイルスソフトウェアをインストールする関連付けの実行に失敗する場合、Compliance イベントが発生したときに、`AWS-RunPatchBaseline` ドキュメントまたは `AWS-RefreshAssociation` ドキュメントを実行するよう EventBridge を設定できます。

以下の手順を使用して、設定コンプライアンスを EventBridge イベントのターゲットとして設定します。

設定コンプライアンスを EventBridge イベントのターゲットとして設定する (コンソール)

1. Amazon EventBridge コンソール (https://console.aws.amazon.com/events/) を開きます。
2. ナビゲーションペインで ルール] を選択します。
3. [ルールの作成] を選択します。
4. ルールの名前と説明を入力します。

   ルールには、同じ AWS リージョン 内および同じイベントバス上の別のルールと同じ名前を付けることはできません。
5. [イベントバス] で、このルールに関連付けるイベントバスを選択します。このルールを使用して、自分の AWS アカウント の一致するイベントに応答する場合は、[default] (デフォルト) を選択します。アカウントの AWS のサービスで発生したイベントは、常にアカウントのデフォルトのイベントバスに移動します。
6. [ルールタイプ] で、[イベントパターンを持つルール] を選択してください。
7. [Next] を選択します。

8. [Event source] (イベントソース) で、[AWS events or EventBridge partner events] (イベントまたは EventBridge パートナーイベント) を選択してください。
9. [Event pattern] (イベントパターン) セクションで [Event pattern form] (イベントパターンフォーム) を選択します。
10. [イベントソース] で、[AWS のサービス] を選択してください。
11. [AWS のサービス] で、[Systems Manager] を選択します。
12. [イベントタイプ] で、[設定コンプライアンス] を選択します。
13. [特定の詳細タイプ] で [設定コンプライアンスのステータスの変更] を選択します。
14. [Next] を選択します。
15. [ターゲットタイプ] で、[AWS のサービス] を選択します。
16. [Select a target] (ターゲットを選択) で [Systems ManagerRun Command] を選択します。
17. [ドキュメント] リストで、ターゲットが呼び出されたときに実行する Systems Manager ドキュメント (SSM ドキュメント) を選択します。例えば、非準拠のパッチイベントの場合は `AWS-RunPatchBaseline` を選択するか、非準拠の関連付けイベントの場合は `AWS-RefreshAssociation` を選択します。
18. 残りのフィールドとパラメータの情報を指定します。

> **Note**
>
> 必須フィールドとパラメータには、名前の横にアスタリスク (*) が付いています。ターゲットを作成するには、各必須パラメータまたはフィールドの値を指定する必要があります。指定しないと、システムはルールを作成しますが、ルールは実行されません。

19. [Next] を選択します。
20. (オプション) ルールに 1 つ以上のタグを入力します。詳細については、Amazon EventBridge ユーザーガイドの「Amazon EventBridge リソースのタグ付け」を参照してください 。
21. [Next] を選択します。
22. ルールの詳細を確認し、[Create rule] (ルールの作成) を選択します。

AWS CLI を使用してカスタムコンプライアンスメタデータを割り当てる

以下の手順では、AWS Systems Manager PutComplianceItems API オペレーションを呼び出すために AWS Command Line Interface (AWS CLI CLI) を使用して、リソースにカスタムコンプライアンスメタデータを割り当てるプロセスについて説明します。また、この API オペレーションを使用し

て、次のチュートリアルに示すように手動でパッチや関連付けコンプライアンスメタデータをマネージドノードに割り当てることもできます。カスタムコンプライアンスの詳細については、「カスタムコンプライアンスについて」を参照してください。

マネージドインスタンスにカスタムコンプライアンスメタデータを割り当てるには (AWS CLI)

1. まだ AWS Command Line Interface (AWS CLI) をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」を参照してください。

2. 以下のコマンドを実行して、マネージドノードにカスタムコンプライアンスメタデータを割り当てます。各*###############*をユーザー自身の情報に置き換えます。ResourceType パラメーターは、ManagedInstance の値のみをサポートします。マネージド AWS IoT Greengrass コアデバイスにカスタムコンプライアンスメタデータを割り当てる場合であっても、この値を指定します。

   Linux & macOS

   ```
   aws ssm put-compliance-items \
       --resource-id instance_ID \
       --resource-type ManagedInstance \
       --compliance-type Custom:user-defined_string \
       --execution-summary ExecutionTime=user-defined_time_and/or_date_value \
       --items Id=user-defined_ID,Title=user-
   defined_title,Severity=one_or_more_comma-separated_severities:CRITICAL, MAJOR,
    MINOR,INFORMATIONAL, or UNSPECIFIED,Status=COMPLIANT or NON_COMPLIANT
   ```

   Windows

   ```
   aws ssm put-compliance-items ^
       --resource-id instance_ID ^
       --resource-type ManagedInstance ^
       --compliance-type Custom:user-defined_string ^
       --execution-summary ExecutionTime=user-defined_time_and/or_date_value ^
       --items Id=user-defined_ID,Title=user-
   defined_title,Severity=one_or_more_comma-separated_severities:CRITICAL, MAJOR,
    MINOR,INFORMATIONAL, or UNSPECIFIED,Status=COMPLIANT or NON_COMPLIANT
   ```

3. 前のステップを繰り返して、追加のカスタムコンプライアンスメタデータを 1 つ以上のノードに割り当てます。次のコマンドを使用して、マネージドノードにパッチまたは関連付けコンプライアンスメタデータを手動で割り当てることもできます。

   関連付けコンプライアンスメタデータ

   Linux & macOS

   ```
   aws ssm put-compliance-items \
       --resource-id instance_ID \
       --resource-type ManagedInstance \
       --compliance-type Association \
       --execution-summary ExecutionTime=user-defined_time_and/or_date_value \
       --items Id=user-defined_ID,Title=user-
   defined_title,Severity=one_or_more_comma-separated_severities:CRITICAL, MAJOR,
    MINOR,INFORMATIONAL, or UNSPECIFIED,Status=COMPLIANT or NON_COMPLIANT
   ```

   Windows

   ```
   aws ssm put-compliance-items ^
       --resource-id instance_ID ^
       --resource-type ManagedInstance ^
       --compliance-type Association ^
       --execution-summary ExecutionTime=user-defined_time_and/or_date_value ^
       --items Id=user-defined_ID,Title=user-
   defined_title,Severity=one_or_more_comma-separated_severities:CRITICAL, MAJOR,
    MINOR,INFORMATIONAL, or UNSPECIFIED,Status=COMPLIANT or NON_COMPLIANT
   ```

   パッチコンプライアンスメタデータ

   Linux & macOS

   ```
   aws ssm put-compliance-items \
       --resource-id instance_ID \
       --resource-type ManagedInstance \
       --compliance-type Patch \
       --execution-summary ExecutionTime=user-defined_time_and/
   or_date_value,ExecutionId=user-defined_ID,ExecutionType=Command  \
       --items Id=for_example, KB12345,Title=user-
   defined_title,Severity=one_or_more_comma-separated_severities:CRITICAL,
    MAJOR, MINOR,INFORMATIONAL, or UNSPECIFIED,Status=COMPLIANT or
   ```

```
 NON_COMPLIANT,Details="{PatchGroup=name_of_group,PatchSeverity=the_patch_severity,
 for example, CRITICAL}"
```

Windows

```
aws ssm put-compliance-items ^
    --resource-id instance_ID ^
    --resource-type ManagedInstance ^
    --compliance-type Patch ^
    --execution-summary ExecutionTime=user-defined_time_and/
or_date_value,ExecutionId=user-defined_ID,ExecutionType=Command  ^
    --items Id=for_example, KB12345,Title=user-
defined_title,Severity=one_or_more_comma-separated_severities:CRITICAL,
 MAJOR, MINOR,INFORMATIONAL, or UNSPECIFIED,Status=COMPLIANT or
 NON_COMPLIANT,Details="{PatchGroup=name_of_group,PatchSeverity=the_patch_severity,
 for example, CRITICAL}"
```

4. 以下のコマンドを実行して、特定のマネージドノードのコンプライアンス項目を一覧表示します。フィルターを使用して、特定のコンプライアンスデータにドリルダウンします。

Linux & macOS

```
aws ssm list-compliance-items \
    --resource-ids instance_ID \
    --resource-types ManagedInstance \
    --filters one_or_more_filters
```

Windows

```
aws ssm list-compliance-items ^
    --resource-ids instance_ID ^
    --resource-types ManagedInstance ^
    --filters one_or_more_filters
```

次の例では、このコマンドをフィルタとともに使用する方法を示しています。

Linux & macOS

```
aws ssm list-compliance-items \
    --resource-ids i-02573cafcfEXAMPLE \
    --resource-type ManagedInstance \
```

```
    --filters Key=DocumentName,Values=AWS-RunPowerShellScript
 Key=Status,Values=NON_COMPLIANT,Type=NotEqual
 Key=Id,Values=cee20ae7-6388-488e-8be1-a88ccEXAMPLE
 Key=Severity,Values=UNSPECIFIED
```

Windows

```
aws ssm list-compliance-items ^
    --resource-ids i-02573cafcfEXAMPLE ^
    --resource-type ManagedInstance ^
    --filters Key=DocumentName,Values=AWS-RunPowerShellScript
 Key=Status,Values=NON_COMPLIANT,Type=NotEqual
 Key=Id,Values=cee20ae7-6388-488e-8be1-a88ccEXAMPLE
 Key=Severity,Values=UNSPECIFIED
```

Linux & macOS

```
aws ssm list-resource-compliance-summaries \
    --filters Key=OverallSeverity,Values=UNSPECIFIED
```

Windows

```
aws ssm list-resource-compliance-summaries ^
    --filters Key=OverallSeverity,Values=UNSPECIFIED
```

Linux & macOS

```
aws ssm list-resource-compliance-summaries \
    --filters Key=OverallSeverity,Values=UNSPECIFIED
 Key=ComplianceType,Values=Association Key=InstanceId,Values=i-02573cafcfEXAMPLE
```

Windows

```
aws ssm list-resource-compliance-summaries ^
    --filters Key=OverallSeverity,Values=UNSPECIFIED
 Key=ComplianceType,Values=Association Key=InstanceId,Values=i-02573cafcfEXAMPLE
```

5. コンプライアンスステータスの概要を表示するには、次のコマンドを実行します。フィルターを使用して、特定のコンプライアンスデータにドリルダウンします。

```
aws ssm list-resource-compliance-summaries --filters One or more filters.
```

次の例では、このコマンドをフィルタとともに使用する方法を示しています。

Linux & macOS

```
aws ssm list-resource-compliance-summaries \
    --filters Key=ExecutionType,Values=Command
```

Windows

```
aws ssm list-resource-compliance-summaries ^
    --filters Key=ExecutionType,Values=Command
```

Linux & macOS

```
aws ssm list-resource-compliance-summaries \
    --filters Key=AWS:InstanceInformation.PlatformType,Values=Windows
 Key=OverallSeverity,Values=CRITICAL
```

Windows

```
aws ssm list-resource-compliance-summaries ^
    --filters Key=AWS:InstanceInformation.PlatformType,Values=Windows
 Key=OverallSeverity,Values=CRITICAL
```

6. コンプライアンスタイプの準拠しているリソースと準拠していないリソースのカウントの概要を表示するには、次のコマンドを実行します。フィルターを使用して、特定のコンプライアンスデータにドリルダウンします。

```
aws ssm list-compliance-summaries --filters One or more filters.
```

次の例では、このコマンドをフィルタとともに使用する方法を示しています。

Linux & macOS

```
aws ssm list-compliance-summaries \
```

```
    --filters Key=AWS:InstanceInformation.PlatformType,Values=Windows
 Key=PatchGroup,Values=TestGroup
```

Windows

```
aws ssm list-compliance-summaries ^
    --filters Key=AWS:InstanceInformation.PlatformType,Values=Windows
 Key=PatchGroup,Values=TestGroup
```

Linux & macOS

```
aws ssm list-compliance-summaries \
    --filters Key=AWS:InstanceInformation.PlatformType,Values=Windows
 Key=ExecutionId,Values=4adf0526-6aed-4694-97a5-14522EXAMPLE
```

Windows

```
aws ssm list-compliance-summaries ^
    --filters Key=AWS:InstanceInformation.PlatformType,Values=Windows
 Key=ExecutionId,Values=4adf0526-6aed-4694-97a5-14522EXAMPLE
```

AWS Systems Manager Distributor

AWS Systems Manager のツールである Distributor は、ソフトウェアをパッケージ化して AWS Systems Managerマネージドノードに公開するのに役立ちます。独自のソフトウェアをパッケージ化して公開したり、Distributor を使用して AmazonCloudWatchAgent などの AWS から提供されるエージェントソフトウェアパッケージ、または Trend Micro などのサードパーティーパッケージを検索して公開することができます。パッケージを公開することで、ノード ID、AWS アカウント ID、タグ、または AWS リージョン を使用して特定したマネージドノードに、パッケージのドキュメントの特定のバージョンがアドバタイズされます。Distributor の使用を開始するには、Systems Manager コンソールを開きます。ナビゲーションペインで、[Distributor] を選択します。

Distributor でパッケージを作成した後、次のいずれかの方法でパッケージをインストールできます。

- AWS Systems Manager Run Command を使用して単発でインストールする方法。
- AWS Systems Manager State Manager を使用してスケジュールに従ってインストールする方法。

> **Important**
>
> サードパーティの販売者が配布するパッケージは、AWS が管理せず、パッケージのベンダーが公開します。デューディリジェンスを追加で実施して、社内のセキュリティ管理に対するコンプライアンスを確保することをお勧めします。セキュリティは、AWS とお客様の間の共有責任です。これは、責任共有モデルと説明されます。詳細については、責任共有モデルを参照してください。

Distributor はどのように組織にとってメリットになりますか?

Distributor は、以下の利点を提供します。

- 1 つのパッケージで、多くのプラットフォーム

  Distributor でパッケージを作成すると、システムに AWS Systems Manager ドキュメント (SSM ドキュメント) が作成されます。このドキュメントには .zip ファイルをアタッチできます。Distributor を実行すると、システムは SSM ドキュメントにある指示を処理し、指定されたターゲットに .zip ファイルのソフトウェアパッケージをインストールします。Distributor では、Windows、Ubuntu Server、Debian Server、および Red Hat Enterprise Linux を含む複数のオペレーティングシステムがサポートされています。サポートされるプラットフォームの詳細については、「サポートされているパッケージのプラットフォームとアーキテクチャ」を参照してください。

- マネージドインスタンスのグループ間でのパッケージアクセスの制御

  Run Command または State Manager を使用して、パッケージを取得するマネージドノードと、そのパッケージのどのバージョンを取得するかを制御できます。Run Command と State Manager は AWS Systems Manager のツールです。マネージドノードは、インスタンスまたはデバイス ID、AWS アカウント 番号、タグ、または AWS リージョン ごとにグループ化できます。State Manager 関連付けを使用して、さまざまなインスタンスのグループに異なるバージョンのパッケージを配信できます。

- 多くの AWS エージェントパッケージが含まれており、使用する準備ができている

  Distributor には、マネージドノードにすぐにデプロイできる AWS エージェントパッケージが多数含まれています。`Amazon` によって公開された Distributor `Packages` リストページにあるパッケージを探します。例には、`AmazonCloudWatchAgent` や `AWSPVDriver` が含まれます。

- デプロイの自動化

環境を最新の状態に保つには、State Manager を使用して、これらのマシンが最初に起動されたときに、ターゲットとなるマネージドノードに自動デプロイするパッケージをスケジュールします。

Distributor はどのようなユーザーに適していますか?

- 一度に複数の Systems Manager マネージドノードに対して、AWS で公開されたパッケージを含む既存のソフトウェアパッケージを新規作成またはデプロイしたい AWS のお客様。
- ソフトウェアパッケージを作成するソフトウェア開発者。
- Systems Manager のマネージドノードを最新のソフトウェアパッケージで最新の状態に保つ責任がある管理者。

Distributor の特徴は何ですか?

- Windows インスタンスと Linux インスタンスの両方へのパッケージのデプロイ

  Distributor を使用すると、Linux および Windows Server 用の Amazon Elastic Compute Cloud (Amazon EC2) インスタンスおよび AWS IoT Greengrass コアデバイスにソフトウェアパッケージをデプロイできます。サポートされているインスタンスオペレーティングシステムのリストについては、「the section called “サポートされているパッケージのプラットフォームとアーキテクチャ”」を参照してください。

  > **Note**
  >
  > Distributor は、macOS オペレーティングシステムでサポートされていません。

- パッケージを 1 回または自動化されたスケジュールでデプロイする

  パッケージを一度、定期的なスケジュールで、またはデフォルトのパッケージバージョンが別のバージョンに変更されるたびにデプロイするよう選択できます。

- パッケージを完全に再インストールするか、インプレース更新を実行する

  新しいパッケージバージョンをインストールするには、提供するアップデートスクリプトに従って、現在のバージョンを完全にアンインストールして新しいバージョンをインストールするか、新しいコンポーネントと更新されたコンポーネントで現在のバージョンを更新するだけです。再インストール中はパッケージアプリケーションを使用できなくなりますが、インプレース更新中は引き

続き使用できます。インプレース更新は、セキュリティモニタリングアプリケーションや、アプリケーションのダウンタイムを回避する必要があるその他のシナリオで特に役立ちます。

- コンソール、CLI、PowerShell、および SDK の Distributor 機能へのアクセス

  Distributor は、Systems Manager コンソール、任意の AWS Command Line Interface (AWS CLI)、AWS Tools for PowerShell、または AWS SDK で使用できます。

- IAM アクセスコントロール

  AWS Identity and Access Management (IAM) ポリシーを使用すると、組織のどのメンバーがパッケージまたはパッケージのバージョンを作成、更新、デプロイ、削除できるかを制御できます。たとえば、管理者にパッケージをデプロイする権限を与えますが、パッケージを変更したり、新しいパッケージのバージョンを作成する権限は与えないということができます。

- ログ記録および監査機能のサポート

  他の AWS のサービスとの統合を使用して、AWS アカウント の Distributor ユーザーアクションの監査およびログ記録を行うことができます。詳細については、「Distributor アクティビティの監査とログ記録」を参照してください。

Distributor でのパッケージとは何ですか?

パッケージとは、インストール可能なソフトウェアやアセットのコレクションで、以下のものが含まれます。

- ターゲットオペレーティングシステムプラットフォームごとのソフトウェアの .zip ファイル。各 .zip ファイルには以下が含まれている必要があります。
  - install および uninstall スクリプト。PowerShell スクリプトを必要とする Windows Server ベースのマネージドノード (`install.ps1` および `uninstall.ps1` というスクリプト)。Linux ベースのマネージドノードの場合、シェルスクリプト (`install.sh` および `uninstall.sh` という名前のスクリプト) が必要です。AWS Systems Manager SSM Agent は、install および uninstall スクリプトで指示を読み取り、実行します。
  - 実行可能ファイル。SSM Agent が、ターゲットとなるマネージドノードにパッケージをインストールするには、この実行可能ファイルを見つける必要があります。
- パッケージのコンテンツについて説明する JSON 形式のマニフェストファイル。マニフェストは、.zip ファイルに含まれていませんが、パッケージを形成する .zip ファイルと同じ Amazon Simple Storage Service (Amazon S3) バケットに格納されています。マニフェストはパッケージのバージョンを識別し、パッケージ内の .zip ファイルをオペレーティングシステムのバージョンやアーキテクチャなどのターゲットとなるマネージドノードの属性にマップします。マニフェストを

作成する方法については、「ステップ 2: JSON パッケージマニフェストを作成する」を参照してください。

Distributor コンソールで [Simple] パッケージの作成を選択すると、Distributor は、ソフトウェア実行可能ファイルの名前と、ターゲットプラットフォームおよびアーキテクチャに基づき、インストールおよびアンインストールスクリプト、ファイルのハッシュ、JSON パッケージマニフェストを生成します。

サポートされているパッケージのプラットフォームとアーキテクチャ

Distributorを使用して、次の Systems Manager マネージドノードプラットフォームにパッケージを公開できます。バージョン値は、対象とするオペレーティングシステム Amazon Machine Image (AMI) の正確なリリースバージョンと一致する必要があります。このバージョンの確認について詳しくは、「ステップ 2: JSON パッケージマニフェストを作成する」のステップ 4 を参照してください。

> **Note**
>
> Systems Manager は、次の AWS IoT Greengrass コアデバイス向けのオペレーティングシステムをすべてサポートしているわけではありません。詳細については、AWS IoT Greengrass Version 2 デベロッパーガイドの「AWS IoT Greengrass コアデバイスの設定」を参照してください。

プラットフォーム	マニフェストファイルのコード値	対応アーキテクチャ
AlmaLinux	`almalinux`	x86_64 ARM64
Amazon Linux 1、Amazon Linux 2、Amazon Linux 2023	`amazon`	x86_64、または x86 ARM64 (Amazon Linux 2 および AL2023、A1 インスタンスタイプ)
CentOS	`centos`	x86_64 、、または x86

プラットフォーム	マニフェストファイルのコード値	対応アーキテクチャ
Debian Server	`debian`	x86_64 、、または x86
openSUSE	`opensuse`	x86_64 または x86
openSUSE Leap	`opensuseleap`	x86_64 、、または x86
Oracle Linux	`oracle`	x86_64
Red Hat Enterprise Linux (RHEL)	`redhat`	x86_64 、、または x86 ARM64 (RHEL 7.6 以降、A1 インスタンスタイプ)
Rocky Linux	`rocky`	x86_64 ARM64
SUSE Linux Enterprise Server (SLES)	`suse`	x86_64 、、または x86
Ubuntu Server	`ubuntu`	x86_64 、、または x86 ARM64 (Ubuntu Server 16 以降では、A1 インスタンスタイプ)
Windows Server	`windows`	x86_64、または x86

トピック

- Distributor を設定する
- Distributor パッケージを操作する
- Distributor アクティビティの監査とログ記録
- AWS Systems ManagerDistributor のトラブルシューティング

Distributor を設定する

AWS Systems Manager のツールである Distributor を使用してソフトウェアパッケージを作成、管理、デプロイする前に、次の手順を実行します。

Distributor 前提条件を満たす

AWS Systems Manager のツールである Distributor を使用する前に、環境が以下の要件を満たしていることを確認します。

Distributor の前提条件

要件	説明
SSM Agent	デプロイするマネージドノードまたはパッケージを削除するマネージドノードに、AWS Systems Manager SSM Agent バージョン 2.3.274.0 以降をインストールする必要があります。 SSM Agent をインストールまたは更新するには、「「SSM Agent」 の使用」を参照してください。
AWS CLI	(オプション) Systems Manager コンソールの代わりに AWS Command Line Interface (AWS CLI) を使用してパッケージを作成および管理するには、ローカルコンピュータに AWS CLI の最新リリースをインストールします。 CLI のインストールまたはアップグレード方法の詳細については、AWS Command Line Interface ユーザーガイドの「AWS Command Line Interface のインストール」を参照してください。
AWS Tools for PowerShell	(オプション) Systems Manager コンソールの代わりに Tools for PowerShell を使用してパッケージを作成および管理するには、ローカル

要件	説明
	コンピュータに Tools for PowerShell の最新リリースをインストールします。 Tools for PowerShell をインストールまたはアップグレードする方法の詳細については、AWS Tools for Windows PowerShell ユーザーガイドの「AWS Tools for Windows PowerShell または AWS Tools for PowerShell Core のインストール」を参照してください。

> **Note**
>
> Systems Manager では、Distributor を使用した Oracle Linux マネージドノードへのパッケージの配布は現在サポートされていません。

Distributor のアクセス許可を持つ IAM インスタンスプロファイルを確認または作成する

デフォルトでは、AWS Systems Manager にはインスタンスでアクションを実行する権限がありません。AWS Identity and Access Management (IAM) インスタンスプロファイルを使用してアクセスを許可する必要があります。インスタンスプロファイルは、起動時に IAM ロール情報を Amazon Elastic Compute Cloud (Amazon EC2) インスタンスに渡すコンテナです。この要件は、Distributor だけでなく、すべての Systems Manager ツールのアクセス許可に適用されます。

> **Note**
>
> エッジデバイスが AWS IoT Greengrass Core ソフトウェアおよび SSM Agent で実行されるように構成する場合、Systems Manager によるアクションを実行可能にする IAM サービスロールを指定します。マネージドエッジデバイスをインスタンスプロファイルで設定する必要はありません。

Run Command や State Manager など他の Systems Manager ツールを既に使用している場合は、Distributor に必要な権限を持つインスタンスプロファイルがすでにインスタンスにアタッチされています。Distributor タスクを実行するためのアクセス許可を持つための最も簡単な方法は、AmazonSSMManagedInstanceCore ポリシーをお客様のインスタンスプロファイルにアタッチ

することです。詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」を参照してください。

パッケージへのユーザーアクセスを制御する

AWS Identity and Access Management (IAM) ポリシーを使用することで、パッケージの作成、デプロイ、および管理ができます。また、マネージドノードで実行できる Run Command と State Manager API オペレーションを管理することもできます。Distributor と同様、Run Command と State Manager はどちらも AWS Systems Manager のツールです。

ARN 形式

ユーザー定義パッケージは、ドキュメント Amazon リソースネーム (ARN) に関連付けられ、形式は以下のとおりです。

```
arn:aws:ssm:region:account-id:document/document-name
```

以下に例を示します。

```
arn:aws:ssm:us-west-1:123456789012:document/ExampleDocumentName
```

エンドユーザー用と管理者用の 2 つの AWS 提供のデフォルト IAM ポリシーを使用して、Distributor アクティビティのアクセス権限を付与することができます。または、アクセス許可の要件に適したカスタム IAM ポリシーを作成することもできます。

IAM ポリシーで変数を使用する方法の詳細については、「IAM ポリシーエレメント: 変数」を参照してください。

ポリシーの作成方法、およびポリシーをユーザーまたはグループにアタッチする方法については、「IAM ユーザーガイド」の「IAM ポリシーの作成」および「IAM ポリシーの追加と削除」を参照してください。

Distributor パッケージを保存する Amazon S3 バケットを作成または選択する

AWS Systems Manager コンソールで [Simple] ワークフローを使用してパッケージを作成する場合、Distributor がソフトウェアをアップロードする既存の Amazon Simple Storage Service (Amazon S3) バケットを選択します。Distributor は AWS Systems Manager のツールです。[Advanced (アドバンスト)] ワークフローでは、開始する前に、ソフトウェアまたはアセットの .zip ファイルを Amazon S3 バケットにアップロードする必要があります。コンソールで [Simple] または [Advanced]

ワークフローを使用してパッケージを作成するか、API を使用してパッケージを作成するかにかかわらず、パッケージの作成を開始する前に Amazon S3 バケットが必要です。パッケージ作成プロセスの一環として、Distributor は、インストール可能なソフトウェアとアセットをこのバケットから内部の Systems Manager ストアにコピーします。アセットは内部ストアにコピーされるため、パッケージの作成が終了したら、Amazon S3 バケットを削除または再利用できます。

バケットの作成方法の詳細については、Amazon Simple Storage Service 入門ガイドの「バケットの作成」を参照してください。AWS CLI コマンドを実行してバケットを作成する方法の詳細については、AWS CLI コマンドリファレンスの「mb」を参照してください。

Distributor パッケージを操作する

AWS Systems Manager コンソール、AWS コマンドラインツール (AWS CLI と AWS Tools for PowerShell)、AWS SDK を使用して、Distributor でパッケージを追加、管理、またはデプロイできます。Distributor は AWS Systems Manager のツールです。パッケージを Distributor に追加する前に。

- インストール可能なアセットを作成し、圧縮します。
- (オプション) パッケージの JSON マニフェストファイルを作成します。Distributor コンソールで [Simple] パッケージ作成プロセスを使用する場合は必要ありません。Simple パッケージ作成では、JSON マニフェストファイルが生成されます。

  AWS Systems Manager コンソール、テキストまたは JSON エディタを使用してマニフェストファイルを作成します。
- インストール可能なアセットやソフトウェアを保存できるように、Amazon Simple Storage Service (Amazon S3) バケットを用意します。[Advanced] パッケージ作成プロセスを使用している場合は、開始する前にアセットを Amazon S3 バケットにアップロードします。

> **Note**
>
> パッケージ作成プロセスの一部として、パッケージの内容は Distributor から内部 Systems Manager バケットに移行されるため、パッケージの作成が完了したらこのバケットを削除または再利用できます。

AWS で公開されたパッケージは既にパッケージ化され、デプロイできる状態になっています。AWS で公開されたパッケージをマネージドノードにデプロイするには、「Distributor パッケージをインストールまたは更新する」を参照してください。

Distributor パッケージを AWS アカウント 間で共有できます。別のアカウントから共有されたパッケージを AWS CLI コマンドで使用する場合は、パッケージ名の代わりに Amazon リソースネーム (ARN) パッケージを使用します。

トピック

- Distributor でパッケージを表示する
- Distributor でパッケージを作成する
- コンソールで Distributor パッケージの許可を編集する
- コンソールで Distributor パッケージタグを編集する
- Distributor パッケージにバージョンを追加する
- Distributor パッケージをインストールまたは更新する
- Distributor パッケージをアンインストールする
- Distributor パッケージを削除する

Distributor でパッケージを表示する

インストール可能なパッケージを表示するには、AWS Systems Manager コンソールまたは任意の AWS コマンドラインツールを使用します。Distributor は AWS Systems Manager のツールです。Distributor にアクセスするには、AWS Systems Manager コンソールを開き、左側のナビゲーションペインで [Distributor] を選択します。利用可能なパッケージがすべて表示されます。

次のセクションでは、任意のコマンドラインツールを使用して Distributor パッケージを表示する方法について説明します。

コマンドラインを使用してパッケージを表示する

このセクションでは、任意のコマンドラインツールを使用して、提供されたコマンドを使用して Distributor パッケージを表示する方法について説明します。

Linux & macOS

Linux で AWS CLI を使用してパッケージを表示するには

- 共有パッケージを除くすべてのパッケージを表示するには、次のコマンドを実行します。

```
aws ssm list-documents \
    --filters Key=DocumentType,Values=Package
```

- Amazon が所有するすべてのパッケージを表示するには、次のコマンドを実行します。

```
aws ssm list-documents \
    --filters Key=DocumentType,Values=Package Key=Owner,Values=Amazon
```

- サードパーティーが所有するすべてのパッケージを表示するには、次のコマンドを実行します。

```
aws ssm list-documents \
    --filters Key=DocumentType,Values=Package Key=Owner,Values=ThirdParty
```

Windows

Windows で AWS CLI を使用してパッケージを表示するには

- 共有パッケージを除くすべてのパッケージを表示するには、次のコマンドを実行します。

```
aws ssm list-documents ^
    --filters Key=DocumentType,Values=Package
```

- Amazon が所有するすべてのパッケージを表示するには、次のコマンドを実行します。

```
aws ssm list-documents ^
    --filters Key=DocumentType,Values=Package Key=Owner,Values=Amazon
```

- サードパーティーが所有するすべてのパッケージを表示するには、次のコマンドを実行します。

```
aws ssm list-documents ^
    --filters Key=DocumentType,Values=Package Key=Owner,Values=ThirdParty
```

PowerShell

Tools for PowerShell を使用してパッケージを表示するには

- 共有パッケージを除くすべてのパッケージを表示するには、次のコマンドを実行します。

```
$filter = New-Object Amazon.SimpleSystemsManagement.Model.DocumentKeyValuesFilter
$filter.Key = "DocumentType"
$filter.Values = "Package"
```

```
Get-SSMDocumentList `
    -Filters @($filter)
```

- Amazon が所有するすべてのパッケージを表示するには、次のコマンドを実行します。

```
$typeFilter = New-Object
 Amazon.SimpleSystemsManagement.Model.DocumentKeyValuesFilter
$typeFilter.Key = "DocumentType"
$typeFilter.Values = "Package"

$ownerFilter = New-Object
 Amazon.SimpleSystemsManagement.Model.DocumentKeyValuesFilter
$ownerFilter.Key = "Owner"
$ownerFilter.Values = "Amazon"

Get-SSMDocumentList `
    -Filters @($typeFilter,$ownerFilter)
```

- サードパーティーが所有するすべてのパッケージを表示するには、次のコマンドを実行します。

```
$typeFilter = New-Object
 Amazon.SimpleSystemsManagement.Model.DocumentKeyValuesFilter
$typeFilter.Key = "DocumentType"
$typeFilter.Values = "Package"

$ownerFilter = New-Object
 Amazon.SimpleSystemsManagement.Model.DocumentKeyValuesFilter
$ownerFilter.Key = "Owner"
$ownerFilter.Values = "ThirdParty"

Get-SSMDocumentList `
    -Filters @($typeFilter,$ownerFilter)
```

Distributor でパッケージを作成する

パッケージを作成するには、インストール可能なソフトウェアまたはアセットを、オペレーティングシステムプラットフォームごとに 1 ファイルずつ準備します。パッケージを作成するには、少なくとも 1 つのファイルが必要です。

異なるプラットフォームで、同じファイルを使用することはありますが、パッケージにアタッチするすべてのファイルは、マニフェストの `Files` セクションにリストされている必要があります。コン

ソールで simple ワークフローを使用してパッケージを作成している場合は、マニフェストが自動的に生成されます。1 つのドキュメントにアタッチできるファイル数は最大 20 です。各ファイルの最大サイズは 1 GB です。サポートされるプラットフォームの詳細については、「サポートされているパッケージのプラットフォームとアーキテクチャ」を参照してください。

パッケージを作成すると、システムは新しい SSM ドキュメントを作成します。このドキュメントでは、マネージドノードにパッケージをデプロイすることができます。

デモ専用のサンプルパッケージ ExamplePackage.zip をウェブサイトからダウンロードできます。サンプルパッケージには、完成した JSON マニフェストと、PowerShell v7.0.0 のインストーラを含む 3 つの .zip ファイルが含まれています。インストールおよびアンインストールスクリプトには有効なコマンドが含まれていません。[Advanced (アドバンスト)] ワークフローでパッケージを作成するには、インストール可能な各ソフトウェアとスクリプトを .zip ファイルに圧縮する必要がありますが、[Simple (簡易)] ワークフローではインストール可能なアセットを圧縮しないでください。

トピック

- シンプルワークフローを使用してパッケージを作成する
- 高度なワークフローを使用してパッケージを作成する

シンプルワークフローを使用してパッケージを作成する

このセクションでは、Distributor コンソールで [Simple] パッケージ作成ワークフローを選択して、Distributor でパッケージを作成する方法について説明します。Distributor は AWS Systems Manager のツールです。パッケージを作成するには、オペレーティングシステムプラットフォームごとに、インストール可能なアセットを準備します。パッケージを作成するには、少なくとも 1 つのファイルが必要です。[Simple] パッケージ作成プロセスでは、インストールスクリプトおよびアンインストールスクリプト、ファイルのハッシュ、JSON 形式のマニフェストを生成します。[Simple (簡易)] ワークフローでは、インストール可能なファイルをアップロードおよび圧縮し、新しいパッケージと、関連する [SSM ドキュメント] を作成するプロセスを処理します。サポートされるプラットフォームの詳細については、「サポートされているパッケージのプラットフォームとアーキテクチャ」を参照してください。

Simple メソッドを使用してパッケージを作成すると、Distributor によって `install` および `uninstall` スクリプトが作成されます。ただし、インプレース更新用のパッケージを作成する場合は、[Update script (スクリプトの更新)] タブで独自の `update` スクリプトのコンテンツを指定する必要があります。`update` スクリプトに入力コマンドを追加すると、Distributor はこのスクリプトが作成する .zip パッケージに、`install` および `uninstall` をこのスクリプトとともに含めます。

> **Note**
>
> In-place 更新オプションの使用で、関連付けられたアプリケーションをオフラインにすることなく、既存のパッケージインストールに新しいファイルまたは更新されたファイルを追加できます。

シンプルワークフローを使用してパッケージを作成するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Distributor] を選択します。
3. Distributor ホームページで [Create package (パッケージの作成)]、[Simple] の順に選択します。
4. [Create package (パッケージの作成)] ページに、パッケージの名前を入力します。パッケージ名には、文字、数字、ピリオド、ダッシュ、アンダースコアを含めることができます。この名前は、パッケージの添付ファイルのすべてのバージョンに適用できるほど一般的である必要がありますが、パッケージの目的を識別できるよう具体的な名前である必要があります。
5. （オプション）[バージョン名] にバージョン名を入力します。バージョン名は最大 512 文字で、特殊文字を含めることはできません。
6. [Location (ロケーション)] で、バケット名とプレフィックス、またはバケット URL を使用してバケットを選択します。
7. [Upload software] (ソフトウェアのアップロード) で、[Add software] (ソフトウェアの追加) を選択し、`.rpm`、`.msi`、または `.deb` 拡張子が付いたインストール可能なソフトウェアファイルにナビゲートします。ファイル名にスペースが含まれていると、アップロードは失敗します。1 回のアクションで複数のソフトウェアファイルをアップロードできます。
8. [Target platform (ターゲットプラットフォーム)] で、インストール可能な各ファイルに表示されるターゲットオペレーティングシステムプラットフォームが正しいことを確認します。表示されているオペレーティングシステムが正しくない場合は、ドロップダウンリストから正しいオペレーティングシステムを選択します。

   [Simple] パッケージ作成ワークフローでは、各インストール可能ファイルを 1 回だけアップロードするため、Distributor に複数のオペレーティングシステムの単一ファイルをターゲットにするよう指示するための追加のステップが必要です。たとえば、`Logtool_v1.1.1.rpm` という名前のインストール可能なソフトウェアファイルをアップロードする場合、Amazon Linux と Ubuntu オペレーティングシステムの両方で同じソフトウェアがターゲットになるため、

[Simple] ワークフローのデフォルト設定をいくつか変更する必要があります。複数のプラットフォームをターゲットにする場合は、次のいずれかの操作を行います。

- 代わりに [Advanced (アドバンスト)] ワークフローを使用して、開始前に、インストール可能な各ファイルを .zip ファイルに圧縮後、マニフェストを手動で作成して、1 つのインストール可能なファイルが複数のオペレーティングシステムプラットフォーム、またはバージョンでターゲットになるようにします。詳細については、「高度なワークフローを使用してパッケージを作成する」を参照してください。
- .zip ファイルが複数のオペレーティングシステムプラットフォーム、またはバージョンでターゲットになるように、[Simple] ワークフローでマニフェストファイルを手動で編集します。これを行う方法については、ステップ 2: JSON パッケージマニフェストを作成する のステップ 4 の最後を参照してください。

9. [プラットフォームのバージョン] で、表示されているオペレーティングシステムのプラットフォームのバージョンが **_any**、後にワイルドカード (7.*) が続くメジャーリリースバージョン、またはソフトウェアを適用する特定のオペレーティングシステムのリリースバージョンに一致していることを確認します。オペレーティングシステムのプラットフォームのバージョンの指定の詳細については、ステップ 2: JSON パッケージマニフェストを作成する のステップ 4 を参照してください。
10. [Architecture] のドロップダウンリストから、インストール可能なファイルごとに正しいプロセッサアーキテクチャを選択します。サポートされるプロセッサアーキテクチャの詳細については、「サポートされているパッケージのプラットフォームとアーキテクチャ」を参照してください。
11. （オプション）[Scripts (スクリプト)] を展開し、インストール可能なソフトウェア用に Distributor によって生成されるスクリプトを確認します。
12. （オプション）インプレース更新で使用する更新スクリプトを提供するには、[Scripts (スクリプト)] を展開し、[Update script (スクリプトの更新)] タブを選択して、更新スクリプトコマンドを入力します。

    Systems Manager は、ユーザーに代わって更新スクリプトを生成しません。
13. インストール可能なソフトウェアファイルを追加するには、[Add software (ソフトウェアの追加)] を選択します。それ以外の場合は、次のステップに進みます。
14. (オプション) [Manifest (マニフェスト)] を展開し、インストール可能なソフトウェアに対して Distributor が生成する JSON パッケージのマニフェストを確認します。プラットフォームのバージョンやターゲットのプラットフォームなど、この手順を開始してからソフトウェアに関する情報を変更した場合は、[Generate manifest (マニフェストの生成)] を選択して、更新されたパッケージマニフェストを表示します。

ステップ 8 で説明されているように、複数のオペレーティングシステムでインストール可能なソフトウェアをターゲットにする場合は、マニフェストを手動で編集できます。マニフェストの編集の詳細については、「ステップ 2: JSON パッケージマニフェストを作成する」を参照してください。

15. [Create package (パッケージの作成)] を選択します。

Distributor でソフトウェアがアップロードされ、パッケージが作成されるまで待ちます。 Distributor は、インストール可能なファイルごとにアップロードステータスを示します。追加するパッケージの数とサイズによっては、数分かかる場合があります。Distributor では、新しいパッケージの [Package details] ページに自動的にリダイレクトされますが、ソフトウェアのアップロード後にこのページを自分で開くことも選択できます。Distributor でパッケージの作成プロセスが完了するまで、[パッケージの詳細] ページにはパッケージに関する情報は表示されません。アップロードプロセスとパッケージ作成プロセスを停止するには、[Cancel] を選択します。

Distributor でソフトウェアのインストール可能なファイルをアップロードできない場合は、[Upload failed (アップロードに失敗しました)] メッセージが表示されます。アップロードを再試行するには、[Retry upload (アップロードの再試行)] を選択します。パッケージ作成エラーをトラブルシューティングする方法の詳細については、「AWS Systems ManagerDistributor のトラブルシューティング」を参照してください。

高度なワークフローを使用してパッケージを作成する

このセクションでは、インストールスクリプトおよびアンインストールスクリプトで圧縮されたインストール可能なアセットと JSON マニフェストファイルを Amazon S3 バケットにアップロードした後に、高度なユーザーが Distributor でパッケージを作成する方法について説明します。

パッケージを作成するには、オペレーティングシステムプラットフォームごとに 1 つの .zip ファイルで、インストール可能なアセットの .zip ファイルを準備します。パッケージを作成するには、少なくとも 1 つの .zip ファイルが必要です。次に、JSON マニフェストを作成します。マニフェストには、パッケージコードファイルへのポインタが含まれています。必要なコードファイルをフォルダかディレクトリに追加し、マニフェストに正しい値が入力されたら、パッケージを S3 バケットにアップロードします。

サンプルパッケージ、ExamplePackage.zip は、当社のウェブサイトからダウンロードすることができます。サンプルパッケージには、完了した JSON マニフェストと 3 つの .zip ファイルが含まれています。

トピック

- ステップ 1: ZIP ファイルを作成する
- ステップ 2: JSON パッケージマニフェストを作成する
- ステップ 3: Amazon S3 バケットにパッケージとマニフェストをアップロードする
- ステップ 4: パッケージを Distributor に追加する

ステップ 1: ZIP ファイルを作成する

パッケージの基盤は、少なくとも 1 つのソフトウェアの .zip ファイル、またはインストール可能なアセットです。パッケージには、複数のオペレーティングシステムに 1 つの .zip ファイルをインストールできない限り、サポートするオペレーティングシステムごとに 1 つの .zip ファイルが含まれています。例えば、Red Hat Enterprise Linux インスタンスと Amazon Linux インスタンスは、通常同じ .RPM 実行可能ファイルを実行できるため、両方のオペレーティングシステムをサポートするために、パッケージには .zip ファイルを 1 つだけアタッチする必要があります。

必要なファイル

各 .zip ファイルには次の項目が必要です。

- install および uninstall スクリプト。PowerShell スクリプトを必要とする Windows Server ベースのマネージドノード (`install.ps1` および `uninstall.ps1` というスクリプト)。Linux ベースのマネージドノードの場合、シェルスクリプト (`install.sh` および `uninstall.sh` という名前のスクリプト) が必要です。SSM Agent は、install スクリプトと uninstall スクリプトの指示を実行します。

  たとえば、インストールスクリプトは、インストーラ (.rpm や .msi など) を実行したり、ファイルをコピーしたり、設定を構成することがあります。
- 実行可能ファイル、インストーラパッケージ (.rpm、.deb、.msi など)、その他のスクリプト、または設定ファイルなど。

オプションファイル

次の項目は、各 .zip ファイルではオプションです。

- update スクリプト。更新スクリプトを提供することで、`In-place update` オプションを使用してパッケージをインストールすることができます。既存のパッケージインストールに新しいファイルまたは更新されたファイルを追加する場合、`In-place update` オプションでは、更新の実行中にパッケージアプリケーションをオフラインにしません。Windows Server ベースのマネージ

ドノードには PowerShell スクリプト (update.ps1 というスクリプト) が必要です。Linux ベースのマネージドノードには、シェルスクリプト(update.sh という名前のスクリプト)が必要です。SSM Agent は、update スクリプト内の指示を実行します。

パッケージのインストールまたは更新の詳細については、「Distributor パッケージをインストールまたは更新する」を参照してください。

サンプル install と uninstall スクリプトを含む .zip ファイルの例については、サンプルパッケージ、ExamplePackage.zip をダウンロードしてください。

ステップ 2: JSON パッケージマニフェストを作成する

インストール可能なファイルを準備して圧縮したら、JSON マニフェストを作成します。以下はテンプレートです。マニフェストテンプレートの各部分は、このセクションの手順で説明されています。JSON エディタを使用して個別のファイルにこのマニフェストを作成します。または、パッケージの作成時に AWS Systems Manager コンソールでマニフェストを作成できます。

```
{
  "schemaVersion": "2.0",
  "version": "your-version",
  "publisher": "optional-publisher-name",
  "packages": {
    "platform": {
      "platform-version": {
        "architecture": {
          "file": ".zip-file-name-1.zip"
        }
      }
    },
    "another-platform": {
      "platform-version": {
        "architecture": {
          "file": ".zip-file-name-2.zip"
        }
      }
    },
    "another-platform": {
      "platform-version": {
        "architecture": {
          "file": ".zip-file-name-3.zip"
        }
      }
```

```
    }
  },
  "files": {
    ".zip-file-name-1.zip": {
      "checksums": {
        "sha256": "checksum"
      }
    },
    ".zip-file-name-2.zip": {
      "checksums": {
        "sha256": "checksum"
      }
    }
  }
}
```

JSON パッケージマニフェストを作成するには

1. スキーマバージョンをマニフェストに追加します。このリリースでは、スキーマバージョンは常に 2.0 です。

   ```
   { "schemaVersion": "2.0",
   ```

2. ユーザー定義のパッケージのバージョンをマニフェストに追加します。これは、パッケージを Distributor に追加するときに指定する [Version name (バージョン名)] の値でもあります。これは、パッケージを追加するときに Distributor が作成する AWS Systems Manager ドキュメントの一部になります。また、この値を AWS-ConfigureAWSPackage ドキュメントの入力として提供して、最新バージョン以外のバージョンのパッケージをインストールします。version 値には、文字、数字、アンダースコア、ハイフン、およびピリオドを含み、長さは最大 128 文字までです。人間が読み取れるパッケージバージョンを使用して、デプロイ時にユーザーと他の管理者が正確なパッケージバージョンを簡単に指定できるようにすることをお勧めします。以下はその例です。

   ```
   "version": "1.0.1",
   ```

3. (オプション) 発行者名を追加します。以下はその例です。

   ```
   "publisher": "MyOrganization",
   ```

4. パッケージを追加します。この "packages" セクションでは、パッケージ内の .zip ファイルでサポートされているプラットフォーム、リリースバージョン、アーキテクチャについて説明しま

す。詳細については、「サポートされているパッケージのプラットフォームとアーキテクチャ」を参照してください。

platform-version はワイルドカード値 _any にすることができます。このファイルを使用して、.zip ファイルがプラットフォームのリリースをサポートしていることを示します。また、メジャーリリースバージョンの後にワイルドカードを指定して、すべてのマイナーバージョンをサポートすることもできます (たとえば 7.*)。特定のオペレーティングシステムバージョンに対して *platform-version* 値を指定する場合は、ターゲットとするオペレーティングシステム AMI のリリースバージョンと正確に一致していることを確認してください。以下は、オペレーティングシステムの正しい値を得るために推奨されるリソースです。

- Windows Server ベースのマネージドノードでは、リリースバージョンは Windows Management Instrumentation (WMI) データとして使用できます。コマンドプロンプトから次のコマンドを実行すると、バージョン情報が取得され、version の結果が解析されます。

  ```
  wmic OS get /format:list
  ```

- Linux ベースのマネージドノードでは、最初にオペレーティングシステムのリリースをスキャンしてバージョンを取得します (次のコマンド)。VERSION_ID の値を探します。

  ```
  cat /etc/os-release
  ```

  必要な結果が返らない場合は、次のコマンドを実行して LSB リリース情報を /etc/lsb-release ファイルから取得し、DISTRIB_RELEASE の値を探します。

  ```
  lsb_release -a
  ```

  これらのメソッドが失敗した場合は、通常ディストリビューションに基づいたリリースを見つけることができます。例えば、Debian Server では /etc/debian_version ファイル、Red Hat Enterprise Linux では /etc/redhat-release ファイルをスキャンできます。

  ```
  hostnamectl
  ```

```
"packages": {
    "platform": {
      "platform-version": {
        "architecture": {
```

```
          "file": ".zip-file-name-1.zip"
        }
      }
    },
    "another-platform": {
      "platform-version": {
        "architecture": {
          "file": ".zip-file-name-2.zip"
        }
      }
    },
    "another-platform": {
      "platform-version": {
        "architecture": {
          "file": ".zip-file-name-3.zip"
        }
      }
    }
  }
```

以下に例を示します。この例では、オペレーティングシステムプラットフォームは amazon、サポートされているリリースバージョンは 2016.09、アーキテクチャは x86_64、このプラットフォームをサポートする .zip ファイルは test.zip です。

```
{
    "amazon": {
        "2016.09": {
            "x86_64": {
                "file": "test.zip"
            }
        }
    }
},
```

ワイルドカード値 _any を追加して、パッケージが親要素のすべてのバージョンをサポートしていることを示すことができます。例えば、パッケージが Amazon Linux のリリース版でサポートされていることを示すには、パッケージステートメントは以下のようになります。バージョンまたはアーキテクチャレベルで _any ワイルドカードを使用すると、プラットフォームのすべてのバージョン、またはバージョンのすべてのアーキテクチャ、またはプラットフォームのすべてのバージョンとすべてのアーキテクチャをサポートできます。

```
{
    "amazon": {
        "_any": {
            "x86_64": {
                "file": "test.zip"
            }
        }
    }
},
```

次の例では、_any を追加して、最初のパッケージ data1.zip が Amazon Linux 2016.09 のすべてのアーキテクチャでサポートされていることを示します。2 番目のパッケージ data2.zip は、Amazon Linux のすべてのリリースでサポートされていますが、x86_64 アーキテクチャのマネージドノードでのみサポートされています。2016.09 および _any バージョンは両方とも amazon 下にあるエントリです。1 つのプラットフォーム (Amazon Linux) がありますが、サポートされているバージョン、アーキテクチャ、および関連する .zip ファイルは異なります。

```
{
    "amazon": {
        "2016.09": {
            "_any": {
                "file": "data1.zip"
            }
        },
        "_any": {
            "x86_64": {
                "file": "data2.zip"
            }
        }
    }
}
```

.zip ファイルが複数のプラットフォームをサポートしている場合は、マニフェストの "packages" セクションで複数回 .zip ファイルを参照できます。例えば、Red Hat Enterprise Linux 7.x バージョンと Amazon Linux の両方をサポートする .zip ファイルがある場合、次の例に示すように、同じ .zip ファイルを指す 2 つのエントリが "packages" セクションにあります。

```
{
```

```
    "amazon": {
        "2018.03": {
            "x86_64": {
                "file": "test.zip"
            }
        }
    },
    "redhat": {
        "7.*": {
            "x86_64": {
                "file": "test.zip"
            }
        }
    }
},
```

5. ステップ 4。からこのパッケージの一部である .zip ファイルのリストを追加します。各ファイルエントリには、ファイル名と sha256 ハッシュ値チェックサムが必要です。マニフェストのチェックサム値は、パッケージのインストールが失敗しないように、圧縮されたアセットの sha256 ハッシュ値と一致する必要があります。

   インストール可能ファイルから正確なチェックサムを取得するには、次のコマンドを実行します。Linux では、`shasum -a 256 file-name.zip` または `openssl dgst -sha256 file-name.zip` を実行します。Windows では、PowerShell で `Get-FileHash -Path path-to-.zip-file` コマンドレットを実行します。

   マニフェストの "files" セクションには、パッケージ内の各 .zip ファイルへのリファレンスが 1 つ含まれています。

```
"files": {
        "test-agent-x86.deb.zip": {
            "checksums": {
                "sha256":
 "EXAMPLE2706223c7616ca9fb28863a233b38e5a23a8c326bb4ae241dcEXAMPLE"
            }
        },
        "test-agent-x86_64.deb.zip": {
            "checksums": {
                "sha256":
 "EXAMPLE572a745844618c491045f25ee6aae8a66307ea9bff0e9d1052EXAMPLE"
            }
        },
```

```
        "test-agent-x86_64.nano.zip": {
            "checksums": {
                "sha256":
"EXAMPLE63ccb86e830b63dfef46995af6b32b3c52ce72241b5e80c995EXAMPLE"
            }
        },
        "test-agent-rhel5-x86.nano.zip": {
            "checksums": {
                "sha256":
"EXAMPLE13df60aa3219bf117638167e5bae0a55467e947a363fff0a51EXAMPLE"
            }
        },
        "test-agent-x86.msi.zip": {
            "checksums": {
                "sha256":
"EXAMPLE12a4abb10315aa6b8a7384cc9b5ca8ad8e9ced8ef1bf0e5478EXAMPLE"
            }
        },
        "test-agent-x86_64.msi.zip": {
            "checksums": {
                "sha256":
"EXAMPLE63ccb86e830b63dfef46995af6b32b3c52ce72241b5e80c995EXAMPLE"
            }
        },
        "test-agent-rhel5-x86.rpm.zip": {
            "checksums": {
                "sha256":
"EXAMPLE13df60aa3219bf117638167e5bae0a55467e947a363fff0a51EXAMPLE"
            }
        },
        "test-agent-rhel5-x86_64.rpm.zip": {
            "checksums": {
                "sha256":
"EXAMPLE7ce8a2c471a23b5c90761a180fd157ec0469e12ed38a7094d1EXAMPLE"
            }
        }
    }
```

6. パッケージ情報を追加したら、マニフェストファイルを保存して閉じます。

完了したマニフェストの例を次に示します。この例では、複数のプラットフォームをサポートするが、NewPackage_LINUX.zip セクションでは 1 回のみ参照される .zip ファイル "files" があります。

```
{
    "schemaVersion": "2.0",
    "version": "1.7.1",
    "publisher": "Amazon Web Services",
    "packages": {
        "windows": {
            "_any": {
                "x86_64": {
                    "file": "NewPackage_WINDOWS.zip"
                }
            }
        },
        "amazon": {
            "_any": {
                "x86_64": {
                    "file": "NewPackage_LINUX.zip"
                }
            }
        },
        "ubuntu": {
            "_any": {
                "x86_64": {
                    "file": "NewPackage_LINUX.zip"
                }
            }
        }
    },
    "files": {
        "NewPackage_WINDOWS.zip": {
            "checksums": {
                "sha256":
 "EXAMPLEc2c706013cf8c68163459678f7f6daa9489cd3f91d52799331EXAMPLE"
            }
        },
        "NewPackage_LINUX.zip": {
            "checksums": {
                "sha256":
 "EXAMPLE2b8b9ed71e86f39f5946e837df0d38aacdd38955b4b18ffa6fEXAMPLE"
            }
        }
    }
}
```

パッケージの例

サンプルパッケージ、ExamplePackage.zip は、当社のウェブサイトからダウンロードすることができます。サンプルパッケージには、完了した JSON マニフェストと 3 つの .zip ファイルが含まれています。

ステップ 3: Amazon S3 バケットにパッケージとマニフェストをアップロードする

すべての .zip ファイルをフォルダまたはディレクトリにコピーまたは移動して、パッケージを準備します。有効なパッケージには ステップ 2: JSON パッケージマニフェストを作成する で作成したマニフェストとマニフェストファイルリストで特定されたすべての .zip ファイルが必要です。

Amazon S3 にパッケージとマニフェストをアップロードするには

1. マニフェストで指定したすべての .zip アーカイブファイルを、フォルダまたはディレクトリにコピーまたは移動します。.zip アーカイブファイルとマニフェストファイルの移動先のフォルダやディレクトリは圧縮しないでください。
2. バケットを作成するか、既存のバケットを選択します。詳細については、Amazon Simple Storage Service 入門ガイドの「バケットの作成」を参照してください。AWS CLI コマンドを実行してバケットを作成する方法の詳細については、AWS CLI コマンドリファレンスの「mb」を参照してください。
3. フォルダかディレクトリをバケットにアップロードします。詳細については、Amazon Simple Storage Service 入門ガイドの「バケットへのオブジェクトの追加」を参照してください。JSON マニフェストを AWS Systems Manager コンソールに貼り付ける場合は、マニフェストをアップロードしないでください。AWS CLI コマンドを実行してバケットにファイルをアップロードする方法の詳細については、AWS CLI コマンドリファレンスの「mv」を参照してください。
4. バケットのホームページでアップロードしたフォルダかディレクトリを選択します。バケット内のサブフォルダにファイルをアップロードした場合は、サブフォルダ ([prefix] とも呼ばれる) を書き留めます。パッケージを Distributor に追加するには、プレフィックスが必要です。

ステップ 4: パッケージを Distributor に追加する

AWS Systems Manager コンソール、AWS コマンドラインツール (AWS CLI および AWS Tools for PowerShell)、または AWS SDK を使用して、Distributor に新しいパッケージを追加できます。パッケージを追加すると、新しい SSM ドキュメントを追加します。このドキュメントでは、マネージドノードにパッケージをデプロイすることができます。

トピック

- コンソールを使用してパッケージを追加する
- AWS CLI を使用してパッケージを追加する

コンソールを使用してパッケージを追加する

AWS Systems Manager コンソールを使用してパッケージを作成できます。ステップ 3: Amazon S3 バケットにパッケージとマニフェストをアップロードする でパッケージをアップロードしたバケットの名前を用意します。

Distributor にパッケージを追加するには (コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Distributor] を選択します。
3. Distributor ホームページで [Create package (パッケージの作成)]、[Advanced] の順に選択します。
4. [Create package (パッケージの作成)] ページに、パッケージの名前を入力します。パッケージ名には、文字、数字、ピリオド、ダッシュ、アンダースコアを含めることができます。この名前は、パッケージの添付ファイルのすべてのバージョンに適用できるほど一般的である必要がありますが、パッケージの目的を識別できるよう具体的な名前である必要があります。
5. [Version name (バージョン名)] で、マニフェストファイルの `version` エントリの正確な値を入力します。
6. [S3 バケット名] で、the section called “ステップ 3: Amazon S3 バケットにパッケージとマニフェストをアップロードする” で .zip ファイルとマニフェストをアップロードしたバケットの名前を選択します。
7. [S3 キープレフィックス] に、.zip ファイルとマニフェストが保存されているバケットのサブフォルダを入力します。
8. [マニフェスト] で、[パッケージから抽出] を選択して、.zip ファイルとともに Amazon S3 バケットにアップロードしたマニフェストを使用します。

   （オプション）.zip ファイルを保存した S3 バケットに JSON マニフェストをアップロードしなかった場合は、[新しいマニフェスト] を選択します。JSON エディタフィールドで、マニフェスト全体を作成または貼り付けることができます。JSON マニフェストの作成方法の詳細については、「ステップ 2: JSON パッケージマニフェストを作成する」を参照してください。

9. マニフェストの作成または貼り付けが完了したら、[パッケージの作成] を選択します。
10. Distributor で .zip ファイルとマニフェストからパッケージが作成されるまで待ちます。追加するパッケージの数とサイズによっては、数分かかる場合があります。 Distributor では、新しいパッケージの [Package details] ページに自動的にリダイレクトされますが、ソフトウェアのアップロード後にこのページを自分で開くことを選択することもできます。Distributor でパッケージの作成プロセスが完了するまで、[パッケージの詳細] ページにはパッケージに関する情報は表示されません。アップロードプロセスとパッケージ作成プロセスを停止するには、[Cancel] を選択します。

AWS CLI を使用してパッケージを追加する

AWS CLI を使用してパッケージを作成できます。ステップ 3: Amazon S3 バケットにパッケージとマニフェストをアップロードする でパッケージをアップロードしたバケットから URL を準備します。

AWS CLI を使用して Amazon S3 にパッケージを追加するには

1. AWS CLI を使用してパッケージを作成するには、次のコマンドを実行します。コマンドの *package-name* はパッケージ名に、*path-to-manifest-file* は JSON マニフェストファイルのファイルパスに置き換えてください。amzn-s3-demo-bucket は、パッケージ全体が保存されている Amazon S3 バケットの URL です。Distributor で create-document コマンドを実行する場合は、`--document-type` の `Package` 値を指定します。

   マニフェストファイルを Amazon S3 バケットに追加しなかった場合、`--content` パラメータ値は JSON マニフェストファイルへのファイルパスです。

```
aws ssm create-document \
    --name "package-name" \
    --content file://path-to-manifest-file \
    --attachments Key="SourceUrl",Values="amzn-s3-demo-bucket" \
    --version-name version-value-from-manifest \
    --document-type Package
```

   以下はその例です。

```
aws ssm create-document \
    --name "ExamplePackage" \
    --content file://path-to-manifest-file \
```

```
    --attachments Key="SourceUrl",Values="https://s3.amazonaws.com/amzn-s3-demo-
bucket/ExamplePackage" \
    --version-name 1.0.1 \
    --document-type Package
```

2. パッケージが追加されたことを確認し、*package-name* をパッケージ名で置き換えて次のコマンドを実行して、パッケージマニフェストを表示します。ドキュメントの特定のバージョンを取得するには (パッケージのバージョンと同じではありません)、--document-version パラメータを追加します。

```
aws ssm get-document \
    --name "package-name"
```

create-document コマンドで使用できるその他のオプションについては、AWS CLI コマンドリファレンス で AWS Systems Manager のセクションの「create-document」を参照してください。get-document コマンドで使用できるその他のオプションについては、「get-document」を参照してください。

コンソールで Distributor パッケージの許可を編集する

AWS Systems Manager のツールである Distributor にパッケージを追加した後、Systems Manager コンソールでパッケージのアクセス許可を編集できます。パッケージのアクセス許可に他の AWS アカウント を追加することができます。パッケージは、同じ AWS リージョン の他のアカウントとのみ共有できます。クロスリージョン共有はサポートされていません。デフォルトでは、パッケージは [Private (プライベート)] に設定されます。つまり、パッケージ作成者の AWS アカウント へのアクセスが許可されているユーザーのみがパッケージ情報の表示、およびパッケージの更新または削除ができます。[Private (プライベート)] アクセス許可が許容される場合は、この手順をスキップできます。

> **Note**
>
> 20 個以下のアカウントで共有されているパッケージの許可を更新できます。

コンソールでパッケージの許可を編集するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Distributor] を選択します。

3. [Packages (パッケージ)] ページで、アクセス許可を編集するパッケージを選択します。
4. [Package details (パッケージの詳細)] タブで [Edit permissions (アクセス許可の編集)] を選択し、アクセス許可を変更します。
5. [Edit permissions (アクセス許可の編集)] で [Shared with specific accounts (特定のアカウントと共有)] を選択します。
6. [Shared with specific accounts (特定のアカウントと共有)] の下で、AWS アカウント 番号を 1 つずつ追加します。完了したら、[Save] を選択します。

コンソールで Distributor パッケージタグを編集する

AWS Systems Manager のツールである Distributor にパッケージを追加した後、Systems Manager コンソールでパッケージのタグを編集できます。これらのタグはパッケージに適用され、パッケージをデプロイするマネージドノードのタグには接続されません。タグは大文字と小文字を区別するキーと値のペアで、組織に関連する条件でパッケージをグループ化してフィルタリングするのに役立ちます。タグを追加しない場合は、パッケージをインストールするか、新しいバージョンを追加する準備ができました。

コンソールでパッケージタグを編集するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Distributor] を選択します。
3. [Packages (パッケージ)] ページで、タグを編集するパッケージを選択します。
4. [Package details (パッケージの詳細)] タブの [Tags (タグ)] で、[Edit (編集)] を選択します。
5. [Add tags (タグの追加)] で、タグキーまたはタグキーと値のペアを入力してから、[Add (追加)] を選択します。タグを追加するには、これを繰り返します。タグを削除するには、ウィンドウの下部にあるタグで [X] を選択します。
6. パッケージへのタグの追加が完了したら、[Save (保存)] を選択します。

Distributor パッケージにバージョンを追加する

パッケージバージョンを追加するには、パッケージを作成し、Distributor を使用して、以前のバージョン用に既に存在する AWS Systems Manager (SSM) ドキュメントにエントリを追加してパッケージバージョンを追加します。Distributor は AWS Systems Manager のツールです。時間を節約するために、パッケージの古いバージョンのマニフェストを更新し、マニフェストの `version` エン

トリの値を変更し (例: `Test_1.0` から `Test_2.0`)、新しいバージョン用のマニフェストとして保存します。Distributor コンソールの simple ワークフロー [Add version (バージョンの追加)] では、マニフェストファイルを更新します。

新しいパッケージバージョンは以下のことができます。

- 現在のバージョンにアタッチされているインストール可能なファイルのうち、1 つ以上を置き換えます。
- 追加のプラットフォームをサポートする、新しいインストール可能ファイルを追加します。
- 特定のプラットフォームのサポートを中止するためにファイルを削除します。

新しいバージョンでは、同じ Amazon Simple Storage Service (Amazon S3) バケットを使用できますが、最後に異なるファイル名の URL を指定する必要があります。Systems Manager コンソールまたは AWS Command Line Interface (AWS CLI) を使用して、新しいバージョンを追加できます。Amazon S3 バケット内の既存のインストール可能ファイルと同じ名前のインストール可能ファイルをアップロードすると、既存のファイルが上書きされます。古いバージョンから新しいバージョンにインストール可能なファイルはコピーされません。 古いバージョンからインストール可能なファイルをアップロードして、新しいバージョンの一部にする必要があります。Distributor で新しいパッケージバージョンの作成が完了したら、Distributor はバージョン管理プロセスの一環としてソフトウェアを内部 Systems Manager バケットにコピーするため、Amazon S3 バケットを削除または再利用できます。

> **Note**
>
> 各パッケージの最大バージョン数は 25 個に制限されています。不要になったバージョンは削除できます。

トピック

- コンソールを使用してパッケージバージョンを追加する
- AWS CLI を使用したパッケージバージョンの追加

コンソールを使用してパッケージバージョンを追加する

これらのステップを実行する前に「Distributor でパッケージを作成する」の手順どおりに操作を行ってそのバージョンの新しいパッケージを作成します。次に、Systems Manager コンソールを使用して、新しいパッケージバージョンを Distributor に追加します。

シンプルワークフローを使用したパッケージバージョンの追加

[Simple] ワークフローを使用してパッケージバージョンを追加するには、多くのプラットフォームとアーキテクチャをサポートできるように、更新されたインストール可能ファイルを準備するか、インストール可能ファイルを追加します。次に、Distributor を使用して、更新後の新しいインストール可能ファイルをアップロードし、パッケージバージョンを追加します。Distributor コンソールの簡略化された [Add version] ワークフローにより、マニフェストファイルと、関連する SSM ドキュメントが更新されます。

シンプルワークフローを使用してパッケージバージョンを追加するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Distributor] を選択します。
3. Distributor のホームページで、他のバージョンを追加するパッケージを選択します。
4. [Add version] ページで、[Simple] を選択します。
5. [バージョン名] に、バージョン名を入力します。新しいバージョンのバージョン名は、古いバージョン名と異なる必要があります。バージョン名は最大 512 文字で、特殊文字を含めることはできません。
6. [S3 バケット名] で、リストから既存の S3 バケットを選択します。これは、古いバージョンのインストール可能ファイルを保存するために使用したものと同じバケットである場合がありますが、バケット内の既存のインストール可能ファイルが上書きされないように、インストール可能ファイル名は別の名前になっている必要があります。
7. [S3 キープレフィックス] で、インストール可能なアセットが保存されているバケットのサブフォルダを入力します。
8. [Upload software (ソフトウェアのアップロード)] で、新しいバージョンにアタッチするインストール可能なソフトウェアファイルにナビゲートします。既存のバージョンからインストール可能なファイルは、新しいバージョンに自動的にコピーされません。インストール可能な同じファイルのいずれかを新しいバージョンの一部にする場合は、パッケージの古いバージョンのインストール可能ファイルをアップロードする必要があります。1 回のアクションで複数のソフトウェアファイルをアップロードできます。
9. [Target platform (ターゲットプラットフォーム)] で、インストール可能な各ファイルに表示されるターゲットオペレーティングシステムプラットフォームが正しいことを確認します。表示されているオペレーティングシステムが正しくない場合は、ドロップダウンリストから正しいオペレーティングシステムを選択します。

[Simple] バージョニングワークフローでは、各インストール可能ファイルを 1 回だけアップロードするため、複数のオペレーティングシステムで 1 つのファイルをターゲットにするためのステップが別途必要です。たとえば、`Logtool_v1.1.1.rpm` という名前のインストール可能なソフトウェアファイルをアップロードする場合は、Amazon Linux と Ubuntu オペレーティングシステムの両方で同じソフトウェアをターゲットにするように Distributor に指示するために、[Simple] ワークフローのデフォルトを変更する必要があります。この制限を回避するには、次のいずれかの操作を行います。

- 代わりに [Advanced (アドバンスト)] バージョニングワークフローを使用して、開始前に、インストール可能な各ファイルを .zip ファイルに圧縮後、マニフェストを手動で作成して、1 つのインストール可能なファイルが複数のオペレーティングシステムプラットフォーム、またはバージョンでターゲットになるようにします。詳細については、「高度なワークフローを使用したパッケージバージョンの追加」を参照してください。
- .zip ファイルが複数のオペレーティングシステムプラットフォーム、またはバージョンでターゲットになるように、[Simple] ワークフローでマニフェストファイルを手動で編集します。これを行う方法については、ステップ 2: JSON パッケージマニフェストを作成する のステップ 4 の最後を参照してください。

10. [プラットフォームのバージョン] で、表示されているオペレーティングシステムのプラットフォームのバージョンが **_any**、後にワイルドカード (7.*) が続くメジャーリリースバージョン、またはソフトウェアを適用する特定のオペレーティングシステムのリリースバージョンに一致していることを確認します。プラットフォームのバージョンの指定の詳細については、ステップ 2: JSON パッケージマニフェストを作成する のステップ 4 を参照してください。
11. [Architecture] のドロップダウンリストから、インストール可能なファイルごとに正しいプロセッサアーキテクチャを選択します。サポートされるアーキテクチャの詳細については、「サポートされているパッケージのプラットフォームとアーキテクチャ」を参照してください。
12. （オプション）[スクリプト] を展開し、Distributor がインストール可能なソフトウェアに対し生成するインストールおよびアンインストールスクリプトを確認します。
13. インストール可能なソフトウェアファイルを新しいバージョンにさらに追加するには、[Add software (ソフトウェアの追加)] を選択します。それ以外の場合は、次のステップに進みます。
14. (オプション) [Manifest (マニフェスト)] を展開し、インストール可能なソフトウェアに対して Distributor が生成する JSON パッケージのマニフェストを確認します。プラットフォームのバージョンやターゲットのプラットフォームなど、この手順を開始してから、インストール可能なソフトウェアに関する情報を変更した場合は、[Generate manifest (マニフェストの生成)] を選択して、更新されたパッケージマニフェストを表示します。

ステップ 9 で説明されているように、複数のオペレーティングシステムでインストール可能なソフトウェアをターゲットにする場合は、マニフェストを手動で編集できます。マニフェストの編集の詳細については、「ステップ 2: JSON パッケージマニフェストを作成する」を参照してください。

15. ソフトウェアの追加とターゲットプラットフォーム、バージョン、およびアーキテクチャデータの確認が終了したら、[Add version (バージョンの追加)] を選択します。
16. Distributor でソフトウェアがアップロードされ、新しいパッケージバージョンが作成されるまで待ちます。 Distributor は、インストール可能なファイルごとにアップロードステータスを示します。追加するパッケージの数とサイズによっては、数分かかる場合があります。Distributor では、パッケージの [Package details] ページに自動的にリダイレクトされますが、ソフトウェアのアップロード後にこのページを自分で開くことを選択することもできます。Distributor で新しいパッケージバージョンの作成が完了するまで、[Package details] ページに、パッケージに関する情報は表示されません。アップロードとパッケージバージョンの作成を停止するには、[Stop upload (アップロードの停止)] を選択します。
17. Distributor でソフトウェアのインストール可能なファイルをアップロードできない場合は、[Upload failed (アップロードに失敗しました)] メッセージが表示されます。アップロードを再試行するには、[Retry upload (アップロードの再試行)] を選択します。パッケージバージョン作成エラーをトラブルシューティングする方法の詳細については、「AWS Systems ManagerDistributor のトラブルシューティング」を参照してください。
18. Distributor で、新しいパッケージバージョンの作成が完了したら、パッケージの [Details (詳細)] ページの [Versions (バージョン)] タブの使用可能なパッケージバージョンのリストに新しいバージョンが表示されます。バージョンを選択し、[Set default version (デフォルトのバージョンを設定する)] を選択して、パッケージのデフォルトバージョンを設定します。

    デフォルトのバージョンを設定しない場合は、最新のパッケージのバージョンがデフォルトバージョンになります。

高度なワークフローを使用したパッケージバージョンの追加

パッケージバージョンを追加するには、パッケージを作成し、Distributor を使用して、以前のバージョン用に存在するドキュメントにエントリを追加してパッケージバージョンを追加します。時間を節約するために、パッケージの古いバージョンのマニフェストを更新し、マニフェストの `version` エントリの値を変更し (例: `Test_1.0` から `Test_2.0`)、新しいバージョン用のマニフェストとして保存します。[Advanced] ワークフローを使用して、新しいパッケージバージョンを追加するには、更新されたマニフェストが必要です。

高度なワークフローを使用してパッケージバージョンを追加するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Distributor] を選択します。
3. Distributor のホームページで、他のバージョンを追加するパッケージを選択し、[Add version (バージョンの追加)] を選択します。
4. [Version name (バージョン名)] で、マニフェストファイルの `version` エントリ内の正確な値を入力します。
5. [S3 バケット名] で、リストから既存の S3 バケットを選択します。これは、古いバージョンのインストール可能ファイルを保存するために使用したものと同じバケットである場合がありますが、バケット内の既存のインストール可能ファイルが上書きされないように、インストール可能ファイル名は別の名前になっている必要があります。
6. [S3 キープレフィックス] で、インストール可能なアセットが保存されているバケットのサブフォルダを入力します。
7. [マニフェスト] で、[パッケージから抽出] を選択して、.zip ファイルとともに S3 バケットにアップロードしたマニフェストを使用します。

   (オプション) .zip ファイルを保存した Amazon S3 バケットに、改訂された JSON マニフェストをアップロードしなかった場合は、[新しいマニフェスト] を選択します。JSON エディタフィールドで、マニフェスト全体を作成または貼り付けることができます。JSON マニフェストの作成方法の詳細については、「ステップ 2: JSON パッケージマニフェストを作成する」を参照してください。
8. マニフェストの作成または貼り付けが完了したら、[Add package version (パッケージバージョンの追加)] を選択します。
9. パッケージの [Details (詳細)] ページの [Versions (バージョン)] タブで使用可能なパッケージバージョンのリストに新しいバージョンが表示されます。バージョンを選択し、[Set default version (デフォルトのバージョンを設定する)] を選択して、パッケージのデフォルトバージョンを設定します。

   デフォルトのバージョンを設定しない場合は、最新のパッケージのバージョンがデフォルトバージョンになります。

AWS CLI を使用したパッケージバージョンの追加

AWS CLI を使用して、新しいパッケージバージョンを Distributor に追加できます。これらのコマンドを実行する前に、このトピックの冒頭で説明したように、新しいパッケージバージョンを作成して S3 にアップロードする必要があります。

AWS CLI を使用してパッケージバージョンを追加するには

1. 次のコマンドを実行して、新しいパッケージバージョンのエントリを含む AWS Systems Manager ドキュメントを編集します。*document-name* をドキュメントの名前に置き換えます。*amzn-s3-demo-bucket* は、「ステップ 3: Amazon S3 バケットにパッケージとマニフェストをアップロードする」でコピーした JSON マニフェストの URL に置き換えます。*S3-bucket-URL-of-package* は、パッケージ全体が格納される Amazon S3 バケットの URL です。*version-name-from-updated-manifest* をマニフェストの version の値に置き換えます。--document-version パラメータを $LATEST に設定すると、このパッケージバージョンに関連付けられたドキュメントがドキュメントの最新バージョンになります。

```
aws ssm update-document \
    --name "document-name" \
    --content "S3-bucket-URL-to-manifest-file" \
    --attachments Key="SourceUrl",Values="amzn-s3-demo-bucket" \
    --version-name version-name-from-updated-manifest \
    --document-version $LATEST
```

以下はその例です。

```
aws ssm update-document \
    --name ExamplePackage \
    --content "https://s3.amazonaws.com/amzn-s3-demo-bucket/ExamplePackage/
manifest.json" \
    --attachments Key="SourceUrl",Values="https://s3.amazonaws.com/amzn-s3-demo-
bucket/ExamplePackage" \
    --version-name 1.1.1 \
    --document-version $LATEST
```

2. 次のコマンドを実行して、パッケージが更新されたことを確認し、パッケージマニフェストを表示します。*package-name* をパッケージの名前に置き換えます。必要であれば、*document-version* を更新したドキュメントのバージョン数 (パッケージのバージョンと同じではない) と置き換えます。このパッケージバージョンがドキュメントの最新バージョンに関連付けられてい

る場合は、オプションの $LATEST パラメータの値に対して --document-version を指定できます。

```
aws ssm get-document \
    --name "package-name" \
    --document-version "document-version"
```

update-document コマンドで使用できるその他のオプションについては、AWS CLI コマンドリファレンス で AWS Systems Manager のセクションの「update-document」を参照してください。

Distributor パッケージをインストールまたは更新する

AWS Systems Manager のツールである Distributor を使用して、AWS Systems Manager マネージドノードにパッケージをデプロイできます。パッケージをデプロイするには、AWS Management Console または AWS Command Line Interface (AWS CLI) を使います。コマンドごとに 1 つのパッケージの 1 つのバージョンをデプロイできます。新しいパッケージをインストールすることも、既存のインストールを更新することもできます。特定のバージョンをデプロイするか、常にデプロイ用のパッケージの最新バージョンをデプロイするかを選択できます。パッケージをインストールするときは、AWS Systems Manager のツールである State Manager を使用することが推奨されます。State Manager を使用すると、マネージドノードで常に最新バージョンのパッケージが実行されていることを確認できます。

Important

ディストリビューターを使用してインストールしたパッケージは、ディストリビューターを使用してアンインストールします。他の方法を使用すると、Systems Manager はこのアプリケーションを INSTALLED として登録し、意図しない結果を引き起こす可能性があります。

Preference	AWS Systems Manager アクション	詳細情報
パッケージをすぐにインストールまたは更新します。	Run Command	• コンソールを使用したパッケージの 1 回インストールまたは更新

Preference	AWS Systems Manager アクション	詳細情報
		• AWS CLI を使用したパッケージのインストール (1 回) • AWS CLI を使用したパッケージの更新 (1 回)
スケジュールにパッケージをインストールするか更新して、インストールに常にデフォルトバージョンが含まれるようにします。	State Manager	• コンソールを使用したパッケージのインストールまたは更新のスケジュール • AWS CLI を使用してパッケージのインストールをスケジュールする • AWS CLI を使用したパッケージ更新のスケジュール
特定のタグまたはタグのセットを持つ新しいマネージドノードにパッケージを自動的にインストールします。例えば、新しいインスタンスに Amazon CloudWatch エージェントをインストールする場合などです。	State Manager	これを行う 1 つの方法は、新しいマネージドノードにタグを適用し、State Manager の関連付けでタグをターゲットとして指定することです。State Manager は、一致するタグを持つマネージドノードの関連付けにパッケージを自動的にインストールします。「State Manager 関連付けのターゲットとレート制御について」を参照してください。

トピック

- コンソールを使用したパッケージの 1 回インストールまたは更新
- コンソールを使用したパッケージのインストールまたは更新のスケジュール
- AWS CLI を使用したパッケージのインストール (1 回)

- AWS CLI を使用したパッケージの更新 (1 回)
- AWS CLI を使用してパッケージのインストールをスケジュールする
- AWS CLI を使用したパッケージ更新のスケジュール

コンソールを使用したパッケージの 1 回インストールまたは更新

AWS Systems Manager コンソールを使用してパッケージを 1 回インストールまたは更新できます。1 回限りのインストールを設定すると、Distributor は AWS Systems Manager のツールである AWS Systems Manager Run Command を使用してインストールを実行します。

コンソールを使用してパッケージを 1 回インストールまたは更新するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Distributor] を選択します。
3. Distributor ホームページで、インストールするパッケージを選択します。
4. [Install one time (1 回限りインストールする)] を選択します。

   このコマンドによって Run Command が開き、コマンドドキュメント `AWS-ConfigureAWSPackage` と Distributor パッケージがすでに選択されています。
5. [Document version (ドキュメントのバージョン)] で、実行する `AWS-ConfigureAWSPackage` ドキュメントのバージョンを選択します。
6. [Action] で、[Install] を選択します。
7. [Installation type (インストールのタイプ)] で、以下のいずれかを選択します。

   - [Uninstall and reinstall (アンインストールと再インストール)]: パッケージは完全にアンインストールされ、再インストールされます。再インストールが完了まで、アプリケーションは利用できません。
   - [インプレース更新]: `update` スクリプトに指定した指示に従って、新しいファイルまたは変更されたファイルのみが既存のインストールに追加されます。アプリケーションは、更新プロセス中も引き続き使用できます。このオプションは、`AWSEC2Launch-Agent` パッケージを除く AWS 公開パッケージではサポートされていません。
8. [Name (名前)] に、選択したパッケージの名前が入力されていることを確認します。
9. [Version (バージョン)] で、パッケージのバージョン名の値を入力します。このフィールドに何も指定しない場合は、Run Command が Distributor で選択したデフォルトのバージョンをインストールします。

10. [Targets] (ターゲット) セクションで、タグの指定、インスタンスまたはデバイスの手動選択、またはリソースグループを指定し、このオペレーションを実行するマネージドノードを選択します。

> **Note**
>
> リストにマネージドノードが表示されない場合は、「マネージドノードの可用性のトラブルシューティング」を参照してください。

11. [その他のパラメータ] で、以下の操作を行います。

- [コメント] に、このコマンドに関する情報を入力します。
- [タイムアウト (秒)] に、コマンドの実行全体が失敗するまでにシステムが待機する秒数を指定します。

12. [Rate Control] (レート制御) の場合:

- [Concurrency] (同時実行) で、コマンドを同時に実行するインスタンスの数または割合 (%) を指定します。

> **Note**
>
> タグまたは Resource Groups を指定してターゲットを選択し、ターゲットとなるマネージドノードの数が不明な場合は、割合 (%) を指定してドキュメントを同時に実行できるインスタンスの数を制限します。

- [Error threshold] (エラーのしきい値) で、マネージドノードの数または割合 (%) で失敗した後に他のターゲットでのコマンドの実行をいつ停止するか指定します。例えば、3 つのエラーを指定した場合、4 番目のエラーが受信されると、システムマネージャー はコマンドの送信を停止します。コマンドを処理しているマネージドノードもエラーを送信する可能性があります。

13. (オプション) コマンド出力をファイルに保存する場合は、[出力オプション] の [S3 バケットにコマンド出力を書き込む] ボックスを選択します。ボックスにバケット名とプレフィックス (フォルダ) 名を入力します。

> **Note**
>
> S3 バケットにデータを書き込む機能を許可する S3 許可は、このタスクを実行する IAM ユーザーのものではなく、インスタンスに割り当てられたインスタンスプロファイル

(EC2 インスタンスの場合) または IAM サービスロール (ハイブリッドアクティベーションマシン) のものです。詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」または「ハイブリッド環境に IAM サービスロールを作成する」を参照してください。さらに、指定された S3 バケットが別の AWS アカウント にある場合は、マネージドノードに関連付けられたインスタンスプロファイルまたは IAM サービスロールが、そのバケットへの書き込みに必要なアクセス許可があることを確認してください。

14. [SNS Notifications (SNS 通知)] セクションで、コマンドの実行状態に関する通知を受け取る場合は、[Enable SNS notifications (SNS 通知を有効にする)] チェックボックスをオンにします。

    Run Command 用の Amazon SNS 通知の設定の詳細については、「Amazon SNS 通知を使用した Systems Manager のステータス変更のモニタリング」を参照してください。
15. パッケージをインストールする準備ができたら、[Run (実行)] を選択します。
16. [Command status (コマンドのステータス)] 領域には、実行の進行状況が報告されます。コマンドがまだ進行中の場合は、コンソールの左上隅にある更新アイコンを選択して、[Overall status (全体的なステータス)] 列または [Detailed status (詳細ステータス)] 列に [Success (成功)] または [Failed (失敗)] と表示します。
17. [Targets and outputs] (ターゲットと出力) エリアで、マネージドノード名の横にあるボタンを選択し、[View output] (出力を表示) を選択します。

    コマンド出力ページには、コマンドの実行結果が表示されます。
18. (オプション) コマンド出力を S3 バケットに書き込む場合は、[Amazon S3] を選択して出力ログデータを表示します。

コンソールを使用したパッケージのインストールまたは更新のスケジュール

AWS Systems Manager コンソールを使用することで、パッケージのインストールまたは更新をスケジュールします。パッケージのインストールまたは更新をスケジュールする場合、Distributor は AWS Systems Manager State Manager を使用してインストールまたは更新を行います。

コンソールを使用してパッケージのインストールをスケジュールするには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Distributor] を選択します。
3. Distributor ホームページで、インストールまたは更新するパッケージを選択します。

4. [Package (パッケージ)] で、[Install on a schedule (スケジュールに基づいてインストールする)] を選択します。

   このコマンドは、作成された新しい関連付けに State Manager を開きます。

5. [Name (名前)] に、名前を入力します (例: **`Deploy-test-agent-package`**)。これはオプションですが推奨されます。名前にはスペースを使用できません。

6. [Document (ドキュメント)] リストで、ドキュメント名 `AWS-ConfigureAWSPackage` は既に選択されています。

7. [Action (アクション)] で、[Install (インストール)] が選択されていることを確認します。

8. [Installation type (インストールのタイプ)] で、以下のいずれかを選択します。

   - [Uninstall and reinstall (アンインストールと再インストール)]: パッケージは完全にアンインストールされ、再インストールされます。再インストールが完了まで、アプリケーションは利用できません。
   - [インプレース更新]: `update` スクリプトに指定した指示に従って、新しいファイルまたは変更されたファイルのみが既存のインストールに追加されます。アプリケーションは、更新プロセス中も引き続き使用できます。

9. [Name (名前)] に、パッケージの名前が入力されていることを確認します。

10. [Version (バージョン)] で、最新の公開バージョン以外のパッケージバージョンをインストールする場合は、バージョン ID を入力します。

11. [Targets (ターゲット)] では、[Selecting all managed instances in this account (このアカウントのすべてのマネージドインスタンスを選択する)]、[Specifying tags (タグを指定する)] または [Manually Selecting Instance (手動でインスタンスを選択する)] を選択します。タグを使用してリソースをターゲットにする場合は、提供されたフィールドにタグキーとタグ値を入力します。

    > **Note**
    >
    > [Selecting all managed instances in this account] (このアカウントのすべてのマネージドインスタンスの選択) または [Manually Selecting Instance] (インスタンスの手動での選択) を選択して、マネージド AWS IoT Greengrass コアデバイスを選択することができます。

12. [Specify schedule (スケジュールの指定)] では、[On Schedule (スケジュールあり)] を選択して定期スケジュールで関連付けを実行、または [No Schedule (スケジュールなし)] を選択して関連付けを一度実行します。これらのパラメータの詳細については、Systems Manager の関連付けの

使用を参照してください。コントロールを使用して cron、または関連付けの rate スケジュールを作成します。

13. [関連付けの作成] を選択します。
14. [Association (関連付け)] ページで、作成した関連付けの横にあるボタンを選択し、[Apply association now (関連付けを今すぐ適用)] を選択します。

    State Manager は、指定されたターゲットで関連付けを作成してすぐに実行します。関連付けの実行結果の詳細については、このガイドの「Systems Manager の関連付けの使用」を参照してください。

[詳細オプション]、[Rate control (レート制御)]、および [Output options (出力オプション)] のオプションの使用方法の詳細については、「Systems Manager の関連付けの使用」を参照してください。

AWS CLI を使用したパッケージのインストール (1 回)

AWS CLI で send-command を実行して、Distributor パッケージを 1 回インストールします。パッケージがすでにインストールされている場合、パッケージがアンインストールされ、新しいバージョンがインストールされる間、アプリケーションはオフラインになります。

AWS CLI を使用してパッケージを 1 回インストールするには

- AWS CLI で、次のコマンドを実行します。

```
aws ssm send-command \
    --document-name "AWS-ConfigureAWSPackage" \
    --instance-ids "instance-IDs" \
    --parameters '{"action":["Install"],"installationType":["Uninstall and
 reinstall"],"name":["package-name (in same account) or package-ARN (shared from
 different account)"]}'
```

> **Note**
>
> installationType のデフォルトの動作は Uninstall and reinstall です。完全なパッケージをインストールする場合は、このコマンドから "installationType": ["Uninstall and reinstall"] を省略できます。

以下はその例です。

```
aws ssm send-command \
    --document-name "AWS-ConfigureAWSPackage" \
    --instance-ids "i-00000000000000" \
    --parameters '{"action":["Install"],"installationType":["Uninstall and
 reinstall"],"name":["ExamplePackage"]}'
```

send-command コマンドで使用できるその他のオプションについては、AWS CLI コマンドリファレンス で AWS Systems Manager のセクションの「send-command」を参照してください。

AWS CLI を使用したパッケージの更新 (1 回)

AWS CLI で send-command を実行して、関連するアプリケーションをオフラインにすることなく、Distributor パッケージを更新できます。パッケージ内の新規または更新されたファイルのみが置き換えられます。

AWS CLI を使用してパッケージを 1 回更新するには

- AWS CLI で、次のコマンドを実行します。

```
aws ssm send-command \
    --document-name "AWS-ConfigureAWSPackage" \
    --instance-ids "instance-IDs" \
    --parameters '{"action":["Install"],"installationType":["In-place
 update"],"name":["package-name (in same account) or package-ARN (shared from
 different account)"]}'
```

> **Note**
>
> 新規または変更されたファイルを追加する場合は、コマンドに `"installationType":["In-place update"]` を含める必要があります。

以下はその例です。

```
aws ssm send-command \
    --document-name "AWS-ConfigureAWSPackage" \
    --instance-ids "i-02573cafcfEXAMPLE" \
```

```
    --parameters '{"action":["Install"],"installationType":["In-place
 update"],"name":["ExamplePackage"]}'
```

send-command コマンドで使用できるその他のオプションについては、AWS CLI コマンドリファレンス で AWS Systems Manager のセクションの「send-command」を参照してください。

AWS CLI を使用してパッケージのインストールをスケジュールする

AWS CLI で create-association を実行して、Distributor パッケージをスケジュールに基づいてインストールします。--name の値、ドキュメント名は常に AWS-ConfigureAWSPackage です。次のコマンドでは、キー InstanceIds を使用してターゲットマネージドノードを指定します。パッケージがすでにインストールされている場合、パッケージがアンインストールされ、新しいバージョンがインストールされる間、アプリケーションはオフラインになります。

```
aws ssm create-association \
    --name "AWS-ConfigureAWSPackage" \
    --parameters '{"action":["Install"],"installationType":["Uninstall and
 reinstall"],"name":["package-name (in same account) or package-ARN (shared from
 different account)"]}' \
    --targets [{\"Key\":\"InstanceIds\",\"Values\":[\"instance-ID1\",\"instance-
ID2\"]}]
```

> **Note**
>
> installationType のデフォルトの動作は Uninstall and reinstall です。完全なパッケージをインストールする場合は、このコマンドから "installationType": ["Uninstall and reinstall"] を省略できます。

以下はその例です。

```
aws ssm create-association \
    --name "AWS-ConfigureAWSPackage" \
    --parameters '{"action":["Install"],"installationType":["Uninstall and
 reinstall"],"name":["Test-ConfigureAWSPackage"]}' \
    --targets [{\"Key\":\"InstanceIds\",\"Values\":[\"i-02573cafcfEXAMPLE\",
\"i-0471e04240EXAMPLE\"]}]
```

create-association コマンドで使用できるその他のオプションについては、AWS CLI コマンドリファレンス で AWS Systems Manager のセクションの「create-association」を参照してください。

AWS CLI を使用したパッケージ更新のスケジュール

AWS CLI で create-association を実行して、関連付けられたアプリケーションをオフラインにすることなく、スケジュールに従って Distributor パッケージを更新できます。パッケージ内の新規または更新されたファイルのみが置き換えられます。--name の値、ドキュメント名は常に AWS-ConfigureAWSPackage です。次のコマンドでは、キー InstanceIds を使用してターゲットインスタンスを指定します。

```
aws ssm create-association \
    --name "AWS-ConfigureAWSPackage" \
    --parameters '{"action":["Install"],"installationType":["In-place update"],"name":
["package-name (in same account) or package-ARN (shared from different account)"]}' \
    --targets [{\"Key\":\"InstanceIds\",\"Values\":[\"instance-ID1\",\"instance-
ID2\"]}]
```

> **Note**
>
> 新規または変更されたファイルを追加する場合は、コマンドに "installationType": ["In-place update"] を含める必要があります。

以下はその例です。

```
aws ssm create-association \
    --name "AWS-ConfigureAWSPackage" \
    --parameters '{"action":["Install"],"installationType":["In-place update"],"name":
["Test-ConfigureAWSPackage"]}' \
    --targets [{\"Key\":\"InstanceIds\",\"Values\":[\"i-02573cafcfEXAMPLE\",
\"i-0471e04240EXAMPLE\"]}]
```

create-association コマンドで使用できるその他のオプションについては、AWS CLI コマンドリファレンス で AWS Systems Manager のセクションの「create-association」を参照してください。

Distributor パッケージをアンインストールする

AWS Management Consoleまたは AWS Command Line Interface (AWS CLI) を使用して、Distributor パッケージを AWS Systems Manager マネージドノードから Run Command を使ってアンインス

トールします。Distributor と Run Command は AWS Systems Manager のツールです。このリリースでは、コマンドごとに 1 つのパッケージの 1 つのバージョンをアンインストールできます。特定のバージョンやデフォルトのバージョンをアンインストールすることもできます。

> **Important**
>
> ディストリビューターを使用してインストールしたパッケージは、ディストリビューターを使用してアンインストールします。他の方法を使用すると、Systems Manager はこのアプリケーションを `INSTALLED` として登録し、意図しない結果を引き起こす可能性があります。

トピック

- コンソールを使用したパッケージのアンインストール
- AWS CLI を使用したパッケージのアンインストール

コンソールを使用したパッケージのアンインストール

Systems Manager コンソールで Run Command を使用して、パッケージを 1 回アンインストールできます。Distributor は AWS Systems Manager Run Command を使用してパッケージをアンインストールします。

コンソールを使用してパッケージをアンインストールするには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Run Command] を選択します。
3. Run Command ホームページで、[Run command (コマンドの実行)] を選択します。
4. `AWS-ConfigureAWSPackage` コマンドドキュメントを選択します。
5. [Action (アクション)] で、[Uninstall (アンインストール)] を選択します。
6. [Name (名前)] で、アンインストールするパッケージの名前を入力します。
7. [Targets] (ターゲット) で、マネージドノードをターゲットにする方法を選択します。ターゲットで共有されるタグキーと値を指定できます。また、ID、プラットフォーム、および SSM Agent バージョンなどの属性を選択してターゲットを指定することもできます。
8. 詳細オプションを使用して、オペレーションに関するコメントを追加したり、[Rate control (レートの制御)] で [Concurrency (同時実行)] 値と [Error threshold (エラーのしきい値)] を変更したり、出力オプションを指定したり、Amazon Simple Notification Service (Amazon SNS) 通知

を設定したりできます。詳細については、このガイドの「コンソールからコマンドを実行する」を参照してください。

9. パッケージをアンインストールする準備ができたら、[Run (実行)] を選択し、[View results (結果を表示)] を選択します。
10. コマンドリストで、実行した AWS-ConfigureAWSPackage コマンドを選択します。コマンドが進行中の場合は、コンソールの上部右端にある更新アイコンを選択します。
11. [Status] (ステータス) 列に [Success] (成功) または [Failed] (失敗) が表示されたら、[Output] (出力) タブを選択します。
12. [View output (出力を表示)] を選択します。コマンド出力ページには、コマンドの実行結果が表示されます。

AWS CLI を使用したパッケージのアンインストール

AWS CLI を使用して、マネージドノードから Distributor パッケージを Run Command を使用することでアンインストールできます。

AWS CLI を使用してパッケージをアンインストールするには

- AWS CLI で、次のコマンドを実行します。

```
aws ssm send-command \
    --document-name "AWS-ConfigureAWSPackage" \
    --instance-ids "instance-IDs" \
    --parameters '{"action":["Uninstall"],"name":["package-name (in same account)
 or package-ARN (shared from different account)"]}'
```

以下はその例です。

```
aws ssm send-command \
    --document-name "AWS-ConfigureAWSPackage" \
    --instance-ids "i-02573cafcfEXAMPLE" \
    --parameters '{"action":["Uninstall"],"name":["Test-ConfigureAWSPackage"]}'
```

send-command コマンドで使用できるその他のオプションについては、AWS CLI コマンドリファレンス で AWS Systems Manager のセクションの「send-command」を参照してください。

Distributor パッケージを削除する

このセクションでは、 パッケージを削除する方法について説明します。削除はすべてのパッケージが対象になります。パッケージの 1 つのバージョンのみを削除することはできません。

コンソールを使用したパッケージの削除

AWS Systems Manager コンソールを使用して、AWS Systems Manager のツールである Distributor からパッケージまたはパッケージバージョンを削除できます。パッケージを削除すると、Distributor からのパッケージのすべてのバージョンが削除されます。

コンソールを使用してパッケージを削除するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Distributor] を選択します。
3. Distributor ホームページで、削除するパッケージを選択します。
4. パッケージの詳細ページで、[Delete package (パッケージを削除)] を選択します。
5. 削除の確認を求められたら、[Delete package (パッケージを削除)] を選択します。

コンソールを使用したパッケージバージョンの削除

Systems Manager コンソールを使用して、Distributor からパッケージバージョンを削除できます。

コンソールを使用してパッケージバージョンを削除するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Distributor] を選択します。
3. Distributor ホームページで、削除するパッケージのバージョンを選択します。
4. パッケージのバージョンページで、削除するバージョンを選択してから、[Delete version (バージョンの削除)] を選択します。
5. 削除の確認を求められたら、[Delete package version (パッケージのバージョンの削除)] を選択します。

コマンドラインを使用したパッケージの削除

任意のコマンドラインツールを使用して、Distributor からパッケージを削除できます。

Linux & macOS

AWS CLI を使用してパッケージを削除するには

1. 次のコマンドを実行して特定のパッケージのドキュメントを一覧表示します。このコマンドの結果で削除するパッケージを探します。

```
aws ssm list-documents \
    --filters Key=Name,Values=package-name
```

2. 以下のコマンドを実行して、パッケージを削除します。*package-name* をパッケージ名に置き換えます。

```
aws ssm delete-document \
    --name "package-name"
```

3. 再度 list-documents コマンドを実行して、そのパッケージが削除されたことを確認します。削除したパッケージがリストにないことがわかります。

```
aws ssm list-documents \
    --filters Key=Name,Values=package-name
```

Windows

AWS CLI を使用してパッケージを削除するには

1. 次のコマンドを実行して特定のパッケージのドキュメントを一覧表示します。このコマンドの結果で削除するパッケージを探します。

```
aws ssm list-documents ^
    --filters Key=Name,Values=package-name
```

2. 以下のコマンドを実行して、パッケージを削除します。*package-name* をパッケージ名に置き換えます。

```
aws ssm delete-document ^
    --name "package-name"
```

3. 再度 list-documents コマンドを実行して、そのパッケージが削除されたことを確認します。削除したパッケージがリストにないことがわかります。

```
aws ssm list-documents ^
    --filters Key=Name,Values=package-name
```

PowerShell

Tools for PowerShell を使用してパッケージを削除するには

1. 次のコマンドを実行して特定のパッケージのドキュメントを一覧表示します。このコマンドの結果で削除するパッケージを探します。

```
$filter = New-Object
 Amazon.SimpleSystemsManagement.Model.DocumentKeyValuesFilter
$filter.Key = "Name"
$filter.Values = "package-name"

Get-SSMDocumentList `
    -Filters @($filter)
```

2. 以下のコマンドを実行して、パッケージを削除します。*package-name* をパッケージ名に置き換えます。

```
Remove-SSMDocument `
    -Name "package-name"
```

3. 再度 Get-SSMDocumentList コマンドを実行して、そのパッケージが削除されたことを確認します。削除したパッケージがリストにないことがわかります。

```
$filter = New-Object
 Amazon.SimpleSystemsManagement.Model.DocumentKeyValuesFilter
$filter.Key = "Name"
$filter.Values = "package-name"

Get-SSMDocumentList `
    -Filters @($filter)
```

コマンドラインを使用したパッケージバージョンの削除

任意のコマンドラインツールを使用して、Distributor からパッケージのバージョンを削除できます。

Linux & macOS

AWS CLI を使用してパッケージバージョンを削除するには

1. 以下のコマンドを実行して、パッケージのバージョンを一覧表示します。このコマンドの結果で、削除するパッケージのバージョンを探します。

```
aws ssm list-document-versions \
    --name "package-name"
```

2. 次のコマンドを実行して、パッケージのバージョンを削除します。*package-name* をパッケージ名に、*version* をバージョン番号に置き換えます。

```
aws ssm delete-document \
    --name "package-name" \
    --document-version version
```

3. list-document-versions コマンドを実行して、パッケージのバージョンが削除されたことを確認します。削除したパッケージのバージョンがリストにないことがわかります。

```
aws ssm list-document-versions \
    --name "package-name"
```

Windows

AWS CLI を使用してパッケージバージョンを削除するには

1. 以下のコマンドを実行して、パッケージのバージョンを一覧表示します。このコマンドの結果で、削除するパッケージのバージョンを探します。

```
aws ssm list-document-versions ^
    --name "package-name"
```

2. 次のコマンドを実行して、パッケージのバージョンを削除します。*package-name* をパッケージ名に、*version* をバージョン番号に置き換えます。

```
aws ssm delete-document ^
    --name "package-name" ^
    --document-version version
```

3. list-document-versions コマンドを実行して、パッケージのバージョンが削除されたことを確認します。削除したパッケージのバージョンがリストにないことがわかります。

```
aws ssm list-document-versions ^
    --name "package-name"
```

PowerShell

Tools for PowerShell を使用してパッケージバージョンを削除するには

1. 以下のコマンドを実行して、パッケージのバージョンを一覧表示します。このコマンドの結果で、削除するパッケージのバージョンを探します。

```
Get-SSMDocumentVersionList `
    -Name "package-name"
```

2. 次のコマンドを実行して、パッケージのバージョンを削除します。*package-name* をパッケージ名に、*version* をバージョン番号に置き換えます。

```
Remove-SSMDocument `
    -Name "package-name" `
    -DocumentVersion version
```

3. Get-SSMDocumentVersionList コマンドを実行して、パッケージのバージョンが削除されたことを確認します。削除したパッケージのバージョンがリストにないことがわかります。

```
Get-SSMDocumentVersionList `
    -Name "package-name"
```

list-documents コマンドで使用できるその他のオプションについては、AWS CLI コマンドリファレンス で AWS Systems Manager のセクションの「list-documents」を参照してください。delete-document コマンドで使用できるその他のオプションについては、「delete-document」を参照してください。

Distributor アクティビティの監査とログ記録

AWS CloudTrail を使用して、AWS Systems Manager のツールである Distributor に関連するアクティビティを監査できます。Systems Manager の監査とログ記録のオプションに関する詳細については、「AWS Systems Manager でのログ記録とモニタリング」を参照してください。

CloudTrail を使用した Distributor アクティビティの監査

CloudTrail は、AWS Systems Manager コンソール、AWS Command Line Interface (AWS CLI)、および Systems Manager SDK で実行された API 呼び出しをキャプチャします。CloudTrail コンソールで情報を表示でき、また Amazon Simple Storage Service (Amazon S3) バケットで保存できます。アカウントのすべての CloudTrail ログに対して 1 つのバケットが使用されています。

Run Command および State Manager アクションのログには、ドキュメントの作成、パッケージのインストール、およびパッケージのアンインストールのアクティビティが表示されます。Run Command と State Manager は AWS Systems Manager のツールです。Systems Manager アクティビティの CloudTrail ログの表示と使用の詳細については、「AWS Systems Manager による AWS CloudTrail API コールのログ記録」を参照してください。

AWS Systems ManagerDistributor のトラブルシューティング

次の情報は、AWS Systems Manager のツールである Distributor を使用するときに発生する可能性のある問題の、トラブルシューティングに役立ちます。

トピック

- 同じ名前の間違ったパッケージがインストールされている
- エラー: マニフェストの取得に失敗しました: 最新バージョンのパッケージが見つかりませんでした
- エラー: マニフェストの取得に失敗しました: 検証例外
- パッケージはサポートされていません (パッケージのインストールアクションがありません)
- エラー: マニフェストのダウンロードに失敗しました: その名前のドキュメントは存在しません
- アップロード失敗
- エラー: プラットフォームが見つかりませんでした: プラットフォームのマニフェストが見つかりません: oracle、バージョン 8.9、アーキテクチャ x86_64

同じ名前の間違ったパッケージがインストールされている

問題: パッケージをインストールしましたが、Distributor は別のパッケージをインストールしました。

原因: Systems Manager が、インストール中に、結果としてユーザー定義の外部パッケージよりも先に AWS 公開パッケージを検索します。ユーザー定義のパッケージ名が AWS で公開されたパッケージ名と同じ場合、パッケージの代わりに AWS パッケージがインストールされます。

解決策: この問題を回避するには、パッケージに AWS で公開されたパッケージの名前とは異なる名前を付けます。

エラー: マニフェストの取得に失敗しました: 最新バージョンのパッケージが見つかりませんでした

問題: 次のようなエラーが発生しました。

```
Failed to retrieve manifest: ResourceNotFoundException: Could not find the latest
 version of package
arn:aws:ssm:::package/package-name status code: 400, request id: guid
```

原因: バージョン 2.3.274.0 より前の Distributor で SSM Agent のバージョンを使用しています。

解決策: SSM Agent バージョンを 2.3.274.0 以降のバージョンに更新します。詳細については、「Run Command を使用して SSM Agent を更新する」または「チュートリアル: AWS CLI で SSM Agent を自動的に更新する」を参照してください。

エラー: マニフェストの取得に失敗しました: 検証例外

問題: 次のようなエラーが発生しました。

```
Failed to retrieve manifest: ValidationException: 1 validation error detected: Value
 'documentArn'
at 'packageName' failed to satisfy constraint: Member must satisfy regular expression
 pattern:
arn:aws:ssm:region-id:account-id:package/package-name
```

原因: バージョン 2.3.274.0 より前の Distributor で SSM Agent のバージョンを使用しています。

解決策: SSM Agent バージョンを 2.3.274.0 以降のバージョンに更新します。詳細については、「Run Command を使用して SSM Agent を更新する」または「チュートリアル: AWS CLI で SSM Agent を自動的に更新する」を参照してください。

パッケージはサポートされていません (パッケージのインストールアクションがありません)

問題: 次のようなエラーが発生しました。

```
Package is not supported (package is missing install action)
```

原因: パッケージディレクトリ構造が正しくありません。

解決方法: ソフトウェアと必要なスクリプトを含む親ディレクトリを zip 圧縮しないでください。代わりに、必要なすべてのコンテンツの .zip ファイルを絶対パスに直接作成します。.zip ファイルが正しく作成されたことを検証するには、ターゲットプラットフォームディレクトリを解凍し、ディレクトリ構造を確認します。例えば、インストールスクリプトの絶対パスは */ExamplePackage_targetPlatform*/install.sh である必要があります。

エラー: マニフェストのダウンロードに失敗しました: その名前のドキュメントは存在しません

問題: 次のようなエラーが発生しました。

```
Failed to download manifest - failed to retrieve package document description:
 InvalidDocument: Document with name filename does not exist.
```

原因 1: Distributor は別のアカウントからの Distributor パッケージを共有する場合、パッケージ名でパッケージを見つけることはできません。

解決策 1: 別のアカウントからパッケージを共有する場合は、パッケージの名前だけでなく、完全な Amazon リソースネーム (ARN) を使用します。

原因 2: VPC を使用するとき、ターゲットとする AWS リージョンのドキュメント AWS-ConfigureAWSPackage を含む AWS マネージド S3 バケットへのアクセス権を、IAM インスタンスプロファイルに付与しませんでした。

解決策 2: 「SSM Agent と AWS マネージド S3 バケットとの通信」で説明されているように、IAM インスタンスプロファイルが、ターゲットとする AWS リージョンのドキュメント AWS-ConfigureAWSPackage 含む AWS マネージド S3 バケットへのアクセス権を、SSM Agent に付与していることを確認します。

アップロード失敗

問題: 次のようなエラーが発生しました。

```
Upload failed. At least one of your files was not successfully uploaded to your S3
 bucket.
```

原因: ソフトウェアパッケージの名前にスペースが含まれています。例えば、Hello World.msi はアップロードに失敗するでしょう。

エラー: プラットフォームが見つかりませんでした: プラットフォームのマニフェストが見つかりません: oracle、バージョン 8.9、アーキテクチャ x86_64

問題: 次のようなエラーが発生しました。

```
Failed to find platform: no manifest found for platform: oracle, version 8.9,
 architecture x86_64
```

原因: エラーは、JSON パッケージマニフェストに、この場合は Oracle Linux というプラットフォームの定義がないことを意味します。

解決策: Trend Micro Deep Security ソフトウェアサイトから配布するパッケージをダウンロードします。Distributor Simple ワークフロープロセスを使用して .rpm ソフトウェアパッケージを作成します。パッケージに次の値を設定し、Distributor を使用してソフトウェアパッケージのアップロードを完了します。

```
Platform version: _any
Target platform: oracle
Architecture: x86_64
```

AWS Systems Manager Fleet Manager

AWS Systems Manager のツールである Fleet Manager は統合されたユーザーインターフェイス (UI) エクスペリエンスであり、AWS またはオンプレミスで実行されているノードをリモートで管理するのに役立ちます。Fleet Manager では、1 つのコンソールからサーバーフリート全体の正常性とパフォーマンスステータスを表示できます。個々のノードからデータを収集し、コンソールから一般的なトラブルシューティングと管理タスクを実行することもできます。これには、リモートデスクトッププロトコル (RDP) を使用した Windows インスタンスへの接続、フォルダとファイルのコンテンツの表示、Windows レジストリの管理、オペレーティングシステムのユーザー管理などが含まれます。

Fleet Manager の使用を開始するには、Systems Manager コンソールを開きます。ナビゲーションペインで、[Fleet Manager] を選択します。

Fleet Manager はどのようなユーザーに適していますか?

Fleet Manager は、ノードフリートの一元的な管理を希望する、すべての AWS のお客様に適しています。

Fleet Manager はどのように組織にとってメリットになりますか?

Fleet Manager は、以下の利点を提供します。

- マネージドノードに手動で接続することなく、さまざまな一般のシステム管理タスクを実行できます。
- 複数のプラットフォームで実行されているノードを単一の統合コンソールから管理できます。
- 異なるオペレーティングシステムで実行されているノードを単一の統合コンソールから管理できます。
- システム管理の効率性を向上させます。

Fleet Manager の特徴は何ですか?

Fleet Manager の主な機能は以下のとおりです。

- Red Hat ナレッジベースポータルへのアクセス

  Red Hat Enterprise Linux (RHEL) インスタンス経由で Red Hat ナレッジベースポータル上のバイナリ、ナレッジシェア、ディスカッションフォーラムにアクセスできます。

- マネージドノードのステータス

  どのインスタンスが `running` で、どのインスタンスが `stopped` なのかの表示。停止したインスタンスの詳細については、「Amazon EC2 ユーザーガイド」の「インスタンスの停止と起動」を参照してください。AWS IoT Greengrass コアデバイスの場合、どれが `online`、`offline` なのかや、`Connection lost` のステータスを表示できます。

  > **Note**
  >
  > 2021 年 7 月 12 日より前にマネージドインスタンスを停止した場合、`stopped` マーカーは表示されません。マーカーを表示するには、インスタンスを開始して停止します。

- インスタンス情報の表示

マネージドインスタンスにアタッチされているボリュームに保存されているフォルダーとファイルのデータ、リアルタイムのインスタンスに関するパフォーマンスデータ、インスタンスに保存されているログデータに関する情報を表示します。

- エッジデバイス情報の表示

  デバイスの AWS IoT Greengrass モノの名前、SSM Agent ping のステータスおよびバージョンなどの表示。

- アカウントとレジストリの管理

  インスタンス上のオペレーティングシステム (OS) ユーザーアカウントを管理し、Windows インスタンス上のレジストリを管理します。

- 機能へのアクセスを制御

  AWS Identity and Access Management (IAM) ポリシーを使用して Fleet Manager 機能へのアクセスを制御します。これらのポリシーを使用することで、Fleet Manager の各種機能を使用できる組織内の個々のユーザーまたはグループ、およびそれらが管理できるマネージドノードを制御できます。

トピック

- Fleet Manager を設定する
- マネージドノードの使用
- Default Host Management Configuration を使用した EC2 インスタンスの自動管理
- Remote Desktop を使用して Windows Server マネージドインスタンスに接続する
- マネージドインスタンスの Amazon EBS ボリュームの管理
- Red Hat ナレッジベースポータルへのアクセス
- マネージドノードの可用性のトラブルシューティング

Fleet Manager を設定する

AWS アカウントのユーザーが AWS Systems Manager のツールである Fleet Manager を使用してマネージドノードをモニタリングおよび管理できるようにするには、それらのユーザーに必要なアクセス許可を付与する必要があります。また、Fleet Manager を使用してモニタリングおよび管理する Amazon Elastic Compute Cloud (Amazon EC2) インスタンス、AWS IoT Greengrass コアデバイス、オンプレミスサーバー、エッジデバイス、および仮想マシン (VM) は、すべて Systems Manager の

マネージドノードである必要があります。マネージドノードとは、ハイブリッドおよびマルチクラウド環境で Systems Manager で使用するように設定された任意のマシンです。

つまり、ノードが特定の前提条件を満たしており、AWS Systems Manager エージェント (SSM Agent) で構成されている必要があります。

マシンタイプに応じて、次のいずれかのトピックを参照して、当該マシンがマネージドノードの要件を満たしていることを確認します。

- Amazon EC2 インスタンス: Systems Manager を利用した EC2 インスタンスの管理

> **Tip**
>
> AWS Systems Manager のツールである Quick Setup を使用して、Amazon EC2 インスタンスを個別のアカウント内のマネージドインスタンスとしてすばやく設定できます。お客様のビジネスまたは組織が AWS Organizations を使用している場合、複数の組織単位 (OU) や AWS リージョン にわたってインスタンスを設定することもできます。Quick Setupを使用したマネージドインスタンスの設定に関する詳細については、「Quick Setup を使用して Amazon EC2 ホスト管理を設定する」を参照してください。

- クラウド内のオンプレミスおよびその他のサーバータイプ: Systems Manager を利用したハイブリッド環境およびマルチクラウド環境でのノードの管理
- AWS IoT Greengrass (エッジ) デバイス: Systems Manager を利用したエッジデバイスの管理

サンプルポリシー

- Fleet Manager へのアクセスのコントロール

Fleet Manager へのアクセスのコントロール

AWS Systems Manager のツールである Fleet Manager を使用するには、AWS Identity and Access Management (IAM) ユーザーまたはロールに必要なアクセス許可が必要です。すべての Fleet Manager 機能へのアクセス権を提供する IAM ポリシーを作成するか、選択した機能へのアクセス権を付与するようにポリシーを変更することができます。次に、アカウント内のユーザーまたは ID にこれらのアクセス許可を付与します。

タスク 1: アクセス許可を定義する IAM ポリシーを作成する

「IAM ユーザーガイド」の次のトピックで提供されている方法のいずれかに従って、ID (ユーザー、ロール、またはユーザーグループ) に Fleet Manager へのアクセスを提供する IAM を作成します。

- カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する

以下に示すサンプルポリシーのいずれかを使用するか、付与するアクセス許可に従って変更してください。Fleet Manager へのフルアクセスと読み取り専用アクセス用のサンプルポリシーを提供しています。

タスク 2: IAM ポリシーをユーザーにアタッチしてアクセス許可を付与する

Fleet Manager へのアクセス許可を定義する IAM ポリシーを作成したら、「IAM ユーザーガイド」の次のいずれかの手順を使用して、アカウントの ID にこれらのアクセス許可を付与します。

- IAM ID アクセス許可の追加 (コンソール)
- IAM ID アクセス許可の追加 (AWS CLI)
- IAM ID アクセス許可の追加 (AWS API)

トピック

- Fleet Manager 管理者アクセスのサンプルポリシー
- Fleet Manager 読み取り専用アクセスのサンプルポリシー

Fleet Manager 管理者アクセスのサンプルポリシー

以下のポリシーは、すべてのFleet Manager機能へのアクセス許可を提供します。これは、ユーザーがローカルユーザーとグループの作成と削除、ローカルグループのグループメンバーシップの変更、および Windows Server レジストリのキーまたは値の変更を実行できるということです。各#########をユーザー自身の情報に置き換えます。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"EC2",
         "Effect":"Allow",
         "Action":[
            "ec2:CreateTags",
```

```
            "ec2:DeleteTags",
            "ec2:DescribeInstances",
            "ec2:DescribeTags"
         ],
         "Resource":"*"
      },
      {
         "Sid":"General",
         "Effect":"Allow",
         "Action":[
            "ssm:AddTagsToResource",
            "ssm:DescribeInstanceAssociationsStatus",
            "ssm:DescribeInstancePatches",
            "ssm:DescribeInstancePatchStates",
            "ssm:DescribeInstanceProperties",
            "ssm:GetCommandInvocation",
            "ssm:GetServiceSetting",
            "ssm:GetInventorySchema",
            "ssm:ListComplianceItems",
            "ssm:ListInventoryEntries",
            "ssm:ListTagsForResource",
            "ssm:ListCommandInvocations",
            "ssm:ListAssociations",
            "ssm:RemoveTagsFromResource"
         ],
         "Resource":"*"
      },
      {
            "Sid":"DefaultHostManagement",
            "Effect": "Allow",
            "Action": [
                "ssm:ResetServiceSetting",
                "ssm:UpdateServiceSetting"
            ],
            "Resource": "arn:aws:ssm:region:account-id:servicesetting/ssm/managed-
instance/default-ec2-instance-management-role"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "arn:aws:iam::account-id:role/service-role/
AWSSystemsManagerDefaultEC2InstanceManagementRole",
```

```
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "ssm.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Sid":"SendCommand",
            "Effect":"Allow",
            "Action":[
                "ssm:GetDocument",
                "ssm:SendCommand",
                "ssm:StartSession"
            ],
            "Resource":[
                "arn:aws:ec2:*:account-id:instance/*",
                "arn:aws:ssm:*:account-id:managed-instance/*",
                "arn:aws:ssm:*:account-id:document/SSM-SessionManagerRunShell",
                "arn:aws:ssm:*:*:document/AWS-PasswordReset",
                "arn:aws:ssm:*:*:document/AWSFleetManager-AddUsersToGroups",
                "arn:aws:ssm:*:*:document/AWSFleetManager-CopyFileSystemItem",
                "arn:aws:ssm:*:*:document/AWSFleetManager-CreateDirectory",
                "arn:aws:ssm:*:*:document/AWSFleetManager-CreateGroup",
                "arn:aws:ssm:*:*:document/AWSFleetManager-CreateUser",
                "arn:aws:ssm:*:*:document/AWSFleetManager-CreateUserInteractive",
                "arn:aws:ssm:*:*:document/AWSFleetManager-CreateWindowsRegistryKey",
                "arn:aws:ssm:*:*:document/AWSFleetManager-DeleteFileSystemItem",
                "arn:aws:ssm:*:*:document/AWSFleetManager-DeleteGroup",
                "arn:aws:ssm:*:*:document/AWSFleetManager-DeleteUser",
                "arn:aws:ssm:*:*:document/AWSFleetManager-DeleteWindowsRegistryKey",
                "arn:aws:ssm:*:*:document/AWSFleetManager-DeleteWindowsRegistryValue",
                "arn:aws:ssm:*:*:document/AWSFleetManager-GetDiskInformation",
                "arn:aws:ssm:*:*:document/AWSFleetManager-GetFileContent",
                "arn:aws:ssm:*:*:document/AWSFleetManager-GetFileSystemContent",
                "arn:aws:ssm:*:*:document/AWSFleetManager-GetGroups",
                "arn:aws:ssm:*:*:document/AWSFleetManager-GetPerformanceCounters",
                "arn:aws:ssm:*:*:document/AWSFleetManager-GetProcessDetails",
                "arn:aws:ssm:*:*:document/AWSFleetManager-GetUsers",
                "arn:aws:ssm:*:*:document/AWSFleetManager-GetWindowsEvents",
                "arn:aws:ssm:*:*:document/AWSFleetManager-GetWindowsRegistryContent",
                "arn:aws:ssm:*:*:document/AWSFleetManager-MountVolume",
                "arn:aws:ssm:*:*:document/AWSFleetManager-MoveFileSystemItem",
```

```
            "arn:aws:ssm:*:*:document/AWSFleetManager-RemoveUsersFromGroups",
            "arn:aws:ssm:*:*:document/AWSFleetManager-RenameFileSystemItem",
            "arn:aws:ssm:*:*:document/AWSFleetManager-SetWindowsRegistryValue",
            "arn:aws:ssm:*:*:document/AWSFleetManager-StartProcess",
            "arn:aws:ssm:*:*:document/AWSFleetManager-TerminateProcess"
         ]
      },
      {
         "Sid":"TerminateSession",
         "Effect":"Allow",
         "Action":[
            "ssm:TerminateSession"
         ],
         "Resource":"*",
         "Condition": {
            "StringLike":{
               "ssm:resourceTag/aws:ssmmessages:session-id":[
                  "${aws:userid}"
               ]
            }
         }
      }
   ]
}
```

Fleet Manager 読み取り専用アクセスのサンプルポリシー

以下のポリシーは、読み取り専用のFleet Manager機能へのアクセス許可を提供します。各###############をユーザー自身の情報に置き換えます。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"EC2",
         "Effect":"Allow",
         "Action":[
            "ec2:DescribeInstances",
            "ec2:DescribeTags"
         ],
         "Resource":"*"
      },
      {
```

```
            "Sid":"General",
            "Effect":"Allow",
            "Action":[
               "ssm:DescribeInstanceAssociationsStatus",
               "ssm:DescribeInstancePatches",
               "ssm:DescribeInstancePatchStates",
               "ssm:DescribeInstanceProperties",
               "ssm:GetCommandInvocation",
               "ssm:GetServiceSetting",
               "ssm:GetInventorySchema",
               "ssm:ListComplianceItems",
               "ssm:ListInventoryEntries",
               "ssm:ListTagsForResource",
               "ssm:ListCommandInvocations",
               "ssm:ListAssociations"
            ],
            "Resource":"*"
         },
         {
            "Sid":"SendCommand",
            "Effect":"Allow",
            "Action":[
               "ssm:GetDocument",
               "ssm:SendCommand",
               "ssm:StartSession"
            ],
            "Resource":[
               "arn:aws:ec2:*:account-id:instance/*",
               "arn:aws:ssm:*:account-id:managed-instance/*",
               "arn:aws:ssm:*:account-id:document/SSM-SessionManagerRunShell",
               "arn:aws:ssm:*:*:document/AWSFleetManager-GetDiskInformation",
               "arn:aws:ssm:*:*:document/AWSFleetManager-GetFileContent",
               "arn:aws:ssm:*:*:document/AWSFleetManager-GetFileSystemContent",
               "arn:aws:ssm:*:*:document/AWSFleetManager-GetGroups",
               "arn:aws:ssm:*:*:document/AWSFleetManager-GetPerformanceCounters",
               "arn:aws:ssm:*:*:document/AWSFleetManager-GetProcessDetails",
               "arn:aws:ssm:*:*:document/AWSFleetManager-GetUsers",
               "arn:aws:ssm:*:*:document/AWSFleetManager-GetWindowsEvents",
               "arn:aws:ssm:*:*:document/AWSFleetManager-GetWindowsRegistryContent"
            ]
         },
         {
            "Sid":"TerminateSession",
            "Effect":"Allow",
```

```
            "Action":[
               "ssm:TerminateSession"
            ],
            "Resource":"*",
            "Condition": {
               "StringLike":{
                  "ssm:resourceTag/aws:ssmmessages:session-id":[
                     "${aws:userid}"
                  ]
               }
            }
         }
      ]
}
```

マネージドノードの使用

マネージドノードは、AWS Systems Manager 用に設定されたすべてのマシンを指します。以下のマシンタイプをマネージドノードとして設定できます。

- Amazon Elastic Compute Cloud (Amazon EC2) インスタンス
- 自社構築サーバー (オンプレミスサーバー)
- AWS IoT Greengrass コアデバイス
- AWS IoT および非 AWS エッジデバイス
- 他のクラウド環境内の VM を含む仮想マシン (VM)

Systems Manager コンソールで、プレフィックス「mi-」が付いたマシンは、ハイブリッドアクティベーションで実行されているマネージノードとして設定されたマシンです。エッジデバイスには AWS IoT モノの名前が表示されます。

> **Note**
>
> macOS インスタンスでサポートされる機能は、ファイルシステムの表示のみです。

Systems Manager インスタンス層について

AWS Systems Manager は、標準インスタンス層とアドバンストインスタンス層を提供します。どちらもハイブリッドおよびマルチクラウド環境のマネージドノードをサポートします。スタンダードイ

ンスタンス層では、AWS リージョン ごと、AWS アカウント ごとに最大 1,000 のマシンを登録できます。1 つのアカウントとリージョンに 1,000 を超えるマシンを登録する必要がある場合は、アドバンストインスタンス層を使用します。アドバンストインスタンス層には、マネージドノードを好きなだけ作成することができます。Systems Manager 用に構成されたすべてのマネージドノードは、従量制料金ベースで請求されます。アドバンストインスタンス層を有効化する詳細については、「アドバンストインスタンス層を有効にするには」を参照してください。料金の詳細については、「AWS Systems Manager 料金表」を参照してください。

標準インスタンス層とアドバンストインスタンス層に関する次の追加情報に注意してください。

- また、アドバンストインスタンスでは、ハイブリッドおよびマルチクラウド環境において、AWS Systems Manager Session Manager を使用して非 EC2 ノードに接続することができます。Session Manager ではインスタンスへのインタラクティブシェルでアクセスを提供します。詳細については、「AWS Systems Manager Session Manager」を参照してください。
- スタンダードインスタンスのクォータは、Systems Manager オンプレミスアクティベーションを使用する EC2 インスタンスにも適用されます (これは一般的なシナリオではありません)。
- 仮想マシン (VM) のオンプレミスインスで Microsoft がリリースしたアプリケーションにパッチを適用するには、アドバンストインスタンス層を有効化してください。アドバンストインスタンス層の使用には料金が発生します。Amazon Elastic Compute Cloud (Amazon EC2) インスタンスで Microsoft がリリースしたアプリケーションにパッチを適用する場合、追加料金はかかりません。詳細については、「Windows Server で Microsoft がリリースしたアプリケーションへのパッチ適用について」を参照してください。

マネージドノードの表示

マネージドノードがコンソールに表示されていない場合は、次の作業を行います。

1. マネージドインスタンスを作成した AWS リージョン でコンソールを開いていることを確認します。コンソールの右上隅にあるリストを使用して、リージョンを切り替えることができます。
2. マネージドノードのセットアップ手順が Systems Manager の要件を満たしていることを確認します。詳細については、AWS Systems Manager のマネージドノードのセットアップ を参照してください。
3. 非 EC2 マシンでは、ハイブリッドアクティベーションプロセスが完了したことを確認します。詳細については、「Systems Manager を利用したハイブリッド環境およびマルチクラウド環境でのノードの管理」を参照してください。

次の追加情報に注意してください。

- Fleet Manager コンソールには、終了した Amazon EC2 ノードは表示されません。
- Systems Manager では、マシン上でオペレーションを実行するにあたり正確に時間を参照する必要があります。マネージドノードの日時が正しく設定されていない場合、マシンが API リクエストの署名の日付と一致しないことがあります。詳細については、「ユースケースとベストプラクティス」を参照してください。
- タグを作成または編集した場合、テーブルフィルターに変更が表示されるまでに最大で 1 時間かかることがあります。
- マネージドノードのステータスが `Connection Lost` のまま 30 日以上経過すると、そのノードは Fleet Manager コンソールに表示されなくなる場合があります。リストに再度表示するには、接続が失われた原因となった問題を解決する必要があります。トラブルシューティングのヒントについては、「マネージドノードの可用性のトラブルシューティング」を参照してください。

マネージドノードでの Systems Manager のサポートを確認する

AWS Config には、AWS マネージドルールが用意されています。このルールは、AWS Config が AWS リソースの設定が一般的なベストプラクティスに従っているかどうかを評価するために使用する事前定義済みのカスタマイズ可能なルールです。AWS Config マネージドルールには、ec2-instance-managed-by-systems-manager ルールが含まれています。このルールは、アカウント内の Amazon EC2 インスタンスが Systems Manager によって管理されているかどうかを確認します。詳細については、AWS Config 管理ルールを参照してください。

マネージドノードのセキュリティ体制の向上

マネージドノードで許可されていないルートレベルのコマンドに対するセキュリティ体制を向上させる方法については、「SSM Agent を介してルートレベルコマンドへのアクセスを制限する」を参照してください。

マネージドノードの登録解除

マネージドノードはいつでも登録解除できます。たとえば、複数のノードを同じ AWS Identity and Access Management (IAM) ロールで任意の種類の悪意のある動作に気づいた場合、任意の時点で任意の数のマシンの登録を解除できます。(同じマシンを再登録するには、登録時に使用したものとは異なる、ハイブリッドなアクティベーションコードとアクティベーション ID を使用する必要があります)。マネージドノードの登録解除については、「ハイブリッドおよびマルチクラウド環境でのマネージドノードの登録解除」を参照してください。

トピック

- インスタンス層の設定
- マネージドノードのパスワードをリセットする
- ハイブリッドおよびマルチクラウド環境でのマネージドノードの登録解除
- Fleet Manager を使用して OS ファイルシステムを操作する
- マネージドノードのパフォーマンスの監視
- プロセスの操作
- マネージドノードのログを表示する
- Fleet Manager を使用してマネージドノード上の OS ユーザーアカウントとグループを管理する
- マネージドノードでの Windows レジストリの管理

インスタンス層の設定

このトピックでは、アドバンストインスタンス層をアクティブ化する必要があるシナリオについて説明します。

AWS Systems Manager は、ハイブリッドおよびマルチクラウド環境の非 EC2 マシン用に、スタンダードインスタンス層とアドバンストインスタンス層を提供します。

追加コストなしで、アカウントにつき AWS リージョン ごとに最大 1,000 のスタンダードハイブリッドアクティベーションノードを登録できます。ただし、1,000 を超えるハイブリッドノードを登録するには、アドバンストインスタンス層のアクティブ化が必要です。アドバンストインスタンス層の使用には料金が発生します。詳細については、AWS Systems Manager 料金を参照してください。

登録されているハイブリッドアクティベーションノードが 1,000 未満であっても、アドバンストインスタンス層が必要なシナリオはほかに 2 つあります。

- EC2 以外のノードに接続するために Session Manager を使用したい。
- EC2 以外のノードで Microsoft がリリースしたアプリケーション (オペレーティングシステム以外) にパッチを適用したい。

> **Note**
>
> Amazon EC2 インスタンスで Microsoft がリリースしたアプリケーションにパッチを適用する場合、料金はかかりません。

アドバンストインスタンス層の詳細シナリオ

以下の情報は、アドバンストインスタンス層をアクティブ化する必要がある 3 つのシナリオの詳細を示しています。

シナリオ 1: 1,000 を超えるハイブリッドアクティベーションノードを登録したい

スタンダードインスタンス層を使用すると、追加料金なしで、特定のアカウントで AWS リージョン ごとにハイブリッドおよびマルチクラウド環境に最大 1,000 個の非 EC2 ノードを登録できます。リージョンに 1,000 を超える EC2 以外のノードを登録する必要がある場合は、アドバンストインスタンス層を使用する必要があります。その後、任意の数のマシンをハイブリッドおよびマルチクラウド環境内でアクティブ化できます。アドバンストインスタンスは、Systems Manager マネージドノードとしてアクティブ化されたアドバンストノードの数と、それらのノードの実行時間に基づいて課金されます。

アクティベーションプロセスを使用するすべての Systems Manager マネージドノード (「ハイブリッドアクティベーションを作成して、Systems Manager でノードを登録する」で説明されています) は、特定のアカウントのリージョン内でオンプレミスのノード数が 1,000 を超えると課金されます。

> **Note**
>
> Systems Manager ハイブリッドアクティブ化を使用して既存の Amazon Elastic Compute Cloud (Amazon EC2) インスタンスをアクティブ化し、EC2 以外のインスタンスとして利用することもできます (例: テストなど)。これらはハイブリッドノードとしても利用できます。これは一般的なシナリオではありません。

シナリオ 2: ハイブリッドでアクティブ化されたノードで Microsoft がリリースしたアプリケーションにパッチを適用する

ハイブリッドおよびマルチクラウド環境で非 EC2 ノードで Microsoft がリリースしたアプリケーションにパッチを適用する場合も、アドバンストインスタンス層が必要です。アドバンストインスタンス層をアクティブ化して EC2 以外のノードで Microsoft アプリケーションにパッチを適用する場合は、ノードが 1,000 未満であっても、すべてのオンプレミスノードで料金が発生します。

Amazon Elastic Compute Cloud (Amazon EC2) インスタンスで Microsoft がリリースしたアプリケーションにパッチを適用する場合、追加料金はかかりません。詳細については、「Windows

Server で Microsoft がリリースしたアプリケーションへのパッチ適用について」を参照してください。

シナリオ 3: Session Manager を使用してハイブリッドがアクティブ化されたノードに接続する

Session Manager は、インスタンスへの対話的なシェルアクセスを提供します。Session Manager を使用してハイブリッドアクティベーションマネージドノードに接続するには、アドバンストインスタンス層をアクティブ化する必要があります。ノードが 1,000 未満であっても、すべてのハイブリッドがアクティブ化されたノードの料金が発生します。

概要: アドバンストインスタンス層はいつ必要になりますか?

次の表を使用して、アドバンストインスタンス層を使用する必要がある場合と、どのシナリオに追加料金が適用されるかを確認してください。

シナリオ	アドバンストインスタンス層が必要ですか?	追加料金がかかりますか?
リージョンの特定のアカウントのハイブリッドがアクティブ化されたノードの数が 1,000 を超えています。	あり	あり
Patch Manager を使用して 1,000 未満の任意の数のハイブリッドがアクティブ化されたノードで、Microsoft がリリースしたアプリケーションにパッチを適用したい。	あり	あり
Session Manager を使用して 1,000 未満の任意の数のハイブリッドがアクティブ化されたノードに接続したい。	あり	あり
1. リージョンの特定のアカウントのハイブリッドがアクティブ化されたノードの数が 1,000 以下です。	いいえ	いいえ

シナリオ	アドバンストインスタンス層が必要ですか?	追加料金がかかりますか?
2. ハイブリッドがアクティブ化されたノードでは Microsoft アプリケーションにパッチを適用していません。 3. Session Manager を使用してハイブリッドがアクティブ化されたノードに接続していません。		

トピック

- アドバンストインスタンス層を有効にするには
- アドバンストインスタンス層から標準インスタンス層に戻す

アドバンストインスタンス層を有効にするには

AWS Systems Manager は、ハイブリッドおよびマルチクラウド環境の非 EC2 マシン用に、スタンダードインスタンス層とアドバンストインスタンス層を提供します。スタンダードインスタンス層では、AWS アカウント ごと、AWS リージョン ごとに最大 1,000 のハイブリッドがアクティブ化されたマシンを登録できます。EC2 以外のノードで Microsoft がリリースしたアプリケーションにパッチを適用し、Session Manager を使用して EC2 以外のノードに接続するには、アドバンストインスタンス層でも Patch Manager を使用する必要があります。詳細については、「アドバンストインスタンス層を有効にするには」を参照してください。

このセクションでは、ハイブリッドおよびマルチクラウド環境を設定してアドバンストインスタンス層を使用する方法について説明します。

[開始する前に]

アドバンストインスタンス料金の詳細を確認します。アドバンストインスタンスは、従量制料金で利用できます。詳細については、「AWS Systems Manager の料金」を参照してください。

アドバンストインスタンス層を有効にするためのアクセス権限の設定

AWS Identity and Access Management (IAM) にアクセス許可があることを確認して、環境を標準インスタンス層からアドバンストインスタンス層に変更します。AdministratorAccess IAM ポリシーをユーザー、グループ、またはロールにアタッチするか、Systems Manager アクティベーション層サービス設定を変更するアクセス許可を持っている必要があります。アクティベーション層の設定は、次の API オペレーションを使用します。

- GetServiceSetting
- UpdateServiceSetting
- ResetServiceSetting

インライン IAM ポリシーをユーザーアカウントに追加するには、以下の手順に従います。このポリシーにより、ユーザーは現在のマネージドインスタンス層の設定を表示できます。また、このポリシーにより、ユーザーは指定された AWS アカウント および AWS リージョン の現在の設定をリセットまたは変更できます。

1. AWS Management Console にサインインして、IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. ナビゲーションペインで [Users] を選択します。
3. 一覧で、ポリシーを埋め込むユーザーの名前を選択します。
4. [Permissions] タブを選択します。
5. ページ右側にある [Permission policies (権限のポリシー)] で、[Add inline policy (インラインポリシーの追加)] を選択します。
6. [JSON] タブを選択します。
7. デフォルトコンテンツを以下のものと置き換えます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:GetServiceSetting"

            ],
            "Resource": "*"
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:ResetServiceSetting",
                "ssm:UpdateServiceSetting"
            ],
            "Resource": "arn:aws:ssm:region:aws-account-id:servicesetting/ssm/
managed-instance/activation-tier"
        }
    ]
}
```

8. [ポリシーの確認] を選択します。
9. [Review policy (ポリシーの確認)] ページで、[Name (名前)] にインラインポリシーの名前を入力します。例: **`Managed-Instances-Tier`**。
10. [Create policy] を選択します。

管理者は、ユーザーに次のインラインポリシーを割り当てることで、読み取り専用アクセス許可を指定できます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:GetServiceSetting"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "ssm:ResetServiceSetting",
                "ssm:UpdateServiceSetting"
            ],
            "Resource": "*"
        }
    ]
}
```

IAM ユーザーポリシーの作成と編集の詳細については、IAM ユーザーガイドの「IAM ポリシーの作成」を参照してください。

アドバンストインスタンス層を有効にするには (コンソール)

次の手順では、Systems Manager コンソールを使用して、指定した AWS アカウント と AWS リージョン で、マネージドインスタンスのアクティベーションを使用して追加されたすべての非 EC2 ノードでアドバンストインスタンス層を使用するように変更する方法を示します。

[開始する前に]

マネージドインスタンスを作成した AWS リージョン でコンソールを開いていることを確認します。コンソールの右上隅にあるリストを使用して、リージョンを切り替えることができます。

ハイブリッドおよびマルチクラウド環境で、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスと非 EC2 マシンのセットアップ要件を完了していることを確認します。詳細については、AWS Systems Manager のマネージドノードのセットアップ を参照してください。

> **Important**
>
> 次の手順では、アカウントレベルの設定を変更する方法について説明します。この変更の結果、料金がお客様のアカウントに請求されます。

アドバンストインスタンス層を有効にするには (コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. [設定] を選択し、次に [インスタンスティアの設定を変更] を選択します。
4. ダイアログボックスでアカウント設定の変更に関する情報を確認します。
5. 承認する場合、承認するオプションを選択し、[設定を変更] を選択します。

システムがすべてのインスタンスを標準インスタンス層からアドバンストインスタンス層に移動するプロセスを完了するのに数分かかることがあります。

> **Note**
>
> 標準インスタンス層への変更の詳細については、「アドバンストインスタンス層から標準インスタンス層に戻す」を参照してください。

アドバンストインスタンス層を有効にするには (AWS CLI)

次の手順では、AWS Command Line Interface を使用して、指定した AWS アカウント および AWS リージョン で、マネージドインスタンスのアクティベーションを使用して追加されたすべてのオンプレミスサーバーと VM でアドバンストインスタンス層を使用するように変更する方法を示します。

> **Important**
>
> 次の手順では、アカウントレベルの設定を変更する方法について説明します。この変更の結果、料金がお客様のアカウントに請求されます。

AWS CLI を使用してアドバンストインスタンス層を有効にするには

1. AWS CLI を開き、次のコマンドを実行します。各*##############*をユーザー自身の情報に置き換えます。

   Linux & macOS

   ```
   aws ssm update-service-setting \
       --setting-id arn:aws:ssm:region:aws-account-id:servicesetting/ssm/managed-instance/activation-tier \
       --setting-value advanced
   ```

   Windows

   ```
   aws ssm update-service-setting ^
       --setting-id arn:aws:ssm:region:aws-account-id:servicesetting/ssm/managed-instance/activation-tier ^
       --setting-value advanced
   ```

   コマンドが成功した場合、出力はありません。

2. 次のコマンドを実行して、現在の AWS アカウント および AWS リージョン のマネージドノードのサービス設定を表示します。

   Linux & macOS

   ```
   aws ssm get-service-setting \
       --setting-id arn:aws:ssm:region:aws-account-id:servicesetting/ssm/managed-instance/activation-tier
   ```

   Windows

   ```
   aws ssm get-service-setting ^
       --setting-id arn:aws:ssm:region:aws-account-id:servicesetting/ssm/managed-instance/activation-tier
   ```

   このコマンドによって以下のような情報が返されます。

   ```
   {
       "ServiceSetting": {
           "SettingId": "/ssm/managed-instance/activation-tier",
           "SettingValue": "advanced",
           "LastModifiedDate": 1555603376.138,
           "LastModifiedUser": "arn:aws:sts::123456789012:assumed-role/Administrator/User_1",
           "ARN": "arn:aws:ssm:us-east-2:123456789012:servicesetting/ssm/managed-instance/activation-tier",
           "Status": "PendingUpdate"
       }
   }
   ```

アドバンストインスタンス層を有効にするには (PowerShell)

次の手順では、AWS Tools for Windows PowerShell を使用して、指定した AWS アカウント および AWS リージョン で、マネージドインスタンスのアクティベーションを使用して追加されたすべてのオンプレミスサーバーと VM でアドバンストインスタンス層を使用するように変更する方法を示します。

> **Important**
>
> 次の手順では、アカウントレベルの設定を変更する方法について説明します。この変更の結果、料金がお客様のアカウントに請求されます。

PowerShell を使用してアドバンストインスタンス層を有効にするには

1. AWS Tools for Windows PowerShell を開き、次のコマンドを実行します。各*############*をユーザー自身の情報に置き換えます。

   ```
   Update-SSMServiceSetting `
       -SettingId "arn:aws:ssm:region:aws-account-id:servicesetting/ssm/managed-
   instance/activation-tier" `
       -SettingValue "advanced"
   ```

   コマンドが成功した場合、出力はありません。

2. 次のコマンドを実行して、現在の AWS アカウント および AWS リージョン のマネージドノードのサービス設定を表示します。

   ```
   Get-SSMServiceSetting `
       -SettingId "arn:aws:ssm:region:aws-account-id:servicesetting/ssm/managed-
   instance/activation-tier"
   ```

   このコマンドによって以下のような情報が返されます。

   ```
   ARN:arn:aws:ssm:us-east-2:123456789012:servicesetting/ssm/managed-instance/
   activation-tier
   LastModifiedDate : 4/18/2019 4:02:56 PM
   LastModifiedUser : arn:aws:sts::123456789012:assumed-role/Administrator/User_1
   SettingId        : /ssm/managed-instance/activation-tier
   SettingValue     : advanced
   Status           : PendingUpdate
   ```

システムがすべてのノードをスタンダードインスタンス層からアドバンストインスタンス層に移動するプロセスを完了するのに数分かかることがあります。

> **Note**
>
> 標準インスタンス層への変更の詳細については、「アドバンストインスタンス層から標準インスタンス層に戻す」を参照してください。

アドバンストインスタンス層から標準インスタンス層に戻す

このセクションでは、アドバンストインスタンス層で実行されているハイブリッドアクティベーションノードをスタンダードインスタンス層に戻す方法について説明します。この設定は、AWS アカウント のすべてのハイブリッドアクティベーションノードおよび 1 つの AWS リージョン に適用されます。

[開始する前に]

次の重要な詳細を確認してください。

> **Note**
>
> - アカウントおよびリージョンで実行しているハイブリッドアクティベーションノードの数が 1,000 を超える場合、標準インスタンス層に戻すことはできません。最初に一部のノードを登録解除して 1,000 以下にする必要があります。これは、Systems Manager をハイブリッドアクティベーションを使用する Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにも適用されます (これは一般的なシナリオではありません)。詳細については、「ハイブリッドおよびマルチクラウド環境でのマネージドノードの登録解除」を参照してください。
> - 元に戻すと、AWS Systems Manager のツールである Session Manager を使用して、ハイブリッドアクティベーションノードにインタラクティブにアクセスすることはできなくなります。
> - 元に戻すと、AWS Systems Manager のツールである Patch Manager を使用して、ハイブリッドアクティベーションノードの Microsoft アプリケーションにパッチを適用することはできなくなります。
> - すべてのハイブリッドアクティベーションノードを標準インスタンス層に戻すプロセスは、完了するまでに 30 分以上かかることがあります。

このセクションでは、AWS アカウント および AWS リージョン のすべてのハイブリッドアクティベーションノードをアドバンストインスタンス層からスタンダードインスタンス層に戻す方法について説明します。

スタンダードインスタンス層に戻す (コンソール)

次の手順は、Systems Manager コンソールを使用して、指定した AWS アカウント および AWS リージョン で、ハイブリッドおよびマルチクラウド環境のすべてのハイブリッドアクティベーションノードで標準インスタンス層を使用するように変更する方法を示しています。

スタンダードインスタンス層に戻すには (コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. [Account settings] ドロップダウンを選択し、[Instance tier settings] を選択します。
4. [Change account setting (アカウント設定の変更)] を選択します。
5. アカウント設定の変更に関するポップアップの情報を確認し、承認する場合は、同意して続行するオプションを選択します。

標準インスタンス層に戻す (AWS CLI)

次の手順では、AWS Command Line Interface を使用して、指定した AWS アカウント および AWS リージョン で標準インスタンス層を使用するように、ハイブリッドおよびマルチクラウド環境内のすべてのハイブリッドアクティベーションノードを変更する方法を示します。

AWS CLI を使用して標準インスタンス層に戻すには

1. AWS CLI を開き、次のコマンドを実行します。各*###############*をユーザー自身の情報に置き換えます。

   Linux & macOS

   ```
   aws ssm update-service-setting \
       --setting-id arn:aws:ssm:region:aws-account-id:servicesetting/ssm/managed-instance/activation-tier \
       --setting-value standard
   ```

Windows

```
aws ssm update-service-setting ^
    --setting-id arn:aws:ssm:region:aws-account-id:servicesetting/ssm/managed-
instance/activation-tier ^
    --setting-value standard
```

コマンドが成功した場合、出力はありません。

2. 次のコマンドを 30 分後に実行して、現在の AWS アカウント および AWS リージョン のマネージドインスタンスの設定を表示します。

Linux & macOS

```
aws ssm get-service-setting \
    --setting-id arn:aws:ssm:region:aws-account-id:servicesetting/ssm/managed-
instance/activation-tier
```

Windows

```
aws ssm get-service-setting ^
    --setting-id arn:aws:ssm:region:aws-account-id:servicesetting/ssm/managed-
instance/activation-tier
```

このコマンドによって以下のような情報が返されます。

```
{
    "ServiceSetting": {
        "SettingId": "/ssm/managed-instance/activation-tier",
        "SettingValue": "standard",
        "LastModifiedDate": 1555603376.138,
        "LastModifiedUser": "System",
        "ARN": "arn:aws:ssm:us-east-2:123456789012:servicesetting/ssm/managed-
instance/activation-tier",
        "Status": "Default"
    }
}
```

リクエストが承認されると、ステータスが [Default (デフォルト)] に変わります。

標準インスタンス層に戻す (PowerShell)

次の手順では、AWS Tools for Windows PowerShell を使用して、指定した AWS アカウント および AWS リージョン で標準インスタンス層を使用するように、ハイブリッドおよびマルチクラウド環境内のハイブリッドアクティベーションノードを変更する方法を示します。

PowerShell を使用して標準インスタンス層に戻すには

1. AWS Tools for Windows PowerShell を開き、次のコマンドを実行します。

```
Update-SSMServiceSetting `
    -SettingId "arn:aws:ssm:region:aws-account-id:servicesetting/ssm/managed-
instance/activation-tier" `
    -SettingValue "standard"
```

   コマンドが成功した場合、出力はありません。

2. 次のコマンドを 30 分後に実行して、現在の AWS アカウント および AWS リージョン のマネージドインスタンスの設定を表示します。

```
Get-SSMServiceSetting `
    -SettingId "arn:aws:ssm:region:aws-account-id:servicesetting/ssm/managed-
instance/activation-tier"
```

   このコマンドによって以下のような情報が返されます。

```
ARN: arn:aws:ssm:us-east-2:123456789012:servicesetting/ssm/managed-instance/
activation-tier
LastModifiedDate : 4/18/2019 4:02:56 PM
LastModifiedUser : System
SettingId        : /ssm/managed-instance/activation-tier
SettingValue     : standard
Status           : Default
```

   リクエストが承認されると、ステータスが [Default (デフォルト)] に変わります。

マネージドノードのパスワードをリセットする

マネージドノード上の任意のユーザーのパスワードをリセットできます。これには、AWS Systems Manager が管理する Amazon Elastic Compute Cloud (Amazon EC2) インスタンス、AWS IoT

Greengrass コアデバイス、オンプレミスサーバー、エッジデバイス、仮想マシン (VM) が含まれます。パスワードリセット機能は、AWS Systems Manager のツールである Session Manager 上に構築されています。この機能を使用すると、インバウンドポートを開いたり、要塞ホストを維持したり、SSH キーを管理したりせずにマネージドノードに接続できます。

ユーザーがパスワードを忘れた場合、またはマネージドノードへの RDP または SSH 接続を行わずにパスワードをすばやく更新する場合には、パスワードリセットオプションが役立ちます。

前提条件

マネージドノードのパスワードをリセットする前に、次の要件を満たす必要があります。

- パスワードを変更するマネージドノードは、Systems Manager マネージドノードである必要があります。また、SSM Agent バージョン 2.3.668.0 以降をマネージドノードにインストールする必要があります。SSM Agent のインストールまたは更新については、「「SSM Agent」 の使用」を参照してください。
- パスワードリセット機能では、アカウントに設定された Session Manager 設定を使用してマネージドノードに接続します。そのため、Session Manager を使用するための前提条件が、現在の AWS リージョン のアカウントで完了している必要があります。詳細については、「Session Manager を設定する」を参照してください。

  > **Note**
  >
  > オンプレミスノードの Session Manager サポートは、アドバンストインスタンス層に対してのみ提供されています。詳細については、「アドバンストインスタンス層を有効にするには」を参照してください。

- パスワードを変更する AWS ユーザーには、マネージドノードの `ssm:SendCommand` アクセス許可が必要です。詳細については、「タグによる Run Command アクセスを制限」を参照してください。

アクセスの制限

特定のマネージドノードへのパスワードをリセットするユーザーの能力を制限できます。これを行うには、`AWS-PasswordReset` SSM ドキュメントで Session Manager `ssm:StartSession` オペレーションに ID ベースのポリシーを使用します。詳細については、「インスタンスへのユーザーセッションアクセスを制御する」を参照してください。

データの暗号化

マネージドノードのパスワードリセットオプションを使用するには、Session Manager データの AWS Key Management Service (AWS KMS) 完全暗号化を有効にします。詳細については、「セッションデータの KMS キー暗号化を有効にする (コンソール)」を参照してください。

マネージドノードでパスワードをリセットする

Systems Manager Fleet Manager コンソールまたは AWS Command Line Interface (AWS CLI) を使用して、Systems Manager のマネージドノードでパスワードをリセットできます。

マネージドノードのパスワードを変更するには (コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. 新しいパスワードが必要なノードの横にあるボタンを選択します。
4. [インスタンスアクション]、[パスワードのリセット] を選択します。
5. [User name] に、パスワードを変更するユーザーの名前を入力します。ノードのアカウントを持つ任意のユーザー名を使用することができます。
6. [Submit] (送信) をクリックします。
7. [Enter new password] コマンドウィンドウのプロンプトに従って、新しいパスワードを指定します。

> **Note**
>
> マネージドノード上の SSM Agent のバージョンでパスワードのリセットがサポートされていない場合は、AWS Systems Manager のツールである Run Command を使用して、サポートされているバージョンをインストールするように求められます。

マネージドノードのパスワードをリセットするには (AWS CLI)

1. マネージドノードのユーザーのパスワードをリセットするには、次のコマンドを実行します。各##############をユーザー自身の情報に置き換えます。

> **Note**
>
> AWS CLI を使用してパスワードをリセットするには、ローカルマシンに Session Manager プラグインをインストールする必要があります。詳細については、AWS CLI 用の Session Manager プラグインをインストールする を参照してください。

Linux & macOS

```
aws ssm start-session \
    --target instance-id \
    --document-name "AWS-PasswordReset" \
    --parameters '{"username": ["user-name"]}'
```

Windows

```
aws ssm start-session ^
    --target instance-id ^
    --document-name "AWS-PasswordReset" ^
    --parameters username="user-name"
```

2. [Enter new password] コマンドウィンドウのプロンプトに従って、新しいパスワードを指定します。

マネージドノードでのパスワードリセットの問題をトラブルシューティングする

パスワードリセットの問題は通常、パスワードリセット前提条件 を完了することで解決できます。それ以外の問題の場合は、次の情報を使用して、パスワードリセットの問題をトラブルシューティングします。

トピック

- マネージドノードを使用できない
- SSM Agent が最新ではない (コンソール)
- パスワードリセットオプションが提供されていません (AWS CLI)
- ssm:SendCommand を実行する権限がない
- Session Manager エラーメッセージ

マネージドノードを使用できない

問題: マネージドインスタンスコンソールのページでマネージドノードのパスワードをリセットしたいが、ノードがリストにありません。

- 解決方法: 接続するマネージドノードが Systems Manager 向けに設定されていない可能性があります。Systems Manager EC2 でインスタンスを使用するには、AWS Identity and Access Management (IAM) インスタンスプロファイルをインスタンスにアタッチする必要があります。これにより、インスタンスに対してアクションを実行するためのアクセス許可が Systems Manager に付与されます。詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」を参照してください。

  Systems Manager で非 EC2 マシンを使用するには、マネージドノードでアクションを実行するための許可を Systems Manager に付与する IAM サービスロールを作成します。詳細については、「ハイブリッドおよびマルチクラウド環境で Systems Manager に必要な IAM サービスロールを作成する」を参照してください。(オンプレミスサーバーおよび VM に対する Session Manager のサポートは、アドバンストインスタンス層でのみ提供されています。詳細については「アドバンストインスタンス層を有効にするには」を参照してください。)

SSM Agent が最新ではない (コンソール)

問題: SSM Agent のバージョンがパスワードリセット機能をサポートしていないことを示すメッセージが表示される。

- 解決策: パスワードのリセットを実行するには、バージョン 2.3.668.0 以降の SSM Agent が必要です。コンソールで、[SSM Agent を更新] を選択すると、マネージドノード上のエージェントを更新できます。

  新しいツールが Systems Manager に追加されるか、既存のツールが更新されると必ず、更新されたバージョンの SSM Agent がリリースされます。最新バージョンのエージェントを使用しないと、マネージドノードが Systems Manager の各種ツールや機能を使用できなくなる可能性があります。このため、マシン上で SSM Agent を最新状態に維持するプロセスを自動化することをお勧めします。詳細については、SSM Agent への更新の自動化 を参照してください。GitHub の「SSM Agent リリースノート」ページをサブスクライブすると、SSM Agent の更新に関する通知を受け取ることができます。

パスワードリセットオプションが提供されていません (AWS CLI)

問題: AWS CLI `start-session` コマンドを使用してマネージドノードに正常に接続する。SSM ドキュメント `AWS-PasswordReset` を指定し、有効なユーザー名を指定したが、パスワードを変更するプロンプトが表示されない。

- 解決策: マネージドノードの SSM Agent のバージョンが最新ではありません。パスワードのリセットを実行するには、バージョン 2.3.668.0 以降が必要です。

  新しいツールが Systems Manager に追加されるか、既存のツールが更新されると必ず、更新されたバージョンの SSM Agent がリリースされます。最新バージョンのエージェントを使用しないと、マネージドノードが Systems Manager の各種ツールや機能を使用できなくなる可能性があります。このため、マシン上で SSM Agent を最新状態に維持するプロセスを自動化することをお勧めします。詳細については、SSM Agent への更新の自動化 を参照してください。GitHub の「SSM Agent リリースノート」ページをサブスクライブすると、SSM Agent の更新に関する通知を受け取ることができます。

`ssm:SendCommand` を実行する権限がない

問題: マネージドノードに接続してパスワードを変更しようとすると、マネージドノードで `ssm:SendCommand` を実行する権限がないことを示すエラーメッセージが表示される。

- 解決策: IAM ポリシーに、`ssm:SendCommand` コマンドを実行するアクセス許可が含まれている必要があります。詳細については、タグによる Run Command アクセスを制限 を参照してください。

Session Manager エラーメッセージ

問題: Session Manager に関連するエラーメッセージが表示されます。

- 解決策: パスワードリセットをサポートするには、Session Manager が正しく構成されている必要があります。詳細については、「Session Manager を設定する」および「Session Manager のトラブルシューティング」を参照してください。

ハイブリッドおよびマルチクラウド環境でのマネージドノードの登録解除

AWS Systems Manager を使用してオンプレミスサーバー、エッジデバイスまたは仮想マシン (VM) を管理する必要がなくなった場合は、登録解除できます。ハイブリッドアクティベーションノードの登録を解除すると、Systems Manager のマネージドノードの一覧からそのハイブリッドマシンが削

除されます。AWS Systems Managerハイブリッドアクティベーションノードで実行されていたエージェント (SSM Agent) はもう登録されていないため、認可トークンを更新できなくなります。SSM Agent は休止状態になり、クラウド内の Systems Manager に対する ping の回数が 1 時間 1 回に減少します。Systems Manager は、登録解除されたマネージドノードのコマンド履歴を 30 日間保存します。

オンプレミスサーバー、エッジデバイス、VM のいずれかを再登録する場合は、以前にこのマシンを登録したときとは異なるアクティベーションコードとアクティベーション ID を使用する必要があります。アクティベーションコードとアクティベーション ID は、これらの作成時に指定したアクティベーションの最大数で使用されていてはいけません。

次の手順では、Systems Manager コンソールを使用してハイブリッドアクティベーションノードを登録解除する方法を示します。これを AWS Command Line Interface で行う方法については、「deregister-managed-instance」を参照してください。

関連情報については、次のトピックを参照してください。

- マネージドノードの登録解除と再登録 (Linux) (Linux)
- マネージドノードの登録解除と再登録 (Windows Server) (Windows Server)

ハイブリッドアクティベーションノードを登録解除するには (コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. 登録解除するマネージドノードの横にあるチェックボックスを選択します。
4. [ノードアクション、ツール、このマネージドノードの登録を解除] を選択します。
5. [このマネージドノードの登録を解除] ダイアログボックスの情報を確認します。承認する場合は、[登録を解除] を選択します。

Fleet Manager を使用して OS ファイルシステムを操作する

AWS Systems Manager のツールである Fleet Manager を使用すると、マネージドノード上のファイルシステムを操作できます。Fleet Manager を使用して、マネージドノードにアタッチされたボリュームに保存されているディレクトリとファイルのデータに関する情報を表示できます。例えば、ディレクトリとファイルの名前、サイズ、拡張子、所有者、および許可を表示できます。Fleet Managerコンソールからは、最大 10,000 行のファイルデータをテキストとしてプレビューできま

す。この機能は、tail ファイルにも使用できます。tail を使用してファイルデータを表示するときは、ファイルの最後の 10 行が最初に表示されます。ビューは、新しいデータの行がファイルに書き込まれると同時にリアルタイムで更新されます。その結果、コンソールからログデータを確認できるようになり、トラブルシューティングとシステム管理の効率性が向上します。さらに、ディレクトリの作成、ファイルやディレクトリのコピー、切り取り、貼り付け、名前の変更、削除を行うことができます。

定期的にバックアップを作成する、またはマネージドノードにアタッチされた Amazon Elastic Block Store (Amazon EBS) ボリュームのスナップショットを作成することをお勧めします。ファイルのコピー、または切り取り、貼り付けを行うと、新しいファイルまたはディレクトリと同じ名前のデスティネーションパス内の既存のファイルとディレクトリが置き換えられます。システムファイルとディレクトリを置き換えたり変更すると、深刻な問題が発生する可能性があります。AWS は、これらの問題を解決できることを保証しません。システムファイルを変更するには、ご自分の責任で行ってください。すべてのファイルやディレクトリの変更、およびバックアップの確保はユーザーの責任となります。ファイルおよびディレクトリの削除または置換は元に戻せません。

> **Note**
>
> Fleet Manager は、AWS Systems Manager のツールである Session Manager を使用して、テキストプレビューと tail ファイルを表示します。Amazon Elastic Compute Cloud (Amazon EC2) インスタンスの場合、マネージドインスタンスにアタッチされたインスタンスプロファイルは、Session Manager がこの機能を使用する許可を提供する必要があります。インスタンスプロファイルへのSession Managerアクセス許可の追加に関する詳細については、「既存の IAM ロールに Session Manager 許可を追加する」を参照してください。

トピック

- Fleet Manager を使用して OS ファイルシステムを表示する
- Fleet Manager を使用して OS ファイルをプレビューする
- Fleet Manager を使用して OS ファイルをテーリングする
- Fleet Manager を使用して OS ファイルまたはディレクトリのコピー、切り取り、貼り付けを行う
- Fleet Manager を使用して OS ファイルとディレクトリの名前を変更する
- Fleet Manager を使用して OS ファイルとディレクトリを削除する
- Fleet Manager を使用して OS ディレクトリを作成する
- Fleet Manager を使用して OS ディレクトリの切り取り、コピー、貼り付けを行う

Fleet Manager を使用して OS ファイルシステムを表示する

Fleet Manager を使用して、Systems Manager マネージドノード上の OS ファイルシステムを表示できます。

Fleet Manager を使用して OS ファイルシステムを表示するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. 表示するファイルシステムが含まれるマネージドノードのリンクを選択します。
4. [ツール]、[ファイルシステム] を選択します。

Fleet Manager を使用して OS ファイルをプレビューする

Fleet Manager を使用して OS 上のテキストファイルをプレビューできます。

Fleet Manager を使用してファイルのテキストプレビューを表示するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. プレビューするファイルが含まれるマネージドノードのリンクを選択します。
4. [ツール]、[ファイルシステム] を選択します。
5. プレビューするファイルが含まれているディレクトリの [ファイル名] を選択します。
6. コンテンツをプレビューするファイルの横にあるボタンを選択します。
7. [アクション]、[テキストとしてプレビュー] を選択します。

Fleet Manager を使用して OS ファイルをテーリングする

Fleet Manager を使用して、マネージドノードでファイルをテーリングできます。

Fleet Manager でファイルをテーリングするには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。

2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. テールするファイルが含まれるマネージドノードのリンクを選択します。
4. [ツール]、[ファイルシステム] を選択します。
5. テールするファイルが含まれるディレクトリの [File name] (ファイル名) を選択します。
6. コンテンツをテールするファイルの横にあるボタンを選択します。
7. [アクション]、[ファイルの末尾] を選択します。

Fleet Manager を使用して OS ファイルまたはディレクトリのコピー、切り取り、貼り付けを行う

Fleet Manager を使用して、マネージドノードで OS ファイルのコピー、切り取り、貼り付けを行うことができます。

Fleet Manager を使用してファイルまたはディレクトリをコピーまたはカットアンドペーストするには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. コピー、切り取りまたは貼り付けするファイルが含まれるマネージドノードのリンクを選択します。
4. [ツール]、[ファイルシステム] を選択します。
5. ファイルをコピーまたはカットするには、コピーまたはカットするファイルを含むディレクトリのファイル名を選択します。ディレクトリをコピーまたはカットするには、コピーまたはカットするディレクトリの横にあるボタンを選択し、ステップ 8 に進みます。
6. コピーまたはカットするファイルの横にあるボタンを選択します。
7. [アクション] メニューで [コピー] または [カット] を選択します。
8. [ファイルシステム] ビューで、ファイルを貼り付けるディレクトリの横にあるボタンを選択します。
9. [アクション] メニューで [ペースト] を選択します。

Fleet Manager を使用して OS ファイルとディレクトリの名前を変更する

Fleet Manager を使用して、アカウントのマネージドノード上のファイルとディレクトリの名前を変更できます。

Fleet Manager でファイルまたはディレクトリの名前を変更するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. 名前を変更するファイルまたはディレクトリが含まれるマネージドノードのリンクを選択します。
4. [ツール]、[ファイルシステム] を選択します。
5. ファイルの名前を変更するには、名前を変更するファイルが含まれているディレクトリの [ファイル名] を選択します。ディレクトリの名前を変更するには、名前を変更するディレクトリの横にあるボタンを選択し、ステップ 8 に進みます。
6. 名前を変更するファイルの横にあるボタンを選択します。
7. [アクション]、[名前を変更] を選択します。
8. [ファイル名] フィールドにファイルの新しい名前を入力し、[名前を変更] を選択します。

Fleet Manager を使用して OS ファイルとディレクトリを削除する

Fleet Manager を使用して、アカウントのマネージドノード上のファイルとディレクトリを削除できます。

Fleet Manager を使用してファイルまたはディレクトリを削除するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. 削除するファイルまたはディレクトリが含まれるマネージドノードのリンクを選択します。
4. [ツール]、[ファイルシステム] を選択します。
5. ファイルのを削除するには、削除するファイルが含まれているディレクトリの [ファイル名] を選択します。ディレクトリを削除するには、削除するディレクトリの横にあるボタンを選択し、ステップ 7 に進みます。
6. 削除するコンテンツが含まれるファイルの横にあるボタンを選択します。
7. [アクション]、[削除] を選択します。

Fleet Manager を使用して OS ディレクトリを作成する

Fleet Manager を使用して、アカウントのマネージドノードにディレクトリを作成できます。

Fleet Manager を使用してディレクトリを作成するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. ディレクトリを作成するマネージドノードのリンクを選択します。
4. [ツール]、[ファイルシステム] を選択します。
5. 新しいディレクトリを作成するディレクトリの [ファイル名] を選択します。
6. [ディレクトリを作成] を選択します。
7. [ディレクトリ名] フィールドに新しいディレクトリの名前を入力し、[ディレクトリを作成] を選択します。

Fleet Manager を使用して OS ディレクトリの切り取り、コピー、貼り付けを行う

Fleet Manager を使用して、アカウントのマネージドノード上のディレクトリの切り取り、コピー、貼り付けを行うことができます。

Fleet Manager でファイルまたはディレクトリをコピーまたはカットアンドペーストするには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. コピー、切り取りまたは貼り付けするファイルが含まれるマネージドノードのリンクを選択します。
4. [ツール]、[ファイルシステム] を選択します。
5. コピーまたは切り取りを行うディレクトリの横にあるボタンを選択し、ステップ 8 に進みます。
6. [アクション] メニューで [コピー] または [カット] を選択します。
7. [ファイルシステム] ビューで、ファイルを貼り付けるディレクトリの横にあるボタンを選択します。
8. [アクション] メニューで [ペースト] を選択します。

マネージドノードのパフォーマンスの監視

AWS Systems Manager のツールである Fleet Manager を使用すると、マネージドノードに関するパフォーマンスデータをリアルタイムで表示できます。パフォーマンスデータは、パフォーマンスカウンターから取得されます。

Fleet Managerでは、以下のパフォーマンスカウンターを使用できます。

- CPU 使用率
- ディスク入出力 (I/O) 使用率
- ネットワークトラフィック
- メモリ使用量

> **Note**
>
> Fleet Manager は AWS Systems Manager のツールである Session Manager を使用してパフォーマンスデータを取得します。Amazon Elastic Compute Cloud (Amazon EC2) インスタンスの場合、マネージドインスタンスにアタッチされたインスタンスプロファイルは、Session Manager がこの機能を使用する許可を提供する必要があります。インスタンスプロファイルへのSession Managerアクセス許可の追加に関する詳細については、「既存の IAM ロールに Session Manager 許可を追加する」を参照してください。

Fleet Managerでパフォーマンスデータを表示する

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. パフォーマンスを監視するマネージドノードの横にあるボタンを選択します。
4. [詳細を表示] を選択します。
5. [ツール]、[パフォーマンスカウンター] を選択します。

プロセスの操作

AWS Systems Manager のツールである Fleet Manager を使用してマネージドインスタンス上のプロセスを操作します。Fleet Manager では、プロセスに関する情報を表示できます。たとえば、プロセ

スの CPU 使用率とメモリ使用率について、そのハンドルとスレッドとともに確認できます。Fleet Manager では、コンソールからプロセスを開始および終了できます。

> **Note**
>
> Fleet Manager は AWS Systems Manager のツールである Session Manager を使用してプロセスデータを取得します。Amazon Elastic Compute Cloud (Amazon EC2) インスタンスの場合、マネージドインスタンスにアタッチされたインスタンスプロファイルは、Session Manager がこの機能を使用する許可を提供する必要があります。インスタンスプロファイルへのSession Managerアクセス許可の追加に関する詳細については、「既存の IAM ロールに Session Manager 許可を追加する」を参照してください。

トピック

- Fleet Manager を使用して OS プロセスの詳細を表示する
- Fleet Manager を使用してマネージドノードで OS プロセスを開始する
- Fleet Manager を使用して OS プロセスを終了する

Fleet Manager を使用して OS プロセスの詳細を表示する

Fleet Manager ビューを使用してマネージドノードのプロセスに関する詳細を表示できます。

Fleet Manager を使用してプロセスに関する詳細を表示するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. プロセスを表示するノードのリンクを選択します。
4. [ツール]、[プロセス] を選択します。

Fleet Manager を使用してマネージドノードで OS プロセスを開始する

Fleet Manager を使用して、マネージドノードでプロセスを開始できます。

Fleet Manager でプロセスを開始するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. プロセスを開始するマネージドノードのリンクを選択します。
4. [ツール]、[プロセス] を選択します。
5. [Start new process] (新しいプロセスを開始) を選択します。
6. [プロセス名または完全なパス] フィールドに、プロセスの名前または実行可能ファイルへの完全なパスを入力します。
7. (オプション) [作業ディレクトリ] フィールドに、プロセスを実行するディレクトリパスを入力します。

Fleet Manager を使用して OS プロセスを終了する

Fleet Manager を使用して OS プロセスを終了するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. プロセスを開始するマネージドノードのリンクを選択します。
4. [ツール]、[プロセス] を選択します。
5. 終了するプロセスの横にあるボタンを選択します。
6. [アクション]、[プロセスの終了] または [アクション]、[プロセスツリーの終了] のいずれかを選択します。

> **Note**
>
> プロセスツリーを終了すると、そのプロセスを使用するすべてのプロセスとアプリケーションも終了します。

マネージドノードのログを表示する

AWS Systems Manager のツールである Fleet Manager を使用すると、マネージドノードに格納されているログデータを表示できます。Windows マネージドノードの場合は、Windows イベントログを

表示して、コンソールから詳細をコピーできます。イベントを検索しやすくするために、Windows イベントログを [Event level] (イベントレベル)、[Event ID] (イベント ID)、[Event source] (イベントソース)、および [Time created] (作成時刻) でフィルタリングします。ファイルシステムを表示する手順を使用して、他のログデータを表示することもできます。Fleet Managerでのファイルシステムの表示に関する詳細については、「Fleet Manager を使用して OS ファイルシステムを操作する」を参照してください。

Fleet Manager で Windows イベントログを表示する

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. イベントログを表示するマネージドノードの横にあるボタンを選択します。
4. [詳細を表示] を選択します。
5. [ツール]、[Windows イベントログ] を選択します。
6. 表示するイベントが含まれた [Log name] (ログ名) を選択します。
7. 表示する [Log name] (ログ名) の横にあるボタンを選択し、[View events] (イベントを表示) をクリックします。
8. 表示するイベントの横にあるボタンを選択して、[View event details] (イベント詳細を表示) をクリックします。
9. (オプション) [Copy as JSON] (JSONとしてコピー) をクリックして、イベントの詳細をクリップボードにコピーします。

Fleet Manager を使用してマネージドノード上の OS ユーザーアカウントとグループを管理する

AWS Systems Manager のツールである Fleet Manager を使用して、マネージドノード上のオペレーティングシステム (OS) のユーザーアカウントとグループを管理できます。例えば、ユーザーとグループを作成および削除できます。さらに、グループメンバーシップ、ユーザーロール、およびステータスなどの詳細も表示できます。

> **Important**
>
> Fleet Manager は、さまざまなユーザー管理のオペレーションのために、AWS Systems Manager のツールである Run Command と Session Manager を使用します。その結果、ユーザーは、通常はアクセス許可を付与できないオペレーティングシステムのユーザーアカウントにアクセス許可を付与することができます。これは、AWS Systems Manager Agent

(SSM Agent) が Amazon Elastic Compute Cloud (Amazon EC2) インスタンス上でルートアクセス許可 (Linux) またはシステムアクセス許可 (Windows サーバー) を使用して実行されるためです。SSM Agent 経由でのルートレベルのコマンドへのアクセスの制限に関する詳細については、「SSM Agent を介してルートレベルコマンドへのアクセスを制限する」を参照してください。この機能へのアクセスを制限するには、定義したアクションのみへのアクセスを許可する AWS Identity and Access Management (IAM) ポリシーをユーザー用に作成することをお勧めします。Fleet Manager の IAM ポリシー作成の詳細については、「Fleet Manager へのアクセスのコントロール」を参照してください。

トピック

- Fleet Manager を使用して OS ユーザーまたはグループを作成する
- Fleet Manager を使用してユーザーまたはグループのメンバーシップを更新する
- Fleet Manager を使用して OS ユーザーまたはグループを削除する

Fleet Manager を使用して OS ユーザーまたはグループを作成する

> **Note**
>
> Fleet Managerは、新規ユーザーのパスワードの設定にSession Managerを使用します。Amazon EC2 インスタンスの場合、マネージドノードにアタッチされたインスタンスプロファイルは、Session Manager がこの機能を使用する許可を提供する必要があります。インスタンスプロファイルへのSession Managerアクセス許可の追加に関する詳細については、「既存の IAM ロールに Session Manager 許可を追加する」を参照してください。

サーバーに直接ログオンしてユーザーアカウントまたはグループを作成する代わりに、Fleet Manager コンソールを使用して同じタスクを実行できます。

Fleet Manager を使用して OS ユーザーアカウントを作成するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. 新しいユーザーを作成するマネージドノードの横にあるボタンを選択します。
4. [詳細を表示] を選択します。

5. [ツール]、[ユーザーとグループ] を選択します。
6. [Users] (ユーザー) タブを選択してから、[Create user] (ユーザーを作成) をクリックします。
7. 新しいユーザーの [Name] (名前) に値を入力します。
8. (推奨) [Set password] (パスワードを設定) の横にあるチェックボックスをオンにします。手順の最後に、新しいユーザーのパスワードを入力を求められます。
9. [Create user] (ユーザーを作成) をクリックします。新しいユーザーのパスワードを作成するチェックボックスをオンにした場合は、パスワードの値を入力して [Done] (完了) をクリックするように求められます。指定するパスワードが、マネージドノードのローカルポリシーまたはドメインポリシーで指定された要件を満たしていない場合は、エラーが返されます。

Fleet Manager を使用して OS グループを作成するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. グループを作成するマネージドノードの横にあるボタンを選択します。
4. [詳細を表示] を選択します。
5. [ツール]、[ユーザーとグループ] を選択します。
6. [グループ] タブを選択してから、[グループの作成] を選択します。
7. 新しいグループの [Name] (名前) に値を入力します。
8. (オプション) 新しいグループの [Description] (説明) に値を入力します。
9. (オプション) 新しいグループの [Group members] (グループメンバー) に追加するユーザーを選択します。
10. [Create group] (グループを作成) を選択します。

Fleet Manager を使用してユーザーまたはグループのメンバーシップを更新する

サーバーに直接ログオンしてユーザーアカウントまたはグループを更新する代わりに、Fleet Manager コンソールを使用して同じタスクを実行できます。

Fleet Manager を使用して OS ユーザーアカウントを新しいグループに追加するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。

2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. 更新するユーザーアカウントが存在するマネージドノードの横にあるボタンを選択します。
4. [詳細を表示] を選択します。
5. [ツール]、[ユーザーとグループ] を選択します。
6. [Users] (ユーザー) タブを選択します。
7. 更新するユーザーの横にあるボタンを選択します。
8. [アクション]、[ユーザーをグループに追加] を選択します。
9. [Add to group] (グループに追加) で、ユーザーを追加するグループを選択します。
10. [Add user to group] (ユーザーをグループに追加) を選択します。

Fleet Manager を使用して OS グループのメンバーシップを編集するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. 更新するグループが存在するマネージドノードの横にあるボタンを選択します。
4. [詳細を表示] を選択します。
5. [ツール]、[ユーザーとグループ] を選択します。
6. [Groups] (グループ) タブを選択します。
7. 更新するグループの横にあるボタンを選択します。
8. [アクション]、[グループを変更] を選択します。
9. [Group members] (グループメンバー) で、追加または削除するユーザーを選択します。
10. [Modify group] (グループを変更) をクリックします。

Fleet Manager を使用して OS ユーザーまたはグループを削除する

サーバーに直接ログオンしてユーザーアカウントまたはグループを削除する代わりに、Fleet Manager コンソールを使用して同じタスクを実行できます。

Fleet Manager を使用して OS ユーザーアカウントを削除するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。

2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. 削除するユーザーアカウントが存在するマネージドノードの横にあるボタンを選択します。
4. [詳細を表示] を選択します。
5. [ユーザーとグループ] を選択します。
6. [Users] (ユーザー) タブを選択します。
7. 削除するユーザーの横にあるボタンを選択します。
8. [アクション]、[ローカルユーザーの削除] を選択します。

Fleet Manager を使用して OS グループを削除するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. 削除するグループが存在するマネージドノードの横にあるボタンを選択します。
4. [詳細を表示] を選択します。
5. [ツール]、[ユーザーとグループ] を選択します。
6. [Group] (グループ) タブを選択します。
7. 更新するグループの横にあるボタンを選択します。
8. [アクション]、[ローカルグループを削除] を選択します。

マネージドノードでの Windows レジストリの管理

AWS Systems Manager のツールである Fleet Manager を使用すると、Windows Server マネージドノード上のレジストリを管理できます。Fleet Managerコンソールからは、レジストリのエントリと値を作成、コピー、更新、および削除することが可能です。

> **Important**
>
> レジストリを変更する前に、レジストリのバックアップを作成する、またはマネージドノードにアタッチされたルート Amazon Elastic Block Store (Amazon EBS) ボリュームのスナップショットを作成することをお勧めします。レジストリを誤って変更すると、深刻な問題が発生する可能性があります。これらの問題には、オペレーティングシステムの再インストール、またはスナップショットからのノードのルートボリュームの復元が必要になる場合があります。AWS は、これらの問題が解決できることを保証しません。レジストリの変更は自

己責任で行ってください。すべてのレジストリ変更、およびバックアップの確保はユーザーの責任となります。

Windows レジストリキーまたはエントリの作成

Fleet Managerで Windows レジストリキーを作成する

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. レジストリキーを作成するマネージドノードの横にあるボタンを選択します。
4. [詳細を表示] を選択します。
5. [ツール]、[Windows レジストリ] を選択します。
6. [Registry name] (レジストリ名) を選択して、新しいレジストリキーを作成するハイブを選択します。
7. [作成]、[レジストリキーの作成] を選択します。
8. 新しいキーを作成するレジストリエントリの横にあるボタンを選択します。
9. [Create registry key] (レジストリキーを作成) をクリックします。
10. 新しいレジストリキーの [Name] (名前) に値を入力し、[Submit] (送信) をクリックします。

Fleet Managerで Windows レジストリエントリを作成する

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. レジストリエントリを作成するインスタンスの横にあるボタンを選択します。
4. [View details] を選択します。
5. [ツール]、[Windows レジストリ] を選択します。
6. [Registry name] (レジストリ名) を選択してハイブを選択してから、新しいレジストリキーを作成するレジストリキーを選択します。
7. [作成]、[レジストリエントリの作成] を選択します。
8. 新しいレジストリエントリの [Name] (名前) に値を入力します。

9. レジストリエントリに対して作成する値の [Type] (種類) を選択します。レジストリ値の種類の詳細については、Registry value types を参照してください。
10. 新しいレジストリエントリの [Value] (値) に値を入力します。

Windows レジストリエントリを更新する

Fleet Managerで Windows レジストリエントリを更新する

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. レジストリエントリを更新するマネージドノードの横にあるボタンを選択します。
4. [詳細を表示] を選択します。
5. [ツール]、[Windows レジストリ] を選択します。
6. [Registry name] (レジストリ名) を選択してハイブを選択してから、更新するレジストリキーを選択します。
7. 更新するレジストリエントリの横にあるボタンを選択します。
8. [アクション]、[レジストリエントリの更新] を選択します。
9. 新しいレジストリエントリの [Value] (値) に新しい値を入力します。
10. [Update (更新)] を選択します。

Windows レジストリのエントリまたはキーの削除

Fleet Managerで Windows レジストリキーを削除する

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. レジストリキーを削除するマネージドノードの横にあるボタンを選択します。
4. [ツール]、[Windows レジストリ] を選択します。
5. [Registry name] (レジストリ名) を選択してハイブを選択してから、削除するレジストリキーを選択します。
6. 削除するレジストリキーの横にあるボタンを選択します。
7. [アクション]、[レジストリキーの削除] を選択します。

Fleet Managerで Windows レジストリエントリを削除する

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. レジストリエントリを削除するマネージドノードの横にあるボタンを選択します。
4. [詳細を表示] を選択します。
5. [ツール]、[Windows レジストリ] を選択します。
6. [Registry name] (レジストリ名) を選択してハイブを選択してから、削除するエントリが含まれるレジストリキーを選択します。
7. 削除するレジストリエントリの横にあるボタンを選択します。
8. [アクション]、[レジストリエントリの削除] を選択します。

Default Host Management Configuration を使用した EC2 インスタンスの自動管理

デフォルトのホスト管理設定では、AWS Systems Manager が Amazon EC2 インスタンスをマネージドインスタンスとして自動的に管理できます。マネージドインスタンスとは、Systems Manager で使用するために設定された EC2 インスタンスです。

Systems Manager を使用してインスタンスを管理することには、次のような利点があります。

- Session Manager を使用して安全に EC2 インスタンスに接続する。
- Patch Manager を使用して自動パッチスキャンを実行する。
- Systems Manager インベントリを使用して、インスタンスに関する詳細情報を表示する。
- Fleet Manager を使用してインスタンスを追跡、管理する。
- SSM Agent を自動的に最新の状態に保つ。

Fleet Manager、Inventory、Patch Manager、Session Manager は Systems Manager のツールです。

デフォルトのホスト管理設定を使用し、AWS Identity and Access Management (IAM) インスタンスプロファイルを手動で作成しなくても EC2 インスタンスを管理できます。代わりに、デフォルトのホスト管理設定では、デフォルトの IAM ロールを作成して適用し、Systems Manager がアクティブ化された AWS アカウント と AWS リージョン 内のすべてのインスタンスを管理できるアクセス許可を Systems Manager に付与します。

付与されたアクセス許可がユースケースに十分でない場合は、デフォルトのホスト管理設定で作成されたデフォルトの IAM ロールにポリシーを追加することもできます。また、デフォルトの IAM ロールで提供されるすべての機能の一部に対してのみアクセス許可が必要な場合は、独自のカスタムロールとポリシーを作成できます。デフォルトのホスト管理設定で選択した IAM ロールに加えられた変更は、リージョンとアカウントのすべてのマネージド Amazon EC2 インスタンスに適用されます。

デフォルトのホスト管理設定で使用するポリシーの詳細については、「AWS マネージドポリシー: AmazonSSMManagedEC2InstanceDefaultPolicy」を参照してください。

最小特権アクセスの実装

トピックの手順は、管理者のみが実行することを想定しています。したがって、管理者以外のユーザーがデフォルトのホスト管理設定を設定または変更できないように、最小特権アクセスを実装することをお勧めします。デフォルトのホスト管理設定へのアクセスを制限するポリシーの例を確認するには、このトピックの後半の「デフォルトのホスト管理設定の最小特権ポリシーの例」を参照してください。

> **Important**
>
> デフォルトのホスト管理設定を使用して登録されたインスタンスの登録情報は、`var/lib/amazon/ssm` または `C:\ProgramData\Amazon` ディレクトリにローカルに保存されます。これらのディレクトリやファイルを削除すると、インスタンスはデフォルトのホスト管理設定を使用して Systems Manager に接続するために必要な認証情報を取得できなくなります。このような場合は、IAM インスタンスプロファイルを使用してインスタンスに必要なアクセス許可を付与するか、インスタンスを再作成する必要があります。

トピック

- 前提条件
- デフォルトのホスト管理設定の有効化
- デフォルトのホスト管理設定の無効化
- デフォルトのホスト管理設定の最小特権ポリシーの例

前提条件

この設定を有効化した AWS リージョン および AWS アカウント で、デフォルトのホスト管理設定を使用するには、次の要件を満たす必要があります。

- 管理対象となるインスタンスには、インスタンスメタデータサービスのバージョン 2 (IMDSv2) を使用する必要があります。

  デフォルトのホスト管理設定は、インスタンスメタデータサービスバージョン 1 をサポートしていません。IMDSv2 への移行の詳細については、「Amazon EC2 ユーザーガイド」の「インスタンスメタデータサービスバージョン 2 の使用への移行」を参照してください。
- メソッドを使用するには、SSM Agent バージョン 3.2.582.0 以降がインスタンスにインストールされている必要があります。

  インスタンスにインストールされている SSM Agent のバージョンを確認する方法については、「SSM Agent バージョン番号の確認」を参照してください。

  SSM Agent の更新方法については、「SSM Agent の自動更新」を参照してください。
- このトピックのタスクを実行する管理者には、GetServiceSetting、ResetServiceSetting、UpdateServiceSetting API オペレーションのアクセス許可が必要です。さらに、`AWSSystemsManagerDefaultEC2InstanceManagementRole` IAM ロールの `iam:PassRole` アクセス許可を付与する権限が必要です。上記のアクセス許可を付与するポリシーの例を次に示します。各*##############*をユーザー自身の情報に置き換えます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:GetServiceSetting",
                "ssm:ResetServiceSetting",
                "ssm:UpdateServiceSetting"
            ],
            "Resource": "arn:aws:ssm:region:account-id:servicesetting/ssm/managed-
instance/default-ec2-instance-management-role"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "arn:aws:iam::account-id:role/service-role/
AWSSystemsManagerDefaultEC2InstanceManagementRole",
            "Condition": {
```

```
                "StringEquals": {
                    "iam:PassedToService": [
                        "ssm.amazonaws.com"
                    ]
                }
            }
        }
    ]
}
```

- Systems Manager を使用して管理される Amazon EC2 インスタンスに IAM インスタンスプロファイルがすでにアタッチされている場合は、`ssm:UpdateInstanceInformation` 操作を実行するためのアクセス許可をすべて削除します。SSM Agent は、デフォルトのホスト管理設定のアクセス許可を使用する前に、インスタンスプロファイルのアクセス許可の使用を試みます。独自の IAM インスタンスプロファイルで `ssm:UpdateInstanceInformation` オペレーションを許可すると、インスタンスはデフォルトのホスト管理設定のアクセス許可を使用しません。

デフォルトのホスト管理設定の有効化

デフォルトのホスト管理設定は、Fleet Manager コンソールから、または AWS Command Line Interface や AWS Tools for Windows PowerShell を使用して有効化できます。

Amazon EC2 インスタンスをこの設定で管理したい各リージョンに対して、デフォルトのホスト管理設定を 1 つずつオンにする必要があります。

デフォルトのホスト管理設定をオンにした後、以下の手順のステップ 5 で選択したロールの認証情報をインスタンスが使用できるようになるまでに 30 分かかる場合があります。

デフォルトのホスト管理設定を有効化するには (コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. [アカウント管理]、[デフォルトのホスト管理設定を構成] を選択します。
4. [デフォルトのホスト管理設定を有効にする] をオンにします。
5. インスタンスの Systems Manager ツールを有効にするために使用する AWS Identity and Access Management (IAM) ロールを選択します。デフォルトのホスト管理設定で提供されるデフォルトのロールを使用することをお勧めします。このロールには、Systems Manager を使用して Amazon EC2 インスタンスを管理するために必要となる最小限のアクセス許可のセッ

トが含まれています。カスタムロールを使用する場合は、ロールの信頼ポリシーで Systems Manager を信頼できるエンティティとして許可する必要があります。

6. [設定] をクリックして、セットアップを完了します。

デフォルトのホスト管理設定を有効化するには (コマンドライン)

1. ローカルマシンで、次の信頼関係ポリシーを含む JSON ファイルを作成します。

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Sid":"",
            "Effect":"Allow",
            "Principal":{
                "Service":"ssm.amazonaws.com"
            },
            "Action":"sts:AssumeRole"
        }
    ]
}
```

2. AWS CLI または Tools for Windows PowerShell を開き、次のコマンドのいずれかを使用してアカウントにサービスロールを作成します。使用するコマンドはローカルマシンのオペレーティングシステムにより異なります。各*##############*をユーザー自身の情報に置き換えます。

   Linux & macOS

```
aws iam create-role \
--role-name AWSSystemsManagerDefaultEC2InstanceManagementRole \
--path /service-role/ \
--assume-role-policy-document file://trust-policy.json
```

   Windows

```
aws iam create-role ^
--role-name AWSSystemsManagerDefaultEC2InstanceManagementRole ^
--path /service-role/ ^
--assume-role-policy-document file://trust-policy.json
```

PowerShell

```
New-IAMRole `
-RoleName "AWSSystemsManagerDefaultEC2InstanceManagementRole" `
-Path "/service-role/" `
-AssumeRolePolicyDocument "file://trust-policy.json"
```

3. 次のコマンドを実行して、新たに作成したロールに AmazonSSMManagedEC2InstanceDefaultPolicy マネージドポリシーをアタッチします。各##############をユーザー自身の情報に置き換えます。

   Linux & macOS

   ```
   aws iam attach-role-policy \
   --policy-arn arn:aws:iam::aws:policy/AmazonSSMManagedEC2InstanceDefaultPolicy \
   --role-name AWSSystemsManagerDefaultEC2InstanceManagementRole
   ```

   Windows

   ```
   aws iam attach-role-policy ^
   --policy-arn arn:aws:iam::aws:policy/AmazonSSMManagedEC2InstanceDefaultPolicy ^
   --role-name AWSSystemsManagerDefaultEC2InstanceManagementRole
   ```

   PowerShell

   ```
   Register-IAMRolePolicy `
   -PolicyArn "arn:aws:iam::aws:policy/AmazonSSMManagedEC2InstanceDefaultPolicy" `
   -RoleName "AWSSystemsManagerDefaultEC2InstanceManagementRole"
   ```

4. AWS CLI または Tools for Windows PowerShell を開き、次のコマンドを実行します。各##########をユーザー自身の情報に置き換えます。

   Linux & macOS

   ```
   aws ssm update-service-setting \
   --setting-id arn:aws:ssm:region:account-id:servicesetting/ssm/managed-instance/
   default-ec2-instance-management-role \
   --setting-value service-role/AWSSystemsManagerDefaultEC2InstanceManagementRole
   ```

Windows

```
aws ssm update-service-setting ^
--setting-id arn:aws:ssm:region:account-id:servicesetting/ssm/managed-instance/
default-ec2-instance-management-role ^
--setting-value service-role/AWSSystemsManagerDefaultEC2InstanceManagementRole
```

PowerShell

```
Update-SSMServiceSetting `
-SettingId "arn:aws:ssm:region:account-id:servicesetting/ssm/managed-instance/
default-ec2-instance-management-role" `
-SettingValue "service-role/AWSSystemsManagerDefaultEC2InstanceManagementRole"
```

コマンドが成功した場合、出力はありません。

5. 次のコマンドを実行して、現在の AWS アカウント および AWS リージョン におけるデフォルトのホスト管理設定の現在のサービス設定が表示されます。

Linux & macOS

```
aws ssm get-service-setting \
--setting-id arn:aws:ssm:region:account-id:servicesetting/ssm/managed-instance/
default-ec2-instance-management-role
```

Windows

```
aws ssm get-service-setting ^
--setting-id arn:aws:ssm:region:account-id:servicesetting/ssm/managed-instance/
default-ec2-instance-management-role
```

PowerShell

```
Get-SSMServiceSetting `
-SettingId "arn:aws:ssm:region:account-id:servicesetting/ssm/managed-instance/
default-ec2-instance-management-role"
```

このコマンドによって以下のような情報が返されます。

```
{
    "ServiceSetting": {
        "SettingId": "/ssm/managed-instance/default-ec2-instance-management-role",
        "SettingValue": "service-role/
AWSSystemsManagerDefaultEC2InstanceManagementRole",
        "LastModifiedDate": "2022-11-28T08:21:03.576000-08:00",
        "LastModifiedUser": "System",
        "ARN": "arn:aws:ssm:us-east-2:-123456789012:servicesetting/ssm/managed-
instance/default-ec2-instance-management-role",
        "Status": "Custom"
    }
}
```

デフォルトのホスト管理設定の無効化

デフォルトのホスト管理設定は、Fleet Manager コンソールから、または AWS Command Line Interface や AWS Tools for Windows PowerShell を使用して無効化できます。

Amazon EC2 インスタンスをこの設定で管理する必要がなくなった各リージョンに対して、デフォルトのホスト管理設定を 1 つずつオフにする必要があります。あるリージョンで無効化しても、すべてのリージョンで無効化されるわけではありません。

デフォルトのホスト管理設定を無効化し、Amazon EC2 インスタンスに Systems Manager へのアクセスを許可するためのインスタンスプロファイルを添付していない場合、それらのインスタンスは Systems Manager によって管理されなくなります。

デフォルトのホスト管理設定を無効化するには (コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. [アカウント管理]、[デフォルトのホスト管理設定] を選択します。
4. [デフォルトのホスト管理設定を有効にする] をオフにします。
5. [設定] をクリックして、デフォルトのホスト管理設定を無効にします。

デフォルトのホスト管理設定を無効化するには (コマンドライン)

- AWS CLI または Tools for Windows PowerShell を開き、次のコマンドを実行します。各*##########*をユーザー自身の情報に置き換えます。

  Linux & macOS

  ```
  aws ssm reset-service-setting \
  --setting-id arn:aws:ssm:region:account-id:servicesetting/ssm/managed-instance/
  default-ec2-instance-management-role
  ```

  Windows

  ```
  aws ssm reset-service-setting ^
  --setting-id arn:aws:ssm:region:account-id:servicesetting/ssm/managed-instance/
  default-ec2-instance-management-role
  ```

  PowerShell

  ```
  Reset-SSMServiceSetting `
  -SettingId "arn:aws:ssm:region:account-id:servicesetting/ssm/managed-instance/
  default-ec2-instance-management-role"
  ```

デフォルトのホスト管理設定の最小特権ポリシーの例

以下のサンプルポリシーは、組織のメンバーが組織のアカウントで、デフォルトのホスト管理設定を変更できないようにする方法を示しています。

AWS Organizations のサービスコントロールポリシー

以下のポリシーは、AWS Organizations の管理者以外のメンバーがデフォルトのホスト管理設定を更新できないようにする方法を示しています。各*##############*をユーザー自身の情報に置き換えます。

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Deny",
            "Action": [
                "ssm:UpdateServiceSetting",
```

```
                "ssm:ResetServiceSetting"
            ],
            "Resource": "arn:aws:ssm:*:*:servicesetting/ssm/managed-instance/default-
ec2-instance-management-role",
            "Condition": {
                "StringNotEqualsIgnoreCase": {
                    "aws:PrincipalTag/job-function": [
                        "administrator"
                    ]
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "arn:aws:iam::*:role/service-role/
AWSSystemsManagerDefaultEC2InstanceManagementRole",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "ssm.amazonaws.com"
                },
                "StringNotEqualsIgnoreCase": {
                    "aws:PrincipalTag/job-function": [
                        "administrator"
                    ]
                }
            }
        },
        {
            "Effect": "Deny",
            "Resource": "arn:aws:iam::*:role/service-role/
AWSSystemsManagerDefaultEC2InstanceManagementRole",
            "Action": [
                "iam:AttachRolePolicy",
                "iam:DeleteRole"
            ],
            "Condition": {
                "StringNotEqualsIgnoreCase": {
                    "aws:PrincipalTag/job-function": [
                        "administrator"
                    ]
                }
```

```
            }
        }
    ]
}
```

IAM プリンシパルのポリシー

以下のポリシーは、AWS Organizations の IAM グループ、ロール、またはユーザーがデフォルトのホスト管理設定を更新できないようにする方法を示しています。各##############をユーザー自身の情報に置き換えます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ssm:UpdateServiceSetting",
                "ssm:ResetServiceSetting"
            ],
            "Resource": "arn:aws:ssm:region:account-id:servicesetting/ssm/managed-
instance/default-ec2-instance-management-role"
        },
        {
            "Effect": "Deny",
            "Action": [
                "iam:AttachRolePolicy",
                "iam:DeleteRole",
                "iam:PassRole"
            ],
            "Resource": "arn:aws:iam::account-id:role/service-role/
AWSSystemsManagerDefaultEC2InstanceManagementRole"
        }
    ]
}
```

Remote Desktop を使用して Windows Server マネージドインスタンスに接続する

AWS Systems Manager のツール Fleet Manager を使用することで、Remote Desktop Protocol (RDP) を使用した Windows Server Amazon Elastic Compute Cloud (Amazon EC2) インスタンスに接続できます。Fleet ManagerAmazon DCV を利用したリモートデスクトップでは、Systems

Manager コンソールから直接 Windows Server インスタンスに安全に接続できます。1 つのブラウザウィンドウで最大 4 つまで同時に接続できます。

現在、リモートデスクトップは、Windows Server 2012 RTM 以降を実行しているインスタンスのみで使用できます。リモートデスクトップは言語入力として英語のみをサポートしています。

Fleet Manager リモートデスクトップはコンソール専用サービスで、マネージドインスタンスへのコマンドライン接続はサポートしていません。シェルを介して Windows Server マネージドインスタンスに接続するには、AWS Systems Manager の別のツールである Session Manager を使用できます。詳細については、「AWS Systems Manager Session Manager」を参照してください。

> **Note**
>
> RDP 接続の時間は、AWS Identity and Access Management (IAM) 認証情報の継続時間によって決定されません。代わりに、最大接続時間またはアイドル時間の制限のいずれかが満たされるまで、接続は持続します。詳細については、「リモート接続時間と同時実行」を参照してください。

インスタンスが Systems Manager とやり取りできるように AWS Identity and Access Management (IAM) アクセス許可を設定する方法については、「Systems Manager にインスタンスのアクセス許可を設定する」を参照してください。

トピック

- 環境のセットアップ
- リモートデスクトップの IAM 許可の設定
- リモートデスクトップ接続の認証
- リモート接続時間と同時実行
- リモートデスクトップを使用してマネージドノードへ接続する
- 現在および完了した接続に関する情報の表示

環境のセットアップ

リモートデスクトップを使用する前に、環境が以下の要件を満たしていることを確認します。

- マネージドノードの設定

Amazon EC2 インスタンスが Systems Manager のマネージドノードとして設定されていることを確認してください。

- SSM Agent の最小バージョン

  ノードが SSM Agent バージョン 3.0.222.0 以降を実行していることを確認します。ノードで実行されているエージェントのバージョンの確認についての詳細は、「SSM Agent バージョン番号の確認」を参照してください。SSM Agent のインストールまたは更新については、「「SSM Agent」 の使用」を参照してください。

- RDP ポート設定

  リモート接続を受け入れるには、Windows Server ノード上の Remote Desktop Services サービスがデフォルトの RDP ポート 3389 を使用する必要があります。これは、AWS によって提供される Amazon Machine Images (AMIs) のデフォルト設定です。リモートデスクトップを使用するためにインバウンドポートを開く必要は明示的にありません。

- キーボード機能用 PSReadLine モジュールバージョン

  PowerShell でキーボードが正しく機能することを確認するには、Windows Server 2022 を実行しているノードに PSReadLine モジュールバージョン 2.2.2 以降がインストールされていることを確認してください。古いバージョンを使用している場合は、以下のコマンドを使用して、必要なバージョンをインストールできます。

  ```
  Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force
  ```

  NuGet パッケージプロバイダーがインストールされたら、次のコマンドを実行します。

  ```
  Install-Module `
   -Name PSReadLine `
   -Repository PSGallery `
   -MinimumVersion 2.2.2 -Force
  ```

- Session Manager の設定

  リモートデスクトップを使用する前に、Session Manager のセットアップの前提条件を完了する必要があります。リモートデスクトップを使用してインスタンスに接続すると、AWS アカウントおよび AWS リージョン に定義されているすべてのセッション設定が適用されます。詳細については、「Session Manager を設定する」を参照してください。

> **Note**
>
> Amazon Simple Storage Service (Amazon S3) を使用して、Session Manager アクティビティをログに記録すると、リモートデスクトップ接続によって bucket_name/Port/stderr で次のエラーが発生します。このエラーは正常な動作であり、無視してもかまいません。
>
> ```
> Setting up data channel with id SESSION_ID failed: failed to create websocket
>  for datachannel with error: CreateDataChannel failed with no output or
>  error: createDataChannel request failed: unexpected response from the service
>  <BadRequest>
> <ClientErrorMessage>Session is already terminated</ClientErrorMessage>
> </BadRequest>
> ```

リモートデスクトップの IAM 許可の設定

Systems Manager と Session Manager に必要な IAM アクセス許可に加えて、使用するユーザーまたはロールには、接続を開始するためのアクセス許可が必要です。

接続を開始するためのアクセス許可

コンソールで EC2 インスタンスへの RDP 接続を作成するには、次のアクセス許可が必要です。

- `ssm-guiconnect:CancelConnection`
- `ssm-guiconnect:GetConnection`
- `ssm-guiconnect:StartConnection`

接続を一覧表示するためのアクセス許可

コンソールで接続の一覧を表示するには、次のアクセス許可が必要です。

`ssm-guiconnect:ListConnections`

以下は、リモートデスクトップとのさまざまなタイプの対話を許可するためにユーザーまたはロールにアタッチできる IAM ポリシーの例です。各##############をユーザー自身の情報に置き換えます。

EC2 インスタンスに接続するための標準ポリシー

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EC2",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:GetPasswordData"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SSM",
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeInstanceProperties",
                "ssm:GetCommandInvocation",
                "ssm:GetInventorySchema"
            ],
            "Resource": "*"
        },
        {
            "Sid": "TerminateSession",
            "Effect": "Allow",
            "Action": [
                "ssm:TerminateSession"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "ssm:resourceTag/aws:ssmmessages:session-id": [
                        "${aws:userid}"
                    ]
                }
            }
        },
        {
            "Sid": "SSMStartSession",
            "Effect": "Allow",
            "Action": [
                "ssm:StartSession"
```

```
            ],
            "Resource": [
                "arn:aws:ec2:*:account-id:instance/*",
                "arn:aws:ssm:*:account-id:managed-instance/*",
                "arn:aws:ssm:*::document/AWS-StartPortForwardingSession"
            ],
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:CalledVia": "ssm-guiconnect.amazonaws.com"
                }
            }
        },
        {
            "Sid": "GuiConnect",
            "Effect": "Allow",
            "Action": [
                "ssm-guiconnect:CancelConnection",
                "ssm-guiconnect:GetConnection",
                "ssm-guiconnect:StartConnection",
                "ssm-guiconnect:ListConnections"
            ],
            "Resource": "*"
        }
    ]
}
```

特定のタグを持つ EC2 インスタンスへの接続に関するポリシー

> **Note**
>
> 次の IAM ポリシーでは、SSMStartSession セクションで ssm:StartSession アクションの Amazon リソースネーム (ARN) が必要になります。図に示すように、指定した ARN には AWS アカウント ID は必要ありません。アカウント ID を指定すると、Fleet Manager は AccessDeniedException を返します。
> ポリシーの例の下部にある AccessTaggedInstances セクションでは ssm:StartSession の ARN も必要です。これらの ARN には AWS アカウント ID を指定します。

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

```
    "Statement": [
        {
            "Sid": "EC2",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:GetPasswordData"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SSM",
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeInstanceProperties",
                "ssm:GetCommandInvocation",
                "ssm:GetInventorySchema"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SSMStartSession",
            "Effect": "Allow",
            "Action": [
                "ssm:StartSession"
            ],
            "Resource": [
                "arn:aws:ssm:*::document/AWS-StartPortForwardingSession"
            ],
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:CalledVia": "ssm-guiconnect.amazonaws.com"
                }
            }
        },
        {
            "Sid": "AccessTaggedInstances",
            "Effect": "Allow",
            "Action": [
                "ssm:StartSession"
            ],
            "Resource": [
                "arn:aws:ec2:*:account-id:instance/*",
                "arn:aws:ssm:*:account-id:managed-instance/*"
```

```
            ],
            "Condition": {
                "StringLike": {
                    "ssm:resourceTag/tag key": [
                        "tag value"
                    ]
                }
            }
        },
        {
            "Sid": "GuiConnect",
            "Effect": "Allow",
            "Action": [
                "ssm-guiconnect:CancelConnection",
                "ssm-guiconnect:GetConnection",
                "ssm-guiconnect:StartConnection",
                "ssm-guiconnect:ListConnections"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS IAM Identity Center ユーザーが EC2 インスタンスに接続するためのポリシー

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SSO",
            "Effect": "Allow",
            "Action": [
                "sso:ListDirectoryAssociations*",
                "identitystore:DescribeUser"
            ],
            "Resource": "*"
        },
        {
            "Sid": "EC2",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:GetPasswordData"
```

```
            ],
            "Resource": "*"
        },
        {
            "Sid": "SSM",
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeInstanceInformation",
                "ssm:DescribeInstanceProperties",
                "ssm:GetCommandInvocation",
                "ssm:GetInventorySchema"
            ],
            "Resource": "*"
        },
        {
            "Sid": "TerminateSession",
            "Effect": "Allow",
            "Action": [
                "ssm:TerminateSession"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "ssm:resourceTag/aws:ssmmessages:session-id": [
                        "${aws:userName}"
                    ]
                }
            }
        },
        {
            "Sid": "SSMStartSession",
            "Effect": "Allow",
            "Action": [
                "ssm:StartSession"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ssm:*:*:managed-instance/*",
                "arn:aws:ssm:*:*:document/AWS-StartPortForwardingSession"
            ],
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:CalledVia": "ssm-guiconnect.amazonaws.com"
                }
```

```
            }
        },
        {
            "Sid": "SSMSendCommand",
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ssm:*:*:managed-instance/*",
                "arn:aws:ssm:*:*:document/AWSSSO-CreateSSOUser"
            ]
        },
        {
            "Sid": "GuiConnect",
            "Effect": "Allow",
            "Action": [
                "ssm-guiconnect:CancelConnection",
                "ssm-guiconnect:GetConnection",
                "ssm-guiconnect:StartConnection",
                "ssm-guiconnect:ListConnections"
            ],
            "Resource": "*"
        }
    ]
}
```

リモートデスクトップ接続の認証

リモート接続を確立するときは、Windows 認証情報、またはインスタンスに関連付けられている Amazon EC2 キーペア (.pem ファイル) を使用して、認証を行えます。キーペアの詳細については、「Amazon EC2 ユーザーガイド」の「Amazon EC2 キーペアおよび Windows インスタンス」を参照してください。

または、AWS IAM Identity Center を使用して AWS Management Console に認証されている場合は、追加の認証情報を指定せずにインスタンスに接続できます。IAM アイデンティティセンターを使用したリモート接続認証を許可するポリシーの例については、「リモートデスクトップの IAM 許可の設定」を参照してください。

[開始する前に]

リモートデスクトップを使用して接続を開始する前に、IAM Identity Center 認証を使用する際には、以下の条件に注意してください。

- リモートデスクトップは、IAM アイデンティティセンターを有効にしたのと同じ AWS リージョンのノードの IAM アイデンティティセンター認証をサポートします。
- リモートデスクトップは、最大 16 文字の IAM アイデンティティセンターのユーザー名をサポートします。
- リモートデスクトップは、英数字と特殊文字 . - _ で構成される IAM アイデンティティセンターユーザー名をサポートします。

> **Important**
>
> + = , の文字が含まれる IAM アイデンティティセンターユーザー名では、接続が失敗します。
> IAM アイデンティティセンターはユーザー名でこれらの文字をサポートしていますが、Fleet Manager RDP 接続ではサポートされていません。
> さらに、IAM アイデンティティセンターユーザー名に 1 つ、または複数の @ 記号が含まれている場合、Fleet Manager は、@ が E メールアドレスのドメイン部分の先頭に使用されているかどうかにかかわらず、最初の @ 記号とその後に続くすべての文字を無視します。例えば、`diego_ramirez@example.com` という IAM アイデンティティセンターユーザー名の場合は `@example.com` 部分が無視され、Fleet Manager のユーザー名は `diego_ramirez` になります。`diego_r@mirez@example.com` の場合は、Fleet Manager が `@mirez@example.com` を無視し、Fleet Manager のユーザー名は `diego_r` になります。

- IAM アイデンティティセンターを使用して接続を認証すると、Windows リモートデスクトップはインスタンスのローカル管理者グループにローカルユーザーを作成します。このユーザーは、リモート接続が終了した後も存続します。
- リモートデスクトップでは、Microsoft Active Directory ドメインコントローラーであるノードの IAM アイデンティティセンターの認証は許可されません。
- リモートデスクトップでは、Active Directory ドメインに参加しているノードに IAM アイデンティティセンターの認証を使用できますが、お勧めしません。この認証方法ではユーザーに管理者許可を付与しますが、ドメインによって付与されるより制限の厳しい許可よりも優先される可能性があります。

IAM Identity Center 認証のサポート対象リージョン

IAM Identity Center 認証を使用する Remote Desktop 接続は、次の AWS リージョン でサポートされています。

- 米国東部 (オハイオ) (us-east-2)
- 米国東部 (バージニア北部) (us-east-1)
- 米国西部 (北カリフォルニア) (us-west-1)
- 米国西部 (オレゴン) (us-west-2)
- アフリカ (ケープタウン) (af-south-1)
- アジアパシフィック (香港) (ap-east-1)
- アジアパシフィック (ムンバイ) (ap-south-1)
- アジアパシフィック (東京) (ap-northeast-1)
- アジアパシフィック (ソウル) (ap-northeast-2)
- アジアパシフィック (大阪) (ap-northeast-3)
- アジアパシフィック (シンガポール) (ap-southeast-1)
- アジアパシフィック (シドニー) (ap-southeast-2)
- アジアパシフィック (ジャカルタ) (ap-southeast-3)
- カナダ (中部) (ca-central-1)
- ヨーロッパ (フランクフルト) (eu-central-1)
- 欧州 (ストックホルム) (eu-north-1)
- 欧州 (アイルランド) (eu-west-1)
- ヨーロッパ (ロンドン) (eu-west-2)
- 欧州 (パリ) (eu-west-3)
- イスラエル (テルアビブ) (il-central-1)
- 南米 (サンパウロ) (sa-east-1)
- 欧州 (ミラノ) (eu-south-1)
- 中東 (バーレーン) (me-south-1)
- AWS GovCloud (米国東部) (us-gov-east-1)
- AWS GovCloud (米国西部) (us-gov-west-1)

リモート接続時間と同時実行

アクティブなリモートデスクトップ接続には、次の条件が適用されます。

- 接続時間

  デフォルトでは、リモートデスクトップ接続は 60 分後に切断されます。接続が切断されないようにするには、切断される前に [セッションを更新] を選択して、継続時間タイマーをリセットできます。

- 接続タイムアウト

  リモートデスクトップ接続は、10 分以上アイドル状態になると切断されます。

- 接続の持続性

  リモートデスクトップを使用して Windows Server に接続すると、最大接続時間 (60 分) またはアイドルタイムアウト制限 (10 分) に達するまで接続が維持されます。接続時間は、AWS Identity and Access Management (IAM) 認証情報の継続時間によって決定されません。接続時間の制限が満たされない場合、IAM 認証情報の有効期限が切れても接続は維持されます。リモートデスクトップを使用する場合は、IAM 認証情報の有効期限が切れたら、ブラウザページを離れて接続を終了する必要があります。

- 同時接続

  デフォルトでは、同じ AWS アカウント と AWS リージョン で最大 5 つのアクティブなリモートデスクトップ接続を設定できます。最大 25 の同時接続のサービスクォータの引き上げをリクエストするには、「Service Quotas ユーザーガイド」の「クォータ引き上げのリクエスト」を参照してください。

> **Note**
>
> Windows Server の標準ライセンスでは、2 つの同時 RDP 接続が許可されます。さらに多くの接続をサポートするには、Microsoft から追加のクライアントアクセスライセンス (CAL) を購入するか、AWS から Microsoft リモートデスクトップサービスライセンスを購入する必要があります。追加ライセンスの詳細については、次のトピックを参照してください。
>
> - Microsoft ウェブサイトの「Client Access Licenses and Management Licenses」
> - 「License Manager ユーザーガイド」の「Use License Manager user-based subscriptions for supported software products」

リモートデスクトップを使用してマネージドノードへ接続する

ブラウザによるテキストのコピー/貼り付けサポート

Google Chrome と Microsoft Edge ブラウザを使用すると、マネージドノードからローカルマシンに、および、ローカルマシンから接続しているマネージドノードに、テキストをコピーして貼り付けることができます。

Mozilla Firefox ブラウザでは、マネージドノードからローカルマシンにのみテキストをコピーして貼り付けることができます。ローカルマシンからマネージドノードへのコピーはサポートされていません。

Fleet Manager リモートデスクトップを使用してマネージドノードに接続するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. 接続するノードを選択します。チェックボックスまたはノード名を選択できます。
4. [ノードアクション] メニューで、[リモートデスクトップとの接続] を選択します。
5. 必要な [Authentication type] (認証タイプ) を選択します。[ユーザー認証情報] を選択した場合は、接続するノード上の Windows ユーザーアカウントのユーザー名とパスワードを入力します。[キーペア] を選択した場合は、次のいずれかの方法を使用して認証を行うことができます。

   a. インスタンスに関連付けられた PEM キーをローカルファイルシステムから選択する場合は、[ローカルマシンを検索] を選択します。

      - または -

   b. PEM ファイルの内容をコピーして指定されたフィールドに貼り付ける場合は、[キーペアの内容を貼り付け] を選択します。
6. [Connect] (接続) を選択します。
7. 希望のディスプレイ解像度を選択するには、[アクション] メニューで [レゾリューション] を選択し、次の中から選択します。

   - 自動的に適応
   - 1920 x 1080
   - 1400 x 900
   - 1366 x 768
   - 800 x 600

   [自動的に適応] オプションは検出された画面サイズに基づいて最適な解像度を決定します。

現在および完了した接続に関する情報の表示

Systems Manager コンソールの [Fleet Manager] セクションを使用して、アカウントで作成された RDP 接続に関する情報を表示できます。フィルターのセットを使用して、表示される接続のリストを時間範囲、特定のインスタンス、接続を作成したユーザー、特定のステータスの接続に制限することができます。コンソールには、現在アクティブなすべての接続と過去のすべての接続に関する情報を示すタブも用意されています。

現在の接続と完了した接続に関する情報を表示するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. [アカウント] > [リモートデスクトップ (RDP) との接続] の順に選択します。
4. 次のいずれかのタブを選択します。
   - アクティブな接続
   - 接続履歴
5. 表示される接続結果のリストをさらに絞り込むには、検索 ( ) ボックスに 1 つまたは複数のフィルターを指定します。フリーテキスト検索用語を入力することもできます。

マネージドインスタンスの Amazon EBS ボリュームの管理

Amazon Elastic Block Store (Amazon EBS) は、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスで使用するブロックレベルストレージのボリュームを提供します。EBS ボリュームの動作は、未初期化のブロックデバイスに似ています。これらのボリュームは、デバイスとしてインスタンスにマウントできます。

マネージドインスタンス上の Amazon EBS ボリュームを、AWS Systems Manager のツールである Fleet Manager を使って管理できます。例えば、EBS ボリュームを初期化し、パーティションをフォーマットして、ボリュームをマウントして使用できるようにする、といったことが行えます。

> **Note**
>
> Fleet Manager は現在、Windows Server インスタンスの Amazon EBS ボリューム管理のみをサポートしています。

EBS ボリュームの詳細を表示する

Fleet Manager で EBS ボリュームの詳細を表示するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. EBS ボリュームの詳細を表示しようとしているマネージドインスタンスの横にあるボタンを選択します。
4. [詳細を表示] を選択します。
5. [ツール]、[EBS ボリューム] を選択します。
6. EBS ボリュームの詳細を表示するには、[ボリューム ID] 列でその ID を選択します。

EBS ボリュームの初期化とフォーマット

Fleet Manager を使って EBS ボリュームを初期化しフォーマットするには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. EBS ボリュームを初期化、フォーマット、マウントしようとしているマネージドインスタンスの横にあるボタンを選択します。EBS ボリュームを初期化できるのは、そのディスクが空である場合のみです。
4. [詳細を表示] を選択します。
5. [ツール] メニューで [EBS ボリューム] を選択します。
6. 初期化し、フォーマットしようとしている EBS ボリュームの横にあるボタンを選択します。
7. [初期化とフォーマット] を選択します。
8. [パーティションスタイル] で、EBS ボリュームに使用するパーティションスタイルを選択します。

9. (オプション) パーティションのドライブレターを選択します。
10. (オプション) パーティションを識別するパーティション名を入力します。
11. パーティションに保存されているファイルやデータの整理に使用するファイルシステムを選択します。
12. EBS ボリュームを使用可能にするには [確認] を選択します。確認後、パーティションの設定は、AWS Management Consoleからは変更できませんが、SSH または RDP を使用してインスタンスにログインして変更することはできます。

Red Hat ナレッジベースポータルへのアクセス

Red Hat ユーザーの場合は、AWS Systems Manager のツールである Fleet Manager を使用して、ナレッジベースポータルにアクセスできます。Red Hat Enterprise Linux(RHEL) インスタンスを実行しているか、AWS で RHEL サービスを使用している場合に Red Hat ユーザーとみなされます。ナレッジベースポータルには、バイナリ、コミュニティサポートのためのナレッジシェアやディスカッションフォーラムなどがあり、これらはRed Hat ライセンスを保有するお客様のみが利用可能になっています。

必要となる Systems Manager および Fleet Manager の AWS Identity and Access Management (IAM) アクセス許可に加えて、コンソールへのアクセスに使用するユーザーまたはロールには、ナレッジポータルにアクセスできるように `rhelkb:GetRhelURL` アクションも許可する必要があります。

Red Hat ナレッジベースポータルにアクセスするには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. Red Hat ナレッジベースポータルへの接続に使用する RHEL インスタンスを選択します。
4. [アカウント管理] で [Red Hat ナレッジベースへアクセス] を選択し、Red Hat ナレッジベースのページを開きます。

AWS 上の RHEL を使用して完全にサポートされた RHEL ワークロードを実行している場合、AWS 認証情報を使用して Red Hat のウェブサイトから Red Hat ナレッジベースにアクセスすることもできます。

マネージドノードの可用性のトラブルシューティング

Run Command、Distributor、Session Manager などのいくつかの AWS Systems Manager ツールでは、オペレーションを実行するマネージドノードを手動で選択することもできます。このような場合、手動でノードを選択するように指定すると、オペレーションを実行できるマネージドノードのリストが表示されます。

このトピックでは、実行中であることを確認したマネージドノードが、Systems Manager のマネージドノードのリストに含まれていない理由の診断に役立つ情報を提供します。

ノードを Systems Manager で管理し、マネージドノードのリストに表示されるようにするには、次の 3 つの主な要件を満たす必要があります。

- SSM Agent が、サポートされているオペレーティングシステムのノードにインストールされ、実行されている必要があります。

  > **Note**
  >
  > 一部の AWS マネージド Amazon Machine Images (AMIs) は、SSM Agent がプリインストールされたインスタンスを起動するように設定されています。(カスタムの AMI を設定して SSM Agent をプリインストールすることもできます。) 詳細については、「SSM Agent がプリインストールされている AMIs を見つける」を参照してください。

- Amazon Elastic Compute Cloud (Amazon EC2) インスタンスの場合は、AWS Identity and Access Management (IAM) インスタンスプロファイルを、インスタンスにアタッチする必要があります。インスタンスプロファイルにより、インスタンスが Systems Manager サービスと通信できるようになります。インスタンスにインスタンスプロファイルを割り当てない場合は、ハイブリッドアクティベーションを使用して登録しますが、通常はその必要はありません。
- SSM Agent は、それ自体をサービスに登録するために、Systems Manager エンドポイントに接続できる必要があります。そのうえで、マネージドノードがサービスで使用可能である必要があります。これは、サービスが 5 分ごとに信号を送信してインスタンスの正常性をチェックすることによって確認されます。
- マネージドノードのステータスが `Connection Lost` のまま 30 日以上経過すると、そのノードは Fleet Manager コンソールに表示されなくなる場合があります。リストに再度表示するには、接続が失われた原因となった問題を解決する必要があります。

マネージドノードが実行されていることを確認したら、次のコマンドを使用して、SSM Agent で Systems Manager サービスへの登録が正常に完了したかどうかを確認できます。このコマンドは、登録が正常に完了するまで結果を返しません。

Linux & macOS

```
aws ssm describe-instance-associations-status \
    --instance-id instance-id
```

Windows

```
aws ssm describe-instance-associations-status ^
    --instance-id instance-id
```

PowerShell

```
Get-SSMInstanceAssociationsStatus `
    -InstanceId instance-id
```

登録が正常に完了し、マネージドノードが Systems Manager のオペレーションで使用可能になっている場合、コマンドでは次のような結果が返されます。

```
{
    "InstanceAssociationStatusInfos": [
        {
            "AssociationId": "fa262de1-6150-4a90-8f53-d7eb5EXAMPLE",
            "Name": "AWS-GatherSoftwareInventory",
            "DocumentVersion": "1",
            "AssociationVersion": "1",
            "InstanceId": "i-02573cafcfEXAMPLE",
            "Status": "Pending",
            "DetailedStatus": "Associated"
        },
        {
            "AssociationId": "f9ec7a0f-6104-4273-8975-82e34EXAMPLE",
            "Name": "AWS-RunPatchBaseline",
            "DocumentVersion": "1",
            "AssociationVersion": "1",
            "InstanceId": "i-02573cafcfEXAMPLE",
            "Status": "Queued",
```

```
            "AssociationName": "SystemAssociationForScanningPatches"
        }
    ]
}
```

登録がまだ完了していないか失敗した場合、このコマンドは次のような結果を返します。

```
{
    "InstanceAssociationStatusInfos": []
}
```

5 分ほど経ってもコマンドから結果が返されない場合は、以下の情報を使用してマネージドノードの問題のトラブルシューティングを行ってください。

トピック

- 解決策 1: SSM Agent がマネージドノードにインストールされ、実行されていることを確認する
- 解決策 2: インスタンスに IAM インスタンスプロファイルが指定されていることを確認する (EC2 インスタンスのみ)
- 解決策 3: サービスエンドポイントへの接続を確認する
- 解決策 4: 対象のオペレーティングシステムのサポートを確認する
- 解決策 5: Amazon EC2 インスタンスと同じ AWS リージョン で作業していることを確認する
- 解決策 6: マネージドノードで SSM Agent に適用したプロキシ設定を確認する
- 解決策 7: マネージドインスタンスに TLS 証明書をインストールする
- ssm-cli を使用したマネージドノードの可用性のトラブルシューティング

解決策 1: SSM Agent がマネージドノードにインストールされ、実行されていることを確認する

SSM Agent の最新バージョンがマネージドノードにインストールされ、実行されていることを確認します。

SSM Agent がマネージドノードにインストールされ、実行されていることを確認するには、「SSM Agent ステータスの確認とエージェントの起動」を参照してください。

SSM Agent をマネージドノードにインストールまたは再インストールするには、以下のトピックを参照してください。

- Linux 用 EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする

- ハイブリッド Linux ノードで SSM Agent をインストールする方法
- Windows Server 用の EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする
- ハイブリッド Windows ノードで SSM Agent をインストールする方法

解決策 2: インスタンスに IAM インスタンスプロファイルが指定されていることを確認する (EC2 インスタンスのみ)

Amazon Elastic Compute Cloud (Amazon EC2) インスタンスの場合、そのインスタンスに Systems Manager API の通信を許可する AWS Identity and Access Management (IAM) インスタンスプロファイルが設定されていることを確認します。また、ユーザーに Systems Manager API と通信できる IAM ユーザー信頼ポリシーがあることを確認します。

> **Note**
>
> オンプレミスサーバー、エッジデバイス、仮想マシン (VM) が、インスタンスプロファイルの代わりに IAM サービスロールを使用します。詳細については、「ハイブリッドおよびマルチクラウド環境で Systems Manager に必要な IAM サービスロールを作成する」を参照してください。

必要なアクセス権限を持つインスタンスプロファイルが EC2 インスタンスにアタッチされているかどうかを確認するには

1. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
2. ナビゲーションペインで、[インスタンス] を選択します。
3. インスタンスプロファイルを確認するインスタンスを選択します。
4. 下部のペインの [Description (説明)] タブで、[IAM role (IAM ロール)] を見つけ、ロールの名前を選択します。
5. インスタンスプロファイルのロールの [Summary (概要)] ページの [Permissions (アクセス許可)] タブで、[Permissions policies (アクセス許可ポリシー)] に `AmazonSSMManagedInstanceCore` があることを確認します。

   代わりにカスタムポリシーを使用する場合は、`AmazonSSMManagedInstanceCore` と同じアクセス許可があることを確認してください。

AmazonSSMManagedInstanceCore をコンソールで開く

Systems Manager のインスタンスプロファイルにアタッチできるその他のポリシーの詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」を参照してください。

解決策 3: サービスエンドポイントへの接続を確認する

インスタンスに Systems Manager サービスエンドポイントへの接続があることを確認します。この接続は、Systems Manager の VPC エンドポイントを作成して設定するか、サービスエンドポイントへの HTTPS (ポート 443) アウトバウンドトラフィックを許可することによって提供されます。

Amazon EC2 インスタンスでは、仮想プライベートクラウド (VPC) 設定でアウトバウンドトラフィックが許可されている場合、AWS リージョン の Systems Manager サービスエンドポイントがインスタンスの登録に使用されます。ただし、インスタンスが起動された VPC 設定でアウトバウンドトラフィックが許可されず、パブリックサービスエンドポイントへの接続を許可するようにこの設定を変更できない場合は、代わりに VPC のインターフェイスエンドポイントを設定する必要があります。

詳細については、「Systems Manager のために VPC エンドポイントを使用して EC2 インスタンスのセキュリティを強化する」を参照してください。

解決策 4: 対象のオペレーティングシステムのサポートを確認する

選択したオペレーションが、リストに表示されるはずのマネージドノードのタイプで実行できることを確認します。Systems Manager の一部のオペレーションは、Windows インスタンスのみ、または Linux インスタンスのみを対象にすることができます。例えば、Systems Manager (SSM) の `AWS-InstallPowerShellModule` ドキュメントと `AWS-ConfigureCloudWatch` ドキュメントは Windows インスタンスでのみ実行できます。[Run a command (コマンドの実行)] ページでこれらのドキュメントのいずれかを選択して [Choose instances manually (手動でインスタンスを選択する)] を選択すると、Windows インスタンスのみが表示され、選択できるようになります。

解決策 5: Amazon EC2 インスタンスと同じ AWS リージョン で作業していることを確認する

Amazon EC2 インスタンスは、米国東部 (オハイオ) リージョン (us-east-2) や欧州 (アイルランド) リージョン (eu-west-1) など、特定の AWS リージョン で作成および使用できます。使用する Amazon EC2 インスタンスと同じ AWS リージョン で作業していることを確認します。詳細については、AWS Management Console の開始方法のリージョンの選択を参照してください。

解決策 6: マネージドノードで SSM Agent に適用したプロキシ設定を確認する

マネージドノードで SSM Agent に適用したプロキシ設定が正しいことを確認します。プロキシ設定が正しくない場合、ノードは必要なサービスエンドポイントに接続できなくなるか、Systems Manager がマネージドノードのオペレーティングシステムを誤って識別する可能性があります。詳細については、Linux ノードでプロキシを使用するための SSM Agent の設定およびSSM Agent が Windows Server インスタンス用にプロキシを使用するように設定するを参照してください。

解決策 7: マネージドインスタンスに TLS 証明書をインストールする

Transport Layer Security (TLS) 証明書は、AWS Systems Manager で使用する各マネージドインスタンスにインストールする必要があります。AWS のサービスでは、これらの証明書を使用して、他の AWS のサービスへの呼び出しを暗号化します。

TLS 証明書は、Amazon Machine Image (AMI) から作成された各 Amazon EC2 インスタンスにデフォルトでインストールされています。最新のオペレーティングシステムには、信頼ストアに Amazon Trust Services CA からの必要な TLS 証明書が含まれています。

必要な証明書がインスタンスにインストールされているかどうかを確認するには、インスタンスのオペレーティングシステムに基づいて次のコマンドを実行します。URL の*#####*部分は、マネージドインスタンスがある AWS リージョン に必ず置き換えてください。

Linux & macOS

```
curl -L https://ssm.region.amazonaws.com
```

Windows

```
Invoke-WebRequest -Uri https://ssm.region.amazonaws.com
```

コマンドが `UnknownOperationException` エラーを返すはずです。SSL/TLS エラーメッセージが表示される場合は、必要な証明書がインストールされていない可能性があります。

必要な Amazon Trust Services CA の証明書が、基本オペレーティングシステム、Amazon で提供されていない AMIs から作成されたインスタンス、または独自のオンプレミスサーバーおよび VM にインストールされていない場合は、Amazon Trust Services から証明書をインストールして有効にする必要があります。または、AWS Certificate Manager (ACM) を使用して、サポートされている統合サービスの証明書を作成および管理します。

各マネージドインスタンスには、次の Transport Layer Security (TLS) 証明書のいずれかがインストールされている必要があります。

- Amazon Root CA 1
- Starfield Services Root Certificate Authority - G2
- Starfield Class 2 Certificate Authority

ACM の使用については、AWS Certificate Manager ユーザーガイドを参照してください。

コンピューティング環境にある証明書がグループポリシーオブジェクト (GPO) によって管理される場合は、場合により、これらの証明書のいずれかを含めるグループポリシーを設定する必要があります。

Amazon Root および Starfield 証明書の詳細については、ブログ記事「独自の認証機関への AWS の移行の準備方法」を参照してください。

`ssm-cli` を使用したマネージドノードの可用性のトラブルシューティング

`ssm-cli` は SSM Agent のインストールに含まれるスタンドアロンのコマンドラインツールです。SSM Agent 3.1.501.0 以降をマシンにインストールすると、そのマシンで `ssm-cli` コマンドを実行できます。これらのコマンドの出力は、マシンが Amazon EC2 インスタンスまたは AWS Systems Manager で管理される (したがって Systems Manager のマネージドノードのリストに追加される) EC2 以外のマシンの最小要件を満たすかどうかを判断するのに役立ちます。(SSM Agent バージョン 3.1.501.0 は 2021 年 11 月にリリースされました)。

最小要件

Amazon EC2 インスタンスまたは EC2 以外のマシンを AWS Systems Manager で管理し、マネージドノードのリストに表示されるようにするには、次の 3 つの主な要件を満たす必要があります。

- SSM Agent は、サポートされているオペレーティングシステムを搭載したマシンにインストールして実行する必要があります。

  一部の EC2 向けの AWS マネージド Amazon Machine Images (AMIs) は、SSM Agent がプリインストールされたインスタンスを起動するように設定されています。(カスタムの AMI を設定して SSM Agent をプリインストールすることもできます。) 詳細については、「SSM Agent がプリインストールされている AMIs を見つける」を参照してください。

- Systems Manager サービスとの通信に必要な許可を提供する AWS Identity and Access Management (IAM) インスタンスプロファイル (EC2 インスタンスの場合) または IAM サービスロール (EC2 以外のマシンの場合) をマシンにアタッチする必要があります。
- SSM Agent は、それ自体をサービスに登録するために、Systems Manager エンドポイントに接続できる必要があります。そのうえで、マネージドノードがサービスで使用可能である必要があります。これは、サービスが 5 分ごとに信号を送信してマネージドノードの正常性をチェックすることによって確認されます。

ssm-cli に事前設定されているコマンド

実行中であることを確認したマシンが Systems Manager のマネージドノードのリストに含まれていない理由を診断するために必要な情報を収集する、事前設定済みのコマンドが含まれています。`get-diagnostics` オプションを指定したときにこれらのコマンドが実行されます。

マシンで、マネージドノードの可用性のトラブルシューティングに `ssm-cli` を使用するには、次のコマンドを実行します。

Linux & macOS

```
ssm-cli get-diagnostics --output table
```

Windows

Windows Server マシンでは、コマンドを実行する前に `C:\Program Files\Amazon\SSM` ディレクトリに移動する必要があります。

```
ssm-cli.exe get-diagnostics --output table
```

PowerShell

Windows Server マシンでは、コマンドを実行する前に `C:\Program Files\Amazon\SSM` ディレクトリに移動する必要があります。

```
.\ssm-cli.exe get-diagnostics --output table
```

このコマンドにより、次のような出力がテーブルとして返されます。

> **Note**
>
> ssmmessages、s3、kms、logs、および monitoring エンドポイントへの接続チェックは、Amazon Simple Storage Service (Amazon S3) や Amazon CloudWatch Logs へのログ記録、および AWS Key Management Service (AWS KMS) による暗号化の使用が可能な Session Manager などの追加オプション機能に対するものです。

Linux & macOS

```
[root@instance]# ssm-cli get-diagnostics --output table
##############################################################################################
# Check                                  # Status  # Note
                                        #
##############################################################################################
# EC2 IMDS                               # Success # IMDS is accessible and has
 instance id i-0123456789abcdefa in Region  #
#                                       #         # us-east-2
                                        #
##############################################################################################
# Hybrid instance registration           # Skipped # Instance does not have hybrid
 registration                            #
##############################################################################################
# Connectivity to ssm endpoint           # Success # ssm.us-east-2.amazonaws.com is
 reachable                              #
##############################################################################################
# Connectivity to ec2messages endpoint  # Success # ec2messages.us-
east-2.amazonaws.com is reachable                    #
##############################################################################################
# Connectivity to ssmmessages endpoint  # Success # ssmmessages.us-
east-2.amazonaws.com is reachable                    #
##############################################################################################
# Connectivity to s3 endpoint            # Success # s3.us-east-2.amazonaws.com is
 reachable                               #
##############################################################################################
# Connectivity to kms endpoint           # Success # kms.us-east-2.amazonaws.com is
 reachable                              #
##############################################################################################
# Connectivity to logs endpoint          # Success # logs.us-east-2.amazonaws.com is
 reachable                             #
##############################################################################################
```

```
# Connectivity to monitoring endpoint   # Success # monitoring.us-
east-2.amazonaws.com is reachable                      #
##############################################################################
# AWS Credentials                       # Success # Credentials are for
                                      #
#                                       #         #
 arn:aws:sts::123456789012:assumed-role/Fullaccess/i-0123456789abcdefa #
#                                       #         # and will expire at 2021-08-17
 18:47:49 +0000 UTC                     #
##############################################################################
# Agent service                         # Success # Agent service is running and is
 running as expected user              #
##############################################################################
# Proxy configuration                   # Skipped # No proxy configuration detected
                                      #
##############################################################################
# SSM Agent version                     # Success # SSM Agent version is 3.0.1209.0,
 latest available agent version is    #
#                                       #         # 3.1.192.0
                                      #
##############################################################################
```

Windows Server and PowerShell

```
PS C:\Program Files\Amazon\SSM> .\ssm-cli.exe get-diagnostics --output table
##############################################################################
# Check                                 # Status  # Note
                                    #
##############################################################################
# EC2 IMDS                              # Success # IMDS is accessible and has
 instance id i-0123456789EXAMPLE in       #
#                                       #         # Region us-east-2
                                    #
##############################################################################
# Hybrid instance registration          # Skipped # Instance does not have hybrid
 registration                          #
##############################################################################
# Connectivity to ssm endpoint          # Success # ssm.us-east-2.amazonaws.com is
 reachable                            #
##############################################################################
# Connectivity to ec2messages endpoint  # Success # ec2messages.us-
east-2.amazonaws.com is reachable                    #
##############################################################################
```

```
# Connectivity to ssmmessages endpoint  # Success # ssmmessages.us-
east-2.amazonaws.com is reachable                    #
#############################################################################################
# Connectivity to s3 endpoint           # Success # s3.us-east-2.amazonaws.com is
 reachable                              #
#############################################################################################
# Connectivity to kms endpoint          # Success # kms.us-east-2.amazonaws.com is
 reachable                             #
#############################################################################################
# Connectivity to logs endpoint         # Success # logs.us-east-2.amazonaws.com is
 reachable                            #
#############################################################################################
# Connectivity to monitoring endpoint   # Success # monitoring.us-
east-2.amazonaws.com is reachable                     #
#############################################################################################
# AWS Credentials                       # Success # Credentials are for
                                      #
#                                       #         #
 arn:aws:sts::123456789012:assumed-role/SSM-Role/i-123abc45EXAMPLE  #
#                                       #         #  and will expire at 2021-09-02
 13:24:42 +0000 UTC                    #
#############################################################################################
# Agent service                         # Success # Agent service is running and is
 running as expected user             #
#############################################################################################
# Proxy configuration                   # Skipped # No proxy configuration detected
                                     #
#############################################################################################
# Windows sysprep image state           # Success # Windows image state value is at
 desired value IMAGE_STATE_COMPLETE  #
#############################################################################################
# SSM Agent version                     # Success # SSM Agent version is 3.2.815.0,
 latest agent version in us-east-2   #
#                                       #         # is 3.2.985.0
                                     #
#############################################################################################
```

次の表に、ssm-cli によって実行される各チェックの詳細を示します。

ssm-cli 診断チェック

チェック	詳細
Amazon EC2 インスタンスのメタデータサービス	マネージドノードがメタデータサービスに到達できるかどうかを示します。テストの失敗は、`http://169.254.169.254` への接続に問題があることを示しています。これはローカルルート、プロキシ、またはオペレーティングシステム (OS) のファイアウォールとプロキシの構成によって発生している可能性があります。
ハイブリッドインスタンスの登録	SSM Agent がハイブリッドアクティベーションを使用して登録されているかどうかを示します。
`ssm` エンドポイントへの接続	ノードが TCP ポート 443 で Systems Manager のサービスエンドポイントに到達できるかどうかを示します。テストが失敗した場合は、ノードがある AWS リージョン に応じて `https://ssm.` *region* `.amazonaws.com` への接続に問題があることを示します。接続の問題は、セキュリティグループ、ネットワークアクセスコントロールリスト、ルートテーブル、OS ファイアウォールおよびプロキシなどの VPC 設定によって引き起こされている可能性があります。
`ec2messages` エンドポイントへの接続	ノードが TCP ポート 443 で Systems Manager のサービスエンドポイントに到達できるかどうかを示します。テストが失敗した場合は、ノードがある AWS リージョン に応じて `https://ec2messages.` *region* `.amazonaws.com` への接続に問題があることを示します。接続の問題は、セキュリティグループ、ネットワークアクセスコントロールリスト、ルートテーブル、OS ファイアウォールおよび

チェック	詳細
	プロキシなどの VPC 設定によって引き起こされている可能性があります。
ssmmessages エンドポイントへの接続	ノードが TCP ポート 443 で Systems Manager のサービスエンドポイントに到達できるかどうかを示します。テストが失敗した場合は、ノードがある AWS リージョン に応じて https://ssmmessages. *region*.amazonaws.com への接続に問題があることを示します。接続の問題は、セキュリティグループ、ネットワークアクセスコントロールリスト、ルートテーブル、OS ファイアウォールおよびプロキシなどの VPC 設定によって引き起こされている可能性があります。
s3 エンドポイントへの接続	ノードが TCP ポート 443 で Amazon Simple Storage Service のサービスエンドポイントに到達できるかどうかを示します。テストが失敗した場合は、ノードがある AWS リージョン に応じて https://s3. *region*.amazonaws.com への接続に問題があることを示します。ノードをマネージドノードリストに表示するのに、このエンドポイントに接続する必要はありません。
kms エンドポイントへの接続	ノードが TCP ポート 443 で AWS Key Management Service のサービスエンドポイントに到達できるかどうかを示します。テストが失敗した場合は、ノードがある AWS リージョン に応じて https://kms. *region*.amazonaws.com への接続に問題があることを示します。ノードをマネージドノードリストに表示するのに、このエンドポイントに接続する必要はありません。

チェック	詳細
logs エンドポイントへの接続	ノードが TCP ポート 443 で Amazon CloudWatch Logs のサービスエンドポイントに到達できるかどうかを示します。テストが失敗した場合は、ノードがある AWS リージョン に応じて https://logs. *region*.amazonaws.com への接続に問題があることを示します。ノードをマネージドノードリストに表示するのに、このエンドポイントに接続する必要はありません。
monitoring エンドポイントへの接続	ノードが TCP ポート 443 で Amazon CloudWatch のサービスエンドポイントに到達できるかどうかを示します。テストが失敗した場合は、ノードがある AWS リージョン に応じて https://monitoring. *region*.amazonaws.com への接続に問題があることを示します。ノードをマネージドノードリストに表示するのに、このエンドポイントに接続する必要はありません。
AWS 認証情報	マシンにアタッチされている IAM インスタンスプロファイル (EC2 インスタンスの場合) または IAM サービスロール (EC2 以外のマシンの場合) に基づいて、SSM Agent に必要な認証情報があるかどうかを示します。テストに失敗した場合、IAM インスタンスプロファイルまたは IAM サービスロールがマシンにアタッチされていないか、Systems Manager に必要な許可が含まれていないことを示します。

チェック	詳細
エージェントサービス	SSM Agent サービスが実行されているかどうか、およびサービスが Linux もしくは macOS のルートとして、または Windows Server の SYSTEM として実行されているかどうかを示します。テストに失敗した場合、SSM Agent サービスが実行されていないか、ルートまたは SYSTEM として実行されていないことを示します。
プロキシ設定	SSM Agent がプロキシを使用するように設定されているかどうかを示します。
Sysprep イメージの状態 (Windows のみ)	ノード上の Sysprep の状態を示します。Sysprep 状態が IMAGE_STATE_COMPLETE 以外の値の場合、SSM Agent はノード上で起動しません。
SSM Agent バージョン	利用可能な SSM Agent の最新バージョンかインストールされているかどうかを示します。

AWS Systems Manager ハイブリッドアクティベーション

ハイブリッドおよびマルチクラウド環境において、AWS Systems Manager で使用するように非 EC2 マシンを設定するには、ハイブリッドアクティベーションを作成します。マネージドノードとしてサポートされている非 EC2 マシンタイプには以下が含まれます。

- 自社構築サーバー (オンプレミスサーバー)
- AWS IoT Greengrass コアデバイス
- AWS IoT および非 AWS エッジデバイス
- 他のクラウド環境内の VM を含む仮想マシン (VM)

create-activation コマンドを実行してハイブリッドアクティベーションプロセスを開始すると、コマンドのレスポンスでアクティベーションコードと ID を受け取ります。次に、ハイブリッド Linux ノードで SSM Agent をインストールする のステップ 3 と ハイブリッド Windows Server ノードに

SSM Agent をインストールする のステップ 4 で説明したように、アクティベーションコードと ID をコマンドに含めて、SSM Agent をマシンにインストールします。

このアクティベーションプロセスは、AWS IoT Greengrassコアデバイスを除くすべての非 EC2 マシンタイプに適用されます。Systems Manager の AWS IoT Greengrass コアデバイスを設定するための詳細については、「Systems Manager を利用したエッジデバイスの管理」を参照してください。

> **Note**
>
> 現在、EC2 macOS 以外のマシンにはサポートが提供されていません。

Systems Manager インスタンス層について

AWS Systems Manager は、標準インスタンス層とアドバンストインスタンス層を提供します。どちらもハイブリッドおよびマルチクラウド環境のマネージドノードをサポートします。スタンダードインスタンス層では、AWS リージョン ごと、AWS アカウント ごとに最大 1,000 のマシンを登録できます。1 つのアカウントとリージョンに 1,000 を超えるマシンを登録する必要がある場合は、アドバンストインスタンス層を使用します。アドバンストインスタンス層には、マネージドノードを好きなだけ作成することができます。Systems Manager 用に構成されたすべてのマネージドノードは、従量制料金ベースで請求されます。アドバンストインスタンス層を有効化する詳細については、「アドバンストインスタンス層を有効にするには」を参照してください。料金の詳細については、「AWS Systems Manager 料金表」を参照してください。

標準インスタンス層とアドバンストインスタンス層に関する次の追加情報に注意してください。

- また、アドバンストインスタンスでは、ハイブリッドおよびマルチクラウド環境において、AWS Systems Manager Session Manager を使用して非 EC2 ノードに接続することができます。Session Manager ではインスタンスへのインタラクティブシェルでアクセスを提供します。詳細については、「AWS Systems Manager Session Manager」を参照してください。
- スタンダードインスタンスのクォータは、Systems Manager オンプレミスアクティベーションを使用する EC2 インスタンスにも適用されます (これは一般的なシナリオではありません)。
- 仮想マシン (VM) のオンプレミスインスで Microsoft がリリースしたアプリケーションにパッチを適用するには、アドバンストインスタンス層を有効化してください。アドバンストインスタンス層の使用には料金が発生します。Amazon Elastic Compute Cloud (Amazon EC2) インスタンスで Microsoft がリリースしたアプリケーションにパッチを適用する場合、追加料金はかかりません。詳細については、「Windows Server で Microsoft がリリースしたアプリケーションへのパッチ適用について」を参照してください。

AWS Systems Manager インベントリ

AWS Systems Manager インベントリにより、AWS でのコンピューティング環境が可視化されます。インベントリを使用して、マネージドノードからメタデータを収集できます。このメタデータを中央 Amazon Simple Storage Service (Amazon S3) バケットに保存してから、組み込みツールを使用してデータにクエリを実行し、ソフトウェアを実行しているノード、ソフトウェアポリシーに必要な設定、および更新が必要なノードをすばやく判断できます。ワンクリックの手順を使用することで、すべてのマネージドノードでインベントリを設定できます。Amazon Athena を使用して、複数の AWS リージョン と AWS アカウント からのインベントリデータを設定し、表示することもできます。インベントリの使用を開始するには、Systems Manager コンソールを開きます。ナビゲーションペインで[Inventory] (インベントリ) を選択します。

Systems Manager Inventory によって収集された、事前設定されたメタデータのタイプが適切ではない場合は、カスタムインベントリを作成できます。カスタムインベントリは、指定したディレクトリ内のマネージドノードに指定および追加した情報を含む、単純な JSON ファイルです。Systems Manager Inventory がデータを収集するときに、このカスタムインベントリのデータがキャプチャされます。たとえば、大規模なデータセンターを実行している場合、各サーバーのラック位置をカスタムインベントリとして指定できます。その後、他のインベントリデータを表示するときに、ラックスペースのデータを表示できます。

> **Important**
>
> Systems Manager Inventory は、マネージドノードからメタデータのみを収集します。インベントリは、機密情報またはデータにアクセスすることはありません。

次の表に、Systems Manager Inventory で収集できるデータタイプを示します。またこの表では、ノードのターゲッティングや、収集間隔を指定する上での、さまざまな選択肢もご確認いただけます。

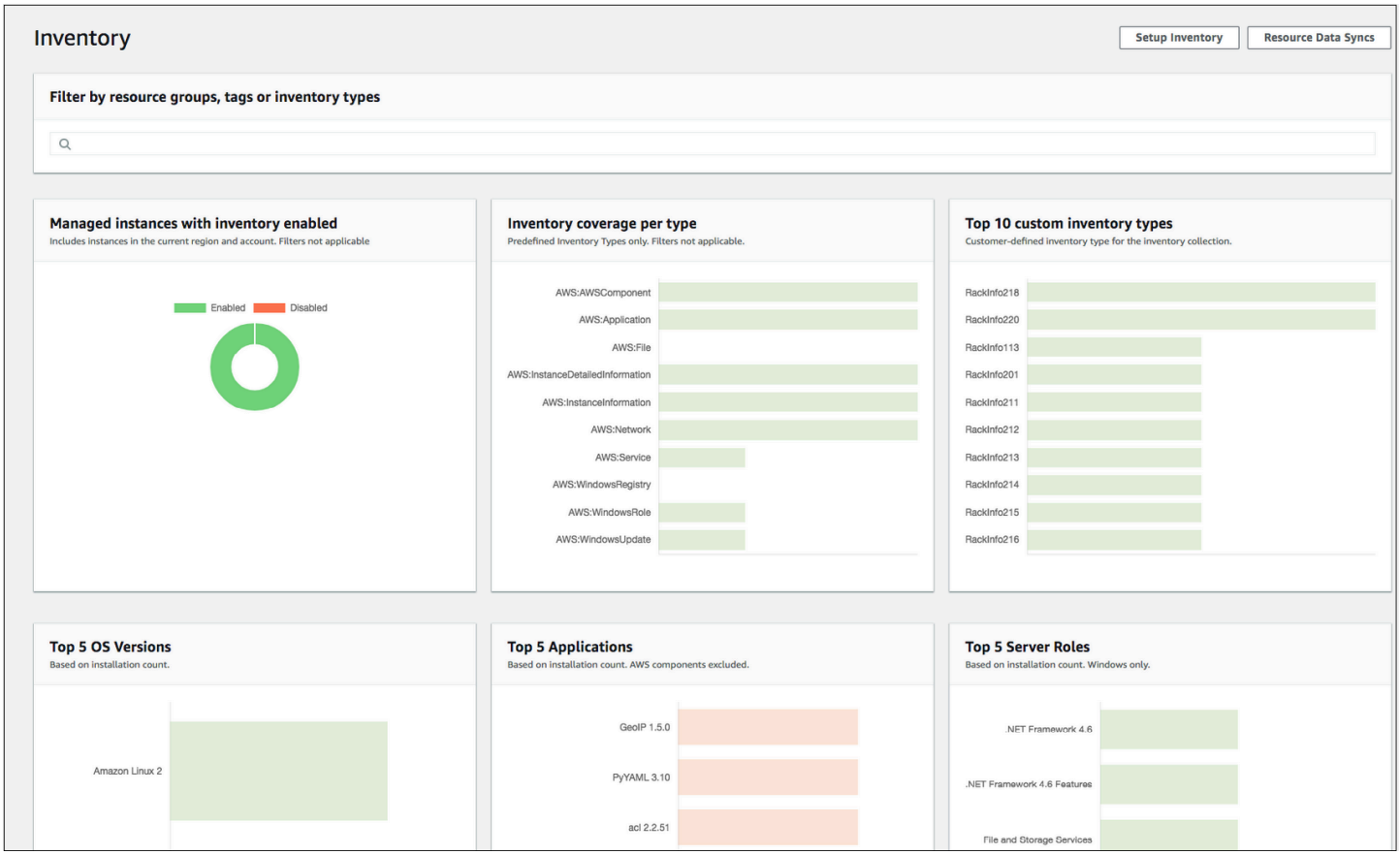
設定	詳細
メタデータタイプ	インベントリを設定すると、以下の各タイプのデータを収集できます。 • アプリケーション: アプリケーション名、発行元、バージョンなど。

設定	詳細
	• AWS コンポーネント: EC2 ドライバー、エージェント、バージョンなど。 • ファイル: 名前、サイズ、バージョン、インストール日、変更および最新アクセス時間など。 • ネットワーク設定の詳細: IP アドレス、MAC アドレス、DNS、ゲートウェイ、サブネットマスクなど。 • Windows 更新: Hotfix ID、インストール者、インストール日など。 • インスタンスの詳細: CPUModel、CPUCores、CPUs、CPUSpeedMHz、CPUSockets、CPUHyperThreadEnabled、OSServicePacketc。 • サービス: 名前、表示名、ステータス、依存サービス、サービスのタイプ、起動タイプなど。 • タグ: ノードに割り当てられるタグ。 • Windows レジストリ: レジストリキーのパス、値の名前、値タイプおよび値。 • Windows ロール: 名前、表示名、パス、機能タイプ、インストール日など。 • カスタムインベントリ: カスタムインベントリの操作 で説明されているように、マネージドノードに割り当てられたメタデータ。 **Note** インベントリで収集されるすべてのメタデータを表示するには、「インベントリによって収集されたメタデータ」を参照してください。

設定	詳細
ターゲットするノード	AWS アカウント 内のすべてのマネージドノードをインベントリする、個別にノードを選択する、またはタグを使用してノードのグループをターゲットにする選択ができます。すべてのマネージド型ノードからのインベントリデータ収集の詳細については、「AWS アカウント のすべてのマネージドイノードインベントリする」を参照してください。
情報を収集する間隔	収集間隔は、分、時間、日単位で指定できます。最短収集間隔は 30 分ごとです。

> **Note**
>
> 収集されるデータの量によっては、指定した出力にデータをレポートするのに数分かかることがあります。情報の収集が完了すると、AWS アカウント からのみアクセス可能な、プレーンテキスト用の AWS ストアに、セキュアな HTTPS チャンネルを介してデータが送信されます。

データのクエリに役立ついくつかの定義済みカードが含まれている、[Inventory] ページの Systems Manager コンソールのデータを表示できます。



> **Note**
>
> Inventory カードは、Terminated および Stopped の状態にある Amazon EC2 マネージドインスタンスを自動的に除外します。オンプレミス管理および AWS IoT Greengrass コアデバイスのマネージドノードの場合、インベントリカードは [Terminated] (終了) 状態にあるノードを自動的にフィルタリングします。

すべてのデータを同期して単一の Amazon S3 バケットに保存するためにリソースデータ同期を作成した場合は、[Inventory Detailed View (インベントリ詳細ビュー)] ページでデータにドリルダウンできます。詳細については、「複数のリージョンとアカウントからのインベントリデータをクエリする」を参照してください。

EventBridge のサポート

この Systems Manager ツールは、Amazon EventBridge ルールのイベントタイプとしてサポートされています。詳細については、「Amazon EventBridge を使用して Systems Manager イベントをモ

ニタリングする」および「リファレンス: Systems Manager 用の Amazon EventBridge イベントパターンとタイプ」を参照してください。

内容

- Systems Manager Inventory の詳細
- Systems Manager Inventory の設定
- インベントリ収集の設定
- 複数のリージョンとアカウントからのインベントリデータをクエリする
- フィルターを使用したインベントリ収集のクエリ
- インベントリデータの集計
- カスタムインベントリの操作
- インベントリ履歴と変更の追跡の表示
- データ収集の停止とインベントリデータの削除
- カスタムインベントリメタデータをマネージドノードに割り当てる
- AWS CLI を使用してインベントリデータ収集を設定する
- チュートリアル: リソースデータの同期を使用してインベントリデータを集計する
- Systems Manager Inventory に関する問題のトラブルシューティング

Systems Manager Inventory の詳細

AWS Systems Manager インベントリを設定する際、収集するメタデータのタイプ、メタデータの収集元となるマネージドノード、メタデータ収集のスケジュールを指定します。これらの設定は AWS アカウント に AWS Systems Manager State Manager の関連付けとして保存されます。関連付けとは単に設定のことです。

> **Note**
>
> インベントリはメタデータのみを収集します。個人のデータや所有権のあるデータは一切収集しません。

トピック

- インベントリによって収集されたメタデータ
- ファイルと Windows レジストリインベントリで作業する

インベントリによって収集されたメタデータ

次のサンプルは、各 AWS Systems Manager インベントリプラグインによって収集されたメタデータの完全リストを示しています。

```
{
    "typeName": "AWS:InstanceInformation",
    "version": "1.0",
    "attributes":[
      { "name": "AgentType",                                "dataType" : "STRING"},
      { "name": "AgentVersion",                             "dataType" : "STRING"},
      { "name": "ComputerName",                            "dataType" : "STRING"},
      { "name": "InstanceId",                              "dataType" : "STRING"},
      { "name": "IpAddress",                               "dataType" : "STRING"},
      { "name": "PlatformName",                            "dataType" : "STRING"},
      { "name": "PlatformType",                            "dataType" : "STRING"},
      { "name": "PlatformVersion",                         "dataType" : "STRING"},
      { "name": "ResourceType",                            "dataType" : "STRING"},
      { "name": "AgentStatus",                             "dataType" : "STRING"},
      { "name": "InstanceStatus",                          "dataType" : "STRING"}
    ]
  },
  {
    "typeName" : "AWS:Application",
    "version": "1.1",
    "attributes":[
      { "name": "Name",               "dataType": "STRING"},
      { "name": "ApplicationType",    "dataType": "STRING"},
      { "name": "Publisher",          "dataType": "STRING"},
      { "name": "Version",            "dataType": "STRING"},
      { "name": "Release",            "dataType": "STRING"},
      { "name": "Epoch",              "dataType": "STRING"},
      { "name": "InstalledTime",      "dataType": "STRING"},
      { "name": "Architecture",       "dataType": "STRING"},
      { "name": "URL",                "dataType": "STRING"},
      { "name": "Summary",            "dataType": "STRING"},
      { "name": "PackageId",          "dataType": "STRING"}
    ]
  },
  {
    "typeName" : "AWS:File",
    "version": "1.0",
    "attributes":[
      { "name": "Name",               "dataType": "STRING"},
```

```
      { "name": "Size",           "dataType": "STRING"},
      { "name": "Description",        "dataType": "STRING"},
      { "name": "FileVersion",        "dataType": "STRING"},
      { "name": "InstalledDate",      "dataType": "STRING"},
      { "name": "ModificationTime",   "dataType": "STRING"},
      { "name": "LastAccessTime",     "dataType": "STRING"},
      { "name": "ProductName",        "dataType": "STRING"},
      { "name": "InstalledDir",       "dataType": "STRING"},
      { "name": "ProductLanguage",    "dataType": "STRING"},
      { "name": "CompanyName",        "dataType": "STRING"},
      { "name": "ProductVersion",       "dataType": "STRING"}
    ]
  },
  {
    "typeName": "AWS:AWSComponent",
    "version": "1.0",
    "attributes":[
      { "name": "Name",               "dataType": "STRING"},
      { "name": "ApplicationType",    "dataType": "STRING"},
      { "name": "Publisher",          "dataType": "STRING"},
      { "name": "Version",            "dataType": "STRING"},
      { "name": "InstalledTime",      "dataType": "STRING"},
      { "name": "Architecture",       "dataType": "STRING"},
      { "name": "URL",                "dataType": "STRING"}
    ]
  },
  {
    "typeName": "AWS:WindowsUpdate",
    "version":"1.0",
    "attributes":[
      { "name": "HotFixId",           "dataType": "STRING"},
      { "name": "Description",        "dataType": "STRING"},
      { "name": "InstalledTime",      "dataType": "STRING"},
      { "name": "InstalledBy",        "dataType": "STRING"}
    ]
  },
  {
    "typeName": "AWS:Network",
    "version":"1.0",
    "attributes":[
      { "name": "Name",               "dataType": "STRING"},
      { "name": "SubnetMask",         "dataType": "STRING"},
      { "name": "Gateway",            "dataType": "STRING"},
      { "name": "DHCPServer",         "dataType": "STRING"},
```

```
      { "name": "DNSServer",          "dataType": "STRING"},
      { "name": "MacAddress",         "dataType": "STRING"},
      { "name": "IPV4",               "dataType": "STRING"},
      { "name": "IPV6",               "dataType": "STRING"}
    ]
  },
  {
    "typeName": "AWS:PatchSummary",
    "version":"1.0",
    "attributes":[
      { "name": "PatchGroup",                      "dataType": "STRING"},
      { "name": "BaselineId",                      "dataType": "STRING"},
      { "name": "SnapshotId",                      "dataType": "STRING"},
      { "name": "OwnerInformation",                "dataType": "STRING"},
      { "name": "InstalledCount",                  "dataType": "NUMBER"},
      { "name": "InstalledPendingRebootCount",     "dataType": "NUMBER"},
      { "name": "InstalledOtherCount",             "dataType": "NUMBER"},
      { "name": "InstalledRejectedCount",          "dataType": "NUMBER"},
      { "name": "NotApplicableCount",              "dataType": "NUMBER"},
      { "name": "UnreportedNotApplicableCount",    "dataType": "NUMBER"},
      { "name": "MissingCount",                    "dataType": "NUMBER"},
      { "name": "FailedCount",                     "dataType": "NUMBER"},
      { "name": "OperationType",                   "dataType": "STRING"},
      { "name": "OperationStartTime",              "dataType": "STRING"},
      { "name": "OperationEndTime",                "dataType": "STRING"},
      { "name": "InstallOverrideList",             "dataType": "STRING"},
      { "name": "RebootOption",                    "dataType": "STRING"},
      { "name": "LastNoRebootInstallOperationTime", "dataType": "STRING"},
      { "name": "ExecutionId",                     "dataType": "STRING",
   "isOptional": "true"},
      { "name": "NonCompliantSeverity",            "dataType": "STRING",
   "isOptional": "true"},
      { "name": "SecurityNonCompliantCount",       "dataType": "NUMBER",
   "isOptional": "true"},
      { "name": "CriticalNonCompliantCount",       "dataType": "NUMBER",
   "isOptional": "true"},
      { "name": "OtherNonCompliantCount",          "dataType": "NUMBER",
   "isOptional": "true"}
    ]
  },
  {
    "typeName": "AWS:PatchCompliance",
    "version":"1.0",
    "attributes":[
```

```
      { "name": "Title",                          "dataType": "STRING"},
      { "name": "KBId",                           "dataType": "STRING"},
      { "name": "Classification",                 "dataType": "STRING"},
      { "name": "Severity",                       "dataType": "STRING"},
      { "name": "State",                          "dataType": "STRING"},
      { "name": "InstalledTime",                  "dataType": "STRING"}
    ]
  },
  {
    "typeName": "AWS:ComplianceItem",
    "version":"1.0",
    "attributes":[
      { "name": "ComplianceType",                 "dataType": "STRING",
"isContext": "true"},
      { "name": "ExecutionId",                    "dataType": "STRING",
"isContext": "true"},
      { "name": "ExecutionType",                  "dataType": "STRING",
"isContext": "true"},
      { "name": "ExecutionTime",                  "dataType": "STRING",
"isContext": "true"},
      { "name": "Id",                             "dataType": "STRING"},
      { "name": "Title",                          "dataType": "STRING"},
      { "name": "Status",                         "dataType": "STRING"},
      { "name": "Severity",                       "dataType": "STRING"},
      { "name": "DocumentName",                   "dataType": "STRING"},
      { "name": "DocumentVersion",                "dataType": "STRING"},
      { "name": "Classification",                 "dataType": "STRING"},
      { "name": "PatchBaselineId",                "dataType": "STRING"},
      { "name": "PatchSeverity",                  "dataType": "STRING"},
      { "name": "PatchState",                     "dataType": "STRING"},
      { "name": "PatchGroup",                     "dataType": "STRING"},
      { "name": "InstalledTime",                  "dataType": "STRING"},
      { "name": "InstallOverrideList",            "dataType": "STRING",
"isOptional": "true"},
      { "name": "DetailedText",                   "dataType": "STRING",
"isOptional": "true"},
      { "name": "DetailedLink",                   "dataType": "STRING",
"isOptional": "true"},
      { "name": "CVEIds",                         "dataType": "STRING",
"isOptional": "true"}
    ]
  },
  {
    "typeName": "AWS:ComplianceSummary",
```

```
    "version":"1.0",
    "attributes":[
      { "name": "ComplianceType",                "dataType": "STRING"},
      { "name": "PatchGroup",                    "dataType": "STRING"},
      { "name": "PatchBaselineId",               "dataType": "STRING"},
      { "name": "Status",                        "dataType": "STRING"},
      { "name": "OverallSeverity",               "dataType": "STRING"},
      { "name": "ExecutionId",                   "dataType": "STRING"},
      { "name": "ExecutionType",                 "dataType": "STRING"},
      { "name": "ExecutionTime",                 "dataType": "STRING"},
      { "name": "CompliantCriticalCount",        "dataType": "NUMBER"},
      { "name": "CompliantHighCount",            "dataType": "NUMBER"},
      { "name": "CompliantMediumCount",          "dataType": "NUMBER"},
      { "name": "CompliantLowCount",             "dataType": "NUMBER"},
      { "name": "CompliantInformationalCount",   "dataType": "NUMBER"},
      { "name": "CompliantUnspecifiedCount",     "dataType": "NUMBER"},
      { "name": "NonCompliantCriticalCount",     "dataType": "NUMBER"},
      { "name": "NonCompliantHighCount",         "dataType": "NUMBER"},
      { "name": "NonCompliantMediumCount",       "dataType": "NUMBER"},
      { "name": "NonCompliantLowCount",          "dataType": "NUMBER"},
      { "name": "NonCompliantInformationalCount", "dataType": "NUMBER"},
      { "name": "NonCompliantUnspecifiedCount",  "dataType": "NUMBER"}
    ]
  },
  {
    "typeName": "AWS:InstanceDetailedInformation",
    "version":"1.0",
    "attributes":[
      { "name": "CPUModel",                    "dataType": "STRING"},
      { "name": "CPUCores",                    "dataType": "NUMBER"},
      { "name": "CPUs",                        "dataType": "NUMBER"},
      { "name": "CPUSpeedMHz",                 "dataType": "NUMBER"},
      { "name": "CPUSockets",                  "dataType": "NUMBER"},
      { "name": "CPUHyperThreadEnabled",       "dataType": "STRING"},
      { "name": "OSServicePack",               "dataType": "STRING"}
    ]
   },
   {
     "typeName": "AWS:Service",
     "version":"1.0",
     "attributes":[
       { "name": "Name",                       "dataType": "STRING"},
       { "name": "DisplayName",                "dataType": "STRING"},
       { "name": "ServiceType",                "dataType": "STRING"},
```

```
        { "name": "Status",                          "dataType": "STRING"},
        { "name": "DependentServices",               "dataType": "STRING"},
        { "name": "ServicesDependedOn",              "dataType": "STRING"},
        { "name": "StartType",                       "dataType": "STRING"}
      ]
    },
    {
      "typeName": "AWS:WindowsRegistry",
      "version":"1.0",
      "attributes":[
        { "name": "KeyPath",                           "dataType": "STRING"},
        { "name": "ValueName",                         "dataType": "STRING"},
        { "name": "ValueType",                         "dataType": "STRING"},
        { "name": "Value",                             "dataType": "STRING"}
      ]
    },
    {
      "typeName": "AWS:WindowsRole",
      "version":"1.0",
      "attributes":[
        { "name": "Name",                            "dataType": "STRING"},
        { "name": "DisplayName",                     "dataType": "STRING"},
        { "name": "Path",                            "dataType": "STRING"},
        { "name": "FeatureType",                     "dataType": "STRING"},
        { "name": "DependsOn",                       "dataType": "STRING"},
        { "name": "Description",                     "dataType": "STRING"},
        { "name": "Installed",                       "dataType": "STRING"},
        { "name": "InstalledState",                  "dataType": "STRING"},
        { "name": "SubFeatures",                     "dataType": "STRING"},
        { "name": "ServerComponentDescriptor",       "dataType": "STRING"},
        { "name": "Parent",                          "dataType": "STRING"}
      ]
    },
    {
      "typeName": "AWS:Tag",
      "version":"1.0",
      "attributes":[
        { "name": "Key",                       "dataType": "STRING"},
        { "name": "Value",                     "dataType": "STRING"}
      ]
    },
    {
      "typeName": "AWS:ResourceGroup",
      "version":"1.0",
```

```
    "attributes":[
      { "name": "Name",                    "dataType": "STRING"},
      { "name": "Arn",                     "dataType": "STRING"}
    ]
  },
  {
    "typeName": "AWS:BillingInfo",
    "version": "1.0",
    "attributes": [
      { "name": "BillingProductId",        "dataType": "STRING"}
    ]
  }
```

Note

- `"typeName": "AWS:InstanceInformation"` の場合、`InstanceStatus` は、Active, ConnectionLost、Stopped、Terminated のいずれかになります。
- バージョン 2.5 のリリースでは、RPM Package Manager で Serial 属性が Epoch 属性に置き換えられました。Epoch 属性は、Serial のように一定間隔で増える整数です。`AWS:Application` タイプを使用してインベントリを作成する場合、Epoch の値が大きいほど新しいバージョンを意味します。Epoch 値が同じ場合または空の場合は、Version または Release 属性の値を使用して、より新しいバージョンを決定します。
- 一部のメタデータは Linux インスタンスからは利用できません。具体的には、"typeName": "AWS:Network" の場合、次のメタデータタイプは Linux インスタンスではまだサポートされていません。これらは Windows でサポートされています。
  - { "name": "SubnetMask", "dataType": "STRING"},
  - { "name": "DHCPServer", "dataType": "STRING"},
  - { "name": "DNSServer", "dataType": "STRING"},
  - { "name": "Gateway", "dataType": "STRING"},

ファイルと Windows レジストリインベントリで作業する

AWS Systems Manager インベントリは、Windows、Linux、macOS オペレーティングシステムでファイルを検索し、インベントリできるようにします。Windows レジストリの検索およびインベントリもできます。

ファイル: ファイル名、ファイル作成時間、ファイルの最終変更時間および最新アクセス時間、およびファイルサイズなど多数のファイルに関するメタデータ情報を収集できます。ファイルインベントリの収集を開始するには、インベントリを実行するファイルパスを指定し、インベントリを行うファイルタイプを定義する 1 つ以上のパターン、そしてパスが再帰的にトラバースすべきかを指定します。Systems Manager は、パターンと一致する指定されたパスのファイルのすべてのファイルメタデータをインベントリします。ファイルインベントリは次の入力パラメータを使用します。

```
{
"Path": string,
"Pattern": array[string],
"Recursive": true,
"DirScanLimit" : number // Optional
}
```

- パス: ファイルをインベントリするディレクトリパス。Windows の場合、変数が単一ディレクトリパスにマッピングする限りにおいて、%PROGRAMFILES% などの環境変数を使用できます。たとえば、複数のディレクトリパスをマッピングする %PATH% を使用すると、インベントリはエラーをスローします。
- パターン: ファイルを識別するためのパターン配列。
- 再帰的: インベントリが再帰的にディレクトリをトラバースすべきかを示すブール値。
- DirScanLimit: スキャンするディレクトリ数を指定するオプションの値。このパラメータを使用して、マネージドノードのパフォーマンスへの影響を最小化します。インベントリは最大で 5,000 ディレクトリまでをスキャンします。

> **Note**
>
> インベントリは、すべての指定したパスから最大で 500 ファイルのメタデータを収集します。

ここでは、ファイルのインベントリを実行する場合にどのようにパラメータを指定するかについての例をいくつか示します。

- Linux および macOS では、すべてのサブディレクトリを除く、/home/ec2-user ディレクトリの .sh ファイルのメタデータを収集します。

```
[{"Path":"/home/ec2-user","Pattern":["*.sh", "*.sh"],"Recursive":false}]
```

- Windows では、サブディレクトリを再帰的に含む、プログラムファイルフォルダのすべての「.exe」ファイルのメタデータを収集します。

```
[{"Path":"C:\Program Files","Pattern":["*.exe"],"Recursive":true}]
```

- Windows では、特定のログパターンのメタデータを収集します。

```
[{"Path":"C:\ProgramData\Amazon","Pattern":["*amazon*.log"],"Recursive":true}]
```

- 再帰的収集を実行する場合には、ディレクトリの数を制限します。

```
[{"Path":"C:\Users","Pattern":["*.ps1"],"Recursive":true, "DirScanLimit": 1000}]
```

Windows のレジストリ: Windows レジストリキーと値を収集することができます。キーパスを選択して、すべてのキーと値を再帰的に収集できます。指定するパスで指定するレジストリキーおよびその値を収集することもできます。インベントリは、キーパス、名前、タイプ、値を収集します。

```
{
"Path": string,
"Recursive": true,
"ValueNames": array[string] // optional
}
```

- パス: レジストリキーへのパス。
- 再帰的: インベントリが再帰的にレジストリパスをトラバースすべきかを示すブール値。
- ValueNames: レジストリキーのインベントリを実行する値名の配列。このパラメータを使用する場合、Systems Manager は指定するパスの指定する値名のみをインベントリします。

> **Note**
>
> インベントリは、すべての指定したパスから最大で 250 レジストリキー値を収集します。

ここでは、Windows レジストリのインベントリを実行する場合にどのようにパラメータを指定するかについての例をいくつか示します。

- 指定したパスのすべてのキーと値を再帰的に収集します。

```
[{"Path":"HKEY_LOCAL_MACHINE\SOFTWARE\Amazon","Recursive": true}]
```

- 指定したパスのすべてのキーと値を収集します (再帰的検索無効)。

```
[{"Path":"HKEY_LOCAL_MACHINE\SOFTWARE\Intel\PSIS\PSIS_DECODER", "Recursive": false}]
```

- `ValueNames` オプションを使用して、指定するキーを収集します。

```
{"Path":"HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\MachineImage","ValueNames":["AMIName"]}
```

Systems Manager Inventory の設定

AWS Systems Manager インベントリを使用して、マネージドノードで実行しているアプリケーション、サービス、AWS コンポーネントなどに関するメタデータを収集する前に、リソースデータ同期を設定して、インベントリデータのストレージを 1 つの Amazon Simple Storage Service (Amazon S3) バケットに一元化することをお勧めします。また、インベントリイベントの Amazon EventBridge モニタリングを設定することをお勧めします。これらのプロセスにより、インベントリデータと収集の表示と管理が簡単になります。

トピック

- インベントリのリソースデータ同期を作成する
- EventBridge を使用して Inventory イベントをモニタリングする

インベントリのリソースデータ同期を作成する

このトピックでは、AWS Systems Manager インベントリのリソースデータ同期を設定および構成する方法について説明します。Systems Manager Explorer のリソースデータ同期については、「複数のアカウントおよびリージョンのデータを表示するように Systems Manager Explorer を設定する」を参照してください。

リソースデータの同期について

Systems Manager のリソースデータ同期を使用して、すべてのマネージドノードから収集されたインベントリデータを、1 つの Amazon Simple Storage Service (Amazon S3) バケットに送信できます。その後、リソースデータの同期により、新しいインベントリデータが収集されると、一元化されたデータが自動的に更新されます。ターゲット Amazon S3 バケットに保存されたすべてのインベン

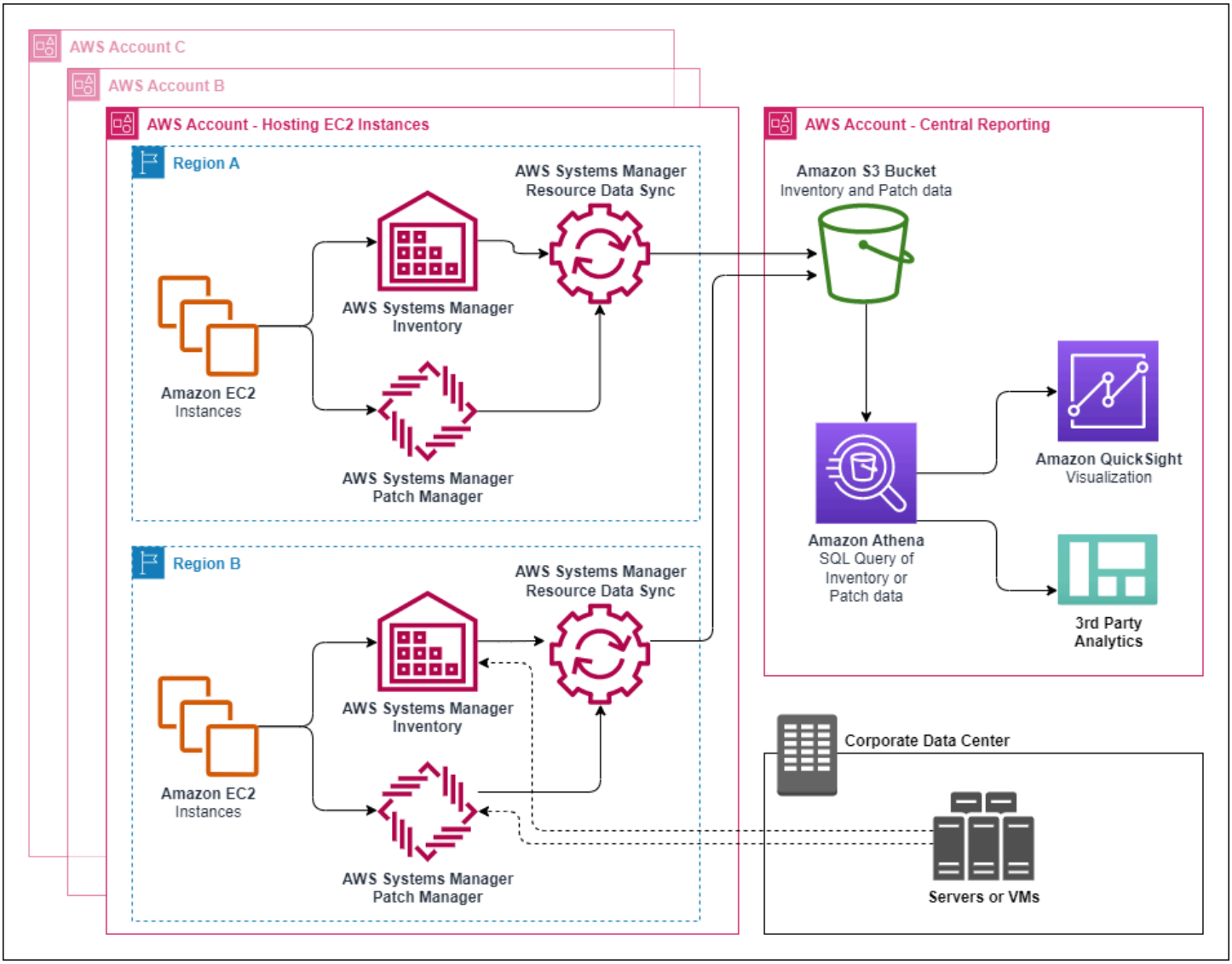
トリデータに対して、Amazon Athena や Amazon QuickSight などのサービスを使用して集計データのクエリや分析ができます。

たとえば、150 個のマネージドノードのフリートで実行されているオペレーティングシステム (OS) およびアプリケーションに関するデータを収集するようにインベントリを設定したとします。これらのノードのいくつかはオンプレミスデータセンターに配置され、その他のインスタンスは複数の AWS リージョン にまたがる Amazon Elastic Compute Cloud (Amazon EC2) で実行されています。リソースデータ同期を設定していない場合、各マネージドノードで収集されたインベントリデータを手動でまとめるか、この情報を収集するスクリプトを作成する必要があります。その後、クエリや分析を実行できるように、データをアプリケーションにポートする必要があります。

リソースデータ同期では、すべてのマネージドノードから収集したすべてのインベントリデータを同期する 1 回限りのオペレーションを実行します。同期が正常に作成されると、Systems Manager はすべてのインベントリデータのベースラインを作成し、それをターゲット Amazon S3 バケットに保存します。新しいインベントリデータが収集されると、Systems Manager は Amazon S3 バケットのデータを自動的に更新します。その後、Amazon Athena および Amazon QuickSight にデータを迅速かつコスト効率よくポートできます。

図 1 は、リソースデータ同期が、Amazon EC2 およびハイブリッドおよびマルチクラウド環境内の他のマシンタイプからターゲットの Amazon S3 バケットにインベントリデータを収集する方法を示しています。またこの図は、リソースデータ同期が複数の AWS アカウント および AWS リージョンと連携する仕組みについても示しています。

図 1: 複数の AWS アカウント とAWS リージョン とのリソースデータ同期



マネージドノードを削除した場合、リソースデータ同期は削除されたノードのインベントリファイルを維持します。ただし、実行中のノードの場合、新しいインベントリファイルが作成され Amazon S3 バケットに書き込まれると、リソースデータ同期は古いインベントリファイルを自動的に上書きします。インベントリの変更を継続的に追跡する場合は、AWS Config サービスを使用して `SSM:ManagedInstanceInventory` リソースタイプを追跡できます。詳細については、「AWS Config の開始方法」を参照してください。

Amazon S3 および AWS Systems Manager コンソールを使用してインベントリのリソースデータ同期を作成するには、このセクションの手順に従います。AWS CloudFormation を使用してリソースデータ同期を作成または削除することもできます。AWS CloudFormation を使用するには、AWS CloudFormation テンプレートに `AWS::SSM::ResourceDataSync` リソースを追加します。詳細については、次のいずれかのドキュメントリソースを参照してください。

- AWS Systems Manager でのリソースデータ同期の AWS CloudFormation リソース (ブログ)
- AWS CloudFormation ユーザーガイドの AWS CloudFormation のテンプレートの使用

> **Note**
>
> AWS Key Management Service (AWS KMS) を使用すると Amazon S3 バケットのインベントリデータを暗号化できます。AWS Command Line Interface (AWS CLI) を使用して暗号化された同期を作成する方法、および Amazon Athena および Amazon QuickSight で一元化されたデータを扱う方法の例については、「チュートリアル: リソースデータの同期を使用してインベントリデータを集計する」を参照してください。

開始する前に

リソースデータ同期を作成する前に、以下の手順に従って、集約されたインベントリデータを格納する中央 Amazon S3 バケットを作成します。この手順では、Systems Manager が複数のアカウントからバケットにインベントリデータを書き込めるようにするバケットポリシーの割り当て方法について説明します。リソースデータ同期のためのインベントリデータ集計に使用する Amazon S3 バケットが既にある場合、次の手順でポリシーを使用するようにバケットを設定する必要があります。

> **Note**
>
> 指定した Amazon S3 バケットに Object Lock を使用するように設定されている場合、Systems Manager インベントリでは、そのバケットにデータを追加できません。リソースデータの同期用に作成または選択した Amazon S3 バケットが、Amazon S3 Object Lock を使用するように設定されていないことを確認します。詳細については、Amazon Simple Storage Service ユーザーガイドの「Amazon S3 Object Lock の仕組み」を参照してください。

リソースデータ同期用に Amazon S3 バケットを作成して設定するには

1. Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 集計されたインベントリデータを保存するバケットを作成します。詳細については、Amazon Simple Storage Service ユーザーガイドの「バケットの作成」を参照してください。バケット名とそれを作成した AWS リージョン を書き留めます。
3. [Permissions] タブを選択し、[Bucket Policy] を選択します。

4. 次のバケットポリシーをコピーし、ポリシーエディタに貼り付けます。*amzn-s3-demo-bucket* を S3 バケットの名前に置き換えます。*account_ID_number* を有効な AWS アカウント ID 番号に置き換えます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
        "Sid": "SSMBucketPermissionsCheck",
        "Effect": "Allow",
        "Principal": {
            "Service": "ssm.amazonaws.com"
        },
        "Action": "s3:GetBucketAcl",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
        },
        {
        "Sid": " SSMBucketDelivery",
        "Effect": "Allow",
        "Principal": {
            "Service": "ssm.amazonaws.com"
        },
        "Action": "s3:PutObject",
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket/*/accountid=account_ID_number/*",
            "arn:aws:s3:::amzn-s3-demo-bucket/*/accountid=account_ID_number/*",
            "arn:aws:s3:::amzn-s3-demo-bucket/*/accountid=account_ID_number/*",
            "arn:aws:s3:::amzn-s3-demo-bucket/*/accountid=account_ID_number/*"
        ],
        "Condition": {
            "StringEquals": {
                "s3:x-amz-acl": "bucket-owner-full-control",
                "aws:SourceAccount": "ID_number"
            },
            "ArnLike": {
                "aws:SourceArn": "arn:aws:ssm:*:account_ID_number:resource-data-
sync/*"
            }
        }
      }
    ]
}
```

5. 変更内容を保存します。

インベントリのリソースデータの同期を作成

Systems Manager コンソールを使用して、Systems Manager Inventory のリソースデータ同期を作成するには、次の手順に従います。AWS CLI を使用したリソースデータ同期の作成については、「AWS CLI を使用してインベントリデータ収集を設定する」を参照してください。

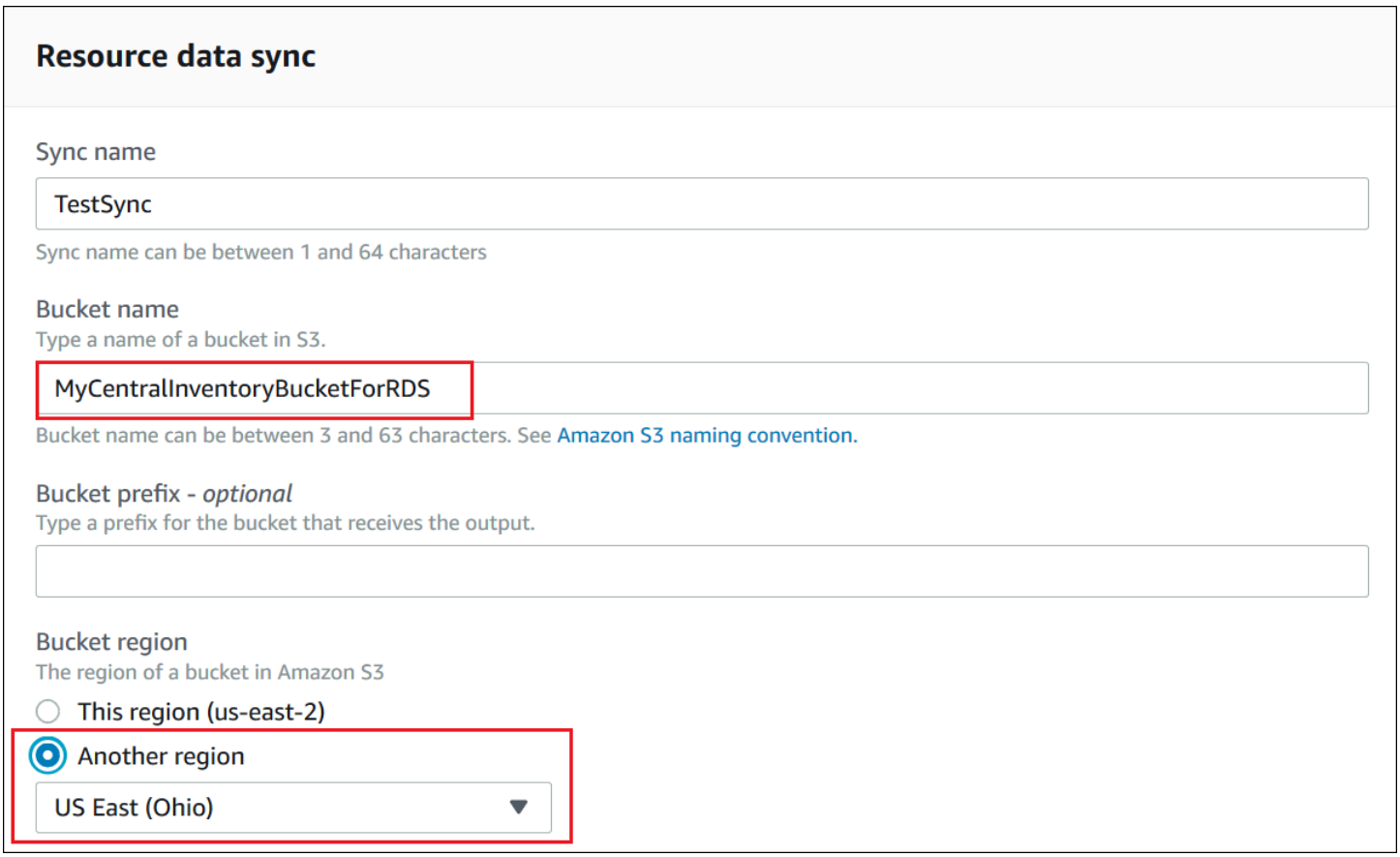
リソースデータの同期を作成するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. [Account management] メニューで、[Resource data sync] を選択します。
4. [Create resource data sync (リソースデータ同期の作成)] を選択します。
5. [Sync name] フィールドに、同期設定の名前を入力します。
6. [Bucket name] フィールドに、 リソースデータ同期用に Amazon S3 バケットを作成して設定するにはの手順を使用して作成した Amazon S3 バケットの名前を入力します。
7. (オプション) [Bucket prefix] フィールドに、Amazon S3 バケットのプレフィックス (サブディレクトリ) の名前を入力します。
8. 作成した Amazon S3 バケットが現在の AWS リージョン にある場合は、[Bucket region (バケットリージョン)] フィールドで [This region (このリージョン)] を選択します。バケットが他の AWS リージョン にある場合は、[Another region(別のリージョン)] を選択して、リージョンの名前を入力します。

   > **Note**
   >
   > 同期とターゲット Amazon S3 バケットが異なるリージョンにある場合は、データ転送料金が発生する場合があります。詳細については、Amazon S3 の料金 を参照してください。

9. (オプション) [KMS キー ARN] フィールドで、KMS キー ARN を入力するか貼り付けて、Amazon S3 のインベントリデータを暗号化します。
10. [Create] を選択します。

複数の AWS リージョン からのインベントリデータを同期させるには、各リージョンでのリソースデータ同期を作成する必要があります。インベントリデータを収集し、中央 Amazon S3 バケットに送信する各 AWS リージョン でこの手順を繰り返します。各リージョンで同期を作成するときは、[Bucket name (バケット名)] フィールドで中央 Amazon S3 バケットを指定します。次に、[Bucket region (バケットリージョン)] オプションを使用して、次のスクリーンショットに示すように、中央 Amazon S3 バケットを作成したリージョンを選択します。次回インベントリデータを収集するために関連付けを実行すると、Systems Manager は中央 Amazon S3 バケットにデータを保存します。



で定義されたアカウントのインベントリリソースデータ同期の作成AWS Organizations

AWS Organizations で定義された AWS アカウント のインベントリデータを中央の Amazon S3 バケットに同期できます。次の手順を完了すると、インベントリデータは中央バケット内の個々の Amazon S3 キープレフィックスに同期されます。各キープレフィックスは、異なる AWS アカウント ID を表します。

開始する前に

開始する前に、AWS Organizations で AWS アカウント が設定および構成されていることを確認してください。詳細については、AWS Organizations ユーザーガイドを参照してください。

また、AWS Organizations で定義されている各 AWS リージョン と AWS アカウント について、組織ベースのリソースデータ同期を作成する必要があることに注意してください。

中央の Amazon S3 バケットを作成する

以下の手順に従って、集約されたインベントリデータを格納する中央 Amazon S3 バケットを作成します。この手順では、Systems Manager が AWS Organizations アカウント ID からバケットにインベントリデータを書き込めるようにするバケットポリシーの割り当て方法について説明します。リソースデータ同期のためのインベントリデータ集計に使用する Amazon S3 バケットが既にある場合、次の手順でポリシーを使用するようにバケットを設定する必要があります。

で定義された複数アカウントのリソースデータ同期用に Amazon S3 バケットを作成して設定するにはAWS Organizations

1. Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 集計されたインベントリデータを保存するバケットを作成します。詳細については、Amazon Simple Storage Service ユーザーガイドの「バケットの作成」を参照してください。バケット名とそれを作成した AWS リージョン を書き留めます。
3. [Permissions] タブを選択し、[Bucket Policy] を選択します。
4. 次のバケットポリシーをコピーし、ポリシーエディタに貼り付けます。*amzn-s3-demo-bucket* と *organization-id* を、作成した Amazon S3 バケットの名前と、有効な AWS Organizations アカウント ID に置き換えます。

   任意で、*bucket-prefix* を Amazon S3 プレフィックス (サブディレクトリ) に置き換えます。プレフィックスを作成していない場合は、次のポリシーの ARN から *bucket-prefix/* を削除します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SSMBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "ssm.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::S3_bucket_name"
    },
    {
```

```
      "Sid": " SSMBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "Service": "ssm.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/bucket-prefix/*/accountid=*/*"
      ],
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control",
          "aws:SourceOrgID": "organization-id"
                  }
      }
    },
    {
      "Sid": " SSMBucketDeliveryTagging",
      "Effect": "Allow",
      "Principal": {
        "Service": "ssm.amazonaws.com"
      },
      "Action": "s3:PutObjectTagging",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/bucket-prefix/*/accountid=*/*"
      ]
    }
  ]
}
```

で定義されたアカウントのインベントリリソースデータ同期を作成するAWS Organizations

次の手順では、AWS CLI を使用して、AWS Organizations で定義されているアカウントのリソースデータ同期を作成する方法について説明します。このタスクを実行するには AWS CLI を使用する必要があります。この手順は、AWS Organizations で定義されている各 AWS リージョン および AWS アカウント に対して実行する必要があります。

AWS Organizations で定義されたアカウントのインベントリリソースデータ同期を作成するには (AWS CLI)

1. まだ AWS Command Line Interface (AWS CLI) をインストールして設定していない場合は、インストールして設定します。

詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」を参照してください。

2. 次のコマンドを実行して、他の AWS Organizations ベースのリソースデータの同期がないことを確認します。複数の標準同期と Organizations ベースの同期を含む、複数の標準同期を設定できます。ただし、Organizations ベースのリソースデータの同期は 1 つだけ設定できます。

```
aws ssm list-resource-data-sync
```

コマンドが他の組織ベースのリソースデータの同期を返す場合は、削除するか、新しいリソースデータ同期を作成しないように選択する必要があります。

3. AWS Organizations で定義されたアカウントのリソースデータ同期を作成するには、次のコマンドを実行します。amzn-s3-demo-bucket には、このトピックで先ほど作成した Amazon S3 バケットの名前を指定します。バケットのプレフィックス (サブディレクトリ) を作成した場合は、[*prefix-name*] にこの情報を指定します。

```
aws ssm create-resource-data-sync --sync-name name --s3-
destination "BucketName=amzn-s3-demo-bucket,Prefix=prefix-
name,SyncFormat=JsonSerDe,Region=AWS #####, for example us-
east-2,DestinationDataSharing={DestinationDataSharingType=Organization}"
```

4. 中央の Amazon S3 バケットにデータを同期する AWS リージョン と AWS アカウント ごとに、ステップ 2 と 3 を繰り返します。

リソースデータの同期を管理する

それぞれの AWS アカウント が AWS リージョン あたり 5 つのリソースデータを同期できます。AWS Systems Manager Fleet Manager コンソールを使って、リソースデータの同期を管理できます。

リソースデータの同期を表示するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. [リソースデータの同期] メニューで、[アカウント管理] ドロップダウンを選択します。
4. テーブルからリソースデータの同期を選択し、[詳細の表示] を選択すると、リソースデータの同期に関する情報が表示されます。

リソースデータ同期を削除するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. [リソースデータの同期] メニューで、[アカウント管理] ドロップダウンを選択します。
4. テーブルからリソースデータの同期を選択し、[削除] を選択します。

EventBridge を使用して Inventory イベントをモニタリングする

Amazon EventBridge でルールを設定して、AWS Systems Manager Inventory のリソース状態の変更に応じてイベントを作成できます。EventBridge では、Inventory の次の状態の変更に関するイベントがサポートされます。すべてのイベントは、ベストエフォートベースで送信されます。

特定のインスタンスのカスタムインベントリタイプの削除: このイベントをモニタリングするようにルールが設定されている場合、EventBridge は、特定のマネージドのカスタムインベントリタイプが削除されたときにイベントを作成します。EventBridge は、カスタムインベントリタイプごとに 1 ノードあたり 1 つのイベントを送信します。イベントパターンの例を次に示します。

```
{
    "timestampMillis": 1610042981103,
    "source": "SSM",
    "account": "123456789012",
    "type": "INVENTORY_RESOURCE_STATE_CHANGE",
    "startTime": "Jan 7, 2021 6:09:41 PM",
    "resources": [
        {
            "arn": "arn:aws:ssm:us-east-1:123456789012:managed-instance/i-12345678"
        }
    ],
    "body": {
        "action-status": "succeeded",
        "action": "delete",
        "resource-type": "managed-instance",
        "resource-id": "i-12345678",
        "action-reason": "",
        "type-name": "Custom:MyCustomInventoryType"
    }
}
```

すべてのインスタンスのカスタムインベントリタイプの削除イベント: このイベントをモニタリングするようにルールが設定されている場合、EventBridge は、すべてのマネージドノードのカスタムインベントリタイプが削除されたときにイベントを作成します。イベントパターンの例を次に示します。

```
{
    "timestampMillis": 1610042904712,
    "source": "SSM",
    "account": "123456789012",
    "type": "INVENTORY_RESOURCE_STATE_CHANGE",
    "startTime": "Jan 7, 2021 6:08:24 PM",
    "resources": [

    ],
    "body": {
        "action-status": "succeeded",
        "action": "delete-summary",
        "resource-type": "managed-instance",
        "resource-id": "",
        "action-reason": "The delete for type name Custom:SomeCustomInventoryType
 was completed. The deletion summary is: {\"totalCount\":1,\"remainingCount\":0,
\"summaryItems\":[{\"version\":\"1.1\",\"count\":1,\"remainingCount\":0}]}",
        "type-name": "Custom:MyCustomInventoryType"
    }
}
```

古いスキーマバージョンイベントで PutInventory 呼び出し: このイベントをモニタリングするようにルールが設定されている場合、EventBridge は、現在のスキーマよりも低いスキーマバージョンを使用する PutInventory 呼び出しが行われたときにイベントを作成します。このイベントは、すべてのインベントリタイプに適用されます。イベントパターンの例を次に示します。

```
{
    "timestampMillis": 1610042629548,
    "source": "SSM",
    "account": "123456789012",
    "type": "INVENTORY_RESOURCE_STATE_CHANGE",
    "startTime": "Jan 7, 2021 6:03:49 PM",
    "resources": [
        {
            "arn": "arn:aws:ssm:us-east-1:123456789012:managed-instance/i-12345678"
        }
    ],
```

```
    "body": {
        "action-status": "failed",
        "action": "put",
        "resource-type": "managed-instance",
        "resource-id": "i-01f017c1b2efbe2bc",
        "action-reason": "The inventory item with type name
 Custom:MyCustomInventoryType was sent with a disabled schema verison 1.0. You must
 send a version greater than 1.0",
        "type-name": "Custom:MyCustomInventoryType"
    }
}
```

このようなイベントをモニタリングするための EventBridge の設定方法については、「Systems Manager イベント用の EventBridge を設定する」を参照してください。

インベントリ収集の設定

このセクションでは、Systems Manager コンソールを使用して、1 つ以上のマネージドノードで AWS Systems Manager インベントリ収集を設定する方法を説明します。AWS Command Line Interface (AWS CLI) を使用してインベントリ収集を設定する方法の例については、「AWS CLI を使用してインベントリデータ収集を設定する」を参照してください。

インベントリ収集の設定を開始するには、AWS Systems Manager State Manager の関連付けを作成します。関連付けが実行されると、Systems Manager はインベントリデータを収集します。最初に関連付けを作成せずに、AWS Systems Manager Run Command などを使用して `aws:softwareInventory` プラグインを呼び出そうとすると、システムは次のエラーを返します: `The aws:softwareInventory plugin can only be invoked via ssm-associate.`。

> **Note**
>
> マネージドノードに対して複数のインベントリの関連付けを作成する場合は、次の動作に注意してください。
>
> - 各ノードには、すべてのノードをターゲットとするインベントリの関連付けを割り当てることができます (--targets "Key=InstanceIds,Values=*")。
> - 各ノードには、タグキーと値のペアまたは AWS リソースグループを使用する特定の関連付けを割り当てることもできます。
> - ノードに複数のインベントリの関連付けが割り当てられている場合、実行されていない関連付けのステータスは [Skipped] (スキップしました) と表示されます。最後に実行された関連付けには、インベントリの関連付けの実際のステータスが表示されます。

- ノードに複数のインベントリの関連付けが割り当てられ、それぞれにタグのキーと値のペアが使用されている場合、タグの競合により、これらのインベントリの関連付けはノードで実行できません。関連付けは、タグのキーと値の競合がないノードで実行されます。

開始する前に

インベントリ収集を設定する前に、以下のタスクを完了します。

- インベントリするノードで AWS Systems Manager SSM Agent を更新します。最新バージョンの SSM Agent を実行することで、すべてのサポートされるインベントリタイプのメタデータを収集することを確保できます。State Manager を使用して SSM Agent を更新する方法については、「チュートリアル: AWS CLI で SSM Agent を自動的に更新する」を参照してください。
- ハイブリッドおよびマルチクラウド環境で、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスと非 EC2 マシンのセットアップ要件を完了していることを確認します。詳細については、「AWS Systems Manager のマネージドノードのセットアップ」を参照してください。
- Microsoft Windows ノードの場合は、マネージドノードが Windows PowerShell 3.0 (またはそれ以降) で構成されていることを確認します。SSM Agentは、PowerShell で `ConvertTo-Json` cmdlet を使用して、Windows 更新プログラムのインベントリデータを必要な形式に変換します。
- (オプション) リソースデータの同期を作成して、Amazon S3 バケットにインベントリデータを一元的に格納します。その後、リソースデータの同期により、新しいインベントリデータが収集されると一元化されたデータが自動的に更新されます。詳細については、「チュートリアル: リソースデータの同期を使用してインベントリデータを集計する」を参照してください。
- (オプション) カスタムインベントリを収集するための JSON ファイルを作成します。詳細については、「カスタムインベントリの操作」を参照してください。

AWS アカウント のすべてのマネージドイノードインベントリする

グローバルなインベントリの関連付けを作成することで、AWS アカウント のすべてのマネージドノードをインベントリできます。グローバルなインベントリの関連付けでは、以下のアクションを実行します。

- AWS アカウント 内のすべての既存のマネージドノードに、グローバルインベントリ設定 (関連付け) を自動的に適用します。インベントリの関連付けが既に存在するマネージドノードは、グローバルなインベントリの関連付けが適用されて実行されると、スキップされます。ノードがスキップされると、詳細なステータスメッセージとして `Overridden By Explicit Inventory`

`Association` と表示されます。これらのノードは、グローバルな関連付けではスキップされても、割り当てられたインベントリの関連付けを実行したときに、依然としてインベントリを報告します。

- AWS アカウント で作成された新しいノードをグローバルなインベントリの関連付けに自動的に追加します。

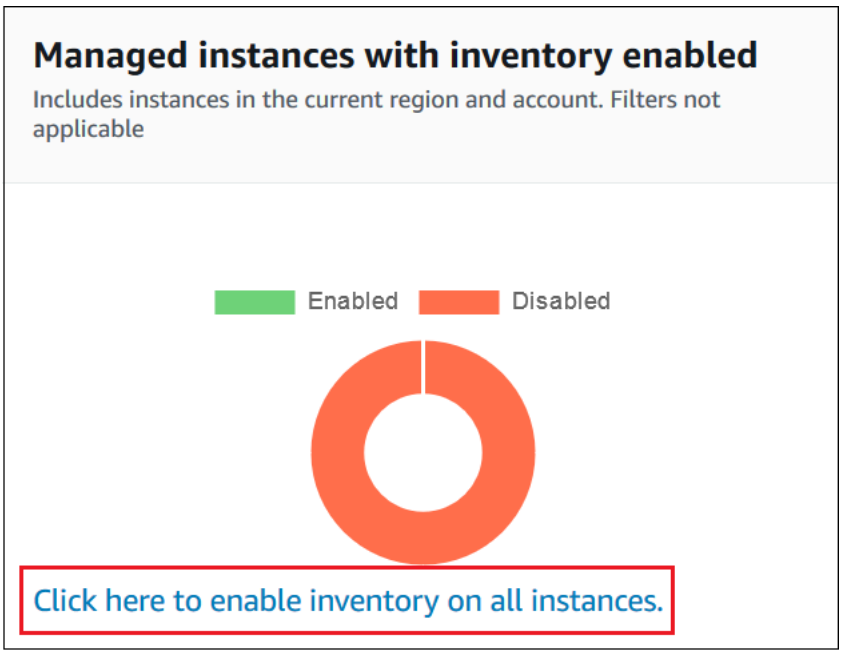
> **Note**
>
> - グローバルなインベントリの関連付けが設定されているマネージドノードに特定の関連付けを割り当てると、Systems Manager Inventory はグローバルな関連付けの優先順位付けを解除して、特定の関連付けを適用します。
> - グローバルなインベントリの関連付けは、SSM Agent バージョン 2.0.790.0 以降で使用できます。ノードで SSM Agent を更新する方法については、「Run Command を使用して SSM Agent を更新する」を参照してください。

1-Click を使用したインベントリ収集の設定 (コンソール)

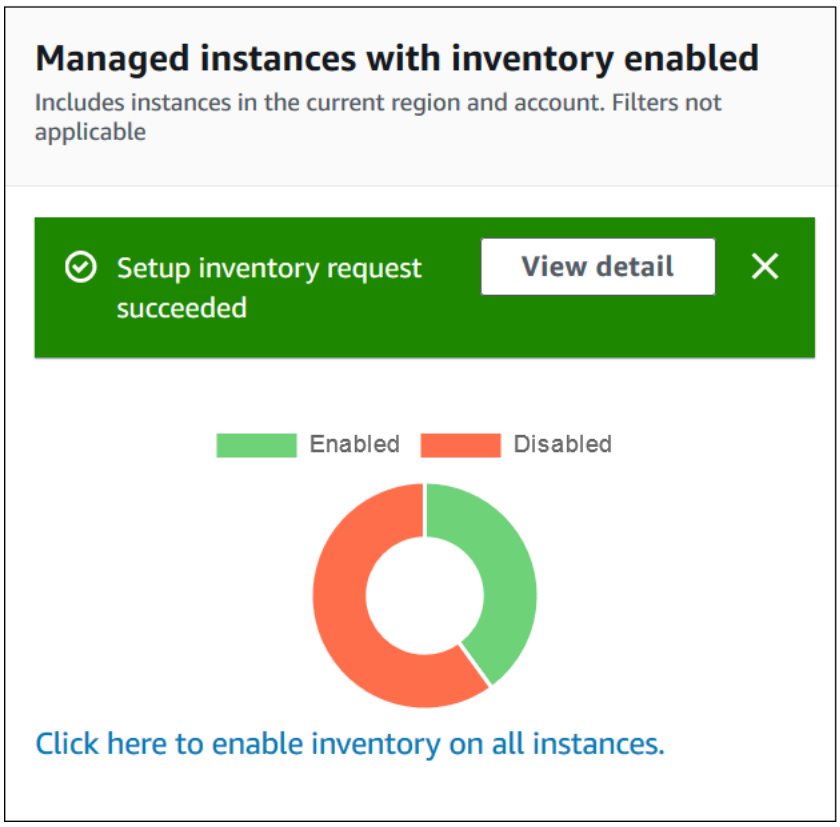
次の手順を使用して、AWS アカウント および単一の AWS リージョン 内のすべてのマネージドノードについて、Systems Manager Inventory を設定します。

現在のリージョン内のすべてのマネージドノードを Systems Manager インベントリ用に設定するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[インベントリ] を選択します。
3. [Managed instances with inventory enabled (インベントリが有効化されているマネージドインスタンス)] カードで、[Click here to enable inventory on all instances (すべてのインスタンスでインベントリを有効にするにはここをクリック)] を選択します。



成功した場合、コンソールに次のメッセージが表示されます。



アカウント内のマネージドノードの数によっては、グローバルインベントリの関連付けが適用されるまでに数分かかる場合があります。数分間待ってから、ページを更新します。グラフィック

が変化して、インベントリがすべてのマネージドノードで設定されたことが反映されることを確認します。

コンソールを使用した収集の設定

このセクションでは、Systems Manager コンソールを使用して、マネージドノードからメタデータを収集するために Systems Manager Inventory を設定する方法について説明します。特定の AWS アカウント にあるすべてのノード (およびそのアカウントで作成される可能性のある将来のノード) から迅速にメタデータを収集できます。またはタグまたはノード ID を使用してインベントリデータを選択して収集できます。

> **Note**
>
> この手順を完了する前に、グローバルなインベントリの関連付けが既に存在しているかどうかを確認してください。グローバルなインベントリの関連付けが既に存在する場合、新しいインスタンスを起動するたびに、その関連付けがそのインスタンスに適用され、新しいインスタンスがインベントリされます。

インベントリ収集を設定するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[インベントリ] を選択します。
3. [Setup Inventory] を選択します。
4. [Targets] (ターゲット) セクションで、以下のいずれかを選択して、このオペレーションを実行するノードを指定します。

   - Selecting all managed instances in this account (このアカウントのすべてのマネージドインスタンスを選択) - このオプションでは、既存のインベントリの関連付けがないすべてのマネージドノードを選択します。このオプションを選択すると、インスタンスの関連付けが既に存在するノードはインベントリ収集時にスキップされ、インベントリ結果にステータスとして [Skipped] (スキップ) と表示されます。詳細については、「AWS アカウント のすべてのマネージドイノードインベントリする」を参照してください。
   - タグの指定 – このオプションを使用すると、インベントリを収集するアカウント内のノードを識別するために 1 つのタグを指定できます。タグを使用すると、以後同じタグで作成されたすべてのノードからインベントリが報告されます。すべてのノードに既存のインベントリの

関連付けがある場合、タグを使用して別のインベントリのターゲットとして特定のノードを選択すると、[All managed instances] (すべてのマネージドインスタンス) ターゲットグループのノードメンバーシップが上書きされます。指定したタグのマネージドノードは、[All managed instances] (すべてのマネージドインスタンス) からのインベントリ収集でスキップされます。

- インスタンスの手動選択 – このオプションを使用すると、アカウントの特定のマネージドノードを選択できます。このオプションを使用して特定のノードを明示的に選択すると、[All managed instances] (すべてのマネージドインスタンス) のインベントリの関連付けが上書きされます。ノードは、[All managed instances] (すべてのマネージドインスタンス) からのインベントリ収集でスキップされます。

> **Note**
>
> 表示されるはずのマネージドノードが表示されない場合は、トラブルシューティングのヒントについて「マネージドノードの可用性のトラブルシューティング」を参照してください。

5. [Schedule] (スケジュール) セクションで、ノードからインベントリメタデータを収集する頻度を選択します。
6. [Parameters] セクションで、リストを使用してさまざまなタイプのインベントリ収集を有効または無効にします。ファイルと Windows レジストリインベントリの収集についての詳細は、「ファイルと Windows レジストリインベントリで作業する」を参照してください。
7. 関連付けの実行ステータスを Amazon S3 バケットに保存する場合は、[詳細] セクションで [Sync inventory execution logs to an Amazon S3 bucket (Amazon S3 バケットにインベントリ実行ログを同期する)] を選択します。
8. [Setup Inventory] を選択します。Systems Manager は、State Manager の関連付けを作成し、ノードで Inventory を直ちに実行します。
9. ナビゲーションペインで、State Manager を選択します。**AWS-GatherSoftwareInventory** ドキュメントを使用する新しい関連付けが作成されたことを確認します。関連付けスケジュールでは、レート式が使用されます。また、[Status] フィールドに [Success] と表示されていることを確認します。オプションとして [インベントリ実行ログを Amazon S3 バケットに同期する] を選択すると、数分後にログデータが Amazon S3 に表示されます。特定のノードのインベントリデータを表示するには、ナビゲーションペインで [Managed Instances] (マネージドインスタンス) を選択します。
10. ノードを選択し、[View details] (詳細を表示) を選択します。
11. ノードの詳細ページで [Inventory] (インベントリ) を選択します。[Inventory type] のリストを使用してインベントリをフィルタします。

複数のリージョンとアカウントからのインベントリデータをクエリする

AWS Systems Manager インベントリは Amazon Athena と統合され、複数の AWS リージョン および AWS アカウント からのインベントリデータをクエリするのに役立ちます。Athena 統合では、リソースデータ同期が使用されるため、AWS Systems Manager コンソールの [Detailed View] (詳細ビュー) ページで、すべてのマネージドノードのインベントリデータを表示できます。

> **Important**
>
> この機能は、AWS Glue を使用して Amazon Simple Storage Service (Amazon S3) バケット内のデータをクロールし、Amazon Athena を使用してデータをクエリします。クロールおよびクエリされたデータ量に応じて、これらのサービスの使用に対して課金されます。AWS Glue を使用すると、クローラ (データの検出) と ETL ジョブ (データの処理とロード) に対して時間あたりの料金が秒単位で課金されます。Athena を使用すると、各クエリでスキャンされるデータ量に基づいて課金されます。Amazon Athena と Systems Manager Inventory の統合を使用する前に、これらのサービスの料金ガイドラインを確認することをお勧めします。詳細については、「Amazon Athena の料金」および「AWS Glue 料金」を参照してください。

Amazon Athena を利用できるすべての AWS リージョン の [Detail View (詳細ビュー)] ページでインベントリデータを表示できます。サポートされているリージョンのリストについては、「Amazon Web Services 全般のリファレンス」の「Amazon Athena サービスエンドポイント」を参照してください。

[開始する前に]

Athena 統合は、リソースデータ同期を使用します。この機能を使用するには、リソースデータ同期をセットアップし、設定する必要があります。詳細については、「チュートリアル: リソースデータの同期を使用してインベントリデータを集計する」を参照してください。

また、[Detail View (詳細ビュー)] ページには、リソースデータ同期によって使用される中央 Amazon S3 バケットの所有者のインベントリデータが表示されることに注意してください。中央 Amazon S3 バケットの所有者でない場合は、Detail View (詳細ビュー) ページにインベントリデータは表示されません。

アクセス設定

Systems Manager コンソールの [詳細ビュー] ページで複数のアカウントおよびリージョンからのデータをクエリおよび表示するには、データを表示するアクセス許可を持つよう IAM エンティティを設定する必要があります。

オプションで、AWS Key Management Service (AWS KMS) 暗号化を使用する Amazon S3 バケットにインベントリデータが保存されている場合は、AWS KMS の暗号化が可能になるように IAM エンティティと `Amazon-GlueServiceRoleForSSM` サービスロールを設定する必要があります。

トピック

- [詳細ビュー] ページにアクセスできるよう IAM ユーザーアカウントを設定
- （オプション）AWS KMS 暗号化データを表示できるようアクセス許可を設定する

[詳細ビュー] ページにアクセスできるよう IAM ユーザーアカウントを設定

以下に、[詳細表示] ページでインベントリデータを表示するために必要な最低限の権限について説明します。

`AWSQuicksightAthenaAccess` マネージドポリシー

以下の `PassRole` およびその他の必要なアクセス許可ブロック

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowGlue",
            "Effect": "Allow",
            "Action": [
                "glue:GetCrawler",
                "glue:GetCrawlers",
                "glue:GetTables",
                "glue:StartCrawler",
                "glue:CreateCrawler"
            ],
            "Resource": "*"
        },
        {
            "Sid": "iamPassRole",
            "Effect": "Allow",
```

```
            "Action": "iam:PassRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "glue.amazonaws.com"
                }
            }
        },
        {
            "Sid": "iamRoleCreation",
           "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
                "iam:AttachRolePolicy"
            ],
            "Resource": "arn:aws:iam::account_ID:role/*"
        },
        {
            "Sid": "iamPolicyCreation",
            "Effect": "Allow",
            "Action": "iam:CreatePolicy",
            "Resource": "arn:aws:iam::account_ID:policy/*"
        }
    ]
}
```

(オプション) インベントリデータの保存に使用される Amazon S3 バケットが AWS KMS を使用して暗号化されている場合は、以下のブロックもポリシーに追加する必要があります。

```
{
    "Effect": "Allow",
    "Action": [
        "kms:Decrypt"
    ],
    "Resource": [
        "arn:aws:kms:Region:account_ID:key/key_ARN"
    ]
}
```

アクセス権限を付与するにはユーザー、グループ、またはロールにアクセス許可を追加します。

- AWS IAM Identity Center のユーザーとグループ:

アクセス許可セットを作成します。「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」の手順に従ってください。

- IAM 内で、ID プロバイダーによって管理されているユーザー:

  ID フェデレーションのロールを作成します。詳細については「IAM ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) 用のロールを作成する」を参照してください。

- IAM ユーザー:
  - ユーザーが担当できるロールを作成します。手順については「IAM ユーザーガイド」の「IAM ユーザーのロールの作成」を参照してください。
  - (お奨めできない方法) ポリシーをユーザーに直接アタッチするか、ユーザーをユーザーグループに追加します。詳細については「IAM ユーザーガイド」の「ユーザー (コンソール) へのアクセス権限の追加」を参照してください。

(オプション) AWS KMS 暗号化データを表示できるようアクセス許可を設定する

インベントリデータの保存に使用される Amazon S3 バケットが AWS Key Management Service (AWS KMS) で暗号化されている場合は、AWS KMS キーの `kms:Decrypt` アクセス許可で IAM エンティティと [Amazon-GlueServiceRoleForSSM] ロールを設定する必要があります。

[開始する前に]

AWS KMS キーに `kms:Decrypt` アクセス許可を与えるには、以下のポリシーブロックを IAM エンティティに追加します。

```
{
    "Effect": "Allow",
    "Action": [
        "kms:Decrypt"
    ],
    "Resource": [
        "arn:aws:kms:Region:account_ID:key/key_ARN"
    ]
}
```

まだ手順を完了していない場合は、手順に従い、AWS KMS キーの `kms:Decrypt` アクセス許可を追加してください。

以下の手順に従って、AWS KMS キーの `kms:Decrypt` アクセス許可で Amazon-GlueServiceRoleForSSM ロールを設定します。

Amazon-GlueServiceRoleForSSM ロールを **`kms:Decrypt`** アクセス許可で設定するには

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. ナビゲーションペインで、[Roles (ロール)] を選択します。検索フィールドを使用して Amazon-GlueServiceRoleForSSM ロールを見つけます。概要 ページが開きます。
3. 検索フィールドを使用して、Amazon-GlueServiceRoleForSSM ロールを見つけます。ロール名を選択します。概要 ページが開きます。
4. ロール名 を選択します。概要 ページが開きます。
5. [Add inline policy] (インラインポリシーの追加) を選択します。[Create policy (ポリシーの作成)] ページが開きます。
6. [JSON] タブを選択します。
7. エディタで既存の JSON テキストを削除し、以下のポリシーを JSON エディタにコピーして貼り付けます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": [
                "arn:aws:kms:Region:account_ID:key/key_ARN"
            ]
        }
    ]
}
```

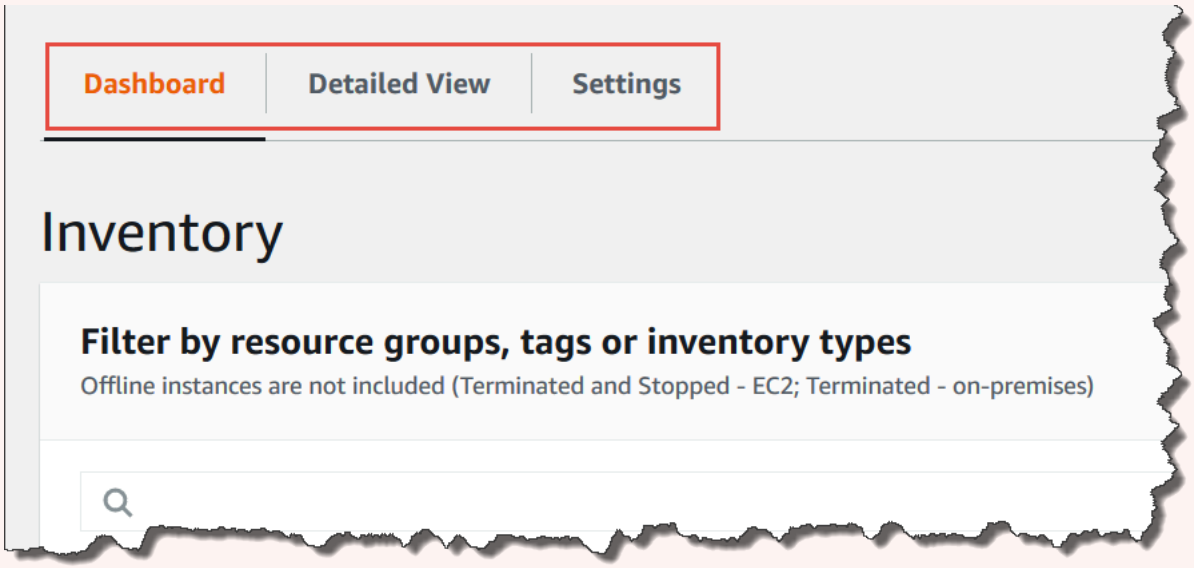
8. [Review policy] (ポリシーの確認) を選択します。
9. [Review Policy (ポリシーの確認)] ページで、[Name (名前)] フィールドに名前を入力します。
10. [Create policy] を選択します。

インベントリの [Detailed View (詳細ビュー)] ページでのデータの照会

Systems Manager Inventory の [Detailed View (詳細ビュー)] ページで複数の AWS リージョン と AWS アカウント のインベントリデータを表示するには、次の手順を使用します。

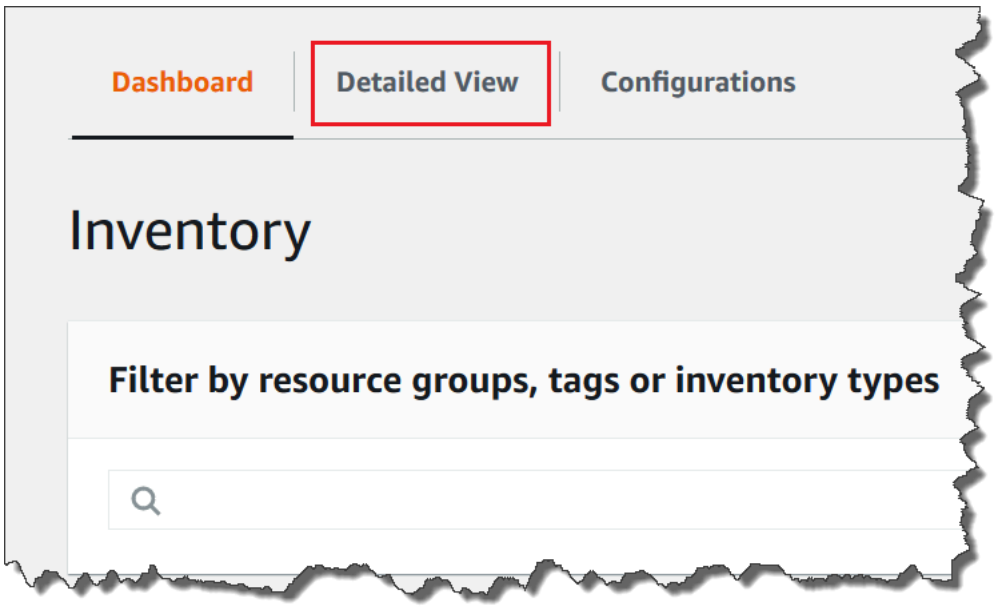
Important

Inventory の [Detailed View (詳細ビュー)] ページは、Amazon Athena を提供する AWS リージョン でのみ利用できます。以下のタブが [Systems Manager Inventory] ページに表示されない場合は、Athena はリージョンで利用できず、データのクエリに [Detailed View (詳細ビュー)] を使用できないことを意味します。

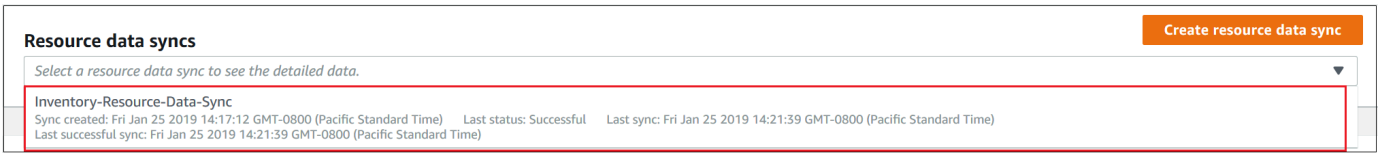


AWS Systems Manager コンソールで複数のリージョンとアカウントのインベントリデータを表示するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[インベントリ] を選択します。
3. [Detailed View (詳細ビュー)] タブを選択します。

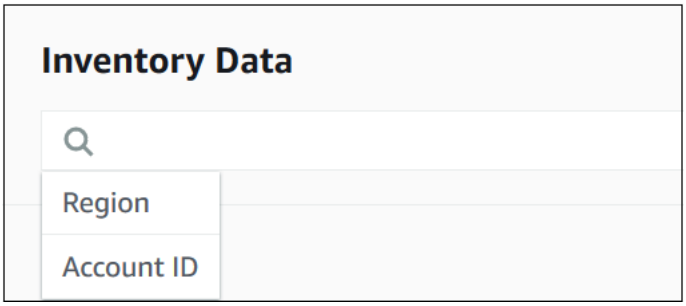


4. データをクエリするリソースデータ同期を選択します。



5. [Inventory Type (インベントリタイプ)] リストで、クエリするインベントリデータのタイプを選択して、Enter キーを押します。

6. データをフィルタリングするには、フィルタバーを選択し、フィルタオプションを選択します。



[Export to CSV (CSV へエクスポート)] ボタンを使用して、Microsoft Excel などのスプレッドシートアプリケーションで現在のクエリセットを表示できます。また、[Query History (クエリ履歴)]

および [Run Advanced Queries (高度なクエリの実行)] ボタンを使用して、履歴の詳細を表示したり、Amazon Athena でデータと通信したりすることができます。

AWS Glue クローラスケジュールの編集

AWS Glue は、デフォルトで毎日 2 回、中央 Amazon S3 バケットのインベントリデータをクロールします。ノードで収集するデータのタイプを頻繁に変更する場合は、次の手順で説明するように、より頻繁にデータをクロールすることをお勧めします。

> **Important**
>
> AWS Glue は、クローラ (データの検出) と ETL ジョブ (データの処理とロード) に対して時間あたりの料金が秒単位で AWS アカウント に課金されます。クローラスケジュールを変更する前に、「AWS Glue 料金表」ページを参照してください。

インベントリデータクローラのスケジュールを変更するには

1. https://console.aws.amazon.com/glue/ で AWS Glue コンソール を開きます。
2. ナビゲーションペインで、[Crawlers (クローラ)] を選択します。
3. クローラリストで、Systems Manager Inventory データクローラの横にあるオプションを選択します。クローラ名は、次の形式を使用します。

   `AWSSystemsManager-`*`s3-bucket-name`*`-`*`Region`*`-`*`account_ID`*
4. [Actions (アクション)] を選択して、[Edit crawler (クローラの編集)] を選択します。
5. ナビゲーションペインで、[Schedule (スケジュール)] を選択します。
6. [Cron expression (Cron 式)] フィールドで、cron 形式を使用して新しいスケジュールを指定します。cron 形式の詳細については、AWS Glue デベロッパーガイドの「ジョブとクローラの時間ベースのスケジュール」を参照してください。

> **Important**
>
> クローラを一時停止して、 に対する料金の発生を停止できますAWS Glue クローラを一時停止した場合、またはデータのクロールの頻度が低くなるように頻度を変更した場合は、インベントリの [Detailed View (詳細ビュー)] に、最新ではないデータが表示されることがあります。

フィルターを使用したインベントリ収集のクエリ

インベントリデータを収集したら、AWS Systems Manager のフィルター機能を使用して特定のフィルター基準を満たすマネージドノードのリストをクエリできます。

インベントリフィルターに基づいてノードをクエリするには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[インベントリ] を選択します。
3. [Filter by resource groups, tags or inventory types] セクションで、フィルタボックスを選択します。定義済みフィルタが一覧表示されます。
4. フィルターを適用する属性を選択します。例えば、[**AWS:Application**] を選択します。指示が表示されたら、フィルターを適用する 2 番目の属性を選択します。例えば、[**AWS:Application.Name**] を選択します。
5. リストから区切り記号を選択します。たとえば、[Begin with] を選択します。フィルタにテキストボックスが表示されます。
6. テキストボックスに値を入力します。たとえば、「Amazon」と入力します (SSM Agent の名前は Amazon SSM Agent)。
7. Enter キーを押します。システムから、Amazon で始まるアプリケーション名を含むマネージドノードのリストが返されます。

> **Note**
>
> 複数のフィルターを組み合わせて検索を絞り込むことができます。

インベントリデータの集計

AWS Systems Manager インベントリのマネージドノードを設定した後、インベントリデータの集計カウントを表示できます。例えば、数十または数百のマネージドノードで `AWS:Application` インベントリタイプを収集するように設定されている場合を考えます。このセクションの情報を使用することで、このデータを収集するように設定されているノードの数を正確に把握できます。

データ型で集計することで、特定のインベントリの詳細を確認することもできます。例えば、`AWS:InstanceInformation` インベントリタイプは、`Platform` データ型とオペレーティングシステムのプラットフォーム情報を収集します。`Platform` データ型でデータを集計すること

で、Windows を実行するノードの数、Linux を実行するノードの数、macOS を実行するノードの数を速やかに確認できます。

このセクションの手順では、AWS Command Line Interface (AWS CLI) を使用して、集計されたインベントリデータ数を表示する方法について説明します。AWS Systems Manager コンソールの [インベントリ] ページで、事前設定された集計カウントを表示することもできます。これらの事前設定されたダッシュボードは、インベントリインサイトと呼ばれ、インベントリ設定の問題を 1 クリックで修復する機能が用意されています。

インベントリデータの集計カウントに関する以下の重要な詳細情報に注意してください。

- インベントリデータを収集するように設定されたマネージドノードを終了すると、Systems Manager はインベントリデータを 30 日間保持し、その後削除します。実行中のノードの場合、システムは 30 日以上経過した古いインベントリデータを削除します。インベントリデータを 30 日以上保存する必要がある場合は、AWS Config を使用して履歴を記録したり、データを定期的にクエリして Amazon Simple Storage Service (Amazon S3) バケットにアップロードしたりできます。
- 以前に特定のインベントリデータタイプ (`AWS:Network` など) をレポートするようにノードが設定されていて、後で設定を変更し、そのタイプの収集を停止する場合は、ノードが終了し 30 日間が経過するまで、集計カウントに `AWS:Network` データが表示されます。

特定の AWS アカウント のすべてのノード (およびそのアカウントで作成される可能性がある将来のノード) に対してインベントリデータを迅速に設定および収集する方法については、「AWS アカウント のすべてのマネージドイノードインベントリする」を参照してください。

トピック

- 特定のタイプのデータを収集するノードのカウントを表示するためのインベントリデータの集計
- インベントリタイプを収集するように設定されている/設定されていないノードを確認するためのグループによるインベントリデータの集計

特定のタイプのデータを収集するノードのカウントを表示するためのインベントリデータの集計

AWS Systems Manager GetInventory API オペレーションを使用して、1 つ以上のインベントリタイプとデータ型を収集するノードの集計数を表示できます。例えば、`AWS:InstanceInformation` インベントリタイプでは、GetInventory API オペレーションで `AWS:InstanceInformation.PlatformType` データ型を使用することにより、オペレーティングシステムの集計を表示できます。AWS CLI コマンドの例と出力を次に示します。

```
aws ssm get-inventory --aggregators "Expression=AWS:InstanceInformation.PlatformType"
```

システムが以下のような情報をレスポンスします。

```
{
   "Entities":[
      {
         "Data":{
            "AWS:InstanceInformation":{
               "Content":[
                  {
                     "Count":"7",
                     "PlatformType":"windows"
                  },
                  {
                     "Count":"5",
                     "PlatformType":"linux"
                  }
               ]
            }
         }
      }
   ]
}
```

開始方法

カウントを表示するインベントリタイプとデータ型を決定します。AWS CLI で次のコマンドを実行して、集計をサポートするインベントリタイプとデータ型のリストを表示できます。

```
aws ssm get-inventory-schema --aggregator
```

このコマンドは、集計をサポートするデータ型とインベントリタイプの JSON リストを返します。[TypeName] フィールドには、サポートされているインベントリタイプが表示されます。また、[Name (名前)] フィールドに各データ型が表示されます。例えば、次のリストでは、AWS:Application インベントリタイプには Name および Version データ型が含まれています。

```
{
    "Schemas": [
        {
```

```
            "TypeName": "AWS:Application",
            "Version": "1.1",
            "DisplayName": "Application",
            "Attributes": [
                {
                    "DataType": "STRING",
                    "Name": "Name"
                },
                {
                    "DataType": "STRING",
                    "Name": "Version"
                }
            ]
        },
        {
            "TypeName": "AWS:InstanceInformation",
            "Version": "1.0",
            "DisplayName": "Platform",
            "Attributes": [
                {
                    "DataType": "STRING",
                    "Name": "PlatformName"
                },
                {
                    "DataType": "STRING",
                    "Name": "PlatformType"
                },
                {
                    "DataType": "STRING",
                    "Name": "PlatformVersion"
                }
            ]
        },
        {
            "TypeName": "AWS:ResourceGroup",
            "Version": "1.0",
            "DisplayName": "ResourceGroup",
            "Attributes": [
                {
                    "DataType": "STRING",
                    "Name": "Name"
                }
            ]
        },
```

```
        {
            "TypeName": "AWS:Service",
            "Version": "1.0",
            "DisplayName": "Service",
            "Attributes": [
                {
                    "DataType": "STRING",
                    "Name": "Name"
                },
                {
                    "DataType": "STRING",
                    "Name": "DisplayName"
                },
                {
                    "DataType": "STRING",
                    "Name": "ServiceType"
                },
                {
                    "DataType": "STRING",
                    "Name": "Status"
                },
                {
                    "DataType": "STRING",
                    "Name": "StartType"
                }
            ]
        },
        {
            "TypeName": "AWS:WindowsRole",
            "Version": "1.0",
            "DisplayName": "WindowsRole",
            "Attributes": [
                {
                    "DataType": "STRING",
                    "Name": "Name"
                },
                {
                    "DataType": "STRING",
                    "Name": "DisplayName"
                },
                {
                    "DataType": "STRING",
                    "Name": "FeatureType"
                },
```

```
                {
                    "DataType": "STRING",
                    "Name": "Installed"
                }
            ]
        }
    ]
}
```

次の構文を使用するコマンドを作成することで、リストされているインベントリタイプのいずれかのデータを集計できます。

```
aws ssm get-inventory --aggregators "Expression=InventoryType.DataType"
```

次に例を示します。

例 1

この例では、ノードによって使用される Windows ロールの数を集計します。

```
aws ssm get-inventory --aggregators "Expression=AWS:WindowsRole.Name"
```

例 2

この例では、ノードにインストールされているアプリケーション数を集計します。

```
aws ssm get-inventory --aggregators "Expression=AWS:Application.Name"
```

複数のアグリゲータの結合

データをさらによく理解できるように、1 つのコマンドで複数のインベントリタイプとデータ型を組み合わせることもできます。次に例を示します。

例 1

この例では、ノードによって使用されるオペレーティングシステムのタイプ数を集計します。また、オペレーティングシステムの個別の名前も返します。

```
aws ssm get-inventory --aggregators '[{"Expression":
 "AWS:InstanceInformation.PlatformType", "Aggregators":[{"Expression":
 "AWS:InstanceInformation.PlatformName"}]}]'
```

例 2

この例では、各アプリケーションの特定のバージョンとノードで実行されているアプリケーションの数を集計します。

```
aws ssm get-inventory --aggregators '[{"Expression": "AWS:Application.Name",
 "Aggregators":[{"Expression": "AWS:Application.Version"}]}]'
```

必要に応じて、JSON ファイルの 1 つまたは複数のインベントリタイプとデータ型に対する集計式を作成し、AWS CLI からファイルを呼び出すことができます。ファイルの JSON には次の構文を使用する必要があります。

```
[
       {
           "Expression": "string",
           "Aggregators": [
               {
                  "Expression": "string"
               }
           ]
       }
]
```

.json 拡張子でファイルを保存する必要があります。

複数のインベントリタイプとデータ型を使用する例を次に示します。

```
[
       {
           "Expression": "AWS:Application.Name",
           "Aggregators": [
               {
                   "Expression": "AWS:Application.Version",
                   "Aggregators": [
                     {
                     "Expression": "AWS:InstanceInformation.PlatformType"
                     }
                   ]
               }
           ]
       }
```

```
]
```

次のコマンドを使用して AWS CLI からファイルを呼び出します。

```
aws ssm get-inventory --aggregators file://file_name.json
```

このコマンドによって以下のような情報が返されます。

```
{"Entities":
 [
   {"Data":
     {"AWS:Application":
       {"Content":
         [
           {"Count": "3",
            "PlatformType": "linux",
            "Version": "2.6.5",
            "Name": "audit-libs"},
           {"Count": "2",
            "PlatformType": "windows",
            "Version": "2.6.5",
            "Name": "audit-libs"},
           {"Count": "4",
            "PlatformType": "windows",
            "Version": "6.2.8",
            "Name": "microsoft office"},
           {"Count": "2",
            "PlatformType": "windows",
            "Version": "2.6.5",
            "Name": "chrome"},
           {"Count": "1",
            "PlatformType": "linux",
            "Version": "2.6.5",
            "Name": "chrome"},
           {"Count": "2",
            "PlatformType": "linux",
            "Version": "6.3",
            "Name": "authconfig"}
         ]
       }
     },
    "ResourceType": "ManagedInstance"}
 ]
```

```
}
```

インベントリタイプを収集するように設定されている/設定されていないノードを確認するためのグループによるインベントリデータの集計

Systems Manager Inventory のグループを使用すると、1 つ以上のインベントリタイプを収集するように設定されている/設定されていないマネージドノードのカウントを迅速に確認できます。グループを使用して、exists オペレータを使用するフィルタと 1 つ以上のインベントリタイプを指定します。

たとえば、以下のインベントリタイプを収集するように設定されている 4 つのマネージドノードがある場合を考えます。

- ノード 1: AWS:Application
- ノード 2: AWS:File
- ノード 3: AWS:Application、AWS:File
- ノード 4: AWS:Network

AWS CLI から次のコマンドを実行して、AWS:Application および AWS:File inventory タイプの両方を収集するように設定されているノードの数を確認できます。レスポンスは、これら両方のインベントリタイプを収集するように設定されていないノードの数も返します。

```
aws ssm get-inventory --aggregators
 'Groups=[{Name=ApplicationAndFile,Filters=[{Key=TypeName,Values=[AWS:Application],Type=Exists}
{Key=TypeName,Values=[AWS:File],Type=Exists}]}]'
```

このコマンドのレスポンスでは、AWS:Application および AWS:File インベントリタイプの両方を収集するように設定されているマネージドノードは 1 つのみであること表しています。

```
{
   "Entities":[
      {
         "Data":{
            "ApplicationAndFile":{
               "Content":[
                  {
                     "notMatchingCount":"3"
                  },
```

```
                {
                   "matchingCount":"1"
                }
             ]
          }
       }
    }
 ]
}
```

> **Note**
>
> グループはデータ型のカウントを返しません。また、インベントリタイプを収集するように設定されているノード ID、または設定されていないノード ID を表示する結果をドリルダウンすることはできません。

必要に応じて、JSON ファイルの 1 つまたは複数のインベントリタイプで集計式を作成し、AWS CLI からファイルを呼び出すことができます。ファイルの JSON には次の構文を使用する必要があります。

```
{
   "Aggregators":[
      {
         "Groups":[
            {
               "Name":"Name",
               "Filters":[
                  {
                     "Key":"TypeName",
                     "Values":[
                        "Inventory_type"
                     ],
                     "Type":"Exists"
                  },
                  {
                     "Key":"TypeName",
                     "Values":[
                        "Inventory_type"
                     ],
                     "Type":"Exists"
                  }
```

```
                ]
            }
         ]
      }
   ]
}
```

.json 拡張子でファイルを保存する必要があります。

次のコマンドを使用して AWS CLI からファイルを呼び出します。

```
aws ssm get-inventory --cli-input-json file://file_name.json
```

その他の例

次の例は、指定されたインベントリタイプを収集するように設定されている/設定されていないマネージドノードを確認するためにインベントリデータを集計する方法を示します。以下の例では、AWS CLI を使用します。それぞれの例には、コマンドラインから実行できるフィルタ付きのフルコマンドと、情報をファイルに入力する場合のサンプル input.json ファイルが含まれています。

例 1

この例では、AWS:Application または AWS:File インベントリタイプを収集するように設定されている/設定されていないノードの数を集計します。

AWS CLI から、次のコマンドを実行します。

```
aws ssm get-inventory --aggregators
 'Groups=[{Name=ApplicationORFile,Filters=[{Key=TypeName,Values=[AWS:Application,
 AWS:File],Type=Exists}]}]'
```

ファイルを使用する場合は、以下のサンプルをコピーしてファイルに貼り付け、input.json ファイルとして保存します。

```
{
   "Aggregators":[
      {
         "Groups":[
            {
               "Name":"ApplicationORFile",
```

```
               "Filters":[
                  {
                     "Key":"TypeName",
                     "Values":[
                        "AWS:Application",
                        "AWS:File"
                     ],
                     "Type":"Exists"
                  }
               ]
            }
         ]
      }
   ]
}
```

AWS CLI から、次のコマンドを実行します。

```
aws ssm get-inventory --cli-input-json file://input.json
```

このコマンドによって以下のような情報が返されます。

```
{
   "Entities":[
      {
         "Data":{
            "ApplicationORFile":{
               "Content":[
                  {
                     "notMatchingCount":"1"
                  },
                  {
                     "matchingCount":"3"
                  }
               ]
            }
         }
      }
   ]
}
```

例 2

この例では、AWS:Application、AWS:File、および AWS:Network インベントリタイプを収集するように設定されているノードとそう設定されていないノードの数を集計します。

AWS CLI から、次のコマンドを実行します。

```
aws ssm get-inventory --aggregators
 'Groups=[{Name=Application,Filters=[{Key=TypeName,Values=[AWS:Application],Type=Exists}]},
 {Name=File,Filters=[{Key=TypeName,Values=[AWS:File],Type=Exists}]},
 {Name=Network,Filters=[{Key=TypeName,Values=[AWS:Network],Type=Exists}]}]'
```

ファイルを使用する場合は、以下のサンプルをコピーしてファイルに貼り付け、input.json ファイルとして保存します。

```
{
   "Aggregators":[
      {
         "Groups":[
            {
               "Name":"Application",
               "Filters":[
                  {
                     "Key":"TypeName",
                     "Values":[
                        "AWS:Application"
                     ],
                     "Type":"Exists"
                  }
               ]
            },
            {
               "Name":"File",
               "Filters":[
                  {
                     "Key":"TypeName",
                     "Values":[
                        "AWS:File"
                     ],
                     "Type":"Exists"
                  }
               ]
            },
            {
               "Name":"Network",
```

```
               "Filters":[
                  {
                     "Key":"TypeName",
                     "Values":[
                        "AWS:Network"
                     ],
                     "Type":"Exists"
                  }
               ]
            }
         ]
      }
   ]
}
```

AWS CLI から、次のコマンドを実行します。

```
aws ssm get-inventory --cli-input-json file://input.json
```

このコマンドによって以下のような情報が返されます。

```
{
   "Entities":[
      {
         "Data":{
            "Application":{
               "Content":[
                  {
                     "notMatchingCount":"2"
                  },
                  {
                     "matchingCount":"2"
                  }
               ]
            },
            "File":{
               "Content":[
                  {
                     "notMatchingCount":"2"
                  },
                  {
                     "matchingCount":"2"
                  }
```

```
            ]
         },
         "Network":{
            "Content":[
               {
                  "notMatchingCount":"3"
               },
               {
                  "matchingCount":"1"
               }
            ]
         }
      }
   ]
}
```

カスタムインベントリの操作

AWS Systems Manager インベントリのカスタムインベントリを作成して、ノードに必要なあらゆるメタデータを割り当てることができます。例えば、データセンターのラック内の多数のサーバーを管理しており、それらのサーバーは Systems Manager マネージドノードとして設定されているとします。現在、サーバーラック位置に関する情報はスプレッドシートに保存しています。カスタムインベントリを使うと、各インスタンスのラック位置をノードのメタデータとして指定できます。Systems Manager を使用してインベントリを収集すると、そのメタデータは他のインベントリメタデータとともに収集されます。その後、リソースデータ同期を使用してすべてのインベントリメタデータを中央 Amazon S3 バケットにポートし、データをクエリできます。

> **Note**
>
> Systems Manager では、 あたり最大 20 のカスタムインベントリタイプをサポートしていますAWS アカウント

カスタムインベントリをノードに割り当てるには、「カスタムインベントリメタデータをマネージドノードに割り当てる」で説明されているように Systems Manager PutInventory API オペレーションを使用できます。または、カスタムインベントリ JSON ファイルを作成し、ノードにアップロードできます。このセクションでは、JSON ファイルを作成する方法について説明します。

カスタムインベントリを含む次の JSON ファイルの例では、オンプレミスサーバーに関するラック情報を指定しています。この例では、1 つのタイプのカスタムインベントリデータ ("TypeName":

"Custom:RackInformation") を指定し、Content の複数のエントリがそのデータを説明します。

```
{
    "SchemaVersion": "1.0",
    "TypeName": "Custom:RackInformation",
    "Content": {
        "Location": "US-EAST-02.CMH.RACK1",
        "InstalledTime": "2016-01-01T01:01:01Z",
        "vendor": "DELL",
        "Zone" : "BJS12",
        "TimeZone": "UTC-8"
      }
 }
```

また、次の例に示すように、Content セクションで異なるエントリを指定することもできます。

```
{
"SchemaVersion": "1.0",
"TypeName": "Custom:PuppetModuleInfo",
    "Content": [{
        "Name": "puppetlabs/aws",
        "Version": "1.0"
      },
      {
        "Name": "puppetlabs/dsc",
        "Version": "2.0"
      }
    ]
}
```

カスタムインベントリ用の JSON スキーマには、SchemaVersion、TypeName、および Content というセクションが必要ですが、これらのセクションの情報を定義できます。

```
{
    "SchemaVersion": "user_defined",
    "TypeName": "Custom:user_defined",
    "Content": {
        "user_defined_attribute1": "user_defined_value1",
        "user_defined_attribute2": "user_defined_value2",
        "user_defined_attribute3": "user_defined_value3",
        "user_defined_attribute4": "user_defined_value4"
```

```
        }
    }
```

TypeName の値は 100 文字に限定されます。また、TypeName 値は大文字の Custom 単語で始まる必要があります。例えば、Custom:PuppetModuleInfo と指定します。そのため、次の例では例外となります:CUSTOM:PuppetModuleInfo、custom:PuppetModuleInfo。

Content セクションには、属性と###を含めます。これらの項目は大文字と小文字は区別されません。ただし、属性 (例: "Vendor": "DELL") を定義する場合、カスタムインベントリファイルで一貫してこの属性を参照する必要があります。あるファイルで "Vendor": "DELL" (vendor の「V」が大文字) と指定した場合、別のファイルで "vendor": "DELL" (vendor の「v」が小文字) と指定すると、システムはエラーを返します。

> **Note**
>
> .json 拡張子を付けてファイルを保存し、定義するインベントリは文字列値のみで構成する必要があります。

ファイルを作成した後、ノードに保存する必要があります。以下の表は、カスタムインベントリの JSON ファイルをノードのどの場所に保存する必要があるかを示します。

オペレーティングシステム	パス
Linux	/var/lib/amazon/ssm/*node-id*/inventory/custom
macOS	/opt/aws/ssm/data/ *node-id*/ inventory/custom
Windows	%SystemDrive%\ProgramData\Amazon\SSM \InstanceData*node-id*\inventory\custom

カスタムインベントリの使用方法の例については、「EC2 Systems Manager カスタムインベントリ型を使用してインスタンスのディスクの利用状況を取得する」を参照してください。

カスタムインベントリの削除

API オペレーションの DeleteInventory を使用して、カスタムインベントリタイプと当該タイプに関連付けられているデータを削除できます。インベントリタイプのすべてのデータを削除するに

は、AWS Command Line Interface (AWS CLI) を使用して delete-inventory コマンドを呼び出します。カスタムインベントリタイプを削除するには、SchemaDeleteOption を使用して delete-inventory コマンドを呼び出します。

> **Note**
>
> インベントリタイプは、インベントリスキーマとも呼ばれます。

SchemaDeleteOption パラメータには次のオプションが含まれます。

- DeleteSchema: このオプションでは、指定したカスタムタイプおよび関連するすべてのデータを削除します。必要に応じて、後でスキーマを再作成できます。
- DisableSchema: このオプションを選択すると、現在のバージョンが無効になり、すべての関連するデータが削除されます。また、無効化したバージョン以下のバージョンでは、すべての新しいデータが無視されます。このインベントリタイプを再度有効にするには、無効になっているバージョンよりも新しいバージョンの PutInventory アクションを呼び出します。

AWS CLI を使用してカスタムインベントリを削除または無効化するには

1. まだ AWS Command Line Interface (AWS CLI) をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」を参照してください。

2. 次のコマンドを実行し、dry-run オプションを使用してシステムから削除されるデータを確認します。このコマンドではデータは削除されません。

   ```
   aws ssm delete-inventory --type-name "Custom:custom_type_name" --dry-run
   ```

   システムが以下のような情報を返します。

   ```
   {
      "DeletionSummary":{
         "RemainingCount":3,
         "SummaryItems":[
            {
               "Count":2,
   ```

```
            "RemainingCount":2,
            "Version":"1.0"
         },
         {
            "Count":1,
            "RemainingCount":1,
            "Version":"2.0"
         }
      ],
      "TotalCount":3
   },
   "TypeName":"Custom:custom_type_name"
}
```

インベントリの削除の要約を理解する方法の詳細については、「インベントリ削除の要約を理解する」を参照してください。

3. カスタムインベントリタイプのすべてのデータを削除するには、次のコマンドを実行します。

```
aws ssm delete-inventory --type-name "Custom:custom_type_name"
```

> **Note**
>
> このコマンドの出力に、削除の進行状況は表示されません。このため、TotalCount および Remaining Count は、システムがまだ何も削除していないため、常に同じです。このトピックの後半で説明するように、describe-inventory-deletions コマンドを使用して、削除の進行状況を表示できます。

システムが以下のような情報を返します。

```
{
   "DeletionId":"system_generated_deletion_ID",
   "DeletionSummary":{
      "RemainingCount":3,
      "SummaryItems":[
         {
            "Count":2,
            "RemainingCount":2,
            "Version":"1.0"
         },
```

```
            {
               "Count":1,
               "RemainingCount":1,
               "Version":"2.0"
            }
         ],
         "TotalCount":3
      },
      "TypeName":"custom_type_name"
}
```

システムは指定されたカスタムインベントリタイプのすべてのデータを Systems Manager Inventory サービスから削除します。

4. 次のコマンドを実行します。このコマンドは、インベントリタイプの現行バージョンに対して次のアクションを実行します。現行バージョンを無効にして、そのすべてのデータを削除し、バージョンが無効にされたバージョン以下の場合はすべての新規データを無視します。

```
aws ssm delete-inventory --type-name "Custom:custom_type_name" --schema-delete-
option "DisableSchema"
```

システムが以下のような情報を返します。

```
{
   "DeletionId":"system_generated_deletion_ID",
   "DeletionSummary":{
      "RemainingCount":3,
      "SummaryItems":[
         {
            "Count":2,
            "RemainingCount":2,
            "Version":"1.0"
         },
         {
            "Count":1,
            "RemainingCount":1,
            "Version":"2.0"
         }
      ],
      "TotalCount":3
   },
   "TypeName":"Custom:custom_type_name"
```

```
}
```

次のコマンドを使用して、無効化されたインベントリタイプを確認できます。

```
aws ssm get-inventory-schema --type-name Custom:custom_type_name
```

5. インベントリタイプを削除するには、以下のコマンドを実行します。

```
aws ssm delete-inventory --type-name "Custom:custom_type_name" --schema-delete-
option "DeleteSchema"
```

システムはスキーマと指定されたカスタムタイプのすべてのデータを削除します。

システムが以下のような情報を返します。

```
{
   "DeletionId":"system_generated_deletion_ID",
   "DeletionSummary":{
      "RemainingCount":3,
      "SummaryItems":[
         {
            "Count":2,
            "RemainingCount":2,
            "Version":"1.0"
         },
         {
            "Count":1,
            "RemainingCount":1,
            "Version":"2.0"
         }
      ],
      "TotalCount":3
   },
   "TypeName":"Custom:custom_type_name"
}
```

削除ステータスの表示

削除オペレーションのステータスは、describe-inventory-deletions AWS CLI コマンドを使用して確認できます。削除 ID を指定して、特定の削除オペレーションを確認できます。または、削除 ID を省略して、過去 30 日間に実行されたすべての削除のリストを表示できます。

1. 以下のコマンドを実行して、削除オペレーションのステータスを表示します。システムは delete-inventory の要約で削除 ID を返します。

```
aws ssm describe-inventory-deletions --deletion-id system_generated_deletion_ID
```

システムは最新のステータスを返します。削除オペレーションがまだ完了しない可能性があります。システムが以下のような情報を返します。

```
{"InventoryDeletions":
  [
    {"DeletionId": "system_generated_deletion_ID",
     "DeletionStartTime": 1521744844,
     "DeletionSummary":
      {"RemainingCount": 1,
       "SummaryItems":
        [
          {"Count": 1,
           "RemainingCount": 1,
           "Version": "1.0"}
        ],
       "TotalCount": 1},
     "LastStatus": "InProgress",
     "LastStatusMessage": "The Delete is in progress",
     "LastStatusUpdateTime": 1521744844,
     "TypeName": "Custom:custom_type_name"}
  ]
}
```

削除オペレーションが成功した場合、LastStatusMessage は削除が成功したことを示します。

```
{"InventoryDeletions":
  [
    {"DeletionId": "system_generated_deletion_ID",
     "DeletionStartTime": 1521744844,
     "DeletionSummary":
      {"RemainingCount": 0,
       "SummaryItems":
        [
          {"Count": 1,
           "RemainingCount": 0,
```

```
            "Version": "1.0"}
         ],
        "TotalCount": 1},
     "LastStatus": "Complete",
     "LastStatusMessage": "Deletion is successful",
     "LastStatusUpdateTime": 1521745253,
     "TypeName": "Custom:custom_type_name"}
  ]
}
```

2. 次のコマンドを実行して、過去 30 日間に実行されたすべての削除のリストを表示します。

```
aws ssm describe-inventory-deletions --max-results a number
```

```
{"InventoryDeletions":
  [
    {"DeletionId": "system_generated_deletion_ID",
     "DeletionStartTime": 1521682552,
     "DeletionSummary":
      {"RemainingCount": 0,
       "SummaryItems":
        [
          {"Count": 1,
           "RemainingCount": 0,
           "Version": "1.0"}
        ],
       "TotalCount": 1},
     "LastStatus": "Complete",
     "LastStatusMessage": "Deletion is successful",
     "LastStatusUpdateTime": 1521682852,
     "TypeName": "Custom:custom_type_name"},
    {"DeletionId": "system_generated_deletion_ID",
     "DeletionStartTime": 1521744844,
     "DeletionSummary":
      {"RemainingCount": 0,
       "SummaryItems":
        [
          {"Count": 1,
           "RemainingCount": 0,
           "Version": "1.0"}
        ],
       "TotalCount": 1},
```

```
      "LastStatus": "Complete",
      "LastStatusMessage": "Deletion is successful",
      "LastStatusUpdateTime": 1521745253,
      "TypeName": "Custom:custom_type_name"},
     {"DeletionId": "system_generated_deletion_ID",
      "DeletionStartTime": 1521680145,
      "DeletionSummary":
       {"RemainingCount": 0,
        "SummaryItems":
         [
           {"Count": 1,
            "RemainingCount": 0,
            "Version": "1.0"}
         ],
        "TotalCount": 1},
      "LastStatus": "Complete",
      "LastStatusMessage": "Deletion is successful",
      "LastStatusUpdateTime": 1521680471,
      "TypeName": "Custom:custom_type_name"}
   ],
  "NextToken": "next-token"
```

インベントリ削除の要約を理解する

インベントリ削除の要約の内容を理解していただくために、次の例を考えてみます。ユーザーは Custom:RackSpace インベントリを 3 つのノードに割り当てています。インベントリ項目 1 および 2 はカスタムタイプのバージョン 1.0 ("SchemaVersion":"1.0") を使用します。インベントリ項目 3 はカスタムタイプのバージョン 2.0 ("SchemaVersion":"2.0") を使用します。

RackSpace カスタムインベントリ 1

```
{
   "CaptureTime":"2018-02-19T10:48:55Z",
   "TypeName":"CustomType:RackSpace",
   "InstanceId":"i-1234567890",
   "SchemaVersion":"1.0"   "Content":[
      {
         content of custom type omitted
      }
   ]
}
```

RackSpace カスタムインベントリ 2

```
{
   "CaptureTime":"2018-02-19T10:48:55Z",
   "TypeName":"CustomType:RackSpace",
   "InstanceId":"i-1234567891",
   "SchemaVersion":"1.0"   "Content":[
      {
         content of custom type omitted
      }
   ]
}
```

RackSpace カスタムインベントリ 3

```
{
   "CaptureTime":"2018-02-19T10:48:55Z",
   "TypeName":"CustomType:RackSpace",
   "InstanceId":"i-1234567892",
   "SchemaVersion":"2.0"   "Content":[
      {
         content of custom type omitted
      }
   ]
}
```

ユーザーは次のコマンドを実行して削除されるデータをプレビューできます。

```
aws ssm delete-inventory --type-name "Custom:RackSpace" --dry-run
```

システムが以下のような情報を返します。

```
{
   "DeletionId":"1111-2222-333-444-66666",
   "DeletionSummary":{
      "RemainingCount":3,
      "TotalCount":3,
                TotalCount and RemainingCount are the number of items that would be
 deleted if this was not a dry run. These numbers are the same because the system
 didn't delete anything.
      "SummaryItems":[
```

```
         {
            "Count":2,             The system found two items that use SchemaVersion
 1.0. Neither item was deleted.
            "RemainingCount":2,
            "Version":"1.0"
         },
         {
            "Count":1,             The system found one item that uses SchemaVersion
 1.0. This item was not deleted.
            "RemainingCount":1,
            "Version":"2.0"
         }
      ],

   },
   "TypeName":"Custom:RackSpace"
}
```

ユーザーは次のコマンドを実行して Custom:RackSpace インベントリを削除します。

> **Note**
>
> このコマンドの出力に、削除の進行状況は表示されません。このため、TotalCount および RemainingCount は、システムがまだ何も削除していないため、常に同じです。describe-inventory-deletions コマンドを実行して、削除の進行状況を表示します。

```
aws ssm delete-inventory --type-name "Custom:RackSpace"
```

システムが以下のような情報をレスポンスします。

```
{
   "DeletionId":"1111-2222-333-444-7777777",
   "DeletionSummary":{
      "RemainingCount":3,           There are three items to delete
      "SummaryItems":[
         {
            "Count":2,             The system found two items that use SchemaVersion
 1.0.
            "RemainingCount":2,
```

```
            "Version":"1.0"
         },
         {
            "Count":1,              The system found one item that uses SchemaVersion
 2.0.
            "RemainingCount":1,
            "Version":"2.0"
         }
      ],
      "TotalCount":3
   },
   "TypeName":"RackSpace"
}
```

EventBridge でインベントリ削除アクションを表示する

ユーザーがカスタムインベントリを削除するときはいつでもイベントを作成するように Amazon EventBridge を設定できます。EventBridge には、カスタムインベントリの削除オペレーションに対して、次の 3 種類のイベントが用意されています。

- インスタンスの削除アクション: 特定のマネージドノードのカスタムインベントリが正常に削除されたかどうか。
- 削除アクションの概要: 削除アクションの概要。
- 無効にされたカスタムインベントリタイプの警告: 以前に無効にされたカスタムインベントリタイプバージョンの PutInventory API オペレーションをユーザーが呼び出した場合の警告イベント。

各イベントの例を以下に示します。

インスタンスの削除アクション

```
{
   "version":"0",
   "id":"998c9cde-56c0-b38b-707f-0411b3ff9d11",
   "detail-type":"Inventory Resource State Change",
   "source":"aws.ssm",
   "account":"478678815555",
   "time":"2018-05-24T22:24:34Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:ssm:us-east-1:478678815555:managed-instance/i-0a5feb270fc3f0b97"
   ],
```

```
   "detail":{
      "action-status":"succeeded",
      "action":"delete",
      "resource-type":"managed-instance",
      "resource-id":"i-0a5feb270fc3f0b97",
      "action-reason":"",
      "type-name":"Custom:MyInfo"
   }
}
```

削除アクションの概要

```
{
   "version":"0",
   "id":"83898300-f576-5181-7a67-fb3e45e4fad4",
   "detail-type":"Inventory Resource State Change",
   "source":"aws.ssm",
   "account":"478678815555",
   "time":"2018-05-24T22:28:25Z",
   "region":"us-east-1",
   "resources":[

   ],
   "detail":{
      "action-status":"succeeded",
      "action":"delete-summary",
      "resource-type":"managed-instance",
      "resource-id":"",
      "action-reason":"The delete for type name Custom:MyInfo was completed. The
 deletion summary is: {\"totalCount\":2,\"remainingCount\":0,\"summaryItems\":
[{\"version\":\"1.0\",\"count\":2,\"remainingCount\":0}]}",
      "type-name":"Custom:MyInfo"
   }
}
```

無効化されたカスタムインベントリタイプの警告

```
{
   "version":"0",
   "id":"49c1855c-9c57-b5d7-8518-b64aeeef5e4a",
   "detail-type":"Inventory Resource State Change",
   "source":"aws.ssm",
   "account":"478678815555",
```

```
   "time":"2018-05-24T22:46:58Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:ssm:us-east-1:478678815555:managed-instance/i-0ee2d86a2cfc371f6"
   ],
   "detail":{
      "action-status":"failed",
      "action":"put",
      "resource-type":"managed-instance",
      "resource-id":"i-0ee2d86a2cfc371f6",
      "action-reason":"The inventory item with type name Custom:MyInfo was sent with a
 disabled schema version 1.0. You must send a version greater than 1.0",
      "type-name":"Custom:MyInfo"
   }
}
```

以下の手順に従って、カスタムインベントリの削除オペレーションの EventBridge ルールを作成します。この手順では、Amazon SNS トピックにカスタムインベントリ削除オペレーションの通知を送信するルールの作成方法を示します。開始する前に、Amazon SNS トピックがあることを確認するか、新規に作成します。詳細については、Amazon Simple Notification Service デベロッパーガイドの「開始方法」を参照してください。

インベントリ削除オペレーションのために EventBridge を設定するには

1. Amazon EventBridge コンソール (https://console.aws.amazon.com/events/) を開きます。
2. ナビゲーションペインで ルール] を選択します。
3. ルールの作成 を選択します。
4. ルールの名前と説明を入力します。

   ルールには、同じリージョン内および同じイベントバス上の別のルールと同じ名前を付けることはできません。
5. イベントバス] では、このルールに関連付けるイベントバスを選択します。このルールを使用して、自分の AWS アカウント の一致するイベントに応答する場合は、[default] (デフォルト) を選択します。アカウントの AWS のサービスで発生したイベントは、常にアカウントのデフォルトのイベントバスに移動します。
6. ルールタイプ では、イベントパターンを持つルール] を選択します。
7. [Next] を選択します。
8. [Event source] (イベントソース) で、[AWS events or EventBridge partner events] (イベントまたは EventBridge パートナーイベント) を選択します。

9. [Event pattern] (イベントパターン) セクションで [Event pattern form] (イベントパターンフォーム) を選択します。
10. [イベントパターンフォーム] では、AWS[サービス] を選択します。
11. [AWS のサービス] で、[Systems Manager] を選択します。
12. [イベントタイプ] で [在庫] を選択します。
13. [特定の詳細タイプ] で [インベントリリソースの状態の変更] を選択します。
14. [Next] を選択します。
15. ターゲットタイプ] では、AWSサービス] を選択します。
16. [Select a target] (ターゲットを選択) で [SNS topic] (SNS トピック) を選択し、[Topic] (トピック) に自分のトピックを選択します。
17. [Additional settings] (追加設定) セクションの [Configure target input] (ターゲット入力の確認) で [Matched event] (一致するイベント) が選択されていることを確認します。
18. [Next] を選択します。
19. (オプション) ルールに 1 つ以上のタグを入力します。詳細については、Amazon EventBridge ユーザーガイドの「Amazon EventBridge リソースのタグ付け」を参照してください 。
20. [Next] を選択します。
21. ルールの詳細を確認し、[Create rule] (ルールの作成) を選択します。

インベントリ履歴と変更の追跡の表示

AWS Config を使用してすべてのマネージドノードに対する AWS Systems Manager インベントリ履歴と変更の追跡を表示できます。AWS Config は、AWS アカウント にある AWS リソースの設定詳細ビューを提供します。これには、リソース間の関係と設定の履歴が含まれるため、時間の経過と共に設定と関係がどのように変わるかを確認できます。インベントリ履歴および変更の追跡を表示するには、AWS Config で以下のリソースを有効にする必要があります。

- SSM:ManagedInstanceInventory
- SSM:PatchCompliance
- SSM:AssociationCompliance
- SSM:FileData

> **Note**
>
> インベントリ履歴と変更の追跡について、次の重要な詳細に注意してください。
>
> - AWS Config を使用してシステム内の変更を追跡する場合は、AWS Config (`SSM:FileData`) でファイルの変更を表示できるように、`AWS:File` メタデータを収集するように Systems Manager インベントリを設定する必要があります。そうしないと、AWS Config はシステム上のファイルの変更を追跡しません。
> - SSM:PatchCompliance および SSM:AssociationCompliance を有効にすると、Systems Manager Patch Manager のパッチ適用と Systems Manager State Manager の関連付けのコンプライアンス履歴と変更の追跡を表示できます。これらのリソースのコンプライアンス管理の詳細については、「コンプライアンスの詳細について」を参照してください。

次の手順では、AWS Command Line Interface (AWS CLI) を使用して AWS Config で変更の追跡の記録とインベントリ履歴を有効化する方法について説明します。AWS Config でこれらのリソースを選択および設定する方法の詳細については、AWS Config デベロッパーガイドの AWS Config で記録するリソースの選択を参照してください。AWS Config の料金については、「料金」を参照してください。

開始する前に

AWS Config では、Systems Manager のリソースに関する設定の詳細を取得するために AWS Identity and Access Management (IAM) アクセス許可が必要です。次の手順では、Systems Manager リソースへの AWS Config アクセス許可を付与する IAM ロールに対して Amazon リソースネーム (ARN) を指定する必要があります。`AWS_ConfigRole` 管理ポリシーは、AWS Config に割り当てる IAM ロールにアタッチできます。このロールの詳細については、AWS Config デベロッパーガイドの「AWS 管理ポリシー: AWS_ConfigRole」(マネージドポリシー: _ConfigRole) を参照してください。IAM ロールの作成と `AWS_ConfigRole` 管理ポリシーの割り当て方法の詳細については、IAM ユーザーガイドの「AWS のサービス のサービスにアクセス許可を委任するロールの作成」を参照してください。

AWS Config でインベントリ履歴と変更追跡の記録を有効にするには

1. まだ AWS Command Line Interface (AWS CLI) をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」を参照してください。

2. 次に示す JSON の例をコピーしてシンプルなテキストファイルに貼り付け、recordingGroup.json として保存します。

```
{
   "allSupported":false,
   "includeGlobalResourceTypes":false,
   "resourceTypes":[
      "AWS::SSM::AssociationCompliance",
      "AWS::SSM::PatchCompliance",
      "AWS::SSM::ManagedInstanceInventory",
      "AWS::SSM::FileData"
   ]
}
```

3. 以下のコマンドを実行して、recordingGroup.json ファイルを にロードしますAWS Config

```
aws configservice put-configuration-recorder --configuration-recorder
 name=myRecorder,roleARN=arn:aws:iam::123456789012:role/myConfigRole --recording-
group file://recordingGroup.json
```

4. 以下のコマンドを実行して、インベントリ履歴と変更の追跡の記録を開始します。

```
aws configservice start-configuration-recorder --configuration-recorder-
name myRecorder
```

履歴と変更の追跡を設定した後、Systems Manager コンソールで [AWS Config] ボタンを選択し、特定のマネージドノードの履歴をドリルダウンすることができます。AWS Config ボタンは、[Managed Instances] (マネージドインスタンス) ページまたは [Inventory] (インベントリ) ページのいずれかからアクセスできます。画面サイズに応じて、ボタンを表示するためにページの右側にスクロールすることが必要になる場合があります。

データ収集の停止とインベントリデータの削除

AWS Systems Manager インベントリを使用して AWS リソースに関するメタデータを表示する必要がなくなったら、データ収集を停止し、すでに収集されたデータを削除できます。このセクションでは、次の情報を紹介します。

トピック

- データ収集の停止
- インベントリリソースデータ同期の削除

データ収集の停止

インベントリデータを収集するように Systems Manager を最初に設定すると、システムはメタデータの収集元になるスケジュールとリソースを定義する State Manager の関連付けを作成します。`AWS-GatherSoftwareInventory` ドキュメントを使用する State Manager の関連付けを削除すると、データ収集を停止できます。

インベントリの関連付けを削除するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[State Manager] を選択します。
3. `AWS-GatherSoftwareInventory` ドキュメントを使用する関連付けを選択してから、[Delete (削除)] を選択します。
4. `AWS-GatherSoftwareInventory` ドキュメントを使用する残りの関連付けでも、ステップ 3 を繰り返します。

インベントリリソースデータ同期の削除

AWS Systems Manager インベントリを使用して AWS リソースに関するメタデータを表示する必要がなくなった場合は、インベントリデータの収集で使用するリソースデータ同期も削除するようお勧めします。

インベントリリソースデータ同期を削除するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[インベントリ] を選択します。
3. [Resource Data Syncs (リソースデータ同期)] を選択します。
4. リストで同期を選択します。

> **Important**
>
> 必ずインベントリに使用する同期を選択してください。Systems Manager では、複数のツールに対するリソースデータ同期がサポートされています。間違った同期を選択すると、Systems Manager Explorer または Systems Manager コンプライアンスのデータ集約が中断される可能性があります。

5. [Delete] (削除) をクリックします
6. 削除する残りのリソースデータ同期でも、この手順を繰り返します。
7. データが保存されている Amazon Simple Storage Service (Amazon S3) バケットを削除します。Amazon S3 バケットを削除する方法については、「バケットの削除」を参照してください。

カスタムインベントリメタデータをマネージドノードに割り当てる

以下の手順では、AWS Systems Manager PutInventory API オペレーションを使用して、マネージドノードにカスタムインベントリメタデータを割り当てるプロセスについて説明します。この例では、ラックの場所情報をノードに割り当てます。カスタムインベントリの詳細については、「カスタムインベントリの操作」を参照してください。

カスタムインベントリメタデータをノードに割り当てる

1. まだ AWS Command Line Interface (AWS CLI) をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」を参照してください。
2. 以下のコマンドを実行して、ノードにラックの場所情報を割り当てます。

   Linux

   ```
   aws ssm put-inventory --instance-id "ID" --items '[{"CaptureTime":
    "2016-08-22T10:01:01Z", "TypeName": "Custom:RackInfo", "Content":[{"RackLocation":
    "Bay B/Row C/Rack D/Shelf E"}], "SchemaVersion": "1.0"}]'
   ```

   Windows

   ```
   aws ssm put-inventory --instance-id "ID" --items
    "TypeName=Custom:RackInfo,SchemaVersion=1.0,CaptureTime=2021-05-22T10:01:01Z,Content=[{Rac
    B/Row C/Rack D/Shelf F'}]"
   ```
3. 以下のコマンドを実行して、このノードのカスタムインベントリエントリを表示します。

   ```
   aws ssm list-inventory-entries --instance-id ID --type-name "Custom:RackInfo"
   ```

システムから以下のような情報が返されます。

```
{
    "InstanceId": "ID",
    "TypeName": "Custom:RackInfo",
    "Entries": [
        {
            "RackLocation": "Bay B/Row C/Rack D/Shelf E"
        }
    ],
    "SchemaVersion": "1.0",
    "CaptureTime": "2016-08-22T10:01:01Z"
}
```

4. 以下のコマンドを実行して、カスタムメのインベントリスキーマを表示します。

```
aws ssm get-inventory-schema --type-name Custom:RackInfo
```

システムから以下のような情報が返されます。

```
{
    "Schemas": [
        {
            "TypeName": "Custom:RackInfo",
            "Version": "1.0",
            "Attributes": [
                {
                    "DataType": "STRING",
                    "Name": "RackLocation"
                }
            ]
        }
    ]
}
```

AWS CLI を使用してインベントリデータ収集を設定する

以下の手順では、AWS Systems Manager インベントリを設定してマネージドノードからメタデータを収集するプロセスについて、順を追って説明します。インベントリ収集の設定を開始するには、Systems Manager State Manager の関連付けを作成します。関連付けが実行されると、Systems

Manager はインベントリデータを収集します。最初に関連付けを作成せずに、Systems Manager Run Command などを使用して aws:softwareInventory プラグインを呼び出そうとすると、次のエラーが返されます。

```
The aws:softwareInventory plugin can only be invoked via ssm-associate.
```

> **Note**
>
> ノードには、一度に 1 つのインベントリのみ関連付けることができます。ノードに 2 つ以上インベントリの関連付けを設定した場合、その関連付けは実行されず、インベントリデータは収集されません。

すべてのマネージドノードをインベントリ用にすばやく設定する (CLI)

AWS アカウント 内および現在のリージョン内のすべてのマネージドノードをすばやく設定して、インベントリデータを収集できます。これはグローバルインベントリの関連付けの作成と呼ばれます。AWS CLI を使用してグローバルなインベントリの関連付けを作成するには、次の手順に示すように、instanceIds 値のワイルドカードオプションを使用します。

AWS アカウント 内および現在のリージョン内のすべてのマネージドノードのインベントリを設定するには (CLI)

1. まだ AWS Command Line Interface (AWS CLI) をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」を参照してください。

2. 以下のコマンドを実行します。

   Linux & macOS

   ```
   aws ssm create-association \
   --name AWS-GatherSoftwareInventory \
   --targets Key=InstanceIds,Values=* \
   --schedule-expression "rate(1 day)" \
   --parameters
    applications=Enabled,awsComponents=Enabled,customInventory=Enabled,instanceDetailedInfo
   ```

Windows

```
aws ssm create-association ^
--name AWS-GatherSoftwareInventory ^
--targets Key=InstanceIds,Values=* ^
--schedule-expression "rate(1 day)" ^
--parameters
 applications=Enabled,awsComponents=Enabled,customInventory=Enabled,instanceDetailedInfo
```

> **Note**
>
> このコマンドでは、インベントリで Windows レジストリまたはファイルのメタデータを収集することはできません。これらのデータ型をインベントリするには、次の手順を使用します。

マネージドノードでインベントリを手動設定する (CLI)

ノード ID またはタグを使用して、マネージドノードに手動で AWS Systems Manager インベントリを設定するには、次の手順に従います。

マネージドノードをインベントリ用に手動設定するには (CLI)

1. まだ AWS Command Line Interface (AWS CLI) をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」を参照してください。

2. 以下のコマンドを実行して、ノードで Systems Manager インベントリを実行する State Manager の関連付けを作成します。各*##############*をユーザー自身の情報に置き換えます。このコマンドは、サービスを 6 時間ごとに実行し、ノードからネットワーク設定、Windows 更新プログラム、アプリケーションメタデータを収集するように設定します。

   Linux & macOS

   ```
   aws ssm create-association \
   --name "AWS-GatherSoftwareInventory" \
   --targets "Key=instanceids,Values=an_instance_ID" \
   ```

```
--schedule-expression "rate(240 minutes)" \
--output-location "{ \"S3Location\": { \"OutputS3Region\": \"region_ID,
 for example us-east-2\", \"OutputS3BucketName\": \"amzn-s3-demo-bucket\",
 \"OutputS3KeyPrefix\": \"Test\" } }" \
--parameters "networkConfig=Enabled,windowsUpdates=Enabled,applications=Enabled"
```

Windows

```
aws ssm create-association ^
--name "AWS-GatherSoftwareInventory" ^
--targets "Key=instanceids,Values=an_instance_ID" ^
--schedule-expression "rate(240 minutes)" ^
--output-location "{ \"S3Location\": { \"OutputS3Region\": \"region_ID,
 for example us-east-2\", \"OutputS3BucketName\": \"amzn-s3-demo-bucket\",
 \"OutputS3KeyPrefix\": \"Test\" } }" ^
--parameters "networkConfig=Enabled,windowsUpdates=Enabled,applications=Enabled"
```

システムから以下のような情報が返されます。

```
{
    "AssociationDescription": {
        "ScheduleExpression": "rate(240 minutes)",
        "OutputLocation": {
            "S3Location": {
                "OutputS3KeyPrefix": "Test",
                "OutputS3BucketName": "Test bucket",
                "OutputS3Region": "us-east-2"
            }
        },
        "Name": "The name you specified",
        "Parameters": {
            "applications": [
                "Enabled"
            ],
            "networkConfig": [
                "Enabled"
            ],
            "windowsUpdates": [
                "Enabled"
            ]
        },
        "Overview": {
```

```
            "Status": "Pending",
            "DetailedStatus": "Creating"
        },
        "AssociationId": "1a2b3c4d5e6f7g-1a2b3c-1a2b3c-1a2b3c-1a2b3c4d5e6f7g",
        "DocumentVersion": "$DEFAULT",
        "LastUpdateAssociationDate": 1480544990.06,
        "Date": 1480544990.06,
        "Targets": [
            {
                "Values": [
                   "i-02573cafcfEXAMPLE"
                ],
                "Key": "InstanceIds"
            }
        ]
    }
}
```

EC2 タグで Targets パラメータを使用することで、ノードの大規模なグループを対象にすることができます。次の例を参照してください。

Linux & macOS

```
aws ssm create-association \
--name "AWS-GatherSoftwareInventory" \
--targets "Key=tag:Environment,Values=Production" \
--schedule-expression "rate(240 minutes)" \
--output-location "{ \"S3Location\": { \"OutputS3Region\": \"us-east-2\",
 \"OutputS3BucketName\": \"amzn-s3-demo-bucket\", \"OutputS3KeyPrefix\": \"Test
\" } }" \
--parameters "networkConfig=Enabled,windowsUpdates=Enabled,applications=Enabled"
```

Windows

```
aws ssm create-association ^
--name "AWS-GatherSoftwareInventory" ^
--targets "Key=tag:Environment,Values=Production" ^
--schedule-expression "rate(240 minutes)" ^
--output-location "{ \"S3Location\": { \"OutputS3Region\": \"us-east-2\",
 \"OutputS3BucketName\": \"amzn-s3-demo-bucket\", \"OutputS3KeyPrefix\": \"Test
\" } }" ^
--parameters "networkConfig=Enabled,windowsUpdates=Enabled,applications=Enabled"
```

Windows Server および `files` インベントリタイプと式を使用して、`windowsRegistry` ノードのファイルおよび Windows レジストリキーをインベントリすることもできます。このインベントリタイプについての詳細は、「ファイルと Windows レジストリインベントリで作業する」を参照してください。

Linux & macOS

```
aws ssm create-association \
--name "AWS-GatherSoftwareInventory" \
--targets "Key=instanceids,Values=i-0704358e3a3da9eb1" \
--schedule-expression "rate(240 minutes)" \
--parameters '{"files":["[{\"Path\": \"C:\\Program Files\", \"Pattern\":
 [\"*.exe\"], \"Recursive\": true}]"], "windowsRegistry": ["[{\"Path\":
\"HKEY_LOCAL_MACHINE\\Software\\Amazon\", \"Recursive\":true}]"]}' \
--profile dev-pdx
```

Windows

```
aws ssm create-association ^
--name "AWS-GatherSoftwareInventory" ^
--targets "Key=instanceids,Values=i-0704358e3a3da9eb1" ^
--schedule-expression "rate(240 minutes)" ^
--parameters '{"files":["[{\"Path\": \"C:\\Program Files\", \"Pattern\":
 [\"*.exe\"], \"Recursive\": true}]"], "windowsRegistry": ["[{\"Path\":
\"HKEY_LOCAL_MACHINE\\Software\\Amazon\", \"Recursive\":true}]"]}' ^
--profile dev-pdx
```

3. 以下のコマンドを実行して、関連付けステータスを表示します。

```
aws ssm describe-instance-associations-status --instance-id an_instance_ID
```

システムから以下のような情報が返されます。

```
{
"InstanceAssociationStatusInfos": [
         {
            "Status": "Pending",
            "DetailedStatus": "Associated",
            "Name": "reInvent2016PolicyDocumentTest",
            "InstanceId": "i-1a2b3c4d5e6f7g",
```

```
            "AssociationId": "1a2b3c4d5e6f7g-1a2b3c-1a2b3c-1a2b3c-1a2b3c4d5e6f7g",
            "DocumentVersion": "1"
        }
]
}
```

チュートリアル: リソースデータの同期を使用してインベントリデータを集計する

次のチュートリアルでは、AWS Command Line Interface (AWS CLI) を使用して AWS Systems Manager インベントリのリソースデータ同期設定を作成する方法について説明します。リソースデータ同期では、すべてのマネージドノードから中央 Amazon Simple Storage Service (Amazon S3) バケットにインベントリデータが自動的にポートされます。新しいインベントリデータが検出されるたびに、同期は中央 Amazon S3 バケットを自動的に更新します。

このチュートリアルでは、Amazon Athena と Amazon QuickSight を使用して、集計されたデータをクエリおよび分析する方法についても説明します。AWS Management Console で Systems Manager を使用してリソースデータ同期を作成する方法については、「チュートリアル: リソースデータの同期を使用してインベントリデータを集計する」を参照してください。AWS Management Console で Systems Manager を使用した複数の AWS リージョン とアカウントからのインベントリのクエリについては、「複数のリージョンとアカウントからのインベントリデータをクエリする」を参照してください。

> **Note**
>
> このチュートリアルには、AWS Key Management Service (AWS KMS) を使用して同期を暗号化する方法に関する情報が含まれています。インベントリではユーザー固有、独自、または重要なデータが収集されないため、暗号化はオプションです。AWS KMS の詳細については、AWS Key Management Service デベロッパーガイドを参照してください。

[開始する前に]

このセクションのチュートリアルを開始する前に、次のタスクを確認するか完了してください。

- マネージドノードからインベントリデータを収集します。このチュートリアルの Amazon Athena および Amazon QuickSight セクションでは、アプリケーションデータを収集するようお勧めします。インベントリデータ収集方法の詳細については、「インベントリ収集の設定」または「AWS CLI を使用してインベントリデータ収集を設定する」を参照してください。

- (オプション) AWS Key Management Service (AWS KMS) 暗号化を使用する Amazon Simple Storage Service (Amazon S3) バケットにインベントリデータが保存されている場合は、AWS KMS の暗号化が可能になるように IAM アカウントと `Amazon-GlueServiceRoleForSSM` サービスロールも設定する必要があります。IAM アカウントとこのロールを設定せずに、[Detailed View (詳細ビュー)] タブを選択すると、Systems Manager には `Cannot load Glue tables` と表示されます。詳細については、「(オプション) AWS KMS 暗号化データを表示できるようアクセス許可を設定する」を参照してください。
- (オプション) AWS KMS を使用してリソースデータの同期を暗号化する場合は、次のポリシーを含む新しいキーを作成するか、既存のキーを更新してこのポリシーを追加する必要があります。

```
{
    "Version": "2012-10-17",
    "Id": "ssm-access-policy",
    "Statement": [
        {
            "Sid": "ssm-access-policy-statement",
            "Action": [
                "kms:GenerateDataKey"
            ],
            "Effect": "Allow",
            "Principal": {
                "Service": "ssm.amazonaws.com"
            },
            "Resource": "arn:aws:kms:us-east-2:123456789012:key/KMS_key_id",
            "Condition": {
                "StringLike": {
                    "aws:SourceAccount": "123456789012"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:ssm:*:123456789012:resource-data-sync/
*"
                }
            }
        }
    ]
}
```

インベントリのリソースデータ同期を作成するには

1. Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。

2. 集計されたインベントリデータを保存するバケットを作成します。詳細については、Amazon Simple Storage Service ユーザーガイドの「バケットの作成」を参照してください。バケット名とそれを作成した AWS リージョン を書き留めます。
3. バケットを作成した後、[Permissions] タブを選択し、[Bucket Policy] を選択します。
4. 次のバケットポリシーをコピーし、ポリシーエディタに貼り付けます。amzn-s3-demo-bucket と *account-id* を、作成した Amazon S3 バケットの名前と有効な AWS アカウント ID に置き換えます。複数のアカウントを追加する場合は、各アカウントの条件文字列と ARN をさらに追加します。1 個のアカウントを追加する場合は、例から追加のプレースホルダーを削除します。任意で、*bucket-prefix* を Amazon S3 プレフィックス (サブディレクトリ) に置き換えます。プレフィックスを作成しなかった場合は、*Bucket-Prefix*/ をこのポリシーの ARN から削除します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": " SSMBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "Service": "ssm.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/bucket-prefix/*/accountid=account-id/*"
      ],
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control",
          "aws:SourceAccount": [
            "account-id1",
            "account-id2",
            "account-id3",
            "account-id4"
          ]
        },
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:ssm:*:account-id1:resource-data-sync/*",
            "arn:aws:ssm:*:account-id2:resource-data-sync/*",
            "arn:aws:ssm:*:account-id3:resource-data-sync/*",
            "arn:aws:ssm:*:account-id4:resource-data-sync/*"
```

```
            ]
          }
        }
      }
    ]
}
```

5. (オプション) 同期を暗号化する場合は、前のステップでリストされたポリシーに以下の条件を追加する必要があります。これらは、StringEquals セクションに追加します。

```
"s3:x-amz-server-side-encryption":"aws:kms",
"s3:x-amz-server-side-encryption-aws-kms-key-
id":"arn:aws:kms:region:account_ID:key/KMS_key_ID"
```

以下がその例です。

```
"StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control",
          "aws:SourceAccount": "account-id",
          "s3:x-amz-server-side-encryption":"aws:kms",
          "s3:x-amz-server-side-encryption-aws-kms-key-
id":"arn:aws:kms:region:account_ID:key/KMS_key_ID"
        }
```

6. まだ AWS Command Line Interface (AWS CLI) をインストールして設定していない場合は、インストールして設定します。

詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」を参照してください。

7. (オプション) 同期を暗号化する場合は、次のコマンドを実行して、バケットポリシーが AWS KMS のキー要件を実行していることを確認します。各###############をユーザー自身の情報に置き換えます。

Linux & macOS

```
aws s3 cp ./A_file_in_the_bucket s3://amzn-s3-demo-bucket/prefix/ \
--sse aws:kms \
--sse-kms-key-id "arn:aws:kms:region:account_ID:key/KMS_key_id" \
--region region, for example, us-east-2
```

Windows

```
aws s3 cp ./A_file_in_the_bucket s3://amzn-s3-demo-bucket/prefix/ ^
    --sse aws:kms ^
    --sse-kms-key-id "arn:aws:kms:region:account_ID:key/KMS_key_id" ^
    --region region, for example, us-east-2
```

8. 次のコマンドを実行して、この手順の最初に作成した Amazon S3 バケットを使用したリソースデータ同期設定を作成します。このコマンドは、ログインしている AWS リージョン からの同期を作成します。

> **Note**
>
> 同期とターゲット Amazon S3 バケットが異なるリージョンにある場合は、データ転送料金が発生する場合があります。詳細については、Amazon S3 の料金 を参照してください。

Linux & macOS

```
aws ssm create-resource-data-sync \
--sync-name a_name \
--s3-destination "BucketName=amzn-s3-demo-bucket,Prefix=prefix_name,
 if_specified,SyncFormat=JsonSerDe,Region=bucket_region"
```

Windows

```
aws ssm create-resource-data-sync ^
--sync-name a_name ^
--s3-destination "BucketName=amzn-s3-demo-bucket,Prefix=prefix_name,
 if_specified,SyncFormat=JsonSerDe,Region=bucket_region"
```

`region` パラメータを使用して、同期設定をどこに作成するかを指定します。次の例では、us-west-1 リージョンからのインベントリデータが us-west-2 リージョンの Amazon S3 バケットに同期されます。

Linux & macOS

```
aws ssm create-resource-data-sync \
    --sync-name InventoryDataWest \
    --s3-destination "BucketName=amzn-s3-demo-
bucket,Prefix=HybridEnv,SyncFormat=JsonSerDe,Region=us-west-2"
    --region us-west-1
```

Windows

```
aws ssm create-resource-data-sync ^
--sync-name InventoryDataWest ^
--s3-destination "BucketName=amzn-s3-demo-
bucket,Prefix=HybridEnv,SyncFormat=JsonSerDe,Region=us-west-2" ^ --region us-
west-1
```

(オプション) AWS KMS を使用して同期を暗号化する場合は、次のコマンドを実行して同期を作成します。同期を暗号化する場合、AWS KMS キーおよび Amazon S3 バケットが同じリージョンにある必要があります。

Linux & macOS

```
aws ssm create-resource-data-sync \
--sync-name sync_name \
--s3-destination "BucketName=amzn-s3-demo-bucket,Prefix=prefix_name,
 if_specified,SyncFormat=JsonSerDe,AWSKMSKeyARN=arn:aws:kms:region:account_ID:key/
KMS_key_ID,Region=bucket_region" \
--region region
```

Windows

```
aws ssm create-resource-data-sync ^
--sync-name sync_name ^
--s3-destination "BucketName=amzn-s3-demo-bucket,Prefix=prefix_name,
 if_specified,SyncFormat=JsonSerDe,AWSKMSKeyARN=arn:aws:kms:region:account_ID:key/
KMS_key_ID,Region=bucket_region" ^
--region region
```

9. 以下のコマンドを実行して、同期設定のステータスを表示します。

```
aws ssm list-resource-data-sync
```

別のリージョンに同期設定を作成する場合は、次の例のように region パラメータを指定する必要があります。

```
aws ssm list-resource-data-sync --region us-west-1
```

10. 同期設定が正常に作成されたら、Amazon S3 のターゲットバケットを確認します。インベントリデータが数分で表示されます。

Amazon Athena でデータを使用する

以下のセクションでは、Amazon Athena でデータをクエリおよび表示する方法について説明します。開始する前に、Athena について学ぶことをお勧めします。詳細については、Amazon Athena ユーザーガイドの「Amazon Athenaとは」および「データの使用」を参照してください。

Amazon Athena でデータを表示およびクエリするには

1. https://console.aws.amazon.com/athena/ で Athena コンソールを開きます。
2. 次のステートメントをクエリエディタにコピーして貼り付け、[Run Query] を選択します。

```
CREATE DATABASE ssminventory
```

システムによって、ssminventory というデータベースが作成されます。

3. 次のステートメントをクエリエディタにコピーして貼り付け、[Run Query] を選択します。amzn-s3-demo-bucket と *bucket_prefix* を、Amazon S3 ターゲットの名前とプレフィックスに置き換えます。

```
CREATE EXTERNAL TABLE IF NOT EXISTS ssminventory.AWS_Application (
Name string,
ResourceId string,
ApplicationType string,
Publisher string,
Version string,
InstalledTime string,
Architecture string,
URL string,
Summary string,
```

```
PackageId string
)
PARTITIONED BY (AccountId string, Region string, ResourceType string)
ROW FORMAT SERDE 'org.openx.data.jsonserde.JsonSerDe'
WITH SERDEPROPERTIES (
  'serialization.format' = '1'
) LOCATION 's3://amzn-s3-demo-bucket/bucket_prefix/AWS:Application/'
```

4. 次のステートメントをクエリエディタにコピーして貼り付け、[Run Query] を選択します。

```
MSCK REPAIR TABLE ssminventory.AWS_Application
```

システムによってテーブルが分割されます。

> **Note**
>
> 他の AWS リージョン または AWS アカウント からリソースデータ同期を作成する場合、このコマンドを再度実行してパーティションを更新する必要があります。また、Amazon S3 バケットポリシーも更新する必要があります。

5. データをプレビューするには、AWS_Application テーブルの横にあるビューアイコンを選択します。

6. 次のステートメントをクエリエディタにコピーして貼り付け、[Run Query] を選択します。

```
SELECT a.name, a.version, count( a.version) frequency
from aws_application a where
a.name = 'aws-cfn-bootstrap'
group by a.name, a.version
order  by frequency desc
```

クエリは、Linux、macOS、および Windows Server 用の Amazon Elastic Compute Cloud (Amazon EC2) インスタンスに存在する AWS アプリケーションである、aws-cfn-bootstrap のさまざまなバージョンの数を返します。

7. 以下のステートメントを個別にコピーしてクエリエディタに張り付け、amzn-s3-demo-bucket と *bucket-prefix* を Amazon S3 の情報に置き換えてから、[クエリを実行] を選択します。これらのステートメントは Athena に追加インベントリテーブルを設定します。

```
CREATE EXTERNAL TABLE IF NOT EXISTS ssminventory.AWS_AWSComponent (
 `ResourceId` string,
  `Name` string,
  `ApplicationType` string,
  `Publisher` string,
  `Version` string,
  `InstalledTime` string,
  `Architecture` string,
  `URL` string
)
PARTITIONED BY (AccountId string, Region string, ResourceType string)
ROW FORMAT SERDE 'org.openx.data.jsonserde.JsonSerDe'
WITH SERDEPROPERTIES (
  'serialization.format' = '1'
) LOCATION 's3://amzn-s3-demo-bucket/bucket-prefix/AWS:AWSComponent/'
```

```
MSCK REPAIR TABLE ssminventory.AWS_AWSComponent
```

```
CREATE EXTERNAL TABLE IF NOT EXISTS ssminventory.AWS_WindowsUpdate (
  `ResourceId` string,
  `HotFixId` string,
  `Description` string,
  `InstalledTime` string,
  `InstalledBy` string
)
PARTITIONED BY (AccountId string, Region string, ResourceType string)
ROW FORMAT SERDE 'org.openx.data.jsonserde.JsonSerDe'
WITH SERDEPROPERTIES (
  'serialization.format' = '1'
) LOCATION 's3://amzn-s3-demo-bucket/bucket-prefix/AWS:WindowsUpdate/'
```

```
MSCK REPAIR TABLE ssminventory.AWS_WindowsUpdate
```

```
CREATE EXTERNAL TABLE IF NOT EXISTS ssminventory.AWS_InstanceInformation (
  `AgentType` string,
  `AgentVersion` string,
  `ComputerName` string,
  `IamRole` string,
  `InstanceId` string,
  `IpAddress` string,
```

```
  `PlatformName` string,
  `PlatformType` string,
  `PlatformVersion` string
)
PARTITIONED BY (AccountId string, Region string, ResourceType string)
ROW FORMAT SERDE 'org.openx.data.jsonserde.JsonSerDe'
WITH SERDEPROPERTIES (
  'serialization.format' = '1'
) LOCATION 's3://amzn-s3-demo-bucket/bucket-prefix/AWS:InstanceInformation/'
```

```
MSCK REPAIR TABLE ssminventory.AWS_InstanceInformation
```

```
CREATE EXTERNAL TABLE IF NOT EXISTS ssminventory.AWS_Network (
  `ResourceId` string,
  `Name` string,
  `SubnetMask` string,
  `Gateway` string,
  `DHCPServer` string,
  `DNSServer` string,
  `MacAddress` string,
  `IPV4` string,
  `IPV6` string
)
PARTITIONED BY (AccountId string, Region string, ResourceType string)
ROW FORMAT SERDE 'org.openx.data.jsonserde.JsonSerDe'
WITH SERDEPROPERTIES (
  'serialization.format' = '1'
) LOCATION 's3://amzn-s3-demo-bucket/bucket-prefix/AWS:Network/'
```

```
MSCK REPAIR TABLE ssminventory.AWS_Network
```

```
CREATE EXTERNAL TABLE IF NOT EXISTS ssminventory.AWS_PatchSummary (
  `ResourceId` string,
  `PatchGroup` string,
  `BaselineId` string,
  `SnapshotId` string,
  `OwnerInformation` string,
  `InstalledCount` int,
  `InstalledOtherCount` int,
  `NotApplicableCount` int,
  `MissingCount` int,
```

```
  `FailedCount` int,
  `OperationType` string,
  `OperationStartTime` string,
  `OperationEndTime` string
)
PARTITIONED BY (AccountId string, Region string, ResourceType string)
ROW FORMAT SERDE 'org.openx.data.jsonserde.JsonSerDe'
WITH SERDEPROPERTIES (
  'serialization.format' = '1'
) LOCATION 's3://amzn-s3-demo-bucket/bucket-prefix/AWS:PatchSummary/'
```

```
MSCK REPAIR TABLE ssminventory.AWS_PatchSummary
```

Amazon QuickSight でデータを使用する

以下のセクションでは、Amazon QuickSight で可視性を高めるための概要とリンクを示します。

Amazon QuickSight で可視性を高めるには

1. Amazon QuickSight にサインアップして、QuickSight コンソールにログインします。
2. AWS_Application テーブルおよび作成済みの他のテーブルからのデータセットを作成します。詳細については、「Amazon Athena データを使用したデータセットの作成」を参照してください。
3. テーブルを結合します。たとえば、instanceid の AWS_InstanceInformation 列は、他のインベントリテーブルの resourceid 列と一致するため、結合できます。テーブルの結合に関する詳細については、「テーブルの結合」を参照してください。
4. 視覚化を構築します。詳細については、「Amazon QuickSight ビジュアルの使用」を参照してください。

Systems Manager Inventory に関する問題のトラブルシューティング

このトピックでは、AWS Systems Manager インベントリの一般的なエラーや問題のトラブルシューティング方法について説明します。Systems Manager でノードを表示できない場合は、「マネージドノードの可用性のトラブルシューティング」を参照してください。

トピック

- 複数に適用される、ドキュメント 'AWS-GatherSoftwareInventory' とのすべての関連付けはサポートされていません

- インベントリ実行ステータスが保留中を終了しない
- AWS-ListWindowsInventory ドキュメントが実行されない
- コンソールに、[Inventory Dashboard | Detailed View | Settings tabs (インベントリダッシュボードの表示 | 詳細表示 | タブの設定)] が表示されない
- UnsupportedAgent
- スキップ
- [失敗]
- Amazon EC2 インスタンスのインベントリコンプライアンスが失敗しました
- S3 バケットオブジェクトに古いデータが含まれている

複数に適用される、ドキュメント '**AWS-GatherSoftwareInventory**' とのすべての関連付けはサポートされていません

エラーは `Multiple apply all associations with document 'AWS-GatherSoftwareInventory' are not supported`、すべてのノードに対してインベントリ関連付けを設定しようとしている 1 つ以上の AWS リージョン が、すべてのノードのインベントリ関連付けを使用して既に設定されていることを意味します。必要に応じて、すべてのノードに存在する既存のインベントリの関連付けを削除してから、新しいものを作成できます。既存のインベントリの関連付けを表示するには、Systems Manager コンソールで [State Manager] を選択し、`AWS-GatherSoftwareInventory` SSM ドキュメントを使用する関連付けを探します。すべてのノードの既存のインベントリ関連付けが複数のリージョン間で作成され、新しい関連付けを作成する場合は、その関連付けを存在する各リージョンから削除する必要があります。

インベントリ実行ステータスが保留中を終了しない

インベントリ収集が `Pending` ステータスを終了しない理由は 2 つあります。

- 選択した AWS リージョン にノードがない:

  Systems Manager Quick Setup を使用してグローバルインベントリ関連付けを作成する場合、選択したリージョンで使用可能なノードがないときは、インベントリ関連付けのステータス (`AWS-GatherSoftwareInventory` ドキュメント) に `Pending` が表示されます。
- アクセス許可が不足している:

  Systems Manager Inventory を実行するアクセス許可がないノードが 1 つ以上ある場合、インベントリの関連付けには `Pending` が表示されます。AWS Identity and Access Management (IAM)

インスタンスプロファイルに AmazonSSMManagedInstanceCore マネージドポリシーが含まれていることを確認します。このポリシーをインスタンスプロファイルに追加する方法については、「EC2 インスタンスのアクセス許可の代替設定」を参照してください。

インスタンスプロファイルには、少なくとも、次の IAM アクセス許可が必要です。

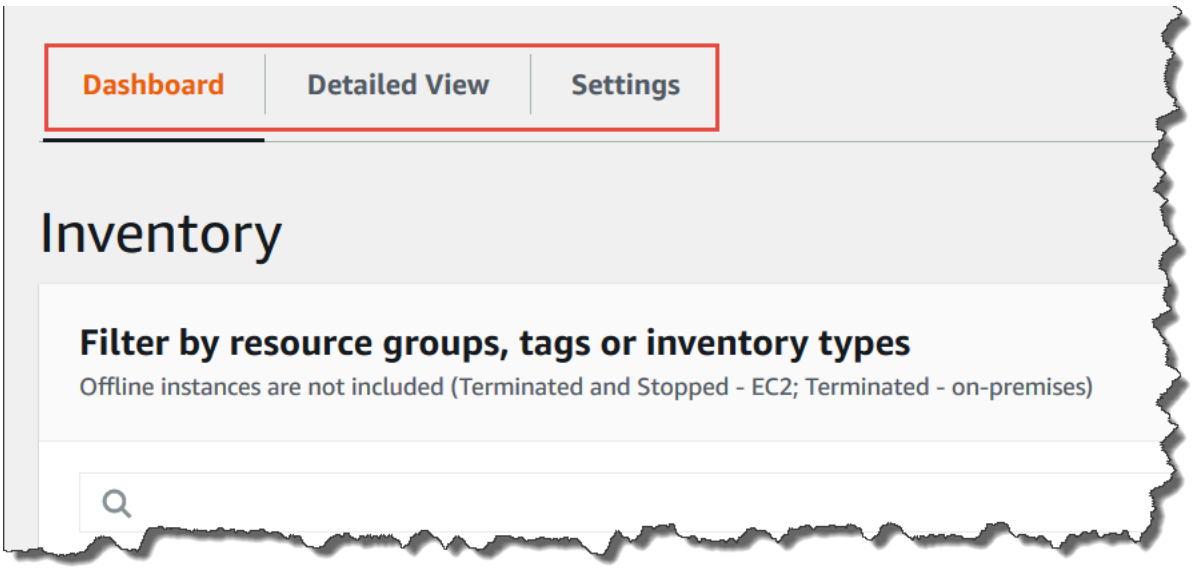
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeAssociation",
                "ssm:ListAssociations",
                "ssm:ListInstanceAssociations",
                "ssm:PutInventory",
                "ssm:PutComplianceItems",
                "ssm:UpdateAssociationStatus",
                "ssm:UpdateInstanceAssociationStatus",
                "ssm:UpdateInstanceInformation",
                "ssm:GetDocument",
                "ssm:DescribeDocument"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS-ListWindowsInventory ドキュメントが実行されない

AWS-ListWindowsInventory ドキュメントは廃止されました。このドキュメントを使用してインベントリを収集しないでください。代わりに、「インベントリ収集の設定」で説明されているプロセスのいずれかを使用してください。

コンソールに、[Inventory Dashboard | Detailed View | Settings tabs (インベントリダッシュボードの表示 | 詳細表示 | タブの設定)] が表示されない

Inventory の [Detailed View (詳細ビュー)] ページは、Amazon Athena を提供する AWS リージョン でのみ利用できます。以下のタブが [Inventory (インベントリ)] ページに表示されない場合は、Athena はリージョンで利用できず、データのクエリに [Detailed View (詳細ビュー)] を使用できないことを意味します。



UnsupportedAgent

インベントリの関連付けのステータス詳細に UnsupportedAgent と表示され、[Association status] (関連付けのステータス) に [Failed] (失敗) と表示される場合、マネージドノードの AWS Systems Manager SSM Agent のバージョンが正しくありません。グローバルなインベントリの関連付けを作成するには (AWS アカウント のすべてのノードをインベントリにする場合など)、SSM Agent バージョン 2.0.790.0 以降を使用する必要があります。各ノードで実行されているエージェントのバージョンは、[Managed Instances] (マネージドインスタンス) ページの [Agent version)] (エージェントのバージョン) 列で確認できます。ノードで SSM Agent を更新する方法については、「Run Command を使用して SSM Agent を更新する」を参照してください。

スキップ

ノードのインベントリの関連付けのステータスに [Skipped] (スキップ) と表示された場合、これは、(すべてのノードからインベントリを収集するために) グローバルなインベントリの関連付けを作成したが、スキップされたノードにはインベントリの関連付けが割り当て済みであったことを意味します。このノードにはグローバルなインベントリの関連付けが割り当てられず、グローバルなインベントリの関連付けで収集されたインベントリはありません。ただし、既存のインベントリの関連付けが実行されると、このノードからは依然としてインベントリデータが報告されます。

グローバルなインベントリの関連付けによってノードをスキップしたくない場合は、既存のインベントリの関連付けを削除する必要があります。既存のインベントリの関連付けを表示するには、Systems Manager コンソールで [State Manager] を選択し、`AWS-GatherSoftwareInventory` SSM ドキュメントを使用する関連付けを探します。

[失敗]

ノードのインベントリの関連付けのステータスが [Failed] (失敗) と表示された場合は、ノードに複数のインベントリの関連付けが割り当てられている可能性があります。ノードに一度に割り当てることができるインベントリの関連付けは 1 つのみです。インベントリの関連付けは、AWS-GatherSoftwareInventory AWS Systems Manager ドキュメント (SSM ドキュメント) を使用します。ノードの関連付けを一覧表示するには、AWS Command Line Interface (AWS CLI) を使用して次のコマンドを実行できます。

```
aws ssm describe-instance-associations-status
                --instance-id instance ID
```

Amazon EC2 インスタンスのインベントリコンプライアンスが失敗しました

Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのインベントリコンプライアンスは、インスタンスに複数のインベントリの関連付けを割り当てると失敗する可能性があります。

この問題を解決するには、インスタンスに割り当てられた 1 つ以上のインベントリの関連付けを削除します。詳細については、「関連付けを削除する」を参照してください。

> **Note**
>
> マネージドノードに対して複数のインベントリの関連付けを作成する場合は、次の動作に注意してください。
>
> - 各ノードには、すべてのノードをターゲットとするインベントリの関連付けを割り当てることができます (--targets "Key=InstanceIds,Values=*")。
> - 各ノードには、タグキーと値のペアまたは AWS リソースグループを使用する特定の関連付けを割り当てることもできます。
> - ノードに複数のインベントリの関連付けが割り当てられている場合、実行されていない関連付けのステータスは [Skipped] (スキップしました) と表示されます。最後に実行された関連付けには、インベントリの関連付けの実際のステータスが表示されます。
> - ノードに複数のインベントリの関連付けが割り当てられ、それぞれにタグのキーと値のペアが使用されている場合、タグの競合により、これらのインベントリの関連付けはノードで実行できません。関連付けは、タグのキーと値の競合がないノードで実行されます。

S3 バケットオブジェクトに古いデータが含まれている

Amazon S3 バケットオブジェクト内のデータは、インベントリの関連付けが成功して新しいデータが検出されたときに更新されます。Amazon S3 バケットオブジェクトは、関連付けが実行されて失敗したときにノードごとに更新されますが、この場合、オブジェクト内のデータは更新されません。Amazon S3 バケットオブジェクト内のデータは、関連付けが正常に実行されたときにのみ更新されます。インベントリ関連付けが失敗すると、Amazon S3 バケットオブジェクトに古いデータが表示されます。

AWS Systems Manager Patch Manager

AWS Systems Manager のツールである Patch Manager は、セキュリティ関連の更新およびその他の種類の更新の両方を使用してマネージドノードにパッチを適用するプロセスを自動化します。

> **Note**
>
> Systems Manager は、AWS Systems Manager のツールである Quick Setup でパッチポリシーをサポートしています。パッチポリシーの使用は、パッチ適用オペレーションの設定向けに推奨される方法です。1 つのパッチポリシー設定を使用して、組織内のすべてのリージョンにおける全アカウント、選択したアカウントとリージョンのみ、または 1 つのアカウントとリージョンのペアにパッチを定義できます。詳細については、「Quick Setup でのパッチポリシー設定」を参照してください。

Patch Manager を使用すると、オペレーティングシステムとアプリケーションの両方にパッチを適用することができます。(Windows Server では、アプリケーションのサポートは、Microsoft がリリースしたアプリケーションの更新に制限されています)。Patch Manager を使用して、Windows ノードにサービスパックをインストールしたり、Linux ノードでマイナーバージョンのアップグレードを実行したりすることができます。オペレーティングシステムのタイプ別に、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのフリート、エッジデバイス、オンプレミスサーバー、および仮想マシン (VM) にパッチを適用できます。「Patch Manager の前提条件」に記載されているように、これにはサポートされているバージョンのオペレーティングシステムが複数含まれます。インスタンスをスキャンし、見つからないパッチのレポートのみを表示できます。または、すべての見つからないパッチをスキャンして自動的にインストールできます。Patch Manager の使用を開始するには、Systems Manager コンソールを開きます。ナビゲーションペインで、[Patch Manager] を選択します。

AWS では、Patch Manager で公開する前にパッチをテストしません。また、Patch Managerでは、Windows Server 2016 ~ Windows Server 2019、SUSE Linux Enterprise Server (SLES) 12.0 ~

SLES 15.0 などのオペレーティングシステムのメジャーバージョンのアップグレードはサポートされていません。

パッチの重要度を報告する Linux ベースタイプのオペレーティングシステムの場合、Patch Manager は更新通知または個々のパッチのために、ソフトウェア発行者によって報告された重要度レベルを使用します。Patch Manager では、CVSS (共通脆弱性評価システム) のような サードパーティのソースからの、または NVD (National Vulnerability Database) がリリースしたメトリクスからの重要度レベルは取得しません。

Patch Manager はどのように組織にとってメリットになりますか?

Patch Manager は、セキュリティ関連の更新およびその他の種類の更新の両方を使用してマネージドノードにパッチを適用するプロセスを自動化します。これにはいくつかの主な利点があります。

- 一元化されたパッチ適用コントロール – パッチポリシーを使用して、組織内のすべてのリージョン、特定のアカウントとリージョン、または単一のアカウントとリージョンのペアのすべてのアカウントに対して、定期的なパッチ適用オペレーションを設定できます。
- フレキシブルなパッチ操作 - スキャンするインスタンスを選択し、検出されなかったパッチのレポートのみを表示できます。または、すべての検出されないパッチをスキャンして自動的にインストールできます。
- 包括的なコンプライアンスレポート – スキャン操作後、パッチコンプライアンスに違反しているマネージドノードと不足しているパッチに関する詳細情報を表示できます。
- クロスプラットフォームサポート – Patch Manager は、さまざまな Linux ディストリビューション、macOS、Windows Server など、複数のオペレーティングシステムをサポートしています。
- カスタムパッチベースライン – インストールが承認されるパッチを指定するカスタムパッチベースラインを使用して、組織のパッチコンプライアンスを構成する内容を定義できます。
- 他の AWS サービスとの統合 – Patch Manager は AWS Organizations、AWS Security Hub、AWS CloudTrail、および AWS Config と統合され、管理とセキュリティを強化します。
- 確定的なアップグレード – Amazon Linux 2023 など、オペレーティングシステム用のバージョン管理されたリポジトリによる確定的なアップグレードのサポート。

Patch Manager はどのようなユーザーに適していますか?

Patch Manager は、以下のユーザー向けに設計されています。

- マネージドノードのフリート全体でパッチコンプライアンスを維持する必要がある IT 管理者

- インフラストラクチャ全体のパッチコンプライアンスステータスを可視化する必要があるオペレーションマネージャー
- 自動パッチ適用ソリューションを大規模に実装したいクラウドアーキテクト
- パッチ適用を運用ワークフローに統合する必要がある DevOps エンジニア
- 一元化されたパッチ管理を必要とするマルチアカウント/マルチリージョンのデプロイを行う組織
- AWS マネージドノード、エッジデバイス、オンプレミスサーバー、仮想マシンのセキュリティ体制と運用状態を維持する責任者

Patch Manager の主な特徴は何ですか?

Patch Manager には、いくつかの主要な機能があります。

- パッチポリシー – AWS Organizations との統合を通じて単一のポリシーを使用して、複数の AWS アカウント およびリージョンにまたがるパッチ適用オペレーションを設定します。
- カスタムパッチベースライン – リリースから数日以内にパッチを自動承認するためのルールと、承認および拒否されたパッチリストを定義します。
- 複数のパッチ適用方法 – 特定のニーズに合わせて、パッチポリシー、メンテナンスウィンドウ、またはオンデマンドの「今すぐパッチ適用」オペレーションから選択します。
- コンプライアンスレポート – CSV 形式で Amazon S3 バケットに送信できるパッチコンプライアンスステータスに関する詳細なレポートを生成します。
- クロスプラットフォームサポート – Windows Server 全体でオペレーティングシステムとアプリケーションの両方に、さまざまな Linux ディストリビューション、および macOS にパッチを適用します。
- スケジューリングの柔軟性 – カスタム CRON 式または Rate 式を使用してパッチをスキャンしてインストールするためのさまざまなスケジュールを設定します。
- ライフサイクルフック – Systems Manager ドキュメントを使用して、パッチ適用操作の前後にカスタムスクリプトを実行します。
- セキュリティの焦点 – デフォルトでは、Patch Manager は利用可能なすべてのパッチをインストールするのではなく、セキュリティ関連の更新に焦点を当てています。
- Rate コントロール – パッチ適用オペレーションの同時実行数とエラーのしきい値を設定して、オペレーションへの影響を最小限に抑えます。

Patch Manager におけるコンプライアンスとは。

Systems Manager フリート内のマネージドノードの パッチコンプライアンス を構成するもののベンチマークは、AWS、オペレーティングシステム (OS) ベンダー、またはセキュリティコンサルティング会社などのサードパーティーによって定義されていません。

代わりに、パッチベースライン の組織またはアカウントのマネージドノードに対するパッチコンプライアンスの意味を定義します。パッチベースラインは、マネージドノードにパッチをインストールする必要があるルールを指定する構成です。パッチベースラインで指定した承認基準を満たすすべてのパッチが最新である場合、マネージドノードはパッチに準拠します。

パッチベースラインに 準拠 しているからといって、マネージドノードが必ずしも 安全 であるとは限らないことに注意してください。準拠とは、パッチベースラインで定義された、使用可能 で、かつ 承認済み のパッチがノードにインストールされていることを意味します。マネージドノードの全体的なセキュリティは、Patch Manager の範囲外の多くの要因によって決まります。詳細については、「セキュリティ」を参照してください。

各パッチベースラインは、Red Hat Enterprise Linux (RHEL)、macOS、または Windows Server など、サポートされている特定のオペレーティングシステム (OS) タイプの構成です。パッチベースラインは、サポートされているすべてのバージョンの OS のパッチ適用ルールを定義することも、RHEL 6.10、RHEL 7.8、および RHEL 9.3 など、指定したもののみに制限することもできます。

パッチベースラインでは、特定の分類と重要度レベルのすべてのパッチのインストールが承認されるように指定できます。例えば、`Security` として分類されるすべてのパッチを含みますが、`Bugfix` や `Enhancement` などの他の分類を除外することもできます。また、重要度が `Critical` のすべてのパッチを含み、`Important` や `Moderate` などの他のパッチを除外することもできます。

また、Windows Server に `KB2736693`、または Amazon Linux 2023 (AL2023)に `dbus.x86_64:1:1.12.28-1.amzn2023.0.1` など、承認または拒否する特定のパッチのリストに IDs を追加することで、パッチベースラインでパッチを明示的に定義することもできます。オプションで、パッチが利用可能になってからパッチ適用を待機する特定の日数を指定できます。Linux および macOS では、パッチベースラインルールで定義されているパッチの代わりに、コンプライアンス用のパッチの外部リスト (Install Override リスト) を指定するオプションがあります。

パッチ適用オペレーションを実行すると、Patch Manager はマネージドノードに現在適用されているパッチとパッチベースライン、または Install Override リストで設定されたルールに従い適用する必要があるパッチを比較します。マネージドノードに不足しているパッチのレポートのみを表示する Patch Manager (`Scan` オペレーション) か、不足しているパッチをすべて自動的にインストールする Patch Manager (`Scan and install` オペレーション) を選択できます。

Patch Manager は、パッチ適用オペレーションに使用できる事前定義されたパッチベースラインを提供します。ただし、これらの事前定義された設定は、推奨されるベストプラクティスではなく、例として提供されています。フリートのパッチコンプライアンスを構成するものをより細かく制御するために、独自のカスタムパッチベースラインを作成することをお勧めします。

パッチベースラインに関する詳細は、以下のトピックを参照してください。

- 事前定義されたパッチベースラインおよびカスタムパッチベースライン
- 承認されたパッチと拒否されたパッチのリストのパッケージ名の形式
- AWS の定義済みパッチベースラインの表示
- カスタムパッチベースラインの操作
- パッチコンプライアンスレポートの使用

プライマリコンポーネント

Patch Manager ツールを使用開始する前に、ツールのパッチ適用オペレーションの主なコンポーネントと機能を理解しておく必要があります。

パッチベースライン

Patch Manager では、承認済みおよび拒否済みパッチの選択可能なリストに加え、リリースから数日以内にパッチを自動承認するためのルールを含むパッチベースラインを使用します。パッチ適用オペレーションを実行すると、Patch Manager はマネージドノードに現在適用されているパッチとパッチベースラインで設定されたルールに従い適用する必要があるパッチを比較します。マネージドノードに不足しているパッチのレポートのみを表示する Patch Manager (`Scan` オペレーション) か、不足しているパッチをすべて自動的にインストールする Patch Manager (`Scan and install` オペレーション) を選択できます。

パッチ適用オペレーションメソッド

現在、Patch Manager で `Scan` および `Scan and install` オペレーションを実行する場合、次の 4 つのメソッドがあります。

- (推奨) Quick Setup で設定されるパッチポリシー — AWS Organizations との統合に基づいて、1 つのパッチ定義ポリシーで組織全体 (複数の AWS アカウントおよびそれらが運用されているすべての AWS リージョンを含む) のパッチ定義スケジュールおよびパッチベースラインを定義できます。また、組織内の一部の組織単位 (OU) のみにパッチポリシーを適用することもできます。1 つ

のパッチポリシーを使用して、さまざまなスケジュールでスキャンおよびインストールを実行できます。詳細については、「Quick Setup パッチポリシーを使用して組織内のインスタンスのためにパッチ適用を設定する」および「Quick Setup でのパッチポリシー設定」を参照してください。

- Quick Setup で設定されるホスト管理オプション — AWS Organizations との統合によりホスト管理設定もサポートされるため、最大で組織全体に対してパッチ適用オペレーションを実行できます。ただしこのオプションでできるのは、現在のデフォルトのパッチベースラインを使用して不足しているパッチをスキャンし、結果をコンプライアンスレポートで提供することに限られます。このオペレーションメソッドでパッチをインストールすることはできません。詳細については、「Quick Setup を使用して Amazon EC2 ホスト管理を設定する」を参照してください。
- パッチの **Scan** または **Install** タスクを実行するためのメンテナンスウィンドウ — Maintenance Windows という Systems Manager ツールで設定できるメンテナンスウィンドウでは、定義したスケジュールに従いさまざまなタイプのタスクを実行するように設定を行えます。Run Command タイプのタスクを使用すると、`Scan` または `Scan and install` タスク、選択したマネージドノードのセットを実行できます。メンテナンスウィンドウの各タスクでは、AWS アカウント と AWS リージョン の 1 つのペアでのみマネージドノードをターゲットにできます。詳細については、「チュートリアル: コンソールを使用してパッチ用メンテナンスウィンドウを作成する」を参照してください。
- Patch Manager でのオンデマンドの[今すぐパッチ適用]オペレーション — [Patch now] (今すぐパッチ適用) オプションを使用すると、マネージドノードにできるだけ早くパッチ適用する必要がある場合に、スケジュール設定をバイパスすることができます。[Patch now] (今すぐパッチ適用) を使用して、`Scan` または `Scan and install` オペレーションを実行するか、どのマネージドノードでオペレーションを実行するかを指定します。また、パッチ適用オペレーション中に、Systems Manager ドキュメント (SSM ドキュメント) をライフサイクルフックとして実行することもできます。[Patch now] (今すぐパッチ適用) の各オペレーションでは、AWS アカウントと AWS リージョンの 1 つのペアでのみマネージドノードノードをターゲットにできます。詳細については、「マネージドノードへのオンデマンド パッチ適用」を参照してください。

コンプライアンスレポート

`Scan` オペレーションの後、Systems Manager コンソールを使用して、パッチのコンプライアンス違反であるマネージドノード、およびこれらの各ノードで不足しているパッチについての情報を確認できます。任意の Amazon Simple Storage Service (Amazon S3) バケットに送信する .csv 形式のパッチコンプライアンスレポートを生成することもできます。1 回限りのレポートを生成することも、定期的なスケジュールでレポートを生成することもできます。単一マネージドノードの場合、レポートにはノードのすべてのパッチの詳細が含まれます。すべてのマネージドノードに関するレポートでは、欠けているパッチの数についての概要のみが提供されます。レポートが生成された

ら、Amazon QuickSight などのツールを使用してデータをインポートおよび分析できます。詳細については、「パッチコンプライアンスレポートの使用」を参照してください。

> **Note**
>
> パッチポリシーを使用して生成されたコンプライアンス項目の実行タイプは、`PatchPolicy` です。パッチポリシーのオペレーションで生成されないコンプライアンス項目の実行タイプは、`Command` です。

統合

Patch Manager は、以下のような他の AWS のサービス サービスと統合します。

- AWS Identity and Access Management (IAM) — IAM を使用して、Patch Manager オペレーションにアクセスできるユーザー、グループ、ロールを制御できます。詳細については、「AWS Systems Manager と IAM の連携方法」および「Systems Manager に必要なインスタンスのアクセス許可を設定する」を参照してください。
- AWS CloudTrail — CloudTrail を使用して、ユーザー、ロール、またはグループによって開始された監査可能なパッチ適用オペレーションのイベント履歴を記録できます。詳細については、「AWS Systems Manager による AWS CloudTrail API コールのログ記録」を参照してください。
- AWS Security Hub — Patch Manager からのパッチコンプライアンスデータを AWS Security Hub に送信できます。Security Hub では、高優先度のセキュリティアラートとコンプライアンス状況を包括的に確認できます。また、フリートのパッチ適用状況も監視できます。詳細については、「Patch Managerと AWS Security Hub の統合」を参照してください。
- AWS Config — Amazon EC2 インスタンスの管理データを Patch Manager ダッシュボードに表示するように AWS Config の記録を設定できます。詳細については、「パッチダッシュボードの概要の表示」を参照してください。

トピック

- Quick Setup でのパッチポリシー設定
- Patch Manager の前提条件
- Patch Managerの動作の仕組み
- マネージドノードへのパッチ適用のための SSM コマンドドキュメント
- パッチベースライン

- Amazon Linux 2 マネージドノードで Kernel Live Patching を使用
- コンソールを使用した Patch Manager リソースとコンプライアンスの操作
- AWS CLI を使用して Patch Manager リソースを操作する
- AWS Systems Manager Patch Manager のチュートリアル
- Patch Manager のトラブルシューティング

Quick Setup でのパッチポリシー設定

AWS では、パッチポリシーを使用して組織と AWS アカウントのパッチ適用を設定することが推奨されています。パッチポリシーは、2022 年 12 月に Patch Manager に導入されました。

パッチポリシーは、AWS Systems Manager のツールである Quick Setup を使用して設定します。パッチポリシーを使用すると、以前のパッチ適用を設定する方法に比べて、パッチ適用オペレーションをより広範囲かつ一元的に制御できます。パッチポリシーは、サポート対象バージョンの Linux、macOS、Windows Server など、Patch Manager がサポートしているすべてのオペレーティングシステムで使用できます。パッチポリシーの作成方法については、「Quick Setup パッチポリシーを使用して組織内のインスタンスのためにパッチ適用を設定する」を参照してください。

パッチポリシーの主な機能

ノードにパッチを適用する他の方法を使用せずに、パッチポリシーを使用して次に示す主な機能を活用してください。

- 一度にセットアップ – メンテナンスウィンドウや State Manager アソシエーションを使用してパッチ適用オペレーションをセットアップするには、Systems Manager コンソールのさまざまな部分で複数のタスクを実行する必要があります。パッチポリシーを使用すると、すべてのパッチ適用オペレーションを 1 つのウィザードでセットアップできます。
- 複数アカウント/複数リージョンのサポート – メンテナンスウィンドウ、State Manager アソシエーションや Patch Manager の [Patch now] (今すぐパッチ適用) 機能を使用すると、1 組の AWS アカウント-AWS リージョン ペアのマネージドノードを対象にすることしかできません。複数のアカウントと複数のリージョンを使用している場合、アカウントとリージョンの各ペアでセットアップタスクを実行する必要があるため、セットアップとメンテナンスのタスクに多大な時間がかかる可能性があります。ただし、AWS Organizations を使用すると、1 つのパッチポリシーを設定して、すべての AWS アカウント のすべての AWS リージョン のすべてのマネージドノードに適用されるようにできます。または、選択したアカウントとリージョンの一部の組織単位 (OU) にのみパッチポリシーを適用することもできます。パッチポリシーは、必要に応じて 1 つのローカルアカウントに適用することもできます。

- 組織レベルでのインストールをサポート – Quick Setup の既存のホスト管理設定オプションでは、マネージドノードを毎日スキャンしてパッチコンプライアンスを確認することができます。ただし、このスキャンは予め決められた時間に行われ、パッチのコンプライアンス情報のみが得られます。パッチのインストールは実行されません。パッチポリシーを使用して、スキャンおよびインストールのさまざまなスケジュールを指定できます。カスタムの CRON 式または Rate 式を使用して、これらのオペレーションの頻度と時間を選択することもできます。例えば、未適用のパッチがないか毎日スキャンして、定期的に更新されるコンプライアンス情報を取得できます。ただし、不要なダウンタイムを避けるため、インストールスケジュールは週に 1 回にすることもできます。
- パッチベースラインの選択の簡略化 – パッチポリシーには引き続きパッチベースラインが組み込まれており、パッチベースラインの設定方法に変更はありません。ただし、パッチポリシーを作成または更新するときは、オペレーティングシステム (OS) の種類ごとに使用する AWS マネージドベースラインまたはカスタムベースラインを 1 つのリストで選択できます。OS の種類ごとにデフォルトベースラインを別々のタスクで指定する必要はありません。

> **Note**
>
> パッチポリシーに基づいてパッチ適用オペレーションが実行される場合、AWS-RunPatchBaseline SSM ドキュメントが使用されます。詳細については、「パッチ適用のための SSM コマンドドキュメント: AWS-RunPatchBaseline」を参照してください。

関連情報

「Systems Manager Quick Setup を使用して AWS Organization 全体で一元的にパッチオペレーションをデプロイする」(AWS クラウド運用と移行に関するブログ)

パッチポリシーとのその他の違い

以前のパッチ適用設定の方法の代わりにパッチポリシーを使用する場合に注意すべきその他の相違点は次のとおりです。

- パッチグループは不要 – 以前のパッチ適用オペレーションでは、パッチグループに属するように複数のノードをタグ付けし、そのパッチグループに使用するパッチベースラインを指定できました。パッチグループがない場合、Patch Manager では、OS の種類に対する現在のデフォルトのパッチベースラインを使用してパッチが適用されました。パッチポリシーを使用すると、パッチグループをセットアップして管理する必要がなくなります。

> **Note**
>
> 2022 年 12 月 22 日にパッチポリシーのサポートがリリースされる前にパッチグループを使用していなかったアカウントとリージョンのペアでは、コンソールでパッチグループの機能がサポートされていません。パッチグループの機能は、この日付より前にパッチグループの使用を開始したアカウントとリージョンのペアで引き続き使用できます。

- [Configure patching] (パッチ適用を設定) ページが削除されました – パッチポリシーがリリースされる前は、[Configure patching] (パッチ適用を設定) ページで、パッチを適用するノード、パッチ適用スケジュール、およびパッチ適用オペレーションのデフォルトを指定できました。このページは Patch Manager から削除されました。これらのオプションは、パッチポリシーで指定することになりました。
- [Patch now] (今すぐパッチ適用) サポートなし – 引き続き、ノードをオンデマンドでパッチできるのは、一度に 1 組の AWS アカウント-AWS リージョン ペアに限られています。詳細については、マネージドノードへのオンデマンド パッチ適用 を参照してください。
- パッチポリシーとコンプライアンス情報 – パッチ適用ポリシーの設定に従ってマネージドノードのコンプライアンスをスキャンすると、コンプライアンスデータが利用可能になります。他のコンプライアンススキャン方法と同じ方法でデータを表示および操作できます。組織全体または複数の組織単位のパッチポリシーをセットアップできますが、AWS アカウント-AWS リージョン ペアそれぞれのコンプライアンス情報はペアごとに個別に報告されます。詳細については、「パッチコンプライアンスレポートの使用」を参照してください。
- 関連付けコンプライアンスステータスとパッチポリシー – Quick Setup パッチポリシーの下にあるマネージドノードのパッチステータスは、そのノードの State Manager 関連付け実行ステータスと一致します。関連付け実行ステータスが `Compliant` の場合、マネージドノードのパッチステータスも `Compliant` とマークされます。関連付け実行ステータスが `Non-Compliant` の場合、マネージドノードのパッチステータスも `Non-Compliant` とマークされます。

パッチポリシーがサポートされている AWS リージョン

Quick Setup でのパッチポリシー設定は、現在、次のリージョンでサポートされています。

- 米国東部 (オハイオ) (us-east-2)
- 米国東部 (バージニア北部) (us-east-1)
- 米国西部 (北カリフォルニア) (us-west-1)
- 米国西部 (オレゴン) (us-west-2)

- アジアパシフィック (ムンバイ) (ap-south-1)
- アジアパシフィック (ソウル) (ap-northeast-2)
- アジアパシフィック (シンガポール) (ap-southeast-1)
- アジアパシフィック (シドニー) (ap-southeast-2)
- アジアパシフィック (東京) (ap-northeast-1)
- カナダ (中部) (ca-central-1)
- ヨーロッパ (フランクフルト) (eu-central-1)
- 欧州 (アイルランド) (eu-west-1)
- ヨーロッパ (ロンドン) (eu-west-2)
- 欧州 (パリ) (eu-west-3)
- 欧州 (ストックホルム) (eu-north-1)
- 南米 (サンパウロ) (sa-east-1)

Patch Manager の前提条件

AWS Systems Manager のツールである Patch Manager を使用する前に、必要な前提条件を満たしていることを確認してください。

トピック

- SSM Agent バージョン
- Python バージョン
- パッチソースへの接続
- S3 エンドポイントアクセス
- パッチをローカルにインストールするためのアクセス許可
- Patch Manager でサポートされているオペレーティングシステム

SSM Agent バージョン

Patch Manager で管理するマネージドノードで SSM Agent のバージョン 2.0.834.0 以降が稼働しています。

> **Note**
>
> 新しいツールが Systems Manager に追加されるか、既存のツールが更新されると必ず、更新されたバージョンの SSM Agent がリリースされます。最新バージョンのエージェントを使用しないと、マネージドノードが Systems Manager の各種ツールや機能を使用できなくなる可能性があります。このため、マシン上で SSM Agent を最新状態に維持するプロセスを自動化することをお勧めします。詳細については、「SSM Agent への更新の自動化」を参照してください。GitHub の「SSM Agent リリースノート」ページをサブスクライブすると、SSM Agent の更新に関する通知を受け取ることができます。

Python バージョン

macOS とほとんどの Linux オペレーティングシステム (OS) では、現在、Patch Manager は Python バージョン 2.6 ~ 3.10 をサポートします。AlmaLinux、Debian Server、Raspberry Pi OS、Ubuntu Server の OS では、サポートされるバージョンの Python 3 (3.0 ~ 3.10) が必要です。

パッチソースへの接続

マネージドノードがインターネットに直接接続しておらず、VPC エンドポイントで Amazon Virtual Private Cloud (Amazon VPC) を使用している場合は、ノードがソース パッチ リポジトリ (repos) に確実にアクセスできるようにしておく必要があります。Linux ノードでは、通常、パッチ更新はノードに設定されているリモートリポジトリからダウンロードされます。したがって、パッチを適用するために、ノードはレポジトリに接続できる必要があります。詳細については、「セキュリティに関連するパッチの選択方法」を参照してください。

CentOS と CentOS Stream: **`EnableNonSecurity`** フラグを有効にする

CentOS 6 および 7 のマネージドノードではパッケージマネージャーとして Yum が使用されます。CentOS 8 および CentOS Stream のノードではパッケージマネージャーとして DNF が使用されます。どちらのパッケージマネージャーでも、更新通知の概念が使用されます。更新通知は、特定の問題を修正するパッケージの集合にすぎません。

ただし、CentOS および CentOS Stream のデフォルトリポは更新通知で設定されません。これは、Patch Manager で CentOS および CentOS Stream のデフォルトリポのパッケージが検出されないことを意味します。Patch Manager を許可して更新通知に含まれていないパッケージを処理するには、パッチベースラインルールで `EnableNonSecurity` フラグを有効にする必要があります。

Windows Server: Windows Update カタログまたは Windows Server Update Services (WSUS) に確実に接続できるようにする

Windows Server マネージドノードは、Windows Update カタログまたは Windows Server Update Services (WSUS) に接続できなくてはなりません。ノードがインターネットゲートウェイ、NAT ゲートウェイ、または NAT インスタンスを介して Microsoft Update Catalog に接続されていることを確認します。WSUS を使用している場合は、ノードがお使いの環境内の WSUS サーバーに接続されていることを確認します。詳細については、「問題: マネージドノードに Windows Update カタログまたは WSUS へのアクセスがない」を参照してください。

S3 エンドポイントアクセス

マネージドノードが動作するのがプライベート ネットワークまたは公開ネットワークのいずれであるかにかかわらず、必要な AWS マネージド Amazon Simple Storage Service (Amazon S3) バケットにアクセスできない場合、パッチ適用オペレーションは失敗します。マネージドノードがアクセスできる必要がある S3 バケットの詳細については、「SSM Agent と AWS マネージド S3 バケットとの通信」および「Systems Manager のために VPC エンドポイントを使用して EC2 インスタンスのセキュリティを強化する」を参照してください。

パッチをローカルにインストールするためのアクセス許可

Windows Server および Linux オペレーティングシステムでは、Patch Manager はそれぞれ Administrator およびルートユーザーアカウントを使用してパッチをインストールします。

しかし、macOS では、Brew と Brew Cask について、Homebrew はルートユーザーアカウントで実行されるコマンドをサポートしていません。その結果、Patch Manager は Homebrew ディレクトリの所有者、または Homebrew ディレクトリの所有者グループに属する有効なユーザーとして、Homebrew コマンドを照会して実行します。したがって、パッチをインストールするには、homebrew ディレクトリの所有者にも /usr/local ディレクトリに対する再帰的な所有者のアクセス許可が必要です。

> **Tip**
>
> 次のコマンドは、指定されたユーザーにこのアクセス許可を付与します。
>
> ```
> sudo chown -R $USER:admin /usr/local
> ```

Patch Manager でサポートされているオペレーティングシステム

Patch Manager のツールでは、Systems Manager の他のツールでサポートされているのと同じオペレーティングシステムのバージョンがすべてサポートされるわけではありません。例えば、Patch Manager では CentOS 6.3 や Raspberry Pi OS 8 (Jessie) はサポートされていません。

(Systems Manager でサポートされるオペレーティングシステムの詳細なリストについては、「System Manager でサポートされているオペレーティングシステム」を参照してください)。そのため、Patch Manager で使用するマネージドノードで、次の表に示すオペレーティングシステムのいずれかが実行されていることを確認してください。

> **Note**
>
> Patch Manager は、インストール可能なパッチを取得するために、Windows Update カタログや Windows Server Update Services for Windows など、マネージドノードに設定されているパッチリポジトリに依拠します。したがって、サポート終了 (EOL) のオペレーティングシステムバージョンでは、新しい更新プログラムが利用できない場合、Patch Manager は新しい更新プログラムについてレポートできない可能性があります。これは、Linux ディストリビューションのメンテナー、Microsoft、もしくは Apple によって新しい更新プログラムがリリースされていないか、またはマネージドノードに新しい更新プログラムにアクセスするための適切なライセンスがないことが原因である可能性があります。
>
> Patch Manager は、マネージドノードで使用可能なパッチに対するコンプライアンスステータスを報告します。したがって、インスタンスが EOL オペレーティングシステムを実行しており、更新プログラムが利用できない場合、Patch Manager はパッチ適用オペレーション用に設定されたパッチベースラインに応じて、ノードが準拠していると報告する可能性があります。

オペレーティングシステム	詳細
リナックス	• AlmaLinux 8.x, 9.x • Amazon Linux 2012.03 ~ 2018.03 • Amazon Linux 2 バージョン2.0 以降のすべてのバージョン • Amazon Linux 2022 • Amazon Linux 2023 • CentOS 6.5 ~ 7.9、8.x • CentOS Stream 8、9 • Debian Server 8.x、9.x、10.x、11.x、および 12.x • Oracle Linux 7.5 ~ 8.x、9.x

オペレーティングシステム	詳細
	• Raspberry Pi OS (旧称: Raspbian) 9 (Stretch) • Red Hat Enterprise Linux (RHEL) 6.5 ~ 8.x、9.x • Rocky Linux 8.x、9.x • SUSE Linux Enterprise Server (SLES) 12.0 および 12.x 以降のバージョン、15.x • Ubuntu Server 14.04 LTS、16.04 LTS、18.04 LTS、20.04 LTS、20.10 STR、22.04 LTS、23.04、23.10、24.04、および 24.10

オペレーティングシステム	詳細
macOS	macOS は Amazon EC2 インスタンスでのみサポートされています。 11.3.1、11.4 ~ 11.7 (Big Sur) 12.0 ~ 12.7 (Monterey) 13.0 ~ 13.7 (Ventura) 14.x (Sonoma) 15.x (Sequoia) macOSOS アップデート Patch Manager では、macOS のオペレーティングシステム (OS) のアップデートやアップグレード (12.x から 13.x、あるいは 13.1 から 13.2 など) をサポートしていません。macOS の OS バージョンを更新するには、Apple に組み込まれている OS アップグレードメカニズムを使用することをおすすめします。詳細については、Apple デベロッパードキュメンテーションウェブサイトの「Device Management」を参照してください。 HomeBrew サポート Patch Manager では、オープンソースのソフトウェアパッケージ管理システムである Homebrew を、次のいずれかのデフォルトのインストール場所にインストールする必要があります。 • `/usr/local/bin` • `/opt/homebrew/bin`

オペレーティングシステム	詳細
	Homebrew がインストールされていない場合、Patch Manager を使用したパッチ適用オペレーションが正しく機能しません。 Homebrew は macOS 10.14.x (Mojave) および 10.15.x (Catalina) のサポートを終了しました。結果として、これらのバージョンでは Patch Manager を使用したパッチ適用オペレーションはサポートされていません。 リージョンのサポート すべての AWS リージョン において macOS はサポートされていません。macOS についての Amazon EC2 のサポートの詳細については、「Amazon EC2 ユーザーガイド」の「Amazon EC2 Mac インスタンス」を参照してください。 macOS エッジデバイス AWS IoT Greengrass コアデバイスの SSM Agent は、macOS ではサポートされていません。macOS エッジデバイスをパッチするために Patch Manager が使用できません。

オペレーティングシステム	詳細
Windows	Windows Server 2008〜Windows Server 2025 (R2 バージョンを含む)。 **Note** AWS IoT Greengrass コアデバイスの SSM Agent は、Windows 10 ではサポートされていません。Windows 10 エッジデバイスをパッチするために Patch Manager が使用できません。 Windows Server 2008 のサポート 2020 年 1 月 14 日以降、Windows Server 2008 は Microsoft の機能更新プログラムまたはセキュリティ更新プログラムでサポートされなくなりました。Windows Server 2008 および 2008 R2 のレガシー Amazon Machine Images (AMIs) には、依然としてバージョン 2 の SSM Agent がプリインストールされていますが、Systems Manager は 2008 バージョンを正式にサポートしなくなり、これらのバージョンの Windows Server のエージェントを更新しなくなりました。さらに、SSM Agent のバージョン 3 は、Windows Server 2008 および 2008 R2 のいずれのオペレーションとも互換性がない場合があります。Windows Server 2008 バージョンで正式にサポートされている最後の SSM Agent のバージョンは 2.3.1644.0 です。 Windows Server 2012 および 2012 R2 のサポート Windows Server 2012 および 2012 R2 は、2023 年 10 月 10 日にサポートが終了しま

オペレーティングシステム	詳細
	した。これらのバージョンで Patch Manager を使用する場合、Microsoft の拡張セキュリティ更新プログラム (ESU) も使用することをお勧めします。詳細については、Microsoft ウェブサイトの「Windows Server 2012 および 2012 R2 のサポート終了」を参照してください。

Patch Managerの動作の仕組み

このセクションでは、サポートされているオペレーティングシステム別に、どのパッチをどのようにインストールするかについて、AWS Systems Manager のツールである Patch Manager で決定する方法を技術的に詳しく説明します。また、Linux オペレーティングシステムの場合に、マネージドノードに設定されたデフォルト以外のパッチ用に、カスタムのパッチベースラインでソースリポジトリを指定する方法についても説明します。さらに、Linux オペレーティングシステムのディストリビューション別に、パッチベースラインルールがどのように動作するかについて詳しく説明します。

> **Note**
>
> 以下のトピックの情報は、パッチ適用オペレーションに使用する設定の方法や種類に関係なく適用されます。
>
> - Quick Setup で設定されているパッチポリシー
> - Quick Setup で設定されているホスト管理オプション
> - パッチ `Scan` または `Install` のタスクを実行するためのメンテナンスウィンドウ
> - オンデマンドの [Patch now] (今すぐパッチ適用) オペレーション

トピック

- パッケージのリリース日と更新日の計算方法
- セキュリティに関連するパッチの選択方法
- 代替パッチソースリポジトリを指定する方法 (Linux)
- パッチのインストール方法
- Linux ベースシステムでのパッチベースラインルールの動作方法

- Linux と Windows Server のパッチ適用オペレーションの違い

パッケージのリリース日と更新日の計算方法

> **Important**
>
> このページの情報は、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスの Amazon Linux 1、Amazon Linux 2、Amazon Linux 2022 および Amazon Linux 2023 オペレーティングシステム (OS) に適用されます。Amazon Web Services では、これらの OS タイプのパッケージが作成、メンテナンスされます。他のオペレーティングシステムのメーカーがパッケージとリポジトリをどのように管理するかは、リリース日と更新日の計算方法に影響します。Red Hat Enterprise Linux (RHEL) と SUSE Linux Enterprise Server (SLES) などの Amazon Linux、Amazon Linux 2、Amazon Linux 2022 および Amazon Linux 2023 以外の OS における、パッケージの更新方法とメンテナンス方法については、製造元のドキュメントを参照してください。

ほとんどの OS タイプでは、作成したカスタムパッチベースラインの設定で、特定の日数が経過するとパッチのインストールが自動承認されるように指定できます。AWS には、7 日間の自動承認日を含む、事前定義済みのパッチベースラインがいくつか用意されています。

自動承認の遅延とは、パッチがリリースされてから自動承認されて適用されるまでの待機日数です。たとえば、`CriticalUpdates` 分類を使用してルールを作成し、7 日間の自動承認遅延を設定します。その結果、リリース日または最終更新日が 7 月 7 日の新しい重大なパッチは 7 月 14 日に自動的に承認されます。

Amazon Linux 1、Amazon Linux 2、Amazon Linux 2022 および Amazon Linux 2023 での自動承認遅延による予期しない結果を避けるには、リリース日と更新日の計算方法を理解することが重要です。

ほとんどの場合、パッチがインストールされるまでの自動承認の待ち時間は、`Release Date` 値ではなく、`updateinfo.xml` の `Updated Date` 値から計算されます。これらの日付計算に関する重要な詳細は次のとおりです。

- `Release Date` は通知がリリースされる日付です。パッケージが必ずしも関連するリポジトリで利用可能であるとは限りません。
- `Update Date` は通知が最後に更新された日付です。通知の更新は、テキストや説明の更新のような小さなものを表すことができます。パッケージが必ずしもその日付からリリースされたり、関連するリポジトリで利用可能であったりするとは限りません。

つまり、パッケージの Update Date 値は 7 月 7 日ですが、(たとえば) 7 月 13 日までインストールできない場合があります。この場合、7 日間の自動承認遅延を指定するパッチベースラインが 7 月 14 日に Install オペレーションで実行されます。なぜなら、Update Date 値は実行日の 7 日前で、パッケージのパッチとアップデートは 7 月 14 日にインストールされるからです。パッケージが実際にインストール可能になってから 1 日しか経過していなくても、インストールは行われます。

- オペレーティングシステムまたはアプリケーションパッチを含むパッケージは、初回リリース後に複数回更新できます。
- パッケージは AWS 管理リポジトリにリリースできますが、後で問題が発見された場合はロールバックされます。

一部のパッチ処理では、これらの要素は重要ではない場合があります。たとえば、重要度の値が Low および Medium、ならびに Recommended の分類のパッチをインストールするようにパッチベースラインが設定されている場合、自動承認が遅れても、運用にほとんど影響しない可能性があります。

ただし、重大なパッチや重要度の高いパッチを配布するタイミングがより重要な場合は、パッチがいつインストールされるかをより細かく制御したい場合があります。これを行うための推奨される方法は、管理対象ノードでのパッチオペレーションでデフォルトリポジトリの代わりに代替のパッチソースリポジトリを使用することです。

カスタムのパッチベースラインを作成するときは、代替パッチソースリポジトリを指定できます。各カスタムのパッチベースラインでは、サポートされている Linux オペレーティングシステムの最大 20 バージョンにパッチソース設定を指定できます。詳細については、「代替パッチソースリポジトリを指定する方法 (Linux)」を参照してください。

セキュリティに関連するパッチの選択方法

AWS Systems Manager のツールである Patch Manager の主な目的は、オペレーティングシステムのセキュリティに関連する更新プログラムをマネージドノードにインストールすることです。デフォルトでは、Patch Manager はすべての利用可能なパッチをインストールするのではなく、一部のセキュリティ関連のパッチをインストールします。

デフォルトでは、Patch Manager は、パッケージリポジトリで廃止とマークされたパッケージを、別のパッケージ更新のインストールでこの置換が必要な場合を除き、別の名前の置換パッケージに置き換えません。代わりに、パッケージを更新するコマンドの場合、Patch Manager はインストールされているが古いパッケージの欠落した更新のみを通知してインストールします。これは、古いパッ

ケージを置き換えるには、通常、既存のパッケージをアンインストールし、改めて新しいパッケージをインストールする必要があるためです。古いパッケージを置き換えると、意図していない重大な変更や追加機能が発生する可能性があります。

この動作は、機能のアップグレードではなくセキュリティ更新に焦点を当てた YUM および DNF の `update-minimal` コマンドと一致しています。詳細については、「the section called “パッチのインストール方法”」を参照してください。

パッチの重要度を報告する Linux ベースタイプのオペレーティングシステムの場合、Patch Manager は更新通知または個々のパッチのために、ソフトウェア発行者によって報告された重要度レベルを使用します。Patch Manager では、CVSS (共通脆弱性評価システム) のような サードパーティのソースからの、または NVD (National Vulnerability Database) がリリースしたメトリクスからの重要度レベルは取得しません。

> **Note**
>
> Patch Manager でサポートされているすべての Linux ベースのシステムでは、セキュリティに関連しない更新プログラムをインストールしたりするために、マネージドノードに別のソースリポジトリを選択することができます。詳細については、「代替パッチソースリポジトリを指定する方法 (Linux)」を参照してください。

このセクションの以降では、サポートされているオペレーティングシステムごとに、Patch Manager がセキュリティパッチを選択する方法について説明します。

Amazon Linux 1, Amazon Linux 2, Amazon Linux 2022, and Amazon Linux 2023

Amazon Linux 1、Amazon Linux 2、Amazon Linux 2022 および Amazon Linux 2023 では、事前設定されたリポジトリの処理とは異なります。

Amazon Linux 1 および Amazon Linux 2 では、Systems Manager のパッチベースライン サービスは、マネージドノード上の事前設定されたリポジトリを使用します。通常、ノードには 2 つの設定済みリポジトリ (リポウズ) があります。

Amazon Linux 1 上

- リポ ID: `amzn-main/latest`

  リポ名: `amzn-main-Base`
- リポ ID: `amzn-updates/latest`

リポ名: amzn-updates-Base

Amazon Linux 2 上

- リポ ID: amzn2-core/2/*architecture*

  リポ名: Amazon Linux 2 core repository
- リポ ID: amzn2extra-docker/2/*architecture*

  リポ名: Amazon Extras repo for docker

> **Note**
>
> *architecture* は x86_64 または aarch64 になります。

Amazon Linux 2023 (AL2023) インスタンスを作成すると、AL2023 のバージョンで利用可能な更新と、選択した特定の AMI の更新が含まれます。AL2023 インスタンスは起動時に追加のクリティカルかつ重要なセキュリティアップデートを自動的に受信しません。代わりに、デフォルトで有効になっている AL2023 のバージョン対応リポジトリによる確定的なアップグレード機能を使用すると、特定のニーズを満たすスケジュールに基づいて更新を適用できます。詳細については、「Amazon Linux 2023 ユーザーガイド」の「バージョン対応リポジトリによる確定的なアップグレード」を参照してください。

Amazon Linux 2022 では、事前設定されたリポジトリはロックされたバージョンのパッケージ更新に関連付けられています。Amazon Linux 2022 用の新規 Amazon Machine Images (AMIs) がリリースされると、特定のバージョンにロックされます。パッチ更新では、Patch Manager は、パッチ更新リポジトリの最新のロックバージョンを取得し、そのロックされたバージョンの内容に基づいてマネージド ノード上のパッケージを更新します。

AL2023 では、事前設定されたリポジトリは次のとおりです。

- リポ ID: amazonlinux

  リポジトリ名: Amazon Linux 2023 リポジトリ

Amazon Linux 2022 (プレビューリリース) では、事前設定されたリポジトリはロックされたバージョンのパッケージ更新に関連付けられています。Amazon Linux 2022 用の新規 Amazon Machine Images (AMIs) がリリースされると、特定のバージョンにロックされます。パッチ更新では、Patch Manager は、パッチ更新リポジトリの最新のロックバージョンを取得し、そのロックされたバージョンの内容に基づいてマネージド ノード上のパッケージを更新します。

Amazon Linux 2022 では、事前設定されたリポジトリは次のとおりです。

- リポ ID: `amazonlinux`

  リポジトリ名: Amazon Linux 2022 リポジトリ

> **Note**
>
> すべての更新は、マネージドノードに設定されているリモートリポジトリからダウンロードされます。したがって、パッチを適用できるようにレポジトリに接続するために、ノードにインターネットへのアウトバウンドアクセスが必要です。

Amazon Linux 1 および Amazon Linux 2 マネージド ノードではパッケージマネージャーとして Yum が使用されます。Amazon Linux 2022 および Amazon Linux 2023 ではパッケージマネージャーとして DNF が使用されます。

どちらのパッケージマネージャーでも、`updateinfo.xml` という名前のファイルとして更新通知の概念が使用されます。更新通知は、特定の問題を修正するパッケージの集合にすぎません。更新通知に含まれているすべてのパッケージは、Patch Manager ではセキュリティ関連とみなされます。個々のパッケージには分類や重要度は割り当てられません。そのため、Patch Manager は関連するパッケージに更新通知の属性を割り当てます。

> **Note**
>
> [パッチベースラインの作成] ページで [セキュリティ以外の更新を含める] チェックボックスをオンにすると、`updateinfo.xml` ファイル (または、正しくフォーマットされた分類、重要度、および日付の値のないファイルを含むパッケージ) に分類されないパッケージは、事前にフィルタリングされたパッチのリストに含まれます。ただし、パッチを適用するためには、パッチはユーザーが指定したパッチベースラインルールを満たしている必要があります。

セキュリティ以外の更新を含めるオプションの詳細については、「パッチのインストール方法」および「Linux ベースシステムでのパッチベースラインルールの動作方法」を参照してください。

CentOS and CentOS Stream

CentOS および CentOS Stream の場合、Systems Manager のパッチベースラインサービスはマネージドノードの設定済みリポジトリ (リポウズ) を使用します。以下のリストは、架空の CentOS 8.2 Amazon Machine Image (AMI) の例を示します。

- リポ ID: `example-centos-8.2-base`

  リポ名: `Example CentOS-8.2 - Base`
- リポ ID: `example-centos-8.2-extras`

  リポ名: `Example CentOS-8.2 - Extras`
- リポ ID: `example-centos-8.2-updates`

  リポ名: `Example CentOS-8.2 - Updates`
- リポ ID: `example-centos-8.x-examplerepo`

  リポ名: `Example CentOS-8.x – Example Repo Packages`

> **Note**
>
> すべての更新は、マネージドノードに設定されているリモートリポジトリからダウンロードされます。したがって、パッチを適用できるようにレポジトリに接続するために、ノードにインターネットへのアウトバウンドアクセスが必要です。

CentOS 6 および 7 のマネージドノードではパッケージマネージャーとして Yum が使用されます。CentOS 8 および CentOS Stream のノードではパッケージマネージャーとして DNF が使用されます。どちらのパッケージマネージャーでも、更新通知の概念が使用されます。更新通知は、特定の問題を修正するパッケージの集合にすぎません。

ただし、CentOS および CentOS Stream のデフォルトリポは更新通知で設定されません。これは、Patch Manager で CentOS および CentOS Stream のデフォルトリポのパッケージが検出さ

れないことを意味します。Patch Manager を許可して更新通知に含まれていないパッケージを処理するには、パッチベースラインルールで `EnableNonSecurity` フラグを有効にする必要があります。

> **Note**
>
> CentOS および CentOS Stream の更新通知がサポートされています。更新通知のあるリポは起動後にダウンロードできます。

Debian サーバー and Raspberry Pi OS

Debian Server および Raspberry Pi OS (旧称 Raspbian) の場合、Systems Manager のパッチベースラインサービスでは、インスタンスの事前設定済みリポジトリ (リポウズ) を使用します。これらの構成済みリポを使用して、使用可能なパッケージアップグレードの最新リストを取得します。このため、Systems Manager は、`sudo apt-get update` コマンドと同等のコマンドを実行します。

その後、パッケージは `debian-security` *`codename`* リポからフィルタリングされます。つまり、Debian Server の各バージョンでは、次のように、Patch Manager は、そのバージョンの関連リポジトリに含まれるアップグレードのみを識別します。

- Debian Server 8: `debian-security jessie`
- Debian Server 9: `debian-security stretch`
- Debian Server 10: `debian-security buster`
- Debian Server 11: `debian-security bullseye`
- Debian Server 12: `debian-security bookworm`

> **Note**
>
> Debian Server 8 のみ: 一部の Debian Server 8.* マネージドノードはサポートされなくなったパッケージリポジトリ (`jessie-backports`) を参照するため、Patch Manager ではパッチ適用オペレーションが正常に完了するように追加の手順を実行します。詳細については、「パッチのインストール方法」を参照してください。

Oracle Linux

Oracle Linux の場合、Systems Manager パッチベースライン サービスはマネージドノードの事前設定済みのリポジトリ (リポウズ) を使用します。通常、ノードには 2 つの設定済みリポウズがあります。

Oracle Linux 7:

- リポ ID: `ol7_UEKR5/x86_64`

  リポ名: `Latest Unbreakable Enterprise Kernel Release 5 for Oracle Linux 7Server (x86_64)`
- リポ ID: `ol7_latest/x86_64`

  リポ名: `Oracle Linux 7Server Latest (x86_64)`

Oracle Linux 8:

- リポ ID: `ol8_baseos_latest`

  リポ名: `Oracle Linux 8 BaseOS Latest (x86_64)`
- リポ ID: `ol8_appstream`

  リポ名: `Oracle Linux 8 Application Stream (x86_64)`
- リポ ID: `ol8_UEKR6`

  リポ名: `Latest Unbreakable Enterprise Kernel Release 6 for Oracle Linux 8 (x86_64)`

Oracle Linux 9:

- リポ ID: `ol9_baseos_latest`

  リポ名: `Oracle Linux 9 BaseOS Latest (x86_64)`
- リポ ID: `ol9_appstream`

  リポ名: `Oracle Linux 9 Application Stream Packages(x86_64)`
- リポ ID: `ol9_UEKR7`

リポ名: `Oracle Linux UEK Release 7 (x86_64)`

> **Note**
>
> すべての更新は、マネージドノードに設定されているリモートリポジトリからダウンロードされます。したがって、パッチを適用できるようにレポジトリに接続するために、ノードにインターネットへのアウトバウンドアクセスが必要です。

Oracle Linux マネージドノードではパッケージマネージャーとして Yum が使用されます。Yum では `updateinfo.xml` という名前のファイルとして、更新通知の概念が使用されます。更新通知は、特定の問題を修正するパッケージの集合にすぎません。個々のパッケージには分類や重要度は割り当てられません。このため、Patch Manager は、更新通知の属性を関連するパッケージに割り当てて、パッチベースラインで指定された分類フィルターに基づいてパッケージをインストールします。

> **Note**
>
> [パッチベースラインの作成] ページで [セキュリティ以外の更新を含める] チェックボックスをオンにすると、`updateinfo.xml` ファイル (または、正しくフォーマットされた分類、重要度、および日付の値のないファイルを含むパッケージ) に分類されないパッケージは、事前にフィルタリングされたパッチのリストに含まれます。ただし、パッチを適用するためには、パッチはユーザーが指定したパッチベースラインルールを満たしている必要があります。

AlmaLinux, RHEL, and Rocky Linux

AlmaLinux では、Red Hat Enterprise Linux および Rocky Linux では、Systems Manager のパッチベースラインサービスでマネージドノードの事前設定済みリポジトリ (リポウズ) が使用されます。通常、ノードには 3 つの設定済みリポウズがあります。

すべての更新は、マネージドノードに設定されているリモートリポジトリからダウンロードされます。したがって、パッチを適用できるようにレポジトリに接続するために、ノードにインターネットへのアウトバウンドアクセスが必要です。

> **Note**
>
> [パッチベースラインの作成] ページで [セキュリティ以外の更新を含める] チェックボックスをオンにすると、updateinfo.xml ファイル (または、正しくフォーマットされた分類、重要度、および日付の値のないファイルを含むパッケージ) に分類されないパッケージは、事前にフィルタリングされたパッチのリストに含まれます。ただし、パッチを適用するためには、パッチはユーザーが指定したパッチベースラインルールを満たしている必要があります。

Red Hat Enterprise Linux 7 のマネージドノードではパッケージマネージャーとして Yum が使用されます。AlmaLinux、Red Hat Enterprise Linux 8、および Rocky Linux のマネージドノードではパッケージマネージャーとして DNF が使用されます。どちらのパッケージマネージャーでも、updateinfo.xml という名前のファイルとして更新通知の概念が使用されます。更新通知は、特定の問題を修正するパッケージの集合にすぎません。個々のパッケージには分類や重要度は割り当てられません。このため、Patch Manager は、更新通知の属性を関連するパッケージに割り当てて、パッチベースラインで指定された分類フィルターに基づいてパッケージをインストールします。

RHEL 7

> **Note**
>
> 以下のレポ ID は RHUI 2 に関連付けられています。RHUI 3 は 2019 年 12 月に開始され、Yum リポジトリ ID に異なる命名スキームを導入しました。マネージドノード作成元の RHEL-7 AMI によっては、コマンドを更新する必要がある場合があります。詳細については、Red Hat カスタマーポータルの「AWS にある RHEL 7 のリポジトリ ID が既に変化した」を参照してください。

- リポ ID: `rhui-REGION-client-config-server-7/x86_64`

  リポ名: `Red Hat Update Infrastructure 2.0 Client Configuration Server 7`
- リポ ID: `rhui-REGION-rhel-server-releases/7Server/x86_64`

  リポ名: `Red Hat Enterprise Linux Server 7 (RPMs)`
- リポ ID: `rhui-REGION-rhel-server-rh-common/7Server/x86_64`

リポ名: `Red Hat Enterprise Linux Server 7 RH Common (RPMs)`

AlmaLinux、8 RHEL 8、および Rocky Linux 8

- リポ ID: `rhel-8-appstream-rhui-rpms`

  リポ名: `Red Hat Enterprise Linux 8 for x86_64 - AppStream from RHUI (RPMs)`
- リポ ID: `rhel-8-baseos-rhui-rpms`

  リポ名: `Red Hat Enterprise Linux 8 for x86_64 - BaseOS from RHUI (RPMs)`
- リポ ID: `rhui-client-config-server-8`

  リポ名: `Red Hat Update Infrastructure 3 Client Configuration Server 8`

AlmaLinux 9、 RHEL 9、および Rocky Linux 9

- リポ ID: `rhel-9-appstream-rhui-rpms`

  リポ名: `Red Hat Enterprise Linux 9 for x86_64 - AppStream from RHUI (RPMs)`
- リポ ID: `rhel-9-baseos-rhui-rpms`

  リポ名: `Red Hat Enterprise Linux 9 for x86_64 - BaseOS from RHUI (RPMs)`
- リポ ID: `rhui-client-config-server-9`

  リポ名:`Red Hat Enterprise Linux 9 Client Configuration`

SLES

SUSE Linux Enterprise Server (SLES) マネージドノードでは、ZYPP ライブラリは使用可能なパッチのリスト (パッケージの集合) を以下の場所から取得します。

- リポジトリのリスト: `etc/zypp/repos.d/*`
- パッケージの情報: `/var/cache/zypp/raw/*`

SLES マネージドノードはパッケージマネージャーとして Zypper を使用し、Zypper はパッチの概念を使用します。パッチは、特定の問題を修正するパッケージのコレクションです。Patch

Manager は、パッチに含まれているすべてのパッケージをセキュリティ関連のパッケージとみなします。個々のパッケージには分類や重要度が与えられていないため、Patch Managerはパッケージにその属しているパッチの属性を割り当てます。

Ubuntu Server

Ubuntu Server の場合、Systems Manager パッチベースライン サービスはマネージドノードの事前設定済みのリポジトリ (リポウズ) を使用します。これらの構成済みリポを使用して、使用可能なパッケージアップグレードの最新リストを取得します。このため、Systems Manager は、`sudo apt-get update` コマンドと同等のコマンドを実行します。

次に、パッケージを *`codename`*`-security` リポジトリでフィルタリングします。この codename はリリースバージョンに固有です (Ubuntu Server 14 の場合は `trusty` など)。Patch Managerは、次のリポジトリに含まれているアップグレードのみを識別します。

- Ubuntu Server 14.04 LTS: `trusty-security`
- Ubuntu Server 16.04 LTS: `xenial-security`
- Ubuntu Server 18.04 LTS: `bionic-security`
- Ubuntu Server 20.04 LTS: `focal-security`
- Ubuntu Server 20.10 STR: `groovy-security`
- Ubuntu Server 22.04 LTS (`jammy-security`)
- Ubuntu Server 23.04 (`lunar-security`)

Windows Server

Microsoft Windows オペレーティングシステムの場合、Patch Manager は Microsoft が Microsoft Update に公開して Windows Server Update Services (WSUS) で自動的に利用可能になる更新プログラムのリストを取得します。

> **Note**
>
> Patch Managerでは、Patch Manager でサポートされている Windows Server オペレーティングシステムのバージョンで利用可能なパッチのみを使用できます。例えば、Patch Managerを使用して Windows RT にパッチを適用することはできません。

Patch Manager は各 AWS リージョン で新しい更新を継続的にモニタリングします。利用可能な更新プログラムのリストは、各リージョンで 1 日 1 回以上更新されます。Microsoft からのパッ

チ情報が処理されると、Patch Manager は最新の更新プログラムで置き換えられた前の更新プログラムをパッチのリストから削除します。したがって、最新の更新のみが表示され、インストール可能になります。例えば、KB3135456 が KB4012214 に置き換えられると、Patch Managerでは KB4012214 のみが利用可能になります。

同様に、Patch Manager がインストールできるのは、パッチ適用オペレーション中にマネージドノードで利用可能になっているパッチのみです。デフォルトで、Windows Server 2019 および Windows Server 2022 は後続の更新に置き換えられた更新を削除します。その結果、Windows Server パッチベースラインで ApproveUntilDate パラメータを使用しても、ApproveUntilDate パラメータで選択された日付が最新パッチの日付よりも前になっている場合は、以下のシナリオが発生します。

- 置き換えられたパッチはノードから削除されるため、Patch Manager を使用してインストールすることができない。
- 最新の代替パッチがノードに存在するが、ApproveUntilDate パラメータで指定された日付に従ったインストールにはまだ承認されていない。

これは、前月の緊急パッチがインストールされていない可能性がある場合でも、Systems Manager オペレーションに関してはマネージドノードが準拠状態にあることを意味します。ApproveAfterDays パラメータの使用時にも同じシナリオが発生する可能性があります。Microsoft の置き換えられたパッチ動作のため、ApproveAfterDays の日数が経過する前に Microsoft からの最新のパッチがリリースされた場合でも Windows Server 向けのパッチがインストールされないように、日数を設定することが可能です (通常は 30 日を超える日数)。マネージドノードで置き換えられたパッチを利用できるように Windows グループポリシーオブジェクト (GPO) 設定を変更した場合、このシステム動作は該当しないことに注意してください。

> **Note**
>
> Microsoft がリリースするアプリケーションのパッチは、更新日時を指定していない場合があります。このような場合、デフォルトでは 01/01/1970 の更新日時が指定されています。

代替パッチソースリポジトリを指定する方法 (Linux)

マネージドノードに設定されているデフォルトのリポジトリをパッチオペレーションに使用すると、AWS Systems Manager のツールである Patch Manager はセキュリティに関連するパッチをスキャンまたはインストールします。これがPatch Managerのデフォルトの動作です。Patch Manager

がセキュリティ関連のパッチを選択してインストールする方法の詳細については、「セキュリティに関連するパッチの選択方法」を参照してください。

ただし、Linux システムでは、Patch Manager を使用して、セキュリティに関連しないパッチや、マネージドノードに設定されているデフォルトのリポジトリとは異なるソースリポジトリにあるパッチをインストールすることもできます。カスタムのパッチベースラインを作成するときは、代替パッチソースリポジトリを指定できます。各カスタムのパッチベースラインでは、サポートされている Linux オペレーティングシステムの最大 20 バージョンにパッチソース設定を指定できます。

例えば、Ubuntu Server フリートに Ubuntu Server 14.04 および Ubuntu Server 16.04 マネージドノードの両方が含まれているとします。この場合、同じカスタムパッチベースラインで、各バージョンの代替リポジトリを指定できます。バージョンごとに、名前、オペレーティングシステムのバージョンタイプ (製品)、リポジトリ設定を指定します。サポートされているオペレーティングシステムのすべてのバージョンに適用される 1 つの代替ソースリポジトリを指定することもできます。

> **Note**
>
> マネージドノードの代替パッチ リポジトリを指定したカスタム パッチベースラインを実行しても、それらがオペレーティングシステム上の新しいデフォルト リポジトリになることはありません。パッチ適用オペレーションが完了すると、ノードのオペレーティングシステムのデフォルトとして以前に構成されたリポジトリーはデフォルトのままです。

このオプションを使用するシナリオの例のリストについては、このトピックの後半の「代替パッチソースリポジトリの使用例」を参照してください。

デフォルトおよびカスタムのパッチベースラインについては、「事前定義されたパッチベースラインおよびカスタムパッチベースライン」を参照してください。

例: コンソールを使用する場合

Systems Manager コンソールでの作業時に代替パッチソースリポジトリを指定するには、[Create patch baseline (パッチベースラインの作成)] ページの [Patch sources (パッチソース)] セクションを使用します。[Patch sources (パッチソース)] のオプションの使用については、「Linux 用 カスタムパッチベースラインの作成」を参照してください。

例: AWS CLI を使用する場合

AWS Command Line Interface (AWS CLI) で `--sources` オプションを使用する例については、「異なる OS バージョン用にカスタムリポジトリのパッチベースラインを作成する」を参照してください。

トピック

- 代替リポジトリに関する重要な考慮事項
- 代替パッチソースリポジトリの使用例

代替リポジトリに関する重要な考慮事項

代替パッチリポジトリを使用してパッチ適用戦略を計画する際は、次の点に注意してください。

指定されたリポジトリのみがパッチ適用に使用されます

代替リポジトリの指定は、追加リポジトリの指定を意味しません。マネージドノードにデフォルトとして設定されているリポジトリ以外のリポジトリを選択することができます。ただし、更新を適用する場合は、代替のパッチソース設定の一部としてデフォルトのリポジトリも指定する必要があります。

例えば、Amazon Linux 2 マネージドノードでは、デフォルトのリポジトリは `amzn2-core` と `amzn2extra-docker` です。パッチ適用オペレーションで Extra Packages for Enterprise Linux (EPEL) リポジトリを含める必要がある場合は、3 つのリポジトリすべてを代替リポジトリとして指定する必要があります。

> **Note**
>
> マネージドノードの代替パッチ リポジトリを指定したカスタム パッチベースラインを実行しても、それらがオペレーティングシステム上の新しいデフォルト リポジトリになることはありません。パッチ適用オペレーションが完了すると、ノードのオペレーティングシステムのデフォルトとして以前に構成されたリポジトリーはデフォルトのままです。

YUM ベースのディストリビューションのパッチ適用の動作は、updateinfo.xml マニフェストに依存します

Amazon Linux 1、Amazon Linux 2、Red Hat Enterprise Linux、CentOS など、YUM ベースのディストリビューション用の代替パッチリポジトリを指定する場合、パッチ適用動作は、リポジトリに更新マニフェストが完全で正しい形式の `updateinfo.xml` ファイルで含まれているかどうかによって異

なります。このファイルは、リリース日、分類、および各種パッケージの重要度を指定します。次のいずれかのパッチ動作に影響を与えます。

- Classification や Severity でフィルターしても、それらが `updateinfo.xml` で指定されていない場合、そのパッケージはフィルターには含まれません。つまり、`updateinfo.xml` ファイルのないパッケージはパッチ適用に含まれません。
- ApprovalAfterDays でフィルターしても、パッケージのリリース日が Unix エポック形式でない場合 (またはリリース日が指定されていない場合)、そのパッケージはフィルターに含まれません。
- [パッチベースラインの作成] ページで [セキュリティ以外の更新を含める] チェックボックスをオンにした場合、例外が発生します。この場合、`updateinfo.xml` ファイルを持たないパッケージ (または、このファイルが含まれていても、分類、重要度、日付について適切にフォーマットされた値が指定されていないパッケージ) は、事前にフィルタリングされたパッチのリストに含まれます。(インストールするには、パッチベースラインルールの他の要件を満たしていなければなりません。)

代替パッチソースリポジトリの使用例

例 1 - Ubuntu Server のセキュリティに関連しない更新プログラム

AWS が提供する事前定義されたパッチベースライン `AWS-UbuntuDefaultPatchBaseline` を使用して、セキュリティパッチを Ubuntu Server マネージドノードのフリート上にインストールするために Patch Manager を既に使用しているとします。このデフォルトに基づいて新しいパッチベースラインを作成できますが、デフォルトのディストリビューションに含まれるセキュリティに関連しない更新プログラムもインストールするように、承認ルールで指定できます。このパッチベースラインがノードに対して実行されると、セキュリティに関連する問題と関連しない問題の両方に対するパッチが適用されます。また、ベースラインに対して指定したパッチ例外で、セキュリティに関連しないパッチを承認することもできます。

例 2 - Ubuntu Server の PPA (Personal Package Archives)

Ubuntu Server マネージドノードで、Personal Package Archives (PPA) for Ubuntu を通じて配布されるソフトウェアを実行するとします。この場合、マネージドノードで設定した PPA リポジトリをパッチ適用オペレーションのソースリポジトリとして指定する、パッチベースラインを作成します。その後、Run Command を使用して、ノードでパッチベースライン ドキュメントを実行します。

例 3 - Amazon Linux の社内アプリケーション

Amazon Linux マネージドノードで、業界の規制コンプライアンスに必要なアプリケーションを実行する必要があるとします。ノードでこれらのアプリケーションのリポジトリを設定し、YUM を使用

してアプリケーションをまずインストールしてから、この新しい企業リポジトリを含むように、新しいパッチベースラインを更新または作成できます。その後、Run Command を使用し、Scan オプション付きで AWS-RunPatchBaseline ドキュメントを実行することで、企業パッケージがインストールされたパッケージに含まれており、マネージドノードで最新かどうかを確認できます。最新でない場合は、Install オプション付きでそのドキュメントを再実行することで、アプリケーションを更新できます。

パッチのインストール方法

AWS Systems Manager のツールである Patch Manager は、オペレーティングシステムのタイプ別に適切な組み込み機構を使用してマネージドノードに更新をインストールします。例えば、Windows Server には Windows Update API を使用し、Amazon Linux 2 には yum パッケージマネージャーを使用します。

Patch Manager は、現在インストールされている古いパッケージを置き換える新しいパッケージをインストールしません。(例外: 新しいパッケージが、インストールされている別のパッケージの更新で依存関係にあるか、新しいパッケージの名前が古いパッケージと同じである場合)。代わりに、Patch Manager はインストールされたパッケージに利用可能な更新を通知し、インストールします。このアプローチは、あるパッケージが別のパッケージを置き換えたときに発生する可能性のあるシステム機能の予期しない変更を防ぐのに役立ちます。

古くなったパッケージをアンインストールして新たなパッケージを改めてインストールする必要がある場合は、カスタムスクリプトを使用するか、Patch Manager の標準オペレーション外でパッケージマネージャーコマンドを使用する必要がある場合があります。

このセクションの以降では、Patch Manager がオペレーティングシステムにパッチをインストールする方法について説明します。

Amazon Linux 1, Amazon Linux 2, Amazon Linux 2022, and Amazon Linux 2023

Amazon Linux 1、Amazon Linux 2、Amazon Linux 2022 および Amazon Linux 2023 のマネージドノードでは、パッチのインストールワークフローは次のとおりです。

1. パッチのリストが https URL または Amazon Simple Storage Service (Amazon S3) パススタイルの URL を使用して、AWS-RunPatchBaseline または AWS-RunPatchBaselineAssociation ドキュメントの InstallOverrideList パラメータを使用して指定されている場合、リストされたパッチがインストールされ、手順 2〜7 はスキップされます。
2. パッチベースラインの指定どおりに GlobalFilters を適用し、対象のパッケージのみを追加処理のために保持します。

3. パッチベースラインの指定どおりに ApprovalRules を適用します。各承認ルールは、承認されたとおりにパッケージを定義できます。

   ただし、承認ルールは、パッチベースラインの作成時または最終更新時に [Include nonsecurity updates (セキュリティ以外の更新を含める)] チェックボックスがオンになっているかどうかによっても影響を受けます。

   セキュリティ以外の更新が除外されている場合、暗黙のルールを適用してセキュリティリポのアップグレードを持つパッケージのみを選択します。選択対象の各パッケージは、セキュリティリポに属する適切なバージョン (通常は最新バージョン) のパッケージであることが必要です。

   セキュリティ以外の更新が含まれている場合は、他のリポジトリからのパッチも考慮されます。

4. パッチベースラインの指定どおりに ApprovedPatches を適用します。承認済みパッチについては、GlobalFilters によって破棄されている場合や、ApprovalRules に指定された承認ルールから承認が付与されていない場合でも、更新が承認されます。
5. パッチベースラインの指定どおりに RejectedPatches を適用します。承認済みパッチのリストから削除された拒否済みパッチは、適用されません。
6. 複数のバージョンのパッチが承認されている場合は、最新バージョンが適用されます。
7. YUM 更新 API (Amazon Linux 1、Amazon Linux 2) または DNF 更新 API (Amazon Linux 2022、Amazon Linux 2023) は、承認されたパッチに次のように適用されます。
   - AWS により事前定義されたデフォルトのパッチベースラインについては、`updateinfo.xml` で指定されたパッチのみが適用されます (セキュリティ更新のみ)。これは、[セキュリティ以外の更新を含める] チェックボックスがオフになっているためです。事前定義されたベースラインは、以下を含むカスタムベースラインと同等です。
     - [セキュリティ以外の更新を含める] チェックボックスはオフになっています。
     - `[Critical, Important]` の重要度リスト
     - `[Security, Bugfix]` の分類リスト

     Amazon Linux 1 および Amazon Linux 2 の場合、このワークフローに対する同等の yum コマンドは次のとおりです。

     ```
     sudo yum update-minimal --sec-severity=Critical,Important --bugfix -y
     ```

Amazon Linux 2022 および Amazon Linux 2023 の場合、このワークフローに対する dnf コマンドは次のとおりです。

```
sudo dnf upgrade-minimal --sec-severity=Critical --sec-severity=Important --
bugfix -y
```

[セキュリティ以外の更新を含める] チェックボックスがオンになっている場合、updateinfo.xml にあるパッチと updateinfo.xml にないパッチの両方が適用されます (セキュリティの更新とセキュリティ以外の更新)。

Amazon Linux 1、Amazon Linux 2 では、[セキュリティ以外の更新を含める] のベースラインが選択され、重要度リストが [Critical, Important] で、分類リストが [Security, Bugfix] である場合、同等の yum コマンドは次のようになります。

```
sudo yum update --security --sec-severity=Critical,Important --bugfix -y
```

Amazon Linux 2022 および Amazon Linux 2023 の場合、同等の dnf コマンドは次のようになります。

```
sudo dnf upgrade --security --sec-severity=Critical --sec-severity=Important --
bugfix -y
```

> **Note**
>
> yum または dnf コマンドを Patch Manager の外で実行すると、古くなったパッケージに代わる新しいパッケージが別の名前でインストールされます。ただし、同等の Patch Manager オペレーションではインストールされません。

> **Note**
>
> Amazon Linux 2022 および Amazon Linux 2023 の場合、パッチの重要度レベル Medium は、一部の外部リポジトリで定義されている重要度レベル Moderate と同等です。パッチベースラインに Medium 重要度パッチを含めると、外部パッチからの Moderate 重要度パッチもインスタンスにインストールされます。

API アクション DescribeInstancePatches を使用してコンプライアンスデータをクエリすると、重要度レベル Medium のフィルタリングによって、重要度レベルが Medium と Moderate の両方のパッチがレポートされます。
Amazon Linux 2022 および Amazon Linux 2023 は、DNF パッケージマネージャーによって認識されるパッチの重要度レベル None もサポートしています。

8. 更新がインストールされると、マネージドノードは再起動されます。(例外: RebootOption パラメータが AWS-RunPatchBaseline ドキュメントの NoReboot で設定されている場合、パッチマネージャーの Patch Manager 実行後にマネージドノードは再起動されません。詳細については、「パラメータ名: RebootOption」を参照してください。)

CentOS and CentOS Stream

CentOS および CentOS Stream マネージドノードの場合、パッチのインストールワークフローは次のとおりです。

1. パッチのリストが https URL または Amazon Simple Storage Service (Amazon S3) パススタイルの URL を使用して、AWS-RunPatchBaseline または AWS-RunPatchBaselineAssociation ドキュメントの InstallOverrideList パラメータを使用して指定されている場合、リストされたパッチがインストールされ、手順 2〜7 はスキップされます。

   パッチベースラインの指定どおりに GlobalFilters を適用し、対象のパッケージのみを追加処理のために保持します。
2. パッチベースラインの指定どおりに ApprovalRules を適用します。各承認ルールは、承認されたとおりにパッケージを定義できます。

   ただし、承認ルールは、パッチベースラインの作成時または最終更新時に [Include nonsecurity updates (セキュリティ以外の更新を含める)] チェックボックスがオンになっているかどうかによっても影響を受けます。

   セキュリティ以外の更新が除外されている場合、暗黙のルールを適用してセキュリティリポのアップグレードを持つパッケージのみを選択します。選択対象の各パッケージは、セキュリティリポに属する適切なバージョン (通常は最新バージョン) のパッケージであることが必要です。

   セキュリティ以外の更新が含まれている場合は、他のリポジトリからのパッチも考慮されます。

3. パッチベースラインの指定どおりに ApprovedPatches を適用します。承認済みパッチについては、GlobalFilters によって破棄されている場合や、ApprovalRules に指定された承認ルールから承認が付与されていない場合でも、更新が承認されます。
4. パッチベースラインの指定どおりに RejectedPatches を適用します。承認済みパッチのリストから削除された拒否済みパッチは、適用されません。
5. 複数のバージョンのパッチが承認されている場合は、最新バージョンが適用されます。
6. 承認済みパッチには、YUM 更新 API (CentOS 6.x および 7.x バージョン) または DNF 更新 (CentOS 8 および CentOS Stream) が適用されます。
7. 更新がインストールされると、マネージドノードは再起動されます。(例外: `RebootOption` パラメータが `AWS-RunPatchBaseline` ドキュメントの `NoReboot` で設定されている場合、パッチマネージャーの Patch Manager 実行後にマネージドノードは再起動されません。詳細については、「パラメータ名: `RebootOption`」を参照してください。)

Debian サーバー and Raspberry Pi OS

Debian Server および Raspberry Pi OS (旧称 Raspbian) インスタンスの場合、パッチのインストール手順は次のとおりです。

1. パッチのリストが https URL または Amazon Simple Storage Service (Amazon S3) パススタイルの URL を使用して、`AWS-RunPatchBaseline` または `AWS-RunPatchBaselineAssociation` ドキュメントの `InstallOverrideList` パラメータを使用して指定されている場合、リストされたパッチがインストールされ、手順 2〜7 はスキップされます。
2. 更新が可能な場合、`python3-apt` (Python ライブラリインターフェイスの `libapt`) は最新バージョンにアップグレードされます。(このセキュリティ以外のパッケージは、[Include nonsecurity updates (セキュリティ以外の更新プログラムを含める)] オプションが選択されていなくてもアップグレードされます。)

> **Important**
>
> Debian Server 8 のみ: 一部の Debian Server 8.* マネージドノードはサポートされなくなったパッケージリポジトリ (`jessie-backports`) を参照するため、Patch Manager ではパッチ適用オペレーションが正常に完了するように次の追加の手順を実行します。
>
> a. お客様のマネージドノードでは、`jessie-backports` リポジトリへのリファレンスはソース場所リスト (`/etc/apt/sources.list.d/jessie-backports`) から

コメントアウトされています。その結果、その場所からのパッチのダウンロードは試みられません。

b. Stretch のセキュリティの更新の署名キーがインポートされます。このキーによって、Debian Server 8.* ディストリビューションでの更新およびインストールオペレーションに必要なアクセス許可が付与されます。

c. この時点で、`apt-get` オペレーションを実行し、パッチ適用プロセスの開始前に最新バージョンの `python3-apt` がインストールされていることを確認します。

d. インストールプロセスが完了すると、`jessie-backports` リポジトリへの参照が復元され、署名キーが apt ソースキーリングから削除されます。これは、パッチ適用オペレーション前のシステム設定をそのまま残すために行われます。

次にPatch Managerがシステムを更新するときにも、同じプロセスが行われます。

3. パッチベースラインの指定どおりに GlobalFilters を適用し、対象のパッケージのみを追加処理のために保持します。
4. パッチベースラインの指定どおりに ApprovalRules を適用します。各承認ルールは、承認されたとおりにパッケージを定義できます。

> **Note**
>
> Debian Server の更新プログラムパッケージのリリース日は確定できないため、このオペレーティングシステムでは自動承認オプションがサポートされていません。

ただし、承認ルールは、パッチベースラインの作成時または最終更新時に [Include nonsecurity updates (セキュリティ以外の更新を含める)] チェックボックスがオンになっているかどうかによっても影響を受けます。

セキュリティ以外の更新が除外されている場合、暗黙のルールを適用してセキュリティリポのアップグレードを持つパッケージのみを選択します。選択対象の各パッケージは、セキュリティリポに属する適切なバージョン (通常は最新バージョン) のパッケージであることが必要です。

セキュリティ以外の更新が含まれている場合は、他のリポジトリからのパッチも考慮されます。

> **Note**
>
> Debian Server および Raspberry Pi OS では、パッチの候補となるバージョンは `debian-security` に含まれているパッチに限定されます。

5. パッチベースラインの指定どおりに ApprovedPatches を適用します。承認済みパッチについては、GlobalFilters によって破棄されている場合や、ApprovalRules に指定された承認ルールから承認が付与されていない場合でも、更新が承認されます。
6. パッチベースラインの指定どおりに RejectedPatches を適用します。承認済みパッチのリストから削除された拒否済みパッチは、適用されません。
7. APT ライブラリを使用してパッケージをアップグレードします。

> **Note**
>
> Patch Manager では、APT `Pin-Priority` オプションを使用したパッケージへの優先順位割り当てはサポートされていません。Patch Manager は、有効なすべてのリポジトリから利用可能な更新を集約し、インストールされた各パッケージのベースラインに一致する最新の更新を選択します。

8. 更新がインストールされると、マネージドノードは再起動されます。(例外: `RebootOption` パラメータが `AWS-RunPatchBaseline` ドキュメントの `NoReboot` で設定されている場合、パッチマネージャーの Patch Manager 実行後にマネージドノードは再起動されません。詳細については、「パラメータ名: `RebootOption`」を参照してください。)

macOS

macOS マネージドノードの場合、パッチのインストール ワークフローは次のとおりです。

1. `/Library/Receipts/InstallHistory.plist` プロパティリストは、`softwareupdate` および `installer` パッケージマネージャーを使用してインストールおよびアップグレードされたソフトウェアのレコードです。`pkgutil` コマンドラインツール (`installer` 用) と `softwareupdate` パッケージマネージャーを使用して、CLI コマンドはこのリストを解析するために実行されます。

   `installer` の場合、CLI コマンドに対する応答には `package name`、`version`、`volume`、`location`、および `install-time` の詳細が含まれますが、Patch Manager で使用されるのは、`package name` と `version` のみです。

`softwareupdate` の場合、CLI コマンドへの応答にはパッケージ名 (`display name`)、`version`、`date` が含まれますが、パッチマネージャーで使用されるのは、パッケージ名とバージョンのみです。

Brew と Brew Cask の場合、Homebrew は root ユーザーで実行されるコマンドをサポートしていません。その結果、Patch Manager は Homebrew ディレクトリの所有者、または Homebrew ディレクトリの所有者グループに属する有効なユーザーとして、Homebrew コマンドを照会して実行します。コマンドは、`softwareupdate` と `installer` に似ており、Python サブプロセスを介してパッケージデータを収集し、出力を解析してパッケージ名とバージョンを識別します。

2. パッチベースラインの指定どおりに GlobalFilters を適用し、対象のパッケージのみを追加処理のために保持します。
3. パッチベースラインの指定どおりに ApprovalRules を適用します。各承認ルールは、承認されたとおりにパッケージを定義できます。
4. パッチベースラインの指定どおりに ApprovedPatches を適用します。承認済みパッチについては、GlobalFilters によって破棄されている場合や、ApprovalRules に指定された承認ルールから承認が付与されていない場合でも、更新が承認されます。
5. パッチベースラインの指定どおりに RejectedPatches を適用します。承認済みパッチのリストから削除された拒否済みパッチは、適用されません。
6. 複数のバージョンのパッチが承認されている場合は、最新バージョンが適用されます。
7. マネージドノードで適切なパッケージ CLI を呼び出し、承認されたパッチを次のように処理します。

> **Note**
>
> `installer` には、更新プログラムを確認してインストールする機能がありません。したがって、`installer` では、Patch Manager はインストールされているパッケージのみをレポートします。その結果、`installer` パッケージは `Missing` として報告されることはありません。

- AWS により事前定義されたデフォルトのパッチベースラインと、カスタムのパッチベースラインについては、[セキュリティ以外の更新を含める] チェックボックスがオフである場合、セキュリティの更新のみが適用されます。

- カスタムのパッチベースラインについては、[セキュリティ以外の更新を含める] チェックボックスがオンである場合、セキュリティの更新とセキュリティ以外の更新の両方が適用されます。

8. 更新がインストールされると、マネージドノードは再起動されます。(例外: `RebootOption` パラメータが `AWS-RunPatchBaseline` ドキュメントの `NoReboot` で設定されている場合、パッチマネージャーの Patch Manager 実行後にマネージドノードは再起動されません。詳細については、「パラメータ名: `RebootOption`」を参照してください。)

Oracle Linux

Oracle Linux マネージドノードの場合、パッチのインストール ワークフローは次のとおりです。

1. パッチのリストが https URL または Amazon Simple Storage Service (Amazon S3) パススタイルの URL を使用して、`AWS-RunPatchBaseline` または `AWS-RunPatchBaselineAssociation` ドキュメントの `InstallOverrideList` パラメータを使用して指定されている場合、リストされたパッチがインストールされ、手順 2〜7 はスキップされます。
2. パッチベースラインの指定どおりに GlobalFilters を適用し、対象のパッケージのみを追加処理のために保持します。
3. パッチベースラインの指定どおりに ApprovalRules を適用します。各承認ルールは、承認されたとおりにパッケージを定義できます。

   ただし、承認ルールは、パッチベースラインの作成時または最終更新時に [Include nonsecurity updates (セキュリティ以外の更新を含める)] チェックボックスがオンになっているかどうかによっても影響を受けます。

   セキュリティ以外の更新が除外されている場合、暗黙のルールを適用してセキュリティリポのアップグレードを持つパッケージのみを選択します。選択対象の各パッケージは、セキュリティリポに属する適切なバージョン (通常は最新バージョン) のパッケージであることが必要です。

   セキュリティ以外の更新が含まれている場合は、他のリポジトリからのパッチも考慮されます。
4. パッチベースラインの指定どおりに ApprovedPatches を適用します。承認済みパッチについては、GlobalFilters によって破棄されている場合や、ApprovalRules に指定された承認ルールから承認が付与されていない場合でも、更新が承認されます。

5. パッチベースラインの指定どおりに RejectedPatches を適用します。承認済みパッチのリストから削除された拒否済みパッチは、適用されません。
6. 複数のバージョンのパッチが承認されている場合は、最新バージョンが適用されます。
7. バージョン 7 マネージドノードでは、YUM 更新 API が、次のように承認済みパッチに適用されます。
   - AWS により事前定義されたデフォルトのパッチベースライン、およびカスタムのパッチベースラインについては、[セキュリティ以外の更新を含める] チェックボックスがオフである場合、updateinfo.xml で指定されたパッチのみが適用されます (セキュリティの更新のみ)。

     このワークフローに該当する yum コマンドは次のとおりです。

     ```
     sudo yum update-minimal --sec-severity=Important,Moderate --bugfix -y
     ```

   - カスタムのパッチベースラインについては、[セキュリティ以外の更新を含める] チェックボックスがオンである場合、updateinfo.xml にあるパッチと updateinfo.xml にないパッチの両方が適用されます (セキュリティの更新とセキュリティ以外の更新)。

     このワークフローに該当する yum コマンドは次のとおりです。

     ```
     sudo yum update --security --bugfix -y
     ```

     バージョン 8 と 9 のマネージドノードでは、DNF 更新 API が、次のように承認済みパッチに適用されます。

   - AWS により事前定義されたデフォルトのパッチベースライン、およびカスタムのパッチベースラインについては、[セキュリティ以外の更新を含める] チェックボックスがオフである場合、updateinfo.xml で指定されたパッチのみが適用されます (セキュリティの更新のみ)。

     このワークフローに該当する yum コマンドは次のとおりです。

     ```
     sudo dnf upgrade-minimal --security --sec-severity=Moderate --sec-
     severity=Important
     ```

   - カスタムのパッチベースラインについては、[セキュリティ以外の更新を含める] チェックボックスがオンである場合、updateinfo.xml にあるパッチと updateinfo.xml にないパッチの両方が適用されます (セキュリティの更新とセキュリティ以外の更新)。

このワークフローに該当する yum コマンドは次のとおりです。

```
sudo dnf upgrade --security --bugfix
```

> **Note**
>
> yum または dnf コマンドを Patch Manager の外で実行すると、古くなったパッケージに代わる新しいパッケージが別の名前でインストールされます。ただし、同等の Patch Manager オペレーションではインストールされません。

8. 更新がインストールされると、マネージドノードは再起動されます。(例外: RebootOption パラメータが AWS-RunPatchBaseline ドキュメントの NoReboot で設定されている場合、パッチマネージャーの Patch Manager 実行後にマネージドノードは再起動されません。詳細については、「パラメータ名: RebootOption」を参照してください。)

AlmaLinux, RHEL, and Rocky Linux

AlmaLinux、Red Hat Enterprise Linux、および Rocky Linux マネージドノードで、パッチのインストール手順は次のとおりです。

1. パッチのリストが https URL または Amazon Simple Storage Service (Amazon S3) パススタイルの URL を使用して、AWS-RunPatchBaseline または AWS-RunPatchBaselineAssociation ドキュメントの InstallOverrideList パラメータを使用して指定されている場合、リストされたパッチがインストールされ、手順 2〜7 はスキップされます。
2. パッチベースラインの指定どおりに GlobalFilters を適用し、対象のパッケージのみを追加処理のために保持します。
3. パッチベースラインの指定どおりに ApprovalRules を適用します。各承認ルールは、承認されたとおりにパッケージを定義できます。

   ただし、承認ルールは、パッチベースラインの作成時または最終更新時に [Include nonsecurity updates (セキュリティ以外の更新を含める)] チェックボックスがオンになっているかどうかによっても影響を受けます。

   セキュリティ以外の更新が除外されている場合、暗黙のルールを適用してセキュリティリポのアップグレードを持つパッケージのみを選択します。選択対象の各パッケージは、セキュリ

ティリポに属する適切なバージョン (通常は最新バージョン) のパッケージであることが必要です。

セキュリティ以外の更新が含まれている場合は、他のリポジトリからのパッチも考慮されます。

4. パッチベースラインの指定どおりに ApprovedPatches を適用します。承認済みパッチについては、GlobalFilters によって破棄されている場合や、ApprovalRules に指定された承認ルールから承認が付与されていない場合でも、更新が承認されます。
5. パッチベースラインの指定どおりに RejectedPatches を適用します。承認済みパッチのリストから削除された拒否済みパッチは、適用されません。
6. 複数のバージョンのパッチが承認されている場合は、最新バージョンが適用されます。
7. YUM 更新 API (RHEL 7) または DNF 更新 API (AlmaLinux 8 および 9、RHEL 8 および 9、および Rocky Linux 8 および 9) は、承認されたパッチに次のルールに従って適用されます。

シナリオ 1: セキュリティ以外の更新が除外される

- 適用先: AWS によって提供される事前定義されたデフォルトのパッチベースラインとカスタムパッチベースライン。
- [セキュリティ以外の更新を含める] チェックボックス: オフ。
- 適用されるパッチ: `updateinfo.xml` で指定されたパッチ (セキュリティ更新のみ) は、どちらもパッチベースライン設定と一致し、設定されたリポジトリで見つかった場合にのみ適用されます。

  場合によっては、`updateinfo.xml` で指定されたパッチが、設定されたリポジトリで使用できなくなっていることがあります。通常、設定されるリポジトリには以前のすべての更新の累積的なロールアップであるパッチの最新バージョンのみが含まれていますが、最新バージョンがパッチベースラインルールと一致せず、パッチ適用オペレーションから除外される可能性があります。
- コマンド: RHEL 7 の場合、このワークフローに対する yum コマンドは次のとおりです。

```
sudo yum update-minimal --sec-severity=Critical,Important --bugfix -y
```

AlmaLinux、RHEL 8、および Rocky Linux の場合、このワークフローに対応する dnf コマンドは次のとおりです。

```
sudo dnf update-minimal --sec-severity=Critical --bugfix -y ; \
sudo dnf update-minimal --sec-severity=Important --bugfix -y
```

シナリオ 2: セキュリティ以外の更新が含まれる

- 適用先: カスタムパッチベースライン。
- [セキュリティ以外の更新を含める] チェックボックス: オン。
- 適用されるパッチ: `updateinfo.xml` にあるパッチと、`updateinfo.xml` にないパッチが適用されます (セキュリティ更新とセキュリティ以外の更新)。
- コマンド: RHEL 7 の場合、このワークフローに対する yum コマンドは次のとおりです。

```
sudo yum update --security --bugfix -y
```

AlmaLinux 8 および 9、RHEL 8 および 9、および Rocky Linux 8 および 9 の場合、このワークフローに相当する dnf コマンドは次のとおりです。

```
sudo dnf update --security --bugfix -y
```

> **Note**
>
> yum または dnf コマンドを Patch Manager の外で実行すると、古くなったパッケージに代わる新しいパッケージが別の名前でインストールされます。ただし、同等の Patch Manager オペレーションではインストールされません。

8. 更新がインストールされると、マネージドノードは再起動されます。(例外: `RebootOption` パラメータが `AWS-RunPatchBaseline` ドキュメントの `NoReboot` で設定されている場合、パッチマネージャーの Patch Manager 実行後にマネージドノードは再起動されません。詳細については、「パラメータ名: `RebootOption`」を参照してください。)

SLES

SUSE Linux Enterprise Server (SLES) マネージドノードの場合、パッチのインストール ワークフローは次のとおりです。

1. パッチのリストが https URL または Amazon Simple Storage Service (Amazon S3) パススタイルの URL を使用して、`AWS-RunPatchBaseline` または `AWS-`

RunPatchBaselineAssociation ドキュメントの InstallOverrideList パラメータを使用して指定されている場合、リストされたパッチがインストールされ、手順 2〜7 はスキップされます。

2. パッチベースラインの指定どおりに GlobalFilters を適用し、対象のパッケージのみを追加処理のために保持します。
3. パッチベースラインの指定どおりに ApprovalRules を適用します。各承認ルールは、承認されたとおりにパッケージを定義できます。

   ただし、承認ルールは、パッチベースラインの作成時または最終更新時に [Include nonsecurity updates (セキュリティ以外の更新を含める)] チェックボックスがオンになっているかどうかによっても影響を受けます。

   セキュリティ以外の更新が除外されている場合、暗黙のルールを適用してセキュリティリポのアップグレードを持つパッケージのみを選択します。選択対象の各パッケージは、セキュリティリポに属する適切なバージョン (通常は最新バージョン) のパッケージであることが必要です。

   セキュリティ以外の更新が含まれている場合は、他のリポジトリからのパッチも考慮されます。
4. パッチベースラインの指定どおりに ApprovedPatches を適用します。承認済みパッチについては、GlobalFilters によって破棄されている場合や、ApprovalRules に指定された承認ルールから承認が付与されていない場合でも、更新が承認されます。
5. パッチベースラインの指定どおりに RejectedPatches を適用します。承認済みパッチのリストから削除された拒否済みパッチは、適用されません。
6. 複数のバージョンのパッチが承認されている場合は、最新バージョンが適用されます。
7. Zypper 更新 API は、承認済みパッチに適用されます。
8. 更新がインストールされると、マネージドノードは再起動されます。(例外: RebootOption パラメータが AWS-RunPatchBaseline ドキュメントの NoReboot で設定されている場合、パッチマネージャーの Patch Manager 実行後にマネージドノードは再起動されません。詳細については、「パラメータ名: RebootOption」を参照してください。)

Ubuntu Server

Ubuntu Server マネージドノードの場合、パッチのインストール ワークフローは次のとおりです。

1. パッチのリストが https URL または Amazon Simple Storage Service (Amazon S3) パススタイルの URL を使用して、`AWS-RunPatchBaseline` または `AWS-RunPatchBaselineAssociation` ドキュメントの `InstallOverrideList` パラメータを使用して指定されている場合、リストされたパッチがインストールされ、手順 2〜7 はスキップされます。
2. 更新が可能な場合、`python3-apt` (Python ライブラリインターフェイスの `libapt`) は最新バージョンにアップグレードされます。(このセキュリティ以外のパッケージは、[Include nonsecurity updates (セキュリティ以外の更新プログラムを含める)] オプションが選択されていなくてもアップグレードされます。)
3. パッチベースラインの指定どおりに GlobalFilters を適用し、対象のパッケージのみを追加処理のために保持します。
4. パッチベースラインの指定どおりに ApprovalRules を適用します。各承認ルールは、承認されたとおりにパッケージを定義できます。

   > **Note**
   >
   > Ubuntu Server の更新プログラムパッケージのリリース日は確定できないため、このオペティングシステムでは自動承認オプションがサポートされていません。

   ただし、承認ルールは、パッチベースラインの作成時または最終更新時に [Include nonsecurity updates (セキュリティ以外の更新を含める)] チェックボックスがオンになっているかどうかによっても影響を受けます。

   セキュリティ以外の更新が除外されている場合、暗黙のルールを適用してセキュリティリポのアップグレードを持つパッケージのみを選択します。選択対象の各パッケージは、セキュリティリポに属する適切なバージョン (通常は最新バージョン) のパッケージであることが必要です。

   セキュリティ以外の更新が含まれている場合は、他のリポジトリからのパッチも考慮されます。

   ただし、承認ルールは、パッチベースラインの作成時または最終更新時に [セキュリティ以外の更新を含める] チェックボックスがオンになっているかどうかによっても影響を受けます。

> **Note**
>
> Ubuntu Server の各バージョンのパッチ候補バージョンは、次のように、そのバージョンの関連リポジトリに含まれるパッチに限定されます。
>
> - Ubuntu Server 14.04 LTS: `trusty-security`
> - Ubuntu Server 16.04 LTS: `xenial-security`
> - Ubuntu Server 18.04 LTS: `bionic-security`
> - Ubuntu Server 20.04 LTS): `focal-security`
> - Ubuntu Server 20.10 STR: `groovy-security`
> - Ubuntu Server 22.04 LTS: `jammy-security`
> - Ubuntu Server 23.04: `lunar-lobster`

5. パッチベースラインの指定どおりに ApprovedPatches を適用します。承認済みパッチについては、GlobalFilters によって破棄されている場合や、ApprovalRules に指定された承認ルールから承認が付与されていない場合でも、更新が承認されます。
6. パッチベースラインの指定どおりに RejectedPatches を適用します。承認済みパッチのリストから削除された拒否済みパッチは、適用されません。
7. APT ライブラリを使用してパッケージをアップグレードします。

> **Note**
>
> Patch Manager では、APT `Pin-Priority` オプションを使用したパッケージへの優先順位割り当てはサポートされていません。Patch Manager は、有効なすべてのリポジトリから利用可能な更新を集約し、インストールされた各パッケージのベースラインに一致する最新の更新を選択します。

8. 更新がインストールされると、マネージドノードは再起動されます。(例外: `RebootOption` パラメータが `AWS-RunPatchBaseline` ドキュメントの `NoReboot` で設定されている場合、パッチマネージャーの Patch Manager 実行後にマネージドノードは再起動されません。詳細については、「パラメータ名: `RebootOption`」を参照してください。)

Windows Server

Windows Server マネージドノードに対してパッチ適用オペレーションを実行すると、このノードは該当するパッチベースラインのスナップショットを Systems Manager にリクエストしま

す。このスナップショットには、デプロイ用に承認されたすべての使用可能な更新がパッチベースラインとして含まれています。この更新のリストが Windows Update API に送信されて、マネージドノードに適用できる更新が確認され、必要に応じてインストールされます。Windows では、KB の使用可能な最新バージョンのみをインストールできます。Patch Manager は、KB の最新バージョンまたは以前のバージョンの KB が、適用されたパッチベースラインと一致する場合に KB の最新バージョンをインストールします。更新のインストール後に、マネージドノードが必要な回数だけ再起動されて、すべての必要なパッチが適用されます。(例外: `RebootOption` パラメータが `AWS-RunPatchBaseline` ドキュメントの `NoReboot` で設定されている場合、パッチマネージャーの Patch Manager 実行後にマネージドノードは再起動されません。詳細については、「パラメータ名: `RebootOption`」を参照してください。) パッチ適用オペレーションの概要は、Run Command リクエストの出力で確認できます。詳細なログは、マネージドノードの `%PROGRAMDATA%\Amazon\PatchBaselineOperations\Logs` フォルダにあります。

KB のダウンロードとインストールには Windows Update API が使用されるため、Windows Update のすべてのグループポリシー設定が適用されます。Patch Manager の使用には、グループポリシー 設定は必須ではありませんが、ユーザー定義のすべての設定 (マネージドノードのターゲットを Windows Server Update Services (WSUS) サーバーにするなど) が適用されます。

> **Note**
>
> Windows では、Patch Managerは Windows Update API を使用して KB のダウンロードとインストールを行うため、デフォルトではすべての KB が Microsoft の Windows Update サイトからダウンロードされます。そのため、マネージドノードは Microsoft Windows Update サイトに接続できる必要があります。そうでないと、パッチ適用は失敗します。別の方法として、WSUS サーバーを KB レポジトリとして設定し、グループポリシーを使用して WSUS サーバーをターゲットとするようマネージドノードを設定できます。Patch Manager は、承認済みパッチリストまたは拒否済みパッチリストがベースライン設定に含まれている場合など、Windows Server のカスタムパッチベースラインを作成するときに KB ID を参照することがあります。Patch Manager がインストールするのは、KB ID が Microsoft Windows Update または WSUS サーバーに割り当てられている更新のみです。KB ID がない更新は、パッチ適用のオペレーションに含まれません。
> カスタムパッチベースラインの作成に関する詳細は、以下のトピックを参照してください。
>
> - Windows Server のカスタムパッチベースラインを作成する
> - パッチベースラインの作成 (CLI)
> - Windows オペレーティングシステムのパッケージ名の形式

Linux ベースシステムでのパッチベースラインルールの動作方法

Linux ディストリビューションのパッチベースラインのルールは、ディストリビューションタイプ別に動作が異なります。Windows Server マネージドノードでのパッチ更新とは異なり、ルールはノードごとに評価され、インスタンスに設定されているリポジトリが考慮されます。AWS Systems Manager のツールである Patch Manager は、ネイティブのパッケージマネージャーを使用して、パッチベースラインで承認されているパッチをインストールします。

パッチの重要度を報告する Linux ベースタイプのオペレーティングシステムの場合、Patch Manager は更新通知または個々のパッチのために、ソフトウェア発行者によって報告された重要度レベルを使用します。Patch Manager では、CVSS (共通脆弱性評価システム) のような サードパーティのソースからの、または NVD (National Vulnerability Database) がリリースしたメトリクスからの重要度レベルは取得しません。

トピック

- Amazon Linux 1、Amazon Linux 2、Amazon Linux 2022、および Amazon Linux 2023 でのパッチベースラインルールの仕組み
- CentOS および CentOS Stream でのパッチベースラインルールの動作方法
- Debian Server および Raspberry Pi OS でのパッチベースラインルールの動作方法
- macOS でのパッチベースラインルールの仕組み
- Oracle Linux でのパッチベースラインルールの仕組み
- AlmaLinux、RHEL、および Rocky Linux でのパッチベースラインルールの動作方法
- SUSE Linux Enterprise Server でのパッチベースラインルールの仕組み
- Ubuntu Server でのパッチベースラインルールの仕組み

Amazon Linux 1、Amazon Linux 2、Amazon Linux 2022、および Amazon Linux 2023 でのパッチベースラインルールの仕組み

> **Note**
>
> Amazon Linux 2023 (AL2023) は、1 つ以上のシステム設定を通じて特定のバージョンにロックできるバージョン管理されたリポジトリを使用します。AL2023 EC2 インスタンスに対するすべてのパッチ適用オペレーションについて、Patch Manager はシステム設定に関係なく、最新のリポジトリバージョンを使用します。詳細については、「Amazon Linux 2023 ユーザーガイド」の「バージョン対応リポジトリによる確定的なアップグレード」を参照してください。

Amazon Linux 1、Amazon Linux 2、Amazon Linux 2022、および Amazon Linux 2023 のパッチの選択プロセスは、次のとおりです。

1. マネージドノードで、YUM ライブラリ (Amazon Linux 1、Amazon Linux 2) または DNF ライブラリ (Amazon Linux 2022 および Amazon Linux 2023) が各設定済みリポジトリの `updateinfo.xml` ファイルにアクセスします。

   `updateinfo.xml` ファイルが見つからない場合、パッチがインストールされるかどうかは、[セキュリティ以外の更新を含める] および [自動承認] の設定に応じます。例えば、セキュリティ以外の更新プログラムが許可されている場合は、自動承認時刻が到来したときにインストールされます。

2. `updateinfo.xml` の更新通知ごとに、次の表に示すように、通知内のパッケージのプロパティを表す複数の属性が含まれています。

   更新通知の属性

属性	説明
type	パッチベースラインの PatchFilter データ型の分類キー属性の値に対応します。更新通知に含まれているパッケージのタイプを表します。 サポートされている値のリストは、AWS CLI コマンド describe-patch-properties または API オペレーション DescribePatchProperties を使用して表示できます。Systems Manager コンソールの [Create patch baseline (パッチベースラインの作成)] ページまたは [Edit patch baseline (パッチベースラインの編集)] ページの [Approval rules (承認ルール)] 領域でリストを表示することもできます。
severity	パッチベースラインの PatchFilter データ型の重要度キー属性の値に対応します。更新通知に含まれているパッケージの重要度を表します。通常、セキュリティ更新通知にのみ適用されます。

属性	説明
	サポートされている値のリストは、AWS CLI コマンド describe-patch-properties または API オペレーション DescribePatchProperties を使用して表示できます。Systems Manager コンソールの [パッチベースラインの作成] ページまたは [パッチベースラインの編集] ページの [承認ルール] 領域でリストを表示することもできます。
update_id	ALAS-2017-867 などのアドバイザリ ID を表します。アドバイザリ ID は、パッチベースラインの ApprovedPatches 属性または RejectedPatches 属性で使用できます。
references	更新通知の詳細情報を示します。CVE ID (形式: CVE-2017-1234567) などが該当します。CVE ID は、パッチベースラインの ApprovedPatches 属性または RejectedPatches 属性で使用できます。
更新済み	パッチベースラインの ApproveAfterDays に対応します。更新通知に含まれているパッケージのリリース日 (更新日) を表します。この属性 (および `ApproveAfterDays`) の値と現在のタイムスタンプとを比較することで、パッチのデプロイを承認するかどうかが決定されます。

承認済みパッチと拒否済みパッチのリストの許容されるフォーマットの詳細については、「承認されたパッチと拒否されたパッチのリストのパッケージ名の形式」を参照してください。

3. マネージドノードの成果は、SSM Agent で決まります。この属性は、パッチベースラインの PatchFilter データ型のプロダクトキー属性の値に対応します。
4. 更新用のパッケージは、次のガイドラインに従って選択されます。

セキュリティオプション	パッチの選択

AWS が提供した事前定義済みのデフォルトパッチベースラインと、[セキュリティ以外の更新を含める] チェックボックスが選択されていないカスタムパッチベースライン	`updateinfo.xml` の更新通知ごとに、パッチベースラインがフィルターとして使用され、該当するパッケージのみが更新に取り込まれます。パッチベースラインの定義の適用後に複数のパッケージが該当する場合は、最新バージョンが使用されます。
	
	Amazon Linux 1 および Amazon Linux 2 の場合、このワークフローに対する同等の yum コマンドは次のとおりです。
	
	`sudo yum update-minimal --sec-severity=Critical,Important --bugfix -y`
	
	Amazon Linux 2022 および Amazon Linux 2023 の場合、このワークフローに対する dnf コマンドは次のとおりです。
	
	`sudo dnf upgrade-minimal --sec-severity=Critical --sec-severity=Important --bugfix -y`

セキュリティオプション	パッチの選択

[セキュリティ以外の更新を含める] チェックボックスがオンで、重要度リストが [Critical, Important] 、分類リストが [Security, Bugfix] である、カスタムパッチベースライン	Patch Manager は、updateinfo.xml から選択したセキュリティ更新を適用するだけでなく、パッチのフィルタリングルールに該当しないセキュリティに関連しない更新を適用します。
	
	Amazon Linux および Amazon Linux 2 の場合、このワークフローに対する yum コマンドは次のとおりです。
	
	`sudo yum update --security --sec-severity=Critical,Important --bugfix -y`
	
	Amazon Linux 2022 および Amazon Linux 2023 の場合、このワークフローに対する dnf コマンドは次のとおりです。
	
	`sudo dnf upgrade --security --sec-severity=Critical --sec-severity=Important --bugfix -y`
	
	Note
	yum または dnf コマンドを Patch Manager の外で実行すると、古くなったパッケージに代わる新しいパッケージが別の名前でインストールされます。ただし、同等の Patch Manager オペレーションではインストールされません。

パッチのコンプライアンスステータス値については、「パッチコンプライアンス状態の値」を参照してください。

CentOS および CentOS Stream でのパッチベースラインルールの動作方法

CentOS と CentOS Stream デフォルトリポジトリに `updateinfo.xml` ファイルは含まれていません。ただし、作成または使用するカスタムリポジトリにはこのファイルが含まれる場合があります。このトピックでは、`updateinfo.xml` への参照はこれらのカスタムリポジトリにのみ適用されます。

CentOS および CentOS Stream の場合、パッチの選択プロセスは次のとおりです。

1. マネージドノードで、YUM ライブラリ (CentOS 6.x および 7.x バージョン) または DNF ライブラリ (CentOS 8.x および CentOS Stream) が各設定済みリポジトリの `updateinfo.xml` ファイル (カスタムリポジトリに存在する場合) にアクセスします。

   必ず含まれるデフォルトリポジトリでも `updateinfo.xml` ファイルが見つからない場合、パッチがインストールされるかどうかは、[セキュリティ以外の更新を含める] および [自動承認] の設定によって異なります。例えば、セキュリティ以外の更新プログラムが許可されている場合は、自動承認時刻が到来したときにインストールされます。
2. `updateinfo.xml` が存在する場合、ファイル内の各更新通知には、次の表に示すように、通知内のパッケージのプロパティを表す複数の属性が含まれています。

   更新通知の属性

属性	説明
type	パッチベースラインの PatchFilter データ型の分類キー属性の値に対応します。更新通知に含まれているパッケージのタイプを表します。 サポートされている値のリストは、AWS CLI コマンド describe-patch-properties または API オペレーション DescribePatchProperties を使用して表示できます。Systems Manager コンソールの [Create patch baseline (パッチベースラインの作成)] ページまたは [Edit patch baseline (パッチベースラインの編集)] ページの [Approval rules (承認ルール)] 領域でリストを表示することもできます。

属性	説明
severity	パッチベースラインの PatchFilter データ型の重要度キー属性の値に対応します。更新通知に含まれているパッケージの重要度を表します。通常、セキュリティ更新通知にのみ適用されます。 サポートされている値のリストは、AWS CLI コマンド describe-patch-properties または API オペレーション DescribePatchProperties を使用して表示できます。Systems Manager コンソールの [パッチベースラインの作成] ページまたは [パッチベースラインの編集] ページの [承認ルール] 領域でリストを表示することもできます。
update_id	CVE-2019-17055 などのアドバイザリ ID を表します。アドバイザリ ID は、パッチベースラインの ApprovedPatches 属性または RejectedPatches 属性で使用できます。
references	更新通知の詳細情報を示します。CVE ID (形式: CVE-2019-17055) または Bugzilla ID (形式: 1463241) などが該当します。CVE ID と Bugzilla ID は、パッチベースラインの ApprovedPatches 属性または RejectedPatches 属性で使用できます。
更新済み	パッチベースラインの ApproveAfterDays に対応します。更新通知に含まれているパッケージのリリース日 (更新日) を表します。この属性 (および `ApproveAfterDays`) の値と現在のタイムスタンプとを比較することで、パッチのデプロイを承認するかどうかが決定されます。

承認済みパッチと拒否済みパッチのリストの許容されるフォーマットの詳細については、「承認されたパッチと拒否されたパッチのリストのパッケージ名の形式」を参照してください。

3. どの場合でも、マネージドノードの成果は、SSM Agent で決まります。この属性は、パッチベースラインの PatchFilter データ型のプロダクトキー属性の値に対応します。
4. 更新用のパッケージは、次のガイドラインに従って選択されます。

セキュリティオプション	パッチの選択

AWS が提供した事前定義済みのデフォルトパッチベースラインと、[セキュリティ以外の更新を含める] チェックボックスが選択されていないカスタムパッチベースライン	`updateinfo.xml` の更新通知ごとに、カスタムリポジトリに存在する場合は、パッチベースラインがフィルターとして使用され、該当するパッケージのみが更新に取り込まれます。パッチベースラインの定義の適用後に複数のパッケージが該当する場合は、最新バージョンが使用されます。
	
	`updateinfo.xml` が存在する CentOS 6 および 7 の場合、このワークフローに対応する yum コマンドは次のとおりです。
	
	`sudo yum update-minimal --sec-severity=Critical,Important --bugfix -y`
	
	`updateinfo.xml` が存在する CentOS 8 および CentOS Stream の場合、このワークフローに対応する dnf コマンドは次のとおりです。
	
	`sudo dnf upgrade-minimal --sec-severity=Critical --sec-severity=Important --bugfix -y`

[セキュリティ以外の更新を含める] チェックボックスがオンで、重要度リストが `[Critical, Important]` 、分類リスト	Patch Manager は、`updateinfo.xml` から選択したセキュリティ更新を適用するだけでなく、カスタムリポジトリに存在する場合、

セキュリティオプション	パッチの選択

が [Security, Bugfix] である、カスタムパッチベースライン	パッチのフィルタリングルールに該当しないセキュリティに関連しない更新を適用します。
	
	updateinfo.xml が存在する CentOS 6 および 7 の場合、このワークフローに対応する yum コマンドは次のとおりです。
	
	`sudo yum update --sec-severity=Critical,Important --bugfix -y`
	
	updateinfo.xml が存在する CentOS 8 および CentOS Stream の場合、このワークフローに対応する dnf コマンドは次のとおりです。
	
	`sudo dnf upgrade --security --sec-severity=Critical --sec-severity=Important --bugfix -y`
	
	デフォルトのリポジトリと updateinfo.xml がないカスタムリポジトリでは、オペレーティングシステム (OS) パッケージを更新するために、[セキュリティ以外のアップデートを含める] チェックボックスを選択する必要があります。
	
	Note
	yum または dnf コマンドを Patch Manager の外で実行すると、古くなったパッケージに代わる新しいパッケージが別の名前でインストールされます。ただし、同等の Patch Manager

セキュリティオプション	パッチの選択
	オペレーションではインストールされません。

パッチのコンプライアンスステータス値については、「パッチコンプライアンス状態の値」を参照してください。

Debian Server および Raspberry Pi OS でのパッチベースラインルールの動作方法

Debian Server および Raspberry Pi OS (旧称 Raspbian) の場合、パッチベースラインサービスにより、[Priority] (優先度) フィールドと [Section] (セクション) フィールドでフィルタリングが行われます。通常、これらのフィールドはすべての Debian Server および Raspberry Pi OS パッケージに存在します。Patch Managerは、パッチベースラインでパッチが選択されているかどうかを確認するために以下の操作を行います。

1. Debian Server および Raspberry Pi OS システムの場合、`sudo apt-get update` と同等のコマンドを実行して使用可能なパッケージのリストを更新します。リポは設定されず、データは `sources` リストに設定されているリポから取得されます。
2. 更新が可能な場合、`python3-apt` (Python ライブラリインターフェイスの `libapt`) は最新バージョンにアップグレードされます。(このセキュリティ以外のパッケージは、[Include nonsecurity updates (セキュリティ以外の更新プログラムを含める)] オプションが選択されていなくてもアップグレードされます。)

> **Important**
>
> Debian Server 8 の場合のみ: Debian Server 8.* オペレーティングシステムはサポートされなくなったパッケージリポジトリ (`jessie-backports`) を参照するため、Patch Managerはパッチ適用オペレーションが正常に完了するように以下の追加の手順を実行します。
>
> a. お客様のマネージドノードでは、`jessie-backports` リポジトリへのリファレンスはソース場所リスト (`/etc/apt/sources.list.d/jessie-backports`) からコメントアウトされています。その結果、その場所からのパッチのダウンロードは試みられません。

b. Stretch のセキュリティの更新の署名キーがインポートされます。このキーによって、Debian Server 8.* ディストリビューションでの更新およびインストールオペレーションに必要なアクセス許可が付与されます。

c. この時点で、`apt-get` オペレーションを実行し、パッチ適用プロセスの開始前に最新バージョンの `python3-apt` がインストールされていることを確認します。

d. インストールプロセスが完了すると、`jessie-backports` リポジトリへの参照が復元され、署名キーが apt ソースキーリングから削除されます。これは、パッチ適用オペレーション前のシステム設定をそのまま残すために行われます。

3. 次に、GlobalFilters、ApprovalRules、ApprovedPatches、および RejectedPatches リストが適用されます。

> **Note**
>
> Debian Server の更新プログラムパッケージのリリース日は確定できないため、このオペレーティングシステムでは自動承認オプションがサポートされていません。

ただし、承認ルールは、パッチベースラインの作成時または最終更新時に [Include nonsecurity updates (セキュリティ以外の更新を含める)] チェックボックスがオンになっているかどうかによっても影響を受けます。

セキュリティ以外の更新が除外されている場合、暗黙のルールを適用してセキュリティリポのアップグレードを持つパッケージのみを選択します。選択対象の各パッケージは、セキュリティリポに属する適切なバージョン (通常は最新バージョン) のパッケージであることが必要です。この場合、Debian Server では、パッチの候補となるバージョンは以下のリポジトリに含まれているパッチに限定されます。

これらのリポは、次のように名前が付けられます。

- Debian Server 8: `debian-security jessie`
- Debian Server および Raspberry Pi OS 9: `debian-security stretch`
- Debian Server 10: `debian-security buster`
- Debian Server 11: `debian-security bullseye`
- Debian Server 12: `debian-security bookworm`

セキュリティ以外の更新が含まれている場合は、他のリポジトリからのパッチも考慮されます。

承認済みパッチと拒否済みパッチのリストの許容されるフォーマットの詳細については、「承認されたパッチと拒否されたパッチのリストのパッケージ名の形式」を参照してください。

[Priority] フィールドと [Section] フィールドの内容を表示するには、次の aptitude コマンドを実行します。

> **Note**
>
> 場合によっては、まず Debian Server システムに Aptitude をインストールする必要があります。

```
aptitude search -F '%p %P %s %t %V#' '~U'
```

このコマンドに対するレスポンスで、すべてのアップグレード可能なパッケージが次の形式で報告されます。

```
name, priority, section, archive, candidate version
```

パッチのコンプライアンスステータス値については、「パッチコンプライアンス状態の値」を参照してください。

macOS でのパッチベースラインルールの仕組み

macOS の場合、パッチの選択プロセスは次のとおりです。

1. マネージドノードで、Patch Manager は `InstallHistory.plist` ファイルの解析済みコンテンツにアクセスし、パッケージ名とバージョンを識別します。

   解析プロセスの詳細については、macOS の「パッチのインストール方法」のセクションを参照してください。
2. マネージドノードの成果は、SSM Agent で決まります。この属性は、パッチベースラインの PatchFilter データ型のプロダクトキー属性の値に対応します。
3. 更新用のパッケージは、次のガイドラインに従って選択されます。

セキュリティオプション	パッチの選択
AWS が提供した事前定義済みのデフォルトパッチベースラインと、[セキュリティ以外の更新を含める] チェックボックスが選択されていないカスタムパッチベースライン	使用可能な更新通知ごとに、パッチベースラインがフィルターとして使用され、該当するパッケージのみが更新に取り込まれます。パッチベースラインの定義の適用後に複数のパッケージが該当する場合は、最新バージョンが使用されます。
[セキュリティ以外の更新を含める] チェックボックスが選択されているカスタムパッチベースライン	パッチマネージャーは、`InstallHistory.plist` を使用して識別されたセキュリティ更新プログラムを適用するだけでなく、パッチフィルタールールに適合するセキュリティ以外の更新プログラムを適用します。

パッチのコンプライアンスステータス値については、「パッチコンプライアンス状態の値」を参照してください。

Oracle Linux でのパッチベースラインルールの仕組み

Oracle Linux の場合、パッチの選択プロセスは次のとおりです。

1. マネージドノードで、YUM ライブラリが各設定済みリポの `updateinfo.xml` ファイルにアクセスします。

   > **Note**
   >
   > `updateinfo.xml` ファイルは、リポジトリが Oracle で管理されていないと使用できない場合があります。`updateinfo.xml` ファイルが見つからない場合、パッチがインストールされるかどうかは、[セキュリティ以外の更新を含める] および [自動承認] の設定に応じます。例えば、セキュリティ以外の更新プログラムが許可されている場合は、自動承認時刻が到来したときにインストールされます。

2. `updateinfo.xml` の更新通知ごとに、次の表に示すように、通知内のパッケージのプロパティを表す複数の属性が含まれています。

更新通知の属性

属性	説明
type	パッチベースラインの PatchFilter データ型の分類キー属性の値に対応します。更新通知に含まれているパッケージのタイプを表します。 サポートされている値のリストは、AWS CLI コマンド describe-patch-properties または API オペレーション DescribePatchProperties を使用して表示できます。Systems Manager コンソールの [Create patch baseline (パッチベースラインの作成)] ページまたは [Edit patch baseline (パッチベースラインの編集)] ページの [Approval rules (承認ルール)] 領域でリストを表示することもできます。
severity	パッチベースラインの PatchFilter データ型の重要度キー属性の値に対応します。更新通知に含まれているパッケージの重要度を表します。通常、セキュリティ更新通知にのみ適用されます。 サポートされている値のリストは、AWS CLI コマンド describe-patch-properties または API オペレーション DescribePatchProperties を使用して表示できます。Systems Manager コンソールの [パッチベースラインの作成] ページまたは [パッチベースラインの編集] ページの [承認ルール] 領域でリストを表示することもできます。

属性	説明
update_id	CVE-2019-17055 などのアドバイザリ ID を表します。アドバイザリ ID は、パッチベースラインの ApprovedPatches 属性または RejectedPatches 属性で使用できます。
references	更新通知の詳細情報を示します。CVE ID (形式: CVE-2019-17055) または Bugzilla ID (形式: 1463241) などが該当します。CVE ID と Bugzilla ID は、パッチベースラインの ApprovedPatches 属性または RejectedPatches 属性で使用できます。
更新済み	パッチベースラインの ApproveAfterDays に対応します。更新通知に含まれているパッケージのリリース日 (更新日) を表します。この属性 (および ApproveAfterDays) の値と現在のタイムスタンプとを比較することで、パッチのデプロイを承認するかどうかが決定されます。

承認済みパッチと拒否済みパッチのリストの許容されるフォーマットの詳細については、「承認されたパッチと拒否されたパッチのリストのパッケージ名の形式」を参照してください。

3. マネージドノードの成果は、SSM Agent で決まります。この属性は、パッチベースラインの PatchFilter データ型のプロダクトキー属性の値に対応します。
4. 更新用のパッケージは、次のガイドラインに従って選択されます。

セキュリティオプション	パッチの選択
AWS が提供した事前定義済みのデフォルトパッチベースラインと、[セキュリティ以外の更新を含める] チェックボックスが選択されていないカスタムパッチベースライン	updateinfo.xml の更新通知ごとに、パッチベースラインがフィルターとして使用され、該当するパッケージのみが更新に取り込まれます。パッチベースラインの定義の適用後に複数のパッケージが該当する場合は、最新バージョンが使用されます。

セキュリティオプション	パッチの選択

	バージョン 7 マネージドノードの場合、このワークフローの同等の yum コマンドは次のとおりです。
	`sudo yum update-minimal --sec-severity=Important,Moderate --bugfix -y`
	バージョン 8 および 9 マネージドノードの場合、このワークフローの同等の dnf コマンドは次のとおりです。
	`sudo dnf upgrade-minimal --security --sec-severity=Moderate --sec-severity=Important`

セキュリティオプション	パッチの選択

[セキュリティ以外の更新を含める] チェックボックスがオンで、重要度リストが [Critical, Important] 、分類リストが [Security, Bugfix] である、カスタムパッチベースライン	Patch Manager は、updateinfo.xml から選択したセキュリティ更新を適用するだけでなく、パッチのフィルタリングルールに該当しないセキュリティに関連しない更新を適用します。
	
	バージョン 7 マネージドノードの場合、このワークフローの同等の yum コマンドは次のとおりです。
	
	`sudo yum update --security --sec-severity=Critical,Important --bugfix -y`
	
	バージョン 8 および 9 マネージドノードの場合、このワークフローの同等の dnf コマンドは次のとおりです。
	
	`sudo dnf upgrade --security --sec-severity=Critical, --sec-severity=Important --bugfix y`
	
	Note
	yum または dnf コマンドを Patch Manager の外で実行すると、古くなったパッケージに代わる新しいパッケージが別の名前でインストールされます。ただし、同等の Patch Manager オペレーションではインストールされません。

パッチのコンプライアンスステータス値については、「パッチコンプライアンス状態の値」を参照してください。

AlmaLinux、RHEL、および Rocky Linux でのパッチベースラインルールの動作方法

AlmaLinux、Red Hat Enterprise Linux (RHEL)、および Rocky Linux では、パッチの選択プロセスは次のとおりです。

1. マネージドノードで、YUM ライブラリ (RHEL 7) または DNF ライブラリ (AlmaLinux 8 および 9、RHEL 8 および 9、Rocky Linux 8 および 9) が各設定済みリポジトリの `updateinfo.xml` ファイルにアクセスします。

   > **Note**
   >
   > リポが Red Hat の管理対象外のものであると、`updateinfo.xml` ファイルは使用できない場合があります。`updateinfo.xml` が見つからない場合、パッチは適用されません。

2. `updateinfo.xml` の更新通知ごとに、次の表に示すように、通知内のパッケージのプロパティを表す複数の属性が含まれています。

   更新通知の属性

属性	説明
type	パッチベースラインの PatchFilter データ型の分類キー属性の値に対応します。更新通知に含まれているパッケージのタイプを表します。 サポートされている値のリストは、AWS CLI コマンド describe-patch-properties または API オペレーション DescribePatchProperties を使用して表示できます。Systems Manager コンソールの [Create patch baseline (パッチベースラインの作成)] ページまたは [Edit patch baseline (パッチベースラインの編集)] ページの [Approval rules (承認ルール)] 領域でリストを表示することもできます。
severity	パッチベースラインの PatchFilter データ型の重要度キー属性の値に対応します。更新通知に含まれているパッケージの重要度を表しま

属性	説明
	す。通常、セキュリティ更新通知にのみ適用されます。 サポートされている値のリストは、AWS CLI コマンド describe-patch-properties または API オペレーション DescribePatchProperties を使用して表示できます。Systems Manager コンソールの [パッチベースラインの作成] ページまたは [パッチベースラインの編集] ページの [承認ルール] 領域でリストを表示することもできます。
update_id	RHSA-2017:0864 などのアドバイザリ ID を表します。アドバイザリ ID は、パッチベースラインの ApprovedPatches 属性または RejectedPatches 属性で使用できます。
references	更新通知の詳細情報を示します。CVE ID (形式: CVE-2017-1000371) または Bugzilla ID (形式: 1463241) などが該当します。CVE ID と Bugzilla ID は、パッチベースラインの ApprovedPatches 属性または RejectedPatches 属性で使用できます。
更新済み	パッチベースラインの ApproveAfterDays に対応します。更新通知に含まれているパッケージのリリース日 (更新日) を表します。この属性 (および `ApproveAfterDays`) の値と現在のタイムスタンプとを比較することで、パッチのデプロイを承認するかどうかが決定されます。

承認済みパッチと拒否済みパッチのリストの許容されるフォーマットの詳細については、「承認されたパッチと拒否されたパッチのリストのパッケージ名の形式」を参照してください。

3. マネージドノードの成果は、SSM Agent で決まります。この属性は、パッチベースラインの PatchFilter データ型のプロダクトキー属性の値に対応します。
4. 更新用のパッケージは、次のガイドラインに従って選択されます。

セキュリティオプション	パッチの選択

AWS により事前定義されたデフォルトのパッチベースラインと [セキュリティ以外の更新を含める] チェックボックスがオフであるカスタムのパッチベースライン	`updateinfo.xml` の更新通知ごとに、パッチベースラインがフィルターとして使用され、該当するパッケージのみが更新に取り込まれます。パッチベースラインの定義の適用後に複数のパッケージが該当する場合は、最新バージョンが使用されます。
	
	RHEL 7 の場合、このワークフローに対する yum コマンドは次のとおりです。
	
	`sudo yum update-minimal --sec-severity=Critical,Important --bugfix -y`
	
	AlmaLinux 8 および 9、RHEL 8 および 9、および Rocky Linux 8 および 9 の場合、このワークフローに相当する dnf コマンドは次のとおりです。
	
	`sudo dnf upgrade-minimal --sec-severity=Critical --sec-severity=Important --bugfix -y`

[セキュリティ以外の更新を含める] チェックボックスがオンで、重要度リストが `[Critical, Important]` 、分類リストが `[Security, Bugfix]` である、カスタムパッチベースライン	Patch Manager は、`updateinfo.xml` から選択したセキュリティ更新を適用するだけでなく、パッチのフィルタリングルールに該当しないセキュリティに関連しない更新を適用します。 RHEL 7 の場合、このワークフローに対する yum コマンドは次のとおりです。

セキュリティオプション	パッチの選択

	`sudo yum update --security --sec-severity=Critical,Important --bugfix -y`
	
	AlmaLinux 8 および 9、RHEL 8 および 9、および Rocky Linux 8 および 9 の場合、このワークフローに相当する dnf コマンドは次のとおりです。
	
	`sudo dnf upgrade --sec-severity=Critical --sec-severity=Important --bugfix -y`
	
	Note
	yum または dnf コマンドを Patch Manager の外で実行すると、古くなったパッケージに代わる新しいパッケージが別の名前でインストールされます。ただし、同等の Patch Manager オペレーションではインストールされません。

パッチのコンプライアンスステータス値については、「パッチコンプライアンス状態の値」を参照してください。

SUSE Linux Enterprise Server でのパッチベースラインルールの仕組み

SLES では、各パッチには、パッチ内のパッケージのプロパティを示す以下の属性が含まれます。

- Category: パッチベースラインの PatchFilter データ型の Classification キー属性の値に対応します。更新通知に含まれているパッチのタイプを表します。

  サポートされている値のリストは、AWS CLI コマンド describe-patch-properties または API オペレーション DescribePatchProperties を使用して表示できます。Systems Manager コンソール

の [Create patch baseline (パッチベースラインの作成)] ページまたは [Edit patch baseline (パッチベースラインの編集)] ページの [Approval rules (承認ルール)] 領域でリストを表示することもできます。

- Severity: パッチベースラインの PatchFilter データ型の Severity キー属性の値に対応します。パッチの重要度を示します。

  サポートされている値のリストは、AWS CLI コマンド describe-patch-properties または API オペレーション DescribePatchProperties を使用して表示できます。Systems Manager コンソールの [Create patch baseline (パッチベースラインの作成)] ページまたは [Edit patch baseline (パッチベースラインの編集)] ページの [Approval rules (承認ルール)] 領域でリストを表示することもできます。

マネージドノードの成果は、SSM Agent で決まります。この属性は、パッチベースラインの PatchFilter データ型の プロダクト キー属性の値に対応します。

パッチごとに、パッチベースラインがフィルターとして使用され、該当するパッケージのみが更新に含まれます。パッチベースラインの定義の適用後に複数のパッケージが該当する場合は、最新バージョンが使用されます。

承認済みパッチと拒否済みパッチのリストの許容されるフォーマットの詳細については、「承認されたパッチと拒否されたパッチのリストのパッケージ名の形式」を参照してください。

Ubuntu Server でのパッチベースラインルールの仕組み

Ubuntu Server では、パッチベースラインサービスは、Priority フィールドと Section フィールドでフィルタリングを行います。通常、これらのフィールドはすべての Ubuntu Server パッケージにあります。Patch Managerは、パッチベースラインでパッチが選択されているかどうかを確認するために以下の操作を行います。

1. Ubuntu Server システムで、`sudo apt-get update` と同等のコマンドを実行して使用可能なパッケージのリストを更新します。リポは設定されず、データは `sources` リストに設定されているリポから取得されます。
2. 更新が可能な場合、`python3-apt` (Python ライブラリインターフェイスの `libapt`) は最新バージョンにアップグレードされます。(このセキュリティ以外のパッケージは、[Include nonsecurity updates (セキュリティ以外の更新プログラムを含める)] オプションが選択されていなくてもアップグレードされます。)
3. 次に、GlobalFilters、ApprovalRules、ApprovedPatches、および RejectedPatches リストが適用されます。

> **Note**
>
> Ubuntu Server の更新プログラムパッケージのリリース日は確定できないため、このオペレーティングシステムでは自動承認オプションがサポートされていません。

ただし、承認ルールは、パッチベースラインの作成時または最終更新時に [Include nonsecurity updates (セキュリティ以外の更新を含める)] チェックボックスがオンになっているかどうかによっても影響を受けます。

セキュリティ以外の更新が除外されている場合、暗黙のルールを適用してセキュリティリポのアップグレードを持つパッケージのみを選択します。選択対象の各パッケージは、セキュリティリポに属する適切なバージョン (通常は最新バージョン) のパッケージであることが必要です。この場合、Ubuntu Server では、パッチの候補となるバージョンは以下のリポジトリに含まれているパッチに限定されます。

- Ubuntu Server 14.04 LTS: `trusty-security`
- Ubuntu Server 16.04 LTS: `xenial-security`
- Ubuntu Server 18.04 LTS: `bionic-security`
- Ubuntu Server 20.04 LTS: `focal-security`
- Ubuntu Server 20.10 STR: `groovy-security`
- Ubuntu Server 22.04 LTS (`jammy-security`)
- Ubuntu Server 23.04 (`lunar-security`)

セキュリティ以外の更新が含まれている場合は、他のリポジトリからのパッチも考慮されます。

承認済みパッチと拒否済みパッチのリストの許容されるフォーマットの詳細については、「承認されたパッチと拒否されたパッチのリストのパッケージ名の形式」を参照してください。

[Priority] フィールドと [Section] フィールドの内容を表示するには、次の `aptitude` コマンドを実行します。

> **Note**
>
> 場合によっては、まず Ubuntu Server 16 システムに Aptitude をインストールする必要があります。

```
aptitude search -F '%p %P %s %t %V#' '~U'
```

このコマンドに対するレスポンスで、すべてのアップグレード可能なパッケージが次の形式で報告されます。

```
name, priority, section, archive, candidate version
```

パッチのコンプライアンスステータス値については、「パッチコンプライアンス状態の値」を参照してください。

Linux と Windows Server のパッチ適用オペレーションの違い

このトピックでは、AWS Systems Manager のツールである Patch Manager での Linux と Windows Server のパッチ適用における重要な違いについて説明します。

> **Note**
>
> Linux マネージドノードにパッチを適用するには、ノードが SSM Agent バージョン 2.0.834.0 以降実行されている必要があります。
> 新しいツールが Systems Manager に追加されるか、既存のツールが更新されると必ず、更新されたバージョンの SSM Agent がリリースされます。最新バージョンのエージェントを使用しないと、マネージドノードが Systems Manager の各種ツールや機能を使用できなくなる可能性があります。このため、マシン上で SSM Agent を最新状態に維持するプロセスを自動化することをお勧めします。詳細については、SSM Agent への更新の自動化 を参照してください。GitHub の「SSM Agent リリースノート」ページをサブスクライブすると、SSM Agent の更新に関する通知を受け取ることができます。

違い 1: パッチ評価

Patch Manager では、Windows マネージドノードと Linux マネージドノードで、どのパッチを提供するかを評価するプロセスが異なります。

リナックス

Linux のパッチ適用では、Systems Manager はパッチベースライン ルールと承認済みおよび拒否済みパッチのリストを各マネージドノードで評価します。Systems Manager が各ノードでパッチ適用を評価する必要があるのは、マネージドノードに設定された複数のリポジトリから既知のパッチと更新のリストが取得されるためです。

Windows

Windows のパッチ適用では、Systems Manager はパッチベースラインルールと承認済みおよび拒否済みパッチのリストをサービス内で直接評価します。これが可能なのは、Windows パッチが単一のリポジトリ (Windows Update) から取得されるためです。

違い 2: **`Not Applicable`** パッチ

Linux オペレーティングシステムには多数の使用可能なパッケージがあるため、Systems Manager では該当なし状態のパッチについて詳細をレポートしません。`Not Applicable` パッチとは、例えば、インスタンスに Apache がインストールされていない場合の Apache ソフトウェア用パッチなどです。Systems Manager は要約で多数の `Not Applicable` パッチをレポートしますが、マネージドノードで DescribeInstancePatches API を呼び出す場合、戻りデータには状態が `Not Applicable` のパッチは含まれません。この動作は、Windows とは異なります。

違い 3: SSM ドキュメントのサポート

`AWS-ApplyPatchBaseline` Systems Manager ドキュメント (SSM ドキュメント) では、Linux マネージドノードはサポートされていません。Linux、macOS、Windows Server マネージドノードにパッチベースラインを適用する上で推奨されている SSM ドキュメントは、`AWS-RunPatchBaseline` です。詳細については、マネージドノードへのパッチ適用のための SSM コマンドドキュメントおよびパッチ適用のための SSM コマンドドキュメント: `AWS-RunPatchBaseline`を参照してください。

違い 4: アプリケーションパッチ

Patch Managerの主な目的は、オペレーティングシステムにパッチを適用することです。ただし、Patch Managerを使用して、マネージドノードの一部のアプリケーションにパッチを適用することもできます。

リナックス

Linux オペレーティングシステムでは、Patch Manager は更新のために設定されたリポジトリを使用し、オペレーティングシステムとアプリケーションのパッチを区別しません。Patch Managerを使用して、更新を取得するリポジトリを定義できます。詳細については、「代替パッチソースリポジトリを指定する方法 (Linux)」を参照してください。

Windows

Windows Server マネージドノードでは、Microsoft Word 2016 や Microsoft Exchange Server 2016 など、Microsoft によってリリースされたアプリケーションに対して、[Approved] (承認済み)および

[Rejected] (拒否された) パッチの例外を適用できます。詳細については、「カスタムパッチベースラインの操作」を参照してください。

違い 5: カスタムパッチベースラインでの拒否されたパッチリストのオプション

カスタムパッチベースラインを作成するときは、拒否されたパッチリストに 1 つ、または複数のパッチを指定できます。Linux マネージドノードでは、パッチがベースラインで許可されている別のパッチの依存関係である場合に、それらのインストールを許可することも選択できます。

ただし、Windows Server はパッチ依存関係の概念をサポートしません。Windows Server 向けのカスタムベースラインの [拒否されたパッチ] リストにパッチを追加することはできますが、その結果は (1) 拒否されたパッチがマネージドノードに既にインストールされているかどうか、および (2) [拒否されたパッチアクション] にどのオプションを選択するかに応じて異なります。

Windows Server での拒否されたパッチオプションの詳細については、以下の表を参照してください。

インストールステータス	オプション:「依存関係として許可する」	オプション:「ブロック」
パッチが既にインストールされている	報告されるステータス: `INSTALLED_OTHER`	報告されるステータス: `INSTALLED_REJECTED`
パッチがまだインストールされていない	パッチがスキップされた	パッチがスキップされた

通常、Microsoft がリリースする Windows Server 用の各パッチには、インストールが正常に行われるために必要なすべての情報が含まれています。ただし、手動でインストールする必要がある前提条件パッケージが必要になる場合もあります。Patch Manager は、これらの前提条件に関する情報を報告しません。関連情報については、Microsoft ウェブサイトで「Windows Update の問題のトラブルシューティング」を参照してください。

マネージドノードへのパッチ適用のための SSM コマンドドキュメント

このトピックでは、マネージドノードが最新のセキュリティアップデートでパッチが適用された状態に維持できるように公開されている 9 種類の Systems Manager ドキュメント (SSM ドキュメント) をご紹介します。

パッチ適用オペレーションで使用が推奨されているのは、これらのうち 5 種類のドキュメントのみです。これらの 5 つの SSM ドキュメントには、 を使用したパッチ適用オプションの詳細が記載されていますAWS Systems Manager これらのうち、4 つのドキュメントは、それらが置き換えられた 4 つのレガシー SSM ドキュメントよりも後にリリースされ、機能の拡張または統合を表しています。

パッチ適用に推奨されている SSM ドキュメント

パッチ適用オペレーションには、以下の 5 種類の SSM ドキュメントの使用をお勧めします。

- `AWS-ConfigureWindowsUpdate`
- `AWS-InstallWindowsUpdates`
- `AWS-RunPatchBaseline`
- `AWS-RunPatchBaselineAssociation`
- `AWS-RunPatchBaselineWithHooks`

パッチ適用のレガシー SSM ドキュメント

次の 4 つのレガシー SSM ドキュメントは、一部の AWS リージョン ではまだ使用できますが、更新されておらず、すべてのシナリオで機能することが保証されているわけではなく、今後サポートされなくなる可能性があります。パッチ適用オペレーションに使用しないことをお勧めします。

- `AWS-ApplyPatchBaseline`
- `AWS-FindWindowsUpdates`
- `AWS-InstallMissingWindowsUpdates`
- `AWS-InstallSpecificWindowsUpdates`

パッチ適用オペレーションでこれらの SSM ドキュメントを使用する方法の詳細については、次のセクションを参照してください。

トピック

- マネージドノードへのパッチ適用に推奨されている SSM ドキュメント
- マネージドノードへのパッチ適用のためのレガシー SSM ドキュメント
- パッチ適用のための SSM コマンドドキュメント: AWS-RunPatchBaseline
- パッチ適用のための SSM コマンドドキュメント: AWS-RunPatchBaselineAssociation

- パッチ適用のための SSM コマンドドキュメント: AWS-RunPatchBaselineWithHooks
- AWS-RunPatchBaseline または AWS-RunPatchBaselineAssociation で InstallOverrideList パラメータを使用するサンプルシナリオ
- BaselineOverride パラメータの使用

マネージドノードへのパッチ適用に推奨されている SSM ドキュメント

マネージドノードのパッチ適用オペレーションで使用が推奨されている SSM ドキュメントは、次の 5 つです。

推奨される SSM ドキュメント

- AWS-ConfigureWindowsUpdate
- AWS-InstallWindowsUpdates
- AWS-RunPatchBaseline
- AWS-RunPatchBaselineAssociation
- AWS-RunPatchBaselineWithHooks

`AWS-ConfigureWindowsUpdate`

Windows Update の基本機能の設定、その機能を使用した更新の自動インストール (または自動更新の無効化) をサポートします。すべての AWS リージョン で利用可能。

この SSM ドキュメントを使用すると、Windows Update において、指定の更新をダウンロードおよびインストールし、必要に応じてマネージドノードを再起動するよう求められます。この文書は、Windows Update がその設定を維持できるようにするために、AWS Systems Manager のツールである State Manager と一緒に使用してください。AWS Systems Manager のツールである Run Command を使用して手動で実行し、Windows Update 設定を変更することもできます。

このドキュメントで利用可能なパラメータを使用することで、インストールする更新のカテゴリ (または自動更新を無効にするかどうか) だけでなく、パッチ適用オペレーションを実行する日時と曜日を指定することができます。この SSM ドキュメントは、Windows updates で厳重に管理する必要なく、コンプライアンス情報を収集する必要がない場合に非常に便利です。

レガシーの SSM ドキュメントを置き換える:

- [なし]

AWS-InstallWindowsUpdates

Windows Server マネージドノードに更新ファイルをインストールします。すべての AWS リージョン で利用できます。

この SSM ドキュメントには、特定の更新をインストール (Include Kbs パラメータを使用) するか、特定の分類やカテゴリのパッチをインストールするが、パッチのコンプライアンス情報が不要な場合の基本パッチ適用機能について記載されています。

レガシーの SSM ドキュメントを置き換える:

- AWS-FindWindowsUpdates
- AWS-InstallMissingWindowsUpdates
- AWS-InstallSpecificWindowsUpdates

3 つのレガシードキュメントを使用してさまざまな機能を実行することができますが、新しい SSM ドキュメント (AWS-InstallWindowsUpdates) で別のパラメータ設定を使用して、同様の結果を得ることができます。これらのパラメータ設定については、「マネージドノードへのパッチ適用のためのレガシー SSM ドキュメント」を参照してください。

AWS-RunPatchBaseline

必要なパッチが適用されているかどうかを確認するには、マネージドノードにパッチをインストールするか、ノードをスキャンします。すべての AWS リージョン で利用できます。

AWS-RunPatchBaseline を使用すると、オペレーティングシステムタイプの「デフォルト」として指定されているパッチベースラインを使用して、パッチの承認を制御できます。Systems Manager Compliance ツールを使用して表示できるパッチコンプライアンス情報をレポートします。これらのツールでは、必要なパッチが適用されていないノードや、そのパッチの内容など、マネージドノードのパッチコンプライアンス状態に関する洞察を得ることができます。AWS-RunPatchBaseline を使用すると、PutInventory API コマンドを使用してパッチコンプライアンス情報が記録されます。Linux オペレーティングシステムの場合、マネージドノードに設定されたデフォルトのソースリポジトリと、カスタムのパッチベースラインで指定した代替のソースリポジトリの両方から、パッチに関するコンプライアンス情報が提供されます。代替ソースリポジトリの詳細については、「代替パッチソースリポジトリを指定する方法 (Linux)」を参照してください。Systems Manager Compliance ツールの詳細については、「AWS Systems Manager のコンプライアンス」を参照してください。

レガシードキュメントを置き換える:

- AWS-ApplyPatchBaseline

レガシー ドキュメント AWS-ApplyPatchBaseline は、Windows Server マネージドノードにのみ適用され、アプリケーションのパッチ適用をサポートしません。新しい AWS-RunPatchBaseline バージョンでは、Windows システムと Linux システムの両方で同じサポートが提供されます。 AWS-RunPatchBaselineドキュメントを使用するには、バージョン 2.0.834.0 以降の SSM Agent が必要です。

AWS-RunPatchBaseline SSM ドキュメントの詳細については、「パッチ適用のための SSM コマンドドキュメント: AWS-RunPatchBaseline」を参照してください。

AWS-RunPatchBaselineAssociation

必要なパッチが適用されているかどうかを確認するには、インスタンスにパッチをインストールするか、インスタンスをスキャンします。すべての商用 AWS リージョン で使用できます。

AWS-RunPatchBaselineAssociation はいくつかの重要な点で AWS-RunPatchBaseline とは異なります。

- AWS-RunPatchBaselineAssociation は、主に AWS Systems Manager のツールである Quick Setup を使用して作成された State Manager 関連付けでの使用を目的としています。具体的には、Quick Setup ホスト管理設定タイプを使用する場合、[Scan instances for missing patches daily] (不足しているパッチがないか毎日インスタンスをスキャンする) オプションを選択すると、システムはオペレーションに AWS-RunPatchBaselineAssociation を使用します。

  ただし、ほとんどの場合、独自のパッチ適用オペレーションを設定する場合は、AWS-RunPatchBaseline の代わりに、AWS-RunPatchBaselineWithHooks または AWS-RunPatchBaselineAssociation を選択する必要があります。

  詳細については、以下のトピックを参照してください。

  - AWS Systems Manager Quick Setup
  - パッチ適用のための SSM コマンドドキュメント: AWS-RunPatchBaselineAssociation
- AWS-RunPatchBaselineAssociation は、実行時にターゲットのセットで使用するパッチベースラインを識別するためのタグの使用をサポートしています。
- AWS-RunPatchBaselineAssociation を使用するパッチ適用オペレーションの場合、パッチコンプライアンスデータは特定の State Manager の関連付けに基づいてコンパイルされます。AWS-RunPatchBaselineAssociation 実行時に収集されたパッチコンプライアンスデータは、PutComplianceItems コマンドではなく、PutInventory API コマンドを使用して記録さ

れます。これにより、この特定の関連付けに関連付けられていないコンプライアンスデータが上書きされるのを防ぐことができます。

Linux オペレーティングシステムの場合、インスタンスに設定されたデフォルトのソースリポジトリと、カスタムのパッチベースラインで指定した代替のソースリポジトリの両方から、パッチに関するコンプライアンス情報が提供されます。代替ソースリポジトリの詳細については、「代替パッチソースリポジトリを指定する方法 (Linux)」を参照してください。Systems Manager Compliance ツールの詳細については、「AWS Systems Manager のコンプライアンス」を参照してください。

レガシードキュメントを置き換える:

- [なし]

AWS-RunPatchBaselineAssociation SSM ドキュメントの詳細については、「パッチ適用のための SSM コマンドドキュメント: AWS-RunPatchBaselineAssociation」を参照してください。

AWS-RunPatchBaselineWithHooks

マネージドノードにパッチをインストールするか、ノードをスキャンして、修飾されたパッチが欠けているかどうかを判断します。オプションのフックを使用すると、パッチ適用サイクル中の 3 つのポイントで SSM ドキュメントを実行できます。すべての商用 AWS リージョン で使用できます。macOS ではサポートされていません。

AWS-RunPatchBaselineWithHooks は その AWS-RunPatchBaseline オペレーションで Install とは異なります。

AWS-RunPatchBaselineWithHooks では、マネージドノードノードのパッチ適用中に指定されたポイントで実行されるライフサイクルフックがサポートされます。パッチのインストールにはマネージドノードの再起動が必要になる場合があるため、パッチ適用オペレーションは 2 つのイベントに分割され、合計 3 つのフックでカスタム機能をサポートします。最初のフックは Install with NoReboot オペレーションの前です。2 番目のフックは Install with NoReboot オペレーションの後です。3 番目のフックは、ノードの再起動後に使用できます。

レガシードキュメントを置き換える:

- [なし]

AWS-RunPatchBaselineWithHooks SSM ドキュメントの詳細については、「パッチ適用のための SSM コマンドドキュメント: AWS-RunPatchBaselineWithHooks」を参照してください。

マネージドノードへのパッチ適用のためのレガシー SSM ドキュメント

次の 4 つの SSM ドキュメントは、一部の AWS リージョン では引き続き使用できます。ただし、更新されておらず、今後サポートされなくなる可能性があるため、使用はお勧めしません。代わりに、「マネージドノードへのパッチ適用に推奨されている SSM ドキュメント」に記載されているドキュメントを使用します。

レガシーの SSM ドキュメント

- AWS-ApplyPatchBaseline
- AWS-FindWindowsUpdates
- AWS-InstallMissingWindowsUpdates
- AWS-InstallSpecificWindowsUpdates

AWS-ApplyPatchBaseline

Windows Server マネージドノードのみをサポートしますが、代わりの AWS-RunPatchBaseline にあるアプリケーションのパッチ適用のサポートは含みません。2017年8月以降にローンチされた AWS リージョン では使用できません。

> **Note**
>
> この SSM ドキュメントに置き換わる AWS-RunPatchBaseline を使用するには、2.0.834.0 以降のバージョンの SSM Agent が必要です。AWS-UpdateSSMAgent ドキュメントを使用して、マネージドノードを最新バージョンのエージェントに更新することができます。

AWS-FindWindowsUpdates

AWS-InstallWindowsUpdates に置き換えられ、すべて同じアクションを実行できます。2017年4月以降にローンチされた AWS リージョン では使用できません。

このレガシー SSM ドキュメントから同様の結果を得るには、推奨されている置換ドキュメント (AWS-InstallWindowsUpdates) で次のパラメータ設定を使用します。

- Action = Scan
- Allow Reboot = False

AWS-InstallMissingWindowsUpdates

AWS-InstallWindowsUpdates に置き換えられ、すべて同じアクションを実行できます。2017 年 4 月以降にローンチされた AWS リージョン では使用できません。

このレガシー SSM ドキュメントから同様の結果を得るには、推奨されている置換ドキュメント (AWS-InstallWindowsUpdates) で次のパラメータ設定を使用します。

- Action = Install
- Allow Reboot = True

AWS-InstallSpecificWindowsUpdates

AWS-InstallWindowsUpdates に置き換えられ、すべて同じアクションを実行できます。2017 年 4 月以降にローンチされた AWS リージョン では使用できません。

このレガシー SSM ドキュメントから同様の結果を得るには、推奨されている置換ドキュメント (AWS-InstallWindowsUpdates) で次のパラメータ設定を使用します。

- Action = Install
- Allow Reboot = True
- Include Kbs = *KB ############*

パッチ適用のための SSM コマンドドキュメント: **AWS-RunPatchBaseline**

AWS Systems Manager は、AWS Systems Manager のツールである Patch Manager 用の Systems Manager ドキュメント (SSM ドキュメント) である AWS-RunPatchBaseline をサポートしています。この SSM ドキュメントでは、セキュリティ関連および他のタイプの更新の両方について、マネージドノードにパッチ適用オペレーションを実行します。パッチグループが指定されていない場合、ドキュメントを実行すると、オペレーティングシステムタイプの「デフォルト」として指定されているパッチベースラインが使用されます。それ以外の場合は、パッチグループに関連付けられているパッチベースラインが使用されます。パッチグループの詳細については、「パッチグループ」を参照してください。

ドキュメント AWS-RunPatchBaseline を使用して、オペレーティングシステムとアプリケーションの両方にパッチを適用することができます。(Windows Server では、アプリケーションのサポートは、Microsoft がリリースしたアプリケーションの更新に制限されています)。

このドキュメントでは、Linux macOS、および Windows Server マネージドノードをサポートしています。ドキュメントは、プラットフォーム別に適切なアクションを実行します。

> **Note**
>
> Patch Manager は、レガシー SSM ドキュメント `AWS-ApplyPatchBaseline` もサポートしています。ただし、このドキュメントが対応するのは Windows マネージドノードのみです。Linux、macOS、および Windows Server マネージドノードでのパッチ適用をサポートしているため、代わりに `AWS-RunPatchBaseline` を使用することをお勧めします。`AWS-RunPatchBaseline`ドキュメントを使用するには、バージョン 2.0.834.0 以降の SSM Agent が必要です。

Windows Server

Windows Server マネージドノードの場合、`AWS-RunPatchBaseline` ドキュメントは、PowerShell モジュールをダウンロードして呼び出します。これに伴って、マネージドノードに適用するパッチベースラインのスナップショットがダウンロードされます。このパッチベースラインスナップショットには、Windows Server Update Services (WSUS) サーバーに対してパッチベースラインを照会することによってコンパイルされる承認済みパッチのリストが含まれています。このリストは、Windows Update API に渡され、ここで承認済みパッチのダウンロードとインストールが適切に制御されます。

Linux

Linux マネージドノードの場合、`AWS-RunPatchBaseline` ドキュメントは、Python モジュールを呼び出します。これに伴って、マネージドノードに適用するパッチベースラインのスナップショットがダウンロードされます。このパッチベースラインのスナップショットは、定義済みルールと、承認済みパッチおよび拒否済みパッチのリストを使用し、ノードタイプ別に適切なパッケージマネージャーを設定します。

- Amazon Linux 1、Amazon Linux 2、CentOS、Oracle Linux、および RHEL 7 マネージドノードでは、YUM が使用されています。YUM のオペレーションでは、Patch Manager には、`Python 2.6` またはそれ以降のサポートされているバージョン (2.6～3.10) が必要です。
- RHEL 8 マネージドノードでは DNF が使用されます。DNF のオペレーションでは、Patch Manager には、サポートされているバージョン (2.6～3.10) の `Python 2` または `Python 3` が必要です。(どちらのバージョンも RHEL 8 にはデフォルトでインストールされていません。どちらか一方を手動でインストールする必要があります。)

- Debian Server、Raspberry Pi OS、および Ubuntu Server インスタンスでは、APT が使用されています。APT のオペレーションでは、Patch Manager には、サポートされているバージョン (3.0 ~ 3.10) の `Python 3` が必要です。
- SUSE Linux Enterprise Server マネージドノードは Zypper を使用します。Zypper のオペレーションでは、Patch Manager には、`Python 2.6` またはそれ以降のサポートされているバージョン (2.6 ~ 3.10) が必要です。

macOS

macOS マネージドノードの場合、`AWS-RunPatchBaseline` ドキュメントは、Python モジュールを呼び出します。これに伴って、マネージドノードに適用するパッチベースラインのスナップショットがダウンロードされます。次に、Python サブプロセスがノードで AWS Command Line Interface (AWS CLI) を呼び出し、指定されたパッケージマネージャーのインストールおよび更新情報を取得し、各更新パッケージに適切なパッケージマネージャーを実行します。

各スナップショットは、AWS アカウント 、パッチグループ、オペレーティングシステム、スナップショット ID に固有のものです。スナップショットは、署名付きの Amazon Simple Storage Service (Amazon S3) URL を介して配信されます。この URL は、スナップショットが作成されてから 24 時間後に期限切れになります。ただし、URL の有効期限が切れた後に、同じスナップショットコンテンツを他のマネージドノードに適用する場合は、スナップショットを作成してから 3 日以内であれば新しい署名付き Amazon S3 URL を生成できます。これを行うには、get-deployable-patch-snapshot-for-instance コマンドを使用します。

すべての承認済みで適用可能な更新プログラムがインストールされ、必要に応じて再起動されると、パッチのコンプライアンス情報がマネージドノードで生成されて Patch Manager にレポートされます。

> **Note**
>
> `AWS-RunPatchBaseline` ドキュメントで `RebootOption` パラメータが `NoReboot` に設定されている場合、Patch Manager の実行後、マネージドノードは再起動されません。詳細については、「パラメータ名: `RebootOption`」を参照してください。

パッチコンプライアンスデータの表示方法については、「パッチコンプライアンスについて」を参照してください。

AWS-RunPatchBaseline 個のパラメータ

AWS-RunPatchBaseline では 6 つのパラメータがサポートされています。Operation パラメータは必須です。InstallOverrideList、BaselineOverride、RebootOption の各パラメータはオプションです。Snapshot-ID は技術的にはオプションですが、メンテナンスウィンドウを使用せずに AWS-RunPatchBaseline を実行する場合はカスタム値を指定することをお勧めします。このドキュメントをメンテナンスウィンドウオペレーションの一部として実行する場合は、Patch Manager がカスタム値を自動的に提供します。

パラメータ

- パラメータ名: Operation
- パラメータ名: AssociationId
- パラメータ名: Snapshot ID
- パラメータ名: InstallOverrideList
- パラメータ名: RebootOption
- パラメータ名: BaselineOverride
- パラメータ名: StepTimeoutSeconds

パラメータ名: **Operation**

使用: 必須。

オプション: Scan | Install。

Scan

Scan オプションを選択すると、AWS-RunPatchBaseline はマネージドノードのパッチコンプライアンス状態を確認し、この情報を Patch Manager に返します。Scan では、更新のインストールや、マネージドノードの再起動を求めません。その代わりに、このオペレーションでは、承認されたノードに適用可能なアップデートがどこに欠けているかを特定します。

インストール

Install オプションを選択すると、AWS-RunPatchBaseline はマネージドノードに見つからない承認済み更新と適用可能な更新のインストールを試行します。Install オペレーションの一部として生成されるパッチコンプライアンス情報には、見つからない更新は示されませんが、更新のインストールが何らかの原因で失敗した場合は「失敗」状態になっている更新がレポートされることがあります。更新がマネージドノードにインストールされるたびに、ノードが再起動さ

れ、更新がインストール済みで有効になっていることが確認されます。(例外: RebootOption パラメータが AWS-RunPatchBaseline ドキュメントの NoReboot で設定されている場合、パッチマネージャーの Patch Manager 実行後にマネージドノードは再起動されません。詳細については、「パラメータ名: RebootOption」を参照してください。)

> **Note**
>
> Patch Manager がマネージドノードを更新する前に、ベースラインルールで指定されているパッチがインストールされている場合、システムが予期したとおりに再起動しないことがあります。この可能性があるのは、パッチがユーザーによって手動でインストールされたか、Ubuntu Server の unattended-upgrades パッケージなどの別のプログラムによって自動的にインストールされた場合です。

パラメータ名: **AssociationId**

使用: オプション。

AssociationId は、AWS Systems Manager のツールである State Manager の、既存の関連付けの ID です。これは、指定した関連付けにコンプライアンスデータを追加するために Patch Manager で使用します。この関連付けは、Quick Setup のパッチポリシーでセットアップされたパッチ適用オペレーションに関連しています。

> **Note**
>
> AWS-RunPatchBaseline では、パッチポリシーベースラインのオーバーライドとともに AssociationId 値を指定すると、パッチ適用は PatchPolicy オペレーションとして実行され、AWS:ComplianceItem で報告される ExecutionType 値も PatchPolicy です。AssociationId 値が指定されていない場合、パッチ適用は Command オペレーションとして実行され、送信される AWS:ComplianceItem の ExecutionType 値のレポートも Command です。

使用する関連付けがまだない場合は、create-association コマンドを実行して関連付けを作成できます。

パラメータ名: **Snapshot ID**

使用: オプション。

Snapshot ID は、Patch Manager が使用する一意の ID (GUID) です。この ID により、1 回のオペレーションでパッチを適用するマネージドノードのすべてに同じ承認済みパッチのセットが適用されます。このパラメータは省略可能ですが、次の表に示すようにメンテナンスウィンドウで AWS-RunPatchBaseline を実行しているかどうかに応じて、推奨されるベストプラクティスが異なります。

AWS-RunPatchBaseline のベストプラクティス

モード	ベストプラクティス	詳細
メンテナンスウィンドウ内で AWS-RunPatchBaseline を実行する	スナップショット ID は指定しないでください。Patch Manager によって指定されます。	メンテナンスウィンドウを使用して AWS-RunPatchBaseline を実行する場合は、独自に生成したスナップショット ID を提供すべきではありません。このシナリオでは、メンテナンスウィンドウの実行 ID に基づく GUID 値が Systems Manager から提供されます。これにより、そのメンテナンスウィンドウでは、AWS-RunPatchBaseline のすべての呼び出しで正しい ID が使用されます。 このシナリオで値を指定しないと、パッチベースラインのスナップショットは 3 日以内に有効期限が切れる場合があります。スナップショットの有効期限が切れると、同じ ID を指定しても、別のスナップショットが生成されます。
メンテナンスウィンドウ外で AWS-RunPatchBaseline を実行する	スナップショット ID のカスタム GUID 値を生成および指定します。[1]	メンテナンスウィンドウを使用しないで AWS-RunPatchBaseline を実行する場合は、パッチベースライン

モード	ベストプラクティス	詳細
		ごとに一意のスナップショット ID を生成し指定することをお勧めします (特に、同一のオペレーションで AWS-RunPatchBaseline ドキュメントを複数のマネージドノードで実行する場合)。このシナリオで ID を指定しないと、コマンドの送信先のマネージドノードごとに異なるスナップショット ID が Systems Manager で生成されます。これにより、マネージドノード間で異なるパッチセットが指定される場合があります。 例えば、AWS Systems Manager のツールである Run Command を使用して AWS-RunPatchBaseline ドキュメントを直接実行し、50 個のマネージドノードのグループをターゲットにしているとします。カスタムスナップショット ID を指定すると、1 つのベースラインスナップショットが作成され、これがすべてのノードの評価とパッチ適用に使用されるため、すべてのノードの状態が一致します。

[1]Snapshot ID パラメータの値を生成するには、GUID を生成できる任意のツールを使用できます。たとえば、PowerShell では、New-Guid cmdlet を使用して 12345699-9405-4f69-bc5e-9315aEXAMPLE という形式の GUID を生成できます。

パラメータ名: **InstallOverrideList**

使用: オプション。

InstallOverrideList を使用すると、インストールするパッチのリストに対する https URL または Amazon S3 パス形式の URL を指定できます。このパッチインストールリストは、YAML 形式で管理され、デフォルトのパッチベースラインで指定されたパッチを上書きします。これにより、どのマネージドノードにどのパッチがインストールされているかを、より詳細にコントロールできます。

> **Important**
>
> InstallOverrideList ファイル名には、バックティック (`)、一重引用符 (')、二重引用符 (")、およびドル記号 ($) を含めることはできません。

InstallOverrideList パラメータを使用する場合のパッチ適用オペレーションの動作は、Linux および macOS マネージドノードと、Windows Server マネージドノードで異なります。Linux および macOS では、パッチがパッチベースラインルールと一致するかどうかにかかわらず、Patch Manager は、ノードで有効になっているリポジトリに存在する InstallOverrideList パッチリストに含まれるパッチを適用しようとします。一方、Windows Server ノードでは、InstallOverrideList パッチリスト内のパッチは、パッチベースラインルールとも一致する場合にのみ適用されます。

コンプライアンスレポートは、パッチの InstallOverrideList リストで指定するものではなく、パッチのベースラインで指定されているものに従ってパッチの状態が反映されることに注意してください。つまり、スキャンオペレーションは InstallOverrideList パラメータを無視します。これは、コンプライアンスレポートが、特定のパッチ適用オペレーションで承認されたものではなく、ポリシーに従ってパッチ状態を一貫して反映することを保証するためです。

単一のパッチベースラインを使用しながら、InstallOverrideList パラメータを使用して、異なるメンテナンスウィンドウスケジュールで異なるタイプのパッチをターゲットグループに適用する方法の詳細については、「AWS-RunPatchBaseline または AWS-RunPatchBaselineAssociation で InstallOverrideList パラメータを使用するサンプルシナリオ」を参照してください。

有効な URL 形式

> **Note**
>
> ファイルが公開されているバケットに格納されている場合は、「https」URL 形式または Amazon S3 パススタイルの URL を指定できます。ファイルがプライベートバケットに格納されている場合は、Amazon S3 パススタイルの URL を指定する必要があります。

- https URL 形式:

```
https://s3.aws-api-domain/amzn-s3-demo-bucket/my-windows-override-list.yaml
```

- Amazon S3 パス形式の URL :

```
s3://amzn-s3-demo-bucket/my-windows-override-list.yaml
```

有効な YAML コンテンツ形式

リストにパッチを指定するために使用する書式は、マネージドノードのオペレーティングシステムによって異なります。ただし、一般的な形式は次のとおりです。

```
patches:
    -
        id: '{patch-d}'
        title: '{patch-title}'
        {additional-fields}:{values}
```

YAML ファイルにフィールドを追加することはできますが、パッチオペレーション中は無視されます。

さらに、S3 バケットのリストを追加または更新する前に、YAML ファイルのフォーマットが有効であることを確認することをお勧めします。YAML 形式の詳細については、yaml.org を参照してください。検証ツールのオプションについては、ウェブで「yaml 形式の検証」を検索します。

Linux

id

id フィールドは必須です。これにより、パッケージ名とアーキテクチャを使用してパッチを指定します。例: `'dhclient.x86_64'`。ID にワイルドカードを使用すると、複数のパッケージを指定できます。例: `'dhcp*'` および `'dhcp*1.*'`。

タイトル

title フィールドはオプションですが、Linux システムでは追加のフィルタリング機能を提供します。title を使用する場合は、次のいずれかの形式でパッケージのバージョン情報を含める必要があります。

YUM/SUSE Linux Enterprise Server (SLES):

```
{name}.{architecture}:{epoch}:{version}-{release}
```

APT

```
{name}.{architecture}:{version}
```

Linux のパッチタイトルでは、任意の位置に 1 つ以上のワイルドカードを使用して一致するパッケージの数を拡張することができます。例: `'*32:9.8.2-0.*.rc1.57.amzn1'`。

例:

- apt パッケージのバージョン 1.2.25 が現在マネージドノードにインストールされていますが、バージョン 1.2.27 が利用できるようになりました。
- apt.amd64 バージョン 1.2.27 をパッチリストに追加します。これは apt utils.amd64 バージョン 1.2.27 に依存しますが、apt-utils.amd64 バージョン 1.2.25 がリストで指定されています。

この場合、apt バージョン 1.2.27 のインストールはブロックされ、「Failed-NonCompliant」として報告されます。

Windows Server

id

id フィールドは必須です。Microsoft Knowledge Base ID (KB2736693 など) および Microsoft Security Bulletin ID (MS17-023 など) を使用してパッチを指定する場合に使用します。

Windows 用のパッチリストで提供する他のフィールドはオプションであり、情報提供のみを目的としています。特定のパッチに関する詳細情報を提供するために、title、classification、severity などの追加フィールドを使用することができます。

macOS

id

id フィールドは必須です。id フィールドの値は、{package-name}.{package-version} 形式または {package_name} 形式のいずれかを使用して指定することができます。

サンプルパッチリスト

- Amazon Linux

```
patches:
    -
        id: 'kernel.x86_64'
    -
        id: 'bind*.x86_64'
        title: '32:9.8.2-0.62.rc1.57.amzn1'
    -
        id: 'glibc*'
    -
        id: 'dhclient*'
        title: '*12:4.1.1-53.P1.28.amzn1'
    -
        id: 'dhcp*'
        title: '*10:3.1.1-50.P1.26.amzn1'
```

- CentOS

```
patches:
    -
        id: 'kernel.x86_64'
    -
        id: 'bind*.x86_64'
        title: '32:9.8.2-0.62.rc1.57.amzn1'
    -
        id: 'glibc*'
    -
        id: 'dhclient*'
        title: '*12:4.1.1-53.P1.28.amzn1'
    -
        id: 'dhcp*'
        title: '*10:3.1.1-50.P1.26.amzn1'
```

- Debian Server

```
patches:
```

```
    -
        id: 'apparmor.amd64'
        title: '2.10.95-0ubuntu2.9'
    -
        id: 'cryptsetup.amd64'
        title: '*2:1.6.6-5ubuntu2.1'
    -
        id: 'cryptsetup-bin.*'
        title: '*2:1.6.6-5ubuntu2.1'
    -
        id: 'apt.amd64'
        title: '*1.2.27'
    -
        id: 'apt-utils.amd64'
        title: '*1.2.25'
```

- macOS

```
patches:
    -
        id: 'XProtectPlistConfigData'
    -
        id: 'MRTConfigData.1.61'
    -
        id: 'Command Line Tools for Xcode.11.5'
    -
        id: 'Gatekeeper Configuration Data'
```

- Oracle Linux

```
patches:
    -
        id: 'audit-libs.x86_64'
        title: '*2.8.5-4.el7'
    -
        id: 'curl.x86_64'
        title: '*.el7'
    -
        id: 'grub2.x86_64'
        title: 'grub2.x86_64:1:2.02-0.81.0.1.el7'
    -
        id: 'grub2.x86_64'
        title: 'grub2.x86_64:1:*-0.81.0.1.el7'
```

- Red Hat Enterprise Linux (RHEL)

```
patches:
    -
        id: 'NetworkManager.x86_64'
        title: '*1:1.10.2-14.el7_5'
    -
        id: 'NetworkManager-*.x86_64'
        title: '*1:1.10.2-14.el7_5'
    -
        id: 'audit.x86_64'
        title: '*0:2.8.1-3.el7'
    -
        id: 'dhclient.x86_64'
        title: '*.el7_5.1'
    -
        id: 'dhcp*.x86_64'
        title: '*12:5.2.5-68.el7'
```

- SUSE Linux Enterprise Server (SLES)

```
patches:
    -
        id: 'amazon-ssm-agent.x86_64'
    -
        id: 'binutils'
        title: '*0:2.26.1-9.12.1'
    -
        id: 'glibc*.x86_64'
        title: '*2.19*'
    -
        id: 'dhcp*'
        title: '0:4.3.3-9.1'
    -
        id: 'lib*'
```

- Ubuntu Server

```
patches:
    -
        id: 'apparmor.amd64'
```

```
        title: '2.10.95-0ubuntu2.9'
    -
        id: 'cryptsetup.amd64'
        title: '*2:1.6.6-5ubuntu2.1'
    -
        id: 'cryptsetup-bin.*'
        title: '*2:1.6.6-5ubuntu2.1'
    -
        id: 'apt.amd64'
        title: '*1.2.27'
    -
        id: 'apt-utils.amd64'
        title: '*1.2.25'
```

- Windows

```
patches:
    -
        id: 'KB4284819'
        title: '2018-06 Cumulative Update for Windows Server 2016 (1709) for x64-
based Systems (KB4284819)'
    -
        id: 'KB4284833'
    -
        id: 'KB4284835'
        title: '2018-06 Cumulative Update for Windows Server 2016 (1803) for x64-
based Systems (KB4284835)'
    -
        id: 'KB4284880'
    -
        id: 'KB4338814'
```

パラメータ名: **RebootOption**

使用: オプション。

オプション: RebootIfNeeded | NoReboot

デフォルト: RebootIfNeeded

> **Warning**
>
> デフォルトのオプションは RebootIfNeeded です。ユースケースに適したオプションを必ず選択してください。例えば、設定プロセスを完了するためにマネージドノードをすぐに再起動する必要がある場合は、RebootIfNeeded を選択します。または、スケジュールされた再起動時間までマネージドノードの可用性を維持する必要がある場合は、NoReboot を選択します。

> **Important**
>
> Amazon EMR (以前は Amazon Elastic MapReduce と呼ばれていました) のクラスターインスタンスへのパッチ適用には、Patch Manager を使用しないことをお勧めします。特に、RebootOption パラメータの RebootIfNeeded オプションは選択しないでください。(このオプションは、AWS-RunPatchBaseline、AWS-RunPatchBaselineAssociation、および AWS-RunPatchBaselineWithHooks のパッチ適用用の SSM コマンドドキュメントに記載されています。)
> Patch Manager を使用してパッチを適用する基本コマンドは、yum と dnf コマンドを使用します。そのため、パッケージのインストール方法が原因となり、オペレーションの互換性が失われます。Amazon EMR クラスターのソフトウェアを更新するための推奨方法については、「Amazon EMR 管理ガイド」の「Amazon EMR のデフォルト AMI の使用」を参照してください。

RebootIfNeeded

RebootIfNeeded オプションを選択すると、次のいずれかの場合にマネージドノードが再起動されます。

- Patch Manager が 1 つ以上のパッチをインストールしている場合。

  Patch Manager は、パッチによる再起動が必要かどうか評価しない場合。パッチで再起動が必要ない場合でも、システムは再起動されます。

- Patch Manager は、Install オペレーションの実行中、ステータスが INSTALLED_PENDING_REBOOT のパッチをひとつ以上検出します。

  INSTALLED_PENDING_REBOOT ステータスは、前回 Install オペレーションを実行したときにオプション NoReboot が選択されたことを意味する場合や、マネージドノードが最後に再起

動されたとき以降にパッチが Patch Manager 以外でインストールされたことを意味する場合があります。

上記 2 つの場合にマネージドノードを再起動すると、更新されたパッケージがメモリからフラッシュされ、パッチ適用と再起動の動作があらゆるオペレーティングシステムで一貫して維持されます。

NoReboot

NoReboot オプションを選択すると、Patch Manager が Install オペレーション中にパッチをインストールした場合でも、マネージドノードは再起動されません。このオプションは、パッチ適用後にマネージドノードを再起動する必要がないことがわかっている場合や、パッチ適用操作の再起動によって中断されないアプリケーションまたはプロセスがノードで実行されている場合に便利です。また、メンテナンスウィンドウを使用するなど、マネージドノードの再起動のタイミングをより詳細に制御する場合にも役立ちます。

パッチがインストールされている場合に NoReboot オプションを選択すると、ステータス InstalledPendingReboot がパッチに割り当てられます。ただし、マネージドノード自体は、Non-Compliant と表示されています。再起動が発生し、Scan オペレーションが実行されると、マネージドノードのステータスは Compliant に更新されます。

> **Important**
>
> NoReboot オプションは、オペレーティングシステムレベルの再起動のみを防ぎます。サービスレベルの再起動は、パッチ適用プロセスの一環として引き続き発生する可能性があります。例えば、Docker が更新されると、NoReboot が有効にされていても Amazon Elastic Container Service などの依存サービスが自動的に再起動される場合があります。中断してはならない重要なサービスがある場合は、一時的にインスタンスをサービスから削除したり、メンテナンス期間中にパッチ適用をスケジュールしたりするなどの追加の対策を検討してください。

パッチのインストール追跡ファイル: パッチ (特にシステムの最後の再起動以降にインストールされたパッチ) のインストールを追跡するために、Systems Manager は、マネージドノードのファイルを管理します。

> **Important**
>
> 追跡ファイルを削除または変更しないでください。このファイルを削除または破損すると、マネージドノードのパッチコンプライアンスレポートが不正確になります。ファイルを削

除または破損した場合は、ノードを再起動し、パッチのスキャンオペレーションを実行してファイルを復元します。

この追跡ファイルは、マネージドノードの以下の場所に保存されます。

- Linux オペレーティングシステム:
  - `/var/log/amazon/ssm/patch-configuration/patch-states-configuration.json`
  - `/var/log/amazon/ssm/patch-configuration/patch-inventory-from-last-operation.json`
- Windows Server オペレーティングシステム:
  - `C:\ProgramData\Amazon\PatchBaselineOperations\State\PatchStatesConfiguration.json`
  - `C:\ProgramData\Amazon\PatchBaselineOperations\State\PatchInventoryFromLastOperation.json`

パラメータ名: **`BaselineOverride`**

使用: オプション。

`BaselineOverride` パラメータを使用して、実行時にパッチ定義設定を定義できます。このベースラインオーバーライドは、S3 バケット内の JSON オブジェクトとして維持されます。これにより、パッチ適用操作で、デフォルトのパッチベースラインのルールを適用する代わりに、ホストオペレーティングシステムに一致する指定されたベースラインが使用されるようにします。

> **Important**
>
> `BaselineOverride` ファイル名には、バックティック (`)、一重引用符 (')、二重引用符 (")、およびドル記号 ($) を含めることはできません。

`BaselineOverride` パラメータの使用方法の詳細については、「BaselineOverride パラメータの使用」を参照してください。

パラメータ名: **`StepTimeoutSeconds`**

使用: オプション。

コマンドが失敗したとみなされるまでの経過時間 (秒、1 ~ 36,000 秒 (10 時間))。

パッチ適用のための SSM コマンドドキュメント: **AWS-RunPatchBaselineAssociation**

AWS-RunPatchBaseline ドキュメントと同様に、AWS-RunPatchBaselineAssociation では、セキュリティ関連および他のタイプの更新の両方について、インスタンスにパッチ適用オペレーションを実行します。また、ドキュメント AWS-RunPatchBaselineAssociation を使用して、オペレーティングシステムとアプリケーションの両方にパッチを適用することもできます。(Windows Server では、アプリケーションのサポートは、Microsoft がリリースしたアプリケーションの更新に制限されています)。

このドキュメントでは、Linux、macOS、および Windows Server 用の Amazon Elastic Compute Cloud (Amazon EC2) インスタンスがサポートされています。ハイブリッドおよびマルチクラウド環境内の非 EC2 ノードは、サポートされていません。このドキュメントでは、各プラットフォームに対して適切なアクションを実行し、Linux インスタンスおよび macOS インスタンスでは Python モジュールを、Windows インスタンスでは PowerShell モジュールを呼び出します。

ただし、AWS-RunPatchBaselineAssociation は、次の点で AWS-RunPatchBaseline とは異なります。

- AWS-RunPatchBaselineAssociation は、主に AWS Systems Manager のツールである Quick Setup を使用して作成された State Manager 関連付けでの使用を目的としています。具体的には、Quick Setup ホスト管理設定タイプを使用する場合、[Scan instances for missing patches daily] (不足しているパッチがないか毎日インスタンスをスキャンする) オプションを選択すると、システムはオペレーションに AWS-RunPatchBaselineAssociation を使用します。

  ただし、ほとんどの場合、独自のパッチ適用オペレーションを設定する場合は、AWS-RunPatchBaselineAssociation の代わりに、AWS-RunPatchBaseline または AWS-RunPatchBaselineWithHooks を選択する必要があります。
- AWS-RunPatchBaselineAssociation ドキュメントを使用すると、ドキュメントの BaselineTags パラメータフィールドでタグのキーペアを指定できます。AWS アカウント内のカスタムパッチベースラインがこれらのタグを共有している場合、AWS Systems Manager のツールである Patch Manager は、ターゲットインスタンスでの実行時に、オペレーティングシステムタイプに対して現在指定されている「デフォルト」パッチベースラインではなく、そのタグ付きベースラインを使用します。

> **Note**
>
> Quick Setup を使用してセットアップした以外のパッチオペレーションで AWS-RunPatchBaselineAssociation を使用することを選択し、そのオプションの BaselineTags パラメータを使用する場合は、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのインスタンスプロファイルに対する追加のアクセス許可を指定する必要があります。詳細については、「パラメータ名: BaselineTags」を参照してください。

次の形式はどちらも BaselineTags パラメータに対して有効です。

`Key=tag-key,Values=tag-value`

`Key=tag-key,Values=tag-value1,tag-value2,tag-value3`

> **Important**
>
> タグキーと値には、バックティック (`)、一重引用符 (')、二重引用符 (")、およびドル記号 ($) を含めることはできません。

- AWS-RunPatchBaselineAssociation の実行時に収集されるパッチコンプライアンスデータは、PutComplianceItems によって使用される PutInventory コマンドではなく、 AWS-RunPatchBaseline API コマンドを使用して記録されます。この違いは、特定の関連付けごとに保存およびレポートされるパッチコンプライアンス情報であることを意味します。この関連付けの外部で生成されたパッチコンプライアンスデータは上書きされません。
- AWS-RunPatchBaselineAssociation の実行後にレポートされるパッチコンプライアンス情報は、インスタンスが準拠しているかどうかを示します。次の AWS Command Line Interface (AWS CLI)コマンドの出力で示されているように、パッチレベルの詳細は含まれません。コマンドはコンプライアンスタイプとして Association でフィルタリングされます。

```
aws ssm list-compliance-items \
    --resource-ids "i-02573cafcfEXAMPLE" \
    --resource-types "ManagedInstance" \
    --filters "Key=ComplianceType,Values=Association,Type=EQUAL" \
    --region us-east-2
```

システムが以下のような情報をレスポンスします。

```
{
    "ComplianceItems": [
        {
            "Status": "NON_COMPLIANT",
            "Severity": "UNSPECIFIED",
            "Title": "MyPatchAssociation",
            "ResourceType": "ManagedInstance",
            "ResourceId": "i-02573cafcfEXAMPLE",
            "ComplianceType": "Association",
            "Details": {
                "DocumentName": "AWS-RunPatchBaselineAssociation",
                "PatchBaselineId": "pb-0c10e65780EXAMPLE",
                "DocumentVersion": "1"
            },
            "ExecutionSummary": {
                "ExecutionTime": 1590698771.0
            },
            "Id": "3e5d5694-cd07-40f0-bbea-040e6EXAMPLE"
        }
    ]
}
```

AWS-RunPatchBaselineAssociation ドキュメントのパラメータとしてタグのキーペア値が指定されている場合、Patch Manager は、オペレーティングシステムのタイプと一致し、同じタグのキーペアでタグ付けされているカスタムパッチベースラインを検索します。この検索は、現在指定されているデフォルトのパッチベースライン、またはパッチグループに割り当てられたベースラインに制限されません。指定されたタグを持つベースラインが見つからない場合は、Patch Managerはパッチグループを検索します (AWS-RunPatchBaselineAssociation を実行するコマンドで指定されている場合)。一致するパッチグループがない場合、Patch Managerはオペレーティングシステムのアカウントにデフォルトに設定されているパッチベースラインを使用します。

AWS-RunPatchBaselineAssociation ドキュメントで指定されているタグを持つパッチベースラインが複数見つかった場合、Patch Managerは、オペレーションを続行するために、そのキーと値のペアでタグ付けできるパッチベースラインは 1 つだけであることを示すエラーメッセージを返します。

> **Note**
>
> Linux インスタンスでは、各インスタンスタイプに適切なパッケージマネージャーを使用してパッケージをインストールします。
>
> - Amazon Linux 1、Amazon Linux 2、CentOS、Oracle Linux、および RHEL インスタンスでは、YUM が使用されています。YUM のオペレーションでは、Patch Manager には、Python 2.6 またはそれ以降のサポートされているバージョン (2.6 ~ 3.10) が必要です。
> - Debian Server、Raspberry Pi OS、および Ubuntu Server インスタンスでは、APT が使用されています。APT のオペレーションでは、Patch Manager には、サポートされているバージョン (3.0 ~ 3.10) の Python 3 が必要です。
> - SUSE Linux Enterprise Server インスタンスでは Zypper が使用されています。Zypper のオペレーションでは、Patch Manager には、Python 2.6 またはそれ以降のサポートされているバージョン (2.6 ~ 3.10) が必要です。

スキャンが完了した後、またはすべての承認済み更新と該当する更新がインストールされた後、必要に応じて再起動されると、パッチコンプライアンス情報がインスタンスで生成されてパッチコンプライアンスサービスにレポートされます。

> **Note**
>
> AWS-RunPatchBaselineAssociation ドキュメントで RebootOption パラメータが NoReboot に設定されている場合、Patch Managerの実行後、インスタンスは再起動されません。詳細については、「パラメータ名: RebootOption」を参照してください。

パッチコンプライアンスデータの表示方法については、「パッチコンプライアンスについて」を参照してください。

AWS-RunPatchBaselineAssociation 個のパラメータ

AWS-RunPatchBaselineAssociation は 5 つのパラメータをサポートしています。Operation および AssociationId パラメータが必要です。InstallOverrideList、RebootOption および BaselineTags パラメータはオプションです。

パラメータ

- パラメータ名: Operation
- パラメータ名: BaselineTags
- パラメータ名: AssociationId
- パラメータ名: InstallOverrideList
- パラメータ名: RebootOption

パラメータ名: **`Operation`**

使用: 必須。

オプション: `Scan` | `Install`。

Scan

`Scan` オプションを選択すると、`AWS-RunPatchBaselineAssociation` はインスタンスのパッチコンプライアンス状態を確認し、この情報を Patch Manager に返します。`Scan` では、更新のインストールや、インスタンスの再起動を求めません。代わりに、承認済み更新でインスタンスに適用可能なものが見つからない個所を示します。

インストール

`Install` オプションを選択すると、`AWS-RunPatchBaselineAssociation` はインスタンスに見つからない承認済み更新と適用可能な更新のインストールを試行します。`Install` オペレーションの一部として生成されるパッチコンプライアンス情報には、見つからない更新は示されませんが、更新のインストールが何らかの原因で失敗した場合は「失敗」状態になっている更新がレポートされることがあります。更新がインスタンスにインストールされるたびに、インスタンスが再起動され、更新がインストール済みで有効になっていることが確認されます。（例外: `RebootOption` パラメータが `AWS-RunPatchBaselineAssociation` ドキュメントの `NoReboot` で設定されている場合、Patch Manager の実行後にインスタンスは再起動されません。詳細については、「パラメータ名: `RebootOption`」を参照してください。）

> **Note**
>
> Patch Managerがインスタンスを更新する前に、ベースラインルールで指定されているパッチがインストールされている場合、システムが予期したとおりに再起動しないことがあります。この可能性があるのは、パッチがユーザーによって手動でインストールされたか、Ubuntu Server の `unattended-upgrades` パッケージなどの別のプログラムによって自動的にインストールされた場合です。

パラメータ名: **BaselineTags**

使用: オプション。

BaselineTags は、一意のタグのキーと値のペアで、選択して個々のカスタムパッチベースラインに割り当てます。このパラメータには、1 つ以上の値を指定できます。次の形式はどちらも有効です。

Key=*tag-key*,Values=*tag-value*

Key=*tag-key*,Values=*tag-value1*,*tag-value2*,*tag-value3*

> **Important**
>
> タグキーと値には、バックティック (`)、一重引用符 (')、二重引用符 (")、およびドル記号 ($) を含めることはできません。

Patch Manager は、BaselineTags の値を使用して、1 回のオペレーションでパッチを適用するインスタンスのすべてに同じ承認済みパッチのセットが適用されるようにします。 パッチ適用オペレーションが実行すると、Patch Manager は、オペレーティングシステムのタイプのパッチベースラインが BaselineTags で指定したものと同じキーと値のペアでタグ付けされているか確認します。一致するものがある場合は、このカスタムパッチベースラインが使用されます。一致するものがない場合、パッチ適用オペレーションに指定されたパッチグループに従って、パッチベースラインが識別されます。存在しない場合は、そのオペレーティングシステムの AWS マネージド定義済みパッチベースラインが使用されます。

追加のアクセス許可要件

Quick Setup を使用してセットアップした以外のパッチオペレーションで AWS-RunPatchBaselineAssociation を使用し、オプションの BaselineTags パラメータを使用する場合は、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのインスタンスプロファイルに対する以下のアクセス許可を追加する必要があります。

> **Note**
>
> Quick Setup と AWS-RunPatchBaselineAssociation は、オンプレミスのサーバーと仮想マシン (VM) をサポートしていません。

```
{
    "Effect": "Allow",
    "Action": [
        "ssm:DescribePatchBaselines",
        "tag:GetResources"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "ssm:GetPatchBaseline",
        "ssm:DescribeEffectivePatchesForPatchBaseline"
    ],
    "Resource": "patch-baseline-arn"
}
```

patch-baseline-arn を、アクセス許可を付与するパッチベースラインの Amazon リソースネーム (ARN) に、arn:aws:ssm:us-east-2:123456789012:patchbaseline/pb-0c10e65780EXAMPLE 形式で置き換えます。

パラメータ名: **AssociationId**

使用: 必須。

AssociationId は、AWS Systems Manager のツールである State Manager の、既存の関連付けの ID です。これは、指定した関連付けにコンプライアンスデータを追加するために Patch Manager で使用します。この関連付けは、Quick Setup で作成されたホスト管理設定で有効になっているパッチ Scan オペレーションに関連しています。パッチ適用の結果をインベントリコンプライアンスデータではなく関連付けコンプライアンスデータとして送信することで、インスタンスの既存のインベントリコンプライアンス情報は、パッチ適用オペレーションの後やその他の関連付け ID に対して上書きされません。使用する関連付けがまだない場合は、create-association コマンドを実行して関連付けを作成できます。例:

Linux & macOS

```
aws ssm create-association \
    --name "AWS-RunPatchBaselineAssociation" \
    --association-name "MyPatchHostConfigAssociation" \
```

```
    --targets
 "Key=instanceids,Values=[i-02573cafcfEXAMPLE,i-07782c72faEXAMPLE,i-07782c72faEXAMPLE]"
 \
    --parameters "Operation=Scan" \
    --schedule-expression "cron(0 */30 * * * ? *)" \
    --sync-compliance "MANUAL" \
    --region us-east-2
```

Windows Server

```
aws ssm create-association ^
    --name "AWS-RunPatchBaselineAssociation" ^
    --association-name "MyPatchHostConfigAssociation" ^
    --targets
 "Key=instanceids,Values=[i-02573cafcfEXAMPLE,i-07782c72faEXAMPLE,i-07782c72faEXAMPLE]"
 ^
    --parameters "Operation=Scan" ^
    --schedule-expression "cron(0 */30 * * * ? *)" ^
    --sync-compliance "MANUAL" ^
    --region us-east-2
```

パラメータ名: **`InstallOverrideList`**

使用: オプション。

`InstallOverrideList` を使用して、インストールするパッチのリストに対する https URL または Amazon Simple Storage Service (Amazon S3) パス形式の URL を指定します。このパッチインストールリストは、YAML 形式で管理され、デフォルトのパッチベースラインで指定されたパッチを上書きします。これにより、どのインスタンスにどのパッチがインストールされているかを、より詳細にコントロールできます。

> **Important**
>
> `InstallOverrideList` ファイル名には、バックティック (`)、一重引用符 (')、二重引用符 (")、およびドル記号 ($) を含めることはできません。

`InstallOverrideList` パラメータを使用する場合のパッチ適用オペレーションの動作は、Linux および macOS マネージドノードと、Windows Server マネージドノードで異なります。Linux および macOS では、パッチがパッチベースラインルールと一致するかどうかにかかわらず、Patch

Manager は、ノードで有効になっているリポジトリに存在する InstallOverrideList パッチリストに含まれるパッチを適用しようとします。一方、Windows Server ノードでは、InstallOverrideList パッチリスト内のパッチは、パッチベースラインルールとも一致する場合にのみ適用されます。

コンプライアンスレポートは、パッチの InstallOverrideList リストで指定するものではなく、パッチのベースラインで指定されているものに従ってパッチの状態が反映されることに注意してください。つまり、スキャンオペレーションは InstallOverrideList パラメータを無視します。これは、コンプライアンスレポートが、特定のパッチ適用オペレーションで承認されたものではなく、ポリシーに従ってパッチ状態を一貫して反映することを保証するためです。

有効な URL 形式

> **Note**
>
> ファイルが公開されているバケットに格納されている場合は、「https」URL 形式または Amazon S3 パススタイルの URL を指定できます。ファイルがプライベートバケットに格納されている場合は、Amazon S3 パススタイルの URL を指定する必要があります。

- https URL 形式の例:

```
https://s3.amazonaws.com/amzn-s3-demo-bucket/my-windows-override-list.yaml
```

- Amazon S3 パス形式 URL の例:

```
s3://amzn-s3-demo-bucket/my-windows-override-list.yaml
```

有効な YAML コンテンツ形式

リストにパッチを指定するために使用する書式は、インスタンスのオペレーティングシステムによって異なります。ただし、一般的な形式は次のとおりです。

```
patches:
    -
        id: '{patch-d}'
        title: '{patch-title}'
        {additional-fields}:{values}
```

YAML ファイルにフィールドを追加することはできますが、パッチオペレーション中は無視されます。

さらに、S3 バケットのリストを追加または更新する前に、YAML ファイルのフォーマットが有効であることを確認することをお勧めします。YAML 形式の詳細については、yaml.org を参照してください。検証ツールのオプションについては、ウェブで「yaml 形式の検証」を検索します。

- Microsoft Windows

  id

  id フィールドは必須です。Microsoft Knowledge Base ID (KB2736693 など) および Microsoft Security Bulletin ID (MS17-023 など) を使用してパッチを指定する場合に使用します。

  Windows 用のパッチリストで提供する他のフィールドはオプションであり、情報提供のみを目的としています。特定のパッチに関する詳細情報を提供するために、title、classification、severity などの追加フィールドを使用することができます。

- リナックス

  id

  id フィールドは必須です。これにより、パッケージ名とアーキテクチャを使用してパッチを指定します。例: `'dhclient.x86_64'`。ID にワイルドカードを使用すると、複数のパッケージを指定できます。例: `'dhcp*'` および `'dhcp*1.*'`。

  title

  title フィールドはオプションですが、Linux システムでは追加のフィルタリング機能を提供します。title を使用する場合は、次のいずれかの形式でパッケージのバージョン情報を含める必要があります。

  YUM/SUSE Linux Enterprise Server (SLES):

  ```
  {name}.{architecture}:{epoch}:{version}-{release}
  ```

  APT

  ```
  {name}.{architecture}:{version}
  ```

Linux のパッチタイトルでは、任意の位置に 1 つ以上のワイルドカードを使用して一致するパッケージの数を拡張することができます。例: `'*32:9.8.2-0.*.rc1.57.amzn1'`。

以下に例を示します。

- apt パッケージのバージョン 1.2.25 が現在インスタンスにインストールされていますが、バージョン 1.2.27 が利用できるようになりました。
- apt.amd64 バージョン 1.2.27 をパッチリストに追加します。これは apt utils.amd64 バージョン 1.2.27 に依存しますが、apt-utils.amd64 バージョン 1.2.25 がリストで指定されています。

この場合、apt バージョン 1.2.27 のインストールはブロックされ、「Failed-NonCompliant」として報告されます。

その他のフィールド

Linux 用のパッチリストで提供する他のフィールドはオプションであり、情報提供のみを目的としています。特定のパッチに関する詳細情報を提供するために、classification、severity などの追加フィールドを使用することができます。

サンプルパッチリスト

- Windows

```
patches:
    -
        id: 'KB4284819'
        title: '2018-06 Cumulative Update for Windows Server 2016 (1709) for x64-
based Systems (KB4284819)'
    -
        id: 'KB4284833'
    -
        id: 'KB4284835'
        title: '2018-06 Cumulative Update for Windows Server 2016 (1803) for x64-
based Systems (KB4284835)'
    -
        id: 'KB4284880'
    -
        id: 'KB4338814'
```

- APT

```
patches:
    -
        id: 'apparmor.amd64'
        title: '2.10.95-0ubuntu2.9'
    -
        id: 'cryptsetup.amd64'
        title: '*2:1.6.6-5ubuntu2.1'
    -
        id: 'cryptsetup-bin.*'
        title: '*2:1.6.6-5ubuntu2.1'
    -
        id: 'apt.amd64'
        title: '*1.2.27'
    -
        id: 'apt-utils.amd64'
        title: '*1.2.25'
```

- Amazon Linux

```
patches:
    -
        id: 'kernel.x86_64'
    -
        id: 'bind*.x86_64'
        title: '32:9.8.2-0.62.rc1.57.amzn1'
    -
        id: 'glibc*'
    -
        id: 'dhclient*'
        title: '*12:4.1.1-53.P1.28.amzn1'
    -
        id: 'dhcp*'
        title: '*10:3.1.1-50.P1.26.amzn1'
```

- Red Hat Enterprise Linux (RHEL)

```
patches:
    -
        id: 'NetworkManager.x86_64'
        title: '*1:1.10.2-14.el7_5'
    -
        id: 'NetworkManager-*.x86_64'
```

```
        title: '*1:1.10.2-14.el7_5'
    -
        id: 'audit.x86_64'
        title: '*0:2.8.1-3.el7'
    -
        id: 'dhclient.x86_64'
        title: '*.el7_5.1'
    -
        id: 'dhcp*.x86_64'
        title: '*12:5.2.5-68.el7'
```

- SUSE Linux Enterprise Server (SLES)

```
patches:
    -
        id: 'amazon-ssm-agent.x86_64'
    -
        id: 'binutils'
        title: '*0:2.26.1-9.12.1'
    -
        id: 'glibc*.x86_64'
        title: '*2.19*'
    -
        id: 'dhcp*'
        title: '0:4.3.3-9.1'
    -
        id: 'lib*'
```

- Ubuntu Server

```
patches:
    -
        id: 'apparmor.amd64'
        title: '2.10.95-0ubuntu2.9'
    -
        id: 'cryptsetup.amd64'
        title: '*2:1.6.6-5ubuntu2.1'
    -
        id: 'cryptsetup-bin.*'
        title: '*2:1.6.6-5ubuntu2.1'
    -
```

```
        id: 'apt.amd64'
        title: '*1.2.27'
    -
        id: 'apt-utils.amd64'
        title: '*1.2.25'
```

- Windows

```
patches:
    -
        id: 'KB4284819'
        title: '2018-06 Cumulative Update for Windows Server 2016 (1709) for x64-
based Systems (KB4284819)'
    -
        id: 'KB4284833'
    -
        id: 'KB4284835'
        title: '2018-06 Cumulative Update for Windows Server 2016 (1803) for x64-
based Systems (KB4284835)'
    -
        id: 'KB4284880'
    -
        id: 'KB4338814'
```

パラメータ名: **RebootOption**

使用: オプション。

オプション: RebootIfNeeded | NoReboot

デフォルト: RebootIfNeeded

> **Warning**
>
> デフォルトのオプションは RebootIfNeeded です。ユースケースに適したオプションを必ず選択してください。例えば、設定プロセスを完了するためにインスタンスをすぐに再起動する必要がある場合は、RebootIfNeeded を選択します。または、スケジュールされた再起動時間までインスタンスの可用性を維持する必要がある場合は、NoReboot を選択します。

> **Important**
>
> NoReboot オプションは、オペレーティングシステムレベルの再起動のみを防ぎます。サービスレベルの再起動は、パッチ適用プロセスの一環として引き続き発生する可能性があります。例えば、Docker が更新されると、NoReboot が有効にされていても Amazon Elastic Container Service などの依存サービスが自動的に再起動される場合があります。中断してはならない重要なサービスがある場合は、一時的にインスタンスをサービスから削除したり、メンテナンス期間中にパッチ適用をスケジュールしたりするなどの追加の対策を検討してください。

> **Important**
>
> Amazon EMR (以前は Amazon Elastic MapReduce と呼ばれていました) のクラスターインスタンスへのパッチ適用には、Patch Manager を使用しないことをお勧めします。特に、RebootOption パラメータの RebootIfNeeded オプションは選択しないでください。(このオプションは、AWS-RunPatchBaseline、AWS-RunPatchBaselineAssociation、および AWS-RunPatchBaselineWithHooks のパッチ適用用の SSM コマンドドキュメントに記載されています。)
> Patch Manager を使用してパッチを適用する基本コマンドは、yum と dnf コマンドを使用します。そのため、パッケージのインストール方法が原因となり、オペレーションの互換性が失われます。Amazon EMR クラスターのソフトウェアを更新するための推奨方法については、「Amazon EMR 管理ガイド」の「Amazon EMR のデフォルト AMI の使用」を参照してください。

RebootIfNeeded

RebootIfNeededオプションを選択すると、次のいずれかの場合にインスタンスが再起動されます。

- Patch Manager が 1 つ以上のパッチをインストールしている場合。

  Patch Manager は、パッチによる再起動が必要かどうか評価しない場合。パッチで再起動が必要ない場合でも、システムは再起動されます。

- Patch Manager は、Install オペレーションの実行中、ステータスが INSTALLED_PENDING_REBOOT のパッチをひとつ以上検出します。

`INSTALLED_PENDING_REBOOT` ステータスは、前回 `Install` オペレーションを実行したときにオプション `NoReboot` が選択されたことを意味する場合や、マネージドノードが最後に再起動されたとき以降にパッチが Patch Manager 以外でインストールされたことを意味する場合があります。

上記 2 つの場合にインスタンスを再起動すると、更新されたパッケージがメモリからフラッシュされ、パッチ適用と再起動の動作があらゆるオペレーティングシステムで一貫して維持されます。

NoReboot

`NoReboot` オプションを選択すると、Patch Manager が `Install` オペレーション中にパッチをインストールした場合でも、インスタンスは再起動されません。このオプションは、パッチ適用後にインスタンスを再起動する必要がないことがわかっている場合や、パッチ適用操作の再起動によって中断されないアプリケーションまたはプロセスがインスタンスで実行されている場合に便利です。また、メンテナンスウィンドウを使用するなど、インスタンスの再起動のタイミングをより詳細に制御する場合にも役立ちます。

パッチのインストール追跡ファイル: パッチ (特にシステムの最後の再起動以降にインストールされたパッチ) のインストールを追跡するために、Systems Manager は、マネージドインスタンスのファイルを管理します。

> **Important**
>
> 追跡ファイルを削除または変更しないでください。このファイルを削除または破損すると、インスタンスのパッチコンプライアンスレポートが不正確になります。ファイルを削除または破損した場合は、インスタンスを再起動し、パッチのスキャンオペレーションを実行してファイルを復元します。

この追跡ファイルは、マネージドインスタンスの以下の場所に保存されます。

- Linux オペレーティングシステム:
  - `/var/log/amazon/ssm/patch-configuration/patch-states-configuration.json`
  - `/var/log/amazon/ssm/patch-configuration/patch-inventory-from-last-operation.json`
- Windows Server オペレーティングシステム:

- C:\ProgramData\Amazon\PatchBaselineOperations\State\PatchStatesConfiguration.json
- C:\ProgramData\Amazon\PatchBaselineOperations\State\PatchInventoryFromLastOperation.json

パッチ適用のための SSM コマンドドキュメント: **AWS-RunPatchBaselineWithHooks**

AWS Systems Manager は、AWS Systems Manager のツールである Patch Manager 用の Systems Manager ドキュメント (SSM ドキュメント) である AWS-RunPatchBaselineWithHooks をサポートしています。この SSM ドキュメントでは、セキュリティ関連および他のタイプの更新の両方について、マネージドノードにパッチ適用オペレーションを実行します。

AWS-RunPatchBaselineWithHooks は、次の点で AWS-RunPatchBaseline とは異なります。

- ラッパードキュメント – AWS-RunPatchBaselineWithHooks は、AWS-RunPatchBaseline のラッパーであり、そのオペレーションの一部で AWS-RunPatchBaseline に依存しています。
- **Install** オペレーション – AWS-RunPatchBaselineWithHooks では、マネージドノードのパッチ適用中に指定されたポイントで実行されるライフサイクルフックがサポートされます。パッチのインストールにはマネージドノードの再起動が必要になる場合があるため、パッチ適用オペレーションは 2 つのイベントに分割され、合計 3 つのフックでカスタム機能をサポートします。最初のフックは Install with NoReboot オペレーションの前です。2 番目のフックは Install with NoReboot オペレーションの後です。3 番目のフックは、マネージドノードの再起動後に使用できます。
- カスタムパッチリストはサポートしません – AWS-RunPatchBaselineWithHooks では、InstallOverrideList パラメータはサポートされません。
- SSM Agent サポート – AWS-RunPatchBaselineWithHooks では、パッチを適用するために SSM Agent 3.0.502 以降をマネージドノードにインストールする必要があります。

パッチグループが指定されていない場合、ドキュメントを実行すると、オペレーティングシステムタイプの「デフォルト」として現在指定されているパッチベースラインが使用されます。それ以外の場合は、パッチグループに関連付けられているパッチベースラインが使用されます。パッチグループの詳細については、「パッチグループ」を参照してください。

ドキュメント AWS-RunPatchBaselineWithHooks を使用して、オペレーティングシステムとアプリケーションの両方にパッチを適用することができます。(Windows Server では、アプリケーションのサポートは、Microsoft がリリースしたアプリケーションの更新に制限されています)。

このドキュメントでは、Linux および Windows Server マネージドノードをサポートしています。ドキュメントは、プラットフォーム別に適切なアクションを実行します。

> **Note**
>
> `AWS-RunPatchBaselineWithHooks` は macOS ではサポートされていません。

Linux

Linux マネージドノードの場合、`AWS-RunPatchBaselineWithHooks` ドキュメントは、Python モジュールを呼び出します。これに伴って、マネージドノードに適用するパッチベースラインのスナップショットがダウンロードされます。このパッチベースラインのスナップショットは、定義済みルールと、承認済みパッチおよび拒否済みパッチのリストを使用し、ノードタイプ別に適切なパッケージマネージャーを設定します。

- Amazon Linux 1、Amazon Linux 2、CentOS、Oracle Linux、および RHEL 7 マネージドノードでは、YUM が使用されています。YUM のオペレーションでは、Patch Manager には、`Python 2.6` またはそれ以降のサポートされているバージョン (2.6 ~ 3.10) が必要です。
- RHEL 8 マネージドノードでは DNF が使用されます。DNF のオペレーションでは、Patch Manager には、サポートされているバージョン (2.6 ~ 3.10) の `Python 2` または `Python 3` が必要です。(どちらのバージョンも RHEL 8 にはデフォルトでインストールされていません。どちらか一方を手動でインストールする必要があります。)
- Debian Server、Raspberry Pi OS、および Ubuntu Server インスタンスでは、APT が使用されています。APT のオペレーションでは、Patch Manager には、サポートされているバージョン (3.0 ~ 3.10) の `Python 3` が必要です。
- SUSE Linux Enterprise Server マネージドノードは Zypper を使用します。Zypper のオペレーションでは、Patch Manager には、`Python 2.6` またはそれ以降のサポートされているバージョン (2.6 ~ 3.10) が必要です。

Windows Server

Windows Server マネージドノードの場合、`AWS-RunPatchBaselineWithHooks` ドキュメントは、PowerShell モジュールをダウンロードして呼び出します。これに伴って、マネージドノードに適用するパッチベースラインのスナップショットがダウンロードされます。このパッチベースラインスナップショットには、Windows Server Update Services (WSUS) サーバーに対してパッチベースラインを照会することによってコンパイルされる承認済みパッチのリストが含まれてい

ます。このリストは、Windows Update API に渡され、ここで承認済みパッチのダウンロードとインストールが適切に制御されます。

各スナップショットは、AWS アカウント 、パッチグループ、オペレーティングシステム、スナップショット ID に固有のものです。スナップショットは、署名付きの Amazon Simple Storage Service (Amazon S3) URL を介して配信されます。この URL は、スナップショットが作成されてから 24 時間後に期限切れになります。ただし、URL の有効期限が切れた後に、同じスナップショットコンテンツを他のマネージドノードに適用する場合は、スナップショットを作成してから 3 日以内であれば新しい署名付き Amazon S3 URL を生成できます。これを行うには、get-deployable-patch-snapshot-for-instance コマンドを使用します。

すべての承認済みで適用可能な更新プログラムがインストールされ、必要に応じて再起動されると、パッチのコンプライアンス情報がマネージドノードで生成されて Patch Manager にレポートされます。

AWS-RunPatchBaselineWithHooks ドキュメントで RebootOption パラメータが NoReboot に設定されている場合、Patch Manager の実行後、マネージドノードは再起動されません。詳細については、「パラメータ名: RebootOption」を参照してください。

> **Important**
>
> NoReboot オプションはオペレーティングシステムの再起動を防止しますが、特定のパッケージの更新時に発生する可能性のあるサービスレベルの再起動は防止しません。例えば、Docker などのパッケージを更新すると、NoReboot が指定されていても依存サービス (コンテナオーケストレーションサービスなど) の自動再起動がトリガーされる場合があります。

パッチコンプライアンスデータの表示方法については、「パッチコンプライアンスについて」を参照してください。

AWS-RunPatchBaselineWithHooks オペレーションステップ

AWS-RunPatchBaselineWithHooks が実行されると、次の手順が実行されます。

1. スキャン - Scan を使用した AWS-RunPatchBaseline オペレーションがマネージドノードで実行され、コンプライアンスレポートが生成され、アップロードされます。
2. ローカルパッチ状態の確認 - スクリプトを実行して、選択したオペレーションとステップ 1 の Scan 結果に基づいて実行されるステップを決定します。

a. 選択したオペレーションが Scan の場合、そのオペレーションは完了としてマークされます。オペレーションは終了します。

b. 選択したオペレーションが Install の場合、Patch Manager はステップ 1 の Scan 結果を評価し、次に実行するオペレーションを決定します。

i. パッチの欠落が検出されず、保留中の再起動が必要ない場合は、オペレーションは最後のステップ (ステップ 8) に直接進みます。これには、指定したフックが含まれます。その間のステップはすべてスキップされます。

ii. パッチの欠落が検出されないが、保留中の再起動が必要で、選択した再起動オプションが NoReboot である場合、オペレーションは最後のステップ (ステップ 8) に直接進みます。これには、指定したフックが含まれます。その間のステップはすべてスキップされます。

iii. それ以外の場合、オペレーションは次のステップに進みます。

3. パッチ適用前のフックオペレーション - 最初のライフサイクルフック用に指定した SSM ドキュメント (PreInstallHookDocName) は、マネージドノードで実行されます。

4. 再起動せずにインストール - Install を使用して NoReboot の再起動オプションを含む AWS-RunPatchBaseline オペレーションがマネージドノードで実行され、コンプライアンスレポートが生成され、アップロードされます。

5. インストール後のフックオペレーション - 2 番目のライフサイクルフック用に指定した SSM ドキュメント (PostInstallHookDocName) は、マネージドノードで実行されます。

6. パッチ適用前のフックオペレーション - 最初のライフサイクルフック用に指定した SSM ドキュメントは、インスタンスで実行されます。

a. 選択した再起動オプションが NoReboot の場合、オペレーションは最後のステップ (ステップ 8) に直接進みます。これには、指定したフックが含まれます。その間のステップはすべてスキップされます。

b. 選択した再起動オプションが RebootIfNeeded の場合、Patch Manager はステップ4で収集されたインベントリから保留中の再起動が必要かどうかをチェックします。つまり、次のいずれかの場合に操作をステップ 7 に進み、マネージド ノードが再起動されます。

i. Patch Manager は、1 つ以上のパッチをインストールしました。(Patch Manager は、パッチに再起動が必要かどうかを評価しません。パッチに再起動が必要ない場合でも、システムは再起動されます。)

ii. Patch Manager は、インストールの実行中、INSTALLED_PENDING_REBOOT の状態によってパッチをひとつ以上検出します。INSTALLED_PENDING_REBOOT ステータスは、前回インストールオペレーションを実行したときにオプション NoReboot が選択されたことを意味する場合や、マネージドノードが最後に再起動されたとき以降にパッチが Patch Manager 以外でインストールされたことを意味する場合があります。

これらの条件を満たすパッチが見つからない場合は、マネージド ノードのパッチ適用操作が完了し、操作は最終ステップ (ステップ 8) に直接進みます。これには、提供されたフックが含まれます。その間のステップはすべてスキップされます。

7. 再起動とレポート - 再起動オプションが RebootIfNeeded であるインストールオペレーションは、AWS-RunPatchBaseline を使用してマネージドノードで実行され、コンプライアンスレポートが生成され、アップロードされます。
8. 再起動後のフックオペレーション - 3 番目のライフサイクルフック用に指定した SSM ドキュメント (OnExitHookDocName) は、マネージドノードで実行されます。

Scan オペレーションの場合、ステップ 1 が失敗すると、ドキュメントの実行プロセスは停止し、ステップは失敗として報告されますが、後続のステップは成功として報告されます。

Install オペレーションの場合、オペレーション中にいずれかの aws:runDocument ステップが失敗すると、そのようなステップは失敗として報告され、オペレーションは直接最終ステップ (ステップ 8) に進みます。これには、指定したフックが含まれます。その間のステップはすべてスキップされます。このステップは失敗として報告され、最後のステップはそのオペレーション結果のステータスを報告し、その間にあるすべてのステップは成功として報告されます。

AWS-RunPatchBaselineWithHooks 個のパラメータ

AWS-RunPatchBaselineWithHooks では 6 つのパラメータがサポートされています。

Operation パラメータは必須です。

RebootOption、PreInstallHookDocName、PostInstallHookDocName および OnExitHookDocName パラメータはオプションです。

Snapshot-ID は技術的にはオプションですが、AWS-RunPatchBaselineWithHooks をメンテナンスウィンドウ以外で実行する場合は、カスタム値を指定することをお勧めします。ドキュメントがメンテナンスウィンドウオペレーションの一部として実行されるときに、Patch Manager に値を自動的に指定させましょう。

パラメータ

- パラメータ名: Operation
- パラメータ名: Snapshot ID
- パラメータ名: RebootOption

- パラメータ名: PreInstallHookDocName
- パラメータ名: PostInstallHookDocName
- パラメータ名: OnExitHookDocName

パラメータ名: **Operation**

使用: 必須。

オプション: Scan | Install。

Scan

Scan オプションを選択すると、システムは AWS-RunPatchBaseline ドキュメントを使用してマネージドノードのパッチコンプライアンスの状態を判断し、その情報を Patch Manager にレポートします。Scan では、更新のインストールやマネージドノードの再起動は行われません。その代わりに、このオペレーションでは、承認されたノードに適用可能なアップデートがどこに欠けているかを特定します。

インストール

Install オプションを選択すると、AWS-RunPatchBaselineWithHooks はマネージドノードに見つからない承認済み更新と適用可能な更新のインストールを試行します。Install オペレーションの一部として生成されるパッチコンプライアンス情報には、見つからない更新は示されませんが、更新のインストールが何らかの原因で失敗した場合は「失敗」状態になっている更新がレポートされることがあります。更新がマネージドノードにインストールされるたびに、ノードが再起動され、更新がインストール済みで有効になっていることが確認されます。(例外: RebootOption パラメータが AWS-RunPatchBaselineWithHooks ドキュメントの NoReboot で設定されている場合、パッチマネージャーの Patch Manager 実行後にマネージドノードは再起動されません。詳細については、「パラメータ名: RebootOption」を参照してください。)

> **Note**
>
> Patch Manager がマネージドノードを更新する前に、ベースラインルールで指定されているパッチがインストールされている場合、システムが予期したとおりに再起動しないことがあります。この可能性があるのは、パッチがユーザーによって手動でインストールされたか、Ubuntu Server の unattended-upgrades パッケージなどの別のプログラムによって自動的にインストールされた場合です。

パラメータ名: **Snapshot ID**

使用: オプション。

Snapshot ID は、Patch Manager が使用する一意の ID (GUID) です。この ID により、1 回のオペレーションでパッチを適用するマネージドノードのすべてに同じ承認済みパッチのセットが適用されます。このパラメータは省略可能ですが、次の表に示すようにメンテナンスウィンドウで AWS-RunPatchBaselineWithHooks を実行しているかどうかに応じて、推奨されるベストプラクティスが異なります。

AWS-RunPatchBaselineWithHooks のベストプラクティス

モード	ベストプラクティス	詳細
メンテナンスウィンドウ内で AWS-RunPatchBaselineWithHooks を実行する	スナップショット ID は指定しないでください。Patch Manager によって指定されます。	メンテナンスウィンドウを使用して AWS-RunPatchBaselineWithHooks を実行する場合は、独自に生成したスナップショット ID を提供すべきではありません。このシナリオでは、メンテナンスウィンドウの実行 ID に基づく GUID 値が Systems Manager から提供されます。これにより、そのメンテナンスウィンドウでは、AWS-RunPatchBaselineWithHooks のすべての呼び出しで正しい ID が使用されます。 このシナリオで値を指定しないと、パッチベースラインのスナップショットは 3 日以内に有効期限が切れる場合があります。スナップショットの有効期限が切れると、同じ ID

モード	ベストプラクティス	詳細
		を指定しても、別のスナップショットが生成されます。

モード	ベストプラクティス	詳細
メンテナンスウィンドウ外で AWS-RunPatchBaselineWithHooks を実行する	スナップショット ID のカスタム GUID 値を生成および指定します。[1]	メンテナンスウィンドウを使用しないで AWS-RunPatchBaselineWithHooks を実行する場合は、パッチベースラインごとに一意のスナップショット ID を生成し指定することをお勧めします (特に、同一のオペレーションで AWS-RunPatchBaselineWithHooks ドキュメントを複数のマネージドノードで実行する場合)。このシナリオで ID を指定しないと、コマンドの送信先のマネージドノードごとに異なるスナップショット ID が Systems Manager で生成されます。これにより、ノード間で異なるパッチセットが指定される場合があります。 例えば、AWS Systems Manager のツールである Run Command を使用して AWS-RunPatchBaselineWithHooks ドキュメントを直接実行し、50 個のマネージドノードのグループをターゲットにしているとします。カスタムスナップショット ID を指定すると、1 つのベースラインスナップショットが作成され、これがすべてのマネージドノードの評価とパッチ適用に使用されるため

モード	ベストプラクティス	詳細
		、すべてのノードの状態が一致します。

[1]Snapshot ID パラメータの値を生成するには、GUID を生成できる任意のツールを使用できます。たとえば、PowerShell では、New-Guid cmdlet を使用して 12345699-9405-4f69-bc5e-9315aEXAMPLE という形式の GUID を生成できます。

パラメータ名: **RebootOption**

使用: オプション。

オプション: RebootIfNeeded | NoReboot

デフォルト: RebootIfNeeded

> **Warning**
>
> デフォルトのオプションは RebootIfNeeded です。ユースケースに適したオプションを必ず選択してください。例えば、設定プロセスを完了するためにマネージドノードをすぐに再起動する必要がある場合は、RebootIfNeeded を選択します。または、スケジュールされた再起動時間までマネージドノードの可用性を維持する必要がある場合は、NoReboot を選択します。

> **Important**
>
> Amazon EMR (以前は Amazon Elastic MapReduce と呼ばれていました) のクラスターインスタンスへのパッチ適用には、Patch Manager を使用しないことをお勧めします。特に、RebootOption パラメータの RebootIfNeeded オプションは選択しないでください。(このオプションは、AWS-RunPatchBaseline、AWS-RunPatchBaselineAssociation、および AWS-RunPatchBaselineWithHooks のパッチ適用用の SSM コマンドドキュメントに記載されています。)
> Patch Manager を使用してパッチを適用する基本コマンドは、yum と dnf コマンドを使用します。そのため、パッケージのインストール方法が原因となり、オペレーションの互換性が失われます。Amazon EMR クラスターのソフトウェアを更新するための推奨方法について

は、「Amazon EMR 管理ガイド」の「Amazon EMR のデフォルト AMI の使用」を参照してください。

RebootIfNeeded

RebootIfNeeded オプションを選択すると、次のいずれかの場合にマネージドノードが再起動されます。

- Patch Manager が 1 つ以上のパッチをインストールしている場合。

  Patch Manager は、パッチによる再起動が必要かどうか評価しない場合。パッチで再起動が必要ない場合でも、システムは再起動されます。

- Patch Manager は、Install オペレーションの実行中、ステータスが INSTALLED_PENDING_REBOOT のパッチをひとつ以上検出します。

  INSTALLED_PENDING_REBOOT ステータスは、前回 Install オペレーションを実行したときにオプション NoReboot が選択されたことを意味する場合や、マネージドノードが最後に再起動されたとき以降にパッチが Patch Manager 以外でインストールされたことを意味する場合があります。

上記 2 つの場合にマネージドノードを再起動すると、更新されたパッケージがメモリからフラッシュされ、パッチ適用と再起動の動作があらゆるオペレーティングシステムで一貫して維持されます。

NoReboot

NoReboot オプションを選択すると、Patch Manager が Install オペレーション中にパッチをインストールした場合でも、マネージドノードは再起動されません。このオプションは、パッチ適用後にマネージドノードを再起動する必要がないことがわかっている場合や、パッチ適用操作の再起動によって中断されないアプリケーションまたはプロセスがノードで実行されている場合に便利です。また、メンテナンスウィンドウを使用するなど、マネージドノードの再起動のタイミングをより詳細に制御する場合にも役立ちます。

> **Note**
>
> パッチがインストールされている場合に　NoReboot オプションを選択すると、ステータス InstalledPendingReboot がパッチに割り当てられます。ただし、マネージドノード自体は、Non-Compliant と表示されています。再起動が発生し、Scan オペレーションが実行されると、ノードのステータスは Compliant に更新されます。

パッチのインストール追跡ファイル: パッチ (特にシステムの最後の再起動以降にインストールされたパッチ) のインストールを追跡するために、Systems Manager は、マネージドノードのファイルを管理します。

> **Important**
>
> 追跡ファイルを削除または変更しないでください。このファイルを削除または破損すると、マネージドノードのパッチコンプライアンスレポートが不正確になります。ファイルを削除または破損した場合は、ノードを再起動し、パッチのスキャンオペレーションを実行してファイルを復元します。

この追跡ファイルは、マネージドノードの以下の場所に保存されます。

- Linux オペレーティングシステム:
  - `/var/log/amazon/ssm/patch-configuration/patch-states-configuration.json`
  - `/var/log/amazon/ssm/patch-configuration/patch-inventory-from-last-operation.json`
- Windows Server オペレーティングシステム:
  - `C:\ProgramData\Amazon\PatchBaselineOperations\State\PatchStatesConfiguration.json`
  - `C:\ProgramData\Amazon\PatchBaselineOperations\State\PatchInventoryFromLastOperation.json`

パラメータ名: **`PreInstallHookDocName`**

使用: オプション。

デフォルト: `AWS-Noop`。

`PreInstallHookDocName` パラメータに指定する値は、選択した SSM ドキュメントの名前または Amazon リソースネーム (ARN) です。AWS マネージドドキュメントの名前や、作成したか共有されたカスタム SSM ドキュメントの名前または ARN を指定できます。(別の AWS アカウント から共有されている SSM ドキュメントの場合は、`arn:aws:ssm:us-east-2:123456789012:document/MySharedDocument` などの完全なリソース ARN を指定する必要があります)。

指定した SSM ドキュメントは、Install オペレーションの前に実行され、マネージドノードでパッチ適用が実行される前にアプリケーションのヘルスチェックを行うシェルスクリプトなど、SSM Agent がサポートするアクションを実行します。(アクションの一覧については、「コマンドドキュメントプラグインリファレンス」を参照してください)。デフォルトの SSM ドキュメント名は AWS-Noop で、マネージドノードに対するオペレーションは実行されません。

カスタム SSM ドキュメントの作成方法については、「SSM ドキュメントコンテンツを作成する」を参照してください。

パラメータ名: **PostInstallHookDocName**

使用: オプション。

デフォルト: AWS-Noop。

PostInstallHookDocName パラメータに指定する値は、選択した SSM ドキュメントの名前または Amazon リソースネーム (ARN) です。AWS マネージドドキュメントの名前や、作成したか共有されたカスタム SSM ドキュメントの名前または ARN を指定できます。(別の AWS アカウント から共有されている SSM ドキュメントの場合は、arn:aws:ssm:us-east-2:123456789012:document/MySharedDocument などの完全なリソース ARN を指定する必要があります)。

指定した SSM ドキュメントは、Install with NoReboot オペレーション後に実行され、再起動前にサードパーティ製の更新プログラムをインストールするためのシェルスクリプトなど、SSM Agent がサポートするアクションを実行します。(アクションの一覧については、「コマンドドキュメントプラグインリファレンス」を参照してください)。デフォルトの SSM ドキュメント名は AWS-Noop で、マネージドノードに対するオペレーションは実行されません。

カスタム SSM ドキュメントの作成方法については、「SSM ドキュメントコンテンツを作成する」を参照してください。

パラメータ名: **OnExitHookDocName**

使用: オプション。

デフォルト: AWS-Noop。

OnExitHookDocName パラメータに指定する値は、選択した SSM ドキュメントの名前または Amazon リソースネーム (ARN) です。AWS マネージドドキュメントの名前や、作成したか共有されたカスタム SSM ドキュメントの名前または ARN を指定できます。(別の

AWS アカウント から共有されている SSM ドキュメントの場合は、arn:aws:ssm:us-east-2:123456789012:document/MySharedDocument などの完全なリソース ARN を指定する必要があります)。

指定した SSM ドキュメントは、マネージドノードの再起動オペレーションの後に実行され、パッチ適用オペレーションの完了後にノードの状態を確認するシェルスクリプトなど、SSM Agent がサポートするアクションを実行します。(アクションの一覧については、「コマンドドキュメントプラグインリファレンス」を参照してください)。デフォルトの SSM ドキュメント名は AWS-Noop で、マネージドノードに対するオペレーションは実行されません。

カスタム SSM ドキュメントの作成方法については、「SSM ドキュメントコンテンツを作成する」を参照してください。

AWS-RunPatchBaseline または **AWS-RunPatchBaselineAssociation** で InstallOverrideList パラメータを使用するサンプルシナリオ

InstallOverrideList パラメータを使用すると、AWS Systems Manager のツールである Patch Manager の、現在のデフォルトのパッチベースラインで指定されたパッチを上書きできます。このトピックでは、このパラメータを使用して次のことを実現する方法の例を示します。

- マネージドノードのターゲットグループに異なるパッチセットを適用する。
- これらのパッチセットを異なる頻度で適用する。
- 両方の操作に同じパッチベースラインを使用する。

Amazon Linux 2 マネージドノードに 2 つの異なるカテゴリのパッチをインストールするとします。メンテナンスウィンドウを使用して、これらのパッチを異なるスケジュールでインストールします。毎週 1 つのメンテナンスウィンドウを実行し、すべての Security パッチをインストールする必要があります。月に 1 回は、別のメンテナンスウィンドウを実行し、使用可能なすべてのパッチ、または Security 以外のカテゴリのパッチをインストールする必要があります。

ところが、オペレーティングシステムのデフォルトとして定義できるパッチベースラインは、一度に 1 つだけです。この要件は、あるパッチベースラインでパッチが承認され、別のパッチベースラインでパッチがブロックされる (これによって競合するバージョン間で問題が発生する) 状況を回避するために役立ちます。

次の方法では、同じパッチベースラインを使用しながら、InstallOverrideList パラメータを使用して、異なるスケジュールで異なるタイプのパッチをターゲットグループに適用します。

1. デフォルトのパッチベースラインで、Security 更新のみが指定されていることを確認します。

2. AWS-RunPatchBaseline または AWS-RunPatchBaselineAssociation を毎週実行するメンテナンスウィンドウを作成します。上書きリストは指定しないでください。
3. 毎月適用するすべてのタイプのパッチの上書きリストを作成し、Amazon Simple Storage Service (Amazon S3) バケットに保存します。
4. 1 か月に 1 回実行する 2 番目のメンテナンスウィンドウを作成します。ただし、このメンテナンスウィンドウで登録する Run Command タスクについては、上書きリストの場所を指定します。

その結果、デフォルトのパッチベースラインで定義されている Security パッチのみが毎週インストールされます。利用可能なすべてのパッチや、定義したパッチのサブセットがすべて、毎月インストールされます。

詳細とサンプルの一覧については、「パラメータ名: InstallOverrideList」を参照してください。

BaselineOverride パラメータの使用

AWS Systems Manager のツールである Patch Manager のベースラインオーバーライド機能を使用して、実行時にパッチ適用設定を定義できます。これを行うには、パッチベースラインのリストを備えた JSON オブジェクトを含む Amazon Simple Storage Service (Amazon S3) バケットを指定します。パッチ適用操作では、デフォルトのパッチベースラインのルールを適用する代わりに、ホストオペレーティングシステムに一致する JSON オブジェクトで指定されるベースラインを使用します。

> **Important**
>
> BaselineOverride ファイル名には、バックティック (`)、一重引用符 (')、二重引用符 (")、およびドル記号 ($) を含めることはできません。

パッチ適用オペレーションでパッチポリシーが使用される場合を除き、BaselineOverride パラメータを使用しても、パラメータで指定されたベースラインのパッチコンプライアンスはオーバーライドされません。出力結果は、AWS Systems Manager のツールである Run Command から Stdout ログに記録されます 結果は、NON_COMPLIANT としてマークされているパッケージのみを出力します。つまり、パッケージは Missing、Failed、InstalledRejected、または InstalledPendingReboot としてマークされます。

ただし、パッチオペレーションでパッチポリシーが使用される場合、システムは関連付けられた S3 バケットからオーバーライドパラメータを渡し、マネージドノードのコンプライアンスの値は更新さ

れます。パッチポリシーの動作の詳細については、「Quick Setup でのパッチポリシー設定」を参照してください。

スナップショット ID またはインストールオーバーライドリストパラメータでパッチベースラインオーバーライドを使用する

パッチベースラインオーバーライドが注目に値する動作をするケースが 2 つあります。

ベースラインオーバーライドとスナップショット ID を同時に使用する

スナップショット ID により、特定のパッチ適用コマンドのすべてのマネージドノードがすべて同じことを適用するようにします。例えば、一度に 1,000 個のノードにパッチを適用すると、パッチは同じになります。

スナップショット ID とパッチベースラインオーバーライドの両方を使用する場合、スナップショット ID はパッチベースラインオーバーライドよりも優先されます。ベースラインオーバーライドルールは引き続き使用されますが、評価されるのは 1 回だけです。前の例では、1,000 マネージドノード間のパッチは常に同じになります。パッチ適用操作の途中で参照先の S3 バケット内の JSON ファイルを別のものに変更した場合、適用されたパッチは同じままになります。これは、スナップショット ID が指定されたためです。

ベースラインオーバーライドとインストールオーバーライドリストを同時に使用する

これら 2 つのパラメータを同時に使用することはできません。両方のパラメータが指定されると、パッチ適用ドキュメントは失敗し、マネージドノードに対するスキャンまたはインストールは実行されません。

コードの例

次の Python のコード例は、パッチベースラインオーバーライドを生成する方法を示しています。

```
import boto3
import json

ssm = boto3.client('ssm')
s3 = boto3.resource('s3')
s3_bucket_name = 'my-baseline-override-bucket'
s3_file_name = 'MyBaselineOverride.json'
baseline_ids_to_export = ['pb-0000000000000000', 'pb-0000000000000001']

baseline_overrides = []
for baseline_id in baseline_ids_to_export:
```

```
    baseline_overrides.append(ssm.get_patch_baseline(
        BaselineId=baseline_id
    ))

json_content = json.dumps(baseline_overrides, indent=4, sort_keys=True, default=str)
s3.Object(bucket_name=s3_bucket_name, key=s3_file_name).put(Body=json_content)
```

これにより、次のようなパッチベースラインオーバーライドが生成されます。

```
[
    {
        "ApprovalRules": {
            "PatchRules": [
                {
                    "ApproveAfterDays": 0,
                    "ComplianceLevel": "UNSPECIFIED",
                    "EnableNonSecurity": false,
                    "PatchFilterGroup": {
                        "PatchFilters": [
                            {
                                "Key": "PRODUCT",
                                "Values": [
                                    "*"
                                ]
                            },
                            {
                                "Key": "CLASSIFICATION",
                                "Values": [
                                    "*"
                                ]
                            },
                            {
                                "Key": "SEVERITY",
                                "Values": [
                                    "*"
                                ]
                            }
                        ]
                    }
                }
            ]
        },
        "ApprovedPatches": [],
```

```
        "ApprovedPatchesComplianceLevel": "UNSPECIFIED",
        "ApprovedPatchesEnableNonSecurity": false,
        "GlobalFilters": {
            "PatchFilters": []
        },
        "OperatingSystem": "AMAZON_LINUX_2",
        "RejectedPatches": [],
        "RejectedPatchesAction": "ALLOW_AS_DEPENDENCY",
        "Sources": []
    },
    {
        "ApprovalRules": {
            "PatchRules": [
                {
                    "ApproveUntilDate": "2021-01-06",
                    "ComplianceLevel": "UNSPECIFIED",
                    "EnableNonSecurity": true,
                    "PatchFilterGroup": {
                        "PatchFilters": [
                            {
                                "Key": "PRODUCT",
                                "Values": [
                                    "*"
                                ]
                            },
                            {
                                "Key": "CLASSIFICATION",
                                "Values": [
                                    "*"
                                ]
                            },
                            {
                                "Key": "SEVERITY",
                                "Values": [
                                    "*"
                                ]
                            }
                        ]
                    }
                }
            ]
        },
        "ApprovedPatches": [
            "open-ssl*"
```

```
        ],
        "ApprovedPatchesComplianceLevel": "UNSPECIFIED",
        "ApprovedPatchesEnableNonSecurity": false,
        "GlobalFilters": {
            "PatchFilters": []
        },
        "OperatingSystem": "CENTOS",
        "RejectedPatches": [
            "python*"
        ],
        "RejectedPatchesAction": "ALLOW_AS_DEPENDENCY",
        "Sources": []
    }
]
```

パッチベースライン

このセクションのトピックでは、Scan または Install オペレーションをマネージドノードで実行した場合、AWS Systems Manager のツールである Patch Manager でパッチベースラインがどのように機能するのかについて説明します。

トピック

- 事前定義されたパッチベースラインおよびカスタムパッチベースライン
- 承認されたパッチと拒否されたパッチのリストのパッケージ名の形式
- パッチグループ
- Windows Server で Microsoft がリリースしたアプリケーションへのパッチ適用について

事前定義されたパッチベースラインおよびカスタムパッチベースライン

AWS Systems Manager のツールである Patch Manager には、Patch Manager のサポート対象のオペレーティングシステムごとに定義済みのパッチベースラインがあります。これらのベースラインは、現在設定されているとおりに使用することも (カスタマイズすることはできません)、独自のカスタムパッチベースラインを作成することもできます。カスタムパッチベースラインを使用すると、環境に対してどのパッチを承認または拒否するかをより詳細に制御できます。また、定義済みのベースラインでは、これらのベースラインを使用してインストールされるすべてのパッチに、コンプライアンスレベル Unspecified が割り当てられます。コンプライアンス値を割り当てるには、定義済みのベースラインのコピーを作成し、パッチに割り当てるコンプライアンス値を指定できます。詳細については、「カスタムベースライン」および「カスタムパッチベースラインの操作」を参照してください。

> **Note**
>
> このトピックの情報は、パッチ適用オペレーションに使用している設定方法やタイプに関係なく適用されます。
>
> - Quick Setup で設定されているパッチポリシー
> - Quick Setup で設定されているホスト管理オプション
> - パッチ `Scan` または `Install` のタスクを実行するためのメンテナンスウィンドウ
> - オンデマンドの [今すぐパッチ適用] オペレーション

トピック

- 事前定義されたベースライン
- カスタムベースライン

事前定義されたベースライン

次の表に、Patch Manager に用意されている事前定義されたパッチベースラインを示します。

Patch Manager でサポートされている各オペレーティングシステムのバージョンについては、「Patch Manager の前提条件」を参照してください。

名前	サポートされるオペレーティングシステム	詳細
`AWS-AlmaLinuxDefaultPatchBaseline`	AlmaLinux	分類が「セキュリティ」で、重要度レベルが「非常事態」または「重要」のすべてのオペレーティングシステムパッチを承認します。また、分類が「Bugfix」(バグ修正) のすべてのパッチを承認します。パッチは、リリースまたは更新されてから 7 日後に自動承認されます。[1]

名前	サポートされるオペレーティングシステム	詳細
AWS-AmazonLinuxDefaultPatchBaseline	Amazon Linux 1	分類が「セキュリティ」で、重要度レベルが「非常事態」または「重要」のすべてのオペレーティングシステムパッチを承認します。また、分類が「Bugfix」(バグ修正) のすべてのパッチを自動承認します。パッチは、リリースまたは更新されてから 7 日後に自動承認されます。[1]
AWS-AmazonLinux2DefaultPatchBaseline	Amazon Linux 2	分類が「セキュリティ」で、重要度レベルが「非常事態」または「重要」のすべてのオペレーティングシステムパッチを承認します。また、分類が「Bugfix」(バグ修正) のすべてのパッチを承認します。パッチはリリースから 7 日後に自動承認されます。[1]
AWS-AmazonLinux2022DefaultPatchBaseline	Amazon Linux 2022	分類が「セキュリティ」で、重要度レベルが「非常事態」または「重要」のすべてのオペレーティングシステムパッチを承認します。パッチはリリースから 7 日後に自動承認されます。また、分類が "Bugfix" のすべてのパッチをリリースから 7 日後に承認します。

名前	サポートされるオペレーティングシステム	詳細
AWS-AmazonLinux2023DefaultPatchBaseline	Amazon Linux 2023	分類が「セキュリティ」で、重要度レベルが「非常事態」または「重要」のすべてのオペレーティングシステムパッチを承認します。パッチはリリースから 7 日後に自動承認されます。また、分類が "Bugfix" のすべてのパッチをリリースから 7 日後に承認します。
AWS-CentOSDefaultPatchBaseline	CentOS および CentOS Stream	すべての更新は、更新 (セキュリティ以外の更新を含む) が使用可能になってから 7 日後に承認されます。
AWS-DebianDefaultPatchBaseline	Debian Server	優先度が「Required」、「Important」、「Standard」、「Optional」、「Extra」のすべてのオペレーティングシステムのセキュリティに関連するパッチを即時に承認します。リポジトリに信頼できるリリース日がないため、承認前の待機期間はありません。
AWS-MacOSDefaultPatchBaseline	macOS	「セキュリティ」に分類されるすべてのオペレーティングシステムパッチを承認します。また、現在の更新を含むすべてのパッケージを承認します。

名前	サポートされるオペレーティングシステム	詳細
AWS-OracleLinuxDefaultPatchBaseline	Oracle Linux	分類が「セキュリティ」で、重要度レベルが「重要」または「中」のすべてのオペレーティングシステムパッチを承認します。また、分類が「Bugfix」(バグ修正) のすべてのパッチをリリースから 7 日後に承認します。パッチは、リリースまたは更新されてから 7 日後に自動承認されます。[1]
AWS-DefaultRaspbianPatchBaseline	Raspberry Pi OS	優先度が「Required」、「Important」、「Standard」、「Optional」、「Extra」のすべてのオペレーティングシステムのセキュリティに関連するパッチを即時に承認します。リポジトリに信頼できるリリース日がないため、承認前の待機期間はありません。
AWS-RedHatDefaultPatchBaseline	Red Hat Enterprise Linux (RHEL)	分類が「セキュリティ」で、重要度レベルが「非常事態」または「重要」のすべてのオペレーティングシステムパッチを承認します。また、分類が「Bugfix」(バグ修正) のすべてのパッチを承認します。パッチは、リリースまたは更新されてから 7 日後に自動承認されます。[1]

名前	サポートされるオペレーティングシステム	詳細
AWS-RockyLinuxDefaultPatchBaseline	Rocky Linux	分類が「セキュリティ」で、重要度レベルが「非常事態」または「重要」のすべてのオペレーティングシステムパッチを承認します。また、分類が「Bugfix」(バグ修正) のすべてのパッチを承認します。パッチは、リリースまたは更新されてから 7 日後に自動承認されます。[1]
AWS-SuseDefaultPatchBaseline	SUSE Linux Enterprise Server (SLES)	分類が「セキュリティ」で、重要度が「非常事態」または「重要度」のすべてのオペレーティングシステムパッチを承認します。パッチは、リリースまたは更新されてから 7 日後に自動承認されます。[1]
AWS-UbuntuDefaultPatchBaseline	Ubuntu Server	優先度が「Required」、「Important」、「Standard」、「Optional」、「Extra」のすべてのオペレーティングシステムのセキュリティに関連するパッチを即時に承認します。リポジトリに信頼できるリリース日がないため、承認前の待機期間はありません。

名前	サポートされるオペレーティングシステム	詳細
AWS-DefaultPatchBaseline	Windows Server	分類が「CriticalUpdates」または「SecurityUpdates」で、MSRC 重要度が「非常事態」または「重要」のすべての Windows Server オペレーティングシステムパッチを承認します。パッチは、リリースまたは更新されてから 7 日後に自動承認されます。[2]
AWS-WindowsPredefinedPatchBaseline-OS	Windows Server	分類が「CriticalUpdates」または「SecurityUpdates」で、MSRC 重要度が「非常事態」または「重要」のすべての Windows Server オペレーティングシステムパッチを承認します。パッチは、リリースまたは更新されてから 7 日後に自動承認されます。[2]
AWS-WindowsPredefinedPatchBaseline-OS-Applications	Windows Server	Windows Server オペレーティングシステムの場合は、分類が「CriticalUpdates」または「SecurityUpdates」で、MSRC 重要度が「非常事態」または「重要」のすべてのパッチを承認します。Microsoft がリリースしたアプリケーションについては、すべてのパッチを承認します。OS とアプリケーションのパッチのどちらも、リリースまたは更新から 7 日後に自動承認されます。[2]

[1] Amazon Linux 1 と Amazon Linux 2 の場合、パッチが自動承認されるまでの 7 日間の待機時間は、`Release Date` 値ではなく、`updateinfo.xml` の `Updated Date` 値から計算されます。さまざまな要因が `Updated Date` 値に影響を与える可能性があります。他のオペレーティングシステムでは、リリース日と更新日の処理が異なります。自動承認の遅延による予期しない結果を避けるのに役立つ情報については、「パッケージのリリース日と更新日の計算方法」を参照してください。

[2] Windows Server の場合、デフォルトのベースラインには 7 日間の自動承認遅延が含まれています。リリース後 7 日以内にパッチをインストールするには、カスタムベースラインを作成する必要があります。

カスタムベースライン

次の情報は、パッチ適用目標を達成するためのカスタムパッチベースラインの作成に役立ちます。

トピック

- カスタムベースラインでの自動承認の使用
- パッチベースラインを作成するための追加情報

カスタムベースラインでの自動承認の使用

独自のパッチベースラインを作成する場合は、以下のカテゴリを使用して自動承認するパッチを選択できます。

- オペレーティングシステム: Windows Server、Amazon Linux、Ubuntu Server など。
- 製品名 (オペレーティングシステム): 例えば、RHEL 6.5、Amazon Linux 2014.09、Windows Server 2012、Windows Server 2012 R2 など。
- 製品名 (Windows Server で Microsoft がリリースしたアプリケーションのみ): 例えば、Word 2016、BizTalk Server など。
- 分類: 例えば、緊急更新プログラム、セキュリティ更新プログラムなど。
- 重大度: 例えば、緊急、重要など。

作成する承認ルールごとに、自動承認の遅延を指定するか、パッチ承認の期限日を指定するかを選択できます。

> **Note**
>
> Ubuntu Server の更新プログラムパッケージのリリース日は確定できないため、このオペレーティングシステムでは自動承認オプションがサポートされていません。

自動承認の遅延とは、パッチがリリースまたは最後に更新されてから自動承認されて適用されるまでの待機日数です。例えば、`CriticalUpdates` 分類を使用してルールを作成し、自動承認の遅延として 7 日間を設定した場合、7 月 7 日にリリースされた新しい重要なパッチは 7 月 14 日に自動的に承認されます。

Linux リポジトリがパッケージのリリース日情報を提供しない場合、Patch Manager はパッケージのビルド時間を Amazon Linux 1、Amazon Linux 2、SUSE Linux Enterprise Server (SLES)、Red Hat Enterprise Linux (RHEL)、および CentOS の自動承認日指定の日付として使用します。パッケージのビルド時間が特定できない場合、Patch Manager はデフォルトの日付である 1970 年 1 月 1 日を使用します。これにより、Patch Manager は 1970 年 1 月 1 日以降の任意の日付のパッチを承認するように設定されたパッチベースラインの自動承認日指定をバイパスします。

自動承認の期限日を指定すると、Patch Manager はその日付以前にリリースまたは最後に更新されたすべてのパッチを自動的に適用します。例えば、期限日として 2023 年 7 月 7 日を指定すると、2023 年 7 月 8 日以降にリリースまたは最終更新されたパッチは自動的にインストールされません。

カスタムのパッチベースラインを作成する場合、そのパッチベースラインによって承認されたパッチのコンプライアンスの重要度レベル (`Critical` または `High` など) を指定できます。承認された任意のパッチのパッチ状態が `Missing` と報告された場合、パッチベースラインで報告される全体的なコンプライアンスの重要度は、指定した重要度レベルになります。

パッチベースラインを作成するための追加情報

パッチベースラインを作成する場合は、以下の点に注意してください。

- Patch Manager には、サポートされているオペレーティングシステムごとに 1 つの事前定義されたパッチベースラインがあります。対応するオペレーティングシステムの種類ごとに、独自のパッチベースラインを作成して、デフォルトとして指定してする場合を除き、これらの事前定義されたパッチベースラインが、オペレーティングシステムの種類ごとの、デフォルトのパッチベースラインとして使用されます。

> **Note**
>
> Windows Server では、3 つの事前に定義されたパッチベースラインが提供されます。パッチベースラインの AWS-DefaultPatchBaseline と AWS-WindowsPredefinedPatchBaseline-OS は、Windows オペレーティングシステム自体のオペレーティングシステム更新プログラムのみをサポートしています。AWS-DefaultPatchBaseline は、別のパッチベースラインを指定しない限り、Windows Server マネージドノードのデフォルトのパッチベースラインとして使用されます。これら 2 つのパッチベースラインの構成設定は同じです。2 つのうち新しい方である AWS-WindowsPredefinedPatchBaseline-OS は、Windows Server 用の 3 つ目の事前定義されたパッチベースラインと区別するために作成されました。そのパッチベースライン AWS-WindowsPredefinedPatchBaseline-OS-Applications を使用して、Windows Server オペレーティングシステムおよびサポートされている Microsoft アプリケーションの両方にパッチを適用できます。

- デフォルトで、Windows Server 2019 および Windows Server 2022 は後続の更新に置き換えられた更新を削除します。その結果、Windows Server パッチベースラインで ApproveUntilDate パラメータを使用しても、ApproveUntilDate パラメータで選択された日付が最新パッチの日付よりも前になっている場合は、パッチ適用オペレーションの実行時に新しいパッチがインストールされません。Windows Server パッチ適用ルールの詳細については、「セキュリティに関連するパッチの選択方法」の [Windows Server] タブを参照してください。

  これは、前月の緊急パッチがインストールされていない可能性がある場合でも、Systems Manager オペレーションに関してはマネージドノードが準拠状態にあることを意味します。ApproveAfterDays パラメータの使用時にも同じシナリオが発生する可能性があります。Microsoft の置き換えられたパッチ動作のため、ApproveAfterDays の日数が経過する前に Microsoft からの最新のパッチがリリースされた場合でも Windows Server 向けのパッチがインストールされないように、日数を設定することが可能です (通常は 30 日を超える日数)。

- Windows Server の場合のみ、パッチベースラインで承認されていない使用可能なセキュリティ更新パッチは、カスタムパッチベースラインでの定義に従い、コンプライアンス値 (Compliant または Non-Compliant) を持つことができます。

  パッチベースラインを作成または更新するときに、パッチベースラインで指定されたインストール基準を満たしていないため、使用可能ではあるものの承認されていないセキュリティパッチに割り当てるステータスを選択します。例えば、パッチがリリースされてからインストールされるまでに待機する期間を長く指定している場合は、インストールするセキュリティパッチをスキップできま

す。指定した待機期間中にパッチの更新がリリースされると、パッチのインストールの待機期間がもう一度開始されます。待機期間が長すぎる場合、複数のバージョンのパッチがリリースされ、インストールされない可能性があります。

コンソールを使用してパッチベースラインを作成または更新するには、[使用可能なセキュリティ更新のコンプライアンスステータス] フィールドでこのオプションを指定します。AWS CLI を使用して create-patch-baseline または update-patch-baseline コマンドを実行し、`available-security-updates-compliance-status` パラメータでこのオプションを指定します。

- オンプレミスのサーバーおよび仮想マシン (VM) の場合、Patch Manager では独自にデフォルトとして指定したパッチベースラインが使用されます。独自のデフォルトパッチベースラインがない場合は、事前定義済みのパッチベースラインが対応するオペレーティングシステムに使用されます。
- 同じパッチベースラインで承認および拒否の両方の対象に指定されているパッチがある場合、そのパッチは拒否されます。
- 1 つのマネージドノードに定義できるパッチベースラインは 1 つに限ります。
- パッチベースラインの承認されたパッチと拒否されたパッチのリストに追加できるパッケージ名の形式は、パッチするオペレーティングシステムにより異なります。

  承認済みパッチと拒否済みパッチのリストの許容されるフォーマットの詳細については、「承認されたパッチと拒否されたパッチのリストのパッケージ名の形式」を参照してください。
- Quick Setup でパッチポリシー設定を使用している場合、カスタムパッチベースラインに加えた更新は 1 時間に 1 回 Quick Setup と同期されます。

  パッチポリシーで参照されていたカスタムパッチベースラインを削除すると、Quick Setup のそのパッチポリシーについての [Configuration details] (設定の詳細) ページにバナーが表示されます。バナーには、パッチポリシーが既に存在しないパッチベースラインを参照していること、およびそれ以降のパッチ適用オペレーションができないことが示されます。この場合は、Quick Setup の [Configurations] (設定) ページに戻り、Patch Manager 設定を選択し、[Actions] (アクション)、[Edit configuration] (設定を編集) を選択します。削除されたパッチベースライン名が強調表示されます。影響を受けるオペレーティングシステム用の新しいパッチベースラインを選択する必要があります。

パッチベースラインの作成については、「カスタムパッチベースラインの操作」および「チュートリアル: AWS CLI を使用してサーバー環境にパッチを適用する」を参照してください。

承認されたパッチと拒否されたパッチのリストのパッケージ名の形式

承認されたパッチと拒否されたパッチのリストに追加できるパッケージ名の形式は、パッチするオペレーティングシステムにより異なります。

Linux オペレーティングシステムのパッケージ名の形式

パッチベースラインで承認されたパッチと拒否されたパッチに指定できる形式は Linux タイプにより異なります。具体的には、サポートされている形式は、Linux オペレーティングシステムのタイプで使用されているパッケージマネージャーにより異なります。

トピック

- Amazon Linux 1、Amazon Linux 2、Amazon Linux 2022、Amazon Linux 2023、CentOS、Oracle Linux、および Red Hat Enterprise Linux (RHEL)
- Debian Server、Raspberry Pi OS (旧称 Raspbian)、および Ubuntu Server
- SUSE Linux Enterprise Server (SLES)

Amazon Linux 1、Amazon Linux 2、Amazon Linux 2022、Amazon Linux 2023、CentOS、Oracle Linux、および Red Hat Enterprise Linux (RHEL)

パッケージマネージャー: YUM (パッケージマネージャーとして DNF を使用する Amazon Linux 2022、Amazon Linux 2023、RHEL 8 および CentOS 8 を除く)

承認されたパッチ: 承認されたパッチでは、次のいずれかを指定できます。

- 1234567 形式の Bugzilla ID (システムは数字のみの文字列を Bugzilla ID として処理します)。
- CVE-2018-1234567 形式の CVE ID
- RHSA-2017:0864 や ALAS-2018-123 などの形式のアドバイザリ ID
- パッケージ名の指定に使用可能なコンポーネントを 1 つ以上使用して作成されたパッケージ名。例として、dbus.x86_64:1:1.12.28-1.amzn2023.0.1 という名前のパッケージでは、コンポーネントは以下のとおりです。
  - name: dbus
  - architecture: x86_64
  - epoch: 1
  - version: 1.12.28
  - release: 1.amzn2023.0.1

次の構造のパッケージ名がサポートされます。

- name
- name.arch
- name-version
- name-version-release
- name-version-release.arch
- version
- version-release
- epoch:version-release
- name-epoch:version-release
- name-epoch:version-release.arch
- epoch:name-version-release.arch
- name.arch:epoch:version-release

例:

- dbus.x86_64
- dbus-1.12.28
- dbus-1.12.28-1.amzn2023.0.1
- dbus-1:1.12.28-1.amzn2023.0.1.x86_64

- また、以下のように、上記の形式で 1 つのワイルドカードを含むパッケージ名コンポーネントもサポートされます。
  - dbus*
  - dbus-1.12.2*
  - dbus-*:1.12.28-1.amzn2023.0.1.x86_64

拒否されたパッチ: 拒否されたパッチでは、次のいずれかを指定できます。

- パッケージ名の指定に使用可能なコンポーネントを 1 つ以上使用して作成されたパッケージ名。例として、dbus.x86_64:1:1.12.28-1.amzn2023.0.1 という名前のパッケージでは、コンポーネントは以下のとおりです。
  - name: dbus
  - architecture; x86_64

- epoch: 1
- version: 1.12.28
- release: 1.amzn2023.0.1

次の構造のパッケージ名がサポートされます。

- name
- name.arch
- name-version
- name-version-release
- name-version-release.arch
- version
- version-release
- epoch:version-release
- name-epoch:version-release
- name-epoch:version-release.arch
- epoch:name-version-release.arch
- name.arch:epoch:version-release

例:

- dbus.x86_64
- dbus-1.12.28
- dbus-1.12.28-1.amzn2023.0.1
- dbus-1:1.12.28-1.amzn2023.0.1.x86_64

- また、以下のように、上記の形式で 1 つのワイルドカードを含むパッケージ名コンポーネントもサポートされます。
  - dbus*
  - dbus-1.12.2*
  - dbus-*:1.12.28-1.amzn2023.0.1.x86_64

Debian Server、Raspberry Pi OS (旧称 Raspbian)、および Ubuntu Server

パッケージマネージャー: APT

承認されたパッチと拒否されたパッチ: 承認されたパッチと拒否されたパッチの両方で、以下を指定します。

- `ExamplePkg33` 形式のパッケージ名

> **Note**
>
> Debian Server のリスト、Raspberry Pi OS のリスト、および Ubuntu Server のリストでは、アーキテクチャやバージョンなどの要素は含めません。たとえば、パッケージ名 `ExamplePkg33` を指定し、パッチリストに次のすべてが含まれるようにします。
>
> - `ExamplePkg33.x86.1`
> - `ExamplePkg33.x86.2`
> - `ExamplePkg33.x64.1`
> - `ExamplePkg33.3.2.5-364.noarch`

SUSE Linux Enterprise Server (SLES)

パッケージマネージャー: Zypper

承認されたパッチと拒否されたパッチ: 承認されたパッチリストと拒否されたパッチリストの両方で、以下のいずれかを指定します。

- 以下のような形式の完全パッケージ名
  - `SUSE-SLE-Example-Package-12-2018-123`
  - `example-pkg-2018.11.4-46.17.1.x86_64.rpm`
- 以下のような単一のワイルドカードのあるパッケージ名
  - `SUSE-SLE-Example-Package-12-2018-*`
  - `example-pkg-2018.11.4-46.17.1.*.rpm`

macOS のパッケージ名の形式

サポートされているパッケージマネージャー: softwareupdate、installer、Brew、Brew Cask

承認されたパッチと拒否されたパッチ: 承認されたパッチと拒否されたパッチリストの両方について、次のような形式で詳細なパッケージ名を指定します。

- `XProtectPlistConfigData`
- `MRTConfigData`

macOS の承認済みおよび拒否されたパッチリストでは、ワイルドカードはサポートされません。

Windows オペレーティングシステムのパッケージ名の形式

Windows オペレーティングシステムでは、Microsoft Knowledge Base ID と Microsoft Security Bulletin ID を使用して、以下の例のようにパッチを指定します。

```
KB2032276,KB2124261,MS10-048
```

パッチグループ

> **Note**
>
> パッチグループは、パッチポリシーに基づくパッチ適用オペレーションでは使用されません。パッチポリシーの使用については、「Quick Setup でのパッチポリシー設定」を参照してください。
> 2022 年 12 月 22 日にパッチポリシーのサポートがリリースされる前にパッチグループを使用していなかったアカウントとリージョンのペアでは、コンソールでパッチグループの機能がサポートされていません。パッチグループの機能は、この日付より前にパッチグループの使用を開始したアカウントとリージョンのペアで引き続き使用できます。

パッチグループを使用して、AWS Systems Manager のツールである Patch Manager でマネージドノードを特定のパッチベースラインに関連付けることができます。パッチグループは、正しい一連のノードに、関連するパッチベースラインのルールに基づいて、適切なパッチをデプロイしていることを確認するのに役立ちます。パッチグループを使用すると、適切なテストの完了前にパッチがデプロイされることも回避できます。たとえば、環境別 (開発、テスト、実稼働など) にパッチグループを作成して、適切なパッチベースラインに各パッチグループを登録できます。

パッチ適用のために `AWS-RunPatchBaseline` またはその他の SSM コマンドドキュメントを実行する場合は、ノード ID やタグを使用して、マネージドノードをターゲットにすることができます。SSM Agent と Patch Manager は、マネージドノードに追加したパッチグループの値に基づいて、使用するパッチベースラインを評価します。

タグを使用してパッチグループを定義する

ハイブリッドおよびマルチクラウド環境では、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスと非 EC2 ノードに適用されたタグを使用して、パッチグループを作成します。パッチグループのタグの使用に関する以下の詳細に注意してください。

- パッチグループは、マネージドノードに適用されたタグキー `Patch Group` または `PatchGroup` のいずれかを使用して定義する必要があります。パッチベースラインのパッチグループを登録する場合、これら 2 つのキーに指定された同一の値は、同じグループの一部であると解釈されます。例えば、次のキーと値のペアの 1 つ目で 5 つのノードにタグ付けし、2 つ目で 5 つのノードにタグ付けしたとします。
  - `key=PatchGroup,value=DEV`
  - `key=Patch Group,value=DEV`

  ベースラインを作成する Patch Manager コマンドは、これらの 10 個のマネージドノードを、値 DEV に基づいて 1 つのグループに結合します。AWS CLI でパッチグループのパッチベースラインを作成するコマンドは次のとおりです。

  ```
  aws ssm register-patch-baseline-for-patch-group \
      --baseline-id pb-0c10e65780EXAMPLE \
      --patch-group DEV
  ```

  異なるキーの値を 1 つのターゲットに結合することは、新しいパッチグループを作成するこの Patch Manager コマンドに固有であり、他の API アクションではサポートされていません。例えば、同じ値を持つ `PatchGroup` キーと `Patch Group` キーを使用して send-command アクションを実行する場合、2 つのまったく異なるノードセットをターゲットにしています。

  ```
  aws ssm send-command \
      --document-name AWS-RunPatchBaseline \
      --targets "Key=tag:PatchGroup,Values=DEV"
  ```

  ```
  aws ssm send-command \
      --document-name AWS-RunPatchBaseline \
      --targets "Key=tag:Patch Group,Values=DEV"
  ```

- タグベースのターゲティングには制限があります。`SendCommand` のターゲットの各配列には、最大 5 つのキーと値のペアを含めることができます。

- これらのタグキー規則は、PatchGroup (スペースなし) または Patch Group (スペースあり) のいずれか 1 つだけ選択することをお勧めします。ただし、インスタンス上の EC2 インスタンスメタデータでタグを許可している場合は、PatchGroup を使用する必要があります。
- キーでは大文字と小文字が区別されます。グループのリソースを特定し対象としやすくするために任意の値 (「Web サーバー」や「US-EAST-PROD」など) を指定できますが、キーは Patch Group または PatchGroup でなければなりません。

パッチグループを作成してマネージドノードにタグを付けたら、パッチグループをパッチベースラインに登録できます。パッチグループをパッチベースラインに登録することで、パッチグループ内のノードは、関連付けられたパッチベースラインで定義されているルールを使用します。

パッチグループを作成する方法とパッチグループをパッチベースラインに関連付ける方法の詳細については、「パッチグループの作成と管理」および「パッチグループをパッチベースラインに追加する」を参照してください。

AWS Command Line Interface (AWS CLI)を使用したパッチベースラインとパッチグループの作成例については、「チュートリアル: AWS CLI を使用してサーバー環境にパッチを適用する」を参照してください。Amazon EC2 タグの詳細については、「Amazon EC2 ユーザーガイド」の「Amazon EC2 リソースのタグ付け」を参照してください。

使用方法

システムでタスクを実行してマネージドノードにパッチベースラインを適用するときに、SSM Agent はそのノードにパッチグループの値が定義されているかどうかを確認します。ノードがパッチグループに割り当てられている場合、Patch Manager はそのパッチグループにどのパッチベースラインが登録されているかを確認します。そのグループにパッチベースラインがある場合、Patch Manager は関連付けられているパッチベースラインを使用するように SSM Agent に通知します。ノードにパッチグループが設定されていない場合、Patch Manager は現在設定されているデフォルトのパッチベースラインを使用するように SSM Agent に自動的に通知します。

Important

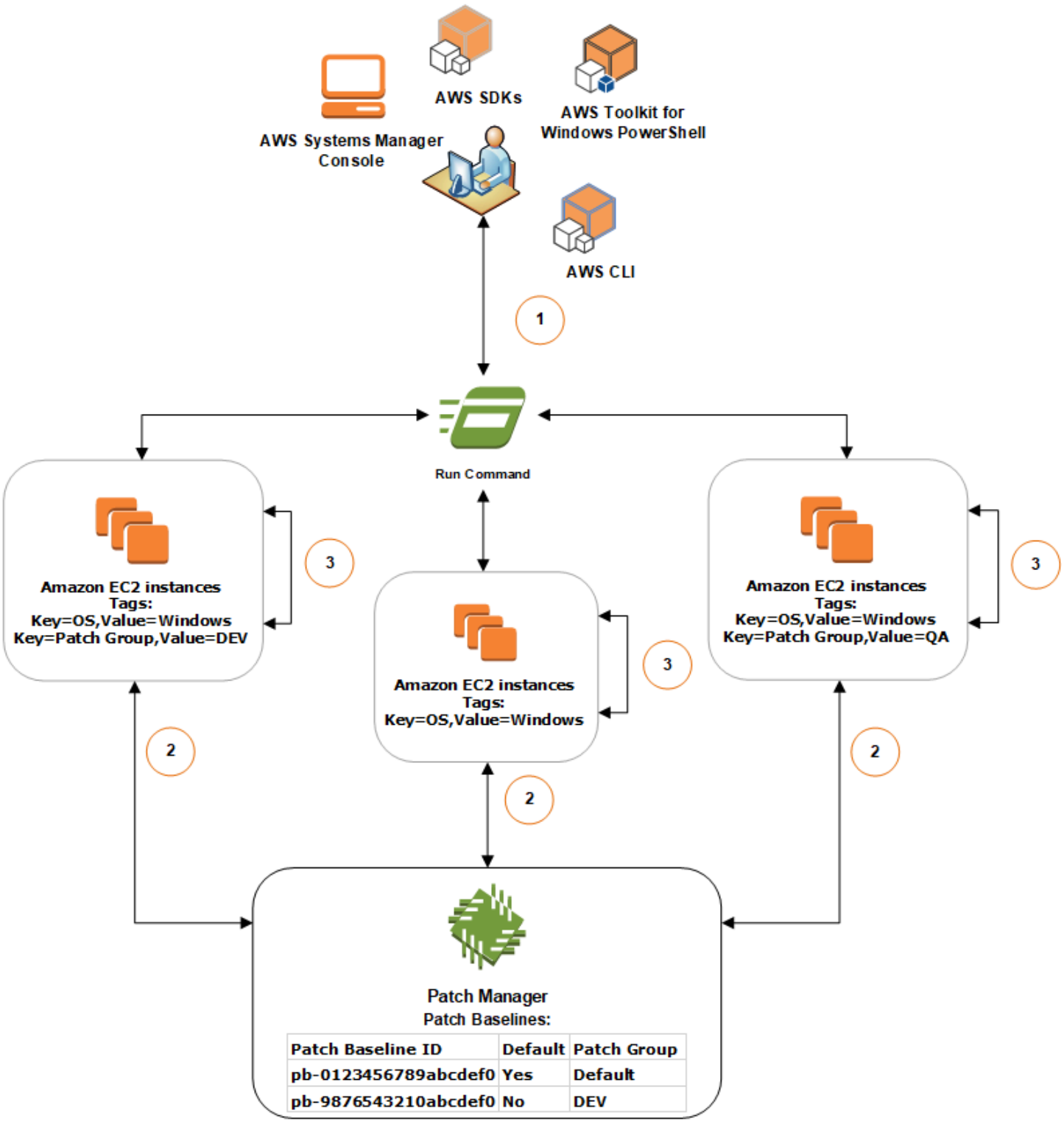
マネージドノードは 1 つのパッチグループのみ所属できます。
パッチグループは、オペレーティングシステムタイプごとに 1 つのパッチベースラインのみに登録できます。
インスタンスで [Allow tags in instance metadata] (インスタンスメタデータ内のタグを許可する) オプションを有効にした場合は、Amazon EC2 インスタンスに Patch Group タグ (スペースなし) を適用することはできません。インスタンスメタデータでタグを許可すると、

タグキー名にスペースが含まれなくなります。EC2 インスタンスのメタデータでタグを許可している場合は、スペースなしでタグキー `PatchGroup` を使用する必要があります。

図 1: パッチ適用オペレーションのプロセスの流れの一般的な例

次の図は、Run Command タスクをサーバーのフリートに送信し、Patch Manager を使用してパッチを適用する場合に、Systems Manager が実行するプロセスの一般的な例を示しています。これらのプロセスは、パッチ適用オペレーションで使用するパッチベースラインを決定します。(コマンドを送信して Patch Manager を使用してパッチを適用するようにメンテナンスウィンドウを設定した場合にも、同様のプロセスが使用されます。)

完全なプロセスについては、以下の図で説明します。



この例では、次のタグが適用される、Windows Server 用の 3 つの EC2 インスタンスのグループがあります。

EC2 インスタンスグループ	タグ
グループ 1	key=OS,value=Windows key=PatchGroup,value=DEV
グループ 2	key=OS,value=Windows
グループ 3	key=OS,value=Windows key=PatchGroup,value=QA

この例では、これら 2 つの Windows Server パッチベースラインも用意されています。

パッチベースライン ID	デフォルト	関連するパッチグループ
pb-0123456789abcdef0	はい	Default
pb-9876543210abcdef0	いいえ	DEV

AWS Systems Manager のツールである Run Command、および Patch Manager を使用して、パッチのスキャンまたはインストールを行う場合の一般的な手順は以下のとおりです。

1. パッチにコマンドを送信する: ドキュメント AWS-RunPatchBaseline を使用して Run Command タスクを送信するには、Systems Manager コンソール、SDK、AWS Command Line Interface (AWS CLI)、または AWS Tools for Windows PowerShell を使用します。key=OS,value=Windows タグをターゲットにして、マネージドインスタンスにパッチを適用する Run Command タスクを図に示します。
2. パッチベースラインの確認: SSM Agentは、EC2 インスタンスに適用されているパッチグループタグを確認し、対応するパッチベースラインを Patch Manager に問い合わせます。
   - パッチベースラインに関連付けられている一致するパッチグループの値:
     1. グループ 1 の EC2 インスタンスにインストールされている SSM Agent は、ステップ 1 で発行されたコマンドを受け取ってパッチ適用オペレーションを開始します。SSM Agent は、EC2 インスタンスのパッチグループタグの値に DEV が適用されていることを確認し、関連付けられているパッチベースラインをPatch Managerに問い合わせます。

2. Patch Managerは、パッチベースラインの pb-9876543210abcdef0 がパッチグループの DEV に関連付けられていることを確認し、SSM Agentに通知します。
3. SSM Agent は、pb-9876543210abcdef0 で設定されている承認ルールと例外に基づいてPatch Managerからパッチベースラインのスナップショットを取得して、次のステップに進みます。

- インスタンスに追加されたパッチグループタグはありません。

1. グループ 2 の EC2 インスタンスにインストールされている SSM Agent は、ステップ 1 で発行されたコマンドを受け取ってパッチ適用オペレーションを開始します。SSM Agent は、EC2 インスタンスに Patch Group または PatchGroup タグが適用されていないことを確認します。そのため、SSM Agent はデフォルトの Windows のパッチベースラインを Patch Manager に問い合わせます。
2. Patch Managerは、デフォルトの Windows Server のパッチベースラインが pb-0123456789abcdef0 であることを確認し、SSM Agentに通知します。
3. SSM Agent は、デフォルトのパッチベースラインの pb-0123456789abcdef0 で設定されている承認ルールと例外に基づいてPatch Managerからパッチベースラインのスナップショットを取得して、次のステップに進みます。

- パッチベースラインに一致するパッチグループの値が関連付けられていません。

1. グループ 3 の EC2 インスタンスにインストールされている SSM Agentは、ステップ 1 で発行されたコマンドを受け取ってパッチ適用オペレーションを開始します。SSM Agent は、EC2 インスタンスのパッチグループタグの値に QA が適用されていることを確認し、関連付けられているパッチベースラインをPatch Managerに問い合わせます。
2. Patch Manager は、パッチグループの QA に関連付けられているパッチベースラインを見つけられません。
3. Patch Managerは、デフォルトの Windows のパッチベースラインの pb-0123456789abcdef0 を使用するように SSM Agentに通知します。
4. SSM Agent は、デフォルトのパッチベースラインの pb-0123456789abcdef0 で設定されている承認ルールと例外に基づいてPatch Managerからパッチベースラインのスナップショットを取得して、次のステップに進みます。

3. パッチのスキャンまたはインストール。使用する適切なパッチベースラインを決定したら、SSM Agent は、ステップ 1 で指定されたオペレーションの値に基づいてスキャンまたはインストールのいずれかを開始します。スキャンまたはインストールするパッチは、Patch Managerによって提供されるパッチベースラインのスナップショットで定義されている承認ルールとパッチの例外に基づいて決定されます。

詳細情報

- パッチコンプライアンス状態の値

Windows Server で Microsoft がリリースしたアプリケーションへのパッチ適用について

このトピックの情報は、AWS Systems Manager のツールである Patch Manager を使用して Windows Server のアプリケーションにパッチを適用する準備を行う場合に役立ちます。

Microsoft アプリケーションのパッチ適用

Windows Server マネージドノードのアプリケーションのパッチ適用のサポートは、Microsoft がリリースしたアプリケーションに限定されます。

> **Note**
>
> Microsoft がリリースするアプリケーションのパッチは、更新日時を指定していない場合があります。このような場合、デフォルトでは 01/01/1970 の更新日時が指定されています。

Microsoft がリリースしたパッチ適用アプリケーションのパッチベースライン

Windows Server では、3 つの事前に定義されたパッチベースラインが提供されます。パッチベースラインの AWS-DefaultPatchBaseline と AWS-WindowsPredefinedPatchBaseline-OS は、Windows オペレーティングシステム自体のオペレーティングシステム更新プログラムのみをサポートしています。AWS-DefaultPatchBaseline は、別のパッチベースラインを指定しない限り、Windows Server マネージドノードのデフォルトのパッチベースラインとして使用されます。これら 2 つのパッチベースラインの構成設定は同じです。2 つのうち新しい方である AWS-WindowsPredefinedPatchBaseline-OS は、Windows Server 用の 3 つ目の事前定義されたパッチベースラインと区別するために作成されました。そのパッチベースライン AWS-WindowsPredefinedPatchBaseline-OS-Applications を使用して、Windows Server オペレーティングシステムおよびサポートされている Microsoft リリースのアプリケーションの両方にパッチを適用できます。

Windows Server マシンの Microsoft リリースのアプリケーションを更新するカスタムパッチベースラインを作成することもできます。

オンプレミスサーバー、エッジデバイス、VM、その他の EC2 以外のノードでの Microsoft がリリースしたアプリケーションへのパッチ適用のサポート

仮想マシン (VM) およびその他の EC2 以外のマネージドノードで Microsoft がリリースしたアプリケーションにパッチを適用するには、アドバンストインスタンス層を有効にする必要があります。アドバンストインスタンス層の使用には料金が発生します。ただし、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスで Microsoft がリリースしたアプリケーションにパッチを適用する場合、追加料金はかかりません。詳細については、「インスタンス層の設定」を参照してください。

「他の Microsoft 製品」の Windows 更新オプション

Patch Manager が Windows Server マネージドノードで Microsoft リリースのアプリケーションにパッチを適用できるようにするには マネージドノードで Windows Update オプションの [Give me updates for other Microsoft products when I update Windows] (Windows を更新するときに他の Microsoft 製品の更新を提供する) が有効になっている必要があります。

単一マネージドノードでこのオプションを有効にする方法の詳細については、Microsoft Support ウェブサイトの「Update Office with Microsoft Update」をご参照ください。

Windows Server 2016 以降を実行しているマネージドノードのフリートでは、グループ ポリシー オブジェクト (GPO) を使用して設定を有効にできます。グループポリシー管理エディターで、[Computer Configuration] (コンピューターの構成)、[Administrative Templates] (管理用テンプレート)、[Windows Components] (Windows コンポーネント)、[Windows Updates] (Windows の更新プログラム) にアクセスして、[Install updates for other Microsoft products] (他の Microsoft 製品の更新プログラムのインストール) を選択します。また、予定外の自動更新や Patch Manager 外部での再起動を防止する追加のパラメーターを使用して GPO を構成することをお勧めします。詳細については、Microsoft の技術文書ウェブサイトで公開されている「Configuring Automatic Updates in a Non-Active Directory Environment」(非 Active Directory 環境での自動更新の構成) を参照してください。

Windows Server 2012 または 2012 R2 を実行しているマネージドノードのフリートの場合、スクリプトを使用してオプションを有効にできます。詳細については、Microsoft ドキュメント ブログのウェブサイトの「Enabling and Disabling Microsoft Update in Windows 7 via Script」を参照してください。例えば、次の操作を実行できます。

1. ブログ投稿のスクリプトをファイルに保存します。
2. ファイルを Amazon Simple Storage Service (Amazon S3) バケットまたはその他のアクセス可能な場所にアップロードします。
3. AWS Systems Manager のツールである Run Command を使用して、次のようなコマンドを実行して、Systems Manager ドキュメント (SSM ドキュメント) `AWS-RunPowerShellScript` を使ってマネージドノードでスクリプトを実行します。

```
Invoke-WebRequest `
    -Uri "https://s3.aws-api-domain/amzn-s3-demo-bucket/script.vbs" `
    -Outfile "C:\script.vbs" cscript c:\script.vbs
```

パラメータの最小要件

カスタムパッチベースラインに Microsoft がリリースしたアプリケーションを含めるには、少なくとも、パッチを適用する製品を指定する必要があります。次の AWS Command Line Interface (AWS CLI)コマンドは、Microsoft Office 2016 などの製品にパッチを適用する最小限の要件を示します。

Linux & macOS

```
aws ssm create-patch-baseline \
    --name "My-Windows-App-Baseline" \
    --approval-rules
 "PatchRules=[{PatchFilterGroup={PatchFilters=[{Key=PRODUCT,Values='Office 2016'},
{Key=PATCH_SET,Values='APPLICATION'}]},ApproveAfterDays=5}]"
```

Windows Server

```
aws ssm create-patch-baseline ^
    --name "My-Windows-App-Baseline" ^
    --approval-rules
 "PatchRules=[{PatchFilterGroup={PatchFilters=[{Key=PRODUCT,Values='Office 2016'},
{Key=PATCH_SET,Values='APPLICATION'}]},ApproveAfterDays=5}]"
```

Microsoft アプリケーション製品ファミリーを指定した場合、指定する各製品は、選択した製品ファミリーのサポートされたメンバーである必要があります。たとえば、「Active Directory Rights Management Services Client 2.0」という製品にパッチを適用する場合、「Office」や「SQL Server」などではなく、「Active Directory」を製品ファミリーに指定する必要があります。次の AWS CLI コマンドは、製品ファミリーと製品の一致したペアを示します。

Linux & macOS

```
aws ssm create-patch-baseline \
    --name "My-Windows-App-Baseline" \
    --approval-rules
 "PatchRules=[{PatchFilterGroup={PatchFilters=[{Key=PRODUCT_FAMILY,Values='Active
```

```
Directory'},{Key=PRODUCT,Values='Active Directory Rights Management Services Client
2.0'},{Key=PATCH_SET,Values='APPLICATION'}]},ApproveAfterDays=5}]"
```

Windows Server

```
aws ssm create-patch-baseline ^
    --name "My-Windows-App-Baseline" ^
    --approval-rules
 "PatchRules=[{PatchFilterGroup={PatchFilters=[{Key=PRODUCT_FAMILY,Values='Active
 Directory'},{Key=PRODUCT,Values='Active Directory Rights Management Services Client
 2.0'},{Key=PATCH_SET,Values='APPLICATION'}]},ApproveAfterDays=5}]"
```

> **Note**
>
> 商品とファミリーのペアリングのミスマッチに関するエラーメッセージが表示される場合は、「問題:製品ファミリ/製品ペアの不一致」を参照すると問題解決に役立ちます。

Amazon Linux 2 マネージドノードで Kernel Live Patching を使用

Amazon Linux 2 の Kernel Live Patching により、実行中のアプリケーションを再起動や中断せずに、実行中の Linux カーネルにセキュリティの脆弱性や重大なバグのパッチを適用できます。これにより、インフラストラクチャを安全かつ最新に保つとともに、サービスとアプリケーションの可用性を向上させることができます。Kernel Live Patching は、Amazon EC2 インスタンス、AWS IoT Greengrass コアのデバイス、および Amazon Linux 2 を実行する [on-premises virtual machines] (オンプレミスの仮想マシン) でサポートされます。

Kernel Live Patching の一般的な情報については、Amazon Linux 2 ユーザーガイドの「Kernel Live Patching on AL2」を参照してください。

Amazon Linux 2 マネージドノードで Kernel Live Patching を有効にした後、AWS Systems Manager のツールである Patch Manager を使用すると、カーネルライブパッチをマネージドノードに適用できます。Patch Manager は、ノードで既存の yum ワークフローを使用して更新を適用する代わりに使用できます。

[開始する前に]

Patch Manager を使用してカーネルライブパッチを Amazon Linux 2 マネージドノードに適用するには、ノードが正しいアーキテクチャとカーネルバージョンに基づいていることを確認します。詳細に

ついては、「Amazon EC2 ユーザーガイド」の「サポートされる設定と前提条件」を参照してください。

トピック

- Patch Manager を使用した Kernel Live Patching
- Patch Manager を使用した Kernel Live Patching の仕組み
- Run Command を使用して Kernel Live Patching をオンにする
- Run Command の使用によるカーネルライブパッチの適用
- Run Command を使用して Kernel Live Patching をオフにする

Patch Manager を使用した Kernel Live Patching

カーネルバージョンの更新

カーネルライブ パッチ更新を適用した後、マネージドノードを再起動する必要はありません。ただし AWS では、リリース後最長 3 か月間、Amazon Linux 2 カーネルバージョンのカーネルライブパッチが提供されます。3 か月が過ぎた後にカーネルライブパッチを引き続き入手するには、新しいカーネルバージョンに更新する必要があります。メンテナンスウィンドウを使用して、少なくとも 3 か月に一度、ノードの再起動をスケジュールし、カーネルバージョンの更新を促すことをお勧めします。

カーネルライブパッチのアンインストール

カーネルライブパッチは、Patch Manager を使用してアンインストールすることはできません。代わりに Kernel Live Patching を無効にすることができます。これにより、適用されたカーネルライブパッチの RPM パッケージが削除されます。詳細については、「Run Command を使用して Kernel Live Patching をオフにする」を参照してください。

カーネルのコンプライアンス

場合によっては、現在のカーネルバージョンのライブパッチからすべての CVE 修正をインストールすると、そのカーネルが新しいカーネルバージョンと同じコンプライアンス状態になることがあります。この場合は、新しいバージョンが `Installed` と報告され、マネージドノードノードは `Compliant` と報告されます。ただし、新しいカーネルバージョンのインストール時間は報告されません。

1 つのカーネルライブパッチ、複数の CVE

カーネルライブパッチが複数の CVE に対応していて、これらの CVE にさまざまな分類や重要度値がある場合、そのパッチに対してレポートされるのは、CVE の中から最も高い分類と重要度だけです。

このセクションの以降では、Patch Manager を使用して、これらの要件を満たすマネージドノードノードにカーネルライブパッチを適用する方法について説明します。

Patch Manager を使用した Kernel Live Patching の仕組み

AWS では、セキュリティ更新とバグ修正の 2 種類を Amazon Linux 2 用のカーネルライブパッチとしてリリースしています。これらのタイプのパッチを適用するには、次の表に示す分類と重要度のみを対象としたパッチベースラインドキュメントを使用します。

分類	重要度
`Security`	`Critical`, `Important`
`Bugfix`	`All`

これらのパッチのみを対象としたカスタムパッチベースラインを作成することも、定義済みの `AWS-AmazonLinux2DefaultPatchBaseline` パッチベースラインを使用することもできます。つまり、`AWS-AmazonLinux2DefaultPatchBaseline` が有効になっている Amazon Linux 2 マネージドノードで Kernel Live Patching を使用でき、カーネルライブアップデートが適用されます。

> **Note**
>
> この `AWS-AmazonLinux2DefaultPatchBaseline` 設定では、パッチがリリースまたは最後に更新されてからパッチが自動的にインストールされるまでに 7 日間の待機期間が指定されます。カーネルライブパッチが自動承認されるまで 7 日間待機しない場合は、カスタムパッチベースラインを作成して使用できます。パッチベースラインでは、自動承認待機期間を指定しない、または短期間や長期間を指定できます。詳細については、「カスタムパッチベースラインの操作」を参照してください。

カーネルライブアップデートでマネージドノードにパッチを適用するには、以下の戦略をお勧めします。

1. Amazon Linux 2 マネージドノードの Kernel Live Patching を有効にします。
2. AWS Systems Manager のツールである Run Command を使用し、マネージドノードに対して `Scan` オペレーションを実行します。このとき、定義済みの `AWS-AmazonLinux2DefaultPatchBaseline` を使用するか、`Critical` および `Important` として重要度が分類される `Security` 更新と `All` の `Bugfix` 重要度のみを対象としたカスタムパッチベースラインを使用します。
3. スキャンされたマネージドノードについてパッチ適用の非準拠が報告されているかどうかを調べるには、AWS Systems Manager のツールである Compliance を使用します。報告されている場合は、ノードのコンプライアンス 詳細を表示して、マネージドノードに適用されていないカーネルライブパッチがないかどうかを確認します。
4. 適用されていないカーネルライブパッチをインストールするには、前に指定したものと同じパッチベースラインで Run Command を使用します。ただし今回は `Install` 操作ではなく `Scan` 操作を実行します。

   カーネルライブパッチは再起動しなくてもインストールされるため、この操作では再起動オプションとして `NoReboot` を選択できます。

   > **Note**
   >
   > マネージドノードにインストールされている他のタイプのパッチに必要な場合や、新しいカーネルに更新する場合は、マネージドノードを再起動できます。このような場合は、再起動オプション `RebootIfNeeded` を代わりに選択します。

5. Compliance に戻り、カーネルライブパッチがインストールされていることを確認します。

Run Command を使用して Kernel Live Patching をオンにする

Kernel Live Patching を有効にするには、お使いのマネージドノードで yum コマンドを実行するか、Run Command および作成するカスタム Systems Manager ドキュメント (SSM ドキュメント) を使用します。

マネージドノードで yum コマンドを直接実行して Kernel Live Patching をオンにする方法については、「Amazon EC2 ユーザーガイド」の「Kernel Live Patching の有効化」を参照してください。

> **Note**
>
> カーネルライブパッチを有効にしたときに、マネージドノードですでに実行されているカーネルが `kernel-4.14.165-131.185.amzn2.x86_64` (サポートされ

ている最小バージョン) より前の場合、プロセスは、利用可能な最新のカーネルバージョンをインストールしてマネージドノードを再起動します。ノードがすでに `kernel-4.14.165-131.185.amzn2.x86_64` 以降を実行している場合、プロセスは、新しいバージョンをインストールせず、ノードを再起動しません。

Run Command を使用して Kernel Live Patching をオンにするには (コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Run Command] を選択します。
3. [Run command (コマンドの実行)] を選択します。
4. [コマンドドキュメント] リストで、カスタム SSM ドキュメント `AWS-ConfigureKernelLivePatching` を選択します。
5. [Command parameters] (コマンドのパラメータ) セクションで、このオペレーションのパートとしてマネージドノードを再起動するかどうかを指定します。
6. このページの残りのコントロールを操作する方法については、「コンソールからコマンドを実行する」を参照してください。
7. [Run (実行)] を選択します。

Kernel Live Patching をオンにするには (AWS CLI)

- ローカルマシンで次のコマンドを実行します。

  Linux & macOS

  ```
  aws ssm send-command \
      --document-name "AWS-ConfigureKernelLivePatching" \
      --parameters "EnableOrDisable=Enable" \
      --targets "Key=instanceids,Values=instance-id"
  ```

  Windows Server

  ```
  aws ssm send-command ^
      --document-name "AWS-ConfigureKernelLivePatching" ^
      --parameters "EnableOrDisable=Enable" ^
      --targets "Key=instanceids,Values=instance-id"
  ```

instance-id は、この機能を有効にする Amazon Linux 2 マネージドノードの ID (例えば、i-02573cafcfEXAMPLE) に置き換えます。複数のマネージドノードでこの機能を有効にするには、次のいずれかの形式を使用できます。

- `--targets "Key=instanceids,Values=instance-id1,instance-id2"`
- `--targets "Key=tag:tag-key,Values=tag-value"`

コマンドで使用できるその他のオプションについては、AWS CLI コマンドリファレンス の send-command を参照してください。

Run Command の使用によるカーネルライブパッチの適用

カーネルライブパッチを適用するには、マネージドノードで yum コマンドを実行するか、Run Command および SSM ドキュメント `AWS-RunPatchBaseline` を使用します。

マネージドノードで直接 yum コマンドを実行してカーネルライブパッチを適用する方法については、「Amazon EC2 ユーザーガイド」の「カーネルライブパッチの適用」を参照してください。

Run Command を使用してカーネルライブパッチを適用するには (コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Run Command] を選択します。
3. [Run command (コマンドの実行)] を選択します。
4. [Command document] リストで、SSM ドキュメント `AWS-RunPatchBaseline` を選択します。
5. [コマンドのパラメータ] セクションで、次のいずれかの操作を行います。
   - 新しいカーネルライブパッチが利用可能かどうかをチェックする場合は、[オペレーション] で `Scan` を選択します。[Reboot Option] (再起動オプション) で、この操作後にマネージドノードを再起動しない場合は、`NoReboot` を選択します。操作が完了したら、Compliance で新しいパッチとコンプライアンスのステータスを確認できます。
   - パッチコンプライアンスをすでにチェック済みであり、利用可能なカーネルライブパッチを適用する準備ができている場合は、[操作] で `Install` を選択します。[Reboot Option] (再起動

オプション) で、この操作後にマネージドノードを再起動しない場合は、NoReboot を選択します。

6. このページの残りのコントロールを操作する方法については、「コンソールからコマンドを実行する」を参照してください。
7. [Run (実行)] を選択します。

Run Command を使用してカーネルライブパッチを適用するには (AWS CLI)

1. Compliance で結果を確認する前に Scan 操作を実行するには、ローカルマシンで次のコマンドを実行します。

   Linux & macOS

   ```
   aws ssm send-command \
       --document-name "AWS-RunPatchBaseline" \
       --targets "Key=InstanceIds,Values=instance-id" \
       --parameters '{"Operation":["Scan"],"RebootOption":["RebootIfNeeded"]}'
   ```

   Windows Server

   ```
   aws ssm send-command ^
       --document-name "AWS-RunPatchBaseline" ^
       --targets "Key=InstanceIds,Values=instance-id" ^
       --parameters {\"Operation\":[\"Scan\"],\"RebootOption\":[\"RebootIfNeeded
   \"]}
   ```

   コマンドで使用できるその他のオプションについては、AWS CLI コマンドリファレンス の send-command を参照してください。

2. Compliance で結果を確認した後に Install 操作を実行するには、ローカルマシンで次のコマンドを実行します。

   Linux & macOS

   ```
   aws ssm send-command \
       --document-name "AWS-RunPatchBaseline" \
       --targets "Key=InstanceIds,Values=instance-id" \
       --parameters '{"Operation":["Install"],"RebootOption":["NoReboot"]}'
   ```

Windows Server

```
aws ssm send-command ^
    --document-name "AWS-RunPatchBaseline" ^
    --targets "Key=InstanceIds,Values=instance-id" ^
    --parameters {\"Operation\":[\"Install\"],\"RebootOption\":[\"NoReboot\"]}
```

上記の両方のコマンドで、*instance-id* は、カーネルライブパッチを適用する Amazon Linux 2 マネージドノードの ID に置き換えます (i-02573cafcfEXAMPLE など)。複数のマネージドノードでこの機能を有効にするには、次のいずれかの形式を使用できます。

- `--targets "Key=instanceids,Values=instance-id1,instance-id2"`
- `--targets "Key=tag:tag-key,Values=tag-value"`

これらのコマンドで使用できるその他のオプションについては、AWS CLI コマンドリファレンス の send-command を参照してください。

Run Command を使用して Kernel Live Patching をオフにする

Kernel Live Patching をオフにするには、マネージドノードで yum コマンドを実行するか、Run Command およびカスタム SSM ドキュメント `AWS-ConfigureKernelLivePatching` を使用します。

> **Note**
>
> カーネルライブパッチを使用する必要がなくなった場合は、いつでも無効にできます。ほとんどの場合、この機能を無効にする必要はありません。

マネージドノードで yum コマンドを直接実行して Kernel Live Patching をオフにする方法については、「Amazon EC2 ユーザーガイド」の「Kernel Live Patching の有効化」を参照してください。

> **Note**
>
> Kernel Live Patching をオフにすると、プロセスは、Kernel Live Patching プラグインをアンインストールしてマネージドノードを再起動します。

Run Command を使用して Kernel Live Patching をオフにするには (コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Run Command] を選択します。
3. [Run command (コマンドの実行)] を選択します。
4. [Command document] リストで、SSM ドキュメント `AWS-ConfigureKernelLivePatching` を選択します。
5. [Command parameters] セクションで、必須パラメータの値を指定します。
6. このページの残りのコントロールを操作する方法については、「コンソールからコマンドを実行する」を参照してください。
7. [Run (実行)] を選択します。

Kernel Live Patching をオフにするには (AWS CLI)

- 以下のようなコマンドを使用します。

  Linux & macOS

  ```
  aws ssm send-command \
      --document-name "AWS-ConfigureKernelLivePatching" \
      --targets "Key=instanceIds,Values=instance-id" \
      --parameters "EnableOrDisable=Disable"
  ```

  Windows Server

  ```
  aws ssm send-command ^
      --document-name "AWS-ConfigureKernelLivePatching" ^
      --targets "Key=instanceIds,Values=instance-id" ^
      --parameters "EnableOrDisable=Disable"
  ```

  instance-id は、この機能を無効にする Amazon Linux 2 マネージドノードの ID (例えば、i-02573cafcfEXAMPLE) に置き換えます。複数のマネージドノードでこの機能を無効にするには、次のいずれかの形式を使用できます。

  - `--targets "Key=instanceids,Values=instance-id1,instance-id2"`
  - `--targets "Key=tag:tag-key,Values=tag-value"`

コマンドで使用できるその他のオプションについては、AWS CLI コマンドリファレンス の send-command を参照してください。

コンソールを使用した Patch Manager リソースとコンプライアンスの操作

AWS Systems Manager のツールである Patch Manager を使用するには、以下のタスクを実行します。各タスクについては、このセクションで詳しく説明します。

1. 使用するオペレーティングシステムの種類ごとに、AWS の定義済みのパッチベースラインがニーズを満たしていることを確認します。そうでない場合は、そのマネージドノードタイプの標準パッチセットを定義するパッチベースラインを作成し、代わりにそれをデフォルトとして設定します。
2. Amazon Elastic Compute Cloud (Amazon EC2) タグを使用してマネージドノードをパッチグループに整理します (オプションですが推奨します)。
3. 次のいずれかを行います :
   - (推奨) Systems Manager のツールである Quick Setup でパッチポリシーを設定すると、組織全体、組織単位の一部、またはシングル AWS アカウントに対して、未適用のパッチをスケジュールに従ってインストールできます。詳細については、「Quick Setup パッチポリシーを使用して組織内のインスタンスのためにパッチ適用を設定する」を参照してください。
   - Run Command タスクタイプで、Systems Manager ドキュメント (SSM ドキュメント) `AWS-RunPatchBaseline` を使用するメンテナンスウィンドウを作成します。詳細については、「チュートリアル: コンソールを使用してパッチ用メンテナンスウィンドウを作成する」を参照してください。
   - Run Command オペレーションで `AWS-RunPatchBaseline` を手動で実行します。詳細については、「コンソールからコマンドを実行する」を参照してください。
   - [Patch now] (今すぐパッチ適用) 機能を使用して、必要に応じてノードに手動でパッチを適用します。詳細については、「マネージドノードへのオンデマンド パッチ適用」を参照してください。
4. パッチ適用をモニタリングして、コンプライアンスを確認し、失敗を調査します。

トピック

- パッチポリシーの作成
- パッチダッシュボードの概要の表示

- パッチコンプライアンスレポートの使用
- マネージドノードへのオンデマンド パッチ適用
- パッチベースラインの操作
- 利用可能なパッチの表示
- パッチグループの作成と管理
- Patch Managerと AWS Security Hub の統合

パッチポリシーの作成

パッチポリシーは、AWS Systems Manager のツールである Quick Setup を使用して設定します。パッチポリシーを使用すると、他のパッチ適用の設定方法に比べて、パッチ適用オペレーションをより広範囲かつ一元的に制御できます。パッチポリシーでは、ノードとアプリケーションに自動的にパッチを適用するときに使用するスケジュールとベースラインを定義します。

詳細については、以下の各トピックを参照してください。

- Quick Setup でのパッチポリシー設定
- Quick Setup パッチポリシーを使用して組織内のインスタンスのためにパッチ適用を設定する

パッチダッシュボードの概要の表示

Patch Manager の [ダッシュボード] タブでは、コンソールの概要ビューが表示され、パッチ適用オペレーションを統合ビューで監視するために使用できます。Patch Manager は AWS Systems Manager のツールです。[Dashboard (ダッシュボード)] タブでは以下を表示できます。

- パッチ適用ルールに準拠している マネージドノードの数と非準拠の数のスナップショット。
- マネージドノードのパッチコンプライアンス結果の経過時間のスナップショット。
- 非準拠の最も一般的な理由ごとに、非準拠のマネージドノードの数を示すリンク数。
- 最新のパッチ適用オペレーションのリンクされたリスト。
- 設定された反復パッチ適用タスクのリンクされたリスト。

パッチダッシュボードの概要を表示するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。

2. ナビゲーションペインで、[Patch Manager] を選択します。
3. [Dashboard (ダッシュボード)] タブを選択します。
4. 表示したい概要データを含むセクションまでスクロールします。

   - Amazon EC2 インスタンスの管理
   - コンプライアンスの概要
   - コンプライアンス違反数
   - コンプライアンスレポート
   - パッチポリシーに基づかないオペレーション
   - パッチポリシーに基づかない繰り返しタスク

パッチコンプライアンスレポートの使用

次のトピックの情報を使用して、AWS Systems Manager のツールである Patch Manager でパッチコンプライアンスレポートの生成と操作を行います。

以下のトピックの情報は、パッチ適用オペレーションに使用する設定の方法や種類に関係なく適用されます。

- Quick Setup で設定されているパッチポリシー
- Quick Setup で設定されているホスト管理オプション
- パッチ `Scan` または `Install` のタスクを実行するためのメンテナンスウィンドウ
- オンデマンドの [Patch now] (今すぐパッチ適用) オペレーション

> **Important**
>
> パッチコンプライアンスのためにインスタンスをスキャンするオペレーションが複数種類ある場合は、スキャンするたびに以前のスキャンのパッチコンプライアンスデータが上書きされることに注意してください。その結果、パッチコンプライアンスデータで想定外の結果を得ることがあります。詳細については、「パッチコンプライアンスデータに対する意図しない上書きの回避」を参照してください。
>
> どのパッチベースラインが最新のコンプライアンス情報の生成に使用されたかを確認するには、Patch Manager の [コンプライアンスレポート] タブに移動し、情報を確認するマネージドノードの行を探して、[使用されたベースライン ID] 列にあるベースライン ID を選択します。

トピック

- パッチコンプライアンス結果の表示
- .csv パッチコンプライアンスレポートの生成
- Patch Manager で非準拠のマネージドノードを修復するには
- パッチコンプライアンスデータに対する意図しない上書きの回避

パッチコンプライアンス結果の表示

これらの手順を使用して、マネージドノードに関するパッチコンプライアンス情報を表示します。

この手順は、AWS-RunPatchBaseline ドキュメントを使用するパッチ操作に適用されます。AWS-RunPatchBaselineAssociation ドキュメントを使用するパッチ操作のパッチコンプライアンス情報の表示については、「非準拠のマネージドノードの識別」を参照してください。

> **Note**
>
> Quick Setup と Explorer のパッチスキャンオペレーションでは、AWS-RunPatchBaselineAssociation ドキュメントが使用されます。Quick Setup と Explorer はどちらも AWS Systems Manager のツールです。

特定の CVE の問題を解決するパッチの識別 (Linux)

多くの Linux ベースのオペレーティングシステムでは、パッチのコンプライアンスの結果にどの共通脆弱性識別子 (CVE) の問題がどのパッチによって解決されるかが示されます。この情報は、不足または失敗したパッチのインストールを緊急に行う必要があるかどうかを判断するために役立ちます。

CVE の詳細は、以下のタイプのオペレーティングシステムでサポートされるバージョンについて表示されます。

- AlmaLinux
- Amazon Linux 1
- Amazon Linux 2
- Amazon Linux 2022
- Amazon Linux 2023
- Oracle Linux

- Red Hat Enterprise Linux (RHEL)
- Rocky Linux
- SUSE Linux Enterprise Server (SLES)

> **Note**
>
> デフォルトでは、CentOS および CentOS Stream の更新に関する CVE 情報は提供されません。ただし、サードパーティーのリポジトリ (Fedora によって公開されている Extra Packages for Enterprise Linux (EPEL) リポジトリなど) を使用して、このサポートを許可することができます。詳細については、Fedora Wiki の EPEL を参照してください。
> 現在、CVE ID の値は、ステータスが `Missing` または `Failed` のパッチについてのみ報告されます。

状況やパッチ適用の目的に応じて、パッチベースラインの承認済みパッチまたは拒否済みパッチのリストに CVE ID を追加することもできます。

承認済みパッチおよび拒否済みパッチのリストの使用については、以下のトピックを参照してください。

- カスタムパッチベースラインの操作
- 承認されたパッチと拒否されたパッチのリストのパッケージ名の形式
- Linux ベースシステムでのパッチベースラインルールの動作方法
- パッチのインストール方法

> **Note**
>
> Microsoft がリリースするアプリケーションのパッチは、更新日時を指定していない場合があります。このような場合、デフォルトでは `01/01/1970` の更新日時が指定されています。

パッチ適用のコンプライアンス結果を表示する

AWS Systems Manager コンソールでパッチコンプライアンス結果を表示するには、以下の手順に従います。

> **Note**
>
> Amazon Simple Storage Service (Amazon S3) バケットにダウンロードされるパッチコンプライアンスレポートの生成については、「.csv パッチコンプライアンスレポートの生成」を参照してください。

パッチコンプライアンス結果を表示するには

1. 以下のいずれかを行ってください。

   オプション 1 (推奨) – AWS Systems Manager のツールである Patch Manager から移動します。

   - ナビゲーションペインで、Patch Manager を選択します。
   - [Compliance reporting] (コンプライアンスレポート) タブを選択します。
   - [ノードのパッチ適用の詳細] 領域で、パッチコンプライアンス結果を確認するマネージドノードのノード ID を選択します。
   - [詳細] 領域の [プロパティ] リストで、[パッチ]を選択します。

   オプション 2 – AWS Systems Manager のツールである Compliance から移動します。

   - ナビゲーションペインで、[コンプライアンス] を選択します。
   - [コンプライアンスリソースの概要] で、確認するパッチリソースのタイプ ([非準拠リソース] など) の列で数値を選択します。
   - 下方の [リソース] リストで、パッチコンプライアンス結果を確認するマネージドノードの ID を選択します。
   - [詳細] 領域の [プロパティ] リストで、[パッチ]を選択します。

   オプション 3 – AWS Systems Manager のツールである Fleet Manager から移動します。

   - ナビゲーションペインで、Fleet Manager を選択します。
   - [マネージドインスタンス] 領域で、パッチコンプライアンス結果を確認するマネージドノードの ID を選択します。
   - [詳細] 領域の [プロパティ] リストで、[パッチ]を選択します。

2. (オプション) [検索] ボックス
( )
で、利用可能なフィルターから選択します。

   たとえば、Red Hat Enterprise Linux (RHEL)の場合は、以下から選択します。

   - 名前
   - 分類
   - 状態
   - 重要度

   Windows Server の場合は、次の中から選択します。

   - KB
   - 分類
   - 状態
   - 重要度

3. 選択したフィルタータイプに使用可能な値の 1 つを選択します。例えば、[状態] を選択した場合は、[InstalledPendingReboot]、[失敗] や [見つかりません] などのコンプライアンス状態を選択します。

   > **Note**
   >
   > 現在、CVE ID の値は、ステータスが `Missing` または `Failed` のパッチについてのみ報告されます。

4. マネージドノードのコンプライアンス状態に応じて、準拠していないノードを修正するために実行するアクションを選択できます。

   例えば、準拠していないマネージドノードにすぐにパッチを適用するよう選択できます。オンデマンドでマネージドノードにパッチを適用する方法については、「マネージドノードへのオンデマンド パッチ適用」を参照してください。

   パッチコンプライアンス状態の詳細については、「パッチコンプライアンス状態の値」を参照してください。

.csv パッチコンプライアンスレポートの生成

AWS Systems Manager コンソールを使用して、任意の Amazon Simple Storage Service (Amazon S3) バケットに .csv ファイルとして保存されるパッチコンプライアンスレポートを生成できます。オンデマンドレポートを 1 つだけ生成することも、レポートを自動的に生成するスケジュールを指定することもできます。

レポートは、単一のマネージドノードに対して、または選択した AWS アカウント および AWS リージョン のすべてのマネージドノードに対して生成することができます。単一のノードの場合、レポートには、非準拠のノードに関連するパッチの ID など、包括的な詳細が含まれます。すべてのマネージドノードに関するレポートでは、非準拠ノードのパッチ概要情報と数のみが表示されます。

レポートが生成されたら、Amazon QuickSight などのツールを使用してデータをインポートおよび分析できます。QuickSight は、インタラクティブなビジュアル環境で情報を探索および解釈するために使用できるビジネスインテリジェンス (BI) サービスです。詳細については、「Amazon QuickSight ユーザーガイド」を参照してください。

> **Note**
>
> カスタムのパッチベースラインを作成する場合、そのパッチベースラインによって承認されたパッチのコンプライアンスの重要度レベル (`Critical` または `High` など) を指定できます。承認された任意のパッチのパッチ状態が `Missing` と報告された場合、パッチベースラインで報告される全体的なコンプライアンスの重要度は、指定した重要度レベルになります。

レポートが生成されたときに通知を送信するために使用する Amazon Simple Notification Service (Amazon SNS) トピックを指定することもできます。

パッチコンプライアンスレポートを生成するためのサービスロール

レポートを初めて生成する場合、Systems Manager は、S3 へのエクスポートプロセスに使用する `AWS-SystemsManager-PatchSummaryExportRole` という名前のオートメーション仮定ロールを作成します。

> **Note**
>
> コンプライアンスデータを暗号化された S3 バケットにエクスポートする場合は、関連する AWS KMS キーポリシーを更新して、`AWS-SystemsManager-`

PatchSummaryExportRole に必要な許可を与える必要があります。例えば、S3 バケットの AWS KMS ポリシーに次のような許可を追加してください。

```
{
    "Effect": "Allow",
    "Action": [
        "kms:GenerateDataKey"
    ],
    "Resource": "role-arn"
}
```

role-arn を、アカウントで作成した Amazon リソースネーム (ARN) に、arn:aws:iam::*111222333444*:role/service-role/AWS-SystemsManager-PatchSummaryExportRole 形式で置き換えます。
詳細については、「AWS Key Management Service デベロッパーガイド」の「AWS KMS でのキーポリシー」を参照してください。

スケジュールに基づいてレポートを初めて生成する際に、Systems Manager は、エクスポートプロセスに使用するサービスロール AWS-SystemsManager-PatchSummaryExportRole (まだ作成されていない場合) とともに、AWS-EventBridge-Start-SSMAutomationRole という名前の別のサービスロールを作成します。AWS-EventBridge-Start-SSMAutomationRole は、Amazon EventBridge を有効にしてランブック AWS-ExportPatchReportToS3 を使用してオートメーションを開始できるようにします。

これらのポリシーとロールを変更することはお勧めしません。変更することにより、パッチコンプライアンスレポートの生成が失敗する可能性があります。詳細については、「」を参照してくださいパッチコンプライアンスレポートの生成のトラブルシューティング

トピック

- 生成されたパッチコンプライアンスレポートには何が含まれていますか?
- 単一マネージドノードのパッチコンプライアンスレポートの生成
- すべてのマネージドノードのパッチコンプライアンスレポートの生成
- パッチコンプライアンスレポートの履歴の表示
- パッチコンプライアンスレポートのスケジュールの表示
- パッチコンプライアンスレポートの生成のトラブルシューティング

生成されたパッチコンプライアンスレポートには何が含まれていますか?

このトピックでは、指定された S3 バケットに生成およびダウンロードされるパッチコンプライアンスレポートに含まれるコンテンツの種類について説明します。

単一のマネージドノードのレポートの形式

単一のマネージドノードノードについて生成されるレポートには、概要情報と詳細情報の両方が含まれています。

[Download a sample report (single node)] (サンプルレポートをダウンロードする (単一ノード))

単一マネージドノードの概要情報には、次の情報が含まれます。

- [Index] (インデックス)
- インスタンス ID
- Instance name
- インスタンス IP
- プラットフォーム名
- プラットフォームバージョン
- SSM Agent バージョン
- パッチベースライン
- パッチグループ
- コンプライアンス状況
- コンプライアンスの重要度
- 非準拠のパッチ数 (重大)
- 非準拠のパッチ数 (高)
- 非準拠のパッチ数 (中)
- 非準拠のパッチ数 (低)
- 非準拠のパッチ数 (情報)
- 非準拠のパッチ数 (指定なし)

単一マネージドノードの詳細情報には、次の情報が含まれます。

- [Index] (インデックス)
- インスタンス ID

- Instance name
- パッチ名
- KB ID/パッチ ID
- パッチ状態
- 最終レポート時刻
- コンプライアンスレベル
- パッチの重大度
- パッチの分類
- CVE ID
- パッチベースライン
- ログ URL
- インスタンス IP
- プラットフォーム名
- プラットフォームバージョン
- SSM Agent バージョン

> **Note**
>
> カスタムのパッチベースラインを作成する場合、そのパッチベースラインによって承認されたパッチのコンプライアンスの重要度レベル (`Critical` または `High` など) を指定できます。承認された任意のパッチのパッチ状態が `Missing` と報告された場合、パッチベースラインで報告される全体的なコンプライアンスの重要度は、指定した重要度レベルになります。

すべてのマネージドノードのレポートの形式

すべてのマネージドノードについて生成されたレポートには、概要情報のみが含まれています。

[Download a sample report (all managed nodes)] (サンプルレポートをダウンロードする (すべてのマネージドノード))

すべてのマネージドノードの概要情報には、次の情報が含まれます。

- [Index] (インデックス)

- インスタンス ID
- Instance name
- インスタンス IP
- プラットフォーム名
- プラットフォームバージョン
- SSM Agent バージョン
- パッチベースライン
- パッチグループ
- コンプライアンス状況
- コンプライアンスの重要度
- 非準拠のパッチ数 (重大)
- 非準拠のパッチ数 (高)
- 非準拠のパッチ数 (中)
- 非準拠のパッチ数 (低)
- 非準拠のパッチ数 (情報)
- 非準拠のパッチ数 (指定なし)

単一マネージドノードのパッチコンプライアンスレポートの生成

AWS アカウント の単一マネージドノードのパッチ概要レポートを生成するには、以下の手順を実行します。単一マネージドノードのレポートには、コンプライアンス違反の各パッチの詳細 (パッチ名やIDなど) が表示されます。

単一マネージドノードのパッチコンプライアンスレポートを生成するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Patch Manager] を選択します。
3. [Compliance reporting] (コンプライアンスレポート) タブを選択します。
4. レポートを生成するマネージドノードの行のボタンを選択し、[View detail] (詳細の表示) を選択します。
5. [Patch summary] (パッチの概要) セクションで、[Export to S3] (S3 へのエクスポート) を選択します。

6. [Report name] (レポート名) で、後でレポートを識別しやすくするための名前を入力します。
7. [Reporting frequency] (レポートの頻度) で、次のいずれかを選択します。
   - オンデマンド – 1 回限りのレポートを作成します。ステップ 9 に進みます。
   - スケジュール – レポートを自動的に生成する定期的なスケジュールを指定します。ステップ 8 に進みます。
8. [Schedule type] (スケジュールタイプ) で、3 日ごとなどのレート式を指定するか、または cron 式を指定してレポートの頻度を設定します。

   cron 式の詳細については、「リファレンス: Systems Manager の Cron 式および rate 式」を参照してください。
9. [Bucket name] (バケット名) で、.csv レポートファイルを保存する S3 バケットの名前を選択します。

   > **Important**
   >
   > 2019 年 3 月 20 日以降に立ち上げられた AWS リージョン で作業している場合は、同じリージョンで S3 バケットを選択する必要があります。その日付以降に立ち上げられたリージョンは、デフォルトでは無効になっています。これらのリージョンの詳細およびリストについては、「Amazon Web Services 全般のリファレンス」の「リージョンの有効化」を参照してください。
10. (オプション) レポートの生成時に通知を送信するには、[SNS topic] (SNS トピック) セクションを消費して、[SNS topic Amazon Resource Name (ARN)] (SNS トピック Amazon リソースネーム (ARN)) から既存の Amazon SNS トピックを選択します。
11. [Submit] (送信) をクリックします。

生成されたレポートの履歴の表示については、「パッチコンプライアンスレポートの履歴の表示」を参照してください。

作成したレポートスケジュールの詳細を表示する方法については、「パッチコンプライアンスレポートのスケジュールの表示」を参照してください。

すべてのマネージドノードのパッチコンプライアンスレポートの生成

AWS アカウント のすべてのマネージドノードのパッチ概要レポートを生成するには、以下の手順を実行します。すべてのマネージドノードのレポートには、どのノードがコンプライアンス違反であるか、非準拠のパッチの数が表示されます。パッチの名前やその他の識別子は提供しません。これらの

追加の詳細情報を確認するには、単一のマネージドノードのパッチコンプライアンスレポートを生成できます。詳細については、このトピックの前半の「単一マネージドノードのパッチコンプライアンスレポートの生成」を参照してください。

すべてのマネージドノードのパッチコンプライアンスレポートを生成するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Patch Manager] を選択します。
3. [Compliance reporting] (コンプライアンスレポート) タブを選択します。
4. [Export to S3] (S3 へのエクスポート) を選択します。(最初にノード ID を選択しないでください。)
5. [Report name] (レポート名) で、後でレポートを識別しやすくするための名前を入力します。
6. [Reporting frequency] (レポートの頻度) で、次のいずれかを選択します。
   - オンデマンド – 1 回限りのレポートを作成します。ステップ 8 に進みます。
   - スケジュール – レポートを自動的に生成する定期的なスケジュールを指定します。ステップ 7 に進みます。
7. [Schedule type] (スケジュールタイプ) で、3 日ごとなどのレート式を指定するか、または cron 式を指定してレポートの頻度を設定します。

   cron 式の詳細については、「リファレンス: Systems Manager の Cron 式および rate 式」を参照してください。
8. [Bucket name] (バケット名) で、.csv レポートファイルを保存する S3 バケットの名前を選択します。

   > **Important**
   >
   > 2019 年 3 月 20 日以降に立ち上げられた AWS リージョン で作業している場合は、同じリージョンで S3 バケットを選択する必要があります。その日付以降に立ち上げられたリージョンは、デフォルトでは無効になっています。これらのリージョンの詳細およびリストについては、「Amazon Web Services 全般のリファレンス」の「リージョンの有効化」を参照してください。
9. (オプション) レポートの生成時に通知を送信するには、[SNS topic] (SNS トピック) セクションを消費して、[SNS topic Amazon Resource Name (ARN)] (SNS トピック Amazon リソースネーム (ARN)) から既存の Amazon SNS トピックを選択します。

10. [Submit] (送信) をクリックします。

生成されたレポートの履歴の表示については、「パッチコンプライアンスレポートの履歴の表示」を参照してください。

作成したレポートスケジュールの詳細を表示する方法については、「パッチコンプライアンスレポートのスケジュールの表示」を参照してください。

パッチコンプライアンスレポートの履歴の表示

このトピックの情報は、 で生成されたパッチコンプライアンスレポートの詳細を表示するのに役立ちますAWS アカウント

パッチコンプライアンスのレポート履歴を表示するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Patch Manager] を選択します。
3. [Compliance reporting] (コンプライアンスレポート) タブを選択します。
4. [View all S3 exports] (すべての S3 エクスポートを表示) を選択し、[Export history] (エクスポート履歴) タブを選択します。

パッチコンプライアンスレポートのスケジュールの表示

このトピックの情報は、 で作成されるパッチコンプライアンスレポートのスケジュールの詳細を表示するのに役立ちますAWS アカウント

パッチコンプライアンスのレポート履歴を表示するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Patch Manager] を選択します。
3. [Compliance reporting] (コンプライアンスレポート) タブを選択します。
4. [View all S3 exports] (すべての S3 エクスポートを表示) を選択し、[Scheduled report] (スケジュールされたレポート) タブを選択します。

パッチコンプライアンスレポートの生成のトラブルシューティング

以下の情報は、AWS Systems Manager のツールである Patch Manager でパッチコンプライアンスレポートを生成する際に発生する問題のトラブルシューティングに役立ちます。

トピック

- AWS-SystemsManager-PatchManagerExportRolePolicy ポリシーが壊れているというメッセージが表示される
- パッチコンプライアンスポリシーまたはロールを削除した後、スケジュールされたレポートが正常に生成されない

AWS-SystemsManager-PatchManagerExportRolePolicy ポリシーが壊れているというメッセージが表示される

問題: AWS-SystemsManager-PatchManagerExportRolePolicy が破損していることを示す、次のようなエラーメッセージが表示されます。

```
An error occurred while updating the AWS-SystemsManager-PatchManagerExportRolePolicy
policy. If you have edited the policy, you might need to delete the policy, and any
role that uses it, then try again. Systems Manager recreates the roles and policies
you have deleted.
```

- 解決策: 新しいパッチコンプライアンスレポートを生成する前に、Patch Manager コンソールまたは AWS CLI を使用して、影響を受けるロールとポリシーを削除します。

  コンソールを使用して破損したポリシーを削除するには

  1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
  2. 次のいずれかを行ってください。

     オンデマンドレポート – 1 回限りのオンデマンドレポートの生成中に問題が発生した場合は、左側のナビゲーションで [Policies] (ポリシー) を選択し、AWS-SystemsManager-PatchManagerExportRolePolicy を検索して、ポリシーを削除します。次に、[Roles] (ロール) を選択し、AWS-SystemsManager-PatchSummaryExportRole を検索して、ロールを削除します。

     スケジュールされたレポート – スケジュールに従ってレポートを生成しているときに問題が発生した場合は、左側のナビゲーションで [ポリシー] を選択し、AWS-EventBridge-Start-SSMAutomationRolePolicy と AWS-SystemsManager-

PatchManagerExportRolePolicy をそれぞれ検索して、各ポリシーを削除します。次に、[Roles] (ロール) を選択し、AWS-EventBridge-Start-SSMAutomationRole と AWS-SystemsManager-PatchSummaryExportRole をそれぞれ検索して、各ロールを削除します。

AWS CLI を使用して破損したポリシーを削除するには

placeholder values をアカウントID に置き換えます。

- 1 回限りのオンデマンドレポートの生成中に問題が発生した場合は、次のコマンドを実行します。

```
aws iam delete-policy --policy-arn arn:aws:iam::account-id:policy/AWS-SystemsManager-PatchManagerExportRolePolicy
```

```
aws iam delete-role --role-name AWS-SystemsManager-PatchSummaryExportRole
```

スケジュールに基づくレポートの生成中に問題が発生した場合は、次のコマンドを実行します。

```
aws iam delete-policy --policy-arn arn:aws:iam::account-id:policy/AWS-EventBridge-Start-SSMAutomationRolePolicy
```

```
aws iam delete-policy --policy-arn arn:aws:iam::account-id:policy/AWS-SystemsManager-PatchManagerExportRolePolicy
```

```
aws iam delete-role --role-name AWS-EventBridge-Start-SSMAutomationRole
```

```
aws iam delete-role --role-name AWS-SystemsManager-PatchSummaryExportRole
```

いずれかの手順を完了したら、次のステップに従って新しいパッチコンプライアンスレポートを生成またはスケジュールします。

パッチコンプライアンスポリシーまたはロールを削除した後、スケジュールされたレポートが正常に生成されない

問題: レポートを初めて生成する際、Systems Manager は、エクスポートプロセスに使用するサービスロールとポリシー (AWS-SystemsManager-PatchSummaryExportRole および AWS-SystemsManager-PatchManagerExportRolePolicy) を作成します。スケジュールに基づいてレポートを初めて生成する際、Systems Manager は、別のサービスロールとポリシー (AWS-EventBridge-Start-SSMAutomationRole および AWS-EventBridge-Start-SSMAutomationRolePolicy) を作成します。Amazon EventBridge では、ランブック -AWSExportPatchReportToS3 を使用してオートメーションを開始します。

これらのポリシーまたはロールのいずれかを削除すると、スケジュールと指定した S3 バケットと Amazon SNS トピックの間の接続が失われる可能性があります。

- 解決方法: この問題を回避するには、以前のスケジュールを削除し、問題が発生していたスケジュールの代わりとなる新しいスケジュールを作成することをお勧めします。

Patch Manager で非準拠のマネージドノードを修復するには

このセクションのトピックでは、パッチコンプライアンスに違反しているマネージドノードを識別する方法とノードをコンプライアンスに準拠させる方法の概要を説明します。

トピック

- 非準拠のマネージドノードの識別
- パッチコンプライアンス状態の値
- 非準拠マネージドノードへのパッチ適用

非準拠のマネージドノードの識別

コンプライアンス違反のマネージドノードは、2 つの AWS Systems Manager ドキュメント (SSM ドキュメント) のいずれかが実行されたときに識別されます。このような SSM ドキュメントは、AWS Systems Manager のツールである Patch Manager で各マネージドノードに対する適切なパッチベースラインを参照します。次に、マネージドノードのパッチ状態を評価すると、コンプライアンス結果を利用できるようになります。

非準拠のマネージドノードを識別または更新するために使用される 2 つの SSM ドキュメントは、AWS-RunPatchBaseline と AWS-RunPatchBaselineAssociation です。各ドキュメント

は異なるプロセスで使用され、そのコンプライアンス結果は異なるチャネルを通じて入手できます。次の表に、これらのドキュメントの違いについて説明します。

> **Note**
>
> Patch Manager からパッチコンプライアンスデータを AWS Security Hub に送信できます Security Hub では、高優先度のセキュリティアラートとコンプライアンス状況を包括的に確認できます。また、フリートのパッチ適用状況も監視できます。詳細については、「」を参照してくださいPatch Managerと AWS Security Hub の統合

	AWS-RunPatchBaseline	**AWS-RunPatchBaselineAssociation**
ドキュメントを使用するプロセス	オンデマンドでパッチ - [Patch now] (今すぐパッチ) オプションを使用して、オンデマンドでマネージドノードをスキャンするか、インスタンスにパッチを適用できます。詳細については、マネージドノードへのオンデマンド パッチ適用 を参照してください。 Systems Manager Quick Setup パッチポリシー – 組織全体、組織単位の一部、またはシングル AWS アカウントに対して、未適用のパッチがないかのスキャンと未適用のパッチのインストールを別々のスケジュールで実行できるパッチ適用設定を AWS Systems Manager のツールである Quick Setup で作成できます。詳細については、Quick Setup パッチポリシーを使用	Systems Manager Quick Setup ホスト管理 – Quick Setup でホスト管理設定オプションを有効にすると、マネージインスタンスを毎日スキャンしてパッチコンプライアンスを確認できます。詳細については、Quick Setup を使用して Amazon EC2 ホスト管理を設定する を参照してください。 Systems Manager Explorer – AWS Systems Manager のツールである Explorer を許可すると、マネージドインスタンスを定期的にスキャンしてパッチコンプライアンスと検出結果を Explorer ダッシュボードに表示できます。

	AWS-RunPatchBaseline	AWS-RunPatchBaselineAssociation
	して組織内のインスタンスのためにパッチ適用を設定する を参照してください。 コマンドを実行する – AWS Systems Manager のツールである Run Command 内のオペレーションで AWS-RunPatchBaseline を手動で実行できます。詳細については、コンソールからコマンドを実行する を参照してください。 メンテナンスウィンドウ – Run Command タスクタイプの SSM ドキュメント AWS-RunPatchBaseline を使用するメンテナンスウィンドウを作成できます。詳細については、チュートリアル: コンソールを使用してパッチ用メンテナンスウィンドウを作成する を参照してください。	
パッチスキャン結果データの形式	AWS-RunPatchBaseline の実行後、Patch Manager は AWS:PatchSummary オブジェクトを AWS Systems Manager のツールである Inventory に送信します。	AWS-RunPatchBaselineAssociation の実行後、Patch Manager は AWS:ComplianceItem オブジェクトをSystems Manager Inventory に送信します。

	AWS-RunPatchBaseline	AWS-RunPatchBaselineAssociation
コンソールでのパッチコンプライアンスレポートの表示	Systems Manager Configuration Compliance および AWS-RunPatchBaseline で マネージドノードの使用 を使用するプロセスのパッチコンプライアンス情報を表示できます。詳細については、「パッチコンプライアンス結果の表示」を参照してください。	Quick Setup を使用してマネージドインスタンスをスキャンしてパッチコンプライアンスを確認する場合、[Systems Manager Fleet Manager] でコンプライアンスレポートを確認できます。Fleet Manager コンソールで、マネージドノードのノード ID を選択します。[全般] メニューで、[設定コンプライアンス] を選択します。 Explorer を使用してマネージドインスタンスをスキャンしてパッチコンプライアンスを確認する場合、Explorer と「Systems Manager OpsCenter」の両方でコンプライアンスレポートを表示できます。
AWS CLIパッチコンプライアンス結果を表示するための コマンド	AWS-RunPatchBaseline を使用するプロセスの場合、次の AWS CLI コマンドを使用して、マネージドノードのパッチに関する概要情報を表示できます。 • describe-instance-patch-states • describe-instance-patch-states-for-patch-group • describe-patch-group-state	AWS-RunPatchBaselineAssociation を使用するプロセスの場合、次の AWS CLI コマンドを使用して、インスタンスのパッチに関する概要情報を表示できます。 • list-compliance-items

	AWS-RunPatchBaseline	AWS-RunPatchBaselineAssociation
パッチ適用オペレーション	AWS-RunPatchBaseline を使用するプロセスの場合、オペレーションで Scan オペレーションのみを実行するか、Scan and install オペレーションを実行するかを指定します。 非準拠のマネージドノードを識別し、それらを修正しないことを目標とする場合は、Scan オペレーションのみを実行します。	AWS-RunPatchBaselineAssociation を使用する Quick Setup および Explorer プロセスの場合は、Scan オペレーションのみを実行します。
詳細情報	パッチ適用のための SSM コマンドドキュメント: AWS-RunPatchBaseline	パッチ適用のための SSM コマンドドキュメント: AWS-RunPatchBaselineAssociation

レポートされる可能性のあるさまざまなパッチコンプライアンス状態については、「パッチコンプライアンス状態の値」を参照してください。

パッチコンプライアンスに違反しているマネージドノードの修正については、「非準拠マネージドノードへのパッチ適用」を参照してください。

パッチコンプライアンス状態の値

マネージドノードのパッチに関する情報には、個々のパッチの状態、つまり、状況のレポートが含まれます。

> **Tip**
>
> マネージドノードに特定のパッチコンプライアンス状態を割り当てるには、put-compliance-items AWS Command Line Interface (AWS CLI) コマンドまたは PutComplianceItems API オ

ペレーションを使用できます。コンプライアンス状態の割り当てはコンソールではサポートされていません。

以下の表の情報を使用して、マネージドノードがパッチコンプライアンスに違反している理由を特定します。

Debian Server、Raspberry Pi OS、および Ubuntu Server のパッチコンプライアンスの値

次の表に、Debian Server、Raspberry Pi OS、および Ubuntu Server でパッケージをコンプライアンスの状態別に分類するルールを示します。

> **Note**
>
> INSTALLED、INSTALLED_OTHER、MISSING の状態の値を評価する際は次の点に注意してください: パッチベースラインの作成または更新時に[セキュリティ以外の更新を含める]チェックボックスをオンにしていないと、パッチの候補となるバージョンは、trusty-security (Ubuntu Server 14.04 LTS)、xenial-security (Ubuntu Server 16.04 LTS)、bionic-security (Ubuntu Server 18.04 LTS)、focal-security (Ubuntu Server 20.04 LTS)、groovy-security (Ubuntu Server 20.10 STR)、jammy-security (Ubuntu Server 22.04 LTS)、debian-security (Debian Server および Raspberry Pi OS) のいずれかに含まれているパッチに限定されます。[セキュリティ以外の更新を含める] チェックボックスをオンにした場合は、他のリポジトリからのパッチも考慮されます。

パッチ状態	説明	コンプライアンス状況
INSTALLED	パッチはパッチベースラインにリストされ、マネージドノードにインストールされます。マネージドノードで AWS-RunPatchBaseline ドキュメントを実行している場合は、既に手動で個別にインストールされていたり、Patch Manager で自動的にインスト	準拠

パッチ状態	説明	コンプライアンス状況
	ールされていたりすることがあります。	
INSTALLED_OTHER	パッチがベースラインに含まれていない、またはベースラインによって承認されていませんが、マネージドノードにインストールされています。パッチが手動でインストールされているか、パッケージが別の承認済みパッチの必要な依存関係であるか、パッチが InstallOverrideList オペレーションに含まれている可能性があります。[拒否されたパッチ] アクションとして Block を指定しない場合は、インストール済みでも拒否されたパッチも INSTALLED_OTHER パッチに含まれます。	準拠

パッチ状態	説明	コンプライアンス状況
INSTALLED_PENDING_REBOOT	INSTALLED_PENDING_REBOOT は次の 2 つのいずれかを意味します。 • Patch Manager の Install オペレーションによってパッチがマネージドノードに適用されていますが、パッチの適用後にノードが再起動されていません。通常、これは NoReboot ドキュメントが最後にマネージドノードで実行されたときに、RebootOption パラメータに AWS-RunPatchBaseline オプションが選択されていたことを意味します。 詳細については、「パラメータ名: RebootOption 」を参照してください。 • マネージドノードを最後に再起動したとき以降に、Patch Manager 以外でパッチがインストールされました。 いずれの場合も、このステータスのパッチで再起動が必要という意味ではなく、パッチがインストールされて以降	非準拠

パッチ状態	説明	コンプライアンス状況
	ノードが再起動されていないことを意味します。	
INSTALLED_REJECTED	パッチはマネージドノードにインストールされますが、[Rejected patches] (拒否されたパッチ) リストに指定されています。これは通常、パッチが、拒否されたパッチのリストに追加される前にインストールされたことを意味します。	非準拠
MISSING	ベースラインでフィルターされ、まだインストールされていないパッケージ。	非準拠
FAILED	パッチオペレーション中にインストールに失敗したパッケージ。	非準拠

その他のオペレーティングシステムのパッチコンプライアンスの値

次の表に、Debian Server、Raspberry Pi OS、および Ubuntu Server 以外のすべてのオペレーティングシステムでパッケージをコンプライアンスの状態別に分類するルールを示します。

パッチ状態	説明	コンプライアンスの値
INSTALLED	パッチはパッチベースラインにリストされ、マネージドノードにインストールされます。ノードで `AWS-RunPatchBaseline` ドキュメントを実行している場合は、既に手動で個別にインストールされていたり、Patch	準拠

パッチ状態	説明	コンプライアンスの値
	Manager で自動的にインストールされていたりすることがあります。	

パッチ状態	説明	コンプライアンスの値
INSTALLED_OTHER 1	パッチはベースラインに含まれていませんが、マネージドノードにインストールされています。これには、次の 2 つの理由が考えられます。 1. パッチが手動でインストールされた可能性がある。 2. Linux のみ: パッケージが、異なる承認済みパッチの必須依存関係としてインストールされた可能性がある。[拒否されたパッチ] アクションとして `Allow as dependency` を指定する場合、依存関係としてインストールされたパッチにはレポートステータス `INSTALLED_OTHER` が与えられます。 **Note** Windows Server は、パッチ依存関係の概念をサポートしません。Windows Server の [拒否されたパッチ] リストにあるパッチを Patch Manager が処理する方法については、「カスタムパッチベースラインでの拒否されたパッチリス	準拠

パッチ状態	説明	コンプライアンスの値
	トのオプション」を参照してください。	
INSTALLED_REJECTED	パッチはマネージドノードにインストールされますが、[Rejected patches] (拒否されたパッチ) リストに指定されています。これは通常、パッチが、拒否されたパッチのリストに追加される前にインストールされたことを意味します。	非準拠

パッチ状態	説明	コンプライアンスの値
INSTALLED_PENDING_REBOOT	INSTALLED_PENDING_REBOOT は次の 2 つのいずれかを意味します。 • Patch Manager の Install オペレーションによってパッチがマネージドノードに適用されていますが、パッチの適用後にノードが再起動されていません。通常、これは NoReboot ドキュメントが最後にマネージドノードで実行されたときに、RebootOption パラメータに AWS-RunPatchBaseline オプションが選択されていたことを意味します。 詳細については、「パラメータ名: RebootOption 」を参照してください。 • マネージドノードを最後に再起動したとき以降に、Patch Manager 以外でパッチがインストールされました。 いずれの場合も、このステータスのパッチで再起動が必要という意味ではなく、パッチがインストールされて以降	非準拠

パッチ状態	説明	コンプライアンスの値
	ノードが再起動されていないことを意味します。	
MISSING	このパッチはベースラインで承認されていますが、マネージドノードにインストールされていません。AWS-RunPatchBaseline ドキュメントタスクでスキャン (インストールではなく) するように設定した場合、スキャンで見つかってもインストールされていないパッチがあると、このステータスがレポートされます。	非準拠
FAILED	パッチはベースラインで承認されていますが、インストールできませんでした。この状態のトラブルシューティングを行うには、コマンド出力で問題の理解に役立つ情報を確認します。	非準拠

パッチ状態	説明	コンプライアンスの値
NOT_APPLICABLE 1	このコンプライアンス状態は、Windows Server オペレーティングシステムでのみレポートされます。 パッチはベースラインで承認されていますが、このパッチを使用するサービスまたは機能がマネージドノードにインストールされていません。例えば、Internet Information Services (IIS) などのウェブ サーバーサービスのパッチは、ベースラインで承認されていてもウェブサービスがマネージドノードにインストールされていなければ、NOT_APPLICABLE と表示されます。パッチは、後続の更新によって置き換えられた場合に、NOT_APPLICABLE マークを付けることもできます。これは、新しい更新プログラムがインストールされ、 NOT_APPLICABLE 更新プログラムが不要になったことを意味します。	該当しない

パッチ状態	説明	コンプライアンスの値
AVAILABLE_SECURITY_UPDATES	このコンプライアンス状態は、Windows Server オペレーティングシステムでのみレポートされます。 パッチベースラインで承認されていない使用可能なセキュリティ更新パッチは、カスタムパッチベースラインでの定義に従い、コンプライアンス値 (`Compliant` または `Non-Compliant`) を持つことができます。 パッチベースラインを作成または更新するときに、パッチベースラインで指定されたインストール基準を満たしていないため、使用可能ではあるものの承認されていないセキュリティパッチに割り当てるステータスを選択します。例えば、パッチがリリースされてからインストールされるまでに待機する期間を長く指定している場合は、インストールするセキュリティパッチをスキップできます。指定した待機期間中にパッチの更新がリリースされると、パッチのインストールの待機期間がもう一度開始されます。待機期間が長すぎる場合、複数のバージョンのパッチがリ	使用可能なセキュリティ更新用に選択されたオプションに応じて、準拠または非準拠。 **Note** コンソールを使用してパッチベースラインを作成または更新するには、[使用可能なセキュリティ更新のコンプライアンスステータス] フィールドでこのオプションを指定します。AWS CLI を使用して create-patch-baseline または update-patch-baseline コマンドを実行し、`available-security-updates-compliance-status` パラメータでこのオプションを指定します。

パッチ状態	説明	コンプライアンスの値
	リースされ、インストールされない可能性があります。 パッチの概数では、パッチが AvailableSecurityUpdate としてレポートされる場合は、常に AvailableSecurityUpdateCount に含まれます。これらのパッチを NonCompliant としてレポートするようにベースラインが設定されている場合は、SecurityNonCompliantCount にも含まれます。これらのパッチを Compliant としてレポートするようにベースラインが設定されている場合は、SecurityNonCompliantCount には含まれません。これらのパッチは常に重要度が指定されていない状態でレポートされ、CriticalNonCompliantCount に含まれることはありません。	

[1] 状態が INSTALLED_OTHER および NOT_APPLICABLE のパッチの場合、Patch Manager は describe-instance-patches コマンドに基づいて、クエリ結果から一部のデータを省略します (Classification や Severity の値など)。これにより、AWS Systems Manager のツールである Inventory において、個々のノードのデータ制限を超えないようにすることができます。すべてのパッチの詳細を表示するには、describe-available-patches コマンドを使用します。

非準拠マネージドノードへのパッチ適用

パッチコンプライアンスについてマネージドノードをチェックするために使用できる AWS Systems Manager ツールおよびプロセスの多くは、現在適用されているパッチルールにノードを準拠させるために使用できます。マネージドノードをパッチコンプライアンスにするには、AWS Systems Manager のツールである Patch Manager で `Scan and install` オペレーションを実行する必要があります。(非準拠マネージドノードを識別し、それらを修正しないことを目標とする場合は、代わりに `Scan` オペレーションを実行します。詳細については、「非準拠のマネージドノードの識別」を参照してください。)

Systems Manager を使用してパッチをインストールする

`Scan and install` オペレーションを実行するには、いくつかのツールから選択できます。

- (推奨) Systems Manager のツールである Quick Setup でパッチポリシーを設定すると、組織全体、組織単位の一部、またはシングル AWS アカウントに対して、未適用のパッチをスケジュールに従ってインストールできます。詳細については、「Quick Setup パッチポリシーを使用して組織内のインスタンスのためにパッチ適用を設定する」を参照してください。
- Run Command タスクタイプで、Systems Manager ドキュメント (SSM ドキュメント) `AWS-RunPatchBaseline` を使用するメンテナンスウィンドウを作成します。詳細については、チュートリアル: コンソールを使用してパッチ用メンテナンスウィンドウを作成する を参照してください。
- Run Command オペレーションで `AWS-RunPatchBaseline` を手動で実行します。詳細については、コンソールからコマンドを実行する を参照してください。

- [Patch now (今すぐパッチ)] オプションを使用して、オンデマンドでパッチをインストールします。詳細については、マネージドノードへのオンデマンド パッチ適用 を参照してください。

パッチコンプライアンスデータに対する意図しない上書きの回避

インスタンスに対するパッチコンプライアンスのスキャン処理に複数の種類が存在する場合、スキャンからのパッチコンプライアンスデータは、次のスキャンが行われるたびに上書きされます。その結果、パッチコンプライアンスデータで想定外の結果を得ることがあります。

例えば、現地時間の午前 2 時に毎日、パッチコンプライアンスをスキャンするパッチポリシーを作成したとします。このパッチポリシーでは、重大度が `Critical`、`Important`、および `Moderate` としてマークされたパッチを対象とする、パッチベースラインを使用しています。このパッチベースラインでは、特に拒否されたパッチもいくつか指定されています。

また、毎日、現地時間の午前 4 時に同じマネージドノードのセットをスキャンするメンテナンスウィンドウがすでに設定されていて、それを削除したり無効化したりすることはないとします。このメンテナンスウィンドウのタスクでは、重大度が `Critical` のパッチのみを対象とする別のパッチベースラインを使用しており、また、特定のパッチを除外することはありません。

この 2 回目のスキャンがメンテナンスウィンドウで実行されると、1 回目のスキャンによるパッチコンプライアンスデータは削除され、この 2 回目のスキャンのパッチコンプライアンスデータにより置き換えられます。

そのため、パッチ適用処理においてスキャンとインストールを自動化する場合には、単一の方法のみを使用するように強くお勧めします。パッチポリシーを設定するには、パッチコンプライアンスの他のスキャン方法を削除または無効化する必要があります。詳細については、以下の各トピックを参照してください。

- パッチ適用オペレーションタスクを、メンテナンスウィンドウから削除するには – コンソールを使用してメンテナンスウィンドウタスクを更新または登録解除する
- State Manager の関連付けを削除するには – 関連付けを削除する

ホスト管理設定で毎日のパッチコンプライアンススキャンを無効にするには、Quick Setup で次の操作を行います。

1. ナビゲーションペインで、Quick Setup を選択します。
2. 更新するホスト管理設定を選択します。
3. [Actions, Edit configuration] (アクション、設定の編集) を選択します。
4. [Scan instances for missing patches daily] (不足しているパッチがないか毎日インスタンスをスキャンする) のチェックボックスをオフにします。
5. [Update] (更新) を選択します。

> **Note**
>
> [Patch now] (今すぐパッチ適用) オプションを使用して、マネージドノードのコンプライアンスをスキャンすると、同時にパッチコンプライアンスデータも上書きされます。

マネージドノードへのオンデマンド パッチ適用

AWS Systems Manager のツールである Patch Manager の [今すぐパッチ適用] オプションを使用すると、Systems Manager コンソールからオンデマンドでパッチ適用オペレーションを実行できます。つまり、マネージドノードのコンプライアンス状況を更新したり、準拠していないノードにパッチをインストールしたりするために、スケジュールを作成する必要はありません。また、スケジュールされたパッチ適用ウィンドウを設定または変更するために、Systems Manager コンソールを Patch Manager と、AWS Systems Manager のツールである Maintenance Windows との間で切り替える必要もありません。

[Patch now] (今すぐパッチを適用) は、ゼロデイアップデートを適用したり、マネージドノードに他の重要なパッチをできるだけ早くインストールしたりする必要がある場合に特に便利です。

> **Note**
>
> オンデマンドのパッチ適用では、一度に 1 組の AWS アカウント と AWS リージョン のペアのみサポートされます。パッチポリシーに基づくパッチ適用オペレーションには使用できません。すべてのマネージドノードをコンプライアンス状態にしておくために、パッチポリシーを使用することをお勧めします。パッチポリシーの使用の詳細については、「Quick Setup でのパッチポリシー設定」を参照してください。

トピック

- 「Patch now (今すぐパッチ)」の仕組み
- [今すぐパッチ適用] の実行

「Patch now (今すぐパッチ)」の仕組み

[Patch now (今すぐパッチ)] を実行するには、次の 2 つの必須設定のみを指定します。

- 欠落しているパッチのみをスキャンするか、パッチをスキャンして、かつ、マネージドノードにインストールするか
- どのマネージドノードでオペレーションを実行するか

[今すぐパッチ] オペレーションを実行すると、他のパッチオペレーションで選択するのと同じ方法で使用するパッチベースラインを決定します。マネージドノードがパッチグループに関連付けられている場合は、そのグループに指定されたパッチベースラインが使用されます。マネージドノードがパッ

チグループに関連付けられていない場合、この操作では、マネージドノードのオペレーティングシステムタイプのデフォルトとして現在設定されているパッチベースラインが使用されます。定義済みのベースラインでも、デフォルトとして設定したカスタムベースラインでもかまいません。パッチベースライン選択の詳細については、「パッチグループ」を参照してください。

[Patch now] (今すぐパッチ) で指定できるオプションには、パッチ適用後にマネージドノードを再起動するタイミングまたは再起動するかどうかの選択、パッチ適用オペレーションのログデータを保存する Amazon Simple Storage Service (Amazon S3) バケットの指定、パッチ適用中のライフサイクルフックとしての Systems Manager ドキュメント (SSM ドキュメント) の実行などがあります。

[Patch now (今すぐパッチ適用)] の同時実行とエラーしきい値

[Patch now (今すぐパッチ適用)] オペレーションでは、Patch Manager が同時実行とエラーしきい値のオプションに対応します。一度にパッチを適用するマネージドノードの数を指定する必要も、操作が失敗するまでに許可するエラーの数を指定する必要もありません。Patch Manager は、オンデマンドでパッチを適用するときに、次の表に示す同時実行数とエラーのしきい値の設定を適用します。

> **Important**
>
> 次のしきい値は、`Scan and install` オペレーションのみに適用されます。Scan オペレーションの場合、Patch Manager は最大 1,000 個のノードのスキャンを同時に試みます。また、最大 1,000 個のエラーが発生するまでスキャンを続行します。

同時実行: インストールオペレーション

[Patch now] (今すぐパッチ適用) オペレーションでのマネージドノードの合計数	一度にスキャンされる、またはパッチが適用されるマネージドノードの数
25 未満	1
25 ~ 100	5%
101 ~ 1,000	8%
1000 超	10%

エラーしきい値: インストールオペレーション

[Patch now] (今すぐパッチ適用) オペレーションでのマネージドノードの合計数	操作が失敗する前に許可されるエラーの数
25 未満	1
25 ~ 100	5
101 ~ 1,000	10
1000 超	10

[今すぐパッチ適用] ライフサイクルフックの使用

[Patch now (今すぐパッチ適用)] では、`Install` パッチ適用オペレーション中、ライフサイクルフックとして SSM コマンドドキュメントを実行できます。これらのフックは、パッチの適用前にアプリケーションをシャットダウンしたり、パッチ適用後または再起動後にアプリケーションに対してヘルスチェックを実行したりするといったタスクに使用できます。

ライフサイクルフック使用の詳細については、「パッチ適用のための SSM コマンドドキュメント: AWS-RunPatchBaselineWithHooks」を参照してください。

次の表には、3 つの [今すぐパッチ適用] 再起動オプションのそれぞれで利用できるライフサイクルフックと、各フックの使用例が含まれています。

ライフサイクルフックと使用例

再起動オプション	フック: インストール前	フック: インストール後	フック: 終了時	フック：スケジュールされた再起動後
必要に応じて再起動	パッチ適用を開始する前に SSM ドキュメントを実行します。 使用例：パッチ適用プロセスの開始前に、アプ	パッチ適用の終了時およびマネージドノードの再起動前に SSM ドキュメントを実行します。	パッチ適用オペレーションを完了し、インスタンスが再起動されてから SSM ドキュメントを実行します。	利用不可

再起動オプション	フック: インストール前	フック: インストール後	フック: 終了時	フック：スケジュールされた再起動後
	リケーションを安全にシャットダウンします。	使用例: 再起動前にサードパーティーのアプリケーションのインストールなどの操作を実行します。	使用例: パッチ適用後、アプリケーションが期待どおりに動作していることを確認します。	
インスタンスを再起動しない	上記と同じ。	パッチ適用操作の終了時に SSM ドキュメントを実行します。 使用例: パッチ適用後、アプリケーションが期待どおりに動作していることを確認します。	利用不可	利用不可
再起動時間をスケジュールする	上記と同じ。	インスタンスを再起動しないと同じ。	利用不可	スケジュールされていた再起動が完了した直後に SSM ドキュメントを実行します。 使用例：再起動後にアプリケーションが期待どおりに動作していることを確認します。

[今すぐパッチ適用] の実行

以下の手順に従って、オンデマンドでマネージドノードにパッチを適用します。

「Patch now (今すぐパッチ)」を実行するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Patch Manager] を選択します。
3. [Patch now (今すぐパッチ)] を選択します。
4. [パッチ適用操作] で、次のいずれかを選択します。
   - [Scan] (スキャン): Patch Manager は、マネージドノードに不足しているパッチを検出しますが、インストールしません。結果は、[コンプライアンス] ダッシュボード、またはパッチコンプライアンスの表示に使用するその他のツールで表示できます。
   - [Scan and install] (スキャンとインストール): Patch Manager は、マネージドノードに不足しているパッチを検出してインストールします。
5. この手順は、前の手順で [Scan and install] (スキャンとインストール) を選択した場合にのみ使用します。[Reboot option] (再起動オプション) で 、次のいずれかを選択します。
   - [Reboot if needed] (必要に応じて再起動): インストール後、Patch Manager は、パッチのインストールを完了するために必要な場合にのみマネージドノードを再起動します。
   - [Don't reboot my instances] (インスタンスを再起動しない): インストール後、Patch Manager はマネージドノードを再起動しません。Patch Manager 外での再起動を選択または管理するときに、ノードを手動で再起動できます。
   - [Schedule a reboot time] (再起動時刻をスケジュール): Patch Manager でマネージドノードを再起動する日付、時刻、および UTC タイムゾーンを指定します。[Patch now (今すぐパッチ適用)] 操作の実行後、スケジュールされていた再起動は「`AWS-PatchRebootAssociation`」という名前で関連付けとして State Manager にリストされます。
6. [Instances to patch (パッチを適用するインスタンス)] で、次のいずれかを選択します。
   - [Patch all instances] (すべてのインスタンスにパッチを適用): Patch Manager は、現在の AWS リージョン の AWS アカウント ですべてのマネージドノードに対して、指定したオペレーションを実行します。
   - [Patch only the target instances I specify]: (指定したターゲットインスタンスのみにパッチを適用) 次のステップで対象にするマネージドノードを指定します。

7. このステップは、前のステップで [Patch only the target instances I specify] (指定したターゲットインスタンスのみにパッチを適用) を選択した場合にのみ使用します。[Target selection] (ターゲットの選択) セクションで、タグの指定、ノードの手動選択、またはリソースグループの指定により、このオペレーションを実行するノードを特定します。

   > **Note**
   >
   > 表示されるはずのマネージドノードが表示されない場合は、トラブルシューティングのヒントについて「マネージドノードの可用性のトラブルシューティング」を参照してください。
   > リソースグループを対象にすることを選択した場合、AWS CloudFormation スタックに基づいたリソースグループにデフォルトの `aws:cloudformation:stack-id` タグでタグ付けする必要があることに注意してください。これが削除されている場合、Patch Manager はリソースグループに属するマネージドノードを特定できないことがあります。

8. (オプション) [Patching log storage] (ログストレージのパッチ適用) で、このパッチ適用オペレーションからログを作成して保存する場合は、ログを保存する S3 バケットを選択します。

   > **Note**
   >
   > S3 バケットにデータを書き込む機能を許可する S3 許可は、このタスクを実行する IAM ユーザーのものではなく、インスタンスに割り当てられたインスタンスプロファイル (EC2 インスタンスの場合) または IAM サービスロール (ハイブリッドアクティベーションマシン) のものです。詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」または「ハイブリッドおよびマルチクラウド環境で Systems Manager に必要な IAM サービスロールを作成する」を参照してください。さらに、指定された S3 バケットが別の AWS アカウント にある場合は、マネージドノードに関連付けられたインスタンスプロファイルまたは IAM サービスロールが、そのバケットへの書き込みに必要なアクセス許可があることを確認してください。

9. (オプション) パッチ適用オペレーションの特定の時点で SSM ドキュメントをライフサイクルフックとして実行する場合は、次の手順を実行します。

   - [Use lifecycle hooks] (ライフサイクルフックを使用) を選択します。
   - 使用可能なフックごとに、オペレーションの指定した時点で実行する SSM ドキュメントを選択します。

- インストール前
- インストール後
- 終了時
- スケジュールされた再起動後

> **Note**
>
> デフォルトのドキュメント AWS-Noop では、オペレーションは実行されません。

10. [Patch now (今すぐパッチ)] を選択します。

    [Association execution summary (関連付け実行の概要)] ページが開きます。([今すぐパッチ適用] では、AWS Systems Manager のツールである State Manager の関連付けをオペレーションに使用します)。[Operation summary] (オペレーションの概要) では、指定したマネージドノードのスキャンまたはパッチ適用の状況をモニタリングできます。

パッチベースラインの操作

AWS Systems Manager のツールである Patch Manager のパッチベースラインは、マネージドノードでインストールを承認するパッチを定義します。パッチの承認または拒否は個別に指定できます。また、自動承認ルールを作成して特定のタイプの更新 (例: 重要な更新) を自動承認するよう指定できます。拒否済みリストは、これらのルールと承認リストの両方に優先します。承認済みパッチのリストを使用して特定のパッケージをインストールするには、最初にすべての自動承認ルールを削除します。パッチを明示的に拒否済みとして特定すると、そのパッチは自動承認ルールのすべての基準を満たしていても承認またはインストールされません。また、パッチがマネージドノードに対して承認されていても、パッチがマネージドノードにインストールされるのは、それがノードのソフトウェアに適用される場合に限ります。

トピック

- AWS の定義済みパッチベースラインの表示
- カスタムパッチベースラインの操作
- 既存のパッチベースラインをデフォルトとして設定する

詳細情報

- パッチベースライン

AWS の定義済みパッチベースラインの表示

AWS Systems Manager のツールである Patch Manager には、Patch Manager でサポートされるオペレーティングシステムごとに事前定義されたパッチベースラインが含まれています。これらのパッチベースライン (カスタマイズはできません) を使用するか、独自のパッチベースラインを作成できます。次の手順では、事前定義されたパッチベースラインを表示してニーズに合っているかどうかを確認する方法について説明します。パッチベースラインの詳細については、「事前定義されたパッチベースラインおよびカスタムパッチベースライン」を参照してください。

AWS の定義済みのパッチベースラインを表示するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Patch Manager] を選択します。
3. パッチベースラインのリストで、事前定義されたパッチベースラインのいずれかのベースライン ID を選択します。

   -または-

   現在の AWS リージョン で Patch Manager に初めてアクセスしている場合は、[概要から開始] で [パッチベースライン] を選択してから、事前定義されたパッチベースラインのいずれかのベースライン ID を選択します。

> **Note**
>
> Windows Server では、3 つの事前に定義されたパッチベースラインが提供されます。パッチベースラインの `AWS-DefaultPatchBaseline` と `AWS-WindowsPredefinedPatchBaseline-OS` は、Windows オペレーティングシステム自体のオペレーティングシステム更新プログラムのみをサポートしています。`AWS-DefaultPatchBaseline` は、別のパッチベースラインを指定しない限り、Windows Server マネージドノードのデフォルトのパッチベースラインとして使用されます。これら 2 つのパッチベースラインの構成設定は同じです。2 つのうち新しい方である `AWS-WindowsPredefinedPatchBaseline-OS` は、Windows Server 用の 3 つ目の事前定義されたパッチベースラインと区別するために作成されました。そのパッチベースライン `AWS-WindowsPredefinedPatchBaseline-OS-Applications` を使用して、Windows Server オペレーティングシステムおよびサポートされている Microsoft アプリケーションの両方にパッチを適用できます。

詳細については、「既存のパッチベースラインをデフォルトとして設定する」を参照してください。

4. [承認ルール] セクションで、パッチベースラインの設定を確認します。
5. 設定がマネージドノードで許容されている場合は、省略して パッチグループの作成と管理 の手順に進むことができます。

   -または-

   独自のデフォルトパッチベースラインを作成するには、トピック カスタムパッチベースラインの操作 に進みます。

カスタムパッチベースラインの操作

AWS Systems Manager のツールである Patch Manager には、Patch Manager でサポートされるオペレーティングシステムごとに事前定義されたパッチベースラインが含まれています。これらのパッチベースライン (カスタマイズはできません) を使用するか、独自のパッチベースラインを作成できます。

次の手順では、独自のカスタムパッチベースラインを作成、更新、および削除する方法について説明します。パッチベースラインの詳細については、「事前定義されたパッチベースラインおよびカスタムパッチベースライン」を参照してください。

トピック

- Linux 用 カスタムパッチベースラインの作成
- macOS のカスタムパッチベースラインを作成する
- Windows Server のカスタムパッチベースラインを作成する
- カスタムパッチベースラインの更新または削除

Linux 用 カスタムパッチベースラインの作成

AWS Systems Manager のツールである Patch Manager で Linux マネージドノードのカスタムパッチベースラインを作成するには、以下の手順に従います。

macOS マネージドノードのパッチベースラインの作成については、「macOS のカスタムパッチベースラインを作成する」を参照してください。Windows マネージドノードのパッチベースラインの作成については、「Windows Server のカスタムパッチベースラインを作成する」を参照してください。

Linux マネージドノードのカスタム パッチベースラインを作成するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Patch Manager] を選択します。
3. [パッチベースライン] タブを選択し、[パッチベースラインの作成] を選択します。

   -または-

   現在の AWS リージョン で Patch Manager に初めてアクセスしている場合は、[概要から開始] で [パッチベースライン] タブを選択してから、[パッチベースラインの作成] を選択します。
4. [Name (名前)] フィールドに、新しいパッチベースラインの名前 (例: `MyRHELPatchBaseline`) を入力します。
5. (オプション) [Description (説明)] に、パッチベースラインの説明を入力します。
6. [Operating system (オペレーティングシステム)] リストでオペレーティングシステム (`Red Hat Enterprise Linux` など) を選択します。
7. このパッチベースラインを作成してすぐに、選択したオペレーティングシステムのデフォルトとして使用する場合は、[Set this patch baseline as the default patch baseline for ***operating system name*** instances (このパッチベースラインをオペレーティングシステム名インスタンスのデフォルトのパッチベースラインにする)] の横にあるボックスをオンにします。

   > **Note**
   >
   > このオプションは、2022 年 12 月 22 日のパッチポリシーリリース前に初めて Patch Manager にアクセスした場合にのみ使用できます。
   > 既存のパッチベースラインのデフォルト設定の詳細については、「既存のパッチベースラインをデフォルトとして設定する」を参照してください。
8. [Approval rules for operating-systems (オペレーティングシステムの承認ルール)] セクションで、フィールドを使用して 1 つ以上の自動承認ルールを作成します。

   - [製品]: 承認ルールが適用されるオペレーティングシステムのバージョン (`RedhatEnterpriseLinux7.4` など)。デフォルトの選択は `All` です。
   - [Classification (分類)]: 承認ルールが適用されるパッチのタイプ (`Security` または `Enhancement` など)。デフォルトの選択は `All` です。

> **Tip**
>
> パッチベースラインを設定して、RHEL 7.8 などの Linux 用のマイナーバージョンアップグレードをインストールするかどうかを制御できます。マイナーバージョンのアップグレードは、更新プログラムが適切なリポジトリにある場合は、Patch Managerで自動的にインストールできます。
> Linux オペレーティングシステムの場合、マイナーバージョンのアップグレードは分類が一貫していません。同じカーネルバージョン内であっても、バグ修正やセキュリティアップデートとして分類されることも、分類されないこともあります。パッチベースラインによってインストールされるかどうかを制御するためのいくつかのオプションを以下に示します。
>
> - オプション 1: マイナーバージョンのアップグレードが可能な場合に確実にインストールされるための最も広範な承認ルールは、[分類] を `All` (*) と指定し、[Include nonsecurity updates (セキュリティ以外の更新を含める)] オプションを選択することです。
> - オプション 2: オペレーティングシステムバージョンのパッチを確実にインストールするには、ワイルドカード (*) を使用して、ベースラインの [Patch exceptions (パッチの例外)] セクションでそのカーネル形式を指定できます。例えば、RHEL 7.* のカーネル形式は `kernel-3.10.0-*.el7.x86_64` です。
>
>   パッチベースラインの [Approved patches] (承認済みパッチ) リストに `kernel-3.10.0-*.el7.x86_64` と入力して、マイナーバージョンアップグレードを含むすべてのパッチが RHEL 7.* マネージドノードに適用されるようにします。(マイナーバージョンパッチの正確なパッケージ名がわかっている場合は、代わりにそれを入力できます)。
> - オプション 3: `AWS-RunPatchBaseline` ドキュメントの InstallOverrideList パラメータを使用すると、マイナーバージョンのアップグレードなど、マネージドノードに適用するパッチを最大限に制御できます。詳細については、「パッチ適用のための SSM コマンドドキュメント: `AWS-RunPatchBaseline`」を参照してください。

- [Severity (重要度)]: ルールが適用されるパッチの重要度の値 (`Critical` など)。デフォルトの選択は `All` です。
- [Auto-approval (自動承認)]: 自動承認のためにパッチを選択する方法。

> **Note**
>
> Ubuntu Server の更新プログラムパッケージのリリース日は確定できないため、このオペティングシステムでは自動承認オプションがサポートされていません。

- [Approve patches after a specified number of days] (指定した日数後にパッチを承認): パッチがリリースまたは最後に更新されてから、自動的に承認されるまで Patch Manager が待機する日数。ゼロ (0) から 360 の任意の整数を入力できます。ほとんどのシナリオでは、待機日数を 100 日以内にすることをお勧めします。
- [Approve patches released up to a specific date] (特定の日付までにリリースされたパッチを承認): Patch Manager がその日付以前にリリースまたは最後に更新されたすべてのパッチを自動的に適用するパッチのリリース日。例えば、2023 年 7 月 7 日を指定した場合、リリース日または最後の更新日が 2023 年 7 月 8 日以降であるパッチは、自動的にインストールされません。

- (オプション) [コンプライアンスレポート]: ベースラインで承認されたパッチに割り当てる重要度 (`Critical` または `High` など)。

> **Note**
>
> コンプライアンスレポートレベルを指定し、任意の承認されたパッチのパッチ状態が `Missing` として報告された場合、パッチベースラインで報告されるコンプライアンス全体の重要度は、指定した重要度レベルになります。

- [Include non-security updates (セキュリティに関連しない更新を含める)]: セキュリティに関連するパッチに加えて、ソースリポジトリで使用可能なセキュリティに関連しない Linux オペレーティングシステムのパッチをインストールするには、このチェックボックスをオンにします。

> **Note**
>
> SUSE Linux Enterprise Server (SLES) では、セキュリティに関連する問題とセキュリティに関連しない問題に対するパッチがデフォルトで SLES マネージドノードにインストールされるため、このチェックボックスを選択する必要はありません。詳細については、「SLES」の セキュリティに関連するパッチの選択方法 のコンテンツを参照してください。

カスタムのパッチベースラインでの承認ルールの使用の詳細については、「カスタムベースライン」を参照してください。

9. 承認ルールに適合するパッチに加えて明示的に承認するパッチがある場合は、[パッチの例外] セクションで、以下の操作を実行します。

   - [Approved patches (承認済みパッチ)] ボックスに、承認するパッチのカンマ区切りリストを入力します。

     承認済みパッチと拒否済みパッチのリストの許容されるフォーマットの詳細については、「承認されたパッチと拒否されたパッチのリストのパッケージ名の形式」を参照してください。

   - (オプション) [Approved patches compliance level (承認済みパッチのコンプライアンスレベル)] リストで、リスト内のパッチにコンプライアンスレベルを割り当てます。

   - 指定した承認済みパッチがセキュリティに関連しない場合は、[セキュリティ以外の更新を含める] チェックボックスをオンにして、これらのパッチも Linux オペレーティングシステムにインストールされるようにします。

10. 承認ルールに適合するパッチにもかかわらず明示的に拒否するパッチがある場合は、[パッチの例外] セクションで、以下の操作を実行します。

    - [Rejected patches (拒否済みパッチ)] ボックスに、拒否するパッチのカンマ区切りリストを入力します。

      承認済みパッチと拒否済みパッチのリストの許容されるフォーマットの詳細については、「承認されたパッチと拒否されたパッチのリストのパッケージ名の形式」を参照してください。

    - [Rejected patches action (拒否されたパッチのアクション)] で、[Rejected patches (拒否されたパッチ)] リストに含まれているパッチに実行するPatch Managerのアクションを選択します。

      - 依存関係として許可: [拒否済みパッチ] リスト内のパッケージは、他のパッケージの依存関係である場合にのみインストールされます。これはパッチベースラインに準拠しているとみなされ、そのステータスは InstalledOther として報告されます。オプションが何も指定されていないときは、これがデフォルトのアクションとなります。

      - ブロック: [拒否されたパッチ] リスト内のパッケージ、およびそれらを依存関係として含むパッケージは、いかなる状況でも Patch Manager によってインストールされません。パッケージが [拒否されたパッチ] リストに追加される前にインストールされている場合、または後で Patch Manager 以外でインストールされている場合は、そのパッチはパッチベース

ラインに準拠していないとみなされ、そのステータスは InstalledRejected として報告されます。

> **Note**
>
> Patch Manager はパッチの依存関係を再帰的に検索します。

11. (オプション) AmazonLinux2016.03 や AmazonLinux2017.09 など、異なるバージョンのオペレーティングシステム用に代替パッチリポジトリを指定する場合は、[Patch sources (パッチソース)] セクションで、各製品について以下の操作を行います。

    - [Name (名前)] に、ソース設定を識別するための名前を入力します。
    - [Product (製品)] で、パッチソースリポジトリが使用されるオペレーティングシステムのバージョン (`RedhatEnterpriseLinux7.4` など) を選択します。
    - [設定] に、以下の形式で使用する yum リポジトリ設定の値を入力します。

    ```
    [main]
    name=MyCustomRepository
    baseurl=https://my-custom-repository
    enabled=1
    ```

    > **Tip**
    >
    > yum リポジトリ設定で使用できるその他のオプションについては、 dnf.conf (5) を参照してください。

    [Add another source (別のソースの追加)] を選択して、追加のオペレーティングシステムの最大 20 バージョンのそれぞれにソースリポジトリを指定できます。

    代替ソースパッチリポジトリの詳細については、「代替パッチソースリポジトリを指定する方法 (Linux)」を参照してください。

12. (オプション) [Manage tags (タグの管理)] で、1 つ以上のタグキーの名前と値のペアをパッチベースラインに適用します。

    タグは、リソースに割り当てるオプションのメタデータです。タグを使用すると、目的、所有者、環境などのさまざまな方法でリソースを分類できます。例えば、指定したパッチの重要度

レベル、適用されるオペレーティングシステムファミリー、環境タイプを識別するためにパッチベースラインにタグ付けする場合があります。この場合、次のようなキーの名前と値のペアのタグを指定することができます。

- `Key=PatchSeverity,Value=Critical`
- `Key=OS,Value=RHEL`
- `Key=Environment,Value=Production`

13. [Create patch baseline] を選択します。

macOS のカスタムパッチベースラインを作成する

AWS Systems Manager のツールである Patch Manager で macOS マネージドノードのカスタムパッチベースラインを作成するには、以下の手順に従います。

Windows Server マネージドノードのパッチベースラインの作成については、「Windows Server のカスタムパッチベースラインを作成する」を参照してください。Linux マネージドノードのパッチベースラインの作成については、「Linux 用 カスタムパッチベースラインの作成」を参照してください。

> **Note**
>
> すべての AWS リージョン において macOS はサポートされていません。macOS についての Amazon EC2 のサポートの詳細については、「Amazon EC2 ユーザーガイド」の「Amazon EC2 Mac インスタンス」を参照してください。

macOS マネージドノードのカスタム パッチベースラインを作成するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Patch Manager] を選択します。
3. [パッチベースライン] タブを選択し、[パッチベースラインの作成] を選択します。

   -または-

   現在の AWS リージョン で Patch Manager に初めてアクセスしている場合は、[概要から開始] で [パッチベースライン] タブを選択してから、[パッチベースラインの作成] を選択します。

4. [Name (名前)] フィールドに、新しいパッチベースラインの名前 (例: `MymacOSPatchBaseline`) を入力します。
5. (オプション) [Description (説明)] に、パッチベースラインの説明を入力します。
6. [Operating system (オペレーティングシステム)] で、macOS を選択します。
7. 作成してすぐに、このパッチベースラインを macOS のデフォルトとして使用する場合は、[このパッチベースラインを macOS インスタンスのデフォルトのパッチベースラインとして設定します] を選択します。

   > **Note**
   >
   > このオプションは、2022 年 12 月 22 日のパッチポリシーリリース前に初めて Patch Manager にアクセスした場合にのみ使用できます。
   > 既存のパッチベースラインのデフォルト設定の詳細については、「既存のパッチベースラインをデフォルトとして設定する」を参照してください。

8. [Approval rules for operating-systems (オペレーティングシステムの承認ルール)] セクションで、フィールドを使用して 1 つ以上の自動承認ルールを作成します。

   - [製品]: 承認ルールが適用されるオペレーティングシステムのバージョン (`Mojave10.14.1` または `Catalina10.15.1` など)。デフォルトの選択は `All` です。

     > **Note**
     >
     > Homebrew オープンソースソフトウェアパッケージ管理システムは、macOS 10.14.x (Mojave) および 10.15.x (Catalina) のサポートを終了しました。結果として、これらのバージョンでは Patch Manager を使用したパッチ適用オペレーションはサポートされていません。

   - 分類: パッチ適用プロセス中にパッケージを適用するパッケージマネージャー。以下から選択できます。
     - softwareupdate
     - installer
     - brew
     - brew cask

     デフォルトの選択は `All` です。

- (オプション) [コンプライアンスレポート]: ベースラインで承認されたパッチに割り当てる重要度 (`Critical` または `High` など)。

> **Note**
>
> コンプライアンスレポートレベルを指定し、任意の承認されたパッチのパッチ状態が `Missing` として報告された場合、パッチベースラインで報告されるコンプライアンス全体の重要度は、指定した重要度レベルになります。

カスタムのパッチベースラインでの承認ルールの使用の詳細については、「カスタムベースライン」を参照してください。

9. 承認ルールに適合するパッチに加えて明示的に承認するパッチがある場合は、[パッチの例外] セクションで、以下の操作を実行します。

   - [Approved patches (承認済みパッチ)] ボックスに、承認するパッチのカンマ区切りリストを入力します。

     承認済みパッチと拒否済みパッチのリストの許容されるフォーマットの詳細については、「承認されたパッチと拒否されたパッチのリストのパッケージ名の形式」を参照してください。

   - (オプション) [Approved patches compliance level (承認済みパッチのコンプライアンスレベル)] リストで、リスト内のパッチにコンプライアンスレベルを割り当てます。

10. 承認ルールに適合するパッチにもかかわらず明示的に拒否するパッチがある場合は、[パッチの例外] セクションで、以下の操作を実行します。

    - [Rejected patches (拒否済みパッチ)] ボックスに、拒否するパッチのカンマ区切りリストを入力します。

      承認済みパッチと拒否済みパッチのリストの許容されるフォーマットの詳細については、「承認されたパッチと拒否されたパッチのリストのパッケージ名の形式」を参照してください。

    - [Rejected patches action (拒否されたパッチのアクション)] で、[Rejected patches (拒否されたパッチ)] リストに含まれているパッチに実行するPatch Managerのアクションを選択します。

      - 依存関係として許可: [拒否済みパッチ] リスト内のパッケージは、他のパッケージの依存関係である場合にのみインストールされます。これはパッチベースラインに準拠しているとみなされ、そのステータスは InstalledOther として報告されます。オプションが何も指定されていないときは、これがデフォルトのアクションとなります。

- ブロック: [拒否されたパッチ] リスト内のパッケージ、およびそれらを依存関係として含むパッケージは、いかなる状況でも Patch Manager によってインストールされません。パッケージが [拒否されたパッチ] リストに追加される前にインストールされている場合、または後で Patch Manager 以外でインストールされている場合は、そのパッチはパッチベースラインに準拠していないとみなされ、そのステータスは InstalledRejected として報告されます。

11. (オプション) [Manage tags (タグの管理)] で、1 つ以上のタグキーの名前と値のペアをパッチベースラインに適用します。

    タグは、リソースに割り当てるオプションのメタデータです。タグを使用すると、目的、所有者、環境などのさまざまな方法でリソースを分類できます。例えば、指定したパッチの重要度レベル、適用されるパッケージマネージャー、環境タイプを識別するためにパッチベースラインにタグ付けする場合があります。この場合、次のようなキーの名前と値のペアのタグを指定することができます。

    - `Key=PatchSeverity,Value=Critical`
    - `Key=PackageManager,Value=softwareupdate`
    - `Key=Environment,Value=Production`

12. [Create patch baseline] を選択します。

Windows Server のカスタムパッチベースラインを作成する

AWS Systems Manager のツールである Patch Manager で Windows マネージドノードのカスタムパッチベースラインを作成するには、以下の手順に従います

Linux マネージドノードのパッチベースラインの作成については、「Linux 用 カスタムパッチベースラインの作成」を参照してください。macOS マネージドノードのパッチベースラインの作成については、「macOS のカスタムパッチベースラインを作成する」を参照してください。

Windows サービスパックのインストールのみに限定された修正プログラムベースラインの作成例については、「チュートリアル: コンソールを使用して Windows サービスパックをインストールするためのパッチベースラインを作成する」を参照してください 。

カスタムパッチベースラインを作成するには (Windows)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Patch Manager] を選択します。

3. [パッチベースライン] タブを選択し、[パッチベースラインの作成] を選択します。

   -または-

   現在の AWS リージョン で Patch Manager に初めてアクセスしている場合は、[概要から開始] で [パッチベースライン] タブを選択してから、[パッチベースラインの作成] を選択します。

4. [Name (名前)] フィールドに、新しいパッチベースラインの名前 (例: `MyWindowsPatchBaseline`) を入力します。

5. (オプション) [Description (説明)] に、パッチベースラインの説明を入力します。

6. [Operating system (オペレーティングシステム)] で、`Windows` を選択します。

7. [使用可能なセキュリティ更新のコンプライアンスステータス] で、パッチベースラインで指定されたインストール基準を満たさないため、使用可能ではあるものの承認されていないセキュリティパッチに割り当てるステータス ([非準拠] または [準拠]) を選択します。

   シナリオ例: パッチがリリースされてからインストールされるまでに待機する期間を長く指定している場合は、インストールするセキュリティパッチをスキップできます。指定した待機期間中にパッチの更新がリリースされると、パッチのインストールの待機期間がもう一度開始されます。待機期間が長すぎる場合、複数のバージョンのパッチがリリースされ、インストールされない可能性があります。

8. 作成してすぐに、このパッチベースラインを Windows のデフォルトとして使用する場合は、[Set this patch baseline as the default patch baseline for Windows Server instances (このパッチベースラインを Windows Server インスタンスのデフォルトのパッチベースラインにする)] を選択します。

   > **Note**
   >
   > このオプションは、2022 年 12 月 22 日のパッチポリシーリリース前に初めて Patch Manager にアクセスした場合にのみ使用できます。
   > 既存のパッチベースラインのデフォルト設定の詳細については、「既存のパッチベースラインをデフォルトとして設定する」を参照してください。

9. [Approval rules for operating systems (オペレーティングシステムの承認ルール)] セクションで、フィールドを使用して 1 つ以上の自動承認ルールを作成します。

   - [製品]: 承認ルールが適用されるオペレーティングシステムのバージョン (`WindowsServer2012` など)。デフォルトの選択は `All` です。

- [Classification (分類)]: 承認ルールが適用されるパッチのタイプ (`CriticalUpdates`、`Drivers`、`Tools` など)。デフォルトの選択は `All` です。

  > **Tip**
  >
  > `ServicePacks` を含めるか、Classification リストで `All` を選択して、Windows サービスパックのインストールを承認ルールに含めることができます。例については、「チュートリアル: コンソールを使用して Windows サービスパックをインストールするためのパッチベースラインを作成する」を参照してください。

- [Severity (重要度)]: ルールが適用されるパッチの重要度の値 (`Critical` など)。デフォルトの選択は `All` です。
- [Auto-approval (自動承認)]: 自動承認のためにパッチを選択する方法。
  - [Approve patches after a specified number of days] (指定した日数後にパッチを承認): パッチがリリースまたは更新されてから、自動的に承認されるまで Patch Manager が待機する日数。ゼロ (0) から 360 の任意の整数を入力できます。ほとんどのシナリオでは、待機日数を 100 日以内にすることをお勧めします。
  - [Approve patches released up to a specific date] (特定の日付までにリリースされたパッチを承認): Patch Manager がその日付以前にリリースまたは最後に更新されたすべてのパッチを自動的に適用するパッチのリリース日。例えば、2023 年 7 月 7 日を指定した場合、リリース日または最後の更新日が 2023 年 7 月 8 日以降であるパッチは、自動的にインストールされません。
- (オプション) [Compliance reporting (コンプライアンスレポート)]: ベースラインで承認されたパッチに割り当てる重要度 (`High` など)。

  > **Note**
  >
  > コンプライアンスレポートレベルを指定し、任意の承認されたパッチのパッチ状態が `Missing` として報告された場合、パッチベースラインで報告されるコンプライアンス全体の重要度は、指定した重要度レベルになります。

10. (オプション) [Approval rules for applications (アプリケーションの承認ルール)] セクションで、フィールドを使用して 1 つ以上の自動承認ルールを作成します。

> **Note**
>
> 承認ルールを指定する代わりに、承認されたパッチと拒否されたパッチのリストをパッチ例外として指定できます。手順 10 と 11 を参照してください。

- [Product family (製品ファミリー)]: ルールを指定する Microsoft 製品ファミリー全般 (`Office` や `Exchange Server` など)。
- [製品]: 承認ルールが適用されるアプリケーションのバージョン (`Office 2016` や `Active Directory Rights Management Services Client 2.0 2016` など)。デフォルトの選択は `All` です。
- [Classification (分類)]: 承認ルールが適用されるパッチのタイプ (`CriticalUpdates` など)。デフォルトの選択は `All` です。
- [Severity (重要度)]: ルールが適用されるパッチの重要度の値 (`Critical` など)。デフォルトの選択は `All` です。
- [Auto-approval (自動承認)]: 自動承認のためにパッチを選択する方法。
  - [Approve patches after a specified number of days] (指定した日数後にパッチを承認): パッチがリリースまたは更新されてから、自動的に承認されるまで Patch Manager が待機する日数。ゼロ (0) から 360 の任意の整数を入力できます。ほとんどのシナリオでは、待機日数を 100 日以内にすることをお勧めします。
  - [Approve patches released up to a specific date] (特定の日付までにリリースされたパッチを承認): Patch Manager がその日付以前にリリースまたは最後に更新されたすべてのパッチを自動的に適用するパッチのリリース日。例えば、2023 年 7 月 7 日を指定した場合、リリース日または最後の更新日が 2023 年 7 月 8 日以降であるパッチは、自動的にインストールされません。
- (オプション) [コンプライアンスレポート]: ベースラインで承認されたパッチに割り当てる重要度 (`Critical` または `High` など)。

> **Note**
>
> コンプライアンスレポートレベルを指定し、任意の承認されたパッチのパッチ状態が `Missing` として報告された場合、パッチベースラインで報告されるコンプライアンス全体の重要度は、指定した重要度レベルになります。

11. (オプション) 承認ルールに従ってパッチを選択させるのではなく、パッチを明示的に承認する場合は、[パッチの例外] セクションで次の手順を実行します。

    - [Approved patches (承認済みパッチ)] ボックスに、承認するパッチのカンマ区切りリストを入力します。

      承認済みパッチと拒否済みパッチのリストの許容されるフォーマットの詳細については、「承認されたパッチと拒否されたパッチのリストのパッケージ名の形式」を参照してください。

    - (オプション) [Approved patches compliance level (承認済みパッチのコンプライアンスレベル)] リストで、リスト内のパッチにコンプライアンスレベルを割り当てます。

12. 承認ルールに適合するパッチにもかかわらず明示的に拒否するパッチがある場合は、[パッチの例外] セクションで、以下の操作を実行します。

    - [Rejected patches (拒否済みパッチ)] ボックスに、拒否するパッチのカンマ区切りリストを入力します。

      承認済みパッチと拒否済みパッチのリストの許容されるフォーマットの詳細については、「承認されたパッチと拒否されたパッチのリストのパッケージ名の形式」を参照してください。

    - [Rejected patches action (拒否されたパッチのアクション)] で、[Rejected patches (拒否されたパッチ)] リストに含まれているパッチに実行するPatch Managerのアクションを選択します。

      - 依存関係として許可: Windows Server はパッケージ依存関係の概念をサポートしません。[拒否されたパッチ] リスト内のパッケージが既にノードにインストールされている場合、そのステータスは `INSTALLED_OTHER` として報告されます。ノードに既にインストールされていないパッケージはスキップされます。
      - ブロック: どのような状況下でも、Patch Manager は [拒否されたパッチ] リスト内のパッケージをインストールしません。パッケージが [拒否されたパッチ] リストに追加される前にインストールされた場合、または追加後に Patch Manager 外でインストールされた場合、そのパッケージはパッチベースラインに準拠していないとみなされ、ステータスは `INSTALLED_REJECTED` として報告されます。

      拒否されたパッケージアクションの詳細については、「カスタムパッチベースラインでの拒否されたパッチリストのオプション」を参照してください。

13. (オプション) [Manage tags (タグの管理)] で、1 つ以上のタグキーの名前と値のペアをパッチベースラインに適用します。

タグは、リソースに割り当てるオプションのメタデータです。タグを使用すると、目的、所有者、環境などのさまざまな方法でリソースを分類できます。例えば、指定したパッチの重要度レベル、適用されるオペレーティングシステムファミリー、環境タイプを識別するためにパッチベースラインにタグ付けする場合があります。この場合、次のようなキーの名前と値のペアのタグを指定することができます。

- `Key=PatchSeverity,Value=Critical`
- `Key=OS,Value=RHEL`
- `Key=Environment,Value=Production`

14. [Create patch baseline] を選択します。

カスタムパッチベースラインの更新または削除

AWS Systems Manager のツールである Patch Manager で作成したカスタムパッチベースラインは、更新または削除が可能です。パッチベースラインを更新するときに、名前や説明、承認ルール、および承認されたパッチと却下されたパッチの例外を変更できます。パッチベースラインに適用されたタグを変更することもできます。パッチベースラインが作成されたオペレーティングシステムタイプを変更することはできません。 によって提供される事前定義されたパッチベースラインを変更することはできませんAWS

パッチベースラインの更新または削除

パッチベースラインを更新または削除するには、以下の手順を実行します。

> **Important**
>
> Quick Setup のパッチポリシー設定で使用されている可能性のあるカスタムパッチベースラインを削除する場合は注意が必要です。
> Quick Setup でパッチポリシー設定を使用している場合、カスタムパッチベースラインに加えた更新は 1 時間に 1 回 Quick Setup と同期されます。
> パッチポリシーで参照されていたカスタムパッチベースラインを削除すると、Quick Setup のそのパッチポリシーについての [Configuration details] (設定の詳細) ページにバナーが表示されます。バナーには、パッチポリシーが既に存在しないパッチベースラインを参照していること、およびそれ以降のパッチ適用オペレーションができないことが示されます。この場合は、Quick Setup の [Configurations] (設定) ページに戻り、Patch Manager 設定を選択し、[Actions] (アクション)、[Edit configuration] (設定を編集) を選択します。削除されたパッ

チベースライン名が強調表示されます。影響を受けるオペレーティングシステム用の新しいパッチベースラインを選択する必要があります。

パッチベースラインを更新または削除するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Patch Manager] を選択します。
3. 更新あるいは削除するパッチベースラインを選択してから、次のいずれかを実行します。

   - AWS アカウント からパッチベースラインを削除するには、[Delete (削除)] を選択します。システムからアクションを確認するよう求められます。
   - パッチベースラインの名前または説明を変更するには、承認ルール、またはパッチの例外で、[Edit (編集)] を選択します。[Edit patch baseline (パッチベースラインの編集)] ページで値とオプションを変更してから、[Save changes (変更を保存)] を選択します。
   - パッチベースラインの追加、変更、削除を適用するには、[Tags (タグ)] タブを選択して、[Edit tags (タグの編集)] を選択します。[Edit patch baseline tags (パッチベースラインタグの編集)] ページで、パッチベースラインタグを変更して、[Save changes (変更の保存)] を選択します。

   設定の選択肢については、「カスタムパッチベースラインの操作」を参照してください。

既存のパッチベースラインをデフォルトとして設定する

> **Important**
>
> ここで選択したデフォルトのパッチベースラインは、パッチポリシーに基づくパッチ適用オペレーションには適用されません。パッチポリシーは、独自のパッチベースライン仕様を使用します。パッチポリシーの詳細については、「Quick Setup でのパッチポリシー設定 」を参照してください。

AWS Systems Manager のツールである Patch Manager でカスタムパッチベースラインを作成するときに、作成してすぐに、ベースラインを関連するオペレーティングシステムタイプのデフォルトに設定できます。詳細については、カスタムパッチベースラインの操作 を参照してください。

既存のパッチベースラインを、オペレーティングシステムタイプのデフォルトに設定することもできます。

> **Note**
>
> 実行する手順は、最初に Patch Manager にアクセスしたのが 2022 年 12 月 22 日のパッチポリシーのリリース前か後かによって異なります。その日より前に Patch Manager を使用した場合は、コンソールプロシージャを使用できます。それ以外の場合は、「AWS CLI」の手順に従います。コンソールプロシージャで参照されている [アクション] メニューは、パッチポリシーがリリースされる前に Patch Manager が使用されていないリージョンでは表示されません。

パッチベースラインをデフォルトとして設定するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Patch Manager] を選択します。
3. [パッチベースライン] タブを選択します。
4. パッチベースラインのリストで、現在オペレーティングシステムタイプのデフォルトとして設定されていないパッチベースラインのボタンを選択します。

   [Default baseline (デフォルトベースライン)] 列は、現在デフォルトとして設定されているベースラインを表しています。
5. [Actions (アクション)] メニューで、[Set default patch baseline (デフォルトパッチベースラインに設定)] を選択します。

   > **Important**
   >
   > [アクション] メニューは、2022 年 12 月 22 日より前に現在の AWS アカウント およびリージョンで、Patch Manager と作業していなかった場合、利用できません。詳細については、このトピックの前半の「注意」を参照してください。
6. 確認ダイアログボックスで [Yes, Set (はい、設定します)] を選択します。

パッチベースラインをデフォルトとして設定するには (AWS CLI)

1. 使用可能なパッチベースラインとその ID、Amazon リソースネーム (ARN) のリストを表示するには、describe-patch-baselines コマンドを実行してください。

```
aws ssm describe-patch-baselines
```

2. ベースラインを関連するオペレーティングシステムのデフォルトとして設定するには、register-default-patch-baseline コマンドを実行します。*baseline-id-or-ARN* の部分を、カスタムパッチベースラインまたは使用する定義済みのベースライン ID に置き換えます。

   Linux & macOS

```
aws ssm register-default-patch-baseline \
    --baseline-id baseline-id-or-ARN
```

   以下は、カスタムベースラインをデフォルトとして設定する例です。

```
aws ssm register-default-patch-baseline \
    --baseline-id pb-abc123cf9bEXAMPLE
```

   以下は、デフォルトで AWS によって管理される定義済みベースラインの設定例です。

```
aws ssm register-default-patch-baseline \
    --baseline-id arn:aws:ssm:us-east-2:733109147000:patchbaseline/
pb-0574b43a65ea646e
```

   Windows Server

```
aws ssm register-default-patch-baseline ^
    --baseline-id baseline-id-or-ARN
```

   以下は、カスタムベースラインをデフォルトとして設定する例です。

```
aws ssm register-default-patch-baseline ^
    --baseline-id pb-abc123cf9bEXAMPLE
```

   以下は、デフォルトで AWS によって管理される定義済みベースラインの設定例です。

```
aws ssm register-default-patch-baseline ^
    --baseline-id arn:aws:ssm:us-east-2:733109147000:patchbaseline/
pb-071da192df1226b63
```

利用可能なパッチの表示

AWS Systems Manager のツールである Patch Manager を使用すると、指定されたオペレーティングシステムおよび任意で特定のオペレーティングシステムのバージョンで使用できるすべてのパッチを表示できます。

> **Tip**
>
> 使用可能なパッチのリストを生成し、ファイルに保存するには、describe-available-patches コマンドを使用して、任意の出力を指定します。

利用可能なパッチを表示するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Patch Manager] を選択します。
3. [Patches (パッチ)] タブを選択します。

   -または-

   現在の AWS リージョン で Patch Manager に初めてアクセスしている場合は、[概要から始める] を選択してから、[パッチ] タブを選択します。

   > **Note**
   >
   > Windows Server の場合、[パッチ] タブに、Windows Server Update Service (WSUS) から利用できる更新が表示されます。

4. [Operating system (オペレーティングシステム)] で、利用可能なパッチを表示するオペレーティングシステム (`Windows` や `Amazon Linux` など) を選択します。
5. (オプション) [Product (製品)] で、オペレーティングシステムのバージョン (`WindowsServer2019` や `AmazonLinux2018.03` など) を選択します。

6. (オプション) 結果の情報列を追加または削除するには、[Patches (パッチ)] リストの右上にある設定ボタン
   ( )
   をクリックします。(デフォルトでは、[Patches (パッチ)] タブには、利用可能なパッチのメタデータの一部の列のみが表示されます。)

   ビューに追加できるメタデータのタイプについては、AWS Systems Manager API リファレンスの「パッチ」を参照してください。

パッチグループの作成と管理

オペレーションでパッチポリシーを使用していない場合、タグを使用してマネージドノードをパッチグループに追加することで、パッチ適用作業を整理できます。

> **Note**
>
> パッチグループは、パッチポリシーに基づくパッチ適用オペレーションでは使用されません。パッチポリシーの使用については、「Quick Setup でのパッチポリシー設定」を参照してください。
> 2022 年 12 月 22 日にパッチポリシーのサポートがリリースされる前にパッチグループを使用していなかったアカウントとリージョンのペアでは、コンソールでパッチグループの機能がサポートされていません。パッチグループの機能は、この日付より前にパッチグループの使用を開始したアカウントとリージョンのペアで引き続き使用できます。

パッチオペレーションでタグを使用するには、タグキー `Patch Group` または `PatchGroup` をマネージドノードに適用する必要があります。また、タグの値としてパッチグループに付ける名前を指定する必要があります。任意のタグ値を指定できますが、タグキーは `Patch Group` または `PatchGroup` とする必要があります。

EC2 インスタンスのメタデータでタグを許可している場合は、`PatchGroup` (スペースなし) を使用する必要があります。

タグを使用してマネージドノードをグループ化する場合、パッチグループの値をパッチベースラインに追加します。パッチグループをパッチベースラインに登録することで、パッチ適用の実行時に正しいパッチがインストールされます。パッチグループの詳細については、「パッチグループ」を参照してください。

このトピックのタスクを実行して、ノードとパッチベースラインのタグを使用してマネージドノードにパッチを適用できるように準備します。タスク 1 は、Amazon EC2 インスタンスにパッチ適用する場合にのみ必要です。タスク 2 は、ハイブリッドおよびマルチクラウド環境で EC2 以外のインスタンスにパッチを適用する場合にのみ必要です。タスク 3 は、すべてのマネージドノードで必要です。

> **Tip**
>
> AWS CLI コマンド `add-tags-to-resource` または Systems Manager API オペレーション ssm-agent-minimum-s3-permissions-required`AddTagsToResource` を使用してマネージドノードにタグを追加できます。

タスク

- タスク 1: タグを使用したパッチグループに EC2 インスタンスを追加する
- タスク 2: タグを使用してパッチグループをマネージドノードに追加する
- タスク 3: パッチベースラインにパッチグループを追加します。

タスク 1: タグを使用したパッチグループに EC2 インスタンスを追加する

Systems Manager コンソールまたは Amazon EC2 コンソールを使用して、EC2 インスタンスにタグを追加できます。このタスクは、Amazon EC2 インスタンスにパッチ適用する場合にのみ必要です。

> **Important**
>
> インスタンスで [Allow tags in instance metadata] (インスタンスメタデータ内のタグを許可する) オプションを有効にした場合は、Amazon EC2 インスタンスに `Patch Group` タグ (スペースなし) を適用することはできません。インスタンスメタデータでタグを許可すると、タグキー名にスペースが含まれなくなります。EC2 インスタンスのメタデータでタグを許可している場合は、スペースなしでタグキー `PatchGroup` を使用する必要があります。

オプション 1: EC2 インスタンスをパッチグループに追加するには (Systems Manager コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。

2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. [マネージドインスタンス] リストで、パッチを設定するマネージド EC2 インスタンスの ID を選択します。EC2 インスタンスのノード ID は `i-` で始まります。

> **Note**
>
> Amazon EC2 コンソールと AWS CLI を使用する場合、Systems Manager で使用するようにまだ設定されていないインスタンスに `Key = Patch Group` または `Key = PatchGroup` タグを適用できます。
> 表示されるはずのマネージドノードが表示されない場合は、トラブルシューティングのヒントについて「マネージドノードの可用性のトラブルシューティング」を参照してください。

4. [タグ] タブを選択し、[編集] を選択します。
5. 左側の列に、**`Patch Group`** または **`PatchGroup`** を入力します。EC2 インスタンスのメタデータでタグを許可している場合は、スペースなしで `PatchGroup` を使用する必要があります。
6. 右側の列に、パッチグループの名前として使用するタグ値を入力します。
7. [Save] を選択します。
8. この手順を繰り返して、同じパッチグループに他の EC2 インスタンスを追加します。

オプション 2: EC2 インスタンスをパッチグループに追加するには (Amazon EC2 コンソール)

1. Amazon EC2 コンソールを開き、ナビゲーションペインで [Instances (インスタンス)] を選択します。
2. インスタンスの一覧で、パッチ適用を設定するインスタンスを選択します。
3. [アクション] メニューから、[インスタンスの設定]、[タグの追加/編集] の順に選択します。
4. [新しいタグを追加] をクリックします。
5. [Key] (キー) で **`Patch Group`** または **`PatchGroup`** を入力します。EC2 インスタンスのメタデータでタグを許可している場合は、スペースなしで `PatchGroup` を使用する必要があります。
6. [値] に、パッチグループの名前として使用する値を入力します。
7. [Save] を選択します。
8. この手順を繰り返して、同じパッチグループ内の他のインスタンスを追加します。

タスク 2: タグを使用してパッチグループをマネージドノードに追加する

このトピックの手順に従って、AWS IoT Greengrass コアデバイスと EC2 以外のハイブリッドアクティベーションマネージドノード (mi-*) にタグを追加します。このタスクは、ハイブリッドおよびマルチクラウド環境で EC2 以外のインスタンスにパッチを適用する場合にのみ必要です。

> **Note**
>
> Amazon EC2 コンソールを使用して、非 EC2 マネージドノードにタグを追加することはできません。

EC2 以外のマネージドノードをパッチグループに追加するには (Systems Manager コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. [マネージドノード] リストで、パッチ適用を設定するマネージドノードを選択します。

   > **Note**
   >
   > 表示されるはずのマネージドノードが表示されない場合は、トラブルシューティングのヒントについて「マネージドノードの可用性のトラブルシューティング」を参照してください。

4. [タグ] タブを選択し、[編集] を選択します。
5. 左側の列に、**`Patch Group`** または **`PatchGroup`** を入力します。EC2 インスタンスのメタデータでタグを許可している場合は、スペースなしで `PatchGroup` を使用する必要があります。
6. 右側の列に、パッチグループの名前として使用するタグ値を入力します。
7. [Save] を選択します。
8. この手順を繰り返して、同じパッチグループ内の他のマネージドノードを追加します。

タスク 3: パッチベースラインにパッチグループを追加します。

特定のパッチベースラインをマネージドノードと関連付ける場合は、パッチベースラインにパッチグループの値を追加する必要があります。パッチグループをパッチベースラインに登録することで、パッチ適用の実行時に正しいパッチがインストールされます。このタスクは、EC2 インスタン

ス、EC2 以外のマネージドノード、あるいはその両方にパッチを適用するかどうかにかかわらず必要です。

パッチグループの詳細については、「パッチグループ」を参照してください。

> **Note**
>
> 実行する手順は、最初に Patch Manager にアクセスしたのが 2022 年 12 月 22 日のパッチポリシーのリリース前か後かによって異なります。

パッチグループをパッチベースラインに追加するには (System Manager コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Patch Manager] を選択します。
3. 現在の AWS リージョン で Patch Manager ページに初めてアクセスし、Patch Manager 開始ページが開いた場合は、[概要から開始] を選択します。
4. [パッチベースライン] タブを選択し、[パッチベースライン] リストから、パッチグループに設定するパッチベースラインの名前を選択します。

   パッチポリシーのリリース後まで最初に Patch Manager にアクセスしなかった場合は、作成したカスタムベースラインを選択する必要があります。
5. [ベースライン ID] 詳細ページに [アクション] メニューがある場合は、次の操作を行います。

   - [Actions (アクション)] 、[Modify patch groups (パッチグループの変更)] の順に選択します。
   - タスク 2: タグを使用してパッチグループをマネージドノードに追加する でマネージドノードに追加したタグの値を入力して、[追加] を選択します。

   [ベースライン ID] 詳細ページに [アクション] メニューがない場合は、パッチグループはコンソールで設定できません。代わりに、以下のどちらかを実行できます。

   - (推奨) AWS Systems Manager のツールである Quick Setup にパッチポリシーを設定し、パッチベースラインを 1 つ以上の EC2 インスタンスにマッピングします。

     詳細については、「Quick Setup パッチポリシーの使用」および「Quick Setup パッチポリシーを使用して組織全体のパッチ適用を自動化する」を参照してください。

- AWS Command Line Interface (AWS CLI) の register-patch-baseline-for-patch-group コマンドを使用して、パッチグループを設定します。

Patch Managerと AWS Security Hub の統合

AWS Security Hub は、AWS のセキュリティ状態の包括的なビューを提供します。Security Hub は、AWS アカウント、AWS のサービス、およびサポートされているサードパーティーパートナー製品全体からセキュリティデータを収集します。Security Hub により、セキュリティ業界の標準とベストプラクティスに照らしてお使いの環境をチェックできます。Security Hub を使用すると、セキュリティの傾向を分析し、最も優先度の高いセキュリティ問題を特定できます。

AWS Systems Manager のツールである Patch Manager と Security Hub 間の統合を利用して、Patch Manager から Security Hub に非準拠ノードの検出結果を送信できます。検出結果は、セキュリティチェックまたはセキュリティ関連の検出の監視可能なレコードです。Security Hub では、このようなパッチ関連の検出結果をセキュリティ体制の分析に含めることができます。

以下のトピックの情報は、パッチ適用オペレーションに使用する設定の方法や種類に関係なく適用されます。

- Quick Setup で設定されているパッチポリシー
- Quick Setup で設定されているホスト管理オプション
- パッチ `Scan` または `Install` のタスクを実行するためのメンテナンスウィンドウ
- オンデマンドの [Patch now] (今すぐパッチ適用) オペレーション

目次

- Patch Manager から Security Hub に結果を送信する方法
  - Patch Manager が送信する検出結果の種類
  - 結果が送信されるまでのレイテンシー
  - Security Hub が使用できないときに再試行する
  - Security Hub での 結果の表示
- Patch Manager からの一般的な結果
- 統合の有効化と設定
- 検出結果の送信を停止する方法

Patch Manager から Security Hub に結果を送信する方法

Security Hub では、セキュリティの問題が調査結果として追跡されます。結果の中には、他の AWS のサービスやサードパーティーのパートナーが検出した問題に由来するものもあります。Security Hub には、セキュリティの問題を検出し、検出結果を生成するために使用する一連のルールもあります。

Patch Manager は、Security Hub に検出結果を送信する Systems Manager ツールの 1 つです。SSM ドキュメント (`AWS-RunPatchBaseline`、`AWS-RunPatchBaselineAssociation`、または`AWS-RunPatchBaselineWithHooks`) を実行してパッチ適用オペレーションを実行すると、AWS Systems Manager のツールである Inventory または Compliance、またはその両方にパッチ適用情報が送信されます。インベントリ、Compliance、またはその両方がデータを受け取ると、Patch Manager が通知を受信します。次に、Patch Manager はデータの精度、書式設定、およびコンプライアンスを評価します。すべての条件が満たされた場合、Patch Manager はデータを Security Hub に転送します。

Security Hub には、これらすべてのソースからの結果を管理するためのツールが用意されています。検出結果の一覧を表示およびフィルタリングして、検出結果の詳細を表示できます。詳細については、AWS Security Hub ユーザーガイドの「検出結果の表示」を参照してください。検出結果の調査状況を追跡することもできます 詳細については、AWS Security Hub ユーザーガイドの「検出結果に対するアクションの実行」を参照してください。

Security Hub のすべての検出結果で、AWS Security Finding Format (ASFF) と呼ばれる標準の JSON 形式が使用されます。ASFF には、問題のソース、影響を受けるリソース、および検出結果の現在のステータスに関する詳細が含まれます。詳細については、AWS Security Hub ユーザーガイドの AWS Security Finding Format (ASFF)を参照してください。

Patch Manager が送信する検出結果の種類

Patch Manager は、AWS Security Finding Format (ASFF) を使用して結果を Security Hub に送信します。ASFF では、`Types` フィールドが検出結果タイプを提供します。Patch Manager の検出結果には、`Types` に対する次の値があります。

- ソフトウェアおよび設定のチェック/パッチ管理

Patch Manager は、非準拠マネージドノードごとに 1 つの検出結果を送信します。検出結果は、`AwsEc2Instance` リソースタイプとともに報告されるため、検出結果の `AwsEc2Instance` リソースタイプを報告する他の Security Hub 統合と相関させることができます。Patch Manager は、

オペレーションによってマネージドノードが非準拠であることが検出された場合にのみ Security Hub に検出結果を転送します。検出結果には、パッチのサマリー結果が含まれます。

> **Note**
>
> 非準拠のノードを Security Hub に報告した後は、ノードが準拠した状態になっても、Patch Manager は Security Hub に更新を送信しません。必要なパッチがマネージドノードに適用されたら、Security Hub の検出結果を手動で解決できます。

コンプライアンス定義については、「パッチコンプライアンス状態の値」を参照してください。`PatchSummary` の詳細については、AWS Security Hub API リファレンスの PatchSummary を参照してください。

結果が送信されるまでのレイテンシー

Patch Manager によって新しい検出結果が作成されると、通常は数秒から 2 時間以内に Security Hub に送信されます。速度は、その時点で処理されている AWS リージョン のトラフィックによって異なります。

Security Hub が使用できないときに再試行する

サービスの停止が発生した場合、AWS Lambda 関数が実行され、サービスが再度実行された後、メッセージをメインキューに戻すことができます。メッセージがメインキューに入ると、再試行は自動的に行われます。

Security Hub が使用できない場合、Patch Manager は検出結果が受信されるまでその結果を再送信し続けます。

Security Hub での 結果の表示

以下の手順では、パッチコンプライアンスに違反しているフリート内のマネージドノードに関する Security Hub の検出結果を表示する方法について説明します。

パッチコンプライアンスに関する Security Hub の検出結果を確認するには

1. AWS Management Console にサインインして、AWS Security Hub コンソール (https://console.aws.amazon.com/securityhub/) を開きます。
2. ナビゲーションペインで 調査結果を選択します。

3. [Add filters (フィルターの追加)]
   ( )
   ボックスを選択します。
4. メニューの [フィルタ] で、[製品名] を選択します。
5. 表示されたダイアログボックスの最初のフィールドで [is (=)] を選択し、2 番目のフィールドに「**`Systems Manager Patch Manager`**」と入力します。
6. [Apply] を選択します。
7. 結果を絞り込むために必要なフィルターを追加します。
8. 結果のリストで、詳細情報が必要な検出結果のタイトルを選択します。

   画面の右側にペインが開き、リソース、検出された問題、推奨される修正に関する詳細が表示されます。

> **Important**
>
> 現時点では、Security Hub は、すべてのマネージドインスタンスのリソースタイプを `EC2 Instance` としてレポートします。これには、Systems Manager で使用するために登録したオンプレミスサーバーおよび仮想マシン (VM) が含まれます。

重要度の分類

`Systems Manager Patch Manager` の検出結果の一覧には、検出結果の重大度に関するレポートが含まれています。[重要度] には、低いものから高いものまで、次のものが含まれます。

- [情報] - 問題は見つかりませんでした。
- [低] - この問題はアクションを必要としません。
- [中] - この問題は対処する必要がありますが、緊急ではありません。
- [高] - この問題は優先事項として対処する必要があります。
- [重要] - この問題を悪化させないようにすぐに修正する必要があります。

重要度は、インスタンス上の最も深刻である非準拠パッケージによって決定される。複数の重要度レベルのパッチベースラインを作成できるため、すべての非準拠パッケージの中で最も重要度が高いものが報告されます。例えば、パッケージ A の重要度が「重要」で、パッケージ B の重要度が「低」の 2 つの非準拠パッケージがあるとします。重要度として「重要」が報告されます。

重要度フィールドは Patch Manager Compliance フィールドと直接相関していることに注意してください。このフィールドは、ルールに一致する個々のパッチに割り当てるよう設定します。Compliance フィールドは個々のパッチに割り当てられるため、パッチの概要レベルには反映されません。

関連情報

- 「AWS Security Hub ユーザーガイド」の「検出結果」
- AWS 管理およびガバナンスのブログ内の「Patch Manager およびセキュリティハブマルチを使用するアカウントパッチのコンプライアンス」

Patch Manager からの一般的な結果

Patch Manager は、AWS 脆弱性レポート形式 (ASFF)を使用して結果を Security Hub に送信します。

以下に、Patch Manager からの一般的な検出結果の例を示します。


```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:patchmanager:us-east-2:111122223333:instance/i-02573cafcfEXAMPLE/
document/AWS-RunPatchBaseline/run-command/d710f5bd-04e3-47b4-82f6-df4e0EXAMPLE",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/ssm-patch-manager",
  "GeneratorId": "d710f5bd-04e3-47b4-82f6-df4e0EXAMPLE",
  "AwsAccountId": "111122223333",
  "Types": [
    "Software & Configuration Checks/Patch Management/Compliance"
  ],
  "CreatedAt": "2021-11-11T22:05:25Z",
  "UpdatedAt": "2021-11-11T22:05:25Z",
  "Severity": {
    "Label": "INFORMATIONAL",
    "Normalized": 0
  },
  "Title": "Systems Manager Patch Summary - Managed Instance Non-Compliant",
  "Description": "This AWS control checks whether each instance that is managed by AWS
 Systems Manager is in compliance with the rules of the patch baseline that applies to
 that instance when a compliance Scan runs.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information about bringing instances into patch compliance, see
 'Remediating out-of-compliance instances (Patch Manager)'.",
```

```
      "Url": "https://docs.aws.amazon.com/systems-manager/latest/userguide/patch-
compliance-remediation.html"
    }
  },
  "SourceUrl": "https://us-east-2.console.aws.amazon.com/systems-manager/fleet-manager/
i-02573cafcfEXAMPLE/patch?region=us-east-2",
  "ProductFields": {
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/ssm-
patch-manager/arn:aws:patchmanager:us-east-2:111122223333:instance/i-02573cafcfEXAMPLE/
document/AWS-RunPatchBaseline/run-command/d710f5bd-04e3-47b4-82f6-df4e0EXAMPLE",
    "aws/securityhub/ProductName": "Systems Manager Patch Manager",
    "aws/securityhub/CompanyName": "AWS"
  },
  "Resources": [
    {
      "Type": "AwsEc2Instance",
      "Id": "i-02573cafcfEXAMPLE",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "PatchSummary": {
    "Id": "pb-0c10e65780EXAMPLE",
    "InstalledCount": 45,
    "MissingCount": 2,
    "FailedCount": 0,
    "InstalledOtherCount": 396,
    "InstalledRejectedCount": 0,
    "InstalledPendingReboot": 0,
    "OperationStartTime": "2021-11-11T22:05:06Z",
    "OperationEndTime": "2021-11-11T22:05:25Z",
    "RebootOption": "NoReboot",
    "Operation": "SCAN"
  }
}
```

統合の有効化と設定

Security Hub と Patch Manager 統合を使用するには、Security Hub を有効にする必要があります。Security Hub を有効にする方法の詳細については、AWS Security Hub ユーザーガイドの「Security Hub の設定」を参照してください。

次の手順では、Security Hub が既にアクティブでも、Patch Manager 統合が無効になっている場合に、Patch Manager と Security Hub を統合する方法について説明します。以下の手順を完了する必要があるのは、統合を手動で無効にした場合だけです。

Security Hub 統合に Patch Manager を追加するには

1. ナビゲーションペインで、Patch Manager を選択します。
2. [Settings] (設定) タブを選択します。

   -または-

   現在の AWS リージョン で Patch Manager に初めてアクセスしている場合は、[事前定義されたパッチベースラインを表示する] を選択してから、[設定] タブを選択します。
3. [Patch compliance findings are not being exported to Security Hub (パッチコンプライアンス結果が Security Hub にエクスポートされてない)] の右側にある [Export to Security Hub (Security Hub にエクスポート)] セクションで、[有効にする] を選択します。

検出結果の送信を停止する方法

Security Hub への検出結果の送信を停止するには、Security Hub コンソールまたは API を使用できます。

詳細については、AWS Security Hub ユーザーガイドの次のトピックを参照してください。

- 統合からの検出結果のフローの無効化と有効化 (コンソール)
- 統合からの検出結果のフローの無効化 (Security Hub API、AWS CLI)

AWS CLI を使用して Patch Manager リソースを操作する

このセクションには、AWS Systems Manager のツールである Patch Manager の設定タスクを実行するために使用できる AWS Command Line Interface (AWS CLI) コマンドの例が含まれています。

独自のパッチベースラインを使用して、AWS CLI でサーバー環境にパッチを適用する方法の詳細は、「チュートリアル: AWS CLI を使用してサーバー環境にパッチを適用する」を参照してください。

AWS Systems Manager タスクの AWS CLI の使用の詳細については、AWS CLI コマンドリファレンスの AWS Systems Manager セクションを参照してください。

トピック

- パッチベースラインの AWS CLI コマンド
- パッチグループの AWS CLI コマンド
- パッチの概要と詳細を表示するための AWS CLI コマンド
- AWS CLI マネージドノードのスキャンとパッチ適用のためのコマンド

パッチベースラインの AWS CLI コマンド

パッチベースラインのサンプルコマンド

- パッチベースラインの作成
- 異なる OS バージョン用にカスタムリポジトリのパッチベースラインを作成する
- パッチベースラインの更新
- パッチベースラインの名前変更
- パッチベースラインの削除
- すべてのパッチベースラインのリストアップ
- すべての AWS 提供のパッチベースラインのリストアップ
- ユーザーのパッチベースラインのリストアップ
- パッチベースラインの表示
- デフォルトパッチベースラインの取得
- カスタムパッチベースラインをデフォルトとして設定する
- AWS パッチベースラインをデフォルトとしてリセットする
- パッチベースラインのタグ付け
- パッチベースラインのタグのリストアップ
- パッチベースラインからのタグの削除

パッチベースラインの作成

次のコマンドでは、リリースされてから 5 日後に Windows Server 2012 R2 のすべての緊急および重要なセキュリティ更新プログラムを承認するパッチベースラインを作成します。承認済みおよび拒否済みパッチリストに対しても、パッチが指定されています。また、パッチベースラインが本番環境用であることを示すタグが付けられます。

Linux & macOS

```
aws ssm create-patch-baseline \
    --name "Windows-Server-2012R2" \
    --tags "Key=Environment,Value=Production" \
    --description "Windows Server 2012 R2, Important and Critical security updates"
 \
    --approved-patches "KB2032276,MS10-048" \
    --rejected-patches "KB2124261" \
    --rejected-patches-action "ALLOW_AS_DEPENDENCY" \
    --approval-rules
 "PatchRules=[{PatchFilterGroup={PatchFilters=[{Key=MSRC_SEVERITY,Values=[Important,Critical
{Key=CLASSIFICATION,Values=SecurityUpdates},
{Key=PRODUCT,Values=WindowsServer2012R2}]},ApproveAfterDays=5}]"
```

Windows Server

```
aws ssm create-patch-baseline ^
    --name "Windows-Server-2012R2" ^
    --tags "Key=Environment,Value=Production" ^
    --description "Windows Server 2012 R2, Important and Critical security updates"
 ^
    --approved-patches "KB2032276,MS10-048" ^
    --rejected-patches "KB2124261" ^
    --rejected-patches-action "ALLOW_AS_DEPENDENCY" ^
    --approval-rules
 "PatchRules=[{PatchFilterGroup={PatchFilters=[{Key=MSRC_SEVERITY,Values=[Important,Critical
{Key=CLASSIFICATION,Values=SecurityUpdates},
{Key=PRODUCT,Values=WindowsServer2012R2}]},ApproveAfterDays=5}]"
```

システムが以下のような情報をレスポンスします。

```
{
   "BaselineId":"pb-0c10e65780EXAMPLE"
```

```
}
```

異なる OS バージョン用にカスタムリポジトリのパッチベースラインを作成する

Linux マネージドノードにのみ適用されます。以下のコマンドは、特定バージョンの Amazon Linux オペレーティングシステムに使用するパッチリポジトリを指定する方法を示しています。このサンプルは、Amazon Linux 2017.09 でデフォルトで 許可されているソースリポジトリを使用しますが、マネージドノード用に設定した別のソースリポジトリを使用するように調整することもできます。

> **Note**
>
> この複雑なコマンドをわかりやすく示すために、外部 JSON ファイルに保存されている追加のオプションと共に `--cli-input-json` オプションを使用します。

1. JSON ファイルを `my-patch-repository.json` などの名前で作成し、以下のコンテンツを追加します。

```
{
    "Description": "My patch repository for Amazon Linux 2017.09",
    "Name": "Amazon-Linux-2017.09",
    "OperatingSystem": "AMAZON_LINUX",
    "ApprovalRules": {
        "PatchRules": [
            {
                "ApproveAfterDays": 7,
                "EnableNonSecurity": true,
                "PatchFilterGroup": {
                    "PatchFilters": [
                        {
                            "Key": "SEVERITY",
                            "Values": [
                                "Important",
                                "Critical"
                            ]
                        },
                        {
                            "Key": "CLASSIFICATION",
                            "Values": [
                                "Security",
                                "Bugfix"
```

```
                            ]
                        },
                        {
                            "Key": "PRODUCT",
                            "Values": [
                                "AmazonLinux2017.09"
                            ]
                        }
                    ]
                }
            }
        ]
    },
    "Sources": [
        {
            "Name": "My-AL2017.09",
            "Products": [
                "AmazonLinux2017.09"
            ],
            "Configuration": "[amzn-main] \nname=amzn-main-Base
\nmirrorlist=http://repo./$awsregion./$awsdomain//$releasever/main/
mirror.list //nmirrorlist_expire=300//nmetadata_expire=300 \npriority=10
 \nfailovermethod=priority \nfastestmirror_enabled=0 \ngpgcheck=1
 \ngpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-amazon-ga \nenabled=1 \nretries=3
 \ntimeout=5\nreport_instanceid=yes"
        }
    ]
}
```

2. ファイルを保存したディレクトリで、次のコマンドを実行します。

```
aws ssm create-patch-baseline --cli-input-json file://my-patch-repository.json
```

システムが以下のような情報を返します。

```
{
    "BaselineId": "pb-0c10e65780EXAMPLE"
}
```

パッチベースラインの更新

次のコマンドでは、2 つのパッチを拒否済み、1 つのパッチを承認済みとして既存のパッチベースラインに追加します。

承認済みパッチと拒否済みパッチのリストの許容されるフォーマットの詳細については、「承認されたパッチと拒否されたパッチのリストのパッケージ名の形式」を参照してください。

Linux & macOS

```
aws ssm update-patch-baseline \
    --baseline-id pb-0c10e65780EXAMPLE \
    --rejected-patches "KB2032276" "MS10-048" \
    --approved-patches "KB2124261"
```

Windows Server

```
aws ssm update-patch-baseline ^
    --baseline-id pb-0c10e65780EXAMPLE ^
    --rejected-patches "KB2032276" "MS10-048" ^
    --approved-patches "KB2124261"
```

システムが以下のような情報をレスポンスします。

```
{
   "BaselineId":"pb-0c10e65780EXAMPLE",
   "Name":"Windows-Server-2012R2",
   "RejectedPatches":[
      "KB2032276",
      "MS10-048"
   ],
   "GlobalFilters":{
      "PatchFilters":[

      ]
   },
   "ApprovalRules":{
      "PatchRules":[
         {
            "PatchFilterGroup":{
               "PatchFilters":[
                  {
```

```
                    "Values":[
                       "Important",
                       "Critical"
                    ],
                    "Key":"MSRC_SEVERITY"
                 },
                 {
                    "Values":[
                       "SecurityUpdates"
                    ],
                    "Key":"CLASSIFICATION"
                 },
                 {
                    "Values":[
                       "WindowsServer2012R2"
                    ],
                    "Key":"PRODUCT"
                 }
              ]
           },
           "ApproveAfterDays":5
        }
     ]
  },
  "ModifiedDate":1481001494.035,
  "CreatedDate":1480997823.81,
  "ApprovedPatches":[
     "KB2124261"
  ],
  "Description":"Windows Server 2012 R2, Important and Critical security updates"
}
```

パッチベースラインの名前変更

Linux & macOS

```
aws ssm update-patch-baseline \
    --baseline-id pb-0c10e65780EXAMPLE \
    --name "Windows-Server-2012-R2-Important-and-Critical-Security-Updates"
```

Windows Server

```
aws ssm update-patch-baseline ^
```

```
    --baseline-id pb-0c10e65780EXAMPLE ^
    --name "Windows-Server-2012-R2-Important-and-Critical-Security-Updates"
```

システムが以下のような情報をレスポンスします。

```
{
   "BaselineId":"pb-0c10e65780EXAMPLE",
   "Name":"Windows-Server-2012-R2-Important-and-Critical-Security-Updates",
   "RejectedPatches":[
      "KB2032276",
      "MS10-048"
   ],
   "GlobalFilters":{
      "PatchFilters":[

      ]
   },
   "ApprovalRules":{
      "PatchRules":[
         {
            "PatchFilterGroup":{
               "PatchFilters":[
                  {
                     "Values":[
                        "Important",
                        "Critical"
                     ],
                     "Key":"MSRC_SEVERITY"
                  },
                  {
                     "Values":[
                        "SecurityUpdates"
                     ],
                     "Key":"CLASSIFICATION"
                  },
                  {
                     "Values":[
                        "WindowsServer2012R2"
                     ],
                     "Key":"PRODUCT"
                  }
               ]
```

```
            },
            "ApproveAfterDays":5
         }
      ]
   },
   "ModifiedDate":1481001795.287,
   "CreatedDate":1480997823.81,
   "ApprovedPatches":[
      "KB2124261"
   ],
   "Description":"Windows Server 2012 R2, Important and Critical security updates"
}
```

パッチベースラインの削除

```
aws ssm delete-patch-baseline --baseline-id "pb-0c10e65780EXAMPLE"
```

システムが以下のような情報を返します。

```
{
   "BaselineId":"pb-0c10e65780EXAMPLE"
}
```

すべてのパッチベースラインのリストアップ

```
aws ssm describe-patch-baselines
```

システムが以下のような情報を返します。

```
{
   "BaselineIdentities":[
      {
         "BaselineName":"AWS-DefaultPatchBaseline",
         "DefaultBaseline":true,
         "BaselineDescription":"Default Patch Baseline Provided by AWS.",
         "BaselineId":"arn:aws:ssm:us-east-2:111122223333:patchbaseline/
pb-0c10e65780EXAMPLE"
      },
      {
         "BaselineName":"Windows-Server-2012R2",
         "DefaultBaseline":false,
```

```
         "BaselineDescription":"Windows Server 2012 R2, Important and Critical security
 updates",
         "BaselineId":"pb-0c10e65780EXAMPLE"
      }
   ]
}
```

次に示すのは、 内のすべてのパッチベースラインをリストアップする別のコマンドですAWS リージョン

Linux & macOS

```
aws ssm describe-patch-baselines \
    --region us-east-2 \
    --filters "Key=OWNER,Values=[All]"
```

Windows Server

```
aws ssm describe-patch-baselines ^
    --region us-east-2 ^
    --filters "Key=OWNER,Values=[All]"
```

システムが以下のような情報をレスポンスします。

```
{
   "BaselineIdentities":[
      {
         "BaselineName":"AWS-DefaultPatchBaseline",
         "DefaultBaseline":true,
         "BaselineDescription":"Default Patch Baseline Provided by AWS.",
         "BaselineId":"arn:aws:ssm:us-east-2:111122223333:patchbaseline/
pb-0c10e65780EXAMPLE"
      },
      {
         "BaselineName":"Windows-Server-2012R2",
         "DefaultBaseline":false,
         "BaselineDescription":"Windows Server 2012 R2, Important and Critical security
 updates",
         "BaselineId":"pb-0c10e65780EXAMPLE"
      }
   ]
```

```
}
```

すべての AWS 提供のパッチベースラインのリストアップ

Linux & macOS

```
aws ssm describe-patch-baselines \
    --region us-east-2 \
    --filters "Key=OWNER,Values=[AWS]"
```

Windows Server

```
aws ssm describe-patch-baselines ^
    --region us-east-2 ^
    --filters "Key=OWNER,Values=[AWS]"
```

システムが以下のような情報をレスポンスします。

```
{
   "BaselineIdentities":[
      {
         "BaselineName":"AWS-DefaultPatchBaseline",
         "DefaultBaseline":true,
         "BaselineDescription":"Default Patch Baseline Provided by AWS.",
         "BaselineId":"arn:aws:ssm:us-east-2:111122223333:patchbaseline/
pb-0c10e65780EXAMPLE"
      }
   ]
}
```

ユーザーのパッチベースラインのリストアップ

Linux & macOS

```
aws ssm describe-patch-baselines \
    --region us-east-2 \
    --filters "Key=OWNER,Values=[Self]"
```

Windows Server

```
aws ssm describe-patch-baselines ^
```

```
    --region us-east-2 ^
    --filters "Key=OWNER,Values=[Self]"
```

システムが以下のような情報をレスポンスします。

```
{
   "BaselineIdentities":[
      {
         "BaselineName":"Windows-Server-2012R2",
         "DefaultBaseline":false,
         "BaselineDescription":"Windows Server 2012 R2, Important and Critical security
 updates",
         "BaselineId":"pb-0c10e65780EXAMPLE"
      }
   ]
}
```

パッチベースラインの表示

```
aws ssm get-patch-baseline --baseline-id pb-0c10e65780EXAMPLE
```

> **Note**
>
> カスタムパッチベースラインについては、パッチベースライン ID か完全な Amazon リソースネーム (ARN) のどちらかを指定できます。AWS 提供のパッチベースラインについては、完全な ARN を指定する必要があります。例えば、`arn:aws:ssm:us-east-2:075727635805:patchbaseline/pb-0c10e65780EXAMPLE` と指定します。

システムが以下のような情報を返します。

```
{
   "BaselineId":"pb-0c10e65780EXAMPLE",
   "Name":"Windows-Server-2012R2",
   "PatchGroups":[
      "Web Servers"
   ],
   "RejectedPatches":[

   ],
```

```
   "GlobalFilters":{
      "PatchFilters":[

      ]
   },
   "ApprovalRules":{
      "PatchRules":[
         {
            "PatchFilterGroup":{
               "PatchFilters":[
                  {
                     "Values":[
                        "Important",
                        "Critical"
                     ],
                     "Key":"MSRC_SEVERITY"
                  },
                  {
                     "Values":[
                        "SecurityUpdates"
                     ],
                     "Key":"CLASSIFICATION"
                  },
                  {
                     "Values":[
                        "WindowsServer2012R2"
                     ],
                     "Key":"PRODUCT"
                  }
               ]
            },
            "ApproveAfterDays":5
         }
      ]
   },
   "ModifiedDate":1480997823.81,
   "CreatedDate":1480997823.81,
   "ApprovedPatches":[

   ],
   "Description":"Windows Server 2012 R2, Important and Critical security updates"
}
```

デフォルトパッチベースラインの取得

```
aws ssm get-default-patch-baseline --region us-east-2
```

システムが以下のような情報を返します。

```
{
   "BaselineId":"arn:aws:ssm:us-east-2:111122223333:patchbaseline/pb-0c10e65780EXAMPLE"
}
```

カスタムパッチベースラインをデフォルトとして設定する

Linux & macOS

```
aws ssm register-default-patch-baseline \
    --region us-east-2 \
    --baseline-id "pb-0c10e65780EXAMPLE"
```

Windows Server

```
aws ssm register-default-patch-baseline ^
    --region us-east-2 ^
    --baseline-id "pb-0c10e65780EXAMPLE"
```

システムが以下のような情報をレスポンスします。

```
{
   "BaselineId":"pb-0c10e65780EXAMPLE"
}
```

AWS パッチベースラインをデフォルトとしてリセットする

Linux & macOS

```
aws ssm register-default-patch-baseline \
    --region us-east-2 \
    --baseline-id "arn:aws:ssm:us-east-2:123456789012:patchbaseline/
pb-0c10e65780EXAMPLE"
```

Windows Server

```
aws ssm register-default-patch-baseline ^
    --region us-east-2 ^
    --baseline-id "arn:aws:ssm:us-east-2:123456789012:patchbaseline/
pb-0c10e65780EXAMPLE"
```

システムが以下のような情報をレスポンスします。

```
{
   "BaselineId":"pb-0c10e65780EXAMPLE"
}
```

パッチベースラインのタグ付け

Linux & macOS

```
aws ssm add-tags-to-resource \
    --resource-type "PatchBaseline" \
    --resource-id "pb-0c10e65780EXAMPLE" \
    --tags "Key=Project,Value=Testing"
```

Windows Server

```
aws ssm add-tags-to-resource ^
    --resource-type "PatchBaseline" ^
    --resource-id "pb-0c10e65780EXAMPLE" ^
    --tags "Key=Project,Value=Testing"
```

パッチベースラインのタグのリストアップ

Linux & macOS

```
aws ssm list-tags-for-resource \
    --resource-type "PatchBaseline" \
    --resource-id "pb-0c10e65780EXAMPLE"
```

Windows Server

```
aws ssm list-tags-for-resource ^
```

```
    --resource-type "PatchBaseline" ^
    --resource-id "pb-0c10e65780EXAMPLE"
```

パッチベースラインからのタグの削除

Linux & macOS

```
aws ssm remove-tags-from-resource \
    --resource-type "PatchBaseline" \
    --resource-id "pb-0c10e65780EXAMPLE" \
    --tag-keys "Project"
```

Windows Server

```
aws ssm remove-tags-from-resource ^
    --resource-type "PatchBaseline" ^
    --resource-id "pb-0c10e65780EXAMPLE" ^
    --tag-keys "Project"
```

パッチグループの AWS CLI コマンド

パッチグループのサンプルコマンド

- パッチグループの作成
- パッチグループ "ウェブサーバー" のパッチベースラインへの登録
- パッチグループ "バックエンド" の AWS 提供のパッチベースラインへの登録
- パッチグループの登録の表示
- パッチグループのパッチベースラインからの登録解除

パッチグループの作成

> **Note**
>
> パッチグループは、パッチポリシーに基づくパッチ適用オペレーションでは使用されません。パッチポリシーの使用については、「Quick Setup でのパッチポリシー設定」を参照してください。

パッチ適用の仕組みを整理するため、タグを使用してマネージドノードをパッチグループに追加することをお勧めします。パッチグループでは、タグキー Patch Group または PatchGroup を使用する必要があります。EC2 インスタンスのメタデータでタグを許可している場合は、スペースなしで PatchGroup を使用する必要があります。任意のタグ値を指定できますが、タグキーは Patch Group または PatchGroup とする必要があります。パッチグループの詳細については、「パッチグループ」を参照してください。

タグを使用してマネージドノードをグループ化する場合、パッチグループの値をパッチベースラインに追加します。パッチグループをパッチベースラインに登録することで、パッチ適用の実行時に正しいパッチがインストールされます。

タスク 1: タグを使用したパッチグループに EC2 インスタンスを追加する

> **Note**
>
> Amazon Elastic Compute Cloud (Amazon EC2) コンソールと AWS CLI を使用する場合、Systems Manager で使用するためにまだ設定されていないインスタンスに Key = Patch Group または Key = PatchGroup タグを適用できます。Patch Group または Key = PatchGroup タグを適用しても Patch Manager に表示されるはずの EC2 インスタンスが表示されない場合は、マネージドノードの可用性のトラブルシューティング でトラブルシューティングのヒントを参照してください。

次のコマンドを実行して、EC2 インスタンスに PatchGroup タグを追加します。

```
aws ec2 create-tags --resources "i-1234567890abcdef0" --tags
 "Key=PatchGroup,Value=GroupValue"
```

タスク 2: タグを使用してパッチグループをマネージドノードに追加する

次のコマンドを実行して、マネージドノードに PatchGroup タグを追加します。

Linux & macOS

```
aws ssm add-tags-to-resource \
    --resource-type "ManagedInstance" \
    --resource-id "mi-0123456789abcdefg" \
    --tags "Key=PatchGroup,Value=GroupValue"
```

Windows Server

```
aws ssm add-tags-to-resource ^
    --resource-type "ManagedInstance" ^
    --resource-id "mi-0123456789abcdefg" ^
    --tags "Key=PatchGroup,Value=GroupValue"
```

タスク 3: パッチベースラインにパッチグループを追加します。

次のコマンドを実行して、PatchGroup タグ値を指定されたパッチベースラインに関連付けます。

Linux & macOS

```
aws ssm register-patch-baseline-for-patch-group \
    --baseline-id "pb-0c10e65780EXAMPLE" \
    --patch-group "Development"
```

Windows Server

```
aws ssm register-patch-baseline-for-patch-group ^
    --baseline-id "pb-0c10e65780EXAMPLE" ^
    --patch-group "Development"
```

システムが以下のような情報をレスポンスします。

```
{
  "PatchGroup": "Development",
  "BaselineId": "pb-0c10e65780EXAMPLE"
}
```

パッチグループ "ウェブサーバー" のパッチベースラインへの登録

Linux & macOS

```
aws ssm register-patch-baseline-for-patch-group \
    --baseline-id "pb-0c10e65780EXAMPLE" \
    --patch-group "Web Servers"
```

Windows Server

```
aws ssm register-patch-baseline-for-patch-group ^
    --baseline-id "pb-0c10e65780EXAMPLE" ^
    --patch-group "Web Servers"
```

システムが以下のような情報をレスポンスします。

```
{
   "PatchGroup":"Web Servers",
   "BaselineId":"pb-0c10e65780EXAMPLE"
}
```

パッチグループ "バックエンド" の AWS 提供のパッチベースラインへの登録

Linux & macOS

```
aws ssm register-patch-baseline-for-patch-group \
    --region us-east-2 \
    --baseline-id "arn:aws:ssm:us-east-2:111122223333:patchbaseline/
pb-0c10e65780EXAMPLE" \
    --patch-group "Backend"
```

Windows Server

```
aws ssm register-patch-baseline-for-patch-group ^
    --region us-east-2 ^
    --baseline-id "arn:aws:ssm:us-east-2:111122223333:patchbaseline/
pb-0c10e65780EXAMPLE" ^
    --patch-group "Backend"
```

システムが以下のような情報をレスポンスします。

```
{
   "PatchGroup":"Backend",
   "BaselineId":"arn:aws:ssm:us-east-2:111122223333:patchbaseline/pb-0c10e65780EXAMPLE"
}
```

パッチグループの登録の表示

```
aws ssm describe-patch-groups --region us-east-2
```

システムが以下のような情報を返します。

```
{
   "PatchGroupPatchBaselineMappings":[
      {
         "PatchGroup":"Backend",
         "BaselineIdentity":{
            "BaselineName":"AWS-DefaultPatchBaseline",
            "DefaultBaseline":false,
            "BaselineDescription":"Default Patch Baseline Provided by AWS.",
            "BaselineId":"arn:aws:ssm:us-east-2:111122223333:patchbaseline/
pb-0c10e65780EXAMPLE"
         }
      },
      {
         "PatchGroup":"Web Servers",
         "BaselineIdentity":{
            "BaselineName":"Windows-Server-2012R2",
            "DefaultBaseline":true,
            "BaselineDescription":"Windows Server 2012 R2, Important and Critical
 updates",
            "BaselineId":"pb-0c10e65780EXAMPLE"
         }
      }
   ]
}
```

パッチグループのパッチベースラインからの登録解除

Linux & macOS

```
aws ssm deregister-patch-baseline-for-patch-group \
    --region us-east-2 \
    --patch-group "Production" \
    --baseline-id "arn:aws:ssm:us-east-2:111122223333:patchbaseline/
pb-0c10e65780EXAMPLE"
```

Windows Server

```
aws ssm deregister-patch-baseline-for-patch-group ^
    --region us-east-2 ^
    --patch-group "Production" ^
    --baseline-id "arn:aws:ssm:us-east-2:111122223333:patchbaseline/
pb-0c10e65780EXAMPLE"
```

システムが以下のような情報をレスポンスします。

```
{
   "PatchGroup":"Production",
   "BaselineId":"arn:aws:ssm:us-east-2:111122223333:patchbaseline/pb-0c10e65780EXAMPLE"
}
```

パッチの概要と詳細を表示するための AWS CLI コマンド

パッチの概要と詳細を表示するためのサンプルコマンド

- パッチベースラインで定義されているすべてのパッチの取得
- AmazonLinux2018.03 の分類が SECURITY で重大度が Critical のすべてのパッチの取得
- MSRC の重要度が「 Critical 」である Windows Server 2012 のすべてのパッチを取得する
- すべての利用可能なパッチの取得
- マネージドノードごとのパッチの概要の状態を取得
- マネージドノードのパッチコンプライアンスの詳細の取得
- パッチコンプライアンス結果の表示 (AWS CLI)

パッチベースラインで定義されているすべてのパッチの取得

> **Note**
>
> このコマンドは、Windows Server のパッチベースラインでのみサポートされています。

Linux & macOS

```
aws ssm describe-effective-patches-for-patch-baseline \
```

```
    --region us-east-2 \
    --baseline-id "pb-0c10e65780EXAMPLE"
```

Windows Server

```
aws ssm describe-effective-patches-for-patch-baseline ^
    --region us-east-2 ^
    --baseline-id "pb-0c10e65780EXAMPLE"
```

システムが以下のような情報をレスポンスします。

```
{
   "NextToken":"--token string truncated--",
   "EffectivePatches":[
      {
         "PatchStatus":{
            "ApprovalDate":1384711200.0,
            "DeploymentStatus":"APPROVED"
         },
         "Patch":{
            "ContentUrl":"https://support.microsoft.com/en-us/kb/2876331",
            "ProductFamily":"Windows",
            "Product":"WindowsServer2012R2",
            "Vendor":"Microsoft",
            "Description":"A security issue has been identified in a Microsoft
 software
               product that could affect your system. You can help protect your system
               by installing this update from Microsoft. For a complete listing of the
               issues that are included in this update, see the associated Microsoft
               Knowledge Base article. After you install this update, you may have to
               restart your system.",
            "Classification":"SecurityUpdates",
            "Title":"Security Update for Windows Server 2012 R2 Preview (KB2876331)",
            "ReleaseDate":1384279200.0,
            "MsrcClassification":"Critical",
            "Language":"All",
            "KbNumber":"KB2876331",
            "MsrcNumber":"MS13-089",
            "Id":"e74ccc76-85f0-4881-a738-59e9fc9a336d"
         }
      },
      {
```

```
        "PatchStatus":{
           "ApprovalDate":1428858000.0,
           "DeploymentStatus":"APPROVED"
        },
        "Patch":{
           "ContentUrl":"https://support.microsoft.com/en-us/kb/2919355",
           "ProductFamily":"Windows",
           "Product":"WindowsServer2012R2",
           "Vendor":"Microsoft",
           "Description":"Windows Server 2012 R2 Update is a cumulative
              set of security updates, critical updates and updates. You
              must install Windows Server 2012 R2 Update to ensure that
              your computer can continue to receive future Windows Updates,
              including security updates. For a complete listing of the
              issues that are included in this update, see the associated
              Microsoft Knowledge Base article for more information. After
              you install this item, you may have to restart your computer.",
           "Classification":"SecurityUpdates",
           "Title":"Windows Server 2012 R2 Update (KB2919355)",
           "ReleaseDate":1428426000.0,
           "MsrcClassification":"Critical",
           "Language":"All",
           "KbNumber":"KB2919355",
           "MsrcNumber":"MS14-018",
           "Id":"8452bac0-bf53-4fbd-915d-499de08c338b"
        }
     }
    ---output truncated---
```

AmazonLinux2018.03 の分類が **SECURITY** で重大度が **Critical** のすべてのパッチの取得

Linux & macOS

```
aws ssm describe-available-patches \
    --region us-east-2 \
    --filters Key=PRODUCT,Values=AmazonLinux2018.03 Key=SEVERITY,Values=Critical
```

Windows Server

```
aws ssm describe-available-patches ^
    --region us-east-2 ^
    --filters Key=PRODUCT,Values=AmazonLinux2018.03 Key=SEVERITY,Values=Critical
```

システムが以下のような情報をレスポンスします。

```
{
    "Patches": [
        {
            "AdvisoryIds": ["ALAS-2011-1"],
            "BugzillaIds": [ "1234567" ],
            "Classification": "SECURITY",
            "CVEIds": [ "CVE-2011-3192"],
            "Name": "zziplib",
            "Epoch": "0",
            "Version": "2.71",
            "Release": "1.3.amzn1",
            "Arch": "i686",
            "Product": "AmazonLinux2018.03",
            "ReleaseDate": 1590519815,
            "Severity": "CRITICAL"
        }
    ]
}
---output truncated---
```

MSRC の重要度が「**Critical**」である Windows Server 2012 のすべてのパッチを取得する

Linux & macOS

```
aws ssm describe-available-patches \
    --region us-east-2 \
    --filters Key=PRODUCT,Values=WindowsServer2012 Key=MSRC_SEVERITY,Values=Critical
```

Windows Server

```
aws ssm describe-available-patches ^
    --region us-east-2 ^
    --filters Key=PRODUCT,Values=WindowsServer2012 Key=MSRC_SEVERITY,Values=Critical
```

システムが以下のような情報をレスポンスします。

```
{
   "Patches":[
      {
```

```
         "ContentUrl":"https://support.microsoft.com/en-us/kb/2727528",
         "ProductFamily":"Windows",
         "Product":"WindowsServer2012",
         "Vendor":"Microsoft",
         "Description":"A security issue has been identified that could
           allow an unauthenticated remote attacker to compromise your
           system and gain control over it. You can help protect your
           system by installing this update from Microsoft. After you
           install this update, you may have to restart your system.",
         "Classification":"SecurityUpdates",
         "Title":"Security Update for Windows Server 2012 (KB2727528)",
         "ReleaseDate":1352829600.0,
         "MsrcClassification":"Critical",
         "Language":"All",
         "KbNumber":"KB2727528",
         "MsrcNumber":"MS12-072",
         "Id":"1eb507be-2040-4eeb-803d-abc55700b715"
      },
      {
         "ContentUrl":"https://support.microsoft.com/en-us/kb/2729462",
         "ProductFamily":"Windows",
         "Product":"WindowsServer2012",
         "Vendor":"Microsoft",
         "Description":"A security issue has been identified that could
           allow an unauthenticated remote attacker to compromise your
           system and gain control over it. You can help protect your
           system by installing this update from Microsoft. After you
           install this update, you may have to restart your system.",
         "Classification":"SecurityUpdates",
         "Title":"Security Update for Microsoft .NET Framework 3.5 on
           Windows 8 and Windows Server 2012 for x64-based Systems (KB2729462)",
         "ReleaseDate":1352829600.0,
         "MsrcClassification":"Critical",
         "Language":"All",
         "KbNumber":"KB2729462",
         "MsrcNumber":"MS12-074",
         "Id":"af873760-c97c-4088-ab7e-5219e120eab4"
      }

---output truncated---
```

すべての利用可能なパッチの取得

```
aws ssm describe-available-patches --region us-east-2
```

システムが以下のような情報をレスポンスします。


```
{
   "NextToken":"--token string truncated--",
   "Patches":[
      {
         "ContentUrl":"https://support.microsoft.com/en-us/kb/2032276",
         "ProductFamily":"Windows",
         "Product":"WindowsServer2008R2",
         "Vendor":"Microsoft",
         "Description":"A security issue has been identified that could allow an
           unauthenticated remote attacker to compromise your system and gain
           control over it. You can help protect your system by installing this
           update from Microsoft. After you install this update, you may have to
           restart your system.",
         "Classification":"SecurityUpdates",
         "Title":"Security Update for Windows Server 2008 R2 x64 Edition (KB2032276)",
         "ReleaseDate":1279040400.0,
         "MsrcClassification":"Important",
         "Language":"All",
         "KbNumber":"KB2032276",
         "MsrcNumber":"MS10-043",
         "Id":"8692029b-a3a2-4a87-a73b-8ea881b4b4d6"
      },
      {
         "ContentUrl":"https://support.microsoft.com/en-us/kb/2124261",
         "ProductFamily":"Windows",
         "Product":"Windows7",
         "Vendor":"Microsoft",
         "Description":"A security issue has been identified that could allow
           an unauthenticated remote attacker to compromise your system and gain
           control over it. You can help protect your system by installing this
           update from Microsoft. After you install this update, you may have
           to restart your system.",
         "Classification":"SecurityUpdates",
         "Title":"Security Update for Windows 7 (KB2124261)",
         "ReleaseDate":1284483600.0,
         "MsrcClassification":"Important",
         "Language":"All",
```

```
         "KbNumber":"KB2124261",
         "MsrcNumber":"MS10-065",
         "Id":"12ef1bed-0dd2-4633-b3ac-60888aa8ba33"
      }
      ---output truncated---
```

マネージドノードごとのパッチの概要の状態を取得

マネージドノードごとの概要により、ノードごとに状態が「NotApplicable」、「Missing」、「Failed」、「InstalledOther」、「Installed」に該当するパッチの数を確認できます。

Linux & macOS

```
aws ssm describe-instance-patch-states \
    --instance-ids i-08ee91c0b17045407 i-09a618aec652973a9
```

Windows Server

```
aws ssm describe-instance-patch-states ^
    --instance-ids i-08ee91c0b17045407 i-09a618aec652973a9
```

システムが以下のような情報をレスポンスします。

```
{
   "InstancePatchStates":[
      {
            "InstanceId": "i-08ee91c0b17045407",
            "PatchGroup": "",
            "BaselineId": "pb-0c10e65780EXAMPLE",
            "SnapshotId": "6d03d6c5-f79d-41d0-8d0e-00a9aEXAMPLE",
            "InstalledCount": 50,
            "InstalledOtherCount": 353,
            "InstalledPendingRebootCount": 0,
            "InstalledRejectedCount": 0,
            "MissingCount": 0,
            "FailedCount": 0,
            "UnreportedNotApplicableCount": -1,
            "NotApplicableCount": 671,
            "OperationStartTime": "2020-01-24T12:37:56-08:00",
            "OperationEndTime": "2020-01-24T12:37:59-08:00",
            "Operation": "Scan",
```

```
            "RebootOption": "NoReboot"
        },
        {
            "InstanceId": "i-09a618aec652973a9",
            "PatchGroup": "",
            "BaselineId": "pb-0c10e65780EXAMPLE",
            "SnapshotId": "c7e0441b-1eae-411b-8aa7-973e6EXAMPLE",
            "InstalledCount": 36,
            "InstalledOtherCount": 396,
            "InstalledPendingRebootCount": 0,
            "InstalledRejectedCount": 0,
            "MissingCount": 3,
            "FailedCount": 0,
            "UnreportedNotApplicableCount": -1,
            "NotApplicableCount": 420,
            "OperationStartTime": "2020-01-24T12:37:34-08:00",
            "OperationEndTime": "2020-01-24T12:37:37-08:00",
            "Operation": "Scan",
            "RebootOption": "NoReboot"
        }
    ---output truncated---
```

マネージドノードのパッチコンプライアンスの詳細の取得

```
aws ssm describe-instance-patches --instance-id i-08ee91c0b17045407
```

システムが以下のような情報をレスポンスします。

```
{
   "NextToken":"--token string truncated--",
   "Patches":[
      {
            "Title": "bind-libs.x86_64:32:9.8.2-0.68.rc1.60.amzn1",
            "KBId": "bind-libs.x86_64",
            "Classification": "Security",
            "Severity": "Important",
            "State": "Installed",
            "InstalledTime": "2019-08-26T11:05:24-07:00"
        },
        {
            "Title": "bind-utils.x86_64:32:9.8.2-0.68.rc1.60.amzn1",
            "KBId": "bind-utils.x86_64",
            "Classification": "Security",
```

```
            "Severity": "Important",
            "State": "Installed",
            "InstalledTime": "2019-08-26T11:05:32-07:00"
        },
        {
            "Title": "dhclient.x86_64:12:4.1.1-53.P1.28.amzn1",
            "KBId": "dhclient.x86_64",
            "Classification": "Security",
            "Severity": "Important",
            "State": "Installed",
            "InstalledTime": "2019-08-26T11:05:31-07:00"
        },
    ---output truncated---
```

パッチコンプライアンス結果の表示 (AWS CLI)

1 つのマネージドノードノードのパッチコンプライアンスの結果を表示する

1 つのマネージドノードノードのパッチコンプライアンスの結果を表示するには、AWS Command Line Interface (AWS CLI) で次のコマンドを実行します。

```
aws ssm describe-instance-patch-states --instance-id instance-id
```

instance-id を、結果を確認するマネージドノードの ID に、i-02573cafcfEXAMPLE または mi-0282f7c436EXAMPLE の形式で置き換えます。

以下のような情報が返されます。

```
{
    "InstancePatchStates": [
        {
            "InstanceId": "i-02573cafcfEXAMPLE",
            "PatchGroup": "mypatchgroup",
            "BaselineId": "pb-0c10e65780EXAMPLE",
            "SnapshotId": "a3f5ff34-9bc4-4d2c-a665-4d1c1EXAMPLE",
            "CriticalNonCompliantCount": 2,
            "SecurityNonCompliantCount": 2,
            "OtherNonCompliantCount": 1,
            "InstalledCount": 123,
            "InstalledOtherCount": 334,
            "InstalledPendingRebootCount": 0,
            "InstalledRejectedCount": 0,
```

```
            "MissingCount": 1,
            "FailedCount": 2,
            "UnreportedNotApplicableCount": 11,
            "NotApplicableCount": 2063,
            "OperationStartTime": "2021-05-03T11:00:56-07:00",
            "OperationEndTime": "2021-05-03T11:01:09-07:00",
            "Operation": "Scan",
            "LastNoRebootInstallOperationTime": "2020-06-14T12:17:41-07:00",
            "RebootOption": "RebootIfNeeded"
        }
    ]
}
```

リージョン内のすべての EC2 インスタンスのパッチ数の概要を表示するには

describe-instance-patch-states は、一度に 1 つのマネージドインスタンスの結果の取得をサポートします。ただし、describe-instance-patch-states コマンドでカスタムスクリプトを使用すると、より詳細なレポートを生成できます。

例えば、jq フィルターツールがローカルマシンにインストールされている場合、次のコマンドを実行して、特定の AWS リージョン のどの EC2 インスタンスのステータスが InstalledPendingReboot であるかを特定できます。

```
aws ssm describe-instance-patch-states \
    --instance-ids $(aws ec2 describe-instances --region region | jq
 '.Reservations[].Instances[] | .InstanceId' | tr '\n|"' ' ') \
    --output text --query 'InstancePatchStates[*].{Instance:InstanceId,
 InstalledPendingRebootCount:InstalledPendingRebootCount}'
```

region は、米国東部 (オハイオ) リージョンの us-east-2 のように、AWS Systems Manager でサポートされている AWS リージョン の識別子を表します。サポートされている *region* 値の一覧については、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」にある Region 列を参照してください。

例：

```
aws ssm describe-instance-patch-states \
    --instance-ids $(aws ec2 describe-instances --region us-east-2 | jq
 '.Reservations[].Instances[] | .InstanceId' | tr '\n|"' ' ') \
    --output text --query 'InstancePatchStates[*].{Instance:InstanceId,
 InstalledPendingRebootCount:InstalledPendingRebootCount}'
```

システムが以下のような情報を返します。

```
1       i-02573cafcfEXAMPLE
0       i-0471e04240EXAMPLE
3       i-07782c72faEXAMPLE
6       i-083b678d37EXAMPLE
0       i-03a530a2d4EXAMPLE
1       i-01f68df0d0EXAMPLE
0       i-0a39c0f214EXAMPLE
7       i-0903a5101eEXAMPLE
7       i-03823c2fedEXAMPLE
```

InstalledPendingRebootCount に加えて、検索できるカウントタイプのリストには次のものが含まれます。

- CriticalNonCompliantCount
- SecurityNonCompliantCount
- OtherNonCompliantCount
- UnreportedNotApplicableCount
- InstalledPendingRebootCount
- FailedCount
- NotApplicableCount
- InstalledRejectedCount
- InstalledOtherCount
- MissingCount
- InstalledCount

AWS CLI マネージドノードのスキャンとパッチ適用のためのコマンド

次のコマンドを実行してパッチコンプライアンスをスキャンするか、パッチをインストールした後、「パッチの概要と詳細を表示するための AWS CLI コマンド」セクションのコマンドを使用して、パッチのステータスおよびコンプライアンスに関する情報を表示できます。

サンプルコマンド

- マネージドノードをスキャンしてパッチコンプライアンスを確認する (AWS CLI)
- マネージドノードへのパッチのインストール (AWS CLI)

マネージドノードをスキャンしてパッチコンプライアンスを確認する (AWS CLI)

特定のマネージドノードをスキャンしてパッチコンプライアンスを確認するには

以下のコマンドを実行してください。

Linux & macOS

```
aws ssm send-command \
    --document-name 'AWS-RunPatchBaseline' \
    --targets Key=InstanceIds,Values='i-02573cafcfEXAMPLE,i-0471e04240EXAMPLE' \
    --parameters 'Operation=Scan' \
    --timeout-seconds 600
```

Windows Server

```
aws ssm send-command ^
    --document-name "AWS-RunPatchBaseline" ^
    --targets Key=InstanceIds,Values="i-02573cafcfEXAMPLE,i-0471e04240EXAMPLE" ^
    --parameters "Operation=Scan" ^
    --timeout-seconds 600
```

システムが以下のような情報をレスポンスします。

```
{
    "Command": {
        "CommandId": "a04ed06c-8545-40f4-87c2-a0babEXAMPLE",
        "DocumentName": "AWS-RunPatchBaseline",
        "DocumentVersion": "$DEFAULT",
        "Comment": "",
        "ExpiresAfter": 1621974475.267,
        "Parameters": {
            "Operation": [
                "Scan"
            ]
        },
        "InstanceIds": [],
        "Targets": [
            {
                "Key": "InstanceIds",
                "Values": [
                    "i-02573cafcfEXAMPLE,
```

```
                    i-0471e04240EXAMPLE"
                ]
            }
        ],
        "RequestedDateTime": 1621952275.267,
        "Status": "Pending",
        "StatusDetails": "Pending",
        "TimeoutSeconds": 600,

    ---output truncated---

    }
}
```

パッチグループタグでマネージドノードをスキャンしてパッチコンプライアンスを確認するには

以下のコマンドを実行してください。

Linux & macOS

```
aws ssm send-command \
    --document-name 'AWS-RunPatchBaseline' \
    --targets Key='tag:PatchGroup',Values='Web servers' \
    --parameters 'Operation=Scan' \
    --timeout-seconds 600
```

Windows Server

```
aws ssm send-command ^
    --document-name "AWS-RunPatchBaseline" ^
    --targets Key="tag:PatchGroup",Values="Web servers" ^
    --parameters "Operation=Scan" ^
    --timeout-seconds 600
```

システムが以下のような情報をレスポンスします。

```
{
    "Command": {
        "CommandId": "87a448ee-8adc-44e0-b4d1-6b429EXAMPLE",
        "DocumentName": "AWS-RunPatchBaseline",
        "DocumentVersion": "$DEFAULT",
        "Comment": "",
```

```
        "ExpiresAfter": 1621974983.128,
        "Parameters": {
            "Operation": [
                "Scan"
            ]
        },
        "InstanceIds": [],
        "Targets": [
            {
                "Key": "tag:PatchGroup",
                "Values": [
                    "Web servers"
                ]
            }
        ],
        "RequestedDateTime": 1621952783.128,
        "Status": "Pending",
        "StatusDetails": "Pending",
        "TimeoutSeconds": 600,

    ---output truncated---

    }
}
```

マネージドノードへのパッチのインストール (AWS CLI)

特定のマネージドノードにパッチをインストールするには

以下のコマンドを実行してください。

> **Note**
>
> パッチのインストールを完了するために、ターゲット マネージドノードは必要に応じて再起動します。詳細については、「パッチ適用のための SSM コマンドドキュメント: AWS-RunPatchBaseline」を参照してください。

Linux & macOS

```
aws ssm send-command \
    --document-name 'AWS-RunPatchBaseline' \
    --targets Key=InstanceIds,Values='i-02573cafcfEXAMPLE,i-0471e04240EXAMPLE' \
```

```
    --parameters 'Operation=Install' \
    --timeout-seconds 600
```

Windows Server

```
aws ssm send-command ^
    --document-name "AWS-RunPatchBaseline" ^
    --targets Key=InstanceIds,Values="i-02573cafcfEXAMPLE,i-0471e04240EXAMPLE" ^
    --parameters "Operation=Install" ^
    --timeout-seconds 600
```

システムが以下のような情報をレスポンスします。

```
{
    "Command": {
        "CommandId": "5f403234-38c4-439f-a570-93623EXAMPLE",
        "DocumentName": "AWS-RunPatchBaseline",
        "DocumentVersion": "$DEFAULT",
        "Comment": "",
        "ExpiresAfter": 1621975301.791,
        "Parameters": {
            "Operation": [
                "Install"
            ]
        },
        "InstanceIds": [],
        "Targets": [
            {
                "Key": "InstanceIds",
                "Values": [
                    "i-02573cafcfEXAMPLE,
                     i-0471e04240EXAMPLE"
                ]
            }
        ],
        "RequestedDateTime": 1621953101.791,
        "Status": "Pending",
        "StatusDetails": "Pending",
        "TimeoutSeconds": 600,

    ---output truncated---
```

```
    }
}
```

特定のパッチグループのマネージドノードにパッチをインストールするには

以下のコマンドを実行してください。

Linux & macOS

```
aws ssm send-command \
    --document-name 'AWS-RunPatchBaseline' \
    --targets Key='tag:PatchGroup',Values='Web servers' \
    -parameters 'Operation=Install' \
    --timeout-seconds 600
```

Windows Server

```
aws ssm send-command ^
    --document-name "AWS-RunPatchBaseline" ^
    --targets Key="tag:PatchGroup",Values="Web servers" ^
    --parameters "Operation=Install" ^
    --timeout-seconds 600
```

システムが以下のような情報をレスポンスします。

```
{
    "Command": {
        "CommandId": "fa44b086-7d36-4ad5-ac8d-627ecEXAMPLE",
        "DocumentName": "AWS-RunPatchBaseline",
        "DocumentVersion": "$DEFAULT",
        "Comment": "",
        "ExpiresAfter": 1621975407.865,
        "Parameters": {
            "Operation": [
                "Install"
            ]
        },
        "InstanceIds": [],
        "Targets": [
            {
                "Key": "tag:PatchGroup",
                "Values": [
```

```
                    "Web servers"
                ]
            }
        ],
        "RequestedDateTime": 1621953207.865,
        "Status": "Pending",
        "StatusDetails": "Pending",
        "TimeoutSeconds": 600,

    ---output truncated---

    }
}
```

AWS Systems Manager Patch Manager のチュートリアル

このセクションのチュートリアルでは、AWS Systems Manager のツールである Patch Manager をいくつかのパッチ適用シナリオで使用する方法を示します。

トピック

- チュートリアル: コンソールを使用して Windows サービスパックをインストールするためのパッチベースラインを作成する
- チュートリアル: アプリケーションの依存関係の更新、マネージドノードへのパッチ適用、およびアプリケーション固有のヘルスチェックの実行
- チュートリアル: AWS CLI を使用してサーバー環境にパッチを適用する

チュートリアル: コンソールを使用して Windows サービスパックをインストールするためのパッチベースラインを作成する

カスタムパッチベースラインを作成するときに、サポートされているパッチのすべて、一部、または 1 つのタイプのみをインストールするように指定できます。

Windows のパッチベースラインでは、パッチ適用の更新をサービスパックのみに制限するために、唯一の [分類] オプションとして `ServicePacks` を選択できます。サービスパックは、更新プログラムが Windows Update または Windows Server Update サービス (WSUS) で利用可能であれば、AWS Systems Manager のツールである Patch Manager によって自動的にインストールできます。

パッチベースラインを構成して、すべての Windows バージョンのサービスパックをインストールするか、Windows 7 や Windows Server 2016 などの特定のバージョンのサービスパックだけをインストールするかを制御できます。

Windows マネージドノードにすべてのサービスパックをインストールするためにのみ使用されるカスタム パッチベースラインを作成するには、以下の手順を使用します。

Windows サービスパックをインストールするためのパッチベースラインを作成するには (コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Patch Manager] を選択します。
3. [パッチベースライン] タブを選択し、[パッチベースラインの作成] を選択します。
4. [Name (名前)] フィールドに、新しいパッチベースラインの名前 (例: `MyWindowsServicePackPatchBaseline`) を入力します。
5. (オプション) [Description (説明)] に、パッチベースラインの説明を入力します。
6. [Operating system (オペレーティングシステム)] で、`Windows` を選択します。
7. 作成してすぐに、このパッチベースラインを Windows のデフォルトとして使用する場合は、[Set this patch baseline as the default patch baseline for Windows Server instances (このパッチベースラインを Windows Server インスタンスのデフォルトのパッチベースラインにする)] を選択します。

   > **Note**
   >
   > このオプションは、2022 年 12 月 22 日のパッチポリシーリリース前に初めて Patch Manager にアクセスした場合にのみ使用できます。
   > 既存のパッチベースラインのデフォルト設定の詳細については、「既存のパッチベースラインをデフォルトとして設定する」を参照してください。

8. [Approval rules for operating systems (オペレーティングシステムの承認ルール)] セクションで、フィールドを使用して 1 つ以上の自動承認ルールを作成します。

   - [製品]: 承認ルールが適用されるオペレーティングシステムのバージョン (`WindowsServer2012` など)。1 つ、複数、またはサポートされているすべてのバージョンの Windows を選択できます。デフォルトの選択は `All` です。
   - 分類: `ServicePacks` を選択します。
   - [Severity (重要度)]: ルールが適用されるパッチの重要度の値。ルールによってすべてのサービスパックが含まれるようにするには、`All` を選択します。
   - [Auto-approval (自動承認)]: 自動承認のためにパッチを選択する方法。

- [Approve patches after a specified number of days] (指定した日数後にパッチを承認): パッチがリリースまたは更新されてから、自動的に承認されるまで Patch Manager が待機する日数。ゼロ (0) から 360 の任意の整数を入力できます。ほとんどのシナリオでは、待機日数を 100 日以内にすることをお勧めします。
- [Approve patches released up to a specific date] (特定の日付までにリリースされたパッチを承認): Patch Manager がその日付以前にリリースまたは最後に更新されたすべてのパッチを自動的に適用するパッチのリリース日。例えば、2023 年 7 月 7 日を指定した場合、リリース日または最後の更新日が 2023 年 7 月 8 日以降であるパッチは、自動的にインストールされません。

- (オプション) [Compliance reporting (コンプライアンスレポート)]: ベースラインで承認されたサービスパックに割り当てる重要度 (`High` など)。

> **Note**
>
> コンプライアンスレポートレベルを指定し、承認されたサービスパックのパッチ状態が `Missing` として報告された場合、パッチベースラインで報告されるコンプライアンス全体の重要度は、指定した重要度レベルになります。

9. (オプション) [Manage tags (タグの管理)] で、1 つ以上のタグキーの名前と値のペアをパッチベースラインに適用します。

   タグは、リソースに割り当てるオプションのメタデータです。タグを使用すると、目的、所有者、環境などのさまざまな方法でリソースを分類できます。サービスパックの更新専用のこのパッチベースラインでは、次のようなキーと値のペアを指定できます。

   - `Key=OS,Value=Windows`
   - `Key=Classification,Value=ServicePacks`

10. [Create patch baseline] を選択します。

チュートリアル: アプリケーションの依存関係の更新、マネージドノードへのパッチ適用、およびアプリケーション固有のヘルスチェックの実行

多くの場合、マネージドノードは、最新のソフトウェア更新プログラムでパッチを適用した後に再起動する必要があります。ただし、安全対策を講じずに本番環境でノードを再起動すると、アラームの発動、不正なメトリクス データの記録、データ同期の中断など、いくつかの問題が発生する可能性があります。

このチュートリアルでは、AWS Systems Manager ドキュメント (SSM ドキュメント) AWS-RunPatchBaselineWithHooks を使用して、このような問題を回避する方法を学習します。これにより、複雑なマルチステップのパッチオペレーションを実現し、以下のことを達成できます。

1. アプリケーションへの新しい接続を防止
2. オペレーティングシステムの更新のインストール
3. アプリケーションのパッケージの依存関係の更新
4. システムの再起動
5. アプリケーション固有のヘルスチェックの実行

この例では、インフラストラクチャを次のようにセットアップしました。

- 対象の仮想マシンは、マネージドノードとして Systems Manager に登録されます。
- Iptables はローカルファイアウォールとして使用されます。
- マネージドノードでホストされているアプリケーションは、ポート 443 で実行されています。
- マネージドノードでホストされるアプリケーションは nodeJS アプリケーションです。
- マネージドノードでホストされるアプリケーションは、pm2 プロセスマネージャーによって管理されます。
- アプリケーションには、指定したヘルスチェックエンドポイントが既に存在します。
- アプリケーションのヘルスチェックエンドポイントは、エンドユーザー認証を必要としません。エンドポイントにより、可用性を確立する際に組織の要件を満たすヘルスチェックを行うことが可能になります。(実際の環境では、nodeJS アプリケーションが実行中であり、リクエストをリッスンできることを確認するだけで十分な場合があります。また、キャッシュレイヤーまたはデータベースレイヤーへの接続が既に確立されていることを確認する必要があります)。

このチュートリアルの例は、デモンストレーションのみを目的としており、本番環境にそのまま実装することを意図していません。また、Systems Manager のツールである Patch Manager のライフサイクルフック機能は、AWS-RunPatchBaselineWithHooks ドキュメントとともに他の多数のシナリオをサポートできることに注意してください。次にいくつかの例を示します。

- マネージドノードの再起動後にパッチを適用して再起動する前に、メトリクスレポート エージェントを停止します。
- パッチを適用する前に、CRM または PCS クラスターからマネージドノードをデタッチし、ノードの再起動後に再アタッチします。

- オペレーティングシステム (OS) の更新が適用された後、マネージドノードが再起動する前に、Windows Server マシン上のサードパーティーソフトウェア (Java、Tomcat、Adobe アプリケーションなど) を更新します。

アプリケーションの依存関係を更新し、マネージドノードにパッチを適用し、アプリケーション固有のヘルスチェックを実行するには

1. preinstallation スクリプトの SSM ドキュメントを次の内容で作成し、NodeJSAppPrePatch と名前を付けます。*your_application* をアプリケーションの名前に置き換えます。

   このスクリプトは、新しい受信リクエストを直ちにブロックし、既にアクティブなリクエストが完了するまで 5 秒間待ってからパッチ適用操作を開始します。sleep オプションでは、受信リクエストが完了するのに通常かかる秒数よりも長い秒数を指定します。

   ```
   # exit on error
   set -e
   # set up rule to block incoming traffic
   iptables -I INPUT -j DROP -p tcp --syn --destination-port 443 || exit 1
   # wait for current connections to end. Set timeout appropriate to your
    application's latency
   sleep 5
   # Stop your application
   pm2 stop your_application
   ```

   SSM ドキュメントの作成の詳細については、「SSM ドキュメントコンテンツを作成する」を参照してください。

2. postinstall スクリプト用に次の内容を含む別の SSM ドキュメントを作成し、アプリケーションの依存関係を更新し、NodeJSAppPostPatch と名前を付けます。*/your/application/path* をお使いのアプリケーションへのパスに置き換えます。

   ```
   cd /your/application/path
   npm update
   # you can use npm-check-updates if you want to upgrade major versions
   ```

3. アプリケーションをバックアップし、ヘルスチェックを実行するには、onExit スクリプト用に次の内容を含む別の SSM ドキュメントを作成します。この SSM ドキュメント NodeJSAppOnExitPatch の名前を付けます。*your_application* をアプリケーションの名前に置き換えます。

```
# exit on error
set -e
# restart nodeJs application
pm2 start your_application
# sleep while your application starts and to allow for a crash
sleep 10
# check with pm2 to see if your application is running
pm2 pid your_application
# re-enable incoming connections
iptables -D INPUT -j DROP -p tcp --syn --destination-port
# perform health check
/usr/bin/curl -m 10 -vk -A "" http://localhost:443/health-check || exit 1
```

4. AWS Systems Manager のツールである State Manager で関連付けを作成し、以下の手順を実行してオペレーションを発行します。

   1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
   2. ナビゲーションペインで、[State Manager] を選択し、[Create association (関連付けの作成)] を選択します。
   3. [Name (名前)] に、関連付けの目的を特定するのに役立つ名前を指定します。
   4. [Document (ドキュメント)] リストで、[AWS-RunPatchBaselineWithHooks] を選択します。
   5. [Operation (オペレーション)] で、[Install (インストール)] を選択します。
   6. (オプション) [Snapshot Id] では、GUID を指定します。これは、オペレーションの高速化と一貫性の確保のために生成します。この GUID は 00000000-0000-0000-0000-111122223333 と同じくらいシンプルです。
   7. [Pre Install Hook Doc Name (インストール前のフックドキュメント名)] に、「NodeJSAppPrePatch」と入力します。
   8. [Post Install Hook Doc Name (インストール後のフックドキュメント名)] に、「NodeJSAppPostPatch」と入力します。
   9. [On ExitHook Doc Name (ExitHook ドキュメント名)] に、「NodeJSAppOnExitPatch」と入力します。

5. [Targets] (ターゲット) では、タグの指定、ノードの手動選択、リソースグループの選択、またはすべてのマネージドノードの選択により、マネージドノードを特定します。

6. [Specify schedule (スケジュールの指定)] では、関連付けを実行する頻度を指定します。マネージドノードのパッチ適用では、週に 1 回が一般的な頻度です。
7. [Rate control] (レート制御) セクションで、複数のマネージドノードでの関連付けの実行方法を制御するオプションを選択します。一度に更新されるのは一部のマネージドノードであることを確認します。そうしないと、フリートのすべてまたはほとんどを同時にオフラインにすることになってしまいます。レート制御については、「State Manager 関連付けのターゲットとレート制御について」を参照してください。
8. (オプション) [出力オプション] で、コマンド出力をファイルに保存するには、[S3 への出力の書き込みを有効にします] ボックスをオンにします。ボックスにバケット名とプレフィックス (フォルダ) 名を入力してください。

> **Note**
>
> S3 バケットにデータを書き込む機能を許可する S3 アクセス許可は、このタスクを実行する IAM ユーザーのものではなく、マネージドノードに割り当てられたインスタンスプロファイルのものです。詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」または「ハイブリッド環境に IAM サービスロールを作成する」を参照してください。さらに、指定された S3 バケットが別の AWS アカウント にある場合は、マネージドノードに関連付けられたインスタンスプロファイルまたは IAM サービスロールに、そのバケットへの書き込みに必要なアクセス許可があることを確認してください。

9. [関連付けの作成] を選択します。

チュートリアル: AWS CLI を使用してサーバー環境にパッチを適用する

次の手順では、カスタムパッチベースライン、パッチグループ、メンテナンスウィンドウを使用してサーバー環境にパッチを適用する方法を説明します。

[開始する前に]

- マネージドノードに SSM Agent をインストールまたはアップデートしてください。Linux マネージドノードにパッチを適用するには、ノードが SSM Agent バージョン 2.0.834.0 以降実行されている必要があります。詳細については、「Run Command を使用して SSM Agent を更新する」を参照してください。
- AWS Systems Manager のツールである Maintenance Windows のロールとアクセス許可を設定します 詳細については、「Maintenance Windows を設定する」を参照してください。

- まだ AWS Command Line Interface (AWS CLI) をインストールして設定していない場合は、インストールして設定します。

  詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」を参照してください。

Patch Manager を設定してマネージドノードにパッチを適用するには (コマンドライン)

1. 次のコマンドを実行して、Production-Baseline という名前の Windows のパッチベースラインを作成します。このパッチベースラインは、リリースまたは最後に更新されてから 7 日後に、実稼働環境のパッチを承認します。つまり、パッチベースラインが本番環境用であることを示すタグ付けがされています。

   > **Note**
   >
   > OperatingSystem パラメータおよび PatchFilters は、パッチベースラインが適用されるターゲット マネージドノードのオペレーティングシステムによって異なります。詳細については、「OperatingSystem」および「PatchFilter」を参照してください。

   Linux & macOS

   ```
   aws ssm create-patch-baseline \
       --name "Production-Baseline" \
       --operating-system "WINDOWS" \
       --tags "Key=Environment,Value=Production" \
       --approval-rules
    "PatchRules=[{PatchFilterGroup={PatchFilters=[{Key=MSRC_SEVERITY,Values=[Critical,Impor
   {Key=CLASSIFICATION,Values=[SecurityUpdates,Updates,ServicePacks,UpdateRollups,CriticalU
    \
       --description "Baseline containing all updates approved for production
    systems"
   ```

   Windows Server

   ```
   aws ssm create-patch-baseline ^
       --name "Production-Baseline" ^
       --operating-system "WINDOWS" ^
       --tags "Key=Environment,Value=Production" ^
   ```

```
    --approval-rules
 "PatchRules=[{PatchFilterGroup={PatchFilters=[{Key=MSRC_SEVERITY,Values=[Critical,Impor
{Key=CLASSIFICATION,Values=[SecurityUpdates,Updates,ServicePacks,UpdateRollups,CriticalU
 ^
    --description "Baseline containing all updates approved for production
 systems"
```

システムが以下のような情報をレスポンスします。

```
{
   "BaselineId":"pb-0c10e65780EXAMPLE"
}
```

2. 次のコマンドを実行して、2 つのパッチグループの「実稼働ベースライン」パッチベースラインを登録します。グループの名前は「データベースサーバー」と「フロントエンドサーバー」です。

   Linux & macOS

   ```
   aws ssm register-patch-baseline-for-patch-group \
       --baseline-id pb-0c10e65780EXAMPLE \
       --patch-group "Database Servers"
   ```

   Windows Server

   ```
   aws ssm register-patch-baseline-for-patch-group ^
       --baseline-id pb-0c10e65780EXAMPLE ^
       --patch-group "Database Servers"
   ```

   システムが以下のような情報をレスポンスします。

   ```
   {
      "PatchGroup":"Database Servers",
      "BaselineId":"pb-0c10e65780EXAMPLE"
   }
   ```

   Linux & macOS

   ```
   aws ssm register-patch-baseline-for-patch-group \
   ```

```
    --baseline-id pb-0c10e65780EXAMPLE \
    --patch-group "Front-End Servers"
```

Windows Server

```
aws ssm register-patch-baseline-for-patch-group ^
    --baseline-id pb-0c10e65780EXAMPLE ^
    --patch-group "Front-End Servers"
```

システムが以下のような情報をレスポンスします。

```
{
   "PatchGroup":"Front-End Servers",
   "BaselineId":"pb-0c10e65780EXAMPLE"
}
```

3. 次のコマンドを実行し、実稼働サーバー用の 2 つのメンテナンスウィンドウを作成します。最初のウィンドウは、毎火曜日の午後 10 時に実行します。2 番目のウィンドウは、毎土曜日の午後 10 時に実行します。また、メンテナンスウィンドウが実稼働環境用であることを示すタグが付けられます。

   Linux & macOS

```
aws ssm create-maintenance-window \
    --name "Production-Tuesdays" \
    --tags "Key=Environment,Value=Production" \
    --schedule "cron(0 0 22 ? * TUE *)" \
    --duration 1 \
    --cutoff 0 \
    --no-allow-unassociated-targets
```

   Windows Server

```
aws ssm create-maintenance-window ^
    --name "Production-Tuesdays" ^
    --tags "Key=Environment,Value=Production" ^
    --schedule "cron(0 0 22 ? * TUE *)" ^
    --duration 1 ^
    --cutoff 0 ^
    --no-allow-unassociated-targets
```

システムが以下のような情報をレスポンスします。

```
{
   "WindowId":"mw-0c50858d01EXAMPLE"
}
```

Linux & macOS

```
aws ssm create-maintenance-window \
    --name "Production-Saturdays" \
    --tags "Key=Environment,Value=Production" \
    --schedule "cron(0 0 22 ? * SAT *)" \
    --duration 2 \
    --cutoff 0 \
    --no-allow-unassociated-targets
```

Windows Server

```
aws ssm create-maintenance-window ^
    --name "Production-Saturdays" ^
    --tags "Key=Environment,Value=Production" ^
    --schedule "cron(0 0 22 ? * SAT *)" ^
    --duration 2 ^
    --cutoff 0 ^
    --no-allow-unassociated-targets
```

システムが以下のような情報をレスポンスします。

```
{
   "WindowId":"mw-9a8b7c6d5eEXAMPLE"
}
```

4. 次のコマンドを実行して、Database および Front-End サーバーのパッチグループをそれぞれのメンテナンスウィンドウに登録します。

Linux & macOS

```
aws ssm register-target-with-maintenance-window \
```

```
    --window-id mw-0c50858d01EXAMPLE \
    --targets "Key=tag:PatchGroup,Values=Database Servers" \
    --owner-information "Database Servers" \
    --resource-type "INSTANCE"
```

Windows Server

```
aws ssm register-target-with-maintenance-window ^
    --window-id mw-0c50858d01EXAMPLE ^
    --targets "Key=tag:PatchGroup,Values=Database Servers" ^
    --owner-information "Database Servers" ^
    --resource-type "INSTANCE"
```

システムが以下のような情報をレスポンスします。

```
{
   "WindowTargetId":"e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE"
}
```

Linux & macOS

```
aws ssm register-target-with-maintenance-window \
--window-id mw-9a8b7c6d5eEXAMPLE \
--targets "Key=tag:PatchGroup,Values=Front-End Servers" \
--owner-information "Front-End Servers" \
--resource-type "INSTANCE"
```

Windows Server

```
aws ssm register-target-with-maintenance-window ^
    --window-id mw-9a8b7c6d5eEXAMPLE ^
    --targets "Key=tag:PatchGroup,Values=Front-End Servers" ^
    --owner-information "Front-End Servers" ^
    --resource-type "INSTANCE"
```

システムが以下のような情報をレスポンスします。

```
{
   "WindowTargetId":"faa01c41-1d57-496c-ba77-ff9caEXAMPLE"
```

```
}
```

5. 次のコマンドを実行して、それぞれのメンテナンスウィンドウ中に、Database および Front-End サーバー上に不足している更新プログラムをインストールするパッチタスクを登録します。

   Linux & macOS

   ```
   aws ssm register-task-with-maintenance-window \
       --window-id mw-0c50858d01EXAMPLE \
       --targets "Key=WindowTargetIds,Values=e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE"
    \
       --task-arn "AWS-RunPatchBaseline" \
       --service-role-arn "arn:aws:iam::123456789012:role/MW-Role" \
       --task-type "RUN_COMMAND" \
       --max-concurrency 2 \
       --max-errors 1 \
       --priority 1 \
       --task-invocation-parameters "RunCommand={Parameters={Operation=Install}}"
   ```

   Windows Server

   ```
   aws ssm register-task-with-maintenance-window ^
       --window-id mw-0c50858d01EXAMPLE ^
       --targets "Key=WindowTargetIds,Values=e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE"
    ^
       --task-arn "AWS-RunPatchBaseline" ^
       --service-role-arn "arn:aws:iam::123456789012:role/MW-Role" ^
       --task-type "RUN_COMMAND" ^
       --max-concurrency 2 ^
       --max-errors 1 ^
       --priority 1 ^
       --task-invocation-parameters "RunCommand={Parameters={Operation=Install}}"
   ```

   システムが以下のような情報をレスポンスします。

   ```
   {
      "WindowTaskId":"4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE"
   }
   ```

Linux & macOS

```
aws ssm register-task-with-maintenance-window \
    --window-id mw-9a8b7c6d5eEXAMPLE \
    --targets "Key=WindowTargetIds,Values=faa01c41-1d57-496c-ba77-ff9caEXAMPLE"
 \
    --task-arn "AWS-RunPatchBaseline" \
    --service-role-arn "arn:aws:iam::123456789012:role/MW-Role" \
    --task-type "RUN_COMMAND" \
    --max-concurrency 2 \
    --max-errors 1 \
    --priority 1 \
    --task-invocation-parameters "RunCommand={Parameters={Operation=Install}}"
```

Windows Server

```
aws ssm register-task-with-maintenance-window ^
    --window-id mw-9a8b7c6d5eEXAMPLE ^
    --targets "Key=WindowTargetIds,Values=faa01c41-1d57-496c-ba77-ff9caEXAMPLE"
 ^
    --task-arn "AWS-RunPatchBaseline" ^
    --service-role-arn "arn:aws:iam::123456789012:role/MW-Role" ^
    --task-type "RUN_COMMAND" ^
    --max-concurrency 2 ^
    --max-errors 1 ^
    --priority 1 ^
    --task-invocation-parameters "RunCommand={Parameters={Operation=Install}}"
```

システムが以下のような情報をレスポンスします。

```
{
   "WindowTaskId":"8a5c4629-31b0-4edd-8aea-33698EXAMPLE"
}
```

6. 以下のコマンドを実行して、パッチグループのパッチコンプライアンスの概要を取得します。高レベル パッチコンプライアンスの概要には、それぞれのパッチ状態のパッチがあるマネージドノードの数が含まれます。

> **Note**
>
> 最初のメンテナンスウィンドウ中にパッチ タスクが実行されるまで、サマリー内のマネージドノード数はゼロであることが予想されます。

Linux & macOS

```
aws ssm describe-patch-group-state \
    --patch-group "Database Servers"
```

Windows Server

```
aws ssm describe-patch-group-state ^
    --patch-group "Database Servers"
```

システムが以下のような情報をレスポンスします。

```
{
   "Instances": number,
   "InstancesWithFailedPatches": number,
   "InstancesWithInstalledOtherPatches": number,
   "InstancesWithInstalledPatches": number,
   "InstancesWithInstalledPendingRebootPatches": number,
   "InstancesWithInstalledRejectedPatches": number,
   "InstancesWithMissingPatches": number,
   "InstancesWithNotApplicablePatches": number,
   "InstancesWithUnreportedNotApplicablePatches": number
}
```

7. 以下のコマンドを実行して、パッチグループのマネージドノードごとにパッチ状態の概要を取得します。マネージドノードごとのサマリーには、パッチグループのマネージドノードごとのそれぞれのパッチ状態にある多数のパッチが含まれます。

   Linux & macOS

   ```
   aws ssm describe-instance-patch-states-for-patch-group \
       --patch-group "Database Servers"
   ```

Windows Server

```
aws ssm describe-instance-patch-states-for-patch-group ^
    --patch-group "Database Servers"
```

システムが以下のような情報をレスポンスします。

```
{
   "InstancePatchStates": [
      {
         "BaselineId": "string",
         "FailedCount": number,
         "InstalledCount": number,
         "InstalledOtherCount": number,
         "InstalledPendingRebootCount": number,
         "InstalledRejectedCount": number,
         "InstallOverrideList": "string",
         "InstanceId": "string",
         "LastNoRebootInstallOperationTime": number,
         "MissingCount": number,
         "NotApplicableCount": number,
         "Operation": "string",
         "OperationEndTime": number,
         "OperationStartTime": number,
         "OwnerInformation": "string",
         "PatchGroup": "string",
         "RebootOption": "string",
         "SnapshotId": "string",
         "UnreportedNotApplicableCount": number
      }
   ]
}
```

Patch Managerの設定タスクを実行するために使用できる他の AWS CLI コマンドの例については、「AWS CLI を使用して Patch Manager リソースを操作する」を参照してください。

Patch Manager のトラブルシューティング

AWS Systems Manager のツールである Patch Manager を使用したトラブルシューティングでは、以下の情報を使用します。

トピック

- 問題:「Invoke-PatchBaselineOperation」:baseline_overrides.json についての「アクセスが拒否されました」エラーまたは「S3 からファイルをダウンロードできません」エラー
- 問題: パッチ適用が失敗したものの、明らかな原因やエラーメッセージが表示されない
- 問題: 想定外のパッチコンプライアンス結果
- Linuxで AWS-RunPatchBaseline を実行時のエラー
- Windows Server で AWS-RunPatchBaseline 実行時のエラー
- AWS サポート Automation ランブックの使用方法
- AWS サポートに連絡する

問題:「Invoke-PatchBaselineOperation」:**baseline_overrides.json** についての「アクセスが拒否されました」エラーまたは「S3 からファイルをダウンロードできません」エラー

問題: パッチポリシーによって指定されたパッチ適用オペレーションを実行すると、次の例のようなエラーが表示されます。

Example error on Windows Server

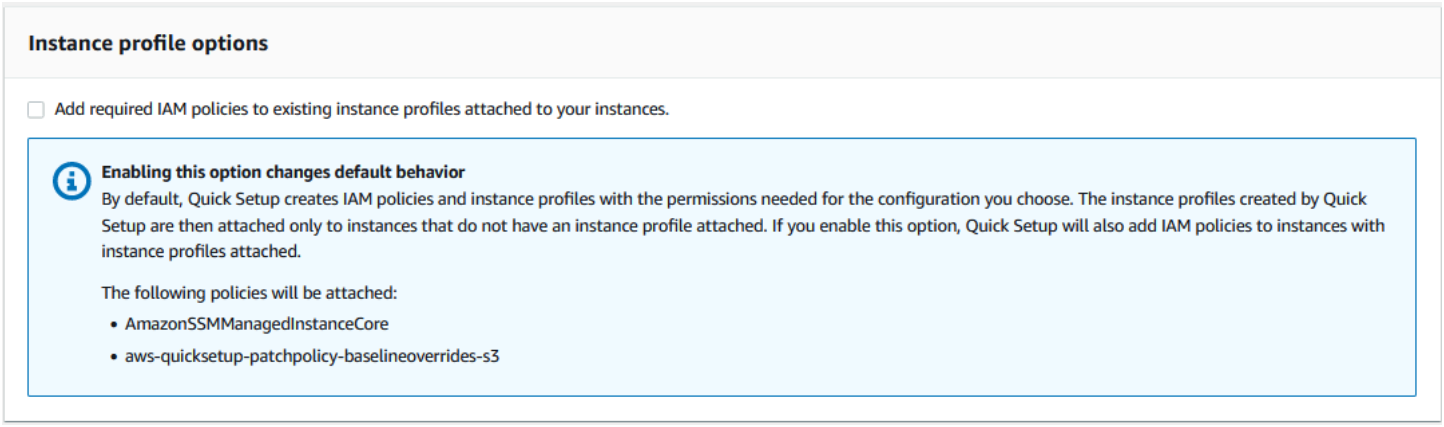
```
----------ERROR-------
Invoke-PatchBaselineOperation : Access Denied
At C:\ProgramData\Amazon\SSM\InstanceData\i-02573cafcfEXAMPLE\document\orchestr
ation\792dd5bd-2ad3-4f1e-931d-abEXAMPLE\PatchWindows\_script.ps1:219 char:13
+ $response = Invoke-PatchBaselineOperation -Operation Install -Snapsho ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
+ CategoryInfo : OperationStopped: (Amazon.Patch.Ba...UpdateOpera
tion:InstallWindowsUpdateOperation) [Invoke-PatchBaselineOperation], Amazo
nS3Exception
+ FullyQualifiedErrorId : PatchBaselineOperations,Amazon.Patch.Baseline.Op
erations.PowerShellCmdlets.InvokePatchBaselineOperation
failed to run commands: exit status 0xffffffff
```

Example error on Linux

```
[INFO]: Downloading Baseline Override from s3://aws-quicksetup-
patchpolicy-123456789012-abcde/baseline_overrides.json
[ERROR]: Unable to download file from S3: s3://aws-quicksetup-
patchpolicy-123456789012-abcde/baseline_overrides.json.
[ERROR]: Error loading entrance module.
```

原因: Quick Setup でパッチポリシーを作成しましたが、マネージドノードの一部には、既にインスタンスプロファイル (EC2 インスタンスの場合) またはサービスロール (EC2 以外のマシンの場合) がアタッチされています。

ただし、次の画像に示すように、[インスタンスにアタッチされている既存のインスタンスプロファイルに必要な IAM ポリシーを追加] チェックボックスをオンにしませんでした。



パッチポリシーを作成すると、ポリシーの設定 `baseline_overrides.json` ファイルを保存するための Amazon S3 バケットも作成されます。ポリシーの作成時に [インスタンスにアタッチされている既存のインスタンスプロファイルに必要な IAM ポリシーを追加] チェックボックスをオンにしない場合、S3 バケット内で `baseline_overrides.json` にアクセスするために必要な IAM ポリシーとリソースタグは、既存の IAM インスタンスのプロファイルとサービスロールに自動的に追加されません。

解決策 1: 既存のパッチポリシー設定を削除し、代わりのポリシーを作成します。その際には、必ず [インスタンスにアタッチされている既存のインスタンスプロファイルに必要な IAM ポリシーを追加] チェックボックスをオンにしてください。これにより、この Quick Setup 設定によって作成された IAM ポリシーは、既にインスタンスプロファイルまたはサービスロールがアタッチされているノードに適用されます。(デフォルトでは、Quick Setup は、インスタンスプロファイルまたはサービスロールをまだ持っていないインスタンスとノードに必要なポリシーを追加します。) 詳細については、「Quick Setup パッチポリシーを使用して組織全体のパッチ適用を自動化する」を参照してください。

解決策 2: Quick Setup で使用する各 IAM インスタンスプロファイルと IAM サービスロールに、必要な許可とタグを手動で追加します。手順については、「パッチポリシー S3 バケットの許可」を参照してください。

問題: パッチ適用が失敗したものの、明らかな原因やエラーメッセージが表示されない

問題: パッチ適用操作はエラーメッセージを返さずに失敗します。

考えられる原因: AWS-RunPatchBaseline の呼び出しが、複数同時に起きた場合、互いに競合し、パッチ適用タスクが失敗する可能性があります。これはパッチログには表示されない場合があります。

同時実行中のパッチ適用操作が相互に中断されたかどうかを確認するには、AWS Systems Manager のツールである Run Command でコマンド履歴をチェックします。パッチ適用に失敗したマネージドノードでは、マシンへパッチを適用するために、複数の操作が 2 分以内の間隔で試行されたかどうかを確認します。このシナリオでは、場合によって処理が失敗する可能性があります。

次のコマンドを使用して、同時パッチ適用を試みているかどうかを確認するために、AWS Command Line Interface (AWS CLI) を使用することもできます。*node-id* の値は、マネージドノードの ID で置き換えてください。

```
aws ssm list-commands \
    --filter "key=DocumentName,value=AWS-RunPatchBaseline" \
    --query 'Commands[*].
{CommandId:CommandId,RequestedDateTime:RequestedDateTime,Status:Status}' \
    --instance-id node-id \
    --output table
```

解決策: 同じマネージドノード上で競合するパッチ適用操作が原因でパッチ適用が失敗したと判断した場合は、パッチ適用の設定を調整して、問題が再度起こらないようにします。例えば、2 つのメンテナンスウィンドウでパッチ適用時間が重複して指定されている場合は、そのうちの 1 つを削除または修正します。メンテナンスウィンドウで 1 つのパッチ適用操作が指定されているが、パッチポリシーで同じ時間に別のパッチ操作が指定されている場合は、そのタスクをメンテナンスウィンドウから削除することを検討してください。

このシナリオでパッチ適用操作の競合が失敗の原因ではないと判断した場合は、AWS サポート に問い合わせることをお勧めします。

問題: 想定外のパッチコンプライアンス結果

問題: Scan オペレーション後に生成されたパッチ適用コンプライアンスの詳細を確認すると、結果にパッチベースラインに設定されたルールを反映していない情報が含まれています。例えば、パッチベースラインの [Rejected patches] (拒否されたパッチ) リストに追加した例外は、Missing として表示されます。または、パッチベースラインで Critical パッチのみと指定されている場合でも、Important に分類されたパッチが未適用と表示されます。

原因: Patch Manager は現在、Scan オペレーションを実行する複数の方法をサポートしています。

- Quick Setup で設定されているパッチポリシー
- Quick Setup で設定されているホスト管理オプション
- パッチ Scan または Install のタスクを実行するためのメンテナンスウィンドウ
- オンデマンドの [Patch now] (今すぐパッチ適用) オペレーション

Scan オペレーションを実行すると、最新のスキャンのコンプライアンスの詳細が上書きされます。Scan オペレーションを実行するために複数の方法を設定していて、それぞれの方法によってルールが異なるさまざまなパッチベースラインが使用されている場合、パッチコンプライアンスの結果も異なります。

解決方法: 想定外のパッチコンプライアンスの結果を避けるため、Patch Manager Scan オペレーションを実行する方法は一度に 1 つだけ使用することをお勧めします。詳細については、「パッチコンプライアンスデータに対する意図しない上書きの回避」を参照してください。

Linuxで **AWS-RunPatchBaseline** を実行時のエラー

トピック

- 問題:「そのようなファイルまたはディレクトリがありません」というエラー
- 問題:「別のプロセスが yum ロックを取得しました」というエラー
- 問題:「権限が拒否された/コマンドを実行できませんでした」というエラー
- 問題:「ペイロードをダウンロードできません」というエラー
- 問題 :「サポートされていないパッケージマネージャとPythonバージョンの組み合わせ」エラー
- 問題: 特定のパッケージを除外するために指定されたルールを Patch Manager が適用しない。
- 問題: パッチ適用が失敗し、TLS へのサーバー名表示拡張を利用できないことが Patch Manager から報告される
- 問題: Patch Manager が「試行するミラーはもうありません」と報告する
- 問題:「curl から返されたエラーコードは 23 です」というメッセージが表示されてパッチが失敗する
- 問題: パッチ適用が失敗し、「Error unpacking rpm package…」(rmp パッケージの解凍中にエラーが発生しました...) というメッセージが表示される
- 問題: パッチ適用が失敗し、「Encounter service side error when uploading the inventory」と表示される
- 問題:「Errors were encountered while downloading packages」(パッケージのダウンロード中にエラーが発生しました) というメッセージが表示されてパッチ適用が失敗する

- 問題:「The following signatures couldn't be verified because the public key is not available」(公開鍵が利用できないため、次の署名を検証できませんでした) というメッセージが表示されてパッチ適用が失敗します。
- 問題:「NoMoreMirrorsRepoError」というメッセージが表示されてパッチ適用が失敗します。
- 問題:「Unable to download payload」(ペイロードをダウンロードできません) というメッセージが表示されてパッチ適用が失敗します。
- 問題:「install errors: dpkg: error: dpkg frontend is locked by another process」(インストールエラー:dpkg: エラー:dpkg フロントエンドが別のプロセスによってロックされています) というメッセージが表示されてパッチ適用が失敗します。
- 問題: Ubuntu Server へのパッチ適用が「dpkg was interrupted」(dpkg が中断されました) というエラーで失敗します。
- 問題: パッケージマネージャーユーティリティがパッケージの依存関係を解決できません。

問題:「そのようなファイルまたはディレクトリがありません」というエラー

問題: AWS-RunPatchBaseline 実行時、パッチ適用が次のいずれかのエラーで失敗する。

```
IOError: [Errno 2] No such file or directory: 'patch-baseline-operations-X.XX.tar.gz'
```

```
Unable to extract tar file: /var/log/amazon/ssm/patch-baseline-operations/patch-
baseline-operations-1.75.tar.gz.failed to run commands: exit status 155
```

```
Unable to load and extract the content of payload, abort.failed to run commands: exit
 status 152
```

原因 1: AWS-RunPatchBaseline を実行する 2 つのコマンドが同じマネージドノード上で同時に実行されています。これにより、競合状態が作成され、正しく作成されていない、またはアクセスされていない一時的な file patch-baseline-operations* という結果になります。

原因 2: /var ディレクトリー以下の不十分なストレージ領域

解決策 1: メンテナンスウィンドウに、AWS-RunPatchBaseline を同じ優先度レベル、同じターゲット ID で実行する 2 つ以上の Run Command タスク がないことを確保します。その場合は、優先順位を並べ替えます。Run Command は AWS Systems Manager のツールです。

解決策 2: 同じターゲットに対し、同じスケジュールで AWS-RunPatchBaseline を使用する Run Command タスクは、一度に 1 つのメンテナンスウィンドウだけが実行するようにします。このような場合は、スケジュールを変更してください。

解決策 3: 同じスケジュールで同じマネージドノードをターゲットにして AWS-RunPatchBaseline を実行する State Manager の関連付けは 1 つだけにしてください。State Manager は AWS Systems Manager のツールです。

解決策 4: アップデートパッケージ用の /var ディレクトリー下に、十分なストレージ領域を解放します。

問題:「別のプロセスが yum ロックを取得しました」というエラー

問題: AWS-RunPatchBaseline を実行すると、パッチ適用は、次のエラーで失敗する。

```
12/20/2019 21:41:48 root [INFO]: another process has acquired yum lock, waiting 2 s and
 retry.
```

原因: マネージドノードが別のオペレーションで実行を開始し、パッケージマネージャ yum プロセスを取得した状態で、AWS-RunPatchBaseline ドキュメントがすでに実行されている。

解決策: State Manager の関連付けやメンテナンスウィンドウタスクなど、スケジュールに従って AWS-RunPatchBaseline を実行する設定が、同じ時間帯に同じマネージドノードをターゲットにしないようにします。

問題:「権限が拒否された/コマンドを実行できませんでした」というエラー

問題: AWS-RunPatchBaseline を実行すると、パッチ適用は、次のエラーで失敗する。

```
sh:
/var/lib/amazon/ssm/instanceid/document/orchestration/commandid/PatchLinux/_script.sh:
 Permission denied
failed to run commands: exit status 126
```

原因:/var/lib/amazon/ が noexec 許可でマウントされている可能性。これは、SSM Agent がペイロードスクリプトを/var/lib/amazon/ssm にダウンロードし、その場所からそれらを実行することが問題です。

解決策: 排他パーティションを /var/log/amazon および /var/lib/amazon に設定し、exec 許可でマウントされているようにする。

問題:「ペイロードをダウンロードできません」というエラー

問題: AWS-RunPatchBaseline を実行すると、パッチ適用は、次のエラーで失敗する。

```
Unable to download payload: https://s3.amzn-s3-demo-bucket.region.amazonaws.com/
aws-ssm-region/patchbaselineoperations/linux/payloads/patch-baseline-operations-
X.XX.tar.gz.failed to run commands: exit status 156
```

原因: マネージドノードには、指定した Amazon Simple Storage Service (Amazon S3) バケットへのアクセスに必要な許可がない。

解決策: S3 エンドポイントに到達できるようにネットワーク設定を更新します。詳細については、SSM Agent と AWS マネージド S3 バケットとの通信 で Patch Manager の S3 バケットへの必要なアクセスに関する情報を参照してください。

問題 : 「サポートされていないパッケージマネージャとPythonバージョンの組み合わせ」エラー

問題: AWS-RunPatchBaseline を実行すると、パッチ適用は、次のエラーで失敗する。

```
An unsupported package manager and python version combination was found. Apt requires
 Python3 to be installed.
failed to run commands: exit status 1
```

原因: サポートされているバージョンの Python 3 が Debian Server、Raspberry Pi OS、または Ubuntu Server インスタンスにインストールされていない。

解決策: Debian Server、Raspberry Pi OS、および Ubuntu Server マネージドノードに必要なサポートされているバージョンの python3 (3.0 ~ 3.10) をサーバーにインストールします。

問題: 特定のパッケージを除外するために指定されたルールを Patch Manager が適用しない。

問題: 形式 exclude=*package-name* の /etc/yum.conf ファイルで指定した特定のパッケージを除外しようとしたが、Patch Manager Install オペレーションでは除外されない。

原因: Patch Manager が、/etc/yum.conf ファイルで指定された除外項目を取り込まない。

解決策: 特定のパッケージを除外するには、カスタムパッチベースラインを作成し、インストールしないパッケージを除外するルールを作成します。

問題: パッチ適用が失敗し、TLS へのサーバー名表示拡張を利用できないことが Patch Manager から報告される

問題: パッチ適用操作が、次のメッセージを発行する。

```
/var/log/amazon/ssm/patch-baseline-operations/urllib3/util/ssl_.py:369:
SNIMissingWarning: An HTTPS request has been made, but the SNI (Server Name Indication)
 extension
to TLS is not available on this platform. This might cause the server to present an
 incorrect TLS
certificate, which can cause validation failures. You can upgrade to a newer version of
 Python
to solve this.
For more information, see https://urllib3.readthedocs.io/en/latest/advanced-
usage.html#ssl-warnings
```

原因: このメッセージはエラーを示していません。代わりに、オペレーティングシステムと共に配布されている古いバージョンの Python が TLS サーバー名表示をサポートしていないという警告が表示されます。Systems Manager のパッチペイロードスクリプトは、SNI をサポートする AWS APIに接続する際に、この警告を出します。

解決策: このメッセージが報告されたときにパッチ適用の失敗をトラブルシューティングするには、stdout および stderr ファイルの内容を確認する。これらのファイルを S3 バケットまたは Amazon CloudWatch Logs に保存するようにパッチベースラインを設定していない場合は、Linux マネージドノードの次の場所にファイルを配置することができます。

/var/lib/amazon/ssm/*instance-id*/document/orchestration/*Run-Command-execution-id*/awsrunShellScript/PatchLinux

問題: Patch Manager が「試行するミラーはもうありません」と報告する

問題: パッチ適用操作が、次のメッセージを発行する。

```
[Errno 256] No more mirrors to try.
```

原因: マネージドノードに設定されているリポジトリーが正しく動作していません。エラーの原因として以下が考えられます。

- yum キャッシュが破損している。
- ネットワーク関連の問題により、リポジトリ URL にアクセスできない。

解決策: Patch Manager は、マネージドノードのデフォルトのパッケージマネージャーを使用してパッチ適用オペレーションを実行します。リポジトリーが正しく構成され、動作していることを確認します。

問題: 「curl から返されたエラーコードは 23 です」というメッセージが表示されてパッチが失敗する

問題: AWS-RunPatchBaseline を使用するパッチオペレーションに失敗すると、次のようなエラーが発生することがあります。

```
05/01/2025 17:04:30 root [ERROR]: Error code returned from curl is 23
```

原因: システムで使用している curl ツールには、ファイルシステムへの書き込みに必要な権限がありません。これは、パッケージマネージャーのデフォルトの curl ツールが、snap でインストールされたものなど、別のバージョンに置き換えられた場合に発生する可能性があります。

解決方法: 別のバージョンがインストールされたときにパッケージマネージャーから提供された curl バージョンがアンインストールされた場合は、再インストールします。

複数の curl バージョンをインストールしたままにしておく必要がある場合は、パッケージマネージャーに関連付けられているバージョンが、PATH 変数にリストされている最初のディレクトリにあることを確認してください。これを確認するには、echo $PATH コマンドを実行して、システム上の実行ファイルがチェックされているディレクトリの現在の順序を確認します。

問題: パッチ適用が失敗し、「Error unpacking rpm package...」(rmp パッケージの解凍中にエラーが発生しました...) というメッセージが表示される

問題: パッチ適用操作が次のような エラーで失敗します。

```
Error : Error unpacking rpm package python-urllib3-1.25.9-1.amzn2.0.2.noarch
python-urllib3-1.25.9-1.amzn2.0.1.noarch was supposed to be removed but is not!
failed to run commands: exit status 1
```

原因 1: 特定のパッケージが複数のパッケージインストーラー (両方など) に存在する場合、pip と yum の両方、または dnf など、デフォルトのパッケージマネージャーを使用したときにコンフリクトが発生する可能性があります。

urllib3 パッケージで発生することが多く、pip、yum、dnf などに見られます。

原因 2: python-urllib3 パッケージが壊れています。これは、yum または dnf によって rpm パッケージが前もってインストールされたあと、pip によってパッケージファイルがインストールまたは更新された場合に発生することがあります。

解決策: コマンド `sudo pip uninstall urllib3` を実行し、デフォルトのパッケージマネージャー (yum または dnf) にのみ、パッケージを保持することで、pip から python-urllib3 パッケージを削除します。

問題: パッチ適用が失敗し、「Encounter service side error when uploading the inventory」と表示される

問題: AWS-RunPatchBaseline ドキュメントを実行すると、次のエラーメッセージが表示されます。

```
Encounter service side error when uploading the inventory
```

原因: AWS-RunPatchBaseline を実行する 2 つのコマンドが同じマネージドノード上で同時に実行されています。これにより、パッチ適用オペレーション中に boto3 クライアントを初期化するときに競合状態が生じています。

解決策: State Manager の関連付けやメンテナンスウィンドウタスクなど、スケジュールに従って AWS-RunPatchBaseline を実行する設定が、同じ時間帯に同じマネージドノードをターゲットにしないようにします。

問題:「Errors were encountered while downloading packages」(パッケージのダウンロード中にエラーが発生しました) というメッセージが表示されてパッチ適用が失敗する

問題: パッチ適用中に、次のようなエラーが表示されます。

```
YumDownloadError: [u'Errors were encountered while downloading
packages.', u'libxml2-2.9.1-6.el7_9.6.x86_64: [Errno 5] [Errno 12]
Cannot allocate memory', u'libxslt-1.1.28-6.el7.x86_64: [Errno 5]
[Errno 12] Cannot allocate memory', u'libcroco-0.6.12-6.el7_9.x86_64:
[Errno 5] [Errno 12] Cannot allocate memory', u'openldap-2.4.44-25.el7_9.x86_64:
[Errno 5] [Errno 12] Cannot allocate memory',
```

原因: このエラーは、マネージドノードで利用可能なメモリが不足している場合に発生する可能性があります。

解決策: スワップメモリを設定するか、インスタンスを別のタイプにアップグレードしてメモリサポートを増やします。その後、新しいパッチ適用操作を開始します。

問題:「The following signatures couldn't be verified because the public key is not available」(公開鍵が利用できないため、次の署名を検証できませんでした) というメッセージが表示されてパッチ適用が失敗します。

問題: Ubuntu Server を使用するパッチ適用に失敗すると、次のようなエラーが発生することがあります。

```
02/17/2022 21:08:43 root [ERROR]: W:GPG error:
http://repo.mysql.com/apt/ubuntu  bionic InRelease: The following
signatures couldn't be verified because the public key is not available:
NO_PUBKEY 467B942D3A79BD29, E:The repository ' http://repo.mysql.com/apt/ubuntu bionic
```

原因:: GNU Privacy Guard (GPG) キーの有効期限が切れているか、キーがありません。

解決策: GPG キーを更新するか、キーをもう一度追加してください。

例えば、前に示したエラーを見ると、467B942D3A79BD29 キーがないため、追加する必要があります。そのためには、次のコマンドのいずれかを実行します。

```
sudo apt-key adv --keyserver hkps://keyserver.ubuntu.com --recv-keys 467B942D3A79BD29
```

```
sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys 467B942D3A79BD29
```

または、すべてのキーを更新するには、以下のコマンドを実行します。

```
sudo apt-key adv --keyserver hkps://keyserver.ubuntu.com --refresh-keys
```

この後も エラーが再発する場合は、リポジトリを管理している組織に問題を報告することをおすすめします。修正が利用できるようになるまでは、パッチ処理中にリポジトリを省略するため `/etc/apt/sources.list` ファイルを編集できます。

そのためには、`sources.list` を編集用に開き、リポジトリの行を見つけて、その行の先頭にコメントアウトする `#` 文字を挿入します。ファイルを保存してから閉じます。

問題:「NoMoreMirrorsRepoError」というメッセージが表示されてパッチ適用が失敗します。

問題: 次のようなエラーが表示されます。

```
NoMoreMirrorsRepoError: failure: repodata/repomd.xml from pgdg94: [Errno 256] No more
 mirrors to try.
```

原因: ソースリポジトリにエラーがあります。

解決策: リポジトリを管理している組織に問題を報告することをおすすめします。エラーが修正されるまでは、オペレーティングシステムレベルでリポジトリを無効にできます。そのためには、以下のコマンドを実行します。*repo-name* の値を次のリポジトリ名で置き換えます。

```
yum-config-manager --disable repo-name
```

次に例を示します。

```
yum-config-manager --disable pgdg94
```

このコマンドを実行した後、別のパッチ適用操作を実行します。

問題: 「Unable to download payload」(ペイロードをダウンロードできません) というメッセージが表示されてパッチ適用が失敗します。

問題: 次のような エラーが表示されます。

```
Unable to download payload:
https://s3.dualstack.eu-west-1.amazonaws.com/aws-ssm-eu-west-1/patchbaselineoperations/
linux/payloads/patch-baseline-operations-1.83.tar.gz.
failed  to run commands: exit status 156
```

原因: マネージドノードの設定にエラーがあるか、不完全です。

解決策: マネージドノードが次のように設定されていることを確認します。

- セキュリティグループのアウトバウンド TCP 443 ルール。
- NACL のエグレス TCP 443 ルール。
- NACL のイングレス TCP 1024-65535 ルール。
- S3 エンドポイントへの接続を提供するルートテーブル内の NAT/IGW。インスタンスがインターネットにアクセスできない場合は、S3 エンドポイントとの接続を確立します。そのためには、VPC に S3 ゲートウェイエンドポイントを追加し、マネージドノードのルートテーブルと統合します。

問題:「install errors: dpkg: error: dpkg frontend is locked by another process」(インストールエラー:dpkg: エラー:dpkg フロントエンドが別のプロセスによってロックされています) というメッセージが表示されてパッチ適用が失敗します。

問題: 次のようなエラーが発生してパッチ適用が失敗することがあります。

```
install errors: dpkg: error: dpkg frontend is locked by another process
failed to run commands: exit status 2
Failed to install package; install status Failed
```

原因: パッケージマネージャーは、オペレーティングシステムレベルのマネージドノード上で既に別のプロセスを実行しています。他のプロセスが完了するまでに長い時間がかかる場合は、Patch Manager パッチ適用操作はタイムアウトして失敗することがあります。

解決策: パッケージマネージャーを使用している他のプロセスが完了したら、新しいパッチ適用操作を実行します。

問題: Ubuntu Server へのパッチ適用が「dpkg was interrupted」(dpkg が中断されました) というエラーで失敗します。

問題: Ubuntu Server では、次のようなエラーで、パッチ適用が失敗します。

```
E: dpkg was interrupted, you must manually run
'dpkg --configure -a' to correct the problem.
```

原因: 1 つまたは複数のパッケージの設定が間違っています。

解決方法: 以下のステップを実行します。

1. 以下のコマンドを 1 つずつ実行して、どのパッケージが影響を受けるか、また各パッケージの問題点を確認してください。

   ```
   sudo apt-get check
   ```

   ```
   sudo dpkg -C
   ```

   ```
   dpkg-query -W -f='${db:Status-Abbrev} ${binary:Package}\n' | grep -E ^.[^nci]
   ```

2. 以下のコマンドを実行して、問題のあるパッケージを修正します。

```
sudo dpkg --configure -a
```

3. 前のコマンドで問題が完全に解決されなかった場合は、以下のコマンドを実行します。

```
sudo apt --fix-broken install
```

問題: パッケージマネージャーユーティリティがパッケージの依存関係を解決できません。

問題: マネージドノード上のネイティブパッケージマネージャーがパッケージの依存関係を解決できず、パッチ適用が失敗します。以下のエラーメッセージ例は、パッケージマネージャーとして yum を使用するオペレーティングシステムでのこのタイプの問題を示しています。

```
09/22/2020 08:56:09 root [ERROR]: yum update failed with result code: 1,
message: [u'rpm-python-4.11.3-25.amzn2.0.3.x86_64 requires rpm = 4.11.3-25.amzn2.0.3',
u'awscli-1.18.107-1.amzn2.0.1.noarch requires python2-botocore = 1.17.31']
```

原因: Linux オペレーティングシステムでは、Patch Manager はマシン上のネイティブパッケージマネージャを使用して、yum、dnf、apt、zypper のようなパッチ操作を実行します。アプリケーションは、必要に応じて依存パッケージを自動的に検出、インストール、更新、または削除します。ただし、次のような状況によっては、パッケージマネージャーが依存関係の操作を完了できなくなる場合があります。

- オペレーティングシステムには複数の競合するリポジトリが設定されています。
- ネットワーク関連の問題により、リモートリポジトリの URL にアクセスできません。
- 間違ったアーキテクチャのパッケージがリポジトリで見つかりました。

解決策: さまざまな理由の依存性の問題で、パッチ適用が失敗する可能性があります。そのため、トラブルシューティングの支援を受けるには、AWS サポート にお問い合わせください。

Windows Server で **AWS-RunPatchBaseline** 実行時のエラー

トピック

- 問題:製品ファミリ/製品ペアの不一致
- 問題:AWS-RunPatchBaseline 出力が HRESULT (Windows Server)を返す。
- 問題: マネージドノードに Windows Update カタログまたは WSUS へのアクセスがない
- 問題:パッチベースラインオペレーション PowerShell モジュールがダウンロードできない

- 問題: パッチが見つからない

問題:製品ファミリ/製品ペアの不一致

問題: Systems Managerコンソールでパッチベースラインを作成するとき、製品ファミリーと製品を指定します。たとえば、以下のように選択します。

- Product family (製品ファミリー)`Office`]:

  Product (製品)`Office 2016`]:

原因: 一致していない製品ファミリー/製品ペアでパッチベースラインを作成しようとすると、エラーメッセージが表示されます。以下の理由で、これが発生する場合があります。

- 有効な製品ファミリーと製品ペアが選択されましたが、その後、製品ファミリーの選択が削除されました。
- [Available and matching options (利用可能なマッチングオプション)] サブリストからではなく、[Obsolete or mismatched options (サポートされなくなった、または不一致のオプション)] サブリストから製品が選択されました。

  製品の [Obsolete or mismatched options (サポートされなくなった、または不一致のオプション)] サブリストの項目が、SDK またはAWS Command Line Interface (AWS CLI) `create-patch-baseline` コマンドにより誤って入力された可能性があります。これは、タイプミスがあったか、製品が間違った製品ファミリーに割り当てられたことを意味します。以前のパッチベースラインに指定されても、 Microsoft から入手可能なパッチがない場合、その製品は、[Obsolete or mismatched options (サポートされなくなった、または不一致のオプション)] サブリストにも含まれます。

解決策: この問題を回避するには、[Currently available options (現在利用可能なオプション)] サブリストから常にオプションを選択します。

AWS CLI の `describe-patch-properties` コマンド、または `DescribePatchProperties` API コマンドを使用して、利用可能なパッチのある製品を表示することもできます。

問題:**`AWS-RunPatchBaseline`** 出力が **`HRESULT`** (Windows Server)を返す。

問題: 次のような エラーが発生しました。

```
----------ERROR-------
```

```
Invoke-PatchBaselineOperation : Exception Details: An error occurred when
attempting to search Windows Update.
Exception Level 1:
 Error Message: Exception from HRESULT: 0x80240437
 Stack Trace: at WUApiLib.IUpdateSearcher.Search(String criteria)..
(Windows updates)
11/22/2020 09:17:30 UTC | Info | Searching for Windows Updates.
11/22/2020 09:18:59 UTC | Error | Searching for updates resulted in error: Exception
 from HRESULT: 0x80240437
----------ERROR-------
failed to run commands: exit status 4294967295
```

原因: この出力は、ネイティブの Windows Update API がパッチ適用操作を実行できなかったことを示します。

解決策: エラーを解決するためのトラブルシューティング手順を特定するには、次の microsoft.com トピックの HResult コードを確認します。

- コンポーネント別の Windows Update エラー コード
- Windows Update の一般的なエラーと軽減策

問題: マネージドノードに Windows Update カタログまたは WSUS へのアクセスがない

問題: 次のようなエラーが発生しました。

```
Downloading PatchBaselineOperations PowerShell module from https://s3.aws-api-
domain/path_to_module.zip to C:\Windows\TEMP\Amazon.PatchBaselineOperations-1.29.zip.

Extracting PatchBaselineOperations zip file contents to temporary folder.

Verifying SHA 256 of the PatchBaselineOperations PowerShell module files.

Successfully downloaded and installed the PatchBaselineOperations PowerShell module.

Patch Summary for

PatchGroup :

BaselineId :

Baseline : null
```

```
SnapshotId :

RebootOption : RebootIfNeeded

OwnerInformation :

OperationType : Scan

OperationStartTime : 1970-01-01T00:00:00.0000000Z

OperationEndTime : 1970-01-01T00:00:00.0000000Z

InstalledCount : -1

InstalledRejectedCount : -1

InstalledPendingRebootCount : -1

InstalledOtherCount : -1

FailedCount : -1

MissingCount : -1

NotApplicableCount : -1

UnreportedNotApplicableCount : -1

EC2AMAZ-VL3099P - PatchBaselineOperations Assessment Results - 2020-12-30T20:59:46.169

----------ERROR-------

Invoke-PatchBaselineOperation : Exception Details: An error occurred when attempting to
 search Windows Update.

Exception Level 1:

Error Message: Exception from HRESULT: 0x80072EE2

Stack Trace: at WUApiLib.IUpdateSearcher.Search(String criteria)

at
 Amazon.Patch.Baseline.Operations.PatchNow.Implementations.WindowsUpdateAgent.SearchForUpdates(
```

```
searchCriteria)

At C:\ProgramData\Amazon\SSM\InstanceData\i-02573cafcfEXAMPLE\document\orchestration
\3d2d4864-04b7-4316-84fe-eafff1ea58

e3\PatchWindows\_script.ps1:230 char:13

+ $response = Invoke-PatchBaselineOperation -Operation Install -Snapsho ...

+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

+ CategoryInfo : OperationStopped:
 (Amazon.Patch.Ba...UpdateOperation:InstallWindowsUpdateOperation) [Inv

oke-PatchBaselineOperation], Exception

+ FullyQualifiedErrorId : Exception Level 1:

Error Message: Exception Details: An error occurred when attempting to search Windows
 Update.

Exception Level 1:

Error Message: Exception from HRESULT: 0x80072EE2

Stack Trace: at WUApiLib.IUpdateSearcher.Search(String criteria)

at
 Amazon.Patch.Baseline.Operations.PatchNow.Implementations.WindowsUpdateAgent.SearchForUpdates(
 searc

---Error truncated----
```

原因: このエラーは、Windows Update コンポーネント、または Windows Update カタログもしくは Windows Server Update Services (WSUS) への接続の欠如にまつわる可能性があります。

解決策: マネージドノードがインターネットゲートウェイ、NAT ゲートウェイ、または NAT インスタンスを介して Microsoft Update Catalog に接続されていることを確認します。WSUS を使用している場合は、マネージドノードがお使いの環境内の WSUS サーバーに接続されていることを確認します。目的の送信先への接続が確立されている場合は、Microsoft のドキュメントで考えられる他の `HResult 0x80072EE2` の原因を確認してください。これは、オペレーティングシステムレベルに問題があることを示している可能性があります。

問題:パッチベースラインオペレーション PowerShell モジュールがダウンロードできない

問題: 次のようなエラーが発生しました。

```
Preparing to download PatchBaselineOperations PowerShell module from S3.

Downloading PatchBaselineOperations PowerShell module from https://s3.aws-api-
domain/path_to_module.zip to C:\Windows\TEMP\Amazon.PatchBaselineOperations-1.29.zip.
----------ERROR-------

C:\ProgramData\Amazon\SSM\InstanceData\i-02573cafcfEXAMPLE\document\orchestration
\aaaaaaaa-bbbb-cccc-dddd-4f6ed6bd5514\

PatchWindows\_script.ps1 : An error occurred when executing PatchBaselineOperations:
 Unable to connect to the remote server

+ CategoryInfo : NotSpecified: (:) [Write-Error], WriteErrorException

+ FullyQualifiedErrorId : Microsoft.PowerShell.Commands.WriteErrorException,_script.ps1

failed to run commands: exit status 4294967295
```

解決策: Amazon Simple Storage Service (Amazon S3) へのマネージドノードの接続とアクセス許可を確認します。マネージドノードの AWS Identity and Access Management (IAM) ロールに使用するのは、「SSM Agent と AWS マネージド S3 バケットとの通信」に挙げた最小限の許可である必要があります。ノードは、Amazon S3 ゲートウェイエンドポイント、NAT ゲートウェイ、またはインターネットゲートウェイを介して Amazon S3 エンドポイントと通信する必要があります。AWS Systems Manager SSM Agent (SSM Agent) の VPC エンドポイント要件の詳細については、「Systems Manager のために VPC エンドポイントを使用して EC2 インスタンスのセキュリティを強化する」を参照してください。

問題: パッチが見つからない

問題: AWS-RunPatchbaseline は正常に完了しましたが、一部のパッチが見つからない。

一般的な原因とその解決策を以下に示します。

原因 1: ベースラインが有効ではありません。

解決策 1: これが原因かどうかを確認するには、以下の手順を実行します。

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。

2. ナビゲーションペインで、[Run Command] を選択します。
3. [Command history (コマンド履歴)] タブをクリックし、ベースラインをチェックするコマンドを選択します。
4. パッチがないマネージドノードを選択します。
5. [Step 1 - Output (ステップ 1 - 出力)] を選択し、`BaselineId` 値を見つけます。
6. 割り当てられたパッチベースライン設定、つまり、パッチベースラインのオペレーティングシステム、製品名、分類、および重大度を確認します。
7. [Microsoft Update Catalog] に移動します。
8. Microsoft Knowledge Base (KB) の記事 ID (KB3216916 など) を検索します。
9. [Product] (成果) の値がマネージドノードの値と一致することを確認し、対応する [Title] (タイトル) を選択します。新しい [Update Details (詳細を更新)] ウィンドウが開きます。
10. [Overview (概要)] タブで、[classification (分類)]と [MSRC severity (MSRC の重大度)]は、前に見つけたパッチベースライン設定と一致する必要があります。

原因 2: パッチが置き換えられました。

解決策 2: これが本当かどうかを確認するには、以下の手順を実行します。

1. [Microsoft Update Catalog] に移動します。
2. Microsoft Knowledge Base (KB) の記事 ID (KB3216916 など) を検索します。
3. [Product] (成果) の値がマネージドノードの値と一致することを確認し、対応する [Title] (タイトル) を選択します。新しい [Update Details (詳細を更新)] ウィンドウが開きます。
4. [Package Details (パッケージの詳細)] タブに移動します。[This update has been replaced by the following updates: (この更新は次の更新に置き換えられました:)] ヘッダーの下でエントリを探します。

原因 3: WSUS と Window のオンライン更新プログラムは、Microsoft によって独立したリリースチャネルとして処理されるため、同じ修正プログラムの KB 番号が異なる可能性があります。

解決策 3: パッチの適格性を確認します。パッケージが WSUS で利用できない場合は、OS Build 14393.3115 をインストールします。パッケージがすべてのオペレーティングシステムビルドで利用できる場合は、OS Build 18362.1256 および 18363.1256 をインストールします。

AWS サポート Automation ランブックの使用方法

AWS サポートには、パッチ適用に関連する特定の問題のトラブルシューティングに使用できる、2 つの Automation ランブックが用意されています。

- `AWSSupport-TroubleshootWindowsUpdate` – `AWSSupport-TroubleshootWindowsUpdate` ランブックは、Amazon Elastic Compute Cloud (Amazon EC2) Windows Server インスタンスの、Windows Server 更新の失敗につながる可能性のある問題を特定するために使用します。
- `AWSSupport-TroubleshootPatchManagerLinux` – `AWSSupport-TroubleshootPatchManagerLinux` ランブックは、Patch Manager を使用して、Linux ベースのマネージドノードでパッチ障害を引き起こす一般的な問題をトラブルシューティングします。このランブックの主な目的は、パッチコマンドが失敗する根本原因を見きわめ、修復プランを提案することにあります。

> **Note**
>
> Automation ランブックの実行には料金がかかります。詳細については、「AWS Systems Manager の料金」の「オートメーション」を参照してください。

AWS サポートに連絡する

トラブルシューティングの解決策がこのセクションまたは AWS re:Postでの Systems Manager問題で見つからない、そして開発者、ビジネス、またはエンタープライズ サポート プランがある場合は、AWS サポート で技術サポートケースを作成できます。

サポート に連絡する前に、以下の情報を収集します。

- SSM Agent ログ
- Run Command コマンド ID、メンテナンスウィンドウ ID、またはオートメーション実行 ID
- Windows Server マネージドノードの場合では、以下も収集します。
  - パッチのインストール方法 の Windows タブで説明されている `%PROGRAMDATA%\Amazon\PatchBaselineOperations\Logs`
  - Windows の更新ログ:Windows Server 2012 R2 以前の場合、`%windir%/WindowsUpdate.log` を使用してください。Windows Server 2016 以降の場合は、`%windir%/WindowsUpdate.log` を使用する前にまず PowerShell コマンド `Get-WindowsUpdateLog` を実行します

- Linux マネージドノードの場合では、以下も収集します。
  - /var/lib/amazon/ssm/*instance-id*/document/orchestration/*Run-Command-execution-id*/awsrunShellScript/PatchLinux ディレクトリの内容。

AWS Systems Manager Run Command

AWS Systems Manager のツールである Run Command では、マネージドノードの設定を安全にリモートで管理することができます。マネージドノードは、Systems Manager のために設定された「ハイブリッドおよびマルチクラウド」環境内の Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは非 EC2 マシンのことです。Run Command を使用すると、一般的な管理タスクを自動化し、1 回限りの大規模な設定変更を実行できます。AWS Management Console の Run Command、AWS Command Line Interface (AWS CLI)、AWS Tools for Windows PowerShell、または AWS SDK から を使用できます。Run Command は追加料金なしで提供されています。Run Command の使用を開始するには、Systems Manager コンソールを開きます。ナビゲーションペインで、[Run Command] を選択します。

管理者は、Run Command を使用することで、アプリケーションのインストールまたはブートストラップ、デプロイ パイプラインの構築、Auto Scaling グループからインスタンスが削除された時のログ ファイルのキャプチャ、インスタンスの Windows ドメインへの結合といったタスクを実行できます。

API をサポートしているシステムの分散特性により、Run Command API は結果整合性モデルに従います。つまり、リソースに影響を及ぼす、実行した API コマンドの結果は、その後に実行するすべてのコマンドにすぐには表示されない可能性があります。前の API コマンドの直後に API コマンドを実行する場合は、この点に留意する必要があります。

概要

次の表には、Run Command の使用を開始するのに役立つ情報が含まれています。

トピック	詳細
AWS Systems Manager のマネージドノードのセットアップ	ハイブリッドおよびマルチクラウド環境で、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスと非 EC2 マシンのセットアップ要件を完了していることを確認します。

トピック	詳細
Systems Manager を利用したハイブリッド環境およびマルチクラウド環境でのノードの管理	(オプション) オンプレミスサーバーと VM を AWS に登録し、Run Command で管理できるようにします。
the section called “Systems Manager を利用したエッジデバイスの管理”	(オプション) Run Command を使ってエッジデバイスを管理できるように設定します。
マネージドノードでのコマンドの実行	AWS Management Console を使用して、1 つ以上のマネージドノードを対象とするコマンドを実行する方法を学習します。
Run Command のチュートリアル	Tools for Windows PowerShell または AWS CLI を使用してコマンドを実行する方法について説明します。

EventBridge のサポート

この Systems Manager のツールは、Amazon EventBridge ルールでイベントタイプおよびターゲットタイプとしてサポートされています。詳細については、「Amazon EventBridge を使用して Systems Manager イベントをモニタリングする」および「リファレンス: Systems Manager 用の Amazon EventBridge イベントパターンとタイプ」を参照してください。

詳細情報

- EC2 インスタンスでリモートに Run Command を実行する (10 分間のチュートリアル)
- Amazon Web Services 全般のリファレンス の Systems Manager Service Quotas
- AWS Systems Manager API リファレンス

トピック

- Run Command を設定する
- マネージドノードでのコマンドの実行
- コマンドでの終了コードの使用
- コマンドのステータスについて
- Run Command のチュートリアル

- Systems Manager Run Command のトラブルシューティング

Run Command を設定する

AWS Systems Manager のツールである Run Command を使用してノードを管理する前に、コマンドを実行するユーザーの AWS Identity and Access Management (IAM) ポリシーを設定する必要があります。IAM ポリシーで SendCommand アクションにグローバル条件キーを使用する場合は、aws:ViaAWSService 条件キーを対象に含め、かつブール値を true に設定する必要があります。以下に例を示します。

```
{
"Version": "2012-10-17",
"Statement": [
    {
    "Effect": "Allow",
    "Action": ["ssm:SendCommand"],
    "Resource": ["arn:aws:ssm:region:account:document/YourDocument"],
    "Condition": {
        "StringEquals": {
        "aws:SourceVpce": ["vpce-example1234"]
        }
    }
    },
    {
    "Effect": "Allow",
    "Action": ["ssm:SendCommand"],
    "Resource": ["arn:aws:ssm:region:account:document/YourDocument"],
    "Condition": {
        "Bool": {"aws:ViaAWSService": "true"}
        }
    }
  ]
}
```

また、Systems Manager 用のノードを設定する必要があります。詳細については、「AWS Systems Manager のマネージドノードのセットアップ」を参照してください。

マネージドノードのセキュリティ体制や日常管理を最小限に抑えるために、以下のオプションのセットアップタスクを実行することを強くお勧めします。

Amazon EventBridge を使用してコマンドの実行をモニタリングする

EventBridge を使用して、コマンド実行ステータスの変更を記録できます。状態の遷移があると実行されるルールや、関心のある 1 以上の遷移があると実行されるルールを作成できます。EventBridge イベントが発生した場合、ターゲットアクションとして Run Command を指定することもできます。詳細については、「Systems Manager イベント用の EventBridge を設定する」を参照してください。

Amazon CloudWatch Logs を使用してコマンドの実行をモニタリングする

すべてのコマンド出力とエラーログを Amazon CloudWatch Logs グループに定期的に送信するように Run Command を設定できます。これらの出力ログは、ほぼリアルタイムでモニタリングし、特定の語句、値、またはパターンを検索して、検索に基づいてアラームを作成できます。詳細については、「Run Command の Amazon CloudWatch Logs の設定」を参照してください。

特定のマネージドノードへの Run Command アクセスを制限

AWS Identity and Access Management (IAM) を使用して、マネージドノードでコマンドを実行するユーザーの能力を制限することができます。具体的には、特定のタグ付けされたマネージドノードでのみユーザーがコマンドを実行できるようにする条件を含む IAM ポリシーを作成できます。詳細については、「タグによる Run Command アクセスを制限」を参照してください。

タグによる Run Command アクセスを制限

このセクションでは、IAM ポリシーでタグ条件を指定して、マネージドノードでコマンドを実行するユーザーの機能を制限する方法について説明します。マネージドノードには、Systems Manager に設定されたハイブリッドおよびマルチクラウド環境で Amazon EC2 インスタンスと非 EC2 ノードが含まれます。情報は明示されていませんが、マネージド AWS IoT Greengrass ヘコアデバイスのアクセスを制限することもできます。開始するには、AWS IoT Greengrass デバイスのタグ付けが必要です。詳細については、「AWS IoT Greengrass Version 2 デベロッパーガイド」の「AWS IoT Greengrass Version 2 リソースのタグ付け」を参照してください。

ユーザーが特定のタグが付けられたノードでのみコマンドを実行できるようにする条件を含む IAM ポリシーを作成して、コマンドの実行を特定のマネージドノードに制限できます。次の例で、ユーザーは、任意のノード (`Resource: arn:aws:ec2:*:*:instance/*`) で任意の SSM ドキュメント (`Resource: arn:aws:ssm:*:*:document/*`) を使うことにより、そのノードが Finance WebServer (`ssm:resourceTag/Finance: WebServer`) であるという条件で、Run Command (`Effect: Allow, Action: ssm:SendCommand`) を使用できます。タグ付けされていないノードや、`Finance: WebServer` 以外のタグを持つノードにコマンドをユーザーが送信した場合、実行結果は `AccessDenied` と表示されます。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "ssm:SendCommand"
         ],
         "Resource":[
            "arn:aws:ssm:*:*:document/*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "ssm:SendCommand"
         ],
         "Resource":[
            "arn:aws:ec2:*:*:instance/*"
         ],
         "Condition":{
            "StringLike":{
               "ssm:resourceTag/Finance":[
                  "WebServers"
               ]
            }
         }
      }
   ]
}
```

複数のタグ付けられたマネージドノードでユーザーがコマンドを実行できるよう許可する IAM ポリシーを作成できます。次のポリシーでは、ユーザーは 2 つのタグがあるマネージドノードでコマンドを実行できます。これらの両方のタグ付けされていていないノードにユーザーがコマンドを送信した場合、実行結果は AccessDenied と表示されます。

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

```
            "ssm:SendCommand"
         ],
         "Resource":"*",
         "Condition":{
            "StringLike":{
               "ssm:resourceTag/tag_key1":[
                  "tag_value1"
               ],
               "ssm:resourceTag/tag_key2":[
                  "tag_value2"
               ]
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":[
            "ssm:SendCommand"
         ],
         "Resource":[
            "arn:aws:ssm:us-west-1::document/AWS-*",
            "arn:aws:ssm:us-east-2::document/AWS-*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "ssm:UpdateInstanceInformation",
            "ssm:ListCommands",
            "ssm:ListCommandInvocations",
            "ssm:GetDocument"
         ],
         "Resource":"*"
      }
   ]
}
```

タグ付けられたマネージドノードの複数のグループでユーザーがコマンドを実行できるようにする IAM ポリシーを作成することもできます。次のサンプルポリシーでは、ユーザーはタグ付けされたノードのいずれかのグループ、または両方のグループでコマンドを実行できます。

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

```
    "Statement":[
       {
          "Effect":"Allow",
          "Action":[
             "ssm:SendCommand"
          ],
          "Resource":"*",
          "Condition":{
             "StringLike":{
                "ssm:resourceTag/tag_key1":[
                   "tag_value1"
                ]
             }
          }
       },
       {
          "Effect":"Allow",
          "Action":[
             "ssm:SendCommand"
          ],
          "Resource":"*",
          "Condition":{
             "StringLike":{
                "ssm:resourceTag/tag_key2":[
                   "tag_value2"
                ]
             }
          }
       },
       {
          "Effect":"Allow",
          "Action":[
             "ssm:SendCommand"
          ],
          "Resource":[
             "arn:aws:ssm:us-west-1::document/AWS-*",
             "arn:aws:ssm:us-east-2::document/AWS-*"
          ]
       },
       {
          "Effect":"Allow",
          "Action":[
             "ssm:UpdateInstanceInformation",
             "ssm:ListCommands",
```

```
            "ssm:ListCommandInvocations",
            "ssm:GetDocument"
         ],
         "Resource":"*"
      }
   ]
}
```

IAM ポリシーの作成の詳細については、「IAM ユーザーガイド」の「マネージドポリシーとインラインポリシー」を参照してください。マネージドノードへのタグ付けの詳細については、「AWS Resource Groups ユーザーガイド」の「タグエディタ」を参照してください。

マネージドノードでのコマンドの実行

このセクションでは、AWS Systems Manager コンソールからマネージドノードにコマンドを送信する方法について説明します。このセクションでは、コマンドをキャンセルする方法についても説明しています。

ノードが var ディレクトリの noexec マウントオプションで設定されている場合、Run Command はコマンドを正常に実行できないことに注意してください。

> **Important**
>
> Run Command を使用してコマンドを送信する場合は、パスワード、設定データ、その他のシークレットなどの機密情報をプレーンテキスト形式で含めないでください。アカウント内のすべての Systems Manager API アクティビティは、AWS CloudTrail ログの S3 バケットにログ記録されます。つまり、その S3 バケットへのアクセス権を持つユーザーは、これらの秘密のプレーンテキスト値を表示できます。このため、Systems Manager オペレーションで使用する機密データを暗号化するために、`SecureString` パラメータを作成して使用することをお勧めします。
> 詳細については、「IAM ポリシーを使用して Parameter Store パラメータへのアクセスを制限する」を参照してください。

実行履歴の保持

各コマンドの履歴は、最大 30 日利用可能です。さらに、すべてのログファイルのコピーを Amazon Simple Storage Service に保存するか、すべての API 呼び出しの監査証跡を AWS CloudTrail に維持することができます。

関連情報

他のツールを使用してコマンドを送信する方法については、次のトピックを参照してください。

- チュートリアル: Run Command で AWS Tools for Windows PowerShell を使用する または、AWS Tools for PowerShell Cmdlet Reference の AWS Systems Manager セクション の例。
- チュートリアル: Run Command で AWS CLI を使用する または SSM CLI リファレンス の例

内容

- コンソールからコマンドを実行する
- 特定のドキュメントバージョンを使用したコマンドの実行
- コマンドを大規模に実行する
- コマンドをキャンセルする

コンソールからコマンドを実行する

AWS Management Consoleから Run Command (AWS Systems Manager のツール) を使って、マネージドノードにログインせずに設定することができます。このトピックでは、Run Command を使用してマネージドノードの SSM Agent を更新する方法の例を示します。

[開始する前に]

Run Command を使用してコマンドを送信する前に、マネージドノードが Systems Manager の設定要件を満たすことを確認します。

Run Command を使用してコマンドを送信するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Run Command] を選択します。
3. [Run command (コマンドの実行)] を選択します。
4. [Command document] リストで、Systems Manager ドキュメントを選択します。
5. [Command parameters] セクションで、必須パラメータの値を指定します。
6. [Targets] (ターゲット) セクションで、タグの指定、インスタンスやエッジデバイスの手動選択、リソースグループの指定により、このオペレーションを実行するマネージドノードを選択します。

> **Tip**
>
> 表示されるはずのマネージドノードが表示されない場合は、トラブルシューティングのヒントについて「マネージドノードの可用性のトラブルシューティング」を参照してください。

7. [その他のパラメータ] で、以下の操作を行います。

   - [コメント] に、このコマンドに関する情報を入力します。
   - [タイムアウト (秒)] に、コマンドの実行全体が失敗するまでにシステムが待機する秒数を指定します。

8. [レート制御] の場合:

   - [同時実行数] の場合、コマンドを同時に実行するマネージドノードの数または割合を指定します。

     > **Note**
     >
     > マネージドノードに適用されるタグを指定するか、AWS リソースグループを指定してターゲットを選択し、ターゲットとなるマネージドノードの数が不明な場合は、割合を指定してドキュメントを同時に実行できるターゲットの数を制限します。

   - [エラーのしきい値] で、ノードの数または割合のいずれかで失敗した後、他のマネージドノードでのコマンドの実行をいつ停止するか指定します。例えば、3 つのエラーを指定した場合、4 番目のエラーが受信されると、システムマネージャー はコマンドの送信を停止します。コマンドを処理しているマネージドノードもエラーを送信する可能性があります。

9. (オプション) モニタリング用のコマンドに適用する CloudWatch アラームを選択します。CloudWatch アラームをコマンドにアタッチするには、コマンドを実行する IAM プリンシパルに `iam:createServiceLinkedRole` アクションの権限が必要です。CloudWatch アラームの詳細については、「Amazon CloudWatch でのアラームの使用」を参照してください。アラームがアクティブ化されると、保留中のコマンド呼び出しは実行されません。

10. (オプション) コマンド出力をファイルに保存する場合は、[出力オプション] の [S3 バケットにコマンド出力を書き込む] ボックスを選択します。ボックスにバケット名とプレフィックス (フォルダ) 名を入力します。

> **Note**
>
> S3 バケットにデータを書き込む機能を許可する S3 許可は、このタスクを実行する IAM ユーザーのものではなく、インスタンスに割り当てられたインスタンスプロファイル (EC2 インスタンスの場合) または IAM サービスロール (ハイブリッドアクティベーションマシン) のものです。詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」または「ハイブリッド環境に IAM サービスロールを作成する」を参照してください。さらに、指定された S3 バケットが別の AWS アカウント にある場合は、マネージドノードに関連付けられたインスタンスプロファイルまたは IAM サービスロールが、そのバケットへの書き込みに必要なアクセス許可があることを確認してください。

11. [SNS Notifications (SNS 通知)] セクションで、コマンドの実行状態に関する通知を受け取る場合は、[Enable SNS notifications (SNS 通知を有効にする)] チェックボックスをオンにします。

    Run Command 用の Amazon SNS 通知の設定の詳細については、「Amazon SNS 通知を使用した Systems Manager のステータス変更のモニタリング」を参照してください。

12. [Run (実行)] を選択します。

コマンドのキャンセルの詳細については、the section called “コマンドをキャンセルする” を参照してください。

コマンドを再実行する

Systems Manager には、Systems Manager コンソールの Run Command ページからコマンドを再実行できる 2 つのオプションがあります。

- Rerun (再実行): このボタンを使用すると、変更を加えずに同じコマンドを実行できます。
- Copy to new (新規にコピー): このボタンをクリックすると、1 つのコマンドの設定が新しいコマンドにコピーされ、実行前にこれらの設定を編集できます。

コマンドを再実行するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Run Command] を選択します。

3. 再実行するコマンドを選択します。コマンドの詳細ページで、コマンドを実行した直後にコマンドを再実行できます。または、以前に実行したコマンドを [Command history] (コマンド履歴) タブから選択することもできます。
4. [Rerun (再実行)] を選択して同じコマンドを変更せずに実行するか、[Copy to new (新規にコピー)] を選択して、実行する前にコマンド設定を編集します。

特定のドキュメントバージョンを使用したコマンドの実行

ドキュメントバージョンパラメータを使用して、コマンドの実行時に使用する AWS Systems Manager ドキュメントのバージョンを指定できます。このパラメータに指定できるオプションは以下のとおりです。

- $DEFAULT
- $LATEST
- バージョン番号

ドキュメントバージョンパラメータを使用してコマンドを実行するには、次の手順を実行します。

Linux

ローカルの Linux マシンで AWS CLI を使用してコマンドを実行するには

1. まだ AWS Command Line Interface (AWS CLI) をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」を参照してください。
2. 利用可能なすべてのドキュメントを表示します。

   このコマンドでは、AWS Identity and Access Management(IAM) アクセス許可に基づいて、アカウントで利用可能なすべてのドキュメントが表示されます。

   ```
   aws ssm list-documents
   ```
3. ドキュメントのバージョンを一覧表示するには、次のコマンドを実行します。*document name* を自分の情報に置き換えます。

   ```
   aws ssm list-document-versions \
   ```

```
    --name "document name"
```

4. SSM ドキュメントバージョンを実行するコマンドを実行するには、次のコマンドを使用します。各##############をユーザー自身の情報に置き換えます。

```
aws ssm send-command \
    --document-name "AWS-RunShellScript" \
    --parameters commands="echo Hello" \
    --instance-ids instance-ID \
    --document-version '$LATEST'
```

Windows

ローカル Windows マシンで AWS CLI を使用してコマンドを実行するには

1. まだ AWS Command Line Interface (AWS CLI) をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」を参照してください。

2. 利用可能なすべてのドキュメントを表示します。

   このコマンドでは、AWS Identity and Access Management(IAM) アクセス許可に基づいて、アカウントで利用可能なすべてのドキュメントが表示されます。

```
aws ssm list-documents
```

3. ドキュメントのバージョンを一覧表示するには、次のコマンドを実行します。*document name* を自分の情報に置き換えます。

```
aws ssm list-document-versions ^
    --name "document name"
```

4. SSM ドキュメントバージョンを実行するコマンドを実行するには、次のコマンドを使用します。各##############をユーザー自身の情報に置き換えます。

```
aws ssm send-command ^
    --document-name "AWS-RunShellScript" ^
    --parameters commands="echo Hello" ^
    --instance-ids instance-ID ^
```

```
    --document-version "$LATEST"
```

PowerShell

Tools for PowerShell を使用してコマンドを実行するには

1. AWS Tools for PowerShell (Tools for Windows PowerShell) をインストールして設定します (まだインストールしていない場合)。

   詳細については、「AWS Tools for PowerShell のインストール」を参照してください。
2. 利用可能なすべてのドキュメントを表示します。

   このコマンドでは、AWS Identity and Access Management(IAM) アクセス許可に基づいて、アカウントで利用可能なすべてのドキュメントが表示されます。

   ```
   Get-SSMDocumentList
   ```
3. ドキュメントのバージョンを一覧表示するには、次のコマンドを実行します。*document name* を自分の情報に置き換えます。

   ```
   Get-SSMDocumentVersionList `
       -Name "document name"
   ```
4. SSM ドキュメントバージョンを実行するコマンドを実行するには、次のコマンドを使用します。各##############をユーザー自身の情報に置き換えます。

   ```
   Send-SSMCommand `
       -DocumentName "AWS-RunShellScript" `
       -Parameter @{commands = "echo helloWorld"} `
       -InstanceIds "instance-ID" `
       -DocumentVersion $LATEST
   ```

コマンドを大規模に実行する

AWS Systems Manager のツールである Run Command を使用すると、targets を使用してマネージドノードのフリートでコマンドを実行できます。targets パラメータは、マネージドノードに指定したタグに基づいて Key,Value の組み合わせを受け取ります。コマンドを実行すると、システムは指定されたタグと一致するすべてのマネージドノードでコマンドの実行を試みます。マネージドインスタンスへのタグ付けの詳細については、「AWS リソースのタグ付けユーザーガイド」の「AWS

リソースのタグ付け」を参照してください。マネージド IoT デバイスへのタグ付けの詳細については、「AWS IoT Greengrass Version 2 デベロッパーガイド」の「AWS IoT Greengrass Version 2 リソースのタグ付け」を参照してください。

以下のセクションで説明しているように、targets パラメータを使用して、特定のマネージドノード ID のリストをターゲットにできます。

数百または数千のマネージドノードでコマンド実行を制御するために、Run Command は、リクエストを同時に処理できるノード数とコマンドがキャンセルされるまでに投げられるエラー数を制限するためのパラメータも用意されています。

内容

- 複数のマネージドノードをターゲットにする
- レート制御の使用

複数のマネージドノードをターゲットにする

タグ、AWS リソースグループ名、またはマネージドノード ID を指定してコマンドを実行しマネージドノードをターゲットにできます。

次の例では、AWS Command Line Interface (AWS CLI) から Run Command を使用した場合のコマンド形式を示します。各*##############*をユーザー自身の情報に置き換えます。このセクションのサンプルコマンドは、[...] で省略されています。

例 1: タグをターゲットにする

Linux & macOS

```
aws ssm send-command \
    --document-name document-name \
    --targets Key=tag:tag-name,Values=tag-value \
    [...]
```

Windows

```
aws ssm send-command ^
    --document-name document-name ^
    --targets Key=tag:tag-name,Values=tag-value ^
    [...]
```

例 2: AWS リソースグループを名前に基づいてターゲットにする

コマンドごとに最大 1 つのリソースグループ名を指定できます。リソースグループを作成する場合は、リソースタイプとして AWS::SSM:ManagedInstance と AWS::EC2::Instance をグループ化の条件に含めることをお勧めします。

> **Note**
>
> リソースグループをターゲットとするコマンドを送信するには、そのグループに属するリソースをリストまたは表示する AWS Identity and Access Management (IAM) 許可が付与されている必要があります。詳細については、AWS Resource Groups ユーザーガイド の「許可の設定」を参照してください。

Linux & macOS

```
aws ssm send-command \
    --document-name document-name \
    --targets Key=resource-groups:Name,Values=resource-group-name \
    [...]
```

Windows

```
aws ssm send-command ^
    --document-name document-name ^
    --targets Key=resource-groups:Name,Values=resource-group-name ^
    [...]
```

例 3: リソースタイプにより AWS リソースグループをターゲットにする

コマンドごとに最大 5 つのリソースグループタイプを指定できます。リソースグループを作成する場合は、リソースタイプとして AWS::SSM:ManagedInstance と AWS::EC2::Instance をグループ化の条件に含めることをお勧めします。

> **Note**
>
> リソースグループをターゲットとするコマンドを送信するには、そのグループに属するリソースをリストまたは表示する IAM アクセス許可が付与されている必要があります。詳細については、AWS Resource Groups ユーザーガイド の「許可の設定」を参照してください。

Linux & macOS

```
aws ssm send-command \
    --document-name document-name \
    --targets Key=resource-groups:ResourceTypeFilters,Values=resource-
type-1,resource-type-2 \
    [...]
```

Windows

```
aws ssm send-command ^
    --document-name document-name ^
    --targets Key=resource-groups:ResourceTypeFilters,Values=resource-
type-1,resource-type-2 ^
    [...]
```

例 4: インスタンス ID をターゲットにする

以下の例では、instanceids キー と targets パラメータを使用してマネージドノードをターゲットにする方法を示します。各デバイスには mi-*ID_number* が割り当てられているので、このキーを使ってマネージド AWS IoT Greengrass コアデバイスをターゲットにすることができます。デバイス ID は AWS Systems Manager のツールである Fleet Manager で確認できます。

Linux & macOS

```
aws ssm send-command \
    --document-name document-name \
    --targets Key=instanceids,Values=instance-ID-1,instance-ID-2,instance-ID-3 \
    [...]
```

Windows

```
aws ssm send-command ^
    --document-name document-name ^
    --targets Key=instanceids,Values=instance-ID-1,instance-ID-2,instance-ID-3 ^
    [...]
```

Development、Test、Pre-production、Production の Environment と Values という名前の Key を使用して、複数の異なる環境のマネージドノードに対してタグ付けされると、次の構文の

targets パラメータを使用してこれらの環境の 1 つにあるすべてのマネージドノードにコマンドを送信できます。

Linux & macOS

```
aws ssm send-command \
    --document-name document-name \
    --targets Key=tag:Environment,Values=Development \
    [...]
```

Windows

```
aws ssm send-command ^
    --document-name document-name ^
    --targets Key=tag:Environment,Values=Development ^
    [...]
```

Values リストに追加して、他の環境の追加マネージドノードをターゲットにすることができます。カンマを使用して項目を区切ります。

Linux & macOS

```
aws ssm send-command \
    --document-name document-name \
    --targets Key=tag:Environment,Values=Development,Test,Pre-production \
    [...]
```

Windows

```
aws ssm send-command ^
    --document-name document-name ^
    --targets Key=tag:Environment,Values=Development,Test,Pre-production ^
    [...]
```

バリエーション: 複数の Key 条件を使用してターゲットを絞り込む

複数の Key 条件を含めて、コマンドのターゲットの数を絞り込むことができます。複数の Key 条件を含めると、システムは全ての条件を満たしたマネージドノードをターゲットにします。次のコマンド

は、Finance Department およびデータベース サーバーロールに対してタグが付いているすべてのマネージドノードをターゲットとします。

Linux & macOS

```
aws ssm send-command \
    --document-name document-name \
    --targets Key=tag:Department,Values=Finance Key=tag:ServerRole,Values=Database \
    [...]
```

Windows

```
aws ssm send-command ^
    --document-name document-name ^
    --targets Key=tag:Department,Values=Finance Key=tag:ServerRole,Values=Database ^
    [...]
```

バリエーション: Key および Value 条件を使用する

前の例を拡大し、Values 条件の項目を追加して含めて、複数の部門とサーバーロールを対象にすることができます。

Linux & macOS

```
aws ssm send-command \
    --document-name document-name \
    --targets Key=tag:Department,Values=Finance,Marketing
 Key=tag:ServerRole,Values=WebServer,Database \
    [...]
```

Windows

```
aws ssm send-command ^
    --document-name document-name ^
    --targets Key=tag:Department,Values=Finance,Marketing
 Key=tag:ServerRole,Values=WebServer,Database ^
    [...]
```

バリエーション: 複数の Values 条件を使用してタグ付けされたマネージドノードをターゲットにします

複数の異なる環境のマネージドノードに対して Sales および Finance のうち Department と Values という Key を使用してタグ付けされた場合、次の targets パラメータを使用した構文でこれらの環境のすべてのマネージドノードに対してコマンドを送信できます。

Linux & macOS

```
aws ssm send-command \
    --document-name document-name \
    --targets Key=tag:Department,Values=Sales,Finance \
    [...]
```

Windows

```
aws ssm send-command ^
    --document-name document-name ^
    --targets Key=tag:Department,Values=Sales,Finance ^
    [...]
```

各キーには、最大 5 つのタグキーと 5 つの値を指定できます。

タグキー (タグの名前) またはタグ値にスペースが含まれる場合、次の例に示すようにタグキーまたは値を疑問符で囲みます。

例: Value タグにスペースが含まれる場合

Linux & macOS

```
aws ssm send-command \
    --document-name document-name \
    --targets Key=tag:OS,Values="Windows Server 2016" \
    [...]
```

Windows

```
aws ssm send-command ^
    --document-name document-name ^
    --targets Key=tag:OS,Values="Windows Server 2016" ^
    [...]
```

例: tag キーと Value にスペースが含まれる場合

Linux & macOS

```
aws ssm send-command \
    --document-name document-name \
    --targets Key="tag:Operating System",Values="Windows Server 2016" \
    [...]
```

Windows

```
aws ssm send-command ^
    --document-name document-name ^
    --targets Key="tag:Operating System",Values="Windows Server 2016" ^
    [...]
```

例: Values のリスト内にある 1 つの項目にスペースが含まれる場合

Linux & macOS

```
aws ssm send-command \
    --document-name document-name \
    --targets Key=tag:Department,Values="Sales","Finance","Systems Mgmt" \
    [...]
```

Windows

```
aws ssm send-command ^
    --document-name document-name ^
    --targets Key=tag:Department,Values="Sales","Finance","Systems Mgmt" ^
    [...]
```

レート制御の使用

コマンドがグループ内のマネージドノードに送信されるレートは、同時実行制御とエラー制御を使用して制御できます。

トピック

- 同時実行制御を使用する
- エラー制御を使用する

同時実行制御を使用する

max-concurrency パラメータ [Run a command] (コマンドを実行) ページの [Concurrency] (同時実行数) オプションを使用して、同時にコマンドを実行するマネージドノードの数を制御できます。マネージドノードの絶対数 (**10** など) またはターゲットセットの割合 (**10%** など) を指定できます。キューシステムにより、コマンドは 1 つのノードに送信され、システムがこの最初の呼び出しを確認するのを待ってから、さらに 2 つのノードにコマンドが送信されます。システムで max-concurrency の値に達するまで、指数関数的に多くのノードにコマンドを送ります。max-concurrency のデフォルト値は 50 です。次の例は、max-concurrency パラメータの値を指定する方法を示しています。

Linux & macOS

```
aws ssm send-command \
    --document-name document-name \
    --max-concurrency 10 \
    --targets Key=tag:Environment,Values=Development \
    [...]
```

```
aws ssm send-command \
    --document-name document-name \
    --max-concurrency 10% \
    --targets Key=tag:Department,Values=Finance,Marketing
 Key=tag:ServerRole,Values=WebServer,Database \
    [...]
```

Windows

```
aws ssm send-command ^
    --document-name document-name ^
    --max-concurrency 10 ^
    --targets Key=tag:Environment,Values=Development ^
    [...]
```

```
aws ssm send-command ^
    --document-name document-name ^
    --max-concurrency 10% ^
    --targets Key=tag:Department,Values=Finance,Marketing
 Key=tag:ServerRole,Values=WebServer,Database ^
    [...]
```

エラー制御を使用する

コマンドの実行を数百または数千のマネージドノードに制限するには、max-errors パラメータを使用してエラー制限を設定することもできます ([Run a command] (コマンドを実行) ページの [Error threshold] (エラーのしきい値) フィールド)。このパラメータは、システムが追加のマネージドノードへのコマンドの送信を停止するまでに許可されるエラーの数を指定します。エラーの絶対数 (**10** など) またはターゲットセットのパーセント数 (**10%** など) を指定できます。たとえば、**3** を指定した場合、4 番目のエラーが受信されると、システムからコマンドが送信されなくなります。**0** を指定した場合、最初のエラー結果が返されると、追加のマネージドノードへのコマンド送信を停止します。コマンドの送信先のマネージノード数が 50 で max-errors を **10%** に設定した場合、6 番目のエラーが受信されると、システムから他のノードにコマンドが送信されなくなります。

max-errors に達したときに既にコマンドを実行中の呼び出しについては、完了はできますが、一部が失敗する場合があります。呼び出しの失敗数が max-errors を超えないようにするには、max-concurrency を **1** に設定して、一度に 1 つの呼び出しが処理されるようにします。max-errors のデフォルト値は 0 です。次の例は、max-errors パラメータの値を指定する方法を示しています。

Linux & macOS

```
aws ssm send-command \
    --document-name document-name \
    --max-errors 10 \
    --targets Key=tag:Database,Values=Development \
    [...]
```

```
aws ssm send-command \
    --document-name document-name \
    --max-errors 10% \
    --targets Key=tag:Environment,Values=Development \
    [...]
```

```
aws ssm send-command \
    --document-name document-name \
    --max-concurrency 1 \
    --max-errors 1 \
    --targets Key=tag:Environment,Values=Production \
    [...]
```

Windows

```
aws ssm send-command ^
    --document-name document-name ^
    --max-errors 10 ^
    --targets Key=tag:Database,Values=Development ^
    [...]
```

```
aws ssm send-command ^
    --document-name document-name ^
    --max-errors 10% ^
    --targets Key=tag:Environment,Values=Development ^
    [...]
```

```
aws ssm send-command ^
    --document-name document-name ^
    --max-concurrency 1 ^
    --max-errors 1 ^
    --targets Key=tag:Environment,Values=Production ^
    [...]
```

コマンドをキャンセルする

コマンドの状態が [Pending] (保留中) または [Executing] (実行中) であるとサービスに示されている間は、コマンドのキャンセルを試行できます。ただし、まだコマンドがこれらの状態のいずれかであっても、コマンドがキャンセルされ、その基盤であるプロセスが停止することは保証されません。

コンソールを使用してコマンドをキャンセルするには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Run Command] を選択します。
3. キャンセルするコマンド呼び出しを選択します。
4. [Cancel command] を選択します。

AWS CLI を使用してコマンドをキャンセルするには

以下のコマンドを実行します。各##############をユーザー自身の情報に置き換えます。

Linux & macOS

```
aws ssm cancel-command \
    --command-id "command-ID" \
    --instance-ids "instance-ID"
```

Windows

```
aws ssm cancel-command ^
    --command-id "command-ID" ^
    --instance-ids "instance-ID"
```

キャンセルしたコマンドのステータスについては、「コマンドのステータスについて」を参照してください。

コマンドでの終了コードの使用

場合によっては、終了コードを使用して、コマンドの処理方法を管理する必要があるかもしれません。

コマンドで終了コードを指定する

AWS Systems Manager のツールである Run Command を使用すると、終了コードを指定してコマンドの処理方法を決定できます。デフォルトでは、スクリプトで最後に実行されたコマンドの終了コードは、スクリプト全体の終了コードとしてレポートされます。たとえば、3 つのコマンドを含むスクリプトがあるとします。最初のコマンドは失敗しますが、その次のコマンドは成功します。最後のコマンドが成功したため、実行のステータスは succeeded としてレポートされます。

シェルスクリプト

最初のコマンド失敗時にスクリプト全体を失敗として処理するには、シェルの条件ステートメントを含めて、最後のコマンドが失敗する前にいずれかのコマンドが失敗した場合にスクリプトを終了させることができます。以下の方法を使用します。

```
<command 1>
    if [ $? != 0 ]
    then
        exit <N>
    fi
    <command 2>
```

```
    <command 3>
```

以下の例では、最初のコマンドが失敗すると、スクリプト全体が失敗します。

```
cd /test
    if [ $? != 0 ]
    then
        echo "Failed"
        exit 1
    fi
    date
```

PowerShell スクリプト

PowerShell では、スクリプトで明示的に `exit` を呼び出して、Run Command が終了コードを取得できるようにする必要があります。

```
<command 1>
    if ($?) {<do something>}
    else {exit <N>}
    <command 2>
    <command 3>
    exit <N>
```

以下がその例です。

```
cd C:\
    if ($?) {echo "Success"}
    else {exit 1}
    date
```

コマンド実行時の再起動の処理

AWS Systems Manager のツールである Run Command を使用してマネージドノードを再起動するスクリプトを実行するには、スクリプトで終了コードを指定することをお勧めします。その他のメカニズムを使用して、スクリプトからノードを再起動しようとすると、再起動がスクリプトの最後のステップであっても、スクリプトの実行ステータスが正しく更新されない場合があります。Windows マネージドインスタンスの場合は、スクリプトで `exit 3010` を指定します。Linux と macOS マネージドノードの場合は、`exit 194` を指定します。終了コードは AWS Systems Manager エージェント (SSM Agent) にマネージドノードの再起動を指示し、再起動の完了後にスクリプトを再起

動します。再起動を開始する前に、SSM Agent はクラウドの Systems Manager サービスに対して、サーバーの再起動中に通信が中断されることを知らせます。

> **Note**
>
> 再起動スクリプトは、aws:runDocument プラグインに含まれていません。ドキュメントに再起動スクリプトが含まれている場合に、別のドキュメントが aws:runDocument プラグインを介してドキュメントを実行しようとすると、SSM Agent はエラーが発生します。

べき等スクリプトの作成

マネージドノードを再起動するスクリプトを開発するときは、スクリプトをべき等にし、再起動後もスクリプトの実行が継続されるようにします。べき等なスクリプトは状態を管理し、アクションが実行されたかどうかを検証します。これにより、1 回のみ実行するように意図されているステップが複数回実行されなくなります。

ここでは、マネージドノードを複数回再起動するべき等なスクリプトの例をご紹介します。

```
$name = Get current computer name
If ($name -ne $desiredName)
    {
        Rename computer
        exit 3010
    }

$domain = Get current domain name
If ($domain -ne $desiredDomain)
    {
        Join domain
        exit 3010
    }

If (desired package not installed)
    {
        Install package
        exit 3010
    }
```

例

次のスクリプトサンプルは、終了コードを使用してマネージドノードを再起動します。Linux の例では、Amazon Linux でパッケージ更新をインストールしてから、ノードを再起動します。Windows Server の例では、Telnet-Client をノードにインストールしてから、再起動します。

Amazon Linux

```
#!/bin/bash
yum -y update
needs-restarting -r
if [ $? -eq 1 ]
then
        exit 194
else
        exit 0
fi
```

Windows

```
$telnet = Get-WindowsFeature -Name Telnet-Client
if (-not $telnet.Installed)
    {
        # Install Telnet and then send a reboot request to SSM Agent.
        Install-WindowsFeature -Name "Telnet-Client"
        exit 3010
    }
```

コマンドのステータスについて

Run Command のツールである AWS Systems Manager は、コマンドの各処理状態とコマンドを処理した各マネージノードの詳細なステータス情報をレポートします。次の方法を使用して、コマンドのステータスをモニタリングできます。

- Run Command コンソールインターフェイスの [Commands] (コマンド) タブで、[Refresh] (更新) アイコンを選択します。
- AWS Command Line Interface (AWS CLI) を使用して list-commands または list-command-invocations を呼び出します。あるいは、AWS Tools for Windows PowerShell を使用して Get-SSMCommand または Get-SSMCommandInvocation を呼び出します。
- 状態またはステータスの変更に応答するように Amazon EventBridge を設定します。

- すべての状況の変化、または Failed や TimedOut など特定のステータスに関する通知を送信するよう、Amazon Simple Notification Service (Amazon SNS) を設定します。

Run Command のステータス

Run Command は、プラグイン、呼び出し、コマンドのステータス全体という 3 つのエリアでステータスの詳細をレポートします。プラグインは、コマンドの (SSM) ドキュメントに定義されているコード実行ブロックです。プラグインの詳細については、「コマンドドキュメントプラグインリファレンス」を参照してください。

複数のマネージノードに、コマンドを同時に送信するとき、各ノードを対象とするコマンドの各コピーは、コマンド呼び出しです。例えば、AWS-RunShellScript ドキュメントを使用して 20 個の Linux インスタンスに ifconfig コマンドを送信すると、そのコマンドには 20 個の呼び出しがあります。各コマンド呼び出しで、個別にステータスが報告されます。コマンド呼び出しに含まれているプラグインも、個々にステータスを報告します。

最後に、Run Command コマンドには、すべてのプラグインと呼び出しの集約されたコマンドステータスがあります。集約されたコマンドステータスは、以下の表に示すように、プラグインまたは呼び出しによってレポートされるステータスとは異なる場合があります。

> **Note**
>
> max-concurrency パラメータまたは max-errors パラメータを使用して多数のマネージノードに対してコマンドを実行する場合は、以下の表に示すように、これらのパラメータによって強制される制限がコマンドのステータスに反映されます。これらのパラメータの詳細については、コマンドを大規模に実行するを参照してください。

コマンドのプラグインと呼び出しの詳細なステータス

ステータス	詳細
保留中	コマンドがまだマネージドノードに送信されていないか、SSM Agent によって受信されていません。Timeout (seconds) パラメータと Execution timeout パラメータの合計に等しい時間が経過する前にエージェントがコマンドを

ステータス	詳細
	受信しなかった場合、ステータスは Delivery Timed Out に変わります。
InProgress	Systems Manager がマネージドノードにコマンドを送信しようとしている、またはコマンドが SSM Agent によって受信され、インスタンスでその実行が開始されました。すべてのコマンドプラグインの結果に応じて、ステータスは Success、Failed、 Delivery Timed Out、Execution Timed Out のいずれかに変わります。例外: エージェントが実行中でないか、ノードで使用できない場合、コマンドステータスはエージェントが再び使用可能になるまで、または実行タイムアウト制限に達するまで In Progress のままになります。その後、ステータスは終了状態に変わります。
Delayed	システムからマネージドノードにコマンドを送信しようとしましたが成功しませんでした。システムは再試行します。

ステータス	詳細
Success (成功)	このステータスはさまざまな条件下で返されます。このステータスは、コマンドがノード上で処理されたという意味ではありません。例えば、コマンドはマネージドノードで SSM Agent によって受信され、PowerShell の `ExecutionPolicy` によってコマンドの実行が阻止された結果として終了コード 0 が返されることがあります。これは終了状態です。コマンドが `Success` ステータスを返す条件は次のとおりです。 • 単一のインスタンスをターゲットにした際に、コマンドはマネージドノードで SSM Agent によって受信され、終了コード 0 が返されました。 • 複数のインスタンスをターゲットとする場合、失敗した呼び出しの数がコマンドで指定されたエラーのしきい値を超えていない。 • 複数のインスタンスをターゲットとする場合、少なくとも 1 つの呼び出しは成功したが、他の呼び出しはタイムアウトした。指定されたエラーしきい値は引き続き適用される。 • タグをターゲットとする場合、そのタグに関連付けられたインスタンスが見つからない。 • タグをターゲットとする場合、失敗した呼び出しの数がコマンドで指定されたエラーのしきい値を超えていない。 • タグをターゲットとする場合、少なくとも 1 つの呼び出しは成功したが、他の呼び出しはタイムアウトした。指定されたエラーしきい値は引き続き適用される。 • OS レベルで強制適用されているアプリケーションまたはポリシーにより、コマンドの

ステータス	詳細
	実行が防止またはオーバーライドされ、終了コード 0 が返されます。 **Note** リソースグループをターゲットにする場合も同じ条件が適用されます。エラーをトラブルシューティングする方法、またはコマンド実行に関する詳細情報を取得するには、適切な終了コード (コマンドのエラーの場合はゼロ以外の終了コード) を返すことでエラーまたは例外を処理するコマンドを送信します。
DeliveryTimedOut	合計タイムアウトが期限切れになるまでに、コマンドがマネージドノードに配信されませんでした。合計タイムアウトは、親コマンドの `max-errors` の制限数には影響しませんが、親コマンドのステータスが `Success`、`Incomplete` 、`Delivery Timed Out` のいずれになるかに影響します。これは終了状態です。
ExecutionTimedOut	コマンドのオートメーションは、マネージドノードで開始されましたが、実行タイムアウトが期限切れになるまでに完了しませんでした。実行タイムアウトは障害としてカウントされます。この場合、ゼロ以外の応答が送信され、Systems Manager はコマンドオートメーションの実行の試行を終了し、障害ステータスを報告します。

ステータス	詳細
失敗	マネージドノードでコマンドは失敗しました。プラグインの場合、これは結果コードがゼロではないことを示します。コマンドの呼び出しの場合、これは 1 つ以上のプラグインの結果コードがゼロではないことを示します。呼び出しの失敗は、親コマンドの max-errors の制限数にカウントされます。これは終了状態です。
Cancelled (キャンセル)	コマンドが完了する前にキャンセルされました。これは終了状態です。
Undeliverable	コマンドをマネージドノードに配信できません。ノードは存在していないか、応答していない可能性があります。配信不能な呼び出しは親コマンドの max-errors の制限数にはカウントされませんが、親コマンドのステータスが Success または Incomplete のいずれになるかには影響します。例えば、コマンドのすべての呼び出しのステータスが Undeliverable である場合、返されるコマンドのステータスは Failed です。ただし、コマンドに 5 つの呼び出しがあり、そのうちの 4 つが返したステータスが Undeliverable で 1 つが返したステータスが Success の場合、親コマンドのステータスは Success になります。これは終了状態です。
Terminated	親コマンドが max-errors の制限数を超え、後続のコマンド呼び出しはシステムによって取り消されました。これは終了状態です。

ステータス	詳細
InvalidPlatform	コマンドは、選択したドキュメントで指定された必須プラットフォームと一致しないマネージノードに送信されました。Invalid Platform は、親コマンドの max-errors 制限にはカウントされませんが、親コマンドのステータスが [Success] (成功) または [Failed] (失敗) であるかどうかに影響します。例えば、コマンドのすべての呼び出しのステータスが Invalid Platform である場合、返されるコマンドのステータスは Failed です。ただし、コマンドに 5 つの呼び出しがあり、そのうちの 4 つが返したステータスが Invalid Platform で 1 つが返したステータスが Success の場合、親コマンドのステータスは Success になります。これは終了状態です。
アクセス拒否	コマンドを実行している AWS Identity and Access Management (IAM) ユーザーまたはロールが対象のマネージドノードにアクセスできません。Access Denied は親コマンドの max-errors 制限数にはカウントされませんが、親コマンドのステータスが Success または Failed のいずれになるかには影響します。例えば、コマンドのすべての呼び出しのステータスが Access Denied である場合、返されるコマンドのステータスは Failed です。ただし、コマンドに 5 つの呼び出しがあり、そのうちの 4 つが返したステータスが Access Denied で 1 つが返したステータスが Success の場合、親コマンドのステータスは Success になります。これは終了状態です。

コマンドの詳細なステータス

ステータス	詳細
保留中	マネージドノードでコマンドはエージェントによってまだ受け取られていません。
InProgress	コマンドは、1 つ以上のマネージドノードに送信されましたが、どのノードも終了状態に達していません。
Delayed	システムから ノードにコマンドを送信しようとしましたが成功しませんでした。システムは再試行します。
Success (成功)	コマンドは、SSM Agent の指定したすべてのインスタンスまたは対象となるマネージドノードで受け取られ、終了コードのゼロが返されました。すべてのコマンドの呼び出しが終了状態に達しましたが、`max-errors` の値には達しませんでした。このステータスは、指定されたまたは対象となるすべてのマネージドノードで、コマンドが正常に処理されたという意味ではありません。これは終了状態です。 **Note** エラーをトラブルシューティングする方法、またはコマンド実行に関する詳細情報を取得するには、適切な終了コード (コマンドのエラーの場合はゼロ以外の終了コード) を返すことでエラーまたは例外を処理するコマンドを送信します。
DeliveryTimedOut	合計タイムアウトが期限切れになるまでに、コマンドがマネージドノードに配信されませんでした。`max-errors` の値を超えるコマンドの

ステータス	詳細
	呼び出しが Delivery Timed Out のステータスを示しています。これは終了状態です。
失敗	マネージドノードでコマンドは失敗しました。max-errors の値を超えるコマンドの呼び出しが Failed のステータスを示しています。これは終了状態です。
Incomplete	コマンドは、すべてのマネージドノードで試行されましたが、1 つ以上の起動が Success の値を持っていません。ただし、スタータスが Failed になるほどの呼び出しの失敗はありません。これは終了状態です。
Cancelled (キャンセル)	コマンドが完了する前にキャンセルされました。これは終了状態です。
RateExceeded	コマンドの対象となるマネージドノードの数が、保留中の呼び出しに対するアカウントクォータを超えています。システムは、どのノードでもコマンドを実行する前にキャンセルしています。これは終了状態です。

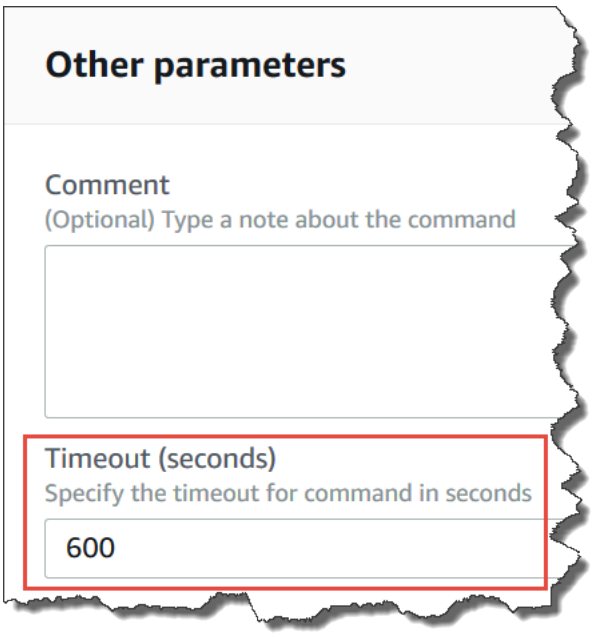
ステータス	詳細
アクセス拒否	コマンドを開始するユーザーまたはロールは、対象のリソースグループにアクセスすることができません。AccessDenied　は親コマンドの max-errors　制限にはカウントされませんが、親コマンドのステータスが Success または Failed になるかどうかに影響します。(例えば、コマンドのすべての呼び出しのステータスが AccessDenied　の場合、返されるコマンドのステータスは Failed です。 ただし、コマンドに 5 つの呼び出しがあり、そのうちの 4 つがステータス AccessDenied　を返し、そのうち 1 はステータス Success を返す場合、親コマンドのステータスは Success になります。) これは終了状態です。
タグにインスタンスがない	コマンドの対象となるタグのキーペア 値またはリソースグループは、どのマネージドノードとも一致しません。これは終了状態です。

コマンドタイムアウト値について

Systems Manager は、コマンドの実行時に以下のタイムアウト値を強制します。

合計タイムアウト

Systems Manager コンソールの [Timeout (seconds)] (タイムアウト (秒)) フィールドでタイムアウト値を指定します。コマンドの送信後、Run Command はコマンドの有効期限が切れているかどうかをチェックします。コマンドの有効期限制限 (合計タイムアウト) に達すると、ステータスが InProgress、Pending または Delayed になっているすべての呼び出しのステータスが DeliveryTimedOut に変わります。



より技術的なレベルで説明すると、合計タイムアウト ([Timeout (seconds)] (タイムアウト (秒))) は、次に示すような 2 つのタイムアウト値の組み合わせです。

```
Total timeout = "Timeout(seconds)" from the console + "timeoutSeconds":
"{{ executionTimeout }}" from your SSM document
```

例えば、Systems Manager コンソールの Timeout (秒) のデフォルト値は 600 秒です。AWS-RunShellScript SSM ドキュメントを使用してコマンドを実行する場合、"timeoutSeconds": "{{ executionTimeout }}" のデフォルト値は、次のドキュメントのサンプルに示すように 3600 秒です。

```
"executionTimeout": {
    "type": "String",
    "default": "3600",

"runtimeConfig": {
  "aws:runShellScript": {
    "properties": [
      {
        "timeoutSeconds": "{{ executionTimeout }}"
```

これは、システムがコマンドステータスを DeliveryTimedOut に設定する前に、コマンドが 4,200 秒 (70 分) 実行されることを意味します。

実行タイムアウト

Systems Manager コンソールで、[Execution Timeout (実行タイムアウト)] フィールド (使用可能な場合) に実行タイムアウト値を指定します。すべての SSM ドキュメントで、実行タイムアウトを指定する必要があるわけではありません。[実行タイムアウト] フィールドは、対応する入力パラメータが SSM ドキュメントで定義されている場合にのみ表示されます。指定した場合、コマンドはこの期間内に完了する必要があります。

> **Note**
>
> Run Command は、SSM Agent ドキュメントの終了応答に依存して、コマンドがエージェントに配信されたかどうかを判断します。SSM Agent は、呼び出しまたはコマンドが `ExecutionTimedOut` としてマークされるための `ExecutionTimedOut` シグナルを送信する必要があります。

デフォルトの実行タイムアウト

SSM ドキュメントで実行タイムアウト値を明示的に指定する必要がない場合、Systems Manager がハードコーディングされたデフォルトの実行タイムアウトを強制します。

Systems Manager がタイムアウトをレポートする方法

Systems Manager がターゲットの SSM Agent から `execution timeout` 応答を受信すると、Systems Manager はコマンド呼び出しを `executionTimeout` としてマークします。

Run Command が SSM Agent からドキュメント終了応答を受信しない場合、コマンド呼び出しは `deliveryTimeout` としてマークされます。

ターゲットのタイムアウトステータスを判断するため、SSM Agent は `executionTimeout` の計算対象の SSM ドキュメントのすべてのパラメータとコンテンツを結合します。SSM Agent がコマンドがタイムアウトしたと判断すると、サービスに `executionTimeout` を送信します。

Timeout (seconds) のデフォルトは 3600 秒です。Execution Timeout のデフォルトも 3600 秒です。したがって、コマンドのデフォルトタイムアウトの合計は 7200 秒です。

> **Note**
>
> SSM Agent による `executionTimeout` の処理方法は、 ドキュメントの種類とドキュメントのバージョンによって異なります。

Run Command のチュートリアル

このセクションのチュートリアルでは、AWS Systems Manager のツールである Run Command で、AWS Command Line Interface (AWS CLI) または AWS Tools for Windows PowerShell を使用してコマンドを実行する方法を説明します。

内容

- Run Command を使用してソフトウェアを更新する
- チュートリアル: Run Command で AWS CLI を使用する
- チュートリアル: Run Command で AWS Tools for Windows PowerShell を使用する

以下のリファレンスでサンプルコマンドも表示できます。

- Systems Manager AWS CLI リファレンス
- AWS Tools for Windows PowerShell - AWS Systems Manager

Run Command を使用してソフトウェアを更新する

以下の手順は、マネージドノードのソフトウェアを更新する方法について説明しています。

Run Command を使用して SSM Agent を更新する

以下の手順は、マネージドノードで実行されている SSM Agent を更新する方法について説明しています。最新の SSM Agent バージョンに更新することも、古いバージョンにダウングレードすることもできます。コマンドを実行すると、システムは該当するバージョンを AWS からダウンロードし、インストールして、コマンドの実行前に存在していたバージョンをアンインストールします。このプロセスの実行中にエラーが発生すると、システムはコマンドの実行前のサーバーバージョンにロールバックし、コマンドステータスにはコマンドの失敗が示されます。

> **Note**
>
> インスタンスが macOS バージョン 11.0 (Big Sur) 以降を実行している場合、AWS-UpdateSSMAgent ドキュメントを実行するにはインスタンスの SSM Agent バージョン 3.1.941.0 以上が必要です。インスタンスが 3.1.941.0 より前にリリースされた SSM Agent バージョンを実行している場合は、`brew update` および `brew upgrade amazon-ssm-agent` コマンドを実行することで AWS-UpdateSSMAgent ドキュメントを実行するように SSM Agent を更新できます。

SSM Agent の更新に関する通知を受け取るには、GitHub の「SSM Agent リリースノート」ページをサブスクライブします。

Run Command を使用して SSM Agent を更新するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Run Command] を選択します。
3. [コマンドの実行] を選択します。
4. [Command document (コマンドのドキュメント)] リストで、[**AWS-UpdateSSMAgent**] を選択します。
5. [Command parameters] セクションで、必要に応じて以下のパラメータの値を指定します。
   a. (オプション) [Version (バージョン)] に、インストールする SSM Agent のバージョンを入力します。エージェントの古いバージョンをインストールできます。バージョンを指定しないと、サービスは最新バージョンをインストールします。
   b. (オプション) 以前のバージョンの SSM Agent をインストールするには、[Allow Downgrade (ダウングレードの許可)] で [true] を選択します。このオプションを選択した場合は、以前のバージョン番号を指定します。[false] を選択すると、最新バージョンのサービスのみがインストールされます。
6. [Targets] (ターゲット) セクションで、タグの指定、インスタンスやエッジデバイスの手動選択、リソースグループの指定により、このオペレーションを実行するマネージドノードを選択します。

> **Tip**
>
> 表示されるはずのマネージドノードが表示されない場合は、トラブルシューティングのヒントについて「マネージドノードの可用性のトラブルシューティング」を参照してください。

7. [その他のパラメータ] で、以下の操作を行います。

   - [コメント] に、このコマンドに関する情報を入力します。
   - [タイムアウト (秒)] に、コマンドの実行全体が失敗するまでにシステムが待機する秒数を指定します。

8. [レート制御] の場合:

   - [同時実行数] の場合、コマンドを同時に実行するマネージドノードの数または割合を指定します。

     > **Note**
     >
     > マネージドノードに適用されるタグを指定するか、AWS リソースグループを指定してターゲットを選択し、ターゲットとなるマネージドノードの数が不明な場合は、割合を指定してドキュメントを同時に実行できるターゲットの数を制限します。

   - [エラーのしきい値] で、ノードの数または割合のいずれかで失敗した後、他のマネージドノードでのコマンドの実行をいつ停止するか指定します。例えば、3 つのエラーを指定した場合、4 番目のエラーが受信されると、Systems Manager はコマンドの送信を停止します。コマンドを処理しているマネージドノードもエラーを送信する可能性があります。

9. (オプション) コマンド出力をファイルに保存する場合は、[出力オプション] の [S3 バケットにコマンド出力を書き込む] ボックスを選択します。ボックスにバケット名とプレフィックス (フォルダ) 名を入力します。

> **Note**
>
> S3 バケットにデータを書き込む機能を許可する S3 許可は、このタスクを実行する IAM ユーザーのものではなく、インスタンスに割り当てられたインスタンスプロファイル (EC2 インスタンスの場合) または IAM サービスロール (ハイブリッドアクティベーションマシン) のものです。詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」または「ハイブリッド環境に IAM サービスロールを作成す

る」を参照してください。さらに、指定された S3 バケットが別の AWS アカウント にある場合は、マネージドノードに関連付けられたインスタンスプロファイルまたは IAM サービスロールが、そのバケットへの書き込みに必要なアクセス許可があることを確認してください。

10. [SNS Notifications (SNS 通知)] セクションで、コマンドの実行状態に関する通知を受け取る場合は、[Enable SNS notifications (SNS 通知を有効にする)] チェックボックスをオンにします。

    Run Command 用の Amazon SNS 通知の設定の詳細については、「Amazon SNS 通知を使用した Systems Manager のステータス変更のモニタリング」を参照してください。
11. [Run (実行)] を選択します。

Run Command を使用して PowerShell を更新する

以下の手順では、Windows Server 2012 および 2012 R2 マネージドノードで PowerShell をバージョン 5.1 に更新する方法について説明します。この手順で提供されるスクリプトは、Windows 管理フレームワーク (WMF) バージョン 5.1 の更新プログラムをダウンロードし、更新プログラムのインストールを開始します。WMF 5.1 のインストール時に必要になるため、このプロセス中にノードが再起動します。更新プログラムのダウンロードとインストールが完了するまでに約 5 分かかります。

Run Command を使用して PowerShell を更新するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Run Command] を選択します。
3. [コマンドの実行] を選択します。
4. [Command document (コマンドのドキュメント)] リストで、[**AWS-RunPowerShellScript**] を選択します。
5. [コマンド] セクションに、使用しているオペレーティングシステム用の以下のコマンドを貼り付けます。

    Windows Server 2012 R2

```
Set-Location -Path "C:\Windows\Temp"

Invoke-WebRequest "https://go.microsoft.com/fwlink/?linkid=839516" -OutFile
 "Win8.1AndW2K12R2-KB3191564-x64.msu"
```

```
Start-Process -FilePath "$env:systemroot\system32\wusa.exe" -Verb RunAs -
ArgumentList ('Win8.1AndW2K12R2-KB3191564-x64.msu', '/quiet')
```

Windows Server 2012

```
Set-Location -Path "C:\Windows\Temp"

Invoke-WebRequest "https://go.microsoft.com/fwlink/?linkid=839513" -OutFile
 "W2K12-KB3191565-x64.msu"

Start-Process -FilePath "$env:systemroot\system32\wusa.exe" -Verb RunAs -
ArgumentList ('W2K12-KB3191565-x64.msu', '/quiet')
```

6. [Targets] (ターゲット) セクションで、タグの指定、インスタンスやエッジデバイスの手動選択、リソースグループの指定により、このオペレーションを実行するマネージドノードを選択します。

> **Tip**
>
> 表示されるはずのマネージドノードが表示されない場合は、トラブルシューティングのヒントについて「マネージドノードの可用性のトラブルシューティング」を参照してください。

7. [その他のパラメータ] で、以下の操作を行います。

   - [コメント] に、このコマンドに関する情報を入力します。
   - [タイムアウト (秒)] に、コマンドの実行全体が失敗するまでにシステムが待機する秒数を指定します。

8. [レート制御] の場合:

   - [同時実行数] の場合、コマンドを同時に実行するマネージドノードの数または割合を指定します。

> **Note**
>
> マネージドノードに適用されるタグを指定するか、AWS リソースグループを指定してターゲットを選択し、ターゲットとなるマネージドノードの数が不明な場合は、割合を指定してドキュメントを同時に実行できるターゲットの数を制限します。

- [エラーのしきい値] で、ノードの数または割合のいずれかで失敗した後、他のマネージドノードでのコマンドの実行をいつ停止するか指定します。例えば、3 つのエラーを指定した場合、4 番目のエラーが受信されると、Systems Manager はコマンドの送信を停止します。コマンドを処理しているマネージドノードもエラーを送信する可能性があります。

9. (オプション) コマンド出力をファイルに保存する場合は、[出力オプション] の [S3 バケットにコマンド出力を書き込む] ボックスを選択します。ボックスにバケット名とプレフィックス (フォルダ) 名を入力します。

> **Note**
>
> S3 バケットにデータを書き込む機能を許可する S3 許可は、このタスクを実行する IAM ユーザーのものではなく、インスタンスに割り当てられたインスタンスプロファイル (EC2 インスタンスの場合) または IAM サービスロール (ハイブリッドアクティベーションマシン) のものです。詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」または「ハイブリッド環境に IAM サービスロールを作成する」を参照してください。さらに、指定された S3 バケットが別の AWS アカウント にある場合は、マネージドノードに関連付けられたインスタンスプロファイルまたは IAM サービスロールが、そのバケットへの書き込みに必要なアクセス許可があることを確認してください。

10. [SNS Notifications (SNS 通知)] セクションで、コマンドの実行状態に関する通知を受け取る場合は、[Enable SNS notifications (SNS 通知を有効にする)] チェックボックスをオンにします。

    Run Command 用の Amazon SNS 通知の設定の詳細については、「Amazon SNS 通知を使用した Systems Manager のステータス変更のモニタリング」を参照してください。

11. [Run (実行)] を選択します。

マネージドノードが再起動し、更新プログラムのインストールが完了したら、ノードに接続し、PowerShell がバージョン 5.1 に正常にアップグレードされたことを確認します。ノードの PowerShell のバージョンをチェックするには、PowerShell を開き、`$PSVersionTable` を入力します。アップグレードが成功した場合、出力テーブルの `PSVersion` の値は 5.1 と表示されます。

`PSVersion` 値が 5.1 と異なる場合 (たとえば 3.0 や 4.0)、[Windows ログ] の下にあるイベントビューアで [セットアップ] ログを確認します。これらのログは、更新プログラムのインストールが失敗した理由を示します。

チュートリアル: Run Command で AWS CLI を使用する

以下のサンプルチュートリアルは、AWS Command Line Interface (AWS CLI) を使用してコマンドとコマンドパラメータに関する情報を表示する方法、コマンドを実行する方法、これらのコマンドのステータスを確認する方法を示しています。

> **Important**
>
> 信頼されている管理者のみが、このトピックで示される AWS Systems Manager で事前設定されたドキュメントの使用を許可されます。Systems Manager ドキュメントで指定されるコマンドまたはスクリプトは、マネージドノードの管理 許可で実行されます。ユーザーに、事前定義済みの Systems Manager ドキュメント (`AWS-` から始まるドキュメント) を実行許可がある場合、そのユーザーには、ノードへの管理者アクセス権もあります。他のすべてのユーザーについては、制限付きドキュメントを作成し、そのドキュメントを特定のユーザーと共有する必要があります。

トピック

- ステップ 1: 開始方法
- ステップ 2: シェルスクリプトを実行してリソースの詳細を表示する
- ステップ 3: AWS-RunShellScript ドキュメントを使用して簡単なコマンドを送信する
- ステップ4: Run Command を使用して簡単な Python スクリプトを実行する
- ステップ5: Run Command を使用して Bash スクリプトを実行する

ステップ 1: 開始方法

ユーザーは、設定するマネージドノードの管理者アクセス許可を持っているか、AWS Identity and Access Management (IAM) で適切なアクセス許可を付与されている必要があります。また、この例では、米国東部 (オハイオ) リージョン (us-east-2) を使用している点に留意してください。Run Command は、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」に記載されている AWS リージョン で利用できます。詳細については、「AWS Systems Manager のマネージドノードのセットアップ」を参照してください。

AWS CLI を使用してコマンドを実行します。

1. まだ AWS Command Line Interface (AWS CLI) をインストールして設定していない場合は、インストールして設定します。

詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」を参照してください。

2. 利用可能なすべてのドキュメントを表示します。

   このコマンドでは、IAM アクセス許可に基づいて、アカウントで利用可能なすべてのドキュメントが表示されます。

   ```
   aws ssm list-documents
   ```

3. マネージドノードでコマンドを受信する準備ができていることを確認します。

   マネージドノードがオンラインの場合は、次のコマンドの出力が表示されます。

   Linux & macOS

   ```
   aws ssm describe-instance-information \
       --output text --query "InstanceInformationList[*]"
   ```

   Windows

   ```
   aws ssm describe-instance-information ^
       --output text --query "InstanceInformationList[*]"
   ```

4. 特定のマネージドノードについての詳細を表示するには、次のコマンドを実行します。

   > **Note**
   >
   > このチュートリアルのコマンドを実行するには、インスタンス ID およびコマンド ID を置き換えます。マネージド AWS IoT Greengrass コアデバイスの場合、インスタンス ID には mi-*ID_Number* を使用します。コマンド ID は send-command に対する応答として返されます。インスタンス ID は AWS Systems Manager のツールである Fleet Manager から入手できます。

   Linux & macOS

   ```
   aws ssm describe-instance-information \
       --instance-information-filter-list key=InstanceIds,valueSet=instance-ID
   ```

Windows

```
aws ssm describe-instance-information ^
    --instance-information-filter-list key=InstanceIds,valueSet=instance-ID
```

ステップ 2: シェルスクリプトを実行してリソースの詳細を表示する

Run Command と AWS-RunShellScript ドキュメントを使用すると、マネージドノード上で、あたかもローカルにログオンしているかのように、任意のコマンドやスクリプトを実行することができます。

説明と使用可能なパラメータを表示する

Systems Manager JSON ドキュメントの説明を表示するには、次のコマンドを実行します。

Linux & macOS

```
aws ssm describe-document \
    --name "AWS-RunShellScript" \
    --query "[Document.Name,Document.Description]"
```

Windows

```
aws ssm describe-document ^
    --name "AWS-RunShellScript" ^
    --query "[Document.Name,Document.Description]"
```

これらのパラメータに使用できるパラメータと詳細を表示するには、次のコマンドを実行します。

Linux & macOS

```
aws ssm describe-document \
    --name "AWS-RunShellScript" \
    --query "Document.Parameters[*]"
```

Windows

```
aws ssm describe-document ^
    --name "AWS-RunShellScript" ^
```

```
    --query "Document.Parameters[*]"
```

ステップ 3: **AWS-RunShellScript** ドキュメントを使用して簡単なコマンドを送信する

Linux マネージドノードの IP 情報を取得するには、次のコマンドを実行します。

Windows Server のマネージドノードを対象としている場合、document-name を AWS-RunPowerShellScript に、command を ifconfig から ipconfig に変更します。

Linux & macOS

```
aws ssm send-command \
    --instance-ids "instance-ID" \
    --document-name "AWS-RunShellScript" \
    --comment "IP config" \
    --parameters commands=ifconfig \
    --output text
```

Windows

```
aws ssm send-command ^
    --instance-ids "instance-ID" ^
    --document-name "AWS-RunShellScript" ^
    --comment "IP config" ^
    --parameters commands=ifconfig ^
    --output text
```

応答データを使用したコマンド情報の取得

次のコマンドは、コマンド ID を使用します。これは、前述のコマンド実行の詳細および応答データを取得するコマンドで返されるものです。コマンドが完了すると、システムは応答データを返します。コマンド実行によって "Pending" または "InProgress" と表示される場合は、もう一度このコマンドを実行して応答データを確認します。

Linux & macOS

```
aws ssm list-command-invocations \
    --command-id $sh-command-id \
    --details
```

Windows

```
aws ssm list-command-invocations ^
    --command-id $sh-command-id ^
    --details
```

ユーザーを識別

次のコマンドは、コマンドを実行するデフォルトのユーザーを表示します。

Linux & macOS

```
sh_command_id=$(aws ssm send-command \
    --instance-ids "instance-ID" \
    --document-name "AWS-RunShellScript" \
    --comment "Demo run shell script on Linux managed node" \
    --parameters commands=whoami \
    --output text \
    --query "Command.CommandId")
```

コマンドステータスの取得

次のコマンドでは、コマンド ID を使用して、マネージドノードでのコマンド実行に関するステータスを取得しています。この例では、前のコマンドで返されたコマンド ID を使用しています。

Linux & macOS

```
aws ssm list-commands \
    --command-id "command-ID"
```

Windows

```
aws ssm list-commands ^
    --command-id "command-ID"
```

コマンドの詳細の取得

次のコマンドでは、前のコマンドのコマンド ID を使用して、マネージドノードごとのコマンド実行に関するステータスを取得しています。

Linux & macOS

```
aws ssm list-command-invocations \
    --command-id "command-ID" \
    --details
```

Windows

```
aws ssm list-command-invocations ^
    --command-id "command-ID" ^
    --details
```

特定のマネージドノードのコマンド情報と応答データを取得

次のコマンドでは、特定のマネージドノードについて、元の aws ssm send-command リクエストに対する出力が返されます。

Linux & macOS

```
aws ssm list-command-invocations \
    --instance-id instance-ID \
    --command-id "command-ID" \
    --details
```

Windows

```
aws ssm list-command-invocations ^
    --instance-id instance-ID ^
    --command-id "command-ID" ^
    --details
```

Python バージョンの表示

次のコマンドは、ノード上で実行している Python のバージョンを返します。

Linux & macOS

```
sh_command_id=$(aws ssm send-command \
    --instance-ids "instance-ID" \
```

```
    --document-name "AWS-RunShellScript" \
    --comment "Demo run shell script on Linux Instances" \
    --parameters commands='python -V' \
    --output text --query "Command.CommandId") \
    sh -c 'aws ssm list-command-invocations \
    --command-id "$sh_command_id" \
    --details \
    --query "CommandInvocations[].CommandPlugins[].{Status:Status,Output:Output}"'
```

ステップ4: Run Command を使用して簡単な Python スクリプトを実行する

次のコマンドでは、Run Command を使用して、Python の簡単な "Hello World" スクリプトが実行されます。

Linux & macOS

```
sh_command_id=$(aws ssm send-command \
    --instance-ids "instance-ID" \
    --document-name "AWS-RunShellScript" \
    --comment "Demo run shell script on Linux Instances" \
    --parameters '{"commands":["#!/usr/bin/python","print \"Hello World from python
\""]}' \
    --output text \
    --query "Command.CommandId") \
    sh -c 'aws ssm list-command-invocations \
    --command-id "$sh_command_id" \
    --details \
    --query "CommandInvocations[].CommandPlugins[].{Status:Status,Output:Output}"'
```

ステップ5: Run Command を使用して Bash スクリプトを実行する

このセクションの例は、Run Command を使用して次の bash スクリプトを実行する方法を示しています。

Run Command を使用して遠隔地に格納されたスクリプトを実行する例については、Amazon S3 からのスクリプトの実行 および GitHub からのスクリプトの実行 を参照してください。

```
#!/bin/bash
yum -y update
yum install -y ruby
cd /home/ec2-user
```

```
curl -O https://aws-codedeploy-us-east-2.s3.amazonaws.com/latest/install
chmod +x ./install
./install auto
```

このスクリプトにより、AWS CodeDeploy ユーザーガイド の「CodeDeploy 用の Amazon EC2 インスタンスを作成する」で説明されているように、Amazon Linux および Red Hat Enterprise Linux (RHEL) インスタンスに AWS CodeDeploy エージェントがインストールされます。

このスクリプトは、米国東部 (オハイオ) リージョン (us-east-2)、`aws-codedeploy-us-east-2` の AWS 管理の Amazon S3 バケットから CodeDeploy エージェントをインストールします。

AWS CLI コマンドで bash スクリプトを実行する

次のサンプルは、`--parameters` オプションを使用して CLI コマンドに bash スクリプトを含める方法を示しています。

Linux & macOS

```
aws ssm send-command \
    --document-name "AWS-RunShellScript" \
    --targets '[{"Key":"InstanceIds","Values":["instance-id"]}]' \
    --parameters '{"commands":["#!/bin/bash","yum -y update","yum
 install -y ruby","cd /home/ec2-user","curl -O https://aws-codedeploy-us-
east-2.s3.amazonaws.com/latest/install","chmod +x ./install","./install auto"]}'
```

JSON ファイルで bash スクリプトを実行する

次の例では、bash スクリプトの内容が JSON ファイルに格納され、`--cli-input-json` オプションを使用してファイルがコマンドに含まれます。

Linux & macOS

```
aws ssm send-command \
    --document-name "AWS-RunShellScript" \
    --targets "Key=InstanceIds,Values=instance-id" \
    --cli-input-json file://installCodeDeployAgent.json
```

Windows

```
aws ssm send-command ^
```

```
    --document-name "AWS-RunShellScript" ^
    --targets "Key=InstanceIds,Values=instance-id" ^
    --cli-input-json file://installCodeDeployAgent.json
```

次の例に、参照する `installCodeDeployAgent.json` ファイルの内容を示します。

```
{
    "Parameters": {
        "commands": [
            "#!/bin/bash",
            "yum -y update",
            "yum install -y ruby",
            "cd /home/ec2-user",
            "curl -O https://aws-codedeploy-us-east-2.s3.amazonaws.com/latest/install",
            "chmod +x ./install",
            "./install auto"
        ]
    }
}
```

チュートリアル: Run Command で AWS Tools for Windows PowerShell を使用する

以下の例では、AWS Tools for Windows PowerShell を使用してコマンドとコマンドパラメータに関する情報を表示する方法、コマンドを実行する方法、これらのコマンドのステータスを確認する方法を示しています。このウォークスルーには、定義済み AWS Systems Manager ドキュメントごとの例が含まれています。

> **Important**
>
> 信頼されている管理者のみが、このトピックで示される Systems Manager で事前設定されたドキュメントの使用を許可されます。Systems Manager ドキュメントで指定されるコマンドまたはスクリプトは、マネージドノードの管理アクセス許可で実行されます。ユーザーに、事前定義済みの Systems Manager ドキュメント (AWS から始まるドキュメント) を実行許可がある場合、そのユーザーには、ノードへの管理者アクセス権もあります。他のすべてのユーザーについては、制限付きドキュメントを作成し、そのドキュメントを特定のユーザーと共有する必要があります。

トピック

- AWS Tools for Windows PowerShell セッションの設定を構成する
- 利用可能なすべてのドキュメントを表示します。
- PowerShell コマンドまたはスクリプトを実行する
- AWS-InstallApplication ドキュメントを使用してアプリケーションをインストールする
- AWS-InstallPowerShellModule JSON ドキュメントを使用して PowerShell モジュールをインストールする
- AWS-JoinDirectoryServiceDomain JSON ドキュメントを使用してマネージドノードをドメインに結合
- AWS-ConfigureCloudWatch ドキュメントを使用して Windows メトリクスを Amazon CloudWatch Logs に送信する
- AWS-UpdateEC2Config ドキュメントを使用して EC2Config を更新する
- AWS-ConfigureWindowsUpdate ドキュメントを使用して、Windows の自動更新を有効または無効にする
- Run Command を使用した Windows の更新プログラムの管理

AWS Tools for Windows PowerShell セッションの設定を構成する

認証情報を指定する

ローカルコンピュータで Tools for Windows PowerShell を開き、次のコマンドを実行して認証情報を指定します。ユーザーは、設定するマネージドノードの管理者アクセス許可を持っているか、AWS Identity and Access Management (IAM) で適切なアクセス許可を付与されている必要があります。詳細については、「AWS Systems Manager のマネージドノードのセットアップ」を参照してください。

```
Set-AWSCredentials -AccessKey key-name -SecretKey key-name
```

デフォルト を設定するAWS リージョン

次のコマンドを実行して、PowerShell セッションのリージョンを設定します。この例では、米国東部 (オハイオ) リージョン (us-east-2) を使用しています。Run Command は、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」に記載されている AWS リージョン で利用できます。

```
Set-DefaultAWSRegion `
```

```
    -Region us-east-2
```

利用可能なすべてのドキュメントを表示します。

このコマンドは、アカウントに使用できるすべてのドキュメントを一覧表示します。

```
Get-SSMDocumentList
```

PowerShell コマンドまたはスクリプトを実行する

Run Command と AWS-RunPowerShell ドキュメントを使用すると、マネージドノード上で、あたかもローカルにログオンしているかのように、任意のコマンドやスクリプトを実行することができます。コマンドを発行することも、コマンドを実行するためのローカルスクリプトのパスを入力することもできます。

> **Note**
>
> Run Command を使用してスクリプトを呼び出すときのマネージドノードの再起動については、「コマンド実行時の再起動の処理」を参照してください。

説明と使用可能なパラメータを表示する

```
Get-SSMDocumentDescription `
    -Name "AWS-RunPowerShellScript"
```

パラメータの詳細情報を表示する

```
Get-SSMDocumentDescription `
    -Name "AWS-RunPowerShellScript" | Select -ExpandProperty Parameters
```

AWS-RunPowerShellScript ドキュメントを使用してコマンドを送信する

次のコマンドでは、2 つのマネージドノードの "C:\Users" ディレクトリの内容と "C:\" ディレクトリの内容が表示されます。

```
$runPSCommand = Send-SSMCommand `
    -InstanceIds @("instance-ID-1", "instance-ID-2") `
```

```
    -DocumentName "AWS-RunPowerShellScript" `
    -Comment "Demo AWS-RunPowerShellScript with two instances" `
    -Parameter @{'commands'=@('dir C:\Users', 'dir C:\')}
```

コマンドリクエストの詳細を取得する

次のコマンドでは、CommandId を使用して、2 つのマネージドノードでのコマンド実行に関するステータスを取得します。この例では、前のコマンドで返された CommandId を使用しています。

```
Get-SSMCommand `
    -CommandId $runPSCommand.CommandId
```

この例のコマンドのステータスは Success、Pending、InProgress のいずれかになります。

マネージドノードごとのコマンド情報を取得

次のコマンドでは、前のコマンドの CommandId を使用して、マネージドノードごとのコマンド実行に関するステータスを取得します。

```
Get-SSMCommandInvocation `
    -CommandId $runPSCommand.CommandId
```

特定のマネージドノードのコマンド情報と応答データを取得

次のコマンドでは、特定のマネージドノードについて、元の Send-SSMCommand の出力を返します。

```
Get-SSMCommandInvocation `
    -CommandId $runPSCommand.CommandId `
    -Details $true `
    -InstanceId instance-ID | Select -ExpandProperty CommandPlugins
```

コマンドをキャンセルする

次のコマンドでは、Send-SSMCommand ドキュメントの AWS-RunPowerShellScript をキャンセルします。

```
$cancelCommand = Send-SSMCommand `
    -InstanceIds @("instance-ID-1","instance-ID-2") `
```

```
    -DocumentName "AWS-RunPowerShellScript" `
    -Comment "Demo AWS-RunPowerShellScript with two instances" `
    -Parameter @{'commands'='Start-Sleep -Seconds 120; dir C:\'}

Stop-SSMCommand -CommandId $cancelCommand.CommandId
```

コマンドの状態を確認する

次のコマンドでは、Cancel コマンドのステータスを確認します。

```
Get-SSMCommand `
    -CommandId $cancelCommand.CommandId
```

AWS-InstallApplication ドキュメントを使用してアプリケーションをインストールする

Run Command と AWS-InstallApplication ドキュメントを使用すると、マネージドノードでアプリケーションをインストール、修復、またはアンインストールできます。このコマンドには、MSI のパスまたはアドレスが必要です。

> **Note**
>
> Run Command を使用してスクリプトを呼び出すときのマネージドノードの再起動については、「コマンド実行時の再起動の処理」を参照してください。

説明と使用可能なパラメータを表示する

```
Get-SSMDocumentDescription `
    -Name "AWS-InstallApplication"
```

パラメータの詳細情報を表示する

```
Get-SSMDocumentDescription `
    -Name "AWS-InstallApplication" | Select -ExpandProperty Parameters
```

AWS-InstallApplication ドキュメントを使用してコマンドを送信する

次のコマンドでは、無人モードでマネージドノードに Python のバージョンをインストールし、出力を C: ドライブにあるローカルテキスト ファイルに記録します。

```
$installAppCommand = Send-SSMCommand `
    -InstanceId instance-ID `
    -DocumentName "AWS-InstallApplication" `
    -Parameter @{'source'='https://www.python.org/ftp/python/2.7.9/python-2.7.9.msi';
 'parameters'='/norestart /quiet /log c:\pythoninstall.txt'}
```

マネージドノードごとのコマンド情報を取得

次のコマンドでは、CommandId を使用して、コマンド実行のステータスを取得します。

```
Get-SSMCommandInvocation `
    -CommandId $installAppCommand.CommandId `
    -Details $true
```

特定のマネージドノードのコマンド情報と応答データを取得

次のコマンドでは、Python のインストール結果が返されます。

```
Get-SSMCommandInvocation `
    -CommandId $installAppCommand.CommandId `
    -Details $true `
    -InstanceId instance-ID | Select -ExpandProperty CommandPlugins
```

AWS-InstallPowerShellModule JSON ドキュメントを使用して PowerShell モジュールをインストールする

Run Command を使用して、マネージドノードに PowerShell モジュールをインストールできます。PowerShell モジュールの詳細については、「Windows PowerShell モジュール」を参照してください。

説明と使用可能なパラメータを表示する

```
Get-SSMDocumentDescription `
    -Name "AWS-InstallPowerShellModule"
```

パラメータの詳細情報を表示する

```
Get-SSMDocumentDescription `
    -Name "AWS-InstallPowerShellModule" | Select -ExpandProperty Parameters
```

PowerShell モジュールをインストールする

次のコマンドでは、EZOut.zip ファイルをダウンロードしてインストールし、XPS ビューアをインストールするための追加コマンドも実行しています。最後に、このコマンドの出力が、「amzn-s3-demo-bucket」という名前の S3 バケットにアップロードされます。

```
$installPSCommand = Send-SSMCommand `
    -InstanceId instance-ID `
    -DocumentName "AWS-InstallPowerShellModule" `
    -Parameter @{'source'='https://gallery.technet.microsoft.com/EZOut-33ae0fb7/
file/110351/1/EZOut.zip';'commands'=@('Add-WindowsFeature -name XPS-Viewer -restart')}
 `
    -OutputS3BucketName amzn-s3-demo-bucket
```

マネージドノードごとのコマンド情報を取得

次のコマンドでは、CommandId を使用して、コマンド実行のステータスを取得します。

```
Get-SSMCommandInvocation `
    -CommandId $installPSCommand.CommandId `
    -Details $true
```

マネージドノードのコマンド情報と応答データを取得

次のコマンドでは、特定の Send-SSMCommand について、元の CommandId の出力を返します。

```
Get-SSMCommandInvocation `
    -CommandId $installPSCommand.CommandId `
    -Details $true | Select -ExpandProperty CommandPlugins
```

AWS-JoinDirectoryServiceDomain JSON ドキュメントを使用してマネージドノードをドメインに結合

Run Command を使用すると、マネージドノードを AWS Directory Service ドメインにすばやく参加させることができます。このコマンドを実行する前に、ディレクトリを作成 する必要があります。また、 についてさらに詳細をご確認いただくことをお勧めしますAWS Directory Service 詳細については、AWS Directory Service 管理ガイドを参照してください。

ドメインにマネージドノードを結合することしかできません。ドメインからノードを削除することはできません。

> **Note**
>
> Run Command を使用してスクリプトを呼び出す場合の、マネージドノードの詳細については「コマンド実行時の再起動の処理」を参照してください。

説明と使用可能なパラメータを表示する

```
Get-SSMDocumentDescription `
    -Name "AWS-JoinDirectoryServiceDomain"
```

パラメータの詳細情報を表示する

```
Get-SSMDocumentDescription `
    -Name "AWS-JoinDirectoryServiceDomain" | Select -ExpandProperty Parameters
```

マネージドノードのドメインへの参加

次のコマンドは、マネージドノードを指定された AWS Directory Service ドメインを作成し、生成された出力を例の Amazon Simple Storage Service (Amazon S3) バケットにアップロードします。

```
$domainJoinCommand = Send-SSMCommand `
    -InstanceId instance-ID `
    -DocumentName "AWS-JoinDirectoryServiceDomain" `
    -Parameter @{'directoryId'='d-example01'; 'directoryName'='ssm.example.com';
 'dnsIpAddresses'=@('192.168.10.195', '192.168.20.97')} `
    -OutputS3BucketName amzn-s3-demo-bucket
```

マネージドノードごとのコマンド情報を取得

次のコマンドでは、CommandId を使用して、コマンド実行のステータスを取得します。

```
Get-SSMCommandInvocation `
    -CommandId $domainJoinCommand.CommandId `
    -Details $true
```

マネージドノードのコマンド情報と応答データを取得

このコマンドでは、特定の Send-SSMCommand について、元の CommandId の出力を返します 。

```
Get-SSMCommandInvocation `
```

```
    -CommandId $domainJoinCommand.CommandId `
    -Details $true | Select -ExpandProperty CommandPlugins
```

AWS-ConfigureCloudWatch ドキュメントを使用して Windows メトリクスを Amazon CloudWatch Logs に送信する

アプリケーション、システム、セキュリティ、および Windows イベントトレーシング (ETW) ログの Windows Server メッセージを Amazon CloudWatch Logs に送信することができます。Systems Manager では、ログ記録を初めて有効にすると、アプリケーション、システム、セキュリティ、および ETW ログについて、ログのアップロードを開始した時点から (1) 分以内に作成されたすべてのログが送信されます。この時点より前に発生したログは含まれません。ログ記録を無効にし、後で再度有効にすると、Systems Manager では無効化の時点からのログが送信されます。カスタムログファイルおよびインターネットインフォメーションサービス (IIS) ログの場合、Systems Manager はログファイルを最初から読み取ります。さらに、Systems Manager は パフォーマンスカウンターデータを CloudWatch Logs に送信することもできます。

以前に EC2Config で CloudWatch 統合を有効にした場合、Systems Manager の設定は、マネージドノードのローカルに保存された `C:\Program Files\Amazon\EC2ConfigService\Settings\AWS.EC2.Windows.CloudWatch.json` ファイル内のに設定よりも優先されます。EC2Config を使用して単一マネージドノードのパフォーマンスカウンターとログを管理する方法の詳細については、「Amazon CloudWatch ユーザーガイド」の「CloudWatch エージェントを使用して Amazon EC2 インスタンスとオンプレミスサーバーからメトリクスとログを収集する」を参照してください。

説明と使用可能なパラメータを表示する

```
Get-SSMDocumentDescription `
    -Name "AWS-ConfigureCloudWatch"
```

パラメータの詳細情報を表示する

```
Get-SSMDocumentDescription `
    -Name "AWS-ConfigureCloudWatch" | Select -ExpandProperty Parameters
```

アプリケーションログを CloudWatch に送信する

次のコマンドでは、マネージドノードを設定し、Windows アプリケーションログを CloudWatch に移動します。

```
$cloudWatchCommand = Send-SSMCommand `
```

```
    -InstanceID instance-ID `
    -DocumentName "AWS-ConfigureCloudWatch" `
    -Parameter @{'properties'='{"engineConfiguration": {"PollInterval":"00:00:15",
 "Components":[{"Id":"ApplicationEventLog",
 "FullName":"AWS.EC2.Windows.CloudWatch.EventLog.EventLogInputComponent,AWS.EC2.Windows.CloudWa
 "Parameters":{"LogName":"Application", "Levels":"7"}},{"Id":"CloudWatch",
 "FullName":"AWS.EC2.Windows.CloudWatch.CloudWatchLogsOutput,AWS.EC2.Windows.CloudWatch",
 "Parameters":{"Region":"region", "LogGroup":"my-log-group", "LogStream":"instance-
id"}}], "Flows":{"Flows":["ApplicationEventLog,CloudWatch"]}}}'}
```

マネージドノードごとのコマンド情報を取得

次のコマンドでは、CommandId を使用して、コマンド実行のステータスを取得します。

```
Get-SSMCommandInvocation `
    -CommandId $cloudWatchCommand.CommandId `
    -Details $true
```

特定のマネージドノードのコマンド情報と応答データを取得

次のコマンドは、Amazon CloudWatch の設定の結果を返します。

```
Get-SSMCommandInvocation `
    -CommandId $cloudWatchCommand.CommandId `
    -Details $true `
    -InstanceId instance-ID | Select -ExpandProperty CommandPlugins
```

AWS-ConfigureCloudWatch ドキュメントを使用して CloudWatch にパフォーマンスカウンターを送信する

次のデモンストレーションコマンドは、パフォーマンスカウンタを CloudWatch にアップロードします。詳細については、Amazon CloudWatch ユーザーガイドを参照してください。

```
$cloudWatchMetricsCommand = Send-SSMCommand `
    -InstanceID instance-ID `
    -DocumentName "AWS-ConfigureCloudWatch" `
    -Parameter @{'properties'='{"engineConfiguration": {"PollInterval":"00:00:15",
 "Components":[{"Id":"PerformanceCounter",
 "FullName":"AWS.EC2.Windows.CloudWatch.PerformanceCounterComponent.PerformanceCounterInputComp
 "Parameters":{"CategoryName":"Memory", "CounterName":"Available
 MBytes", "InstanceName":"", "MetricName":"AvailableMemory",
 "Unit":"Megabytes","DimensionName":"", "DimensionValue":""}},{"Id":"CloudWatch",
```

```
 "FullName":"AWS.EC2.Windows.CloudWatch.CloudWatch.CloudWatchOutputComponent,AWS.EC2.Windows.Cl
 "Parameters":{"AccessKey":"", "SecretKey":"","Region":"region", "NameSpace":"Windows-
Default"}}], "Flows":{"Flows":["PerformanceCounter,CloudWatch"]}}}'}
```

AWS-UpdateEC2Config ドキュメントを使用して EC2Config を更新する

Run Command と AWS-EC2ConfigUpdate ドキュメントを使用すると、Windows Server マネージドノードで実行されている EC2Config サービスを更新できます。このコマンドでは、EC2Config サービスを最新バージョンまたは指定バージョンに更新できます。

説明と使用可能なパラメータを表示する

```
Get-SSMDocumentDescription `
    -Name "AWS-UpdateEC2Config"
```

パラメータの詳細情報を表示する

```
Get-SSMDocumentDescription `
    -Name "AWS-UpdateEC2Config" | Select -ExpandProperty Parameters
```

EC2Config を最新バージョンに更新する

```
$ec2ConfigCommand = Send-SSMCommand `
    -InstanceId instance-ID `
    -DocumentName "AWS-UpdateEC2Config"
```

マネージドノードのコマンド情報と応答データを取得

このコマンドは、前回の Send-SSMCommand で指定されたコマンド出力を返します。

```
Get-SSMCommandInvocation `
    -CommandId $ec2ConfigCommand.CommandId `
    -Details $true `
    -InstanceId instance-ID | Select -ExpandProperty CommandPlugins
```

EC2Config を特定バージョンに更新する

以下のコマンドは、古いバージョンに EC2Config をダウングレードします。

```
Send-SSMCommand `
    -InstanceId instance-ID `
```

```
    -DocumentName "AWS-UpdateEC2Config" `
    -Parameter @{'version'='4.9.3519'; 'allowDowngrade'='true'}
```

AWS-ConfigureWindowsUpdate ドキュメントを使用して、Windows の自動更新を有効または無効にする

Run Command と AWS-ConfigureWindowsUpdate ドキュメントを使用すると、Windows Server マネージドノードに対する Windows 自動更新を有効または無効にできます。このコマンドは、指定の日時に Windows 更新プログラムがダウンロードおよびインストールされるように Windows Update Agent を設定します。更新プログラムで再起動が必要になった場合は、更新プログラムのインストールから 15 分後にマネージドノードが自動的に再起動されます。このコマンドを使用すると、Windows Update で更新プログラムの有無が確認され、インストールは実行されないように設定することもできます。AWS-ConfigureWindowsUpdate ドキュメントは、Windows Server 2008、2008 R2、2012、2012 R2、および 2016 と互換性があります。

説明と使用可能なパラメータを表示する

```
Get-SSMDocumentDescription `
    -Name "AWS-ConfigureWindowsUpdate"
```

パラメータの詳細情報を表示する

```
Get-SSMDocumentDescription `
    -Name "AWS-ConfigureWindowsUpdate" | Select -ExpandProperty Parameters
```

Windows 自動更新を有効にする

次のコマンドでは、毎日 10:00 PM に自動的に更新プログラムがダウンロードおよびインストールされるように Windows Update を設定します。

```
$configureWindowsUpdateCommand = Send-SSMCommand `
    -InstanceId instance-ID `
    -DocumentName "AWS-ConfigureWindowsUpdate" `
    -Parameters @{'updateLevel'='InstallUpdatesAutomatically';
 'scheduledInstallDay'='Daily'; 'scheduledInstallTime'='22:00'}
```

Windows 自動更新を有効にするコマンドのステータスを表示する

次のコマンドでは、CommandId を使用して、Windows 自動更新を有効にするためのコマンド実行のステータスを取得します。

```
Get-SSMCommandInvocation `
    -Details $true `
    -CommandId $configureWindowsUpdateCommand.CommandId | Select -ExpandProperty
 CommandPlugins
```

Windows 自動更新を無効にする

次のコマンドでは、システムによって更新プログラムの有無が確認されても自動的にはマネージドノードが更新されないように、Windows Update の通知レベルを引き下げます。

```
$configureWindowsUpdateCommand = Send-SSMCommand `
    -InstanceId instance-ID `
    -DocumentName "AWS-ConfigureWindowsUpdate" `
    -Parameters @{'updateLevel'='NeverCheckForUpdates'}
```

Windows 自動更新を無効にするコマンドのステータスを表示する

次のコマンドでは、CommandId を使用して、Windows 自動更新を無効にするためのコマンド実行のステータスを取得します。

```
Get-SSMCommandInvocation `
    -Details $true `
    -CommandId $configureWindowsUpdateCommand.CommandId | Select -ExpandProperty
 CommandPlugins
```

Run Command を使用した Windows の更新プログラムの管理

Run Command と AWS-InstallWindowsUpdates のドキュメントを使用して、Windows Server マネージドノードの更新を管理できます。このコマンドは、マネージドノードに不足している更新プログラムをスキャンまたはインストールし、必要に応じてインストール後に再起動します。また、環境にインストールする更新の適切な分類と重大度レベルを指定することもできます。

> **Note**
>
> Run Command を使用してスクリプトを呼び出すときのマネージドノードの再起動については、「コマンド実行時の再起動の処理」を参照してください。

以下の例では、指定した Windows Update 管理タスクを実行する方法を示しています。

不足しているすべての Windows 更新プログラムを検索します。

```
Send-SSMCommand `
    -InstanceId instance-ID `
    -DocumentName "AWS-InstallWindowsUpdates" `
    -Parameters @{'Action'='Scan'}
```

特定の Windows 更新プログラムをインストールします。

```
Send-SSMCommand `
    -InstanceId instance-ID `
    -DocumentName "AWS-InstallWindowsUpdates" `
    -Parameters @{'Action'='Install';'IncludeKbs'='kb-ID-1,kb-ID-2,kb-
ID-3';'AllowReboot'='True'}
```

不足している重要な Windows 更新プログラムをインストールします。

```
Send-SSMCommand `
    -InstanceId instance-ID `
    -DocumentName "AWS-InstallWindowsUpdates" `
    -Parameters @{'Action'='Install';'SeverityLevels'='Important';'AllowReboot'='True'}
```

不足している Windows Update をインストールします (特定の除外あり)。

```
Send-SSMCommand `
    -InstanceId instance-ID `
    -DocumentName "AWS-InstallWindowsUpdates" `
    -Parameters @{'Action'='Install';'ExcludeKbs'='kb-ID-1,kb-
ID-2';'AllowReboot'='True'}
```

Systems Manager Run Command のトラブルシューティング

AWS Systems Manager のツールである Run Command は、各コマンド実行のステータスの詳細を表示します。コマンドのステータスの詳細については、「コマンドのステータスについて」を参照してください。このトピックの情報を使用して、Run Command の問題のトラブルシューティングを行うこともできます。

トピック

- マネージドノードの一部が不足しています
- スクリプトの 1 ステップが失敗しましたが、全体的なステータスは「成功」です。

- SSM Agent が正しく実行されません

マネージドノードの一部が不足しています

[Run a command] (コマンドを実行) ページで、SSM ドキュメントの実行を選択して、[Targets] (ターゲット) セクションで [Manually selecting instances] (インスタンスの手動選択) を選択すると、コマンドを実行するために選択できるマネージドノードのリストが表示されます。

表示されるはずのマネージドノードが表示されない場合は、トラブルシューティングのヒントについて「マネージドノードの可用性のトラブルシューティング」を参照してください。

マネージドノードを作成、アクティブ化、リブート、または再起動し、ノードに Run Command をインストールするか、AWS Identity and Access Management (IAM) インスタンスプロファイルをノードにアタッチした後、リストにマネージドノードが表示されるまでに数分かかる場合があります。

スクリプトの 1 ステップが失敗しましたが、全体的なステータスは「成功」です。

Run Command を使用すると、スクリプトが終了コードを処理する方法を定義できます。デフォルトでは、スクリプトで最後に実行されたコマンドの終了コードは、スクリプト全体の終了コードとしてレポートされます。ただし、条件ステートメントを含めて、最後のコマンドの前のいずれかのコマンドが失敗した場合にスクリプトを終了させることができます。説明と例については、「コマンドで終了コードを指定する」を参照してください。

SSM Agent が正しく実行されません

Run Command を使用したコマンドの実行で問題が発生した場合は、SSM Agent で問題が発生している可能性があります。SSM Agent での問題の調査については、「SSM Agent のトラブルシューティング」を参照してください。

AWS Systems Manager Session Manager

Session Manager はフルマネージド型の AWS Systems Manager ツールです。Session Manager を使用すると、Amazon Elastic Compute Cloud (Amazon EC2) インスタンス、エッジデバイス、オンプレミスサーバー、仮想マシン (VM) を管理できます。ワンクリックのブラウザベースのインタラクティブシェルまたは AWS Command Line Interface (AWS CLI) を使用できます。Session Manager は安全なノード管理を実現し、インバウンドポートを開いたり、踏み台ホストを維持したり、SSH キーを管理したりする必要はありません。また Session Manager はマネージドノードの制御されたアクセス、厳格なセキュリティプラクティス、ノードアクセス詳細がある口グを要件とする社内

ポリシーの尊守を実現しつつ、エンドユーザーが簡単なワンクリックのクロスプラットフォームを使用してマネージドノードにアクセスできるようにします。Session Manager の使用を開始するには、Systems Manager コンソールを開きます。ナビゲーションペインで、[Session Manager] を選択します。

Session Manager はどのように組織にとってメリットになりますか?

Session Manager は、以下の利点を提供します。

- IAM ポリシーを使用してマネージドノードの一元化アクセス制御

  管理者はマネージドノードのアクセスを許可および取り消す場所は1カ所あります。AWS Identity and Access Management (IAM) ポリシーのみを使用して、Session Manager の使用とアクセス可能なマネージドノードにおいて、組織内で対象となる個々のユーザーまたはグループを管理することができます。
- インバウンドポートを開いたり、踏み台ホストや SSH キーを管理したりする必要はありません

  マネージドノードのインバウンド SSH ポートとリモート PowerShell ポートを開いたままにした場合、エンティティが未許可または悪意のあるコマンドをマネージドノード上で実行するリスクが大幅に増加します。Session Manager はこれらのインバウンドポートを塞ぎ、SSH キーと証明書の管理、踏み台ホスト、ジャンプボックスの管理からユーザーを解放して、セキュリティ体制の向上に役立ちます。
- コンソールと CLI からワンクリックでマネージドノードへアクセス

  AWS Systems Manager コンソール、または Amazon EC2 コンソールを使用すると、ワンクリックでセッションを開始できます。AWS CLI を使用して、1 つのコマンドまたは一連のコマンドを実行するセッションを開始することもできます。マネージドノードへのアクセス権限はSSH キーやその他メカニズムではなく、IAM ポリシーによって付与されるため、接続時間が大幅に短縮されます。
- ハイブリッドおよびマルチクラウド環境で Amazon EC2 インスタンスと非 EC2 マネージドノードの両方に接続する

  ハイブリッドおよびマルチクラウド環境では、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスと非 EC2 ノードの両方に接続できます。

  Session Manager を使用して EC2 以外のノードに接続するには、最初にアドバンストインスタンス層をアクティブ化する必要があります。アドバンストインスタンス層の使用には料金が発生します。ただし、Session Manager を使用して EC2 インスタンスに接続するための追加料金はありません。詳細については、インスタンス層の設定 を参照してください。

- ポート転送

  マネージドノード内の任意のポートをクライアントのローカルポートにリダイレクトします。その後、ローカルポートに接続してノード内で実行されているサーバーアプリケーションにアクセスします。

- Windows、Linux、および macOS のクロスプラットフォームサポート

  Session Manager は、Windows、Linux、および macOS に対して単一のツールからサポートを提供します。例えば、Linux と macOS のマネージドノードには SSH クライアントを使用する必要はなく、Windows Server のマネージドノードには RDP 接続も不要です。

- 「セッションアクティビティのログ記録」

  組織内で運用上またはセキュリティ上の要件を満たすため、マネージドノードへの接続記録と実行されたコマンドの記録を提出しなければならない場合があります。組織内のユーザーがセッションアクティビティを開始または終了すると、通知を受け取ることもできます。

  ログ記録機能は、次の AWS のサービスとの統合によって提供されます。

  - AWS CloudTrail – AWS CloudTrail は、AWS アカウント で行われた Session Manager API コールに関する情報をキャプチャし、指定した Amazon Simple Storage Service (Amazon S3) バケットに保存されているログファイルに書き込みます。アカウントのすべての CloudTrail ログに対して 1 つのバケットが使用されています。詳細については、「AWS Systems Manager による AWS CloudTrail API コールのログ記録」を参照してください。
  - Amazon Simple Storage Service - デバッグおよびトラブルシューティングの目的で、選択した Amazon S3 バケットにセッションログデータを保存することができます。ログデータは、AWS KMS key を使用した暗号化の有無にかかわらず、Amazon S3 バケットに送信できます。詳しくは、「Amazon S3 を使用してセッションデータを口グ記録する (コンソール)」を参照してください。
  - Amazon CloudWatch Logs – CloudWatch Logs を使用すると、さまざまな AWS のサービスのログファイルを監視、保存、およびアクセスできます。デバッグおよびトラブルシューティングの目的で、セッションログデータを CloudWatch Logs ロググループに送信できます。ログデータは、KMS キーを使用した AWS KMS 暗号化の有無にかかわらずロググループに送信できます。詳細については、「Amazon CloudWatch Logs を使用してセッションデータを口グ記録する (コンソール)」を参照してください。
  - Amazon EventBridge と Amazon Simple Notification Service – EventBridge では、指定した AWS リソースに変更がいつ発生したかを検出するルールを設定できます。組織内のユーザーがセッションを開始または停止したタイミングを検出し、そのイベントに関する通知を Amazon SNS 経由で (テキストまたは E メールメッセージなど) 受信するルールを作成できま

す。CloudWatch イベントを設定して、他の応答を開始することもできます。詳細については、「Amazon EventBridge を使用してセッションアクティビティをモニタリングする (コンソール)」を参照してください。

> **Note**
>
> ログ記録は、ポート転送または SSH を介して接続する Session Manager セッションでは使用できません。これは、SSH はすべてのセッションデータを暗号化し、Session Manager は SSH 接続のトンネルとしてのみ機能するためです。

Session Manager はどのようなユーザーに適していますか?

- セキュリティの体制を強化し、マネージドノードのアクセス制御を一元化することで運用のオーバーヘッドを削減し、インバウンドノードアクセスを削減することを目指すすべての AWS カスタマー。
- マネージドノードのアクセスとアクティビティの監視と追跡、マネージドノードのインバウンドポートの閉鎖、パブリック IP アドレスがないマネージドノードへの接続許可を希望する情報セキュリティの専門家。
- 単一の場所からアクセス権の付与と取り消しと、Linux、macOS および Windows Server のマネージドノードのユーザーに 1 つのソリューションの提供を希望する管理者。
- ブラウザまたは AWS CLI からワンクリックかつSSH キーを提供せずにマネージドノードに接続を希望するユーザー。

Session Manager の主な特徴は何ですか。

- Windows Server、Linux および macOS のマネージドノードを対象にしたサポート

  Session Manager では Amazon Elastic Compute Cloud (EC2) インスタンス、エッジデバイス、オンプレミスサーバー、仮想マシン (VM) への安全な接続を確立できます。サポートされているオペレーティングシステムタイプのリストについては、「Session Manager を設定する」を参照してください。

> **Note**
>
> オンプレミスマシンの Session Manager サポートは、アドバンストインスタンス層に対してのみ提供されています。詳細については、アドバンストインスタンス層を有効にするには を参照してください。

- コンソール、CLI、および SDK の Session Manager 機能へのアクセス

  次の方法で Session Manager を使用できます。

  AWS Systems Manager コンソールには、管理者とエンドユーザーの両方に向けたすべての Session Manager 機能へのアクセスが含まれています。セッションに関連するタスクは、すべて Systems Manager コンソールを使用して実行できます。

  Amazon EC2 コンソールは、エンドユーザーがセッションアクセス許可を付与されている EC2 インスタンスに接続できるようにします。

  AWS CLI には、エンドユーザー向けの Session Manager 機能へのアクセスが含まれています。AWS CLI を使用すると、セッションを開始したり、セッションのリストを表示したり、セッションを完全に終了させることができます。

  > **Note**
  >
  > AWS CLI を使用してセッションコマンドを実行するには、CLI のバージョン 1.16.12 (またはそれ以降) を使用していて、ローカルマシンに Session Manager プラグインがインストールされている必要があります。詳細については、AWS CLI 用の Session Manager プラグインをインストールする を参照してください。GitHub でプラグインを表示するには、「session-manager-plugin」を参照してください。

- IAM アクセスコントロール

  IAM ポリシーにより、組織のどのメンバーがマネージドノードにセッションを開始できるか、およびどのノードにアクセスできるかについて管理できます。マネージドノードへの一時的なアクセス権を付与することもできます。たとえば、オンコールエンジニア (またはオンコールエンジニアのグループ) に、彼らのローテーション期間に限って本稼働サーバーへのアクセス権を与える場合があります。

- ログ記録のサポート

Session Manager は、他の多くの AWS のサービスとの統合により、AWS アカウント内のセッション履歴を口グに記録するためのオプションを提供します。詳細については、「セッションアクティビティの口グ記録」およびセッション口ギングの有効化と無効化を参照してください。

- 設定可能なシェルプロファイル

  Session Manager には、セッション内でプリファレンスを設定するためのオプションが用意されています。これらのカスタマイズ可能なプロファイルを使用すると、シェルの設定、環境変数、作業ディレクトリ、セッション開始時の複数のコマンドの実行など、セッション内の設定をカスタマイズできます。

- お客様のキーデータ暗号化のサポート

  Amazon Simple Storage Service (Amazon S3) バケットに送信する、または CloudWatch Logs 口ググループにストリームするセッションデータログを暗号化するように、Session Manager を設定できます。セッション中にクライアントマシンとマネージドノード間で送信されるデータをさらに暗号化するように Session Manager を設定することもできます。詳細については、「セッション口ギングの有効化と無効化」および「セッション設定を構成する」を参照してください。

- パブリック IP アドレスのないマネージドノード用の AWS PrivateLink サポート

  また、AWS PrivateLink を使用して Systems Manager の VPC エンドポイントを設定し、セッションのセキュリティ保護を強化することができます。AWS PrivateLink は、マネージドノード、Systems Manager、Amazon EC2 と Amazon ネットワーク間すべてのネットワークトラフィックを制限します。詳細については、「Systems Manager のために VPC エンドポイントを使用して EC2 インスタンスのセキュリティを強化する」を参照してください。

- トンネリング

  セッションの際、セッションタイプ AWS Systems Manager (SSM) ドキュメントを使用して、クライアントマシンのローカルポートとマネージドノードのリモートポート間のトラフィック (http またはカスタムプロトコルなど) をトンネルします。

- インタラクティブコマンド

  セッションを使用して単一のコマンドをインタラクティブに実行するセッションタイプ SSM ドキュメントを作成します。これにより、マネージドノードでユーザーができる操作を管理する手段が得られます。

セッションとは何ですか。

セッションは Session Manager を使用してマネージドノードに確立された接続です。セッションは、クライアント (お客様) とコマンドの入出力をストリーミングするリモートマネージドノードとの間の安全な双方向通信チャネルに基づいています。クライアントとマネージドノード間のトラフィックは TLS 1.2 を使用して暗号化され、接続の作成リクエストは Sigv4 を使用して署名されます。この双方向通信はマネージドノードへのインタラクティブ・バッシュとパワーシェル アクセスが可能になります。AWS Key Management Service (AWS KMS) キーを使用して、デフォルトの TLS 暗号化よりも強力なデータの暗号化を行うこともできます。

たとえば、John が IT 部門のオンコールエンジニアであるとします。彼はトラブルシューティングが必要な障害、またはノードへの簡単な構成オプションを変更するディレクティブなど、マネージドノードにリモート接続を必要とする問題について、通知を受けます。John は AWS Systems Manager コンソール、Amazon EC2 コンソール、または AWS CLI を使用しマネージドノードに接続するセッションを開始し、タスクの完了に必要なコマンドをノード上で実行したらセッションを終了します。

John がセッションを開始するための最初のコマンドを送信すると、Session Manager サービスは ID を認証し、IAM ポリシーにより付与されたアクセス権限を検証して、設定 (セッションの許容限度の確認など) を確認します。それから、SSM Agent にメッセージを送信して双方向接続を開きます。接続の確立後、John が次のコマンドを入力すると、SSM Agent からのコマンド出力がこの通信チャネルにアップロードされ、ローカルマシンに送り返されます。

トピック

- Session Manager を設定する
- Session Manager の使用
- 「セッションアクティビティのログ記録」
- セッションロギングの有効化と無効化
- セッションドキュメントスキーマ
- Session Manager のトラブルシューティング

Session Manager を設定する

AWS Systems Manager の Session Manager を使ってアカウント内のマネージドノードに接続する前に、以下のトピックの手順を完了してください。

トピック

- ステップ 1: Session Manager の前提条件を満たす
- ステップ 2: Session Manager のインスタンスのアクセス権限の確認または追加
- ステップ 3: マネージドノードへのセッションアクセスを制御
- ステップ 4: セッション設定を構成する
- ステップ 5: (オプション) セッションでのコマンドへのアクセスを制限する
- ステップ 6: (オプション) AWS PrivateLink を使用して Session Manager の VPC エンドポイントを設定する
- ステップ 7: (オプション) ssm-user アカウントの管理アクセス許可を有効または無効にする
- ステップ 8: (オプション) Session Manager を通して SSH 接続のアクセス許可を付与および制御する

ステップ 1: Session Manager の前提条件を満たす

Session Manager を使用する前に、環境が以下の要件を満たしていることを確認します。

Session Manager の前提条件

要件	説明
サポートされるオペレーティングシステム	Session Manager はアドバンストインスタンス層を使用するハイブリッドおよびマルチクラウド環境内の非 EC2 マシンに加え、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスへの接続もサポートします。 Session Manager では、次のオペレーティングシステムのバージョンがサポートされています。 **Note** Session Manager はアドバンストインスタンス層を使用するハイブリッドおよびマルチクラウド環境内の EC2 インスタンス、エッジデバイス、オンプレミスサーバー、仮想マシン (VM) をサポートします。アドバンストインスタ

要件	説明
	ンスの詳細については、「インスタンス層の設定」を参照してください。 Linux および macOS Session Manager は、AWS Systems Manager でサポートされている Linux および macOS のすべてのバージョンをサポートしています。詳細については、サポートされているオペレーティングシステムとマシンタイプ を参照してください。 Windows Session Manager は Windows Server 2012 から Windows Server 2022 をサポートします。 **Note** Microsoft Windows Server 2016 Nano はサポートされていません。

要件	説明
SSM Agent	少なくとも、セッションを介して接続するマネージドノードに AWS Systems Manager の SSM Agent バージョン 2.3.68.0 以降をインストールする必要があります。 AWS Key Management Service (AWS KMS) で作成したキーを使用してセッションデータを暗号化するオプションを使用するため、SSM Agent のバージョン 2.3.539.0 以降がマネージドノードにインストールされている必要があります。 セッションでシェルプロファイルを使用するには、マネージドノードに SSM Agent のバージョン 3.0.161.0 以降がインストールされている必要があります。 Session Manager ポート転送または SSH セッションを開始するには、マネージドノードに SSM Agent のバージョン 3.0.222.0 以降がインストールされている必要があります。 Amazon CloudWatch Logs を使用してセッションデータをストリーミングするには、マネージドノードに SSM Agent のバージョン 3.0.284.0 以降がインストールされている必要があります。 インスタンスで実行されているバージョン番号を確認する方法については、「SSM Agent バージョン番号の確認」を参照してください。SSM Agent の手動インストールまたは自動アップグレードについては、「「SSM Agent」 の使用」を参照してください。 ssm-user アカウントについて

要件	説明
	SSM Agent のバージョン 2.3.50.0 以降、エージェントはマネージドノード上にルートまたは管理者アクセス許可 (`ssm-user` と呼ばれる) のあるユーザーアカウントを作成します。(2.3.612.0 より前のバージョンでは、SSM Agent が起動または再起動するときにアカウントが作成されます。2.3.612.0 以降のバージョンでは、マネージドノード上でセッションが開始されるときに `ssm-user` が初めて作成されます) セッションは、このユーザーアカウントの管理者認証情報を使用して起動します。このアカウントの管理上の制御を制限することの詳細については、「ssm-user アカウントの管理権限を無効または有効する」のトピックで入手できます。 Windows Server ドメインコントローラーの ssm-user SSM Agent の バージョン 2.3.612.0 以降、`ssm-user` アカウントは Windows Server のドメインコントローラーとして使用されているマネージドノードに自動的に作成されません。ドメインコントローラーとして使用されている Windows Server マシンで Session Manager を使用するには、 アカウントが存在しない場合は手動で `ssm-user` アカウントを作成し、ユーザーに Domain Administrator のアクセス許可を割り当てる必要があります。Windows Server で、SSM Agent はセッションが開始されるたびに `ssm-user` アカウントの新しいパスワードを設定するので、アカウントを作成するときにパスワードを指定する必要はありません。

要件	説明
エンドポイントへの接続	接続するマネージドノードは、以下のエンドポイントへの HTTPS (ポート 443) アウトバウンド・トラフィックも許可する必要があります: • ec2messages.*region*.amazonaws.com • ssm.*region*.amazonaws.com • ssmmessages.*region*.amazonaws.com 詳細については、以下の各トピックを参照してください。 • リファレンス: ec2messages、ssmmessages およびその他の API オペレーション • AWS re:Post ナレッジセンターの「Systems Manager を使用してインターネットアクセスなしでプライベート EC2 インスタンスを管理できるように、VPC エンドポイントを作成するにはどうすればよいですか?」。 または、インターフェイスエンドポイントを使用して必要なエンドポイントに接続することもできます。詳細については、「ステップ 6: (オプション) AWS PrivateLink を使用して Session Manager の VPC エンドポイントを設定する」を参照してください。

要件	説明
AWS CLI	(オプション) (AWS Systems Manager コンソールまたは Amazon EC2 コンソールを使用する代わりに) AWS Command Line Interface (AWS CLI) を使用してセッションを開始する場合は、CLI のバージョン 1.16.12 以降をローカルマシンにインストールする必要があります。 `aws --version` を呼び出すとバージョンを確認できます。 CLI をインストールまたはアップグレードする必要がある場合は、AWS Command Line Interface ユーザーガイドの「AWS Command Line Interface のインストール」を参照してください。 **Important** 新しいツールが Systems Manager に追加されるか、既存のツールが更新されると必ず、更新されたバージョンの SSM Agent がリリースされます。最新バージョンのエージェントを使用しないと、マネージドノードが Systems Manager の各種ツールや機能を使用できなくなる可能性があります。このため、マシン上で SSM Agent を最新状態に維持するプロセスを自動化することをお勧めします。詳細については、SSM Agent への更新の自動化 を参照してください。GitHub の「SSM Agent リリースノート」ページをサブスクライブすると、SSM Agent の更新に関する通知を受け取ることができます。

要件	説明
	さらに CLI を使って Session Manager でノードを管理する場合、まずローカルマシンに Session Manager プラグインをインストールする必要があります。詳細については、AWS CLI 用の Session Manager プラグインをインストールする を参照してください。
アドバンストインスタンス層 (ハイブリッドおよびマルチクラウド環境) を有効にする	Session Manager で非 EC2 に接続する場合、非 EC2 マシンをマネージドノードとして登録するためにハイブリッドアクティベーションを作成する際に AWS アカウント と AWS リージョン のアドバンストインスタンス層を有効にします。アドバンストインスタンス層の使用には料金が発生します。アドバンストインスタンス層の詳細については、インスタンス層の設定 をご参照ください。

要件	説明
IAM サービスロールの許可 (ハイブリッドおよびマルチクラウド環境) の確認	ハイブリッドアクティベーションノードは Systems Manager API オペレーションと通信するため、ハイブリッドアクティベーションで指定された AWS Identity and Access Management (IAM) サービスロールを使用します。このサービスロールには、Session Manager を使用してハイブリッドおよびマルチクラウドマシンに接続するために必要な許可が含まれている必要があります。サービスロールが AWS 管理ポリシー `AmazonSSMManagedInstanceCore` を含む場合、Session Manager に必要なアクセス許可は既に付与されています。 サービスロールに必要な許可が含まれていない場合、マネージドインスタンスの登録を解除し、必要な許可を持った IAM サービスロールを使用する新しいハイブリッドアクティベーションで登録する必要があります。マネージドインスタンスの登録解除の詳細については「ハイブリッドおよびマルチクラウド環境でのマネージドノードの登録解除」をご参照ください。Session Manager アクセス権限付き IAM ポリシーの作成方法の詳細については「ステップ 2: Session Manager のインスタンスのアクセス権限の確認または追加」を参照してください。

ステップ 2: Session Manager のインスタンスのアクセス権限の確認または追加

デフォルトでは、AWS Systems Manager にはインスタンスでアクションを実行する権限がありません。インスタンスのアクセス許可は、AWS Identity and Access Management (IAM) ロールを使用してアカウントレベルで付与するか、またはインスタンスプロファイルを使用してインスタンスレベルで付与することができます。可能であれば、デフォルトのホスト管理設定を使用してアカウントレベルでアクセスを付与することをお勧めします。`AmazonSSMManagedEC2InstanceDefaultPolicy` ポリシーを使用してアカウントのデフォ

ルトホスト管理設定を既にセットアップしている場合は、次のステップに進むことができます。デフォルトのホスト管理設定の詳細については、「Default Host Management Configuration を使用した EC2 インスタンスの自動管理」を参照してください。

インスタンスプロファイルを使用してインスタンスに必要なアクセス権限を提供することもできます。インスタンスプロファイルは IAM ロールを Amazon EC2 インスタンスに渡します。IAM インスタンスプロファイルは、起動時の Amazon EC2 インスタンスまたは以前に起動したインスタンスにアタッチできます。詳細についてはインスタンスプロファイルの使用をご参照ください。

オンプレミスサーバーまたは仮想マシン (VM) の場合、アクセス許可はハイブリッドアクティベーションに関連付けられた IAM サービスロールによって付与されます。ハイブリッドアクティベーションは、Systems Manager 付きオンプレミスサーバーおよび VM の登録に使用します。オンプレミスサーバーと VM はインスタンスプロファイルを使用しません。

Run Command や Parameter Store など、他の Systems Manager ツールを既に使用している場合、Session Manager に必要な基本許可を持つインスタンスプロファイルが既に Amazon EC2 インスタンスに添付されている可能性があります。AWS 管理ポリシー `AmazonSSMManagedInstanceCore` を含むインスタンスプロファイルが既にインスタンスにアタッチされている場合、Session Manager に必要なアクセス許可は既に付与されています。これはハイブリッドアクティベーションで使用される IAM サービスロールに `AmazonSSMManagedInstanceCore` 管理ポリシーが含まれる場合も適用されます。

ただし、場合によっては、インスタンスプロファイルにアタッチされたアクセス許可を変更する必要があります。例えば、インスタンスのアクセス許可のセットを絞り込む場合、インスタンスプロファイルのカスタムポリシーを作成した場合、Amazon Simple Storage Service (Amazon S3) 暗号化オプションまたは AWS Key Management Service (AWS KMS) 暗号化オプションを使用してセッションデータを保護する場合などです。このような場合は、次のいずれかを実行して、インスタンスで Session Manager アクションを実行できるようにします。

- カスタム IAM ロールの Session Manager アクション用の許可を埋め込む

  AWS が提供するデフォルトのポリシー `AmazonSSMManagedInstanceCore` に依存しない既存の IAM ロールに Session Manager アクションのアクセス許可を追加するには、次の 既存の IAM ロールに Session Manager 許可を追加する の手順に従います。
- Session Manager の許可のみ付与したカスタム IAM ロールを作成

  Session Manager アクションのみの許可を含む IAM ロールを作成する場合、Session Manager のカスタム IAM ロールを作成 のステップにしたがいます。
- すべての Systems Manager アクション用の許可を持った新しい IAM ロールの作成と使用

AWS が提供するデフォルトポリシーを使用する Systems Manager マネージドインスタンスの IAM ロールを作成してすべての Systems Manager にアクセス許可を付与する場合は、「Systems Manager に必要なインスタンスのアクセス許可を設定する」のステップに従います。

トピック

- 既存の IAM ロールに Session Manager 許可を追加する
- Session Manager のカスタム IAM ロールを作成

既存の IAM ロールに Session Manager 許可を追加する

以下の手順を使用して、既存の AWS Identity and Access Management (IAM) ロールに Session Manager 権限を追加します。既存のロールに権限を追加することで、インスタンス権限に AWS `AmazonSSMManagedInstanceCore` ポリシーを使用することなく、コンピューティング環境のセキュリティを強化できます。

> **Note**
>
> 以下の情報に注意してください。
>
> - この手順は、アクセスを許可するアクションに対する他の Systems Manager `ssm` 権限が、既存のロールに既に含まれていることを前提とします。このポリシーだけでは、Session Manager を使用するには十分ではありません。
> - 次のポリシー例には、`s3:GetEncryptionConfiguration` アクションが含まれています。このアクションは、Session Manager 口ギング設定で [S3 ログ暗号化を強制] オプションインを選択した場合に必要です。

Session Manager の許可を既存のロール (コンソール) に追加する場合

1. AWS Management Console にサインインして、IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. ナビゲーションペインで Roles (ロール) を選択します。
3. アクセス許可を追加するロール名を選択します。
4. [アクセス許可] タブを選択します。
5. [アクセス許可の追加]、[インラインポリシーの作成] の順に選択します。

6. [JSON] タブを選択します。
7. デフォルトのポリシーコンテンツを次のコンテンツに置き換えます。*key-name* を、使用する AWS Key Management Service キー (AWS KMS key) の Amazon リソースネーム (ARN) に置き換えます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssmmessages:CreateControlChannel",
                "ssmmessages:CreateDataChannel",
                "ssmmessages:OpenControlChannel",
                "ssmmessages:OpenDataChannel"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetEncryptionConfiguration"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": "key-name"
        }
    ]
}
```

セッションデータを暗号化するための KMS キーの使用については、「セッションデータの KMS キー暗号化を有効にする (コンソール)」を参照してください。

セッションデータに AWS KMS 暗号化を使用しない場合は、ポリシーから以下のコンテンツを削除できます。

```
,
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": "key-name"
        }
```

8. [Next: Tags] (次へ: タグ) を選択します。
9. (オプション) [Add tag] (タグを追加) を選択してタグを追加し、ポリシーの優先タグを入力します。
10. [次へ: レビュー] を選択します。
11. [Review policy (ポリシーの確認)] ページで、[Name (名前)] にインラインポリシーの名前を入力します (**SessionManagerPermissions** など)。
12. (オプション) [Description (説明)] に、ポリシーの説明を入力します。

    [Create policy] を選択します。

ssmmessages アクションの詳細については、「リファレンス: ec2messages、ssmmessages およびその他の API オペレーション」を参照してください。

Session Manager のカスタム IAM ロールを作成

Amazon EC2 マネージドインスタンスでアクションを実行する許可を Session Manager に付与する AWS Identity and Access Management (IAM) ロールを作成できます。Amazon Simple Storage Service (Amazon S3) と Amazon CloudWatch Logs に送信されるセッションログの許可を付与するポリシーを作成することもできます。

IAM ロールを作成後、インスタンスのロールをアタッチする情報については、AWS re:Post ウェブサイトの「インスタンスプロファイルをアタッチまたは置き換え」を参照してください。IAM インスタンスのプロファイルとロールの詳細については、「IAM ユーザーガイド」の「インスタンスプロファイルの使用」と、「Linux インスタンス用 Amazon Elastic Compute Cloud ユーザーガイド」の「Amazon EC2 の IAM ロールの使用」を参照してください。オンプレミスマシンの IAM サービスロールの作成における詳細については、「ハイブリッドおよびマルチクラウド環境で Systems Manager に必要な IAM サービスロールを作成する」を参照してください。

トピック

- 最小限の Session Manager 許可 (コンソール) を付与した IAM ロールの作成
- Session Manager、Amazon S3、CloudWatch Logs (コンソール) の許可を持つIAM ロールの作成

最小限の Session Manager 許可 (コンソール) を付与した IAM ロールの作成

以下の手順にしたがって、インスタンス上の Session Manager アクションのみに許可を付与するポリシーが付いたカスタム IAM ロールを作成します。

最小限の Session Manager アクセス権限でインスタンスプロファイルを作成するには (コンソール)

1. AWS Management Console にサインインして、IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. ナビゲーションペインで、[Policies] を選択し、次に [Create policy] を選択します。([Get Started] ボタンが表示された場合は、そのボタンを選択してから、[Create Policy] を選択します)。
3. [JSON] タブを選択します。
4. デフォルトの内容を次のポリシーに置き換えます。AWS Key Management Service (AWS KMS) を使用してセッションデータを暗号化するには、*key-name* を、使用する AWS KMS key の Amazon リソースネーム (ARN) に置き換えます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:UpdateInstanceInformation",
                "ssmmessages:CreateControlChannel",
                "ssmmessages:CreateDataChannel",
                "ssmmessages:OpenControlChannel",
                "ssmmessages:OpenDataChannel"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": "key-name"
```

```
        }
    ]
}
```

セッションデータを暗号化するための KMS キーの使用については、「セッションデータの KMS キー暗号化を有効にする (コンソール)」を参照してください。

セッションデータに AWS KMS 暗号化を使用しない場合は、ポリシーから以下のコンテンツを削除できます。

```
,
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": "key-name"
        }
```

5. [Next: Tags] (次へ: タグ) を選択します。
6. (オプション) [Add tag] (タグを追加) を選択してタグを追加し、ポリシーの優先タグを入力します。
7. [次へ: レビュー] を選択します。
8. [Review policy (ポリシーの確認)] ページで、[Name (名前)] にインラインポリシーの名前を入力します (**SessionManagerPermissions** など)。
9. (オプション) [Description (説明)] に、ポリシーの説明を入力します。
10. [Create policy] を選択します。
11. ナビゲーションペインで [Roles] を選択し、続いて [Create role] を選択します。
12. [ロールを作成] ページで [AWS サービス] を選択して、[ユースケース] で [EC2] を選択します。
13. [Next] を選択します。
14. [Add permissions] (アクセス許可を追加) ページで、先ほど作成したポリシーの名前 (**SessionManagerPermissions** など) の左側にあるチェックボックスをオンにします。
15. [Next] を選択します。
16. [Name, review, and create] (名前、確認、および作成) ページの [Role name] (ロール名) に、IAM ロールの名前 (**MySessionManagerRole** など) を入力します。

17. (オプション) [Role description (ロールの説明)] に、インスタンスプロファイルの説明を入力します。
18. (オプション) [Add tag] (タグを追加) を選択してタグを追加し、ロールの優先タグを入力します。

    [ロールの作成] を選択します。

ssmmessages アクションの詳細については、「リファレンス: ec2messages、ssmmessages およびその他の API オペレーション」を参照してください。

Session Manager、Amazon S3、CloudWatch Logs (コンソール) の許可を持つIAM ロールの作成

以下の手順にしたがって、インスタンス上の Session Manager アクションに許可を付与するポリシーが付いたカスタム IAM ロールを作成します。このポリシーは、セッションログを Amazon Simple Storage Service (Amazon S3) バケットおよび Amazon CloudWatch Logs ロググループに保存するために必要なアクセス許可も提供します。

> **Important**
>
> セッションログを別の AWS アカウント によって所有されている Amazon S3 バケットに出力するには、IAM ロールポリシーに `s3:PutObjectAcl` の許可を追加する必要があります。さらに、バケットポリシーで、所有アカウントが使用する IAM ロールへのクロスアカウントアクセスを許可して、管理対象インスタンスに Systems Manager 許可を付与するようにする必要があります。バケットが Key Management Service (KMS) 暗号化を使用している場合は、バケットの KMS ポリシーでもこのクロスアカウントアクセスを許可する必要があります。Amazon S3 クロスアカウントバケットの許可の詳細については、「Amazon Simple Storage Service ユーザーガイド」の「クロスアカウントバケットパーミッションを付与する」を参照してください。クロスアカウントの許可が追加されていないと、Amazon S3 バケットを所有するアカウントはセッション出力ログにアクセスできません。

セッションログを保存するための設定の指定方法については、「セッションロギングの有効化と無効化」を参照してください。

Session Manager、Amazon S3、CloudWatch Logs (コンソール) の許可を持つIAM ロールの作成方法

1. AWS Management Console にサインインして、IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. ナビゲーションペインで、[Policies] を選択し、次に [Create policy] を選択します。([Get Started] ボタンが表示された場合は、そのボタンを選択してから、[Create Policy] を選択します)。
3. [JSON] タブを選択します。
4. デフォルトの内容を次のポリシーに置き換えます。各##############をユーザー自身の情報に置き換えます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssmmessages:CreateControlChannel",
                "ssmmessages:CreateDataChannel",
                "ssmmessages:OpenControlChannel",
                "ssmmessages:OpenDataChannel",
                "ssm:UpdateInstanceInformation"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:DescribeLogGroups",
                "logs:DescribeLogStreams"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
```

```
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/s3-prefix/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetEncryptionConfiguration"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": "key-name"
        },
        {
            "Effect": "Allow",
            "Action": "kms:GenerateDataKey",
            "Resource": "*"
        }
    ]
}
```

5. [Next: Tags] (次へ: タグ) を選択します。
6. (オプション) [Add tag] (タグを追加) を選択してタグを追加し、ポリシーの優先タグを入力します。
7. [次へ: レビュー] を選択します。
8. [Review policy (ポリシーの確認)] ページで、[Name (名前)] にインラインポリシーの名前を入力します (**SessionManagerPermissions** など)。
9. (オプション) [Description (説明)] に、ポリシーの説明を入力します。
10. [Create policy] を選択します。
11. ナビゲーションペインで [Roles] を選択し、続いて [Create role] を選択します。
12. [ロールを作成] ページで [AWS サービス] を選択して、[ユースケース] で [EC2] を選択します。
13. [Next] を選択します。
14. [Add permissions] (アクセス許可を追加) ページで、先ほど作成したポリシーの名前 (**SessionManagerPermissions** など) の左側にあるチェックボックスをオンにします。
15. [Next] を選択します。

16. [Name, review, and create] (名前、確認、および作成) ページの [Role name] (ロール名) に、IAM ロールの名前 (**MySessionManagerRole** など) を入力します。
17. (オプション) [Role description] (ロールの説明) に、ロールの説明を入力します。
18. (オプション) [Add tag] (タグを追加) を選択してタグを追加し、ロールの優先タグを入力します。
19. [ロールの作成] を選択します。

ステップ 3: マネージドノードへのセッションアクセスを制御

この方法で、AWS Identity and Access Management (IAM) ポリシーを使用してマネージドノードへの Session Manager のアクセスを許可または取り消すことができます。ポリシーを作成して IAM ユーザーまたはグループにアタッチし、そのユーザーまたはグループが接続できるマネージドノードを指定することができます。また、ユーザーまたはグループがマネージドノードで実行できる Session Manager API オペレーションを指定することもできます。

Session Manager の IAM アクセス許可ポリシーを使い始めるために、エンドユーザーと管理者ユーザー用のサンプルポリシーを作成しました。これらのポリシーは、わずかな変更だけで使用できます。または、これらをガイドとして使用し、カスタム IAM ポリシーを作成することもできます。詳細については、「Session Manager のサンプル IAM ポリシー」を参照してください。IAM ポリシーの作成方法、およびポリシーをユーザーまたはグループにアタッチする方法については、「IAM ユーザーガイド」の「IAM ポリシーの作成」および「IAM ポリシーの追加と削除」を参照してください。

セッション ID の ARN 形式について

Session Manager アクセスの IAM ポリシーを作成する際は、Amazon リソースネーム (ARN) の一部としてセッション ID を指定します。セッション ID にはユーザー名が変数として含まれます。これを説明するために、Session Manager ARN の形式と例を以下に示します。

```
arn:aws:ssm:region-id:account-id:session/session-id
```

例:

```
arn:aws:ssm:us-east-2:123456789012:session/JohnDoe-1a2b3c4d5eEXAMPLE
```

IAM ポリシーで変数を使用する方法の詳細については、「IAM ポリシーエレメント: 変数」を参照してください。

トピック

- IAM ポリシーでデフォルトのセッションドキュメントを指定して、デフォルトのシェルセッションを開始します。
- IAM ポリシーでセッションドキュメントを指定して、ドキュメントでセッションを開始する
- Session Manager のサンプル IAM ポリシー
- Session Manager の追加サンプル IAM ポリシー

IAM ポリシーでデフォルトのセッションドキュメントを指定して、デフォルトのシェルセッションを開始します。

AWS アカウント 用に Session Manager を設定したり、Systems Manager コンソールでセッション設定を変更したりすると、システムによって `SSM-SessionManagerRunShell` という名前の SSM セッションドキュメントが作成されます。これはデフォルトのセッションドキュメントです。Session Manager はこのドキュメントを使用して、次のような情報を含むセッション設定を保存します。

- Amazon Simple Storage Service (Amazon S3) バケットまたは Amazon CloudWatch Logs ロググループなどのセッションデータを格納する場所です。
- セッションデータを暗号化するための AWS Key Management Service (AWS KMS) キー ID。
- セッションで Run As サポートが許可されているかどうか。

`SSM-SessionManagerRunShell` セッションの設定文書に含まれる情報の例を次に示します。

```
{
  "schemaVersion": "1.0",
  "description": "Document to hold regional settings for Session Manager",
  "sessionType": "Standard_Stream",
  "inputs": {
    "s3BucketName": "amzn-s3-demo-bucket",
    "s3KeyPrefix": "MyS3Prefix",
    "s3EncryptionEnabled": true,
    "cloudWatchLogGroupName": "MyCWLogGroup",
    "cloudWatchEncryptionEnabled": false,
    "kmsKeyId": "1a2b3c4d",
    "runAsEnabled": true,
    "runAsDefaultUser": "RunAsUser"
  }
}
```

デフォルトでは、ユーザーが AWS Management Console からセッションを開始すると、Session Manager はデフォルトのセッションドキュメントを使用します。これは、Systems Manager コンソール、Amazon EC2 コンソールの EC2 Connect で Fleet Manager または Session Manager のいずれかに適用されます。また、Session Manager はユーザーが次の例のような AWS CLI コマンドを使用してセッションを開始したときに、デフォルトのセッションドキュメントを使用します。

```
aws ssm start-session \
    --target i-02573cafcfEXAMPLE
```

デフォルトのシェルセッションを開始するには、次の例に示すように、IAM ポリシーでデフォルトのセッションドキュメントを指定する必要があります。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnableSSMSession",
      "Effect": "Allow",
      "Action": [
        "ssm:StartSession"
      ],
      "Resource": [
        "arn:aws:ec2:us-west-2:123456789012:instance/i-02573cafcfEXAMPLE",
        "arn:aws:ssm:us-west-2:123456789012:document/SSM-SessionManagerRunShell"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ssmmessages:OpenDataChannel"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

IAM ポリシーでセッションドキュメントを指定して、ドキュメントでセッションを開始する

デフォルトのセッションドキュメントを使用して start-session AWS CLI コマンドを使用する場合は、ドキュメント名を省略できます。システムは自動的に SSM-SessionManagerRunShell セッションドキュメントを呼び出します。

その他の場合は、document-name パラメータに値を指定する必要があります。ユーザーがコマンドでセッションドキュメントの名前を指定すると、システムは IAM ポリシーをチェックして、そのドキュメントにアクセスするアクセス許可があることを確認します。アクセス許可がないと、接続リクエストは失敗します。以下の例では、AWS-StartPortForwardingSessionセッションドキュメントに document-name パラメータが含まれています。

```
aws ssm start-session \
    --target i-02573cafcfEXAMPLE \
    --document-name AWS-StartPortForwardingSession \
    --parameters '{"portNumber":["80"], "localPortNumber":["56789"]}'
```

IAM ポリシーで Session Manager セッションドキュメントを指定する方法の例については、「クイックスタート Session Manager のエンドユーザーポリシー」を参照してください。

> **Note**
>
> SSH を使用してセッションを開始するには、ターゲットマネージドノードとユーザーのローカルマシンで設定ステップを完了する必要があります。詳細については、「(オプション) Session Manager を通して SSH 接続のアクセス許可を付与して制御する」を参照してください。

Session Manager のサンプル IAM ポリシー

このセクションのサンプルを使用して、一般的に Session Manager のアクセスに最も必要とされるアクセス許可を提供する、AWS Identity and Access Management (IAM) ポリシーを作成します。

> **Note**
>
> AWS KMS key ポリシーを使用して、KMS キーへのアクセス権を付与する IAM エンティティ (ユーザーまたはロール) と AWS アカウント を管理することもできます。詳細については、AWS Key Management Service デベロッパーガイドの「AWS KMS リソースへのアクセス管理の概要」および「AWS KMS でのキーポリシーの使用」を参照してください。

トピック

- クイックスタート Session Manager のエンドユーザーポリシー
- クイックスタート Session Manager の管理者ポリシー

クイックスタート Session Manager のエンドユーザーポリシー

次の例を使用して、Session Manager の IAM エンドユーザーポリシーを作成します。

Session Manager コンソールと AWS Command Line Interface (AWS CLI) のみ、Amazon Elastic Compute Cloud (Amazon EC2) コンソールのみ、または 3 つすべてからセッションを開始できるようにするポリシーを作成できます。

このポリシーはエンドユーザーに対して特定のマネージドノードへのセッションを開始する権限と、自分のセッションのみを終了する権限を提供します。ポリシーに対して行うカスタマイズの例については、「Session Manager の追加サンプル IAM ポリシー」を参照してください。

次のサンプルポリシーで、各##############をユーザー自身の情報に置き換えます。

提供するセッションアクセスの範囲のサンプルポリシーを表示するには、次のセクションを参照してください。

セッションマネージャー and Fleet Manager

ユーザーが Session Manager コンソールと Fleet Manager コンソールからのみセッションを開始および再開できるようにするには、このサンプルポリシーを使用します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:StartSession"
            ],
            "Resource": [
                "arn:aws:ec2:region:account-id:instance/instance-id",
                "arn:aws:ssm:region:account-id:document/SSM-
SessionManagerRunShell" (1)
            ]
        },
        {
```

```
          "Effect": "Allow",
          "Action": ["ssmmessages:OpenDataChannel"],
          "Resource": ["arn:aws:ssm:*:*:session/${aws:userid}-*"]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeSessions",
                "ssm:GetConnectionStatus",
                "ssm:DescribeInstanceProperties",
                "ec2:DescribeInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:TerminateSession",
                "ssm:ResumeSession"
            ],
            "Resource": [
                "arn:aws:ssm:*:*:session/${aws:userid}-*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [

 "kms:GenerateDataKey" (2)
            ],
            "Resource": "key-name"
        }
    ]
}
```

Amazon EC2

ユーザーが Amazon EC2 コンソールからのみセッションを開始および再開できるようにするには、このサンプルポリシーを使用します。このポリシーでは、Session Manager コンソールおよび AWS CLI からセッションを開始するために必要なすべてのアクセス許可は提供されません。

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

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:StartSession",

 "ssm:SendCommand" 3
            ],
            "Resource": [
                "arn:aws:ec2:region:account-id:instance/instance-id",
                "arn:aws:ssm:region:account-id:document/SSM-
SessionManagerRunShell" 1
            ]
        },
        {
         "Effect": "Allow",
         "Action": ["ssmmessages:OpenDataChannel"],
         "Resource": ["arn:aws:ssm:*:*:session/${aws:userid}-*"]
       },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:GetConnectionStatus",
                "ssm:DescribeInstanceInformation"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:TerminateSession",
                "ssm:ResumeSession"
            ],
            "Resource": [
                "arn:aws:ssm:*:*:session/${aws:username}-*"
            ]
        }
    ]
}
```

AWS CLI

ユーザーが AWS CLI からセッションを開始および再開できるようにするには、このサンプルポリシーを使用します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:StartSession",

 "ssm:SendCommand" 3
            ],
            "Resource": [
                "arn:aws:ec2:region:account-id:instance/instance-id",
                "arn:aws:ssm:region:account-id:document/SSM-
SessionManagerRunShell" 1
            ]
        },
        {
         "Effect": "Allow",
         "Action": ["ssmmessages:OpenDataChannel"],
         "Resource": ["arn:aws:ssm:*:*:session/${aws:userid}-*"]
       },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:TerminateSession",
                "ssm:ResumeSession"
            ],
            "Resource": [
                "arn:aws:ssm:*:*:session/${aws:userid}-*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [

 "kms:GenerateDataKey" 2
            ],
            "Resource": "key-name"
```

```
        }
    ]
}
```

[1] SSM-SessionManagerRunShell は、セッションの設定を保存するために Session Manager によって作成される SSM ドキュメントのデフォルト名です。代わりに、カスタムのセッションドキュメントを作成し、このポリシーで指定できます。また、SSH を使用してセッションを開始するユーザー向けに、AWS が提供するドキュメント AWS-StartSSHSession を指定することもできます。SSH を使用したセッションをサポートするために必要な設定手順については、「(オプション) Session Manager を通して SSH 接続のアクセス許可を付与して制御する」を参照してください。

[2] kms:GenerateDataKey 許可により、セッションデータの暗号化に使用されるデータ暗号化キーを作成できます。セッションデータにAWS Key Management Service (AWS KMS) 暗号化を使用する場合は、*key-name* を arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-12345EXAMPLE 形式で、使用する KMS キーの Amazon リソースネーム (ARN) に置き換えてください。セッションデータに KMS キー暗号化を使用しない場合は、ポリシーから次のコンテンツを削除します。

```
{
            "Effect": "Allow",
            "Action": [
                "kms:GenerateDataKey"
            ],
            "Resource": "key-name"
        }
```

セッションデータを暗号化するための AWS KMS の使用の詳細については、「セッションデータの KMS キー暗号化を有効にする (コンソール)」を参照してください。

[3] SendCommand の許可は、ユーザーが Amazon EC2 コンソールからセッションを開始しようとする場合に必要ですが、まず SSM Agent を Session Manager に必要な最小限のバージョンに更新する必要があります。Run Command は、インスタンスにコマンドを送信してエージェントを更新するために使用されます。

クイックスタート Session Manager の管理者ポリシー

次の例を使用して、Session Manager の IAM 管理者ポリシーを作成します。

このポリシーは、Key=Finance,Value=WebServers でタグ付けされたマネージドノードに対してセッションを開始する権限、および作成、更新、削除する許可、自分のセッションのみを終了する許可を管理者に提供します。ポリシーに対して行うカスタマイズの例については、「Session Manager の追加サンプル IAM ポリシー」を参照してください。

管理者が Session Manager コンソールと AWS CLI からのみ、Amazon EC2 コンソールからのみ、または 3 つすべてからこれらのタスクを実行できるようにするポリシーを作成できます。

次のサンプルポリシーで、各###############をユーザー自身の情報に置き換えます。

3 つのアクセス許可シナリオのサンプルポリシーを表示するには、次のセクションを参照してください。

セッションマネージャー and CLI

管理者が Session Manager コンソールと AWS CLI からのみセッション関連のタスクを実行できるようにするには、このサンプルポリシーを使用します。このポリシーでは、Amazon EC2 コンソールからセッション関連のタスクを実行するために必要なすべてのアクセス許可は提供されません。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:StartSession"
            ],
            "Resource": [
                "arn:aws:ec2:region:account-id:instance/*"
            ],
            "Condition": {
                "StringLike": {
                    "ssm:resourceTag/Finance": [
                        "WebServers"
                    ]
                }
            }
        },
        {
         "Effect": "Allow",
         "Action": ["ssmmessages:OpenDataChannel"],
         "Resource": ["arn:aws:ssm:*:*:session/${aws:userid}-*"]
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeSessions",
                "ssm:GetConnectionStatus",
                "ssm:DescribeInstanceProperties",
                "ec2:DescribeInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:CreateDocument",
                "ssm:UpdateDocument",
                "ssm:GetDocument",
                "ssm:StartSession"
            ],
            "Resource": "arn:aws:ssm:region:account-id:document/SSM-
SessionManagerRunShell"
        },
        {
         "Effect": "Allow",
         "Action": ["ssmmessages:OpenDataChannel"],
         "Resource": ["arn:aws:ssm:*:*:session/${aws:userid}-*"]
       },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:TerminateSession",
                "ssm:ResumeSession"
            ],
            "Resource": [
                "arn:aws:ssm:*:*:session/${aws:userid}-*"
            ]
        }
    ]
}
```

Amazon EC2

管理者が Amazon EC2 コンソールからのみセッション関連のタスクを実行できるようにするには、このサンプルポリシーを使用します。このポリシーでは、Session Manager コンソールおよ

び AWS CLI からセッション関連のタスクを実行するために必要なすべてのアクセス許可は提供されません。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:StartSession",

 "ssm:SendCommand" 1
            ],
            "Resource": [
                "arn:aws:ec2:region:account-id:instance/*"
            ],
            "Condition": {
                "StringLike": {
                    "ssm:resourceTag/tag-key": [
                        "tag-value"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:StartSession"
            ],
            "Resource": [
                "arn:aws:ssm:region:account-id:document/SSM-SessionManagerRunShell"
            ]
        },
        {
         "Effect": "Allow",
         "Action": ["ssmmessages:OpenDataChannel"],
         "Resource": ["arn:aws:ssm:*:*:session/${aws:userid}-*"]
       },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:GetConnectionStatus",
                "ssm:DescribeInstanceInformation"
```

```
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:TerminateSession",
                "ssm:ResumeSession"
            ],
            "Resource": [
                "arn:aws:ssm:*:*:session/${aws:userid}-*"
            ]
        }
    ]
}
```

セッションマネージャー, CLI, and Amazon EC2

管理者が Session Manager コンソール、AWS CLI、Amazon EC2 コンソールからセッション関連のタスクを実行できるようにするには、このサンプルポリシーを使用します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:StartSession",

 "ssm:SendCommand" (1)
            ],
            "Resource": [
                "arn:aws:ec2:region:account-id:instance/*"
            ],
            "Condition": {
                "StringLike": {
                    "ssm:resourceTag/tag-key": [
                        "tag-value"
                    ]
                }
            }
        },
        {
```

```
          "Effect": "Allow",
          "Action": ["ssmmessages:OpenDataChannel"],
          "Resource": ["arn:aws:ssm:*:*:session/${aws:userid}-*"]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeSessions",
                "ssm:GetConnectionStatus",
                "ssm:DescribeInstanceInformation",
                "ssm:DescribeInstanceProperties",
                "ec2:DescribeInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:CreateDocument",
                "ssm:UpdateDocument",
                "ssm:GetDocument",
                "ssm:StartSession"
            ],
            "Resource": "arn:aws:ssm:region:account-id:document/SSM-
SessionManagerRunShell"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:TerminateSession",
                "ssm:ResumeSession"
            ],
            "Resource": [
                "arn:aws:ssm:*:*:session/${aws:userid}-*"
            ]
        }
    ]
}
```

[1] ユーザーが Amazon EC2 コンソールからセッションを開始しようとする際、最初に SSM Agent を更新するためのコマンドを送信する必要がある場合は、SendCommand のアクセス許可が必要です。

Session Manager の追加サンプル IAM ポリシー

サポートする Session Manager ユーザーのアクセスシナリオ用のカスタム AWS Identity and Access Management (IAM) ポリシーの作成に役立つ、次のサンプルポリシーを参照してください。

トピック

- 例 1: コンソールでドキュメントへのアクセスを許可する
- 例 2: 特定のマネージドノードへのアクセスを制限
- 例 3: タグに基づいてアクセスを制限
- 例 4: ユーザーが開始したセッションのみを終了できるようにする
- 例 5: すべてのセッションにフル (管理) アクセスを許可する

例 1: コンソールでドキュメントへのアクセスを許可する

ユーザーが Session Manager コンソールを使用してセッションを開始する場合、カスタムドキュメントを指定できるようにすることができます。次の IAM ポリシーの例では、指定された AWS リージョン および AWS アカウント で **SessionDocument-** で始まる名前のドキュメントにアクセスする許可を付与します。

このポリシーを使用するには、独自の情報を含むそれぞれの*###############*を置き換えます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:GetDocument",
                "ssm:ListDocuments"
            ],
            "Resource": [
                "arn:aws:ssm:region:account-id:document/SessionDocument-*"

            ]
        }
    ]
}
```

> **Note**
>
> Session Manager コンソールは、セッションプリファレンスの定義に使用される `Standard_Stream` の `sessionType` を持つセッションドキュメントのみをサポートします。詳細については、「セッションドキュメントスキーマ」を参照してください。

例 2: 特定のマネージドノードへのアクセスを制限

Session Manager を使用して、ユーザーが接続できるマネージドノードを定義する IAM ポリシーを作成できます。例えば、次のポリシーは、特定の 3 つのノードでセッションを開始、終了、再開するアクセス許可をユーザーに付与します。このポリシーは、指定されたノード以外のノードにユーザーが接続することを制限します。

> **Note**
>
> フェデレーテッドユーザーについては、「例 4: ユーザーが開始したセッションのみを終了できるようにする」を参照してください。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:StartSession"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-2:123456789012:instance/i-1234567890EXAMPLE",
                "arn:aws:ec2:us-east-2:123456789012:instance/i-abcdefghijEXAMPLE",
                "arn:aws:ec2:us-east-2:123456789012:instance/i-0e9d8c7b6aEXAMPLE",
                "arn:aws:ssm:us-east-2:123456789012:document/SSM-
SessionManagerRunShell"
            ]
        },
        {
         "Effect": "Allow",
         "Action": ["ssmmessages:OpenDataChannel"],
         "Resource": ["arn:aws:ssm:*:*:session/${aws:userid}-*"]
```

```
        },
         {
             "Effect": "Allow",
             "Action": [
                 "ssm:TerminateSession",
                 "ssm:ResumeSession"
             ],
             "Resource": [
                 "arn:aws:ssm:*:*:session/${aws:userid}-*"
             ]
         },
         {
          "Effect": "Allow",
          "Action": ["ssmmessages:OpenDataChannel"],
          "Resource": ["arn:aws:ssm:*:*:session/${aws:userid}-*"]
        }
    ]
}
```

例 3: タグに基づいてアクセスを制限

特定のタグに基づいてマネージドノードへのアクセスを制限できます。以下の例では、ノードが財務ウェブサーバー (ssm:resourceTag/Finance: WebServer) であるという条件で、ユーザーは任意のマネージドノード (Resource: arn:aws:ec2:*region*:*987654321098*:instance/*) にセッション (Effect: Allow, Action: ssm:StartSession, ssm:ResumeSession) の開始と再開することが許可されます。ユーザーがタグ付けされていない、またはFinance: WebServer 以外のタグ付けされた　マネージドノードにコマンドを送信した場合、コマンド結果に AccessDenied が含まれます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:StartSession"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-2:123456789012:instance/*"
            ],
            "Condition": {
                "StringLike": {
```

```
                    "ssm:resourceTag/Finance": [
                        "WebServers"
                    ]
                }
            }
        },
        {
         "Effect": "Allow",
         "Action": ["ssmmessages:OpenDataChannel"],
         "Resource": ["arn:aws:ssm:*:*:session/${aws:userid}-*"]
       },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:TerminateSession",
                "ssm:ResumeSession"
            ],
            "Resource": [
                "arn:aws:ssm:*:*:session/${aws:userid}-*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:StartSession"
            ],
            "Resource": [
                "arn:aws:ssm:us-east-2:123456789012:document/SSM-
SessionManagerRunShell"
            ]
        }
    ]
}
```

複数のタグが付いたマネージドノードに対してユーザーがセッションを開始することを許可するIAMポリシーを作成できます。以下のポリシーは、指定されたタグが両方とも適用されたマネージドノードに対してユーザーがセッションを開始することを許可します。ユーザーがこれら両方のタグが付いていないマネージドノードにコマンドを送信した場合、コマンド結果に AccessDenied が含まれます。

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

```
      {
         "Effect":"Allow",
         "Action":[
            "ssm:StartSession"
         ],
         "Resource":"*",
         "Condition":{
            "StringLike":{
               "ssm:resourceTag/tag-key1":[
                  "tag-value1"
               ],
               "ssm:resourceTag/tag-key2":[
                  "tag-value2"
               ]
            }
         }
      },
      {
         "Effect": "Allow",
         "Action": ["ssmmessages:OpenDataChannel"],
         "Resource": ["arn:aws:ssm:*:*:session/${aws:userid}-*"]
       },
      {
            "Effect": "Allow",
            "Action": [
                "ssm:StartSession"
            ],
            "Resource": [
                "arn:aws:ssm:us-east-2:123456789012:document/SSM-
SessionManagerRunShell"
            ]
      }
   ]
}
```

IAM ポリシーの作成の詳細については、「IAM ユーザーガイド」の「マネージドポリシーとインラインポリシー」を参照してください。マネージドノードへのタグ付けの詳細については、「Amazon EC2 ユーザーガイド」(内容は Windows と Linux のマネージドノードに適用) の「Amazon EC2 リソースのタグ付け」を参照してください。マネージドノードで許可されていないルートレベルのコマンドに対するセキュリティ体制の強化方法の詳細については、 SSM Agent を介してルートレベルコマンドへのアクセスを制限する をご参照ください

例 4: ユーザーが開始したセッションのみを終了できるようにする

Session Manager では、AWS アカウント のフェデレーションユーザーがどのセッションを終了できるかを制御するために、2 つの方法を使用できます。

- AWS Identity and Access Management (IAM) アクセス権限ポリシーで変数 `{aws:userid}` を使用します。フェデレーションユーザーは、開始したセッションのみを終了できます。非フェデレーティッドユーザーの場合は、方法 1 を使用します。フェデレーティッドユーザーの場合は、方法 2 を使用します。
- IAM アクセス許可ポリシーで AWS タグによって提供されたタグを使用します。このポリシーには、 によって提供された特定のタグでタグ付けされたセッションのみをユーザーが終了できるようにする条件を含めますAWS この方法は、フェデレーション ID を使用して へのアクセスを許可するものを含めて、すべてのアカウントで機能しますAWS

方法 1: 変数 **`{aws:username}`** を使用して TerminateSession 権限を付与する

次の IAM ポリシーでは、ユーザーはアカウントのすべてのセッションの ID を表示できます。ただし、ユーザーは開始したセッションでのみマネージドノードとインタラクトできます。次のポリシーが割り当てられているユーザーは、他のユーザーのセッションに接続したり、終了させることはできません。ポリシーは、このために変数 `{aws:username}` を使用します。

> **Note**
>
> この方法は、フェデレーション ID を使用して AWS へのアクセスを許可するアカウントでは機能しません。

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

```
        {
            "Action": [
                "ssm:TerminateSession"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:ssm:*:*:session/${aws:username}-*"
            ]
        }
    ]
}
```

方法 2: が提供するタグを使用して TerminateSession 権限を付与するAWS

IAM ポリシーに条件タグキー変数を含めることで、ユーザーが終了できるセッションを管理できます。この条件では、ユーザーがこれらの特定のタグキー変数と指定された値のいずれかまたは両方でタグ付けされたセッションのみを終了できることを指定します。

AWS アカウント のユーザーがセッションを開始すると、Session Manager は 2 つのリソースタグをセッションに適用します。最初のリソースタグは `aws:ssmmessages:target-id` で、ユーザーが終了できるターゲットの ID を指定します。もう 1 つのリソースタグは `aws:ssmmessages:session-id` で、*`role-id`*`:`*`caller-specified-role-name`* 形式の値を持ちます。

> **Note**
>
> Session Manager は、この IAM アクセス制御ポリシーのカスタムタグをサポートしていません。以下に説明する、AWS が提供するリソースタグを使用する必要があります。

`aws:ssmmessages:target-id`

このタグキーでポリシーの値としてマネージドノード ID を含めます。以下のポリシーブロックでは、この条件ステートメントはユーザーが 「i-02573cafcfEXAMPLE」 のノードのみを終了することを許可します。

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

```
            "Effect": "Allow",
            "Action": [
               "ssm:TerminateSession"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "ssm:resourceTag/aws:ssmmessages:target-id": [
                       "i-02573cafcfEXAMPLE"
                    ]
                }
            }
        }
    ]
}
```

この TerminateSession アクセス許可が付与されていないセッションをユーザーが終了しようとすると、AccessDeniedException エラーが発生します。

aws:ssmmessages:session-id

このタグキーには、セッションを開始するリクエストの値として、セッション ID の変数が含まれます。

次の例は、発信者のタイプが User である場合のポリシーを示しています。aws:ssmmessages:session-id に指定する値は、ユーザーの ID です。この例では、AIDIODR4TAW7CSEXAMPLE は AWS アカウント のユーザーの ID を表します。AWS アカウント のユーザーの ID を取得するには、IAM コマンド get-user を使用します。詳細については、IAM ユーザーガイドの「AWS Identity and Access Management」セクションの「get-user」を参照してください 。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
               "ssm:TerminateSession"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "ssm:resourceTag/aws:ssmmessages:session-id": [
```

```
                    "AIDIODR4TAW7CSEXAMPLE"
                ]
            }
        }
    ]
}
```

次の例は、発信者のタイプが AssumedRole である場合のポリシーを示しています。{aws:userid} 変数は、aws:ssmmessages:session-id に指定する値として使用できます。または、aws:ssmmessages:session-id に指定する値としてロール ID をハードコードすることもできます。ロール ID をハードコードする場合は、*role-id*:*caller-specified-role-name* 形式で値を指定する必要があります。例えば、AIDIODR4TAW7CSEXAMPLE:MyRole。

> **Important**
>
> システムタグを適用するには、指定するロール ID には、Unicode 文字、0～9、スペース、_、.、:、/、=、+、-、@、および \ のみを含めることができます。

AWS アカウント のロールのロール ID を取得するには、get-caller-identity コマンドを使用します。詳細については、 AWS CLI コマンドリファレンスの「get-caller-identity」を参照してください。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
               "ssm:TerminateSession"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "ssm:resourceTag/aws:ssmmessages:session-id": [
                       "${aws:userid}*"
                    ]
                }
            }
```

```
        }
    ]
}
```

この TerminateSession アクセス許可が付与されていないセッションをユーザーが終了しようとすると、AccessDeniedException エラーが発生します。

aws:ssmmessages:target-id および aws:ssmmessages:session-id

また、この例に示すように、両方のシステムタグでタグ付けされたセッションをユーザーが終了できるようにする IAM ポリシーを作成することもできます。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "ssm:TerminateSession"
         ],
         "Resource":"*",
         "Condition":{
            "StringLike":{
               "ssm:resourceTag/aws:ssmmessages:target-id":[
                  "i-02573cafcfEXAMPLE"
               ],
               "ssm:resourceTag/aws:ssmmessages:session-id":[
                  "${aws:userid}*"
               ]
            }
         }
      }
   ]
}
```

例 5: すべてのセッションにフル (管理) アクセスを許可する

以下の IAM ポリシーは、すべてのユーザーがすべてのノード用に作成したすべてのマネージドノードとすべてのセッションに対して、ユーザーが完全にインタラクトすることを許可します。組織の Session Manager のアクティビティを完全に制御する必要がある管理者にのみ付与されます。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ssm:StartSession",
                "ssm:TerminateSession",
                "ssm:ResumeSession",
                "ssm:DescribeSessions",
                "ssm:GetConnectionStatus"
            ],
            "Effect": "Allow",
            "Resource": [
                "*"
            ]
        },
        {
         "Effect": "Allow",
         "Action": ["ssmmessages:OpenDataChannel"],
         "Resource": ["arn:aws:ssm:*:*:session/${aws:userid}-*"]
       }
    ]
}
```

ステップ 4: セッション設定を構成する

ご使用の AWS Identity and Access Management (IAM) ポリシーで管理者許可を付与されているユーザーは、次のようなセッション設定を設定できます。

- Linux マネージドノードの場合、Run As サポートを有効にします。これにより、AWS Systems Manager Session Manager がマネージドノード上で作成可能なシステム生成される `ssm-user` アカウントの認証情報の代わりに、指定されたオペレーティングシステムユーザーの認証情報を使用してセッションを開始できるようになります。
- AWS KMS key 暗号化プログラムを使用するように Session Manager を設定し、クライアントマシンとマネージドノード間で送信されるデータの保護を強化します。
- セッション履歴ログを作成し、Amazon Simple Storage Service (Amazon S3) バケットまたは Amazon CloudWatch Logs ロググループに送信するように Session Manager を設定します。保存されたログデータを使用して、マネージドノードに対して確立されたセッション接続と、セッション中にそれらのノード上で実行されたコマンドに関するレポートを作成できます。
- セッションタイムアウトを設定します。この設定を使用して、非アクティブ期間後にセッションを終了するタイミングを指定できます。

- 設定可能なシェルプロファイルを使用するように Session Manager を設定します。これらのカスタマイズ可能なプロファイルを使用すると、シェルの設定、環境変数、作業ディレクトリ、セッション開始時の複数のコマンドの実行など、セッション内の設定をカスタマイズできます。

Session Manager プリファレンスを設定するために必要な許可の詳細については、「the section called “Session Manager の設定を更新するためのユーザーアクセス許可を付与または拒否する”」を参照してください。

トピック

- Session Manager の設定を更新するためのユーザーアクセス許可を付与または拒否する
- アイドルセッションのタイムアウト値を指定します。
- 最大セッション時間の指定
- 設定可能なシェルプロファイルを有効にする
- Linux と macOS のマネージドノードで Run As サポートを有効にする
- セッションデータの KMS キー暗号化を有効にする (コンソール)
- Session Manager プリファレンスドキュメントを作成する (コマンドライン)
- Session Manager 設定の更新 (コマンドライン)

Systems Manager コンソールを使用してセッションデータのログを記録するオプションを設定する方法については、次のトピックを参照してください。

- Amazon S3 を使用してセッションデータを口グ記録する (コンソール)
- Amazon CloudWatch Logs を使用してセッションデータをストリーミングする (コンソール)
- Amazon CloudWatch Logs を使用してセッションデータを口グ記録する (コンソール)

Session Manager の設定を更新するためのユーザーアクセス許可を付与または拒否する

アカウントの設定は、各 AWS リージョン の AWS Systems Manager (SSM) ドキュメントとして保存されます。アカウント内のセッションのアカウント設定を更新するには、その設定が保存されている SSM ドキュメントのタイプにアクセスするために必要なアクセス権限を得ている必要があります。これらのアクセス権限は、AWS Identity and Access Management (IAM) ポリシーによって付与されます。

設定を作成および更新できる管理者ポリシー

管理者は、設定を随時作成して更新するために、次のポリシーを持つことができます。次のポリシーは、us-east-2 アカウント 123456789012 にある SSM-SessionManagerRunShell ドキュメントにアクセスして更新するアクセス許可を許可します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ssm:CreateDocument",
                "ssm:GetDocument",
                "ssm:UpdateDocument",
                "ssm:DeleteDocument"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:ssm:us-east-2:123456789012:document/SSM-
SessionManagerRunShell"
            ]
        }
    ]
}
```

設定が更新されないようにするユーザーポリシー

次のポリシーを使用して、アカウントのエンドユーザーが Session Manager の設定を更新または上書きしないようにします。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ssm:CreateDocument",
                "ssm:GetDocument",
                "ssm:UpdateDocument",
                "ssm:DeleteDocument"
            ],
            "Effect": "Deny",
            "Resource": [
                "arn:aws:ssm:us-east-2:123456789012:document/SSM-
SessionManagerRunShell"
```

```
            ]
        }
    ]
}
```

アイドルセッションのタイムアウト値を指定します。

Session Manager は、システムがセッションを終了する前にユーザーを非アクティブにする時間を指定するための、AWS Systems Manager のツールです。デフォルトでは、セッションは 20 分間非アクティブになった後にタイムアウトします。この設定を変更して、セッションが非アクティブ状態の 1～60 分の間にタイムアウトするように指定できます。一部のコンピューティングセキュリティに関する専門機関は、アイドルセッションのタイムアウトを最大でも 15 分に設定することを推奨しています。

アイドルセッションタイムアウトを有効にするには (コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Session Manager] を選択します。
3. [Preferences (設定)] タブを選択してから、[Edit (編集)] を選択します。
4. [Idle session timeout (アイドルセッションタイムアウト)] の [分] フィールドで、セッションが終了するまでのユーザを非アクティブにする時間を指定します。
5. [Save] を選択します。

最大セッション時間の指定

AWS Systems Manager のツールである Session Manager は、セッションが終了するまでの最大時間を指定すること実現します。デフォルトでは、セッションの最大期間はありません。最大セッション時間に指定する値は、1 から 1,440 分の間である必要があります。

最大セッション時間 (コンソール) の指定方法

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Session Manager] を選択します。
3. [設定] タブを選択してから、[編集] を選択します。
4. 最大セッション時間の有効化の隣のチェックボックスをオンにします。

5. セッションが終了するまでの最大時間を最大セッション時間の下にある [minutes] (分) フィールドで指定します。
6. [Save] を選択します。

設定可能なシェルプロファイルを有効にする

デフォルトでは、Linux 用 EC2 インスタンス上のセッションは Bourne シェル (sh) を使用して開始します。ただし、bash のような別のシェルを使用することを好む人もいます。設定可能なシェルプロファイルを有効にすると、シェルの設定、環境変数、作業ディレクトリ、セッション開始時の複数のコマンドの実行など、セッション内の設定をカスタマイズできます。

> **Important**
>
> Systems Manager は、実行前にインスタンスにどのような変更が加えられるかを確認するために、シェルプロファイル内のコマンドやスクリプトをチェックしません。シェルプロファイルに入力されたコマンドやスクリプトのユーザーによる変更を制限するため、次の操作を推奨します。
>
> - AWS Identity and Access Management (IAM) ユーザーおよびロール用にカスタマイズされたセッションタイプのドキュメントを作成します。次に、これらのユーザーとロールの IAM ポリシーを変更して、`StartSession` API オペレーションがユーザー用に作成したセッションタイプのドキュメントのみを使用できるようにします。詳細については、「Session Manager プリファレンスドキュメントを作成する (コマンドライン)」および「クイックスタート Session Manager のエンドユーザーポリシー」を参照してください。
> - IAM ユーザーおよびロールの IAM ポリシーを変更して、作成するセッションタイプのドキュメントリソースについて `UpdateDocument` API オペレーションへのアクセスを拒否します。これにより、ユーザーとロールは、設定の変更を許可されることなく、作成したドキュメントをセッションの環境設定に使用できます。

設定可能なシェルプロファイルを有効にするには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Session Manager] を選択します。
3. [Preferences (設定)] タブを選択してから、[Edit (編集)] を選択します。

4. 該当するオペレーティングシステムのフィールドで、セッションの開始時に実行する環境変数、シェル環境設定、またはコマンドを指定します。
5. [Save] を選択します。

シェルプロファイルに追加できるコマンドの例を次に示します。

Linux インスタンスで bash シェルに移動し、/usr ディレクトリに移動します。

```
exec /bin/bash
cd /usr
```

セッションの開始時にタイムスタンプと「ようこそ」メッセージを出力します。

Linux & macOS

```
timestamp=$(date '+%Y-%m-%dT%H:%M:%SZ')
user=$(whoami)
echo $timestamp && echo "Welcome $user"'!'
echo "You have logged in to a production instance. Note that all session activity is
 being logged."
```

Windows

```
$timestamp = (Get-Date).ToString("yyyy-MM-ddTH:mm:ssZ")
$splitName = (whoami).Split("\")
$user = $splitName[1]
Write-Host $timestamp
Write-Host "Welcome $user!"
Write-Host "You have logged in to a production instance. Note that all session
 activity is being logged."
```

セッション開始時の動的システムアクティビティを表示します。

Linux & macOS

```
top
```

Windows

```
while ($true) { Get-Process | Sort-Object -Descending CPU | Select-Object -First 30;
 `
Start-Sleep -Seconds 2; cls
Write-Host "Handles  NPM(K)    PM(K)      WS(K) VM(M)   CPU(s)     Id ProcessName";
Write-Host "-------  ------    -----      ----- -----   ------     -- -----------"}
```

Linux と macOS のマネージドノードで Run As サポートを有効にする

デフォルトでは、Session Manager がマネージドノード上でシステムによって生成された `ssm-user` アカウントの認証情報を使用して接続を認証します。(Linux および macOS マシンでは、このアカウントは `/etc/sudoers/` に追加されます)。必要に応じて、代わりにオペレーティングシステム (OS) ユーザーアカウントの認証情報、または Active Directory に参加しているインスタンスのドメインユーザーの認証情報を使用してセッションを認証することもできます。この場合、Session Manager は、セッションを開始する前に、指定した OS アカウントがノードまたはドメイン内に存在することを確認します。ノードまたはドメイン内に存在しない OS アカウントを使用してセッションを開始しようとすると、接続に失敗します。

> **Note**
>
> Session Manager では、オペレーティングシステムの `root` ユーザーアカウントを使用して接続を認証することはできません。OS ユーザーアカウントを使用して認証されるセッションでは、ログイン制限やシステムリソースの使用制限など、ノードの OS レベルのポリシーやディレクトリのポリシーが適用されない場合があります。

仕組み

セッションの Run As サポートを有効にすると、システムによってアクセス許可が次のように確認されます。

1. セッションを開始しているユーザーである場合、IAM エンティティ (ユーザーまたはロール) に `SSMSessionRunAs = os user account name` タグが付いていますか?

   「はい」の場合、マネージドノードに OS ユーザー名が存在していますか? 存在する場合は、セッションを開始します。存在しない場合は、セッションの開始を許可しないでください。

IAM エンティティに `SSMSessionRunAs = os user account name` タグが付いていない場合は、ステップ 2 に進みます。

2. IAM エンティティに `SSMSessionRunAs = os user account name` タグが付いていない場合、AWS アカウント の Session Manager の詳細設定で OS ユーザー名が指定されていますか?

   「はい」の場合、マネージドノードに OS ユーザー名が存在していますか? 存在する場合は、セッションを開始します。存在しない場合は、セッションの開始を許可しないでください。

> **Note**
>
> Run As サポートを有効にすると、Session Manager がマネージドノードの `ssm-user` アカウントを使用してセッションを開始することができなくなります。つまり、Session Manager が、指定された OS ユーザーアカウントを使用して接続に失敗しても、デフォルトの方法を使用した接続にはフォールバックしません。
> OS アカウントを指定したり、IAM エンティティをタグ付けしたりせずに Run As をアクティブ化し、Session Manager の詳細設定で OS アカウントを指定していない場合、セッション接続は失敗します。

Linux と macOS のマネージドノードで Run As サポートを有効にするには

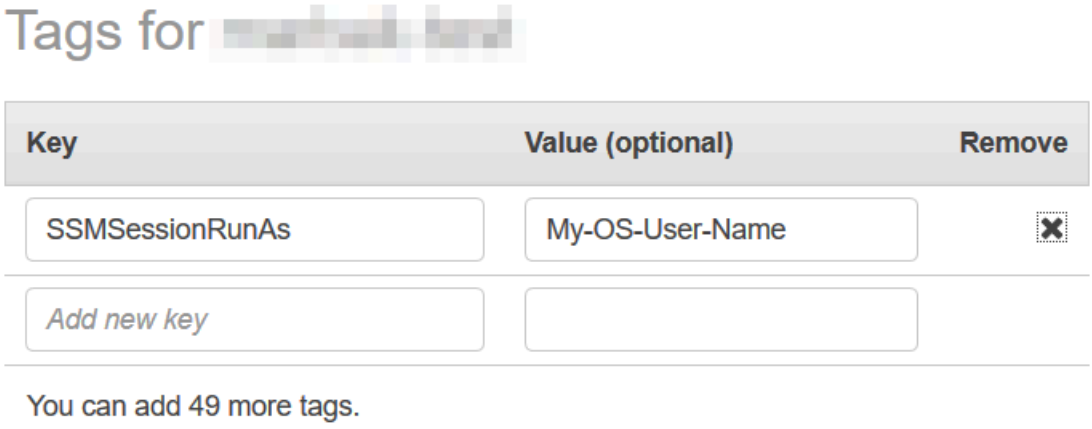
1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Session Manager] を選択します。
3. [設定] タブを選択してから、[編集] を選択します。
4. [Linux インスタンスの Run As サポートを有効にする] の横にあるチェックボックスをオンにします。
5. 次のいずれかを行います :

   - [オプション 1]: [オペレーティングシステムのユーザー名] フィールドに、セッション開始時に使用する OS ユーザーアカウント名を入力します。このオプションを使用すると、Session Manager を使用して接続する AWS アカウント 内のすべてのユーザーに対して、すべてのセッションが同じ OS ユーザーによって実行されます。
   - [オプション 2] (推奨事項): [IAM コンソールを開く] リンクを選択します。ナビゲーションペインで、[ユーザー] または [ロール] を選択します。タグを追加するエンティティ (ユーザーまた

はロール) を選択し、[タグ] タブを選択します。キー名に「SSMSessionRunAs」と入力します。キー値に対応する OS ユーザーアカウント名を入力します。[Save changes] (変更の保存) をクリックします。

このオプションを使用すると、必要に応じて、さまざまな IAM エンティティに固有の OS ユーザーを指定できます。IAM エンティティ (ユーザーまたはロール) のタグ付けの詳細については、「IAM ユーザーガイド」の「IAM リソースのタグ付け」を参照してください。

以下に例を示します。



6. [保存] を選択します。

セッションデータの KMS キー暗号化を有効にする (コンソール)

AWS Key Management Service (AWS KMS)を使用して暗号化キーを作成および管理します。AWS KMS では、幅広い AWS のサービスおよびアプリケーションでの暗号化の使用を制御できます。マネーマネージドノードと AWS アカウント 内のユーザーのローカルマシン間で送信されるセッションデータが、KMS キー暗号化プログラムで暗号化されることを指定できます。(これは AWS が既にデフォルトで提供している TLS 1.2/1.3 暗号化に追加されています)。Session Manager セッションデータを暗号化するには、AWS KMS を使用して対称 KMS キーを作成します。

AWS KMS 暗号化は Standard_Stream、InteractiveCommands、NonInteractiveCommands セッションタイプで使用できます。AWS KMS で作成したキーでセッションデータを暗号化するオプションを使用する場合、AWS Systems Manager SSM Agent におけるバージョンが 2.3.539.0 以降がマネージドノードにインストールされている必要があります。

> **Note**
>
> AWS Systems Manager コンソールからマネージドノードのパスワードをリセットするため、AWS KMS 暗号化を有効にする必要があります。詳細については、「マネージドノードでパスワードをリセットする」を参照してください。

に作成したキーを使用できますAWS アカウント また、別の で作成されたキーを使用することもできますAWS アカウント 別の AWS アカウント でのキーの作成者はキーを使用するために必要なアクセス許可をユーザーに提供する必要があります。

セッションデータの KMS キー暗号化を有効にすると、セッションを開始するユーザーとそのユーザーが接続するマネージドノードの両方が、キーを使用する許可が必要になります。AWS Identity and Access Management (IAM) ポリシーを使用して、Session Manager で KMS キーを使用するアクセス許可を付与します。詳細については、以下のトピックを参照してください。

- アカウント内のユーザーに AWS KMS アクセス権限を追加します: Session Manager のサンプル IAM ポリシー。
- アカウント内のマネージドノードに AWS KMS 権限を追加します: ステップ 2: Session Manager のインスタンスのアクセス権限の確認または追加。

KMS キーの作成と管理の詳細については、AWS Key Management Service デベロッパーガイドを参照してください。

AWS CLI を使用してアカウントのセッションデータの KMS キー暗号化を有効にする方法については、「Session Manager 設定の更新 (コマンドライン)」または「Session Manager プリファレンスドキュメントを作成する (コマンドライン)」を参照してください。

> **Note**
>
> KMS キーの使用には料金が発生します。詳細については、「AWS Key Management Service の料金表」を参照してください。

セッションデータの KMS キー暗号化を有効にするには (コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。

2. ナビゲーションペインで、[Session Manager] を選択します。
3. [設定] タブを選択してから、[編集] を選択します。
4. KMS 暗号化を有効にするの隣のチェックボックスをオンにします。
5. 次のいずれかを行います。

   - [現在のアカウントの KMS キーを選択] の横にあるボタンを選択して、リストからキーを選択します。

     -または-

     [KMS キーエイリアスまたはKMS キー ARN の入力] の横のボタンをクリックします。現在のアカウントで作成されたキーの KMS キーエイリアスを手動で入力するか、別のアカウントのキーのキー Amazon リソースネーム (ARN) を入力します。次に例を示します。

     - キーエイリアス: `alias/my-kms-key-alias`
     - キー ARN: `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-12345EXAMPLE`

     -または-

     [Create new key] (新しいキーを作成) を選択して、アカウントに新しい KMS キーを作成します。新しいキーを作成した後、[Preferences (設定)] タブに戻り、アカウントのセッションデータを暗号化するためのキーを選択します。

   キーの共有の詳細については、AWS Key Management Service デベロッパーガイドの外部 AWS アカウント のキーへのアクセスの許可を参照してください。
6. [Save] を選択します。

Session Manager プリファレンスドキュメントを作成する (コマンドライン)

次の手順を使用して、AWS Systems Manager Session Manager セッションのプリファレンスを定義する SSM ドキュメントを作成します。このドキュメントを使用して、データ暗号化、セッション期間、ログ記録などのセッションオプションを設定できます。例えば、Amazon Simple Storage Service (Amazon S3) バケットまたは Amazon CloudWatch Logs ロググループにセッションログデータを格納するかどうかを指定します。AWS アカウント および AWS リージョン のすべてのセッションの一般的なプリファレンスを定義するドキュメントや、個々のセッションのプリファレンスを定義するドキュメントを作成できます。

> **Note**
>
> Session Manager コンソールを使用して、一般的なセッション設定を設定することもできます。

Session Manager プリファレンスの設定に使用するドキュメントには、`Standard_Stream` の `sessionType` が付いている必要があります。これらの Session ドキュメントの詳細については、「the section called “セッションドキュメントスキーマ”」を参照してください。

コマンドラインを使用して既存の Session Manager 設定を更新する方法については、「Session Manager 設定の更新 (コマンドライン)」を参照してください。

AWS CloudFormation を使用してセッション設定を作成する方法の例については、AWS CloudFormationユーザーガイドで「Session Manager の設定向けに Systems Manager ドキュメントを作成する」を参照してください。

> **Note**
>
> この手順では、AWS アカウント レベルで Session Manager プリファレンスを設定するためのドキュメントを作成する方法について説明します。セッションレベルのプリファレンスの設定に使用されるドキュメントを作成するには、ファイル名関連のコマンド入力に `SSM-SessionManagerRunShell` 以外の値を指定します。
> ドキュメントを使用して AWS Command Line Interface (AWS CLI) から開始されるセッションのプリファレンスを設定するには、`--document-name` パラメータ値としてドキュメント名を指定します。Session Manager コンソールから開始したセッションのプリファレンスを設定するには、ドキュメントの名前を入力するか、リストから選択します。

Session Manager 設定を作成するには (コマンドライン)

1. `SessionManagerRunShell.json` などの名前でローカルマシンに JSON ファイルを作成し、次の内容を貼り付けます。

```
{
    "schemaVersion": "1.0",
    "description": "Document to hold regional settings for Session Manager",
    "sessionType": "Standard_Stream",
    "inputs": {
```

```
        "s3BucketName": "",
        "s3KeyPrefix": "",
        "s3EncryptionEnabled": true,
        "cloudWatchLogGroupName": "",
        "cloudWatchEncryptionEnabled": true,
        "cloudWatchStreamingEnabled": false,
        "kmsKeyId": "",
        "runAsEnabled": false,
        "runAsDefaultUser": "",
        "idleSessionTimeout": "",
        "maxSessionDuration": "",
        "shellProfile": {
            "windows": "date",
            "linux": "pwd;ls"
        }
    }
}
```

次の例に示すように、値をハードコーディングするのではなく、パラメータを使用してセッション設定に値を渡すこともできます。

```
{
   "schemaVersion":"1.0",
   "description":"Session Document Parameter Example JSON Template",
   "sessionType":"Standard_Stream",
   "parameters":{
      "s3BucketName":{
         "type":"String",
         "default":""
      },
      "s3KeyPrefix":{
         "type":"String",
         "default":""
      },
      "s3EncryptionEnabled":{
         "type":"Boolean",
         "default":"false"
      },
      "cloudWatchLogGroupName":{
         "type":"String",
         "default":""
      },
      "cloudWatchEncryptionEnabled":{
```

```
         "type":"Boolean",
         "default":"false"
      }
   },
   "inputs":{
      "s3BucketName":"{{s3BucketName}}",
      "s3KeyPrefix":"{{s3KeyPrefix}}",
      "s3EncryptionEnabled":"{{s3EncryptionEnabled}}",
      "cloudWatchLogGroupName":"{{cloudWatchLogGroupName}}",
      "cloudWatchEncryptionEnabled":"{{cloudWatchEncryptionEnabled}}",
      "kmsKeyId":""
   }
}
```

2. セッションデータを送信する場所を指定します。(オプションでプレフィックスが付いた) S3 バケット名または CloudWatch Logs ロググループ名を指定することができます。ローカルクライアントとマネージドノード間でデータをさらに暗号化する場合、暗号化に使用する KMS キーを指定します。次に例を示します。

```
{
  "schemaVersion": "1.0",
  "description": "Document to hold regional settings for Session Manager",
  "sessionType": "Standard_Stream",
  "inputs": {
    "s3BucketName": "amzn-s3-demo-bucket",
    "s3KeyPrefix": "MyS3Prefix",
    "s3EncryptionEnabled": true,
    "cloudWatchLogGroupName": "MyLogGroupName",
    "cloudWatchEncryptionEnabled": true,
    "cloudWatchStreamingEnabled": false,
    "kmsKeyId": "MyKMSKeyID",
    "runAsEnabled": true,
    "runAsDefaultUser": "MyDefaultRunAsUser",
    "idleSessionTimeout": "20",
    "maxSessionDuration": "60",
    "shellProfile": {
        "windows": "MyCommands",
        "linux": "MyCommands"
    }
  }
}
```

> **Note**
>
> セッションログデータを暗号化しない場合は、`s3EncryptionEnabled` の「`true`」を「`false`」に変更します。
> Amazon S3 バケットまたは CloudWatch Logs ロググループにログを送信しない場合、アクティブなセッションデータを暗号化しない場合、またはアカウントのセッションの Run As サポートを有効にしない場合は、それらのオプション用に次の行を削除できます。「`inputs`」セクションの最後の行がカンマで終わっていないことを確認してください。
> セッションデータを暗号化するために KMS キー ID を追加する場合、セッションを開始するユーザーとそのユーザーが接続するマネージドノードの両方が、キーを使用する許可が必要になります。IAM ポリシーを通して Session Manager で KMS キーを使用するアクセス許可を付与します。詳細については、以下のトピックを参照してください。
>
> - アカウント内のユーザーに AWS KMS アクセス権限を追加します: Session Manager のサンプル IAM ポリシー
> - アカウント内のマネージドノードに AWS KMS 権限を追加します: ステップ 2: Session Manager のインスタンスのアクセス権限の確認または追加。

3. ファイルを保存します。
4. JSON ファイルを作成したディレクトリで、次のコマンドを実行します。

   Linux & macOS

   ```
   aws ssm create-document \
       --name SSM-SessionManagerRunShell \
       --content "file://SessionManagerRunShell.json" \
       --document-type "Session" \
       --document-format JSON
   ```

   Windows

   ```
   aws ssm create-document ^
       --name SSM-SessionManagerRunShell ^
       --content "file://SessionManagerRunShell.json" ^
       --document-type "Session" ^
       --document-format JSON
   ```

PowerShell

```
New-SSMDocument `
    -Name "SSM-SessionManagerRunShell" `
    -Content (Get-Content -Raw SessionManagerRunShell.json) `
    -DocumentType "Session" `
    -DocumentFormat JSON
```

成功すると、コマンドは以下のような出力を返します。

```
{
    "DocumentDescription": {
        "Status": "Creating",
        "Hash": "ce4fd0a2ab9b0fae759004ba603174c3ec2231f21a81db8690a33eb66EXAMPLE",
        "Name": "SSM-SessionManagerRunShell",
        "Tags": [],
        "DocumentType": "Session",
        "PlatformTypes": [
            "Windows",
            "Linux"
        ],
        "DocumentVersion": "1",
        "HashType": "Sha256",
        "CreatedDate": 1547750660.918,
        "Owner": "111122223333",
        "SchemaVersion": "1.0",
        "DefaultVersion": "1",
        "DocumentFormat": "JSON",
        "LatestVersion": "1"
    }
}
```

Session Manager 設定の更新 (コマンドライン)

以下の手順では、好みのコマンドラインツールを使用して、選択した AWS リージョン で AWS アカウント の AWS Systems Manager Session Manager 設定を変更する方法を説明します。Session Manager の設定を用いて、Amazon Simple Storage Service (Amazon S3) バケットまたは Amazon CloudWatch Logs ロググループにセッションデータを記録するためのオプションを指定します。Session Manager 設定を使用して、セッションデータを暗号化することもできます。

Session Manager 設定を更新するには (コマンドライン)

1. SessionManagerRunShell.json などの名前でローカルマシンに JSON ファイルを作成し、次の内容を貼り付けます。

```
{
    "schemaVersion": "1.0",
    "description": "Document to hold regional settings for Session Manager",
    "sessionType": "Standard_Stream",
    "inputs": {
        "s3BucketName": "",
        "s3KeyPrefix": "",
        "s3EncryptionEnabled": true,
        "cloudWatchLogGroupName": "",
        "cloudWatchEncryptionEnabled": true,
        "cloudWatchStreamingEnabled": false,
        "kmsKeyId": "",
        "runAsEnabled": true,
        "runAsDefaultUser": "",
        "idleSessionTimeout": "",
        "maxSessionDuration": "",
        "shellProfile": {
            "windows": "date",
            "linux": "pwd;ls"
        }
    }
}
```

2. セッションデータを送信する場所を指定します。(オプションでプレフィックスが付いた) S3 バケット名または CloudWatch Logs ロググループ名を指定することができます。ローカルクライアントとマネージドノード間でデータをさらに暗号化する場合、暗号化に使用する AWS KMS key キーを指定します。次に例を示します。

```
{
  "schemaVersion": "1.0",
  "description": "Document to hold regional settings for Session Manager",
  "sessionType": "Standard_Stream",
  "inputs": {
    "s3BucketName": "amzn-s3-demo-bucket",
    "s3KeyPrefix": "MyS3Prefix",
    "s3EncryptionEnabled": true,
    "cloudWatchLogGroupName": "MyLogGroupName",
```

```
    "cloudWatchEncryptionEnabled": true,
    "cloudWatchStreamingEnabled": false,
    "kmsKeyId": "MyKMSKeyID",
    "runAsEnabled": true,
    "runAsDefaultUser": "MyDefaultRunAsUser",
    "idleSessionTimeout": "20",
    "maxSessionDuration": "60",
    "shellProfile": {
        "windows": "MyCommands",
        "linux": "MyCommands"
    }
  }
}
```

> **Note**
>
> セッションログデータを暗号化しない場合は、s3EncryptionEnabled の「true」を「false」に変更します。
> Amazon S3 バケットまたは CloudWatch Logs ロググループにログを送信しない場合、アクティブなセッションデータを暗号化しない場合、またはアカウントのセッションの Run As サポートを有効にしない場合は、それらのオプション用に次の行を削除できます。「inputs」セクションの最後の行がカンマで終わっていないことを確認してください。
> セッションデータを暗号化するために KMS キー ID を追加する場合、セッションを開始するユーザーとそのユーザーが接続するマネージドノードの両方が、キーを使用する許可が必要になります。AWS Identity and Access Management (IAM) ポリシーを使用して、Session Manager で KMS キーを使用するアクセス許可を付与します。詳細については、以下のトピックを参照してください。
>
> - アカウント内のユーザーに AWS KMS アクセス権限を追加します: Session Manager のサンプル IAM ポリシー。
> - アカウント内のマネージドノードに AWS KMS 権限を追加します: ステップ 2: Session Manager のインスタンスのアクセス権限の確認または追加。

3. ファイルを保存します。
4. JSON ファイルを作成したディレクトリで、次のコマンドを実行します。

Linux & macOS

```
aws ssm update-document \
    --name "SSM-SessionManagerRunShell" \
    --content "file://SessionManagerRunShell.json" \
    --document-version "\$LATEST"
```

Windows

```
aws ssm update-document ^
    --name "SSM-SessionManagerRunShell" ^
    --content "file://SessionManagerRunShell.json" ^
    --document-version "$LATEST"
```

PowerShell

```
Update-SSMDocument `
    -Name "SSM-SessionManagerRunShell" `
    -Content (Get-Content -Raw SessionManagerRunShell.json) `
    -DocumentVersion '$LATEST'
```

成功すると、コマンドは以下のような出力を返します。

```
{
    "DocumentDescription": {
        "Status": "Updating",
        "Hash": "ce4fd0a2ab9b0fae759004ba603174c3ec2231f21a81db8690a33eb66EXAMPLE",
        "Name": "SSM-SessionManagerRunShell",
        "Tags": [],
        "DocumentType": "Session",
        "PlatformTypes": [
            "Windows",
            "Linux"
        ],
        "DocumentVersion": "2",
        "HashType": "Sha256",
        "CreatedDate": 1537206341.565,
        "Owner": "111122223333",
        "SchemaVersion": "1.0",
        "DefaultVersion": "1",
```

```
        "DocumentFormat": "JSON",
        "LatestVersion": "2"
    }
}
```

ステップ 5: (オプション) セッションでのコマンドへのアクセスを制限する

カスタム Session タイプの AWS Systems Manager (SSM) ドキュメントを使用すると、AWS Systems Manager Session Manager セッションでユーザーが実行できるコマンドを制限できます。ドキュメントでは、ユーザーがセッションを開始したときに実行されるコマンド、およびユーザーがコマンドに指定できるパラメータを定義します。Session ドキュメントの schemaVersion は 1.0 であり、sessionType は InteractiveCommands であることが必要です。その後、お客様が定義した Session ドキュメントのみへのアクセスをユーザーに許可する AWS Identity and Access Management (IAM) ポリシーを作成できます。IAM ポリシーを使用してセッションでのコマンドへのアクセスを制限する方法の詳細については、「対話型コマンドの IAM ポリシーの例」を参照してください。

InteractiveCommands の sessionType を持つドキュメントは、AWS Command Line Interface (AWS CLI) から開始されたセッションでのみサポートされます。ユーザーはカスタムドキュメント名を --document-name パラメータ値として指定し、--parameters オプションを使用して任意のコマンドパラメータ値を指定します。対話型コマンドの実行の詳細については、「セッションの開始 (対話形式と非対話形式のコマンド)」を参照してください。

ユーザーに実行を許可するコマンドを定義するカスタムの Session タイプの SSM ドキュメントを作成するには以下の手順を使用します。

セッションでコマンドへのアクセスを制限する (コンソール)

Session Manager セッションでユーザーが実行できるコマンドを制限するには (コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[ドキュメント] を選択します。
3. [Create command or session (コマンドまたはセッションの作成)] を選択します。
4. [名前] に、ドキュメントのわかりやすい名前を入力します。
5. [Document type (ドキュメントタイプ)] で、[Session document (セッションドキュメント)] を選択します。

6. 以下の例に示すように、JSON または YAML を使用して、Session Manager セッションでユーザーが実行できるコマンドを定義するドキュメントコンテンツを入力します。

   YAML

```
---
schemaVersion: '1.0'
description: Document to view a log file on a Linux instance
sessionType: InteractiveCommands
parameters:
  logpath:
    type: String
    description: The log file path to read.
    default: "/var/log/amazon/ssm/amazon-ssm-agent.log"
    allowedPattern: "^[a-zA-Z0-9-_/]+(.log)$"
properties:
  linux:
    commands: "tail -f {{ logpath }}"
    runAsElevated: true
```

   JSON

```
{
    "schemaVersion": "1.0",
    "description": "Document to view a log file on a Linux instance",
    "sessionType": "InteractiveCommands",
    "parameters": {
        "logpath": {
            "type": "String",
            "description": "The log file path to read.",
            "default": "/var/log/amazon/ssm/amazon-ssm-agent.log",
            "allowedPattern": "^[a-zA-Z0-9-_/]+(.log)$"
        }
    },
    "properties": {
        "linux": {
            "commands": "tail -f {{ logpath }}",
            "runAsElevated": true
        }
    }
}
```

7. [Create document] を選択します。

セッションでコマンドへのアクセスを制限する (コマンドライン)

開始する前に

まだ AWS Command Line Interface (AWS CLI) または AWS Tools for PowerShell をインストールして設定していない場合は、インストールして設定します。詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」および「AWS Tools for PowerShell のインストール」を参照してください。

Session Manager セッションでユーザーが実行できるコマンドを制限するには (コマンドライン)

1. 以下の例に示すように、Session Manager セッションでユーザーが実行できるコマンドを定義するドキュメントコンテンツの JSON または YAML ファイルを作成します。

   YAML

```
---
schemaVersion: '1.0'
description: Document to view a log file on a Linux instance
sessionType: InteractiveCommands
parameters:
  logpath:
    type: String
    description: The log file path to read.
    default: "/var/log/amazon/ssm/amazon-ssm-agent.log"
    allowedPattern: "^[a-zA-Z0-9-_/]+(.log)$"
properties:
  linux:
    commands: "tail -f {{ logpath }}"
    runAsElevated: true
```

   JSON

```
{
    "schemaVersion": "1.0",
    "description": "Document to view a log file on a Linux instance",
    "sessionType": "InteractiveCommands",
    "parameters": {
        "logpath": {
            "type": "String",
            "description": "The log file path to read.",
            "default": "/var/log/amazon/ssm/amazon-ssm-agent.log",
```

```
            "allowedPattern": "^[a-zA-Z0-9-_/]+(.log)$"
        }
    },
    "properties": {
        "linux": {
            "commands": "tail -f {{ logpath }}",
            "runAsElevated": true
        }
    }
}
```

2. 以下のコマンドを実行して、Session Manager セッションでユーザーが実行できるコマンドを定義するコンテンツから、SSM ドキュメントを作成します。

   Linux & macOS

   ```
   aws ssm create-document \
       --content file://path/to/file/documentContent.json \
       --name "exampleAllowedSessionDocument" \
       --document-type "Session"
   ```

   Windows

   ```
   aws ssm create-document ^
       --content file://C:\path\to\file\documentContent.json ^
       --name "exampleAllowedSessionDocument" ^
       --document-type "Session"
   ```

   PowerShell

   ```
   $json = Get-Content -Path "C:\path\to\file\documentContent.json" | Out-String
   New-SSMDocument `
       -Content $json `
       -Name "exampleAllowedSessionDocument" `
       -DocumentType "Session"
   ```

対話型コマンドパラメータと AWS CLI

AWS CLI を使用する際、対話型のコマンドパラメータを指定する方法はさまざまあります。AWS CLI でマネージドノードに接続する際に使用するクライアントマシンのオペレーティングシステム (OS) によっては、特殊またはエスケープ記号を含むコマンドの構文が異なる場合があります。次の

例は、AWS CLI の使用時にコマンドパラメータを指定する方法と、特殊文字またはエスケープ文字の処理方法を示しています。

Parameter Store に保存されたパラメータは、次の例に示すように、 コマンドパラメータの AWS CLI で参照できます。

Linux & macOS

```
aws ssm start-session \
    --target instance-id \
    --document-name MyInteractiveCommandDocument \
    --parameters '{"command":["{{ssm:mycommand}}"]}'
```

Windows

```
aws ssm start-session ^
    --target instance-id ^
    --document-name MyInteractiveCommandDocument ^
    --parameters '{"command":["{{ssm:mycommand}}"]}'
```

次の例は、AWS CLI で省略形構文を使用してパラメータを渡す方法を示しています。

Linux & macOS

```
aws ssm start-session \
    --target instance-id \
    --document-name MyInteractiveCommandDocument \
    --parameters command="ifconfig"
```

Windows

```
aws ssm start-session ^
    --target instance-id ^
    --document-name MyInteractiveCommandDocument ^
    --parameters command="ipconfig"
```

次の例に示すように、JSONでパラメータを指定することもできます。

Linux & macOS

```
aws ssm start-session \
    --target instance-id \
    --document-name MyInteractiveCommandDocument \
    --parameters '{"command":["ifconfig"]}'
```

Windows

```
aws ssm start-session ^
    --target instance-id ^
    --document-name MyInteractiveCommandDocument ^
    --parameters '{"command":["ipconfig"]}'
```

次の例に示すように、パラメータを JSON ファイルに格納し、AWS CLI に提供することもできます。ファイルから AWS CLI パラメータを使用する方法の詳細については、AWS Command Line Interface ユーザーガイドの「ファイルから AWS CLI パラメータをロードする」を参照してください。

```
{
    "command": [
        "my command"
    ]
}
```

Linux & macOS

```
aws ssm start-session \
    --target instance-id \
    --document-name MyInteractiveCommandDocument \
    --parameters file://complete/path/to/file/parameters.json
```

Windows

```
aws ssm start-session ^
    --target instance-id ^
    --document-name MyInteractiveCommandDocument ^
    --parameters file://complete/path/to/file/parameters.json
```

次の例に示すように、JSON 入力ファイルから AWS CLI スケルトンを生成することもできます。JSON 入力ファイルから AWS CLI スケルトンを生成する方法の詳細については、AWS Command Line Interface ユーザーガイドの「JSON または YAML 入力ファイルから AWS CLI スケルトンと入力パラメータを生成する」を参照してください。

```
{
    "Target": "instance-id",
    "DocumentName": "MyInteractiveCommandDocument",
    "Parameters": {
        "command": [
            "my command"
        ]
    }
}
```

Linux & macOS

```
aws ssm start-session \
    --cli-input-json file://complete/path/to/file/parameters.json
```

Windows

```
aws ssm start-session ^
    --cli-input-json file://complete/path/to/file/parameters.json
```

引用符で囲まれた文字をエスケープするには、次の例に示すように、エスケープ文字にバックスラッシュを追加する必要があります。

Linux & macOS

```
aws ssm start-session \
    --target instance-id \
    --document-name MyInteractiveCommandDocument \
    --parameters '{"command":["printf \"abc\\\\tdef\""]}'
```

Windows

```
aws ssm start-session ^
    --target instance-id ^
    --document-name MyInteractiveCommandDocument ^
```

```
    --parameters '{"command":["printf \"abc\\\\tdef\""]}'
```

AWS CLI のコマンドパラメータで引用符を使用する方法については、AWS Command Line Interface ユーザーガイドの「AWS CLI の文字列で引用符を使用する」を参照してください。

対話型コマンドの IAM ポリシーの例

お客様が定義した Session ドキュメントのみへのアクセスをユーザーに許可する IAM ポリシーを作成できます。これにより、Session Manager セッションでユーザーが実行できるコマンドは、カスタムの Session タイプの SSM ドキュメントで定義されたコマンドのみに制限されます。

ユーザーに対して 1 つのマネージドノードに 1 つの対話コマンドの実行を許可

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":"ssm:StartSession",
         "Resource":[
            "arn:aws:ec2:region:987654321098:instance/i-02573cafcfEXAMPLE",
            "arn:aws:ssm:region:987654321098:document/exampleAllowedSessionDocument"
         ]
      }
   ]
},
{
         "Effect": "Allow",
         "Action": ["ssmmessages:OpenDataChannel"],
         "Resource": ["arn:aws:ssm:*:*:session/${aws:userid}-*"]
       }
```

ユーザーに対してすべてのマネージドノードに 1 つの対話コマンドの実行を許可

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":"ssm:StartSession",
         "Resource":[
            "arn:aws:ec2:us-west-2:987654321098:instance/*",
```

```
            "arn:aws:ssm:us-
west-2:987654321098:document/exampleAllowedSessionDocument"
         ]
      }
   ]
},
{
         "Effect": "Allow",
         "Action": ["ssmmessages:OpenDataChannel"],
         "Resource": ["arn:aws:ssm:*:*:session/${aws:userid}-*"]
       }
```

ユーザーに対してすべてのマネージドノードに複数の対話コマンドの実行を許可

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":"ssm:StartSession",
         "Resource":[
            "arn:aws:ec2:us-west-2:987654321098:instance/*",
            "arn:aws:ssm:us-
west-2:987654321098:document/exampleAllowedSessionDocument",
            "arn:aws:ssm:us-
west-2:987654321098:document/exampleAllowedSessionDocument2"
         ]
      }
   ]
},
{
         "Effect": "Allow",
         "Action": ["ssmmessages:OpenDataChannel"],
         "Resource": ["arn:aws:ssm:*:*:session/${aws:userid}-*"]
       }
```

ステップ 6: (オプション) AWS PrivateLink を使用して Session Manager の VPC エンドポイントを設定する

インターフェイス Virtual Private Cloud (VPC) エンドポイントを使用するように AWS Systems Manager を設定することにより、マネージドノードのセキュリティ体制をさら改善することができます。インターフェースエンドポイントは、プライベート IP アドレスを使用して Amazon Elastic

Compute Cloud (Amazon EC2) および Systems Manager API にプライベートにアクセスできるテクノロジーである AWS PrivateLink を使用しています。

AWS PrivateLink はマネージドノード、Systems Manager、Amazon EC2 とAmazon ネットワーク間のすべてのネットワークトラフィックに制限します。(マネージドノードはインターネットへアクセスできません) また、インターネットゲートウェイ、NAT デバイスあるいは仮想プライベートゲートウェイの必要はありません。

VPC エンドポイントの作成については、詳細については、「Systems Manager のために VPC エンドポイントを使用して EC2 インスタンスのセキュリティを強化する」を参照してください。

VPC エンドポイントを使用する代わりに、マネージドノードにアウトバウンド・インターネットアクセスを許可することができます。この場合、マネージドノードは、以下のエンドポイントに HTTPS (ポート 443) アウトバウンドトラフィックも許可する必要があります:

- `ec2messages.region.amazonaws.com`
- `ssm.region.amazonaws.com`
- `ssmmessages.region.amazonaws.com`

Systems Manager は、これらのエンドポイント `ssmmessages.region.amazonaws.com` の最後を使用して、SSM Agent からクラウド上の Session Manager サービスを呼び出します。

AWS Key Management Service (AWS KMS) 暗号化のようなオプション機能を使用、Amazon CloudWatch Logs (CloudWatch Logs) へログをストリーミング、 Amazon Simple Storage Service (Amazon S3) へログを送信する場合、以下のエンドポイントに HTTPS (ポート 443) アウトバウンドトラフィックも許可する必要があります:

- `kms.region.amazonaws.com`
- `logs.region.amazonaws.com`
- `s3.region.amazonaws.com`

Systems Manager に必要なエンドポイントの詳細については、「リファレンス: ec2messages、ssmmessages およびその他の API オペレーション」を参照してください。

ステップ 7: (オプション) ssm-user アカウントの管理アクセス許可を有効または無効にする

AWS Systems Manager SSM Agent のバージョン 2.3.50.0 以降では、エージェントは `ssm-user` という名前のローカルユーザーアカウントを作成し、`/etc/sudoers` (Linux および macOS) または

管理者グループ (Windows) に追加します。2.3.612.0 より前のエージェントバージョンでは、アカウントはインストール後に SSM Agent が最初に起動または再起動するときに作成されます。バージョン 2.3.612.0 以降の場合、`ssm-user` アカウントはノード上でセッションが最初に開始されたときに作成されます。この `ssm-user` は、AWS Systems Manager Session Manager セッションが開始された時のデフォルトオペレーティングシステム (OS) ユーザーです。SSM Agent のバージョン 2.3.612.0 は 2019 年 5 月 8 日にリリースされました。

Session Manager ユーザーがノード上で管理コマンドを実行できないようにする場合、`ssm-user` アカウントの許可を更新できます。これらのアクセス許可は、削除した後で復元することもできます。

トピック

- Linux と macOS で ssm-user sudo アカウントの許可を管理する
- Windows Server で ssm-user の管理者アカウントのアクセス許可を管理する

Linux と macOS で ssm-user sudo アカウントの許可を管理する

Linux と macOS のマネージドノードで ssm-user アカウントの sudo 許可を有効または無効にする場合、以下のいずれかの手順を実行します。

Run Command を使用して ssm-user sudo のアクセス許可を変更する (コンソール)

- コンソールからコマンドを実行する の手順を次の値で使用します。
  - [Command document] (コマンドのドキュメント) で、`AWS-RunShellScript` を選択します。
  - sudo アクセスを削除するには、[Command parameters (コマンドのパラメータ)] 領域で、[コマンド] ボックスに以下を貼り付けます。

    ```
    cd /etc/sudoers.d
    echo "#User rules for ssm-user" > ssm-agent-users
    ```

    -または-

    sudo アクセスを復元するには、[Command parameters (コマンドのパラメータ)] 領域で、[コマンド] ボックスに以下を貼り付けます。

    ```
    cd /etc/sudoers.d
    ```

```
echo "ssm-user ALL=(ALL) NOPASSWD:ALL" > ssm-agent-users
```

コマンドラインを使用して ssm-user sudo のアクセス許可を変更する (AWS CLI)

1. マネージドノードに接続して以下のコマンドを実行します。

   ```
   sudo -s
   ```

2. 次のコマンドを使用して、作業ディレクトリを変更します。

   ```
   cd /etc/sudoers.d
   ```

3. 編集する `ssm-agent-users` という名前のファイルを開きます。
4. sudo アクセスを削除するには、次の行を削除します。

   ```
   ssm-user ALL=(ALL) NOPASSWD:ALL
   ```

   -または-

   sudo アクセスを復元するには、次の行を追加します。

   ```
   ssm-user ALL=(ALL) NOPASSWD:ALL
   ```

5. ファイルを保存します。

Windows Server で ssm-user の管理者アカウントのアクセス許可を管理する

Windows Server のマネージドノードで ssm-user アカウントの 管理者 許可を有効または無効にする場合、以下のいずれかの手順を実行します。

Run Command を使用して管理者権限を変更する (コンソール)

- コンソールからコマンドを実行する の手順を次の値で使用します。

  [Command document] (コマンドのドキュメント) で、`AWS-RunPowerShellScript` を選択します。

  管理アクセスを削除するには、[Command parameters (コマンドのパラメータ)] 領域で、[コマンド] ボックスに以下を貼り付けます。

```
net localgroup "Administrators" "ssm-user" /delete
```

-または-

管理アクセスを復元するには、[Command parameters (コマンドのパラメータ)] 領域で、[コマンド] ボックスに以下を貼り付けます。

```
net localgroup "Administrators" "ssm-user" /add
```

PowerShell またはコマンドプロンプトウィンドウを使用して管理者許可を変更する

1. マネージドノードに接続して PowerShell またはコマンドプロンプトのウィンドウを開きます。
2. 管理アクセスを削除するには、次のコマンドを実行します。

```
net localgroup "Administrators" "ssm-user" /delete
```

-または-

管理アクセスを復元するには、次のコマンドを実行します。

```
net localgroup "Administrators" "ssm-user" /add
```

Windows コンソールを使用して管理者許可を変更する

1. マネージドノードに接続して PowerShell またはコマンドプロンプトのウィンドウを開きます。
2. コマンドラインから `lusrmgr.msc` を実行して、[Local Users and Groups (ローカルユーザーとグループ)] コンソールを開きます。
3. [Users (ユーザー)] ディレクトリを開いて、[ssm-user] を開きます。
4. [Member Of (所属するグループ)] タブで、次のいずれかを実行します。

   - 管理アクセスを削除するには、[Administrators (管理者)] を選択し、[Remove (削除)] を選択します。

     -または-

管理アクセスを復元するには、テキストボックスに **Administrators** と入力し、[追加] を選択します。

5. [OK] を選択します。

ステップ 8: (オプション) Session Manager を通して SSH 接続のアクセス許可を付与および制御する

AWS アカウント のユーザーに AWS Command Line Interface (AWS CLI) を使用する許可を付与して、AWS Systems Manager の Session Manager が適用されたマネージドノードに Secure Shell (SSH) 接続を確立できるようにします。SSH で接続するユーザーは Secure Copy Protocol (SCP) を使用して自分のローカルマシンとマネージドノード間でファイルをコピーすることもできます。この機能を使って、インバウンドポートを開いたり、踏み台ホストを維持したりすることなく、マネージドノードへ接続できます。

SSH 接続を有効にした後、AWS Identity and Access Management (IAM) ポリシーを使用してユーザー、グループ、またはロールが Session Manager で SSH 接続を確立することを明示的に許可または拒否できます。

> **Note**
>
> ログ記録は、ポート転送または SSH を介して接続する Session Manager セッションでは使用できません。これは、SSH はすべてのセッションデータを暗号化し、Session Manager は SSH 接続のトンネルとしてのみ機能するためです。

トピック

- Session Manager で SSH 接続を有効にする手順
- Session Manager による SSH 接続のユーザーアクセス許可の制御

Session Manager で SSH 接続を有効にする手順

マネージドノードで Session Manager を通して SSH 接続を有効にする場合、次の手順を実行します。

Session Managerで SSH 接続を有効にするには

1. SSH 接続を有効にするマネージドノードに対して以下の手順を実行します:

- SSH がマネージドノードに実行されていることを確認します。(ノードのインバウンドポートを閉じることができます)
- SSM Agent のバージョン 2.3.672.0 以降がマネージドノードにインストールされていることを確認します。

  マネージドノードに SSM Agent のインストールまたは更新の詳細については、以下のトピックをご参照ください:

  - Windows Server 用の EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする.
  - Linux 用 EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする
  - macOS 用の EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする
  - ハイブリッド Windows ノードで SSM Agent をインストールする方法
  - ハイブリッド Linux ノードで SSM Agent をインストールする方法

  > **Note**
  >
  > マネージドノードとしてアクティベートしたオンプレミスサーバー、エッジデバイス、仮想マシン (VM) に Session Manager を使用する場合、アドバンストインスタンス層を使用する必要があります。アドバンストインスタンスの詳細については、「インスタンス層の設定」を参照してください。

2. SSH を使用したマネージドノードに接続するローカルマシンで、以下の手順を実行します:

   - Session Manager プラグイン 1.1.23.0 バージョン以降がインストールされていることを確認します。

     Session Manager プラグインのインストールについては、AWS CLI 用の Session Manager プラグインをインストールする を参照してください。
   - SSH 設定ファイルを更新して、Session Manager セッションを開始し、接続を介してすべてのデータを転送するプロキシコマンドを実行できるようにします。

     Linux および macOS

> **Tip**
>
> SSH 設定ファイルは通常 ~/.ssh/config にあります。

ローカルマシンの設定ファイルに以下を追加します。

```
# SSH over Session Manager
Host i-* mi-*
    ProxyCommand sh -c "aws ssm start-session --target %h --document-name AWS-
StartSSHSession --parameters 'portNumber=%p'"
    User ec2-user
```

Windows

> **Tip**
>
> SSH 設定ファイルは通常 C:\Users*<username>*\.ssh\config にあります。

ローカルマシンの設定ファイルに以下を追加します。

```
# SSH over Session Manager
Host i-* mi-*
    ProxyCommand C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe "aws
 ssm start-session --target %h --document-name AWS-StartSSHSession --parameters
 portNumber=%p"
```

- マネージドノードへの接続を確立する際に使用する Privacy Enhanced Mail 証明書 (PEM ファイル) または少なくとも公開キーを作成または確認します。これはマネージドノードにすでに関連付けされたキーでなければなりません。プライベートキーファイルへのアクセス許可を設定し、お客様のみが読み取りできるようにする必要があります 次のコマンドを使用してプライベートキーファイルのアクセス許可を設定することで、お客様以外のユーザーによる読み取りを拒否できます。

```
chmod 400 <my-key-pair>.pem
```

例えば、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスの場合、インスタンスの作成時に作成または選択したキーペアファイルです。(セッションを開始するには、コマンドの一部として証明書またはキーへのパスを指定します。SSH を使用してセッションを開始する方法については、「セッションの開始 (SSH)」を参照してください。)

Session Manager による SSH 接続のユーザーアクセス許可の制御

Session Manager で マネージドノードに SSH 接続を有効にしたら、IAM ポリシーでユーザー、グループ、ロールが Session Manager で SSH 接続を確立する権限を許可または拒否できます。

IAM ポリシーを使用して Session Manager での SSH 接続を許可するには

- 以下のいずれかのオプションを使用します。
  - オプション 1: IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。

    ナビゲーションペインで [Policies (ポリシー)] を選択し、Session Manager を介した SSH 接続の開始を許可するユーザーまたはロールのアクセス許可ポリシーを更新します。

    例えば、クイックスタート Session Manager のエンドユーザーポリシー で作成したクイックスタートポリシーに次の要素を追加します。各###############をユーザー自身の情報に置き換えます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ssm:StartSession",
            "Resource": [
                "arn:aws:ec2:region:account-id:instance/instance-id",
                "arn:aws:ssm:*:*:document/AWS-StartSSHSession"
            ]
        }
    ]
},
{
         "Effect": "Allow",
         "Action": ["ssmmessages:OpenDataChannel"],
         "Resource": ["arn:aws:ssm:*:*:session/${aws:userid}-*"]
```

```
        }
```

- オプション 2: AWS Management Console、AWS CLI、または AWS API を使用して、インラインポリシーをユーザーポリシーにアタッチします。

  任意の方法を使用して、オプション 1 のポリシーステートメントを AWS ユーザー、グループ、またはロールのポリシーにアタッチします。

  詳細については、IAM ユーザーガイド の「IAM ID アクセス許可の追加と削除」を参照してください。

IAM ポリシーを使用して Session Manager での SSH 接続を拒否するには

- 以下のいずれかのオプションを使用します。

  - オプション 1: IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。ナビゲーションペインで [ポリシー] を選択し、ユーザーまたはロールのアクセス許可ポリシーを更新して、Session Manager セッションの開始をブロックします。

    例えば、クイックスタート Session Manager のエンドユーザーポリシー で作成したクイックスタートポリシーに次の要素を追加します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "ssm:StartSession",
            "Resource": "arn:aws:ssm:*:*:document/AWS-StartSSHSession"
        }
    ]
},
{
         "Effect": "Allow",
         "Action": ["ssmmessages:OpenDataChannel"],
         "Resource": ["arn:aws:ssm:*:*:session/${aws:userid}-*"]
       }
```

  - オプション 2: AWS Management Console、AWS CLI、または AWS API を使用して、インラインポリシーをユーザーポリシーにアタッチします。

任意の方法を使用して、オプション 1 のポリシーステートメントを AWS ユーザー、グループ、またはロールのポリシーにアタッチします。

詳細については、IAM ユーザーガイド の「IAM ID アクセス許可の追加と削除」を参照してください。

Session Manager の使用

AWS Systems Manager コンソール、Amazon Elastic Compute Cloud (Amazon EC2) コンソール、AWS Command Line Interface (AWS CLI) を使用して、AWS Identity and Access Management (IAM) ポリシーでシステム管理者がユーザーにアクセス権を付与したマネージドノードに接続するセッションを開始できます。アクセス権限に応じて、セッションに関する情報を表示したり、タイムアウトしていない非アクティブなセッションを再開したり、セッションを終了したりすることもできます。セッションが確立されると、セッションは IAM ロールのセッション期間の影響を受けません。Session Manager によるセッション期間の制限については、「アイドルセッションのタイムアウト値を指定します。」および「最大セッション時間の指定」を参照してください。

セッションの詳細については、「セッションとは何ですか。」を参照してください。

トピック

- AWS CLI 用の Session Manager プラグインをインストールする
- セッションを開始する
- セッションを終了する
- セッション履歴を表示する

AWS CLI 用の Session Manager プラグインをインストールする

AWS Command Line Interface (AWS CLI) を使用してマネージドノードとの Session Manager セッションを開始するには、ローカルマシンに Session Manager プラグインをインストールする必要があります。Microsoft Windows Server、macOS、Linux、および Ubuntu Server のサポート対象のバージョンにプラグインをインストールできます。

> **Note**
>
> Session Manager プラグインを使用するには、AWS CLI バージョン 1.16.12 以降をローカルマシンにインストールする必要があります。詳細については、「Installing or updating the latest version of the AWS Command Line Interface」を参照してください。

トピック

- Session Manager プラグインの最新バージョンとリリース履歴
- Windows での Session Manager プラグインのインストール
- macOS での Session Manager プラグインのインストール
- Linux で Session Manager プラグインをインストールする
- Session Manager プラグインのインストールを検証する
- GitHub での Session Manager プラグイン
- (オプション) Session Manager プラグインのログ記録を有効にする

Session Manager プラグインの最新バージョンとリリース履歴

ローカルマシンで、Session Manager プラグインのサポートされているバージョンを実行する必要があります。現在サポートされている最小バージョンは 1.1.17.0 です。それ以前のバージョンを実行している場合は、Session Manager 操作が失敗する可能性があります。

最新バージョンを使用しているかどうかを確認するには、AWS CLI で次のコマンドを実行します。

> **Note**
>
> このコマンドは、プラグインがご使用のオペレーティングシステムタイプのデフォルトのインストールディレクトリにある場合にのみ結果を返します。プラグインをインストールしたディレクトリの、VERSION ファイルのコンテンツでバージョンを確認することもできます。

```
session-manager-plugin --version
```

次の表は、Session Manager プラグインのすべてのリリースと、各バージョンに含まれている機能や機能強化を示しています。

> **Important**
>
> 常に最新バージョンの使用をお勧めします。最新バージョンには、プラグインの使用エクスペリエンスを改善する機能強化が含まれています。

バージョン	リリース日	詳細
1.2.707.0	2025 年 2 月 6 日	機能強化: Dockerfile で Go バージョンが 1.23 にアップグレードされました。README のバージョン設定ステップを更新しました。
1.2.694.0	2024 年 11 月 20 日	バグ修正: OpenDataChannel リクエストに認証情報を追加した変更がロールバックされました。
1.2.688.0	2024 年 11 月 6 日	このバージョンは 2024 年 11 月 20 日に廃止されました。 機能強化: • OpenDataChannel リクエストに認証情報が追加されました。 • `testify` および `objx` 依存パッケージがアップグレードされました。
1.2.677.0	2024 年 10 月 10 日	拡張機能: OpenDataChannel リクエストでプラグインバージョンを渡すためのサポートが追加されました。
1.2.650.0	2024 年 7 月 2 日	機能強化: aws-sdk-go を 1.54.10 にアップグレードしました。 バグ修正: gofmt チェックのコメントを再フォーマットしました。
1.2.633.0	2024 年 5 月 30 日	機能強化: Amazon Elastic Container Registry (Amazon ECR) イメージを使用するように Dockerfile を更新しました。
1.2.553.0	2024 年 1 月 10 日	機能強化: aws-sdk-go パッケージと依存する Golang パッケージをアップグレードしました。

バージョン	リリース日	詳細
1.2.536.0	2023 年 12 月 4 日	機能強化: StartSession API レスポンスを環境変数としてセッションマネージャープラグインに渡すサポートが追加されました。
1.2.497.0	2023 年 8 月 1 日	エンハンスメント: Go SDK を v1.44.302 にアップグレードしました。
1.2.463.0	2023 年 3 月 15 日	機能強化: macOS バンドルインストーラと署名済みインストーラに Apple Mac (M1) の Mac with Apple silicon サポートを追加しました。
1.2.398.0	2022 年 10 月 14 日	機能強化: golang バージョン 1.17 をサポートします。macOS のデフォルトのセッションマネージャープラグインランナーを python3 を使用するように更新しました。SSMCLI からセッションマネージャープラグインへのインポートパスを更新します。
1.2.339.0	2022 年 6 月 16 日	バグ修正: ポートセッションのアイドルセッションタイムアウトを修正しました。
1.2.331.0	2022 年 5 月 27 日	バグ修正: タイムアウト前にローカルサーバーが接続しないときに、ポートセッションが途中で閉じる問題を修正しました。
1.2.323.0	2022 年 5 月 19 日	バグ修正: smux キープアライブを無効にして、アイドルセッションタイムアウト機能を使用するように修正しました。
1.2.312.0	2022 年 3 月 31 日	機能拡張: より多くの出力メッセージペイロードのタイプをサポート。
1.2.295.0	2022 年 1 月 12 日	バグ修正: エージェントが非アクティブになった場合のクライアントによるストリームデータの再送信、ならびに `start_publication` と `pause_publication` メッセージに関する不正なログが原因で発生するセッションのハングアップ。

バージョン	リリース日	詳細
1.2.279.0	2021 年 10 月 27 日	機能拡張: Windows プラットフォーム用の zip パッケージ。
1.2.245.0	2021 年 8 月 19 日	機能拡張: AWS IAM Identity Center をサポートできるように `aws-sdk-go` を最新バージョン (v1.40.17) にアップグレードします。
1.2.234.0	2021 年 7 月 26 日	バグ修正: セッションが突然終了したシナリオを対話型セッションで処理します。
1.2.205.0	2021 年 6 月 10 日	機能拡張: 署名されたmacOSインストーラのサポートが追加されました。
1.2.54.0	2021 年 1 月 29 日	拡張: NonInteractiveCommands 実行モードでのセッションの実行のサポートが追加されました。
1.2.30.0	2020 年 11 月 24 日	拡張: (ポート転送セッションのみ) 全体的なパフォーマンスが向上しました。
1.2.7.0	2020 年 10 月 15 日	拡張: (ポート転送セッションのみ) レイテンシーを短縮し、全体的なパフォーマンスを向上させました。
1.1.61.0	2020 年 4 月 17 日	機能強化: Linux および Ubuntu の ARM サポートが追加されました。
1.1.54.0	2020 年 1 月 6 日	バグ修正: Session Manager プラグインの準備が完了していないときにドロップされるパケットの競合状態シナリオに対処します。
1.1.50.0	2019 年 11 月 19 日	機能強化: ポートをローカル UNIX ソケットに転送するためのサポートが追加されました。
1.1.35.0	2019 年 11 月 7 日	機能強化: (ポート転送セッションのみ) ローカルユーザーが `Ctrl+C` を押すと、TerminateSession コマンドが SSM Agent に送信されます。

バージョン	リリース日	詳細
1.1.33.0	2019 年 9 月 26 日	機能強化: (ポート転送セッションのみ) クライアントが TCP 接続を中断したときに、サーバーに切断信号を送信します。
1.1.31.0	2019 年 9 月 6 日	機能強化: リモートサーバーが接続を閉じるまでポート転送セッションを開いたままにするための更新です。
1.1.26.0	2019 年 7 月 30 日	機能拡張: セッション中のデータ転送速度を制限するための更新です。
1.1.23.0	2019 年 7 月 9 日	機能拡張: Session Manager を使用して SSH セッションを実行するためのサポートが追加されました。
1.1.17.0	2019 年 4 月 4 日	機能強化: AWS Key Management Service (AWS KMS) を使用してセッションデータをさらに暗号化するためのサポートが追加されました。
1.0.37.0	2018 年 9 月 20 日	機能強化: Windows バージョンのバグ修正。
1.0.0.0	2018 年 9 月 11 日	Session Manager プラグインの初回リリース。

Windows での Session Manager プラグインのインストール

スタンドアロンインストーラを使用して、Windows Vista 以降に Session Manager プラグインをインストールできます。

更新がリリースされたときは、最新バージョンの Session Manager プラグインを取得するため、インストールプロセスを繰り返す必要があります。

> **Note**
>
> 以下の情報に注意してください。
>
> - Session Manager プラグインインストーラには、プラグインをインストールするための管理者権限が必要です。
> - 最良の結果を得るには、Windows PowerShell のバージョン 5 以降を使用して、Windows クライアントでセッションを開始することをお勧めします。または、Windows 10 のコマ

ンドシェルを使用できます。Session Manager プラグインでは、PowerShell とコマンドシェルのみがサポートされています。サードパーティーのコマンドラインツールは、プラグインと互換性がない可能性があります。

EXE インストーラを使用して Session Manager プラグインをインストールするには

1. 次の URL を使用してインストーラをダウンロードします。

   ```
   https://s3.amazonaws.com/session-manager-downloads/plugin/latest/windows/SessionManagerPluginSetup.exe
   ```

   または、次の URL から zip 形式のインストーラーをダウンロードすることもできます。

   ```
   https://s3.amazonaws.com/session-manager-downloads/plugin/latest/windows/SessionManagerPlugin.zip
   ```

2. ダウンロードしたインストーラを実行し、画面の指示に従います。zip 形式のインストーラーをダウンロードした場合は、まずインストーラーを解凍する必要があります。

   インストール先のボックスを空白のままにして、プラグインをデフォルトディレクトリにインストールします。

   - `%PROGRAMFILES%\Amazon\SessionManagerPlugin\bin\`

3. インストールが成功したことを確認します。詳細については、Session Manager プラグインのインストールを検証する を参照してください。

   > **Note**
   >
   > Windows が実行ファイルを見つけることができない場合、コマンドプロンプトを再度開くか、または手動でインストールディレクトリを PATH 環境変数に追加します。詳細については、トラブルシューティングトピック「Session Manager プラグインがコマンドラインパスに自動的に追加されませんでした (Windows)」を参照してください。

macOS での Session Manager プラグインのインストール

Session Manager プラグインを macOS にインストールするには、次のいずれかのトピックを選択します。

> **Note**
>
> 署名付きインストーラーは署名付き .pkg ファイルです。バンドルインストーラーは .zip ファイルを使用します。ファイルを解凍後、バイナリを使用してプラグインをインストールできます。

署名されたインストーラーを使用して Session Manager プラグインを macOS にインストールする

このセクションでは、署名済みのインストーラーを使用して Session Manager プラグインを macOS にインストールする方法について説明します。

署名されたインストーラー (macOS) を使用して Session Manager プラグインをインストールするには

1. 署名されたインストーラーをダウンロードします。

   x86_64

   ```
   curl "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/mac/
   session-manager-plugin.pkg" -o "session-manager-plugin.pkg"
   ```

   Apple シリコン搭載の Mac

   ```
   curl "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/
   mac_arm64/session-manager-plugin.pkg" -o "session-manager-plugin.pkg"
   ```

2. インストールコマンドを実行します。コマンドが失敗した場合は、/usr/local/bin フォルダが存在することを確認します。存在しない場合はこれを作成してから、再度コマンドを実行します。

   ```
   sudo installer -pkg session-manager-plugin.pkg -target /
   sudo ln -s /usr/local/sessionmanagerplugin/bin/session-manager-plugin /usr/local/
   bin/session-manager-plugin
   ```

3. インストールが成功したことを確認します。詳細については、「Session Manager プラグインのインストールを検証する」を参照してください。

macOS での Session Manager プラグインのインストール

このセクションでは、バンドルされたインストーラーを使用して Session Manager プラグインを macOS にインストールする方法について説明します。

> **Important**
>
> 次の重要な情報に注意してください。
>
> - スクリプトはプラグインを `/usr/local/sessionmanagerplugin` システムディレクトリにインストールするため、デフォルトでは、インストーラの実行に sudo アクセスが必要です。プラグインのインストールに sudo を使用しない場合は、インストーラのスクリプトを手動で更新し、プラグインを、sudo アクセスが不要なディレクトリにインストールします。
> - バンドルされたインストーラでは、スペースを含むパスへのインストールはサポートされていません。

バンドルされたインストーラ (macOS) を使用して Session Manager プラグインをインストールするには

1. バンドルされたインストーラをダウンロードします。

   x86_64

   ```
   curl "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/mac/sessionmanager-bundle.zip" -o "sessionmanager-bundle.zip"
   ```

   Apple シリコン搭載の Mac

   ```
   curl "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/mac_arm64/sessionmanager-bundle.zip" -o "sessionmanager-bundle.zip"
   ```

2. パッケージを解凍します。

   ```
   unzip sessionmanager-bundle.zip
   ```

3. インストールコマンドを実行します。

```
sudo ./sessionmanager-bundle/install -i /usr/local/sessionmanagerplugin -b /usr/
local/bin/session-manager-plugin
```

> **Note**
>
> プラグインには、Python 2.6.5 以降、または Python 3.3 以降が必要です。デフォルトでは、インストールスクリプトはシステムのデフォルトバージョンの Python で実行されます。別のバージョンの Python がインストールされており、それを使用して Session Manager プラグインをインストールする場合は、Python の実行可能ファイルへの絶対パスを指定してそのバージョンでインストールスクリプトを実行します。以下に例を示します。
>
> ```
> sudo /usr/local/bin/python3.8 sessionmanager-bundle/install -i /usr/local/
> sessionmanagerplugin -b /usr/local/bin/session-manager-plugin
> ```

インストーラは Session Manager プラグインを `/usr/local/sessionmanagerplugin` にインストールし、シンボリックリンク `session-manager-plugin` を `/usr/local/bin` ディレクトリに作成します。これにより、ユーザーの `$PATH` 変数にインストールディレクトリを指定する必要がなくなります。

`-i` オプションおよび `-b` オプションの説明を表示するには、`-h` オプションを使用します。

```
./sessionmanager-bundle/install -h
```

4. インストールが成功したことを確認します。詳細については、「Session Manager プラグインのインストールを検証する」を参照してください。

> **Note**
>
> プラグインをアンインストールするには、次の 2 つのコマンドを表示順に実行します。
>
> ```
> sudo rm -rf /usr/local/sessionmanagerplugin
> ```
>
> ```
> sudo rm /usr/local/bin/session-manager-plugin
> ```

Linux で Session Manager プラグインをインストールする

このセクションでは、Session Manager プラグインインストーラパッケージの署名を確認し、以下の Linux ディストリビューションにプラグインをインストールする方法について説明します。

- Amazon Linux 2
- AL2023
- RHEL
- Debian
- Ubuntu

トピック

- Session Manager プラグインの署名を確認する
- Amazon Linux 2、Amazon Linux 2023、Red Hat Enterprise Linux ディストリビューションに Session Manager プラグインをインストールする
- Debian Server と Ubuntu Server での Session Manager プラグインのインストール

Session Manager プラグインの署名を確認する

Linux インスタンス用の Session Manager プラグイン RPM および Debian インストーラパッケージは、暗号化で署名されています。パブリックキーを使用して、プラグインバイナリとパッケージがオリジナルであり、変更されていないことを確認できます。ファイルが改変されていたり、損傷があった場合、確認は失敗します。GNU Privacy Guard (GPG) ツールを使用して、インストーラパッケージの署名を確認できます。以下の情報は Session Manager プラグインのバージョン 1.2.707.0 以降のものです。

Session Manager プラグインインストーラパッケージの署名を確認するには、次の手順を実行します。

トピック

- ステップ 1: Session Manager プラグインインストーラーパッケージをダウンロードする
- ステップ 2: 関連付けられた署名ファイルをダウンロードする
- ステップ 3: GPG ツールをインストールする
- ステップ 4: Linux サーバーで Session Manager プラグインインストーラパッケージを確認する

ステップ 1: Session Manager プラグインインストーラーパッケージをダウンロードする

検証する Session Manager プラグインインストーラパッケージをダウンロードします。

Amazon Linux 2、AL2023、および RHEL RPM パッケージ

x86_64

```
curl -o "session-manager-plugin.rpm" "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/linux_64bit/session-manager-plugin.rpm"
```

x86

```
curl -o "session-manager-plugin.rpm" "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/linux_32bit/session-manager-plugin.rpm"
```

ARM64

```
curl -o "session-manager-plugin.rpm" "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/linux_arm64/session-manager-plugin.rpm"
```

Debian および Ubuntu Deb パッケージ

x86_64

```
curl -o "session-manager-plugin.deb" "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/ubuntu_64bit/session-manager-plugin.deb"
```

x86

```
curl -o "session-manager-plugin.deb" "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/ubuntu_32bit/session-manager-plugin.deb"
```

ARM64

```
curl -o "session-manager-plugin.deb" "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/ubuntu_arm64/session-manager-plugin.deb"
```

ステップ 2: 関連付けられた署名ファイルをダウンロードする

インストーラパッケージをダウンロードしたら、パッケージの検証のために関連する署名ファイルをダウンロードします。パッケージ内の session-manager-plugin バイナリファイルの不正なコピーや使用に対する保護を強化するために、個々のバイナリファイルの検証に使用できるバイナリ署名も提供しています。必要なセキュリティに応じて、これらのバイナリ署名を使用することを選択できます。

Amazon Linux 2、AL2023、および RHEL 署名パッケージ

x86_64

パッケージ:

```
curl -o "session-manager-plugin.rpm.sig" "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/linux_64bit/session-manager-plugin.rpm.sig"
```

バイナリ:

```
curl -o "session-manager-plugin.sig" "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/linux_64bit/session-manager-plugin.sig"
```

x86

パッケージ:

```
curl -o "session-manager-plugin.rpm.sig" "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/linux_32bit/session-manager-plugin.rpm.sig"
```

バイナリ:

```
curl -o "session-manager-plugin.sig" "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/linux_32bit/session-manager-plugin.sig"
```

ARM64

パッケージ:

```
curl -o "session-manager-plugin.rpm.sig" "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/linux_arm64/session-manager-plugin.rpm.sig"
```

バイナリ:

```
curl -o "session-manager-plugin.sig" "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/linux_arm64/session-manager-plugin.sig"
```

Debian および Ubuntu Deb 署名パッケージ

x86_64

パッケージ:

```
curl -o "session-manager-plugin.deb.sig" "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/ubuntu_64bit/session-manager-plugin.deb.sig"
```

バイナリ:

```
curl -o "session-manager-plugin.sig" "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/ubuntu_64bit/session-manager-plugin.sig"
```

x86

パッケージ:

```
curl -o "session-manager-plugin.deb.sig" "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/ubuntu_32bit/session-manager-plugin.deb.sig"
```

バイナリ:

```
curl -o "session-manager-plugin.sig" "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/ubuntu_32bit/session-manager-plugin.sig"
```

ARM64

パッケージ:

```
curl -o "session-manager-plugin.deb.sig" "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/ubuntu_arm64/session-manager-plugin.deb.sig"
```

バイナリ:

```
curl -o "session-manager-plugin.sig" "https://s3.amazonaws.com/session-manager-
downloads/plugin/latest/ubuntu_arm64/session-manager-plugin.sig"
```

ステップ 3: GPG ツールをインストールする

Session Manager プラグインの署名を確認するには、システムに GNU Privacy Guard (GPG) ツールがインストールされている必要があります。この検証プロセスには、GPG バージョン 2.1 以降が必要です。GPG バージョンは、以下のコマンドを実行することで確認できます。

```
gpg --version
```

GPG バージョンが 2.1 より古い場合は、検証プロセスに進む前に更新してください。ほとんどのシステムでは、パッケージマネージャーを使用して GPG ツールを更新できます。例えば、Amazon Linux AMI と RHEL システムでは、以下のコマンドを使用できます。

```
sudo yum update
sudo yum install gnupg2
```

Ubuntu または Debian システムでは、以下のコマンドを使用できます。

```
sudo apt-get update
sudo apt-get install gnupg2
```

検証プロセスを続行する前に、必要な GPG バージョンがあることを確認してください。

ステップ 4: Linux サーバーで Session Manager プラグインインストーラパッケージを確認する

Linux サーバーで Session Manager プラグインインストーラパッケージを検証するには、次の手順に従います。

> **Note**
>
> Amazon Linux 2 は、GPG ツールのバージョン 2.1 以降をサポートしていません。次の手順が Amazon Linux 2 インスタンスで機能しない場合は、Amazon Linux 2 インスタンスにインストールする前に、別のプラットフォームで署名を確認してください。

1. 次のパブリックキーをコピーし、session-manager-plugin.gpg という名前のファイルに保存します。

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mFIEZ5ERQxMIKoZIzj0DAQcCAwQjuZy+IjFoYg57sLTGhF3aZLBaGpzB+gY6j7Ix
P7NqbpXyjVj8a+dy79gSd64OEaMxUb7vw/jug+CfRXwVGRMNtIBBV1MgU1NNIFNl
c3Npb24gTWFuYWdlciA8c2Vzc2lvbi1tYW5hZ2VyLXBsdWdpbi1zaWduZXJAYW1h
em9uLmNvbT4gKEFXUyBTeXN0ZW1zIE1hbmFnZXIgU2Vzc2lvbiBNYW5hZ2VyIFBs
dWdpbiBMaW51eCBTaWduZXIgS2V5KYkBAAQQEwgAqAUCZ5ERQ4EcQVdTIFNTTSBT
ZXNzaW9uIE1hbmFnZXIgPHNlc3Npb24tbWFuYWdlci1wbHVnaW4tc2lnbmVyQGFt
YXpvbi5jb20+IChBV1MgU3lzdGVtcyBNYW5hZ2VyIFNlc3Npb24gTWFuYWdlciBQ
bHVnaW4gTGludXggU2lnbmVyIEtleSkWIQR5WWNxJM4JOtUB1HosTUr/b2dX7gIe
AwIbAwIVCAAKCRAsTUr/b2dX7rO1AQCa1kig3lQ78W/QHGU76uHx3XAyv0tfpE9U
oQBCIwFLSgEA3PDHt3lZ+s6m9JLGJsy+Cp5ZFzpiF6RgluR/2gA861M=
=2DQm
-----END PGP PUBLIC KEY BLOCK-----
```

2. 公開鍵をキーリングにインポートします。返されるキー値は 2C4D4AFF6F6757EE である必要があります。

```
$ gpg --import session-manager-plugin.gpg
gpg: key 2C4D4AFF6F6757EE: public key "AWS SSM Session Manager <session-manager-
plugin-signer@amazon.com> (AWS Systems Manager Session Manager Plugin Linux Signer
 Key)" imported
gpg: Total number processed: 1
gpg:               imported: 1
```

3. 次のコマンドを実行して、フィンガープリントを検証します。

```
gpg --fingerprint 2C4D4AFF6F6757EE
```

コマンド出力のフィンガープリントは、次のものと一致する必要があります。

```
7959 6371 24CE 093A D501 D47A 2C4D 4AFF 6F67 57EE
```

```
pub   nistp256 2025-01-22 [SC]
      7959 6371 24CE 093A D501  D47A 2C4D 4AFF 6F67 57EE
uid           [ unknown] AWS SSM Session Manager <session-manager-plugin-
signer@amazon.com> (AWS Systems Manager Session Manager Plugin Linux Signer Key)
```

フィンガープリントが一致しない場合は、プラグインをインストールしないでください。AWS サポート に連絡する。

4. インストーラパッケージの署名を確認します。*signature-filename* および *downloaded-plugin-filename* は、このトピックの表で前述したように、署名ファイルおよび session-manager-plugin をダウンロードするときに指定した値に置き換えてください。

```
gpg --verify signature-filename downloaded-plugin-filename
```

例えば、Amazon Linux 2 の x86_64 アーキテクチャの場合、コマンドは次のとおりです。

```
gpg --verify session-manager-plugin.rpm.sig session-manager-plugin.rpm
```

このコマンドは、次のような出力を返します。

```
gpg: Signature made Mon Feb 3 20:08:32 2025 UTC gpg: using ECDSA key
 2C4D4AFF6F6757EE
gpg: Good signature from "AWS Systems Manager Session Manager <session-manager-
plugin-signer@amazon.com> (AWS Systems Manager Session Manager Plugin Linux Signer
 Key)" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg: There is no indication that the signature belongs to the owner.
Primary key fingerprint: 7959 6371 24CE 093A D501 D47A 2C4D 4AFF 6F67 57EE
```

出力結果に「BAD signature」という句が含まれる場合、手順が正しいことをもう一度確認してください。この応答が続く場合は、AWS サポート に連絡し、パッケージをインストールしないでください。信頼に関する警告メッセージは、署名が無効であることを意味するものではなく、パブリックキーを検証していないことを示すだけです。キーは、自分や信頼する人が署名した場合にのみ信頼できます。出力にフレーズ Can't check signature: No public key が含まれている場合、Session Manager バージョン 1.2.707.0 以降をダウンロードしたことを確認します。

Amazon Linux 2、Amazon Linux 2023、Red Hat Enterprise Linux ディストリビューションに Session Manager プラグインをインストールする

次の手順を使用して、Session Manager プラグインを Amazon Linux 2、Amazon Linux 2023 (AL2023)、RHEL ディストリビューションにインストールします。

> **Note**
>
> Session Manager プラグインは、Amazon Linux 1 ではサポートされません。Amazon Linux 2 以降のディストリビューションでサポートされます。

1. Session Manager プラグイン RPM パッケージをダウンロードしてインストールします。

   x86_64

   Amazon Linux 2 と RHEL 7 では、次のコマンドを実行します。

   ```
   sudo yum install -y https://s3.amazonaws.com/session-manager-downloads/plugin/
   latest/linux_64bit/session-manager-plugin.rpm
   ```

   AL2023、RHEL 8 および 9 では、次のコマンドを実行します。

   ```
   sudo dnf install -y https://s3.amazonaws.com/session-manager-downloads/plugin/
   latest/linux_64bit/session-manager-plugin.rpm
   ```

   x86

   RHEL 7 では、次のコマンドを実行します。

   ```
   sudo yum install -y https://s3.amazonaws.com/session-manager-downloads/plugin/
   latest/linux_32bit/session-manager-plugin.rpm
   ```

   RHEL 8 と 9 では、次のコマンドを実行します。

   ```
   sudo dnf install -y https://s3.amazonaws.com/session-manager-downloads/plugin/
   latest/linux_32bit/session-manager-plugin.rpm
   ```

   ARM64

   Amazon Linux 2 と RHEL 7 では、次のコマンドを実行します。

   ```
   sudo yum install -y https://s3.amazonaws.com/session-manager-downloads/plugin/
   latest/linux_arm64/session-manager-plugin.rpm
   ```

   AL2023、RHEL 8 および 9 では、次のコマンドを実行します。

   ```
   sudo dnf install -y https://s3.amazonaws.com/session-manager-downloads/plugin/
   latest/linux_arm64/session-manager-plugin.rpm
   ```

2. インストールが成功したことを確認します。詳細については、Session Manager プラグインのインストールを検証する を参照してください。

> **Note**
>
> プラグインをアンインストールする必要がある場合は、`sudo yum erase session-manager-plugin -y` を実行します。

Debian Server と Ubuntu Server での Session Manager プラグインのインストール

1. Session Manager プラグイン deb パッケージをダウンロードします。

   x86_64

   ```
   curl "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/ubuntu_64bit/session-manager-plugin.deb" -o "session-manager-plugin.deb"
   ```

   x86

   ```
   curl "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/ubuntu_32bit/session-manager-plugin.deb" -o "session-manager-plugin.deb"
   ```

   ARM64

   ```
   curl "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/ubuntu_arm64/session-manager-plugin.deb" -o "session-manager-plugin.deb"
   ```

2. インストールコマンドを実行します。

   ```
   sudo dpkg -i session-manager-plugin.deb
   ```

3. インストールが成功したことを確認します。詳細については、Session Manager プラグインのインストールを検証する を参照してください。

> **Note**
>
> プラグインをアンインストールする必要がある場合は、`sudo dpkg -r session-manager-plugin` を実行します。

Session Manager プラグインのインストールを検証する

Session Manager プラグインが正常にインストールされたことを確認するには、次のコマンドを実行します。

```
session-manager-plugin
```

インストールが成功すると、次のメッセージが返されます。

```
The Session Manager plugin is installed successfully. Use the AWS CLI to start a
 session.
```

AWS Command Line Interface (AWS CLI) 内の start-session コマンドを実行してインストールをテストすることもできます。次のコマンドで、「*instance-id*」をユーザー自身の情報に置き換えます。

```
aws ssm start-session --target instance-id
```

このコマンドは、AWS CLI をインストールして設定し、Session Manager を使用してターゲットマネージドノードにアクセスするために必要な IAM 許可を Session Manager 管理者がユーザーに付与している場合にのみ機能します。

GitHub での Session Manager プラグイン

ニーズに応じてプラグインを調整できるように、Session Manager プラグインのソースコードが GitHub に用意されています。含めることを希望する変更について、プルリクエストを送信することをお勧めします。ただし、Amazon Web Services はこのソフトウェアの変更されたコピーの実行をサポートしていません。

(オプション) Session Manager プラグインのログ記録を有効にする

Session Manager プラグインには、実行するセッションのログ記録を有効にするオプションが含まれています。デフォルトでは、ログは無効化されています。

ログ記録を有効にすると、Session Manager プラグインは、ローカルマシン上のアプリケーションアクティビティ (`session-manager-plugin.log`) とエラー (`errors.log`) のログファイルを作成します。

トピック

- Session Manager プラグインのログ記録を有効にする (Windows)

- Session Manager プラグインのログ記録を有効にする (Linux および macOS)

Session Manager プラグインのログ記録を有効にする (Windows)

1. プラグインの `seelog.xml.template` ファイルを探します。

   デフォルトの場所は `C:\Program Files\Amazon\SessionManagerPlugin\seelog.xml.template` です。
2. ファイルの名前を `seelog.xml` に変更します。
3. ファイルを開き、`minlevel="off"` を `minlevel="info"` または `minlevel="debug"` に変更します。

   > **Note**
   >
   > デフォルトでは、データチャネルのオープンとセッションの再接続に関するログエントリは、INFO レベルで記録されます。データフロー (パケットおよび送達確認) エントリは、DEBUG レベルで記録されます。

4. 変更が必要なその他の設定オプションを変更します。変更できるオプションには、次のようなものがあります。

   - デバッグレベル: デバッグレベルを `formatid="fmtinfo"` から `formatid="fmtdebug"` に変更することができます。
   - ログファイルのオプション: ログファイルの保存場所を含むログファイルオプションを変更できます (ログファイル名を除く)。

     > **Important**
     >
     > ファイル名を変更しないでください。ログが正しく機能しなくなります。

     ```
     <rollingfile type="size" filename="C:\Program Files\Amazon\SessionManagerPlugin
     \Logs\session-manager-plugin.log" maxsize="30000000" maxrolls="5"/>
     <filter levels="error,critical" formatid="fmterror">
     <rollingfile type="size" filename="C:\Program Files\Amazon\SessionManagerPlugin
     \Logs\errors.log" maxsize="10000000" maxrolls="5"/>
     ```

5. ファイルを保存します。

Session Manager プラグインのログ記録を有効にする (Linux および macOS)

1. プラグインの `seelog.xml.template` ファイルを探します。

   デフォルトの場所は `/usr/local/sessionmanagerplugin/seelog.xml.template` です。

2. ファイルの名前を `seelog.xml` に変更します。

3. ファイルを開き、`minlevel="off"` を `minlevel="info"` または `minlevel="debug"` に変更します。

   > **Note**
   >
   > デフォルトでは、データチャネルのオープンとセッションの再接続に関するログエントリは、INFO レベルで記録されます。データフロー (パケットおよび送達確認) エントリは、DEBUG レベルで記録されます。

4. 変更が必要なその他の設定オプションを変更します。変更できるオプションには、次のようなものがあります。

   - デバッグレベル: デバッグレベルを `formatid="fmtinfo"` から `outputs formatid="fmtdebug"` に変更することができます。
   - ログファイルのオプション: ログファイルの保存場所を含むログファイルオプションを変更できます (ログファイル名を除く)。

     > **Important**
     >
     > ファイル名を変更しないでください。ログが正しく機能しなくなります。

```
<rollingfile type="size" filename="/usr/local/sessionmanagerplugin/logs/session-
manager-plugin.log" maxsize="30000000" maxrolls="5"/>
<filter levels="error,critical" formatid="fmterror">
<rollingfile type="size" filename="/usr/local/sessionmanagerplugin/logs/
errors.log" maxsize="10000000" maxrolls="5"/>
```

> **Important**
>
> ログを保存するために指定されたデフォルトのディレクトリを使用する場合は、sudo を使用してセッションコマンドを実行するか、プラグインがインストールされているディレクトリに完全な読み取りおよび書き込みのアクセス権限を与える必要があります。これらの制限を回避するには、ログを保存する場所を変更します。

5. ファイルを保存します。

セッションを開始する

AWS Systems Manager コンソール、Amazon Elastic Compute Cloud (Amazon EC2) コンソール、AWS Command Line Interface (AWS CLI)、または SSH を使用してセッションを開始できます。

トピック

- セッションを開始する (Systems Manager コンソール)
- セッションを開始する (Amazon EC2 コンソール)
- セッションの開始 (AWS CLI)
- セッションの開始 (SSH)
- セッションの開始 (ポート転送)
- セッションの開始 (リモートホストへのポート転送)
- セッションの開始 (対話形式と非対話形式のコマンド)

セッションを開始する (Systems Manager コンソール)

AWS Systems Manager コンソールを使用してアカウント内のマネージドノードとセッションを開始できます。

> **Note**
>
> セッションを開始する前に、Session Manager のセットアップ手順を完了していることを確認してください。詳細については、Session Manager を設定する を参照してください。

セッションを開始する方法 (Systems Manager コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Session Manager] を選択します。
3. [Start session (セッションの開始)] を選択します。
4. (オプション) [セッションの理由] フィールドにセッションの説明を入力します。
5. [ターゲットインスタンス] の場合、接続先のマネージドノードの左側にあるオプションボタンを選択します。

   目的のノードがリストにない場合や、ノードを選択して設定エラーが表示される場合は、トラブルシューティングの手順について「Session Manager が使用できない、または使用に設定されていないマネージドノード。」を参照してください。
6. [セッションを開始] を選択すると、セッションがすぐに開始されます。

   -または-

   セッションオプションで [次へ] を選択します。
7. (オプション) [セッションドキュメント] では、セッションの開始時に実行するドキュメントを選択します。ドキュメントがランタイムパラメータをサポートしている場合は、各パラメータフィールドに 1 つ以上の値をカンマで区切って入力できます。
8. [Next] を選択します。
9. [Start session (セッションの開始)] を選択します。

接続が確立されたら、他の接続タイプと同様に、bash コマンド (Linux および macOS) または PowerShell コマンド (Windows) を実行できます。

> **Important**
>
> Session Manager コンソールでセッションを開始するときにユーザーがドキュメントを指定できるようにするには、次の点に注意してください。
>
> - IAM ポリシーでユーザーに `ssm:GetDocument` および `ssm:ListDocuments` 許可を付与する必要があります。詳細については、「コンソールでカスタムセッションドキュメントへのアクセスを許可する」を参照してください。

- コンソールは、`Standard_Stream` として定義されている `sessionType` を持つセッションドキュメントのみをサポートします。詳細については、「セッションドキュメントスキーマ」を参照してください。

セッションを開始する (Amazon EC2 コンソール)

Amazon Elastic Compute Cloud (Amazon EC2) コンソールを使用して、アカウント内のインスタンスとのセッションを開始できます。

> **Note**
>
> Systems Manager アクション (`ssm:command-name`) を実行する権限がないというエラーが表示された場合、管理者に問い合わせ、サポートを依頼する必要があります。管理者とは、サインイン認証情報を提供した担当者です。ポリシーを更新して、Amazon EC2 コンソールからセッションを開始できるようにしてもらいます。管理者の場合は、「Session Manager のサンプル IAM ポリシー」を参照してください。

セッションを開始するには (Amazon EC2 コンソール)

1. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
2. ナビゲーションペインで、[インスタンス] を選択します。
3. インスタンスを選択し、[接続] を選択します。
4. [Connection method (接続方法)] で、[Session Manager] を選択します。
5. [接続]を選択します。

接続が確立されたら、他の接続タイプと同様に、bash コマンド (Linux および macOS) または PowerShell コマンド (Windows) を実行できます。

セッションの開始 (AWS CLI)

まだ AWS Command Line Interface (AWS CLI) をインストールして設定していない場合は、インストールして設定します。

詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」を参照してください。

セッションを開始する前に、Session Manager のセットアップ手順を完了していることを確認してください。詳細については、Session Manager を設定する を参照してください。

AWS CLI を使用してセッションコマンドを実行するには、ローカルマシンにも Session Manager プラグインがインストールされている必要があります。詳細については、AWS CLI 用の Session Manager プラグインをインストールする を参照してください。

AWS CLI を使用してセッションを開始するには、「*instance-id*」をユーザー自身の情報で置き換えて、次のコマンドを実行します。

```
aws ssm start-session \
    --target instance-id
```

start-session コマンドで使用できるその他のオプションについては、AWS CLI コマンドリファレンスの AWS Systems Manager のセクションの「start-session」を参照してください。

セッションの開始 (SSH)

Session Manager SSH セッションを開始する場合、SSM Agent のバージョン 2.3.672.0 以降がマネージドノードにインストールされている必要があります。

SSH 接続の要件

SSH を使用したセッション接続に関する次の要件と制限事項に注意してください。

- ターゲットのマネージドノードは SSH 接続をサポートするように設定する必要があります。詳細については、「(オプション) Session Manager を通して SSH 接続のアクセス許可を付与して制御する」を参照してください。
- 他のタイプのセッション接続に使用される `ssm-user` アカウントではなく、Privacy Enhanced Mail (PEM) 証明書に関連付けされたマネージドノードのアカウントで接続する必要があります。例えば、Linux および macOS の EC2 インスタンスでは、デフォルトのユーザーは `ec2-user` です。各インスタンスタイプのデフォルトのユーザーを特定する方法については、「Amazon EC2 ユーザーガイド」の「インスタンスに関する情報を取得する」を参照してください。
- ログ記録は、ポート転送または SSH を介して接続する Session Manager セッションでは使用できません。これは、SSH はすべてのセッションデータを暗号化し、Session Manager は SSH 接続のトンネルとしてのみ機能するためです。

> **Note**
>
> セッションを開始する前に、Session Manager のセットアップ手順を完了していることを確認してください。詳細については、Session Manager を設定する を参照してください。

SSH を使用してセッションを開始するには、次のコマンドを実行します。各##############をユーザー自身の情報に置き換えます。

```
ssh -i /path/my-key-pair.pem username@instance-id
```

> **Tip**
>
> SSH でセッションを開始する際、以下のコマンド形式を使用してローカルファイルをターゲットのマネージドノードにコピーできます。
>
> ```
> scp -i /path/my-key-pair.pem /path/ExampleFile.txt username@instance-id:~
> ```

start-session コマンドで使用できるその他のオプションについては、AWS CLI コマンドリファレンスの AWS Systems Manager のセクションの「start-session」を参照してください。

セッションの開始 (ポート転送)

Session Manager ポート転送セッションを開始する場合、SSM Agent のバージョン 2.3.672.0 以降がマネージドノードにインストールされている必要があります。

> **Note**
>
> セッションを開始する前に、Session Manager のセットアップ手順を完了していることを確認してください。詳細については、Session Manager を設定する を参照してください。
> AWS CLI を使用してセッションコマンドを実行するには、ローカルマシンにも Session Manager プラグインをインストールする必要があります。詳細については、AWS CLI 用の Session Manager プラグインをインストールする を参照してください。
> オペレーティングシステムおよびコマンドラインツールによっては、引用符の配置が異なり、エスケープ文字が必要になる場合があります。

ポート転送セッションを開始するには、CLI から次のコマンドを実行します。各*############*をユーザー自身の情報に置き換えます。

Linux & macOS

```
aws ssm start-session \
    --target instance-id \
    --document-name AWS-StartPortForwardingSession \
    --parameters '{"portNumber":["80"], "localPortNumber":["56789"]}'
```

Windows

```
aws ssm start-session ^
    --target instance-id ^
    --document-name AWS-StartPortForwardingSession ^
    --parameters portNumber="3389",localPortNumber="56789"
```

`portNumber` は、セッショントラフィックをリダイレクトするマネージドノードのリモートポートです。例えば、リモートデスクトッププロトコル (RDP) を使用した Windows ノードへの接続にポート 3389 を指定する場合があります。`portNumber` パラメータを指定しない場合、Session Manager はデフォルトの値として `80` を使用します。

`localPortNumber` は、トラフィックが開始されるローカルコンピュータのポート (56789 など) です。この値は、クライアントを使用してマネージドノードに接続する際に入力します。例えば、**`localhost:56789`** と指定します。

start-session コマンドで使用できるその他のオプションについては、AWS CLI コマンドリファレンスの AWS Systems Manager のセクションの「start-session」を参照してください。

ポート転送セッションの詳細については、AWS ニュースブログの「AWS Systems ManagerSession Manager を使用したポート転送」を参照してください。

セッションの開始 (リモートホストへのポート転送)

リモートホストへの Session Manager ポート転送セッションを開始するには、SSM Agent のバージョン 3.1.1374.0 以降がマネージドノードにインストールされている必要があります。リモートホストは Systems Manager によって管理される必要はありません。

> **Note**
>
> セッションを開始する前に、Session Manager のセットアップ手順を完了していることを確認してください。詳細については、Session Manager を設定する を参照してください。
> AWS CLI を使用してセッションコマンドを実行するには、ローカルマシンにも Session Manager プラグインをインストールする必要があります。詳細については、AWS CLI 用の Session Manager プラグインをインストールする を参照してください。
> オペレーティングシステムおよびコマンドラインツールによっては、引用符の配置が異なり、エスケープ文字が必要になる場合があります。

ポート転送セッションを開始するには、AWS CLI から次のコマンドを実行します。各*##############*をユーザー自身の情報に置き換えます。

Linux & macOS

```
aws ssm start-session \
    --target instance-id \
    --document-name AWS-StartPortForwardingSessionToRemoteHost \
    --parameters '{"host":["mydb.example.us-east-2.rds.amazonaws.com"],"portNumber":
["3306"], "localPortNumber":["3306"]}'
```

Windows

```
aws ssm start-session ^
    --target instance-id ^
    --document-name AWS-StartPortForwardingSessionToRemoteHost ^
    --parameters host="mydb.example.us-
east-2.rds.amazonaws.com",portNumber="3306",localPortNumber="3306"
```

host の値は、接続するリモートホストのホスト名または IP アドレスを表します。マネージドノードとリモートホスト間の一般的な接続および名前解決の要件が引き続き適用されます。

portNumber は、セッショントラフィックをリダイレクトするマネージドノードのリモートポートです。例えば、リモートデスクトッププロトコル (RDP) を使用した Windows ノードへの接続にポート 3389 を指定する場合があります。portNumber パラメータを指定しない場合、Session Manager はデフォルトの値として 80 を使用します。

`localPortNumber` は、トラフィックが開始されるローカルコンピュータのポート (56789 など) です。この値は、クライアントを使用してマネージドノードに接続する際に入力します。例えば、**`localhost:56789`** と指定します。

start-session コマンドで使用できるその他のオプションについては、AWS CLI コマンドリファレンスの AWS Systems Manager のセクションの「start-session」を参照してください。

Amazon ECS タスクを使用してセッションを開始する

Session Manager は、Amazon Elastic Container Service (Amazon ECS) クラスター内のタスクによるポート転送セッションの開始をサポートします。それを実行するには、IAM 内のタスクロールを更新して以下のアクセス許可を含めます。

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
       "Effect": "Allow",
       "Action": [
            "ssmmessages:CreateControlChannel",
            "ssmmessages:CreateDataChannel",
            "ssmmessages:OpenControlChannel",
            "ssmmessages:OpenDataChannel"
       ],
      "Resource": "*"
      }
   ]
}
```

Amazon ECS タスクを使用してポート転送セッションを開始するには、AWS CLI から次のコマンドを実行します。各##############をユーザー自身の情報に置き換えます。

> **Note**
>
> `target` パラメータから < and > 記号を削除します。これらの記号は読者への説明のみを目的としています。

Linux & macOS

```
aws ssm start-session \
```

```
    --target ecs:<ECS_cluster_name>_<ECS_container_ID>_<container_runtime_ID> \
    --document-name AWS-StartPortForwardingSessionToRemoteHost \
    --parameters '{"host":["URL"],"portNumber":["port_number"], "localPortNumber":
["port_number"]}'
```

Windows

```
aws ssm start-session ^
    --target ecs:<ECS_cluster_name>_<ECS_container_ID>_<container_runtime_ID> ^
    --document-name AWS-StartPortForwardingSessionToRemoteHost ^
    --parameters host="URL",portNumber="port_number",localPortNumber="port_number"
```

セッションの開始 (対話形式と非対話形式のコマンド)

セッションを開始する前に、Session Manager のセットアップ手順を完了していることを確認してください。詳細については、Session Manager を設定する を参照してください。

AWS CLI を使用してセッションコマンドを実行するには、ローカルマシンにも Session Manager プラグインがインストールされている必要があります。詳細については、AWS CLI 用の Session Manager プラグインをインストールする を参照してください。

インタラクティブ・コマンドセッションを開始する場合、以下のコマンドを実行します。各*##########*をユーザー自身の情報に置き換えます。

Linux & macOS

```
aws ssm start-session \
    --target instance-id \
    --document-name CustomCommandSessionDocument \
    --parameters '{"logpath":["/var/log/amazon/ssm/amazon-ssm-agent.log"]}'
```

Windows

```
aws ssm start-session ^
    --target instance-id ^
    --document-name CustomCommandSessionDocument ^
    --parameters logpath="/var/log/amazon/ssm/amazon-ssm-agent.log"
```

start-session コマンドで使用できるその他のオプションについては、AWS CLI コマンドリファレンスの AWS Systems Manager のセクションの「start-session」を参照してください。

詳細情報

- AWS Systems ManagerSession Manager でポート転送を使用してリモートホストに接続する
- AWS Systems Manager を使用した Amazon EC2 インスタンスのポート転送
- Session Manager ポート転送による AWS Managed Microsoft AD リソースの管理
- AWS ニュースブログの AWS Systems ManagerSession Manager を使用したポート転送

セッションを終了する

AWS Systems Manager コンソールまたは AWS Command Line Interface (AWS CLI) を使用して、アカウントで開始したセッションを終了できます。コンソールでセッションの [終了] ボタンを選択するか、AWS CLI を使用して TerminateSession API アクションを呼び出すと、Session Manager はセッションを完全に終了し、Session Manager クライアントとマネージドノード上の SSM Agent の間のデータ接続を閉じます。終了したセッションを再開することはできません。

開いているセッションで 20 分間ユーザーアクティビティがない場合、アイドル状態によってタイムアウトがトリガーされます。Session Manager は `TerminateSession` を呼び出しませんが、基盤となるチャネルを閉じます。アイドルタイムアウトで終了したセッションを再開することはできません。

AWS CLI を使用する場合は `terminate-session` コマンドを、コンソールを使用する場合は [終了] ボタンを使用して、常に明示的にセッションを終了することをお勧めします。([終了] ボタンはセッションウィンドウとメイン Session Manager コンソールページの両方にあります)。ブラウザまたはコマンドウィンドウのみを閉じると、セッションはコンソールに [アクティブ] として 30 日間表示されます。セッションを明示的に終了しない場合、またはセッションがタイムアウトした場合、その時点でマネージドノードで実行されていたプロセスは引き続き実行されます。

トピック

- セッションの開始 (コンソール)
- セッション (AWS CLI) を終了する

セッションの開始 (コンソール)

AWS Systems Manager コンソールを使用して、アカウントで開始したセッションを終了できます。

セッションを終了するには (コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Session Manager] を選択します。
3. [Sessions (セッション)] で、終了するセッションの左にあるオプションボタンを選択します。
4. [Terminate] を選択します。

セッション (AWS CLI) を終了する

AWS CLI を使用してセッションを終了するには、次のコマンドを実行します。「*session-id*」を、ユーザー自身の情報に置き換えます。

```
aws ssm terminate-session \
    --session-id session-id
```

terminate-session コマンドの詳細については、AWS CLI コマンドリファレンスの「AWS Systems Manager」セクションの「terminate-session」を参照してください。

セッション履歴を表示する

AWS Systems Manager コンソールまたは AWS Command Line Interface (AWS CLI) を使用して、アカウント内のセッションについての詳細を表示できます。コンソールでは、次のようなセッションの詳細を表示できます。

- セッションの ID
- セッションを介してマネージドノードに接続したユーザー
- マネージドノードの ID
- セッションの開始時刻と終了時刻
- セッションのステータス
- セッションログの保存に指定された場所 (有効な場合)

AWS CLI を使用すると、アカウント内のセッションの一覧は表示できますが、コンソールで使用可能な追加の詳細は表示されません。

ログ作成セッション履歴の詳細については、「セッションロギングの有効化と無効化」を参照してください。

トピック

- セッション履歴の表示 (コンソール)
- セッション履歴の表示 (AWS CLI)

セッション履歴の表示 (コンソール)

AWS Systems Manager コンソールを使用して、アカウント内のセッションに関する詳細を表示することができます。

セッション履歴を表示するには (コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Session Manager] を選択します。
3. [Session history (セッション履歴)] タブを選択します。

   -または-

   Session Manager のホームページが最初に開いた場合は、[設定の指定] をクリックしてから、[セッション履歴] タブをクリックします。

セッション履歴の表示 (AWS CLI)

AWS CLI を使用してアカウント内のセッションの一覧を表示するには、次のコマンドを実行します。

```
aws ssm describe-sessions \
    --state History
```

> **Note**
>
> このコマンドは、Session Manager を使用して開始されたターゲットへの接続の結果のみを返します。リモートデスクトッププロトコル (RDP) やセキュアシェルプロトコル (SSH) など、他の手段で行われた接続は一覧表示されません。

describe-sessions コマンドで使用できるその他のオプションについては、AWS CLI コマンドリファレンスの AWS Systems Manager のセクションの「describe-sessions」を参照してください。

「セッションアクティビティのログ記録」

Session Manager は、Systems Manager コンソールで現在のセッションと完了したセッションに関する情報を提供するだけでなく、AWS CloudTrail を使用して AWS アカウントでのセッションアクティビティをログに記録する機能も提供します。

CloudTrail は、Systems Manager コンソール、AWS Command Line Interface (AWS CLI)、および Systems Manager SDK を介した API 呼び出しをキャプチャします。情報は、CloudTrail コンソールで表示することも、指定した Amazon Simple Storage Service (Amazon S3) バケットに保存することもできます。アカウントのすべての CloudTrail ログに対して 1 つの Amazon S3 バケットが使用されます。詳細については、「AWS Systems Manager による AWS CloudTrail API コールのログ記録」を参照してください。

> **Note**
>
> ログファイルの繰り返し分析、履歴分析、解析的分析では、CloudTrail Lake または維持するテーブルを使用して CloudTrail ログのクエリを実行することを検討してください。詳細については、「AWS CloudTrail ユーザーガイド」の「AWS CloudTrail ログのクエリ」を参照してください。

Amazon EventBridge を使用してセッションアクティビティをモニタリングする (コンソール)

EventBridge を使用すると、AWS リソースの変更の発生を検出するルールを設定できます。組織内のユーザーがセッションを開始または終了したタイミングを検出し、例えば、そのイベントに関する通知を Amazon SNS 経由で受信するなどのルールを作成できます。

Session Manager の EventBridge のサポートは、CloudTrail で記録された API オペレーションの記録に左右されます。(CloudTrail と EventBridge の統合を使用して、ほとんどの AWS Systems Manager のイベントに応答できます)。API 呼び出しを実行しない `exit` コマンドなど、セッション内で実行されるアクションは、EventBridge では検出されません。

以下の手順では、Session Manager API イベント (StartSession など) が発生したときに、Amazon Simple Notification Service (Amazon SNS) を通じて通知を開始する方法の概要を示します。

Amazon EventBridge を使用してセッションアクティビティをモニタリングするには (コンソール)

1. 追跡する Session Manager イベントが発生したとき、通知を送信するために使用する Amazon SNS トピックを作成します。

詳細については、Amazon Simple Notification Service デベロッパーガイドの「トピックの作成」を参照してください。

2. 追跡する Session Manager イベントのタイプの Amazon SNS ターゲットを呼び出すには、EventBridge ルールを作成します。

   ルールの作成方法に関する詳細については、Amazon EventBridge ユーザーガイドの「イベントに反応する Amazon EventBridge ルールの作成」を参照してください。

   ルールを作成するステップに従うときには、以下のように選択します。

   - [AWS のサービス] で、[Systems Manager] を選択します。
   - [イベントタイプ] で、[CloudTrail 経由の AWS API 呼び出し] を選択します。
   - [Specific operation(s) (特定のオペレーション)] を選択し、通知を受け取る Session Manager のコマンド (一度に 1 つずつ) を入力します。StartSession、ResumeSession、TerminateSession を選択できます。(EventBridge では、`Get*`、 `List*`、`Describe*` コマンドはサポートされていません)。
   - [Select a target] (ターゲットの選択) には、[SNS topic] (SNS トピック) を選択してください。[Topic (トピック)] で、ステップ 1 で作成した Amazon SNS トピックの名前を選択します。

詳細については、Amazon EventBridge ユーザーガイドおよび Amazon Simple Notification Service 入門ガイドを参照してください。

セッションロギングの有効化と無効化

セッションロギングは、Systems Manager コンソールでの現在のセッションと完了済みのセッションに関する情報を記録します。また、AWS アカウント でのセッション中に実行されるコマンドの詳細をログに記録することもできます。セッションロギングでは、以下を実行できます。

- アーカイブの目的でセッションログを作成し、保存する。
- 過去 30 日間に、Session Manager を使用してマネージドノードに実行されたすべての接続の詳細を示すレポートを生成する。
- Amazon Simple Notification Service (Amazon SNS) 通知など、AWS アカウント でのセッションロギングに関する通知を生成する。
- AWS Lambda 関数の実行、AWS CodePipeline パイプラインの開始、または AWS Systems Manager Run Command ドキュメントの実行など、セッション中に行われたアクションの結果として、AWS リソースで別のアクションを自動的に開始する。

Important

Session Manager の次の要件と制限事項に注意してください。

- Session Manager は、セッション設定に応じて、セッション中に入力したコマンドとその出力を記録します。パスワードなどの機密データがセッションログに表示されないようにするには、セッション中に機密データを入力するときに次のコマンドを使用することをお勧めします。

  Linux & macOS

  ```
  stty -echo; read passwd; stty echo;
  ```

  Windows

  ```
  $Passwd = Read-Host -AsSecureString
  ```

- Windows Server 2012 またはそれ以前を使用している場合、ログ内のデータが最適にフォーマットされていない可能性があります。最適なログ形式のために、Windows Server 2012 R2 以降の使用をお勧めします。
- Linux または macOS のマネージドノードを使用している場合は、スクリーンユーティリティがインストールされていることを確認します。インストールされていない場合、ログデータが切り捨てられることがあります。Amazon Linux 1、Amazon Linux 2、AL2023、および Ubuntu Server では、スクリーンユーティリティがデフォルトでインストールされています。スクリーンを手動でインストールするには、Linux のバージョンに応じて、`sudo yum install screen` または `sudo apt-get install screen` のいずれかを実行します。
- ログ記録は、ポート転送または SSH を介して接続する Session Manager セッションでは使用できません。これは、SSH はすべてのセッションデータを暗号化し、Session Manager は SSH 接続のトンネルとしてのみ機能するためです。

セッションデータのログ記録に Amazon S3 または Amazon CloudWatch Logs を使用するために必要なアクセス許可の詳細については、「Session Manager、Amazon S3、CloudWatch Logs (コンソール) の許可を持つIAM ロールの作成」を参照してください。

Session Manager のログ記録のオプションの詳細については、次のトピックを参照してください。

トピック

- Amazon CloudWatch Logs を使用してセッションデータをストリーミングする (コンソール)
- Amazon S3 を使用してセッションデータを log 記録する (コンソール)
- Amazon CloudWatch Logs を使用してセッションデータを log 記録する (コンソール)
- ディスクへのセッション log 記録の設定
- Session Manager 一時 log ファイルをディスクに保存する期間の調整
- CloudWatch Logs と Amazon S3 での Session Manager log ギングの無効化

Amazon CloudWatch Logs を使用してセッションデータをストリーミングする (コンソール)

セッションデータ log の連続ストリームを Amazon CloudWatch Logs に送信できます。セッションデータのストリーミングには、ユーザーがセッションで実行したコマンド、コマンドを実行したユーザーの ID、セッションデータが CloudWatch Logs にストリーミングされた時のタイムスタンプなど、重要な詳細情報が含まれます。セッションデータをストリーミングする場合、log は JSON 形式で、既存の log ソリューションとの統合に役立ちます。対話型コマンドでは、セッションデータのストリーミングはサポートされていません。

> **Note**
>
> Windows Server のマネージドノードからセッションデータをストリーミングする場合、PowerShell 5.1 以降がインストールされている必要があります。デフォルトでは、Windows Server 2016 以降には必要な PowerShell バージョンがインストールされています。ただし、Windows Server 2012 と 2012 R2 には、デフォルトで必要な PowerShell バージョンがインストールされていません。Windows Server 2012 または 2012 R2 マネージドノードの PowerShell をまだ更新していない場合、Run Command を使用して更新できます。Run Command を使用した PowerShell の更新方法については、「Run Command を使用して PowerShell を更新する」を参照してください。

> **Important**
>
> Windows Server のマネージドノードに PowerShell トランスクリプションポリシー設定が構成されている場合、セッションデータをストリーミングができません。

Amazon CloudWatch Logs を使用してセッションデータをストリーミングするには (コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Session Manager] を選択します。
3. [Preferences (設定)] タブを選択してから、[Edit (編集)] を選択します。
4. CloudWatch のログ記録で [有効にする] の横にあるチェックボックスをオンにします。
5. [Stream session logs (セッションログのストリーム)] オプションを選択します。
6. (推奨) [Allow only encrypted CloudWatch log groups (暗号化された CloudWatch ロググループのみを許可する)] の横にあるチェックボックスをオンにします。このオプションが有効になっている場合、ログデータはロググループに指定されたサーバー側の暗号化キーを使用して暗号化されます。CloudWatch Logs に送信されるログデータを暗号化しない場合は、このチェックボックスをオフにします。ロググループで暗号化が有効になっていない場合も、このチェックボックスをオフにする必要があります。
7. [CloudWatch Logs] の場合、セッションログのアップロード先である AWS アカウント の既存の CloudWatch Logs ロググループを指定するには、次のいずれかを選択します。
   - セッションログデータを保存するためにアカウントにすでに作成されているテキストボックスにロググループの名前を入力します。
   - ロググループを参照: セッションログデータを保存するためにアカウントですでに作成されているロググループを選択します。
8. [Save] を選択します。

Amazon S3 を使用してセッションデータを ログ記録する (コンソール)

デバッグおよびトラブルシューティングの目的で、指定した Amazon Simple Storage Service (Amazon S3) バケットにセッションログデータを保存することができます。デフォルトのオプションでは、ログは暗号化された Amazon S3 バケットに送信されます。暗号化は、AWS KMS key または Amazon S3 サーバー側暗号化 (SSE) キー (AES-256) のいずれかで、バケットに指定されたキーを使用して実行されます。

> **Important**
>
> 仮想ホスティング形式のバケットを Secure Sockets Layer (SSL) で使用する場合、SSL ワイルドカード証明書はピリオドを含まないバケットにのみ一致します。この問題を回避するには、HTTP を使用するか、または独自の証明書検証ロジックを記述します。仮想ホスティン

グ形式のバケットを使用するときは、バケット名にピリオド (「.」) を使用しないことをお勧めします。

Amazon S3 バケットの暗号化

暗号化を使用して Amazon S3 バケットにログを送信するには、バケット上で暗号化を有効にする必要があります。S3 バケットの暗号化の詳細については、「Amazon S3 バケット用の Amazon S3 デフォルト暗号化」を参照してください。

カスタマー管理のキー

ユーザー自身が管理する KMS キーを使用してバケットを暗号化する場合、インスタンスにアタッチされた IAM インスタンスプロファイルには、キーを読み取るための明示的なアクセス許可が必要です。AWS マネージドキーを使用している場合は、インスタンスにこの明示的なアクセス許可は必要ありません。インスタンスプロファイルに CMK 使用のためのアクセスを提供する方法の詳細については、AWS Key Management Service デベロッパーガイドのキーユーザーにキーの使用を許可するを参照してください。

Amazon S3 バケットにセッションログを保存するように Session Manager を設定するには、次の手順に従います。

> **Note**
>
> AWS CLI を使用して、セッションデータ送信先の Amazon S3 バケットを指定したり変更したりすることもできます。詳細については、Session Manager 設定の更新 (コマンドライン) を参照してください。

Amazon S3 を使用してセッションデータをログに記録するには (コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Session Manager] を選択します。
3. [Preferences (設定)] タブを選択してから、[Edit (編集)] を選択します。
4. [S3 ロギング] で [有効にする] チェックボックスをオンにします。
5. (推奨) [Allow only encrypted S3 buckets (暗号化された S3 バケットのみを許可する)] の横にあるチェックボックスをオンにします。このオプションが有効になっている場合、ログデータはバ

ケットに指定されたサーバー側の暗号化キーを使用して暗号化されます。Amazon S3 に送信されるログデータを暗号化しない場合は、このチェックボックスをオフにします。S3 バケットで暗号化が有効になっていない場合も、このチェックボックスをオフにする必要があります。

6. [S3 bucket name (S3 バケット名)] には、次のいずれかを選択します。

> **Note**
>
> 仮想ホスティング形式のバケットを使用するときは、バケット名にピリオド (「.」) を使用しないことをお勧めします。Amazon S3 バケット命名規則の詳細については、Amazon Simple Storage Service ユーザーガイドの「バケットの制約と制限」を参照してください。

- [Choose a bucket name from the list (リストからバケット名を選択)]: アカウントに既に作成された Amazon S3 バケットを選択してセッションログデータを保存します。
- [Enter a bucket name in the text box (テキストボックスにバケット名を入力)]: セッションログデータを保存するためにアカウントに既に作成されている Amazon S3 バケットの名前を入力します。

7. (オプション) [S3 key prefix (S3 キープレフィックス)] には、選択したバケットにログを保存する既存のフォルダまたは新しいフォルダの名前を入力します。
8. [保存] を選択します。

Amazon S3 および Amazon S3 バケットの使用の詳細については、Amazon Simple Storage Service ユーザーガイドおよび Amazon Simple Storage Service ユーザーガイドを参照してください。

Amazon CloudWatch Logs を使用してセッションデータを ログ記録する (コンソール)

Amazon CloudWatch Logs を使用すると、さまざまな AWS のサービス からのログファイルについて、モニタリング、保存、アクセスを行うことができます。デバッグおよびトラブルシューティングの目的で、セッションログデータを CloudWatch Logs ロググループに送信できます。デフォルトのオプションでは、KMS キーを使用してログデータを暗号化して送信するように設定されていますが、暗号化の有無にかかわらずデータをロググループに送信できます。

セッションの最後にセッションログデータを CloudWatch Logs ロググループに送信するように AWS Systems Manager Session Manager を設定するには、以下の手順を実行します。

> **Note**
>
> AWS CLI を使用して、セッションデータの送信先の CloudWatch Logs ロググループを指定したり変更したりすることもできます。詳細については、Session Manager 設定の更新 (コマンドライン) を参照してください。

Amazon CloudWatch Logs を使用してセッションデータを口グ記録するには (コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Session Manager] を選択します。
3. [Preferences (設定)] タブを選択してから、[Edit (編集)] を選択します。
4. CloudWatch のロ グ記録で [有効にする] の横にあるチェックボックスをオンにします。
5. [セッションログをアップロード] オプションを選択します。
6. (推奨) [Allow only encrypted CloudWatch log groups (暗号化された CloudWatch ロググループのみを許可する)] の横にあるチェックボックスをオンにします。このオプションが有効になっている場合、ログデータはロググループに指定されたサーバー側の暗号化キーを使用して暗号化されます。CloudWatch Logs に送信されるログデータを暗号化しない場合は、このチェックボックスをオフにします。ロググループで暗号化が有効になっていない場合も、このチェックボックスをオフにする必要があります。
7. [CloudWatch Logs] の場合、セッションログのアップロード先である AWS アカウント の既存の CloudWatch Logs ロググループを指定するには、次のいずれかを選択します。
   - [Choose a log group from the list (リストからロググループを選択する)]: アカウントに既に作成されたロググループを選択してセッションログデータを保存します。
   - [Enter a log group name in the text box (テキストボックスにロググループ名を入力)]: セッションログデータを保存するためにアカウントにすでに作成されているロググループの名前を入力します。
8. [Save] を選択します。

CloudWatch Logs の使用の詳細については、Amazon CloudWatch Logs ユーザーガイドを参照してください。

ディスクへのセッションログ記録の設定

CloudWatch または Amazon S3 への Session Manager ログ記録を有効にすると、セッション中に実行されたすべてのコマンド (およびそれらのコマンドの出力結果) が、ターゲットインスタンスのディスク上の一時ファイルにログ記録されます。一時ファイルの名前は ipcTempFile.log です。

ipcTempFile.log は、SSM Agent 設定ファイルの SessionLogsDestination パラメータによって制御されます。このパラメータには、次の値を指定できます。

- disk: このパラメータを指定し、CloudWatch または Amazon S3 へのセッションログ記録が有効になっている場合、SSM Agent は ipcTempFile.log という一時ログファイルを作成し、セッションコマンドと出力をディスクにログ記録します。Session Manager は、ログ記録設定に応じて、セッション中またはセッション後にこのログを CloudWatch または S3 にアップロードします。その後、このログは、SSM Agent の SessionLogsRetentionDurationHours 設定パラメータに指定された期間に基づいて削除されます。

  このパラメータを指定し、CloudWatch と Amazon S3 へのセッションログ記録が無効になっている場合でも、SSM Agent はコマンド履歴と出力を ipcTempFile.log ファイルにログ記録します。ファイルは、SSM Agent の SessionLogsRetentionDurationHours 設定パラメータに指定された期間に基づいて削除されます。
- none: このパラメータを指定し、CloudWatch または Amazon S3 へのセッションログ記録が有効になっている場合、ディスクへのログ記録は、disk パラメータを指定した場合とまったく同じように機能します。CloudWatch または Amazon S3 へのセッションログ記録が有効になっている場合、SSM Agent は一時ファイルを必要とします。

  このパラメータを指定し、CloudWatch または Amazon S3 へのセッションログ記録が無効になっている場合、SSM Agent は ipcTempFile.log ファイルを作成しません。

セッション開始時のディスクへの ipcTempFile.log 一時ログファイルの作成を有効または無効にするには、次の手順を使用します。

ディスクへの Session Manager 一時ログファイルの作成を有効または無効にする手順

1. インスタンスに SSM Agent をインストールするか、バージョン 3.2.2086 以降にアップグレードします。エージェントのバージョン番号を確認する方法については、「SSM Agent バージョン番号の確認」を参照してください。エージェントを手動でインストールする方法については、以下のセクションでご使用のオペレーティングシステムに対応した手順を確認してください。

   - Linux 用 EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする

- macOS 用の EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする
- Windows Server 用の EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする

2. インスタンスに接続し、以下の場所で `amazon-ssm-agent.json` ファイルを見つけます。

   - Linux: /etc/amazon/ssm/
   - macOS: /opt/aws/ssm/
   - Windows Server: C:\Program Files\Amazon\SSM

   `amazon-ssm-agent.json` ファイルが存在しない場合は、`amazon-ssm-agent.json.template` のコンテンツを同じディレクトリ内の新しいファイルにコピーします。この新しいファイルに `amazon-ssm-agent.json` という名前を付けます。

3. none パラメータには、`disk` または `SessionLogsDestination` のいずれかを指定します。変更内容を保存します。

4. SSM Agent を再起動します。

`SessionLogsDestination` パラメータに `disk` を指定した場合は、新しいセッションを開始して以下の場所で `ipcTempFile.log` を見つけることで、SSM Agent が一時ログファイルを作成することを確認できます。

- Linux: /var/lib/amazon/ssm/***##### ID***/session/orchestration/***##### ID***/Standard_Stream/ipcTempFile.log
- macOS: /opt/aws/ssm/data/***##### ID***/session/orchestration/***##### ID***/Standard_Stream/ipcTempFile.log
- Windows Server: C:\ProgramData\Amazon\SSM\InstanceData***##### ID***\session\orchestration***### ID***\Standard_Stream\ipcTempFile.log

> **Note**
>
> デフォルトでは、一時ログファイルはインスタンスに 14 日間保存されます。

複数のインスタンスで SessionLogsDestination パラメータを更新する場合は、新しい設定を指定する SSM ドキュメントを作成することをお勧めします。その後、Systems Manager の Run Command を使用してインスタンスに変更を実装できます。詳細については、「Writing your own AWS Systems Manager documents (ブログ)」および「マネージドノードでのコマンドの実行」を参照してください。

Session Manager 一時ログファイルをディスクに保存する期間の調整

CloudWatch または Amazon S3 への Session Manager ログ記録を有効にすると、セッション中に実行されたすべてのコマンド (およびそれらのコマンドの出力結果) が、ターゲットインスタンスのディスク上の一時ファイルにログ記録されます。一時ファイルの名前は ipcTempFile.log です。セッション中、またはセッションの完了後に、Session Manager はこの一時ログを CloudWatch または S3 にアップロードします。その後、SSM Agent の SessionLogsRetentionDurationHours 設定パラメータで指定された期間に基づいて一時ログが削除されます。デフォルトでは、一時ログファイルはインスタンスの次の場所に 14 日間保存されます。

- Linux: /var/lib/amazon/ssm/##### *ID*/session/orchestration/##### *ID*/Standard_Stream/ipcTempFile.log
- macOS: /opt/aws/ssm/data/##### *ID*/session/orchestration/##### *ID*/Standard_Stream/ipcTempFile.log
- Windows Server: C:\ProgramData\Amazon\SSM\InstanceData\##### *ID*\session\orchestration\##### *ID*\Standard_Stream\ipcTempFile.log

Session Manager 一時ログファイルがディスクに保存される期間を調整するには、次の手順を使用します。

ディスクに **ipcTempFile.log** ファイルを保存する期間を調整する手順

1. インスタンスに接続し、以下の場所で amazon-ssm-agent.json ファイルを見つけます。
   - Linux: /etc/amazon/ssm/
   - macOS: /opt/aws/ssm/
   - Windows Server: C:\Program Files\Amazon\SSM

amazon-ssm-agent.json ファイルが存在しない場合は、amazon-ssm-agent.json.template のコンテンツを同じディレクトリ内の新しいファイルにコピーします。この新しいファイルに amazon-ssm-agent.json という名前を付けます。

2. SessionLogsRetentionDurationHours の値を目的の時間数に変更します。SessionLogsRetentionDurationHours を 0 に設定した場合、一時ログファイルはセッション中に作成され、セッションの完了時に削除されます。この設定により、セッション終了後にログファイルが保持されないようにすることができます。
3. 変更内容を保存します。
4. SSM Agent を再起動します。

CloudWatch Logs と Amazon S3 での Session Manager ロギングの無効化

アカウントでセッションロギングを無効にするには、Systems Manager コンソールまたは AWS CLI を使用できます。

セッションロギングを無効にする (コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Session Manager] を選択します。
3. [設定] タブを選択してから、[編集] を選択します。
4. CloudWatch ロギングを無効にするには、[CloudWatch ロギング] セクションで、[有効化] チェックボックスをオフにします。
5. S3 ロギングを無効にするには、[S3 ロギング] セクションで、[有効化] チェックボックスをオフにします。
6. [Save] を選択します。

セッションロギングを無効にする (AWS CLI)

AWS CLI を使用してセッションロギングを無効にするには、「Session Manager 設定の更新 (コマンドライン)」の手順を実行してください。

JSON ファイルで、s3BucketName と cloudWatchLogGroupName の入力には値が含まれないようにしてください。以下に例を示します。

```
"inputs": {
        "s3BucketName": "",
        ...
        "cloudWatchLogGroupName": "",
        ...
    }
```

代わりに、S3* および cloudWatch* のすべての入力を JSON ファイルから削除することで、ロギングを無効にすることもできます。

> **Note**
>
> 設定によっては、CloudWatch または S3 を無効にした後も、SSM Agent によって一時ログファイルがディスクに生成される場合があります。ディスクへのロギングを無効にする方法については、「ディスクへのセッションログ記録の設定」を参照してください。

セッションドキュメントスキーマ

次の情報では、セッションドキュメントのスキーマ要素について説明します。AWS Systems Manager Session Manager では、セッションドキュメントを使用して、標準セッション、ポート転送セッション、対話型コマンドを実行するセッションなど、開始するセッションの種類を決定します。

schemaVersion

セッションドキュメントのスキーマバージョン。セッションドキュメントはバージョン 1.0 のみがサポートされています。

型: 文字列

必須: はい

description

セッションドキュメントついてに指定する説明。たとえば、「Session Manager でポート転送セッションを開始するドキュメント」などです。

タイプ: 文字列。

必須: いいえ

sessionType

セッションドキュメントを確立するために使用されるセッションの種類。

型: 文字列

必須: はい

有効な値: `InteractiveCommands` | `NonInteractiveCommands` | `Port` | `Standard_Stream`

inputs

このセッションドキュメントを使用して確立されたセッションに使用するセッション設定。`Standard_Stream` セッションの作成に使用されるセッションドキュメントの場合、この要素は必要です。

型: StringMap

必須: いいえ

s3BucketName

セッションの最後にセッションログを送信する宛先となる Amazon Simple Storage Service (Amazon S3) バケット。

型: 文字列

必須: いいえ

s3KeyPrefix

`s3BucketName` 入力で指定した Amazon S3 バケットにログを送信するときに使用するプレフィックス。Amazon S3 に保存されたオブジェクトで共有プレフィックスを使用する方法の詳細については、Amazon Simple Storage Service ユーザーガイドの「S3 バケットのフォルダの使用方法」を参照してください。

タイプ: 文字列。

必須: いいえ

s3EncryptionEnabled

`true` に設定すると、 `s3BucketName` 入力で指定した Amazon S3 バケットは暗号化する必要があります。

タイプ: ブール値

必須: はい

cloudWatchLogGroupName

セッションの最後にセッションログを送信する宛先となる Amazon CloudWatch Logs (CloudWatch Logs) グループの名前。

型: 文字列

必須: いいえ

cloudWatchEncryptionEnabled

`true` に設定すると、 `cloudWatchLogGroupName` 入力で指定したロググループは暗号化する必要があります。

タイプ: ブール値

必須: はい

cloudWatchStreamingEnabled

`true` に設定すると、セッションデータログの連続ストリームが、`cloudWatchLogGroupName` 入力で指定したロググループに送信されます。`false` に設定した場合、セッションログは、セッションの終了時に `cloudWatchLogGroupName` 入力で指定したロググループに送信されます。

タイプ: ブール値

必須: はい

kmsKeyId

ローカルクライアントマシンと接続先の Amazon Elastic Compute Cloud (Amazon EC2) マネージドノード間のデータをさらに暗号化するために使用する AWS KMS key の ID。

タイプ: 文字列。

必須: いいえ

runAsEnabled

`true` に設定した場合、 `runAsDefaultUser` 入力で接続先のマネージドノードに存在するユーザーアカウントを指定する必要があります。そうしないと、セッションが開始されません。デフォルトでは、AWS Systems Manager SSM Agent によって作成された `ssm-user` ア

カウントを使用してセッションが開始されます。Run As 機能は Linux および macOS のマネージドノードに接続する場合のみサポートされます。

型: ブール値

必須: はい

runAsDefaultUser

runAsEnabled 入力が true に設定されている場合、Linux および macOS のマネージドノードでセッションを開始するユーザーアカウント名。この入力に指定するユーザーアカウントは接続先のマネージドノードに存在する必要があります。存在しない場合、セッションが開始されません。

タイプ: 文字列。

必須: いいえ

idleSessionTimeout

セッションが終了する前に許可する非アクティブの時間。この入力は分単位で測定されます。

型: 文字列

有効な値: 1 ~ 60

必須: いいえ

maxSessionDuration

セッションが終了する前に許可する最大時間。この入力は分単位で測定されます。

タイプ: 文字列。

有効な値: 1 ~ 1440

必須: いいえ

shellProfile

シェルプリファレンス、環境変数、作業ディレクトリ、セッション開始時の複数のコマンドの実行など、セッション内で適用する、オペレーティングシステムごとに指定する設定。

型: StringMap

必須: いいえ

windows

Windows Server のマネージドノード上のセッションに指定するシェルプリファレンス、環境変数、作業ディレクトリ、コマンド。

タイプ: 文字列

必須: いいえ

linux

Linux および macOS のマネージドノード上のセッションに指定するシェルプリファレンス、環境変数、作業ディレクトリ、コマンド。

タイプ: 文字列

必須: いいえ

parameters

ドキュメントが受け入れるパラメータを定義するオブジェクト。ドキュメントパラメータの定義の詳細については、最上位のデータ要素 の「パラメータ」を参照してください。頻繁に参照するパラメータの場合は、そのパラメータを Systems Manager Parameter Store に保存してそこを参照することをお勧めします。`String` および `StringList` Parameter Store パラメータは、ドキュメントの本セクションで参照できます。`SecureString`Parameter Store パラメータは、ドキュメントの本セクションでは参照できません。次の形式を使用して、Parameter Store パラメータを参照できます。

```
{{ssm:parameter-name}}
```

Parameter Store の詳細については、「AWS Systems Manager Parameter Store」を参照してください。

型: StringMap

必須: いいえ

properties

指定した値を持つオブジェクトで、 `StartSession` API オペレーションで使用されるもの。

`InteractiveCommands` セッションに使用されるセッションドキュメントの場合、properties オブジェクトには、指定したオペレーティングシステムで実行するコマンドが含まれます。また、`runAsElevated` ブール値プロパティを使用して、コマンドを `root` として実行するかどう

かを決定することもできます。詳細については、「セッションでのコマンドへのアクセスを制限する」を参照してください。

Port セッションに使用されるセッションドキュメントの場合、properties オブジェクトには、トラフィックのリダイレクト先のポート番号が含まれます。例については、本トピックで後ほど取り扱う Port タイプのセッションドキュメントの例を参照してください。

型: StringMap

必須: いいえ

Standard_Stream タイプのセッションドキュメントの例

YAML

```
---
schemaVersion: '1.0'
description: Document to hold regional settings for Session Manager
sessionType: Standard_Stream
inputs:
  s3BucketName: ''
  s3KeyPrefix: ''
  s3EncryptionEnabled: true
  cloudWatchLogGroupName: ''
  cloudWatchEncryptionEnabled: true
  cloudWatchStreamingEnabled: true
  kmsKeyId: ''
  runAsEnabled: true
  runAsDefaultUser: ''
  idleSessionTimeout: '20'
  maxSessionDuration: '60'
  shellProfile:
    windows: ''
    linux: ''
```

JSON

```
{
    "schemaVersion": "1.0",
    "description": "Document to hold regional settings for Session Manager",
    "sessionType": "Standard_Stream",
    "inputs": {
```

```
        "s3BucketName": "",
        "s3KeyPrefix": "",
        "s3EncryptionEnabled": true,
        "cloudWatchLogGroupName": "",
        "cloudWatchEncryptionEnabled": true,
        "cloudWatchStreamingEnabled": true,
        "kmsKeyId": "",
        "runAsEnabled": true,
        "runAsDefaultUser": "",
        "idleSessionTimeout": "20",
        "maxSessionDuration": "60",
        "shellProfile": {
            "windows": "date",
            "linux": "pwd;ls"
        }
    }
}
```

InteractiveCommands タイプのセッションドキュメントの例

YAML

```
---
schemaVersion: '1.0'
description: Document to view a log file on a Linux instance
sessionType: InteractiveCommands
parameters:
  logpath:
    type: String
    description: The log file path to read.
    default: "/var/log/amazon/ssm/amazon-ssm-agent.log"
    allowedPattern: "^[a-zA-Z0-9-_/]+(.log)$"
properties:
  linux:
    commands: "tail -f {{ logpath }}"
    runAsElevated: true
```

JSON

```
{
    "schemaVersion": "1.0",
    "description": "Document to view a log file on a Linux instance",
```

```
    "sessionType": "InteractiveCommands",
    "parameters": {
        "logpath": {
            "type": "String",
            "description": "The log file path to read.",
            "default": "/var/log/amazon/ssm/amazon-ssm-agent.log",
            "allowedPattern": "^[a-zA-Z0-9-_/]+(.log)$"
        }
    },
    "properties": {
        "linux": {
            "commands": "tail -f {{ logpath }}",
            "runAsElevated": true
        }
    }
}
```

Port タイプのセッションドキュメントの例

YAML

```
---
schemaVersion: '1.0'
description: Document to open given port connection over Session Manager
sessionType: Port
parameters:
  paramExample:
    type: string
    description: document parameter
properties:
  portNumber: anyPortNumber
```

JSON

```
{
    "schemaVersion": "1.0",
    "description": "Document to open given port connection over Session Manager",
    "sessionType": "Port",
    "parameters": {
        "paramExample": {
            "type": "string",
            "description": "document parameter"
```

```
        }
    },
    "properties": {
        "portNumber": "anyPortNumber"
    }
}
```

特殊文字を使用したセッションドキュメントの例

YAML

```
---
schemaVersion: '1.0'
description: Example document with quotation marks
sessionType: InteractiveCommands
parameters:
  Test:
    type: String
    description: Test Input
    maxChars: 32
properties:
  windows:
    commands: |
        $Test = '{{ Test }}'
        $myVariable = \"Computer name is $env:COMPUTERNAME\"
        Write-Host "Test variable: $myVariable`.`nInput parameter: $Test"
    runAsElevated: false
```

JSON

```
{
   "schemaVersion":"1.0",
   "description":"Test document with quotation marks",
   "sessionType":"InteractiveCommands",
   "parameters":{
      "Test":{
         "type":"String",
         "description":"Test Input",
         "maxChars":32
      }
   },
   "properties":{
```

```
      "windows":{
         "commands":[
            "$Test = '{{ Test }}'",
            "$myVariable = \\\"Computer name is $env:COMPUTERNAME\\\"",
            "Write-Host \"Test variable: $myVariable`.`nInput parameter: $Test\""
         ],
         "runAsElevated":false
      }
   }
}
```

Session Manager のトラブルシューティング

以下の情報を参考にして、AWS Systems Manager Session Manager に関する問題のトラブルシューティングを行います。

トピック

- TerminateSession オペレーションを呼び出すときの AccessDeniedException
- ドキュメントプロセスが予期せず失敗しました: ドキュメントワーカーがタイムアウトしました
- Session Manager が Amazon EC2 コンソールから接続できない
- セッションを開始するアクセス許可がありません
- SSM Agent がオンラインになっていません
- セッション設定を変更するためのアクセス許可がありません
- Session Manager が使用できない、または使用に設定されていないマネージドノード。
- Session Manager プラグインが見つからない
- Session Manager プラグインがコマンドラインパスに自動的に追加されませんでした (Windows)
- Session Manager プラグインが応答しなくなる
- TargetNotConnected
- セッション開始後に空白の画面が表示される
- 長時間実行しているセッション中にマネージドノードが応答しなくなる
- StartSession オペレーションを呼び出すときにエラーが発生しました (InvalidDocument)

TerminateSession オペレーションを呼び出すときの AccessDeniedException

問題: セッションを終了しようとすると、Systems Manager が次のエラーを返します。

```
An error occurred (AccessDeniedException) when calling the TerminateSession operation:
User: <user_arn> is not authorized to perform: ssm:TerminateSession on resource:
<ssm_session_arn> because no identity-based policy allows the ssm:TerminateSession
 action.
```

ソリューション A: 最新バージョンの Session Manager プラグインがノードにインストールされていることを確認します。

ターミナルに以下のコマンドを入力して、Enter キーを押します。

```
session-manager-plugin --version
```

ソリューション B: プラグインの最新バージョンをインストールまたは再インストールします。

詳細については、「AWS CLI 用の Session Manager プラグインをインストールする」を参照してください。

ソリューション C: ノードへの接続の再確立を試みます。

ノードがリクエストに応答していることを確認します。セッションを再確立してみてください。または、必要に応じて Amazon EC2 コンソールを開き、インスタンスのステータスが実行中であることを確認します。

ドキュメントプロセスが予期せず失敗しました: ドキュメントワーカーがタイムアウトしました

問題: Linux ホストへのセッションを開始すると、Systems Manager が次のエラーを返します。

```
document process failed unexpectedly: document worker timed out,
check [ssm-document-worker]/[ssm-session-worker] log for crash reason
```

「SSM Agent ログの表示」で説明されているように SSM Agent ログ記録を設定している場合、デバッグログで詳細を確認できます。この問題では、Session Manager に次のログエントリが表示されます。

```
failed to create channel: too many open files
```

通常、このエラーは、実行中の Session Manager ワーカープロセスが多すぎて、基盤となるオペレーティングシステムが制限に達したことを示します。この問題を解決するには、2 つのオプションがあります。

解決策 A: オペレーティングシステムファイルの通知制限を増やす

制限は、別の Linux ホストから次のコマンドを実行することによって増やすことができます。このコマンドは Systems Manager Run Command を使用します。指定した値によって max_user_instances が 8192 に増加します。この値はデフォルト値の 128 よりも大幅に高くなりますが、ホストリソースに負荷がかかることはありません。

```
aws ssm send-command --document-name AWS-RunShellScript \
--instance-id i-02573cafcfEXAMPLE  --parameters \
"commands=sudo sysctl fs.inotify.max_user_instances=8192"
```

解決策 B: ターゲットホストで Session Manager が使用するファイル通知を減らす

別の Linux ホストから次のコマンドを実行して、ターゲットホストで実行しているセッションを一覧表示します。

```
aws ssm describe-sessions --state Active --filters key=Target,value=i-02573cafcfEXAMPLE
```

コマンド出力を確認して、不要になったセッションを特定します。これらのセッションは、別の Linux ホストから次のコマンドを実行することによって終了できます。

```
aws ssm terminate-session –session-id session ID
```

リモートサーバーで実行しているセッションがなくなったら、別の Linux ホストから次のコマンドを実行して追加のリソースを解放できます (オプション)。このコマンドは、リモートホストで実行しているすべての Session Manager プロセスを終了するので、その結果、リモートホストへのすべてのセッションが終了します。このコマンドを実行する前に、保持すべき進行中のセッションがないことを確認してください。

```
aws ssm send-command --document-name AWS-RunShellScript \
            --instance-id i-02573cafcfEXAMPLE --parameters \
'{"commands":["sudo kill $(ps aux | grep ssm-session-worker | grep -v grep | awk
 '"'"'{print $2}'"'"')"]}'
```

Session Manager が Amazon EC2 コンソールから接続できない

問題: 新しいインスタンスを作成した後、Amazon Elastic Compute Cloud (Amazon EC2) コンソールの [接続] ボタン > [セッションマネージャー] タブが表示されません。

解決策 A: インスタンスプロファイルを作成する: (EC2 コンソールの [セッションマネージャー] タブの情報の指示に従って) まだ作成していない場合は、Quick Setup を使用して AWS Identity and

Access Management (IAM) インスタンスプロファイルを作成します。Quick Setup は AWS Systems Manager のツールです。

Session Manager がインスタンスに接続するには IAM インスタンスプロファイルが必要です。Quick Setup を使用して ホスト管理設定を作成することで、インスタンスプロファイルを作成してインスタンスに割り当てることができます。ホスト管理設定により、必要なアクセス権限を持つインスタンスプロファイルが作成され、インスタンスに割り当てられます。ホスト管理設定では、他の Systems Manager ツールも有効にし、それらのツールを実行するための IAM ロールを作成します。Quick Setup またはホスト管理設定によって有効になっているツールの使用料は発生しません。Quick Setup を開きホスト管理設定を開いて作成します。

> **Important**
>
> ホスト管理設定を作成した後、Amazon EC2 が変更を登録し、[セッションマネージャ] タブを更新するまでに数分かかる場合があります。2 分経ってもタブに [接続] ボタンが表示されない場合は、インスタンスを再起動します。再起動しても接続するオプションが表示されない場合は、[Quick Setup] を開き、ホスト管理設定が 1 つだけであることを確認します。2 つある場合は、古いほうの設定を削除して数分待ってください。

ホスト管理設定を作成した後も接続できない場合、または SSM Agent に関するエラーなどのエラーが表示される場合は、次のいずれかの解決策を参照してください。

- 解決策 B: エラーは発生しないが、依然として接続できない
- 解決策 C: SSM Agent が見つからないことに関するエラー

解決策 B: エラーは発生しないが、依然として接続できない

ホスト管理設定を作成し、数分間待ってから接続を試行しても、依然として接続できない場合は、ホスト管理設定をインスタンスに手動で適用する必要がある場合があります。次の手順を使用して、Quick Setup ホスト管理設定を更新し、変更をインスタンスに適用します。

Quick Setup を使用してホスト管理設定を更新するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Quick Setup] を選択します。
3. [設定] リストで、作成した [ホスト管理] 設定を選択します。

4. [アクション]、[設定を編集] の順に選択します。
5. [ターゲット] セクションのほぼ最下部にある [インスタンスをどのようにターゲットにするかを選択] で、[手動] を選択します。
6. [インスタンス] セクションで、作成したインスタンスを選択します。
7. [Update] (更新) を選択します。

EC2 が [セッションマネージャー] タブを更新するまで数分待ちます。それでも接続できない場合、またはエラーが表示される場合は、この問題の他の解決策を確認してください。

解決策 C: SSM Agent が見つからないことに関するエラー

Quick Setup を使用してホスト管理設定を作成できなかった場合、または SSM Agent がインストールされていないことに関するエラーが表示される場合は、インスタンスに SSM Agent を手動でインストールする必要がある場合があります。SSM Agent は、Systems Manager が Session Manager を使用してインスタンスに接続できるようにする Amazon のソフトウェアです。SSM Agent は、ほとんどの Amazon マシンイメージ (AMI) にデフォルトでインストールされます。インスタンスが非標準 AMI または古い AMI で作成された場合は、エージェントを手動でインストールしなければならない場合があります。SSM Agent のインストールの手順については、ご使用のインスタンスのオペレーティングシステムに対応する次のトピックを参照してください。

- Windows Server
- macOS
- AlmaLinux
- Amazon Linux 1
- Amazon Linux 2 および AL2023
- CentOS
- CentOS Stream
- Debian Server
- Oracle Linux
- Red Hat Enterprise Linux
- Rocky Linux
- SUSE Linux Enterprise Server
- Ubuntu Server

SSM Agent に関する問題については、SSM Agent のトラブルシューティング を参照してください。

セッションを開始するアクセス許可がありません

問題: セッションを開始しようとしましたが、システムから必要なアクセス権限がないと通知されました。

- 解決策: システム管理者から、Session Manager セッションを開始するための AWS Identity and Access Management (IAM) ポリシーのアクセス許可が与えられていません。詳細については、「インスタンスへのユーザーセッションアクセスの制御」を参照してください。

SSM Agent がオンラインになっていません

問題: Amazon EC2 インスタンスの [Session Manager] タブに、次のメッセージが表示されます。「SSM Agent がオンラインになっていません。SSM Agent は、Systems Manager エンドポイントに接続して、それ自体をサービスに登録することができませんでした。」

解決策: SSM Agent は、Session Manager が Amazon EC2 インスタンスに接続できるように、これらのインスタンス上で実行される Amazon ソフトウェアです。このエラーが表示される場合、SSM Agent は Systems Manager エンドポイントとの接続を確立できません。可能性のある問題の原因としては、ファイアウォール制限、ルーティング問題、またはインターネット接続がないことが考えられます。この問題を解決するには、ネットワーク接続問題を調査してください。詳細については、SSM Agent のトラブルシューティングおよびマネージドノードの可用性のトラブルシューティングを参照してください。Systems Manager エンドポイントについては、AWS 全般リファレンスの「AWS Systems Manager エンドポイントとクォータ」を参照してください。

セッション設定を変更するためのアクセス許可がありません

問題: 組織のグローバルなセッション設定を更新しようとしましたが、システムから必要なアクセス権限がないと通知されました。

- 解決策: システム管理者から、Session Manager を設定するための IAM ポリシーのアクセス許可が与えられていません。詳細については、Session Manager の設定を更新するためのユーザーアクセス許可を付与または拒否する を参照してください。

Session Manager が使用できない、または使用に設定されていないマネージドノード。

問題 1: セッションの開始のコンソールページでセッションを開始したくても、あるマネージドノードがリストにありません。

- 解決策 A: 接続したいマネージドノードが AWS Systems Manager 用に設定されていない可能性があります。詳細については、「組織用の Systems Manager 統合コンソールのセットアップ」を参照してください。

  > **Note**
  >
  > IAM インスタンスプロファイルをアタッチする際に AWS Systems ManagerSSM Agent がマネージドノード上ですでに実行されている場合、セッションの開始コンソールページにインスタンスが表示される前に、エージェントを再起動しなければならない場合があります。

- 解決策 B: マネージドノードの SSM Agent に適用したプロキシ設定が正しくない可能性があります。プロキシ設定が正しくない場合、マネージドノードは必要なサービスエンドポイントに到達できないか、またはノードがに異なるオペレーティングシステムとして Systems Manager にレポートする可能性があります。詳細については、Linux ノードでプロキシを使用するための SSM Agent の設定およびSSM Agent が Windows Server インスタンス用にプロキシを使用するように設定するを参照してください。

問題 2: 接続したいマネージドノードがセッションの開始コンソールページのリストにありますが、「選択したインスタンスは Session Manager を使用するように構成されていません」というページが表示されます。

- 解決策 A: マネージドノードは Systems Manager サービスで使用されるように設定されていますが、ノードに添付された IAM インスタンスプロファイルに Session Manager ツールの許可が含まれていない可能性があります。詳細については、「Session Manager アクセス権限を使用し、IAM インスタンスプロファイルロールを確認するか作成する」を参照してください。
- 解決策 B: マネージドノードは、Session Manager をサポートする SSM Agent のバージョンを実行していません。ノードの SSM Agent をバージョン 2.3.68.0 以降に更新します。

  オペレーティングシステムに応じて Windows Server 用の EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする、Linux 用 EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする、macOS 用の EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする の手順にしたがって、マネージドノードの SSM Agent を手動で更新します。

または、Run Command ドキュメントの AWS-UpdateSSMAgent を使用して、1 つ以上のマネージドノードのエージェントバージョンを一度に更新します。詳細については、Run Command を使用して SSM Agent を更新する を参照してください。

> **Tip**
>
> エージェントを常に最新の状態に保つには、次のいずれかの方法で定義した自動スケジュールを使用して、SSM Agent を最新バージョンにアップデートすることをお勧めします。
>
> - State Manager 関連付けの一部として AWS-UpdateSSMAgent を実行します。詳細については、チュートリアル: AWS CLI で SSM Agent を自動的に更新する を参照してください。
> - メンテナンスウィンドウの一部として AWS-UpdateSSMAgent を実行します。メンテナンスウィンドウの使用については、「コンソールを使用してメンテナンスウィンドウを作成および管理する」と「チュートリアル: AWS CLI を使用してメンテナンスウィンドウを作成および設定する」を参照してください。

- 解決方法 C: マネージドノードは必要なサービスエンドポイントに到達できません。AWS PrivateLink によるインターフェイス・エンドポイントを使用して Systems Manager エンドポイントに接続することにより、マネージドノードのセキュリティ体制を改善できます。インターフェイス・エンドポイントを使用する代わりに、マネージドノードでアウトバウンド・インターネットアクセスを有効にする方法があります。詳細については、「PrivateLink を使用して Session Manager の VPC エンドポイントをセットアップする」を参照してください。
- 解決策 D: マネージドノードの使用可能な CPU またはメモリリソースが制限されています。マネージドノードが機能していても、ノードに十分な使用可能なリソースがなければセッションを確立できません。詳細については、「接続できないインスタンスのトラブルシューティング」を参照してください。

Session Manager プラグインが見つからない

AWS CLI を使用してセッションコマンドを実行するには、ローカルマシンにも Session Manager プラグインがインストールされている必要があります。詳細については、AWS CLI 用の Session Manager プラグインをインストールする を参照してください。

Session Manager プラグインがコマンドラインパスに自動的に追加されませんでした (Windows)

Session Manager プラグインを Windows にインストールする場合、オペレーティングシステムの PATH 環境変数に `session-manager-plugin` 実行可能なファイルが自動的に追加されます。Session Manager プラグインが正しくインストールされているか (`aws ssm start-session --target` *`instance-id`*) 確認して、コマンド実行後に失敗した場合は、次の手順を使用して手動で設定する必要があります。

PATH 変数を変更するには (Windows)

1. Windows キーを押し、「**`environment variables`**」と入力します。
2. [Edit environment variables for your account] を選択します。
3. [PATH] を選択して、[Edit] を選択します。
4. 次の例に示すように、セミコロンで区切って [Variable value (変数値)] フィールドにパスを追加します: *`C:\existing\path`*;***`C:\new\path`***

   次の例に示すように、*`C:\existing\path`* は既にフィールドにある値を表します。***`C:\new\path`*** は追加するパスを表します。

   - 64 ビットコンピュータ: `C:\Program Files\Amazon\SessionManagerPlugin\bin\`
   - 32 ビットコンピュータ: `C:\Program Files (x86)\Amazon\SessionManagerPlugin\bin\`
5. [OK] を 2 回選択して、新しい設定を適用します。
6. 実行中のコマンドプロンプトを閉じ、もう一度開きます。

Session Manager プラグインが応答しなくなる

ローカルマシンにウイルス対策ソフトウェアがインストールされている場合、ポート転送セッション中にトラフィックの転送が停止することがあります。場合によっては、ウイルス対策ソフトウェアが Session Manager プラグインがプロセスのデッドロックを引き起こします。この問題を解決するには、ウィルス対策ソフトウェアから Session Manager プラグインを許可するか除外します。Session Manager プラグインのデフォルトのインストールパスの詳細については、「AWS CLI 用の Session Manager プラグインをインストールする」を参照してください。

TargetNotConnected

問題: セッションを開始しようとしましたが、システムは「StartSession オペレーションの呼び出し時にエラー (TargetNotConnected) が発生しました。*InstanceID* が接続されていません」というエラーメッセージを返します。

- 解決策 A: このエラーは、セッションに指定されたターゲットのマネージドノードが Session Manager で使用するように完全に設定されていない場合に返されます。詳細については、Session Manager を設定する を参照してください。
- 解決策 B: このエラーは、別の AWS アカウント または AWS リージョン にあるマネージドノードでセッションを開始しようとした場合も返されます。

セッション開始後に空白の画面が表示される

問題: セッションを開始すると、Session Manager に空白の画面が表示される。

- 解決策 A: この問題は、マネージドノードのルートボリュームがいっぱいになったときに発生する可能性があります。ディスク容量不足のため、ノードの SSM Agent が動作を停止します。この問題を解決するには、Amazon CloudWatch を使用して、オペレーティングシステムからメトリクスとログを収集します。詳細については、「Amazon CloudWatch ユーザーガイド」の「CloudWatch エージェントを使用してメトリクス、ログ、トレースを収集する」を参照してください。
- 解決策 B: エンドポイントとリージョンのペアが一致しないリンクを使用してコンソールにアクセスした場合、空白の画面が表示されることがあります。例えば、次のコンソール URL では、us-west-2 は指定されたエンドポイントですが、us-west-1 は指定された AWS リージョン です。

```
https://us-west-2.console.aws.amazon.com/systems-manager/session-manager/sessions?
region=us-west-1
```

- 解決策 C: VPC エンドポイントを使用してマネージドノードが Systems Manager に接続し、Session Manager の設定に基づいてセッション出力が Amazon S3 バケットまたは Amazon CloudWatch Logs のロググループに書き込みますが、s3 ゲートウェイ・エンドポイントまたは logs インターフェイス・エンドポイントは VPC に存在しません。マネージドノードが VPC エンドポイントを使用して Systems Manager に接続し、Session Manager の設定に基づいてセッション出力が Amazon S3 バケット に書き込まれる場合、**com.amazonaws.*region*.s3** 形式の s3 エンドポイントが必要です。マネージドノードが VPC エンドポイントを使用して Systems Manager に接続し、Session Manager の設定に基づいてセッション出力が CloudWatch Logs のロググループに書き込まれる場合、**com.amazonaws.*region*.logs** 形式の logs エンドポイントが必要で

す。詳細については、「Systems Manager 用の VPC エンドポイントを作成する」を参照してください。

- 解決策 D: セッション設定で指定したロググループまたは Amazon S3 バケットが削除されました。この問題を解決するには、有効なロググループまたは S3 バケットを使用してセッション設定を更新します。
- 解決策 E: セッション設定で指定したロググループまたは Amazon S3 バケットは暗号化されませんが、 `cloudWatchEncryptionEnabled` または `s3EncryptionEnabled` の入力を `true` に設定しています。この問題を解決するには、暗号化されたロググループまたは Amazon S3 バケットを使用してセッション設定を更新するか、`cloudWatchEncryptionEnabled` または `s3EncryptionEnabled` 入力を `false` に設定します。このシナリオは、コマンドラインツールを使用してセッション設定を作成する顧客にのみ適用されます。

長時間実行しているセッション中にマネージドノードが応答しなくなる

問題: 長時間実行しているセッション中にマネージドノードが応答しなくなるか、またはクラッシュします。

解決策: Session Manager の SSM Agent ログ保持期間を減らします。

セッションの SSM Agent ログの保持期間を短縮するには

1. Linux 向けの `/etc/amazon/ssm/` ディレクトリ、または Windows 向けの `C:\Program Files\Amazon\SSM` 内で `amazon-ssm-agent.json.template` を検索します。
2. `amazon-ssm-agent.json.template` の内容を、`amazon-ssm-agent.json` という名前の同じディレクトリ内の新しいファイルにコピーします。
3. `SessionLogsRetentionDurationHours` プロパティの `SSM` 値のデフォルト値を小さくして、ファイルを保存します。
4. [SSM Agent] を再起動する

StartSession オペレーションを呼び出すときにエラーが発生しました (InvalidDocument)

問題: AWS CLI を使用してセッションを開始すると、次のエラーが表示される。

```
An error occurred (InvalidDocument) when calling the StartSession operation: Document
 type: 'Command' is not supported. Only type: 'Session' is supported for Session
 Manager.
```

解決策: `--document-name` パラメータに指定した SSM ドキュメントがセッションドキュメントではありません。次の手順を使用して、AWS Management Console のセッションドキュメントのリストを表示します。

セッションドキュメントのリストを表示するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[ドキュメント] を選択します。
3. [カテゴリ] リストで [セッションドキュメント] を選択します。

AWS Systems Manager State Manager

AWS Systems Manager のツールである State Manager は、安全でスケーラブルな設定管理サービスであり、これによってマネージドノードおよび他の AWS リソースを定義された状態に保つプロセスが自動化されます。State Manager の使用を開始するには、Systems Manager コンソールを開きます。ナビゲーションペインで、[State Manager] を選択します。

> **Note**
>
> State Manager および Maintenance Windows は、マネージドノードで同様の種類の更新を実行できます。どちらを選択するかは、システムコンプライアンスを自動化する必要があるか、指定した期間中に優先度の高い、時間的制約のあるタスクを実行するかによって異なります。
> 詳細については、「State Manager または Maintenance Windows の選択」を参照してください。

State Manager はどのように組織にとってメリットになりますか?

State Manager で事前設定された Systems Manager ドキュメント (SSM ドキュメント) を使用することによって、ノードを管理する際に、次の利点が得られます。

- スタートアップ時に特定のソフトウェアを使用してノードをブートストラップする。
- 定義済みのスケジュールに従ってエージェント (SSM Agent など) をダウンロードして更新する。
- ネットワーク設定を設定する。
- Microsoft Active Directory ドメインにノードを結合する。

- ライフサイクルを通じて Linux、macOS、および Windows マネージドノードでスクリプトを実行します。

他の AWS リソースにまたがって設定のずれを管理するには、Systems Manager のツールである Automation を State Manager とともに使用して、次のタイプのタスクを実行します。

- Amazon Elastic Compute Cloud (Amazon EC2) インスタンスに Systems Manager ロールをアタッチして、これらのインスタンスをマネージドノードにします。
- セキュリティグループに Ingress ルールと Egress ルールを適用します。
- Amazon DynamoDB バックアップを作成または削除します。
- Amazon Elastic Block Store (Amazon EBS) スナップショットを作成または削除します。
- Amazon Simple Storage Service (Amazon S3) バケットの読み取りおよび書き込みのアクセス許可をオフにします。
- マネージドノードと Amazon Relational Database Service (Amazon RDS) インスタンスを起動、再起動、または停止します。
- Linux、macOS、Window AMIs にパッチを適用します。

Automation ランブックを使用した State Manager の使用については、「State Manager 関連付けでのオートメーションのスケジュール設定」を参照してください。

State Manager はどのようなユーザーに適していますか?

State Manager は、AWS リソースの管理とガバナンスを改善し、設定のずれを軽減したい AWS のお客様に適しています。

State Manager の特徴は何ですか?

State Manager の主な機能は以下のとおりです。

- State Manager 関連付け

  State Manager 関連付け とは、AWS リソースに割り当てる設定です。この設定では、リソースで維持したい状態を定義します。例えば、関連付けでは、アンチウイルスソフトウェアがマネージドノードにインストールされて実行されている必要があることや、特定のポートを閉じる必要があることなどを指定できます。

関連付けでは、設定を適用するスケジュールと、関連付けのターゲットを指定します。例えば、アンチウイルスソフトウェアに関する関連付けが AWS アカウントのすべてのマネージドノードで 1 日に 1 回実行されるとします。ソフトウェアがノードにインストールされていない場合、関連付けによって State Manager にインストールするように指示することができます。ソフトウェアがインストールされていてもサービスが実行されていない場合、関連付けによって State Manager にサービスを開始するように指示することができます。

- 柔軟なスケジューリングオプション

  State Manager には、関連付けの実行時のスケジュール設定に関する次のオプションがあります。

  - 即時処理または遅延処理

    関連付けを作成すると、デフォルトでは、システムによって指定したリソースで関連付けがすぐに実行されます。最初の実行後、関連付けは定義したスケジュールに従って間隔を空けて実行されます。

    コンソールの [Apply association only at the next specified Cron interval] (次に指定した Cron の間隔でのみ関連付けを適用する) オプションまたはコマンドラインの `ApplyOnlyAtCronInterval` パラメータを使用して、関連付けを直ちに実行しないように State Manager に指示できます。

  - cron 式と rate 式

    関連付けを作成するときは、State Manager が設定を適用するスケジュールを指定します。State Manager は、関連付けの実行時にスケジューリングするためのほとんどの標準の cron 式と rate 式をサポートしています。State Manager はまた、関連付けを実行する曜日と月の n 番目の日を指定する番号記号 (#)、および月の最後の X 曜日を示す (L) 記号を含む cron 式をサポートしています。

    > **Note**
    >
    > 現在、State Manager では、関連付けの cron 式での月の指定はサポートされていません。

    パッチした火曜日の 2 日後に関連付けを実行するなど、関連付けを実行するタイミングをさらに制御するには、オフセットを指定できます。オフセットでは、関連付けの実行がスケジュールされている日の後に待機する日数を定義します。

cron 式と rate 式の作成の詳細については、「リファレンス: Systems Manager の Cron 式および rate 式」を参照してください。

- 複数のターゲットオプション

  関連付けは、関連付けのターゲットも指定します。State Manager は、ターゲットの AWS リソースとして、タグ、AWS Resource Groups、個々のノード ID、または現在の AWS リージョン と AWS アカウント 内にあるすべてのマネージドノードの指定をサポートしています。

- Amazon S3 のサポート

  アソシエーション実行からのコマンド出力は、選択した Amazon S3 バケットに保存します。詳細については、「Systems Manager の関連付けの使用」を参照してください。

- EventBridge のサポート

  この Systems Manager のツールは、Amazon EventBridge ルールでイベントタイプおよびターゲットタイプとしてサポートされています。詳細については、「Amazon EventBridge を使用して Systems Manager イベントをモニタリングする」および「リファレンス: Systems Manager 用の Amazon EventBridge イベントパターンとタイプ」を参照してください。

State Manager の使用料金はかかりますか?

State Manager は追加料金なしでご利用いただけます。

トピック

- State Manager の仕組みについて
- Systems Manager の関連付けの使用
- MOF ファイルを実行する関連付けの作成
- Ansible プレイブックを実行する関連付けの作成
- Chef recipe を実行する関連付けの作成
- チュートリアル: AWS CLI で SSM Agent を自動的に更新する
- チュートリアル: Windows Server の EC2 インスタンスで PV ドライバーを自動的に更新する

詳細情報

- Amazon EC2 Systems Manager と Windows PowerShell DSC を使用して設定のずれに対処する

- State Manager を使用して、Auto Scaling グループで Amazon EC2 インスタンスを設定する

State Manager の仕組みについて

AWS Systems Manager のツールである State Manager は、ハイブリッドおよびマルチクラウドインフラストラクチャ内のマネージドノードを定義した状態に維持するプロセスを自動化する、安全でスケーラブルなサービスです。

State Manager の仕組みを以下に示します。

1. AWS リソースに適用する状態を決定します。

   マネージドノードが、アンチウイルスやマルウェアのアプリケーションなど、特定のアプリケーションを使用して設定されるようにしたいですか? SSM Agent、または `AWSPVDriver` などの他の AWS パッケージを更新するプロセスを自動化しますか? 特定のポートが確実に閉じられている、または開かれているようにする必要がおありですか? State Manager の使用を開始するには、AWS リソースに適用する状態を決定します。適用する状態では、どの SSM ドキュメントを使用して State Manager の関連付けを作成するか決定します。

   State Manager 関連付け とは、AWS リソースに割り当てる設定です。この設定では、リソースで維持したい状態を定義します。例えば、関連付けでは、アンチウイルスソフトウェアがマネージドノードにインストールされて実行されている必要があることや、特定のポートを閉じる必要があることなどを指定できます。

   関連付けでは、設定を適用するスケジュールと、関連付けのターゲットを指定します。例えば、アンチウイルスソフトウェアに関する関連付けが AWS アカウントのすべてのマネージドノードで 1 日に 1 回実行されるとします。ソフトウェアがノードにインストールされていない場合、関連付けによって State Manager にインストールするように指示することができます。ソフトウェアがインストールされていてもサービスが実行されていない場合、関連付けによって State Manager にサービスを開始するように指示することができます。
2. 事前設定された SSM ドキュメントが、AWS リソースで目的の状態の作成に役立つかどうかを確認します。

   Systems Manager には、関連付けの作成に使用できる事前設定された SSM ドキュメントが何十も含まれています。事前設定されたドキュメントでは、アプリケーションのインストール、Amazon CloudWatch の設定、AWS Systems Manager Automation の実行、PowerShell および Shell スクリプトの実行、マネージドノードを Active Directory のディレクトリサービスドメインに結合することなどの一般的なタスクがすぐに実行できるようになっています。

Systems Manager コンソールですべての SSM ドキュメントを表示できます。ドキュメントの名前を選択して各ドキュメントの詳細について確認します。ここでは、AWS-ConfigureAWSPackage と AWS-InstallApplication の 2 つの例を示します。

3. 関連付けを作成します。

関連付けは、Systems Manager コンソール、AWS Command Line Interface (AWS CLI)、AWS Tools for Windows PowerShell (Tools for Windows PowerShell)、または Systems Manager API を使用して作成できます。関連付けを作成するときは、以下の情報を指定します。

- 関連付けの名前。
- SSM ドキュメントのパラメータ (例えば、インストールするアプリケーションへのパス、またはノードで実行するスクリプト)。
- 関連付けのターゲット。マネージドノードをターゲットにするには、タグを指定するか、個々のノード ID を選択するか、AWS Resource Groups でグループを選択します。現在の AWS リージョン と AWS アカウント 内にあるすべてのマネージドノードをターゲットにすることもできます。ターゲットに 1,000 個を超えるノードが含まれている場合、システムは 1 時間ごとのスロットリングメカニズムを使用します。これは、ステータス集計プロセスが 1 時間ごとに実行され、ノードの実行ステータスが変更された場合にのみ更新されるため、集計されたステータスのカウントに不正確さが生じる可能性があることを意味します。
- 状態を適用する時期または頻度のスケジュール。cron 式またはレート式を指定できます。cron および rate 式を使用したスケジュールの作成の詳細については、「関連付けのための cron および rate 式」を参照してください。

> **Note**
>
> 現在、State Manager では、関連付けの cron 式での月の指定はサポートされていません。

関連付けを作成するコマンドを実行すると、Systems Manager は指定した情報 (スケジュール、ターゲット、SSM ドキュメント、パラメータ) をターゲットのリソースにバインドします。システムがすべてのターゲットに接続しようとすると関連付けのステータスは最初 [Pending (保留)] と表示され、関連付けで指定された状態を 即時に適用します。

> **Note**
>
> 以前の関連付けがまだ実行中に、新しく作成した関連付けを実行するようにスケジュールすると、以前の関連付けはタイムアウトし、新しい関連付けが実行されます。

Systems Manager は、リソースの関連付けを作成するリクエストのステータスをレポートします。ステータスの詳細は、コンソールまたは (マネージドノードについては) DescribeInstanceAssociationsStatus API オペレーションを使用して表示できます。関連付けの作成時に Amazon Simple Storage Service (Amazon S3) にコマンドの出力を書き込むことを選択した場合、指定した Amazon S3 バケットで出力を表示することもできます。

詳細については、「Systems Manager の関連付けの使用」を参照してください。

> **Note**
>
> 関連付けの実行中に SSM ドキュメントによって開始される API オペレーションは、AWS CloudTrail でログ記録されません。

4. モニタリングと更新。

   関連付けが作成されると、State Manager は、関連付けで定義されたスケジュールに従って設定を再適用します。関連付けのステータスは、コンソールの State Manager ページで、または関連付けを作成したときに Systems Manager によって生成された関連付け ID を直接呼び出すことで表示できます。詳細については、「関連付けの履歴の表示」を参照してください。関連付けドキュメントを更新して、必要に応じて再適用できます。関連付けの複数のバージョンを作成することもできます。詳細については、「関連付けの編集と新しいバージョンの作成」を参照してください。

関連付けがリソースに適用されるタイミングについて

関連付けの作成時に、設定を定義する SSM ドキュメント、ターゲットリソースのリスト、および設定を適用するためのスケジュールを指定します。デフォルトでは、State Manager は関連付けを、作成時およびスケジュールに従って実行します。さらに State Manager は次の状況でも関連付けの実行を試行します。

- 関連付けの編集 – State Manager はユーザーが編集し、それらの変更を次の関連付けフィールド: `DOCUMENT_VERSION`、`PARAMETERS`、`SCHEDULE_EXPRESSION`、`OUTPUT_S3_LOCATION` のいずれかに保存した後に関連付けを実行します。
- ドキュメントの編集 – State Manager はユーザーが編集し、関連付けの設定状態に定義する SSM ドキュメントに変更を保存した後に関連付けを実行します。具体的には、関連付けは、ドキュメントに対する以下の編集の後に実行されます。

  - ユーザーが新しい $DEFAULT ドキュメントバージョンを指定し、$DEFAULT バージョンを使用して関連付けが作成された。
  - ユーザーがドキュメントを更新し、$LATEST バージョンを使用して関連付けが作成された。
  - ユーザーは、関連付けの作成時に指定されたドキュメントを削除します。
- 手動開始 — State Manager は、ユーザーが Systems Manager コンソールまたはプログラムのいずれかから開始したときに関連付けを実行します。
- ターゲットの変更 — State Manager ターゲットノードで次のいずれかのアクティビティが発生した後に関連付けを実行します。
  - マネージドノードが初めてオンラインになります。
  - スケジュールされた関連付けの実行を逃した後、マネージドノードがオンラインになります。
  - 30 日以上停止された後、マネージドノードがオンラインになります。

> **Note**
>
> State Manager は、AWS アカウント全体の関連付けで使用されるドキュメントまたはパッケージを監視しません。1 つのアカウントでドキュメントまたはパッケージを更新しても、この更新では関連付けが 2 番目のアカウントで実行されることはありません。2 番目のアカウントで関連付けを手動で実行する必要があります。

ターゲットが変更されたときの関連付けの実行の防止

場合によっては、マネージドノードで構成されるターゲットが変更されたときに関連付けを実行せず、指定されたスケジュールに従ってのみ関連付けを実行したい場合があります。

> **Note**
>
> Automation ランブックを実行すると、コストが発生します。Automation ランブックとの関連付けがアカウント内のすべてのインスタンスを対象としており、定期的に多数のインスタンスを起動する場合、ランブックは起動時に各インスタンスで実行されます。これにより、自動化料金が上昇する可能性があります。

関連付けのターゲットが変更されたときに関連付けが実行されないようにするには、[次に指定された cron 間隔のチェックボックスでのみ関連付けを適用する] チェックボックスを選択します。このチェックボックスは、[関連付けの作成] ページと [関連付けの編集] ページの [スケジュールの指定] エリアにあります。

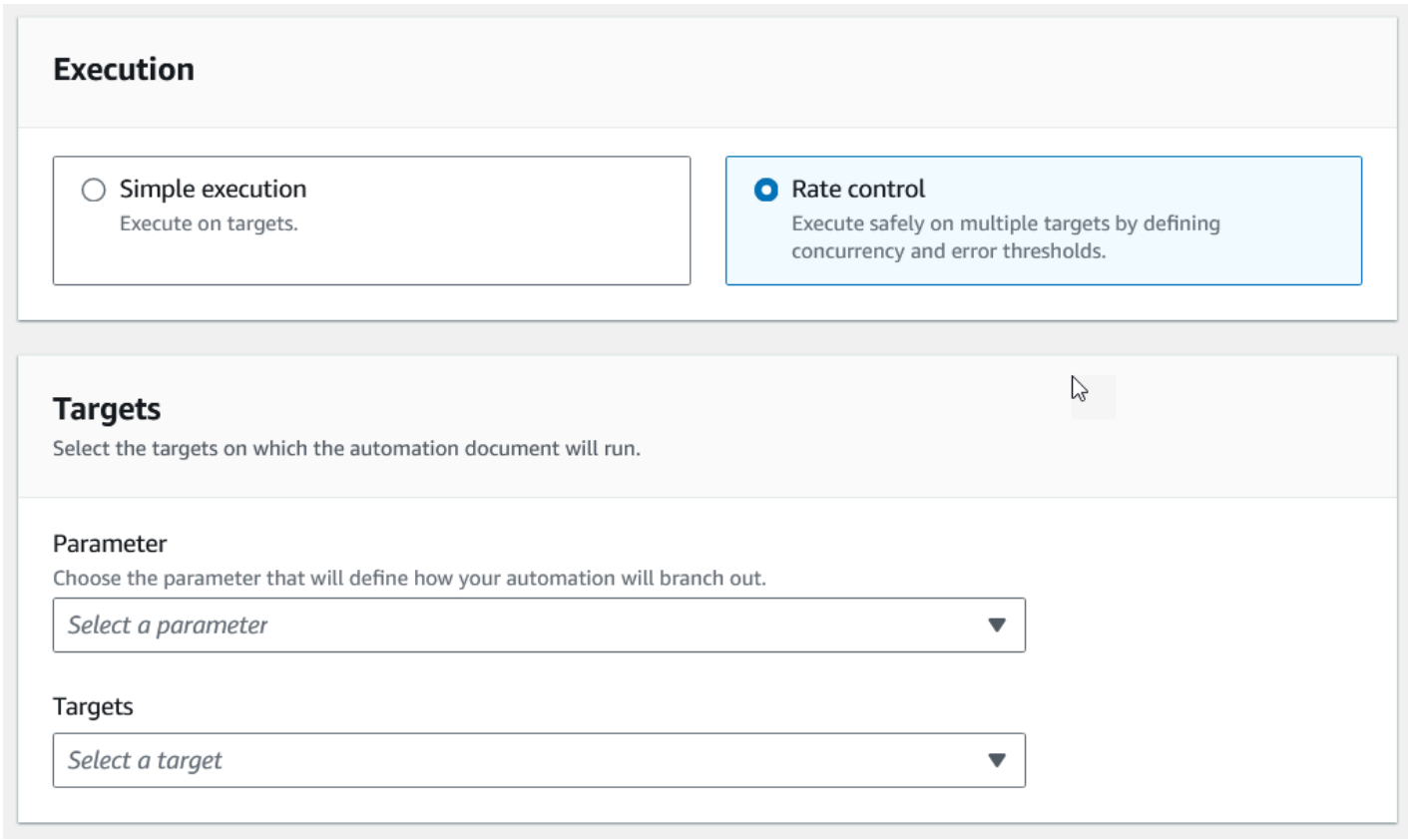
このオプションは、オートメーションランブックまたは SSM ドキュメントを組み込む関連付けに適用されます。

Automation ランブックによるターゲット更新について

新しいターゲットノードが検出されたときに、Automation ランブックで作成された関連付けを適用するには、以下の条件が満たされている必要があります。

- Quick Setup 設定によって関連付けを作成する必要があります。Quick Setup は AWS Systems Manager のツールです。他のプロセスによって作成された関連付けは、現時点ではサポートされていません。
- Automation ランブックは、リソースタイプ `AWS::EC2::Instance` または `AWS::SSM::ManagedInstance` を明示的にターゲットにする必要があります。
- 関連付けには、パラメータとターゲットの両方を指定する必要があります。

  レート制御実行を選択すると、コンソールに [パラメータ] フィールドと [ターゲット] フィールドが表示されます。



CreateAssociation、CreateAssociationBatch、UpdateAssociation の API アクションを使用するときに、AutomationTargetParameterName と Targets の入力を使用してこれらの値を指定できます。これらの各 API アクションでは、ApplyOnlyAtCronInterval パラメータを true に設定することで、ターゲットが変更されるたびに関連付けが実行されないようにすることもできます。

コンソールを使用して、オートメーション実行の予想外に高いコストを回避する方法など、関連付けの実行時期を制御する方法については、「関連付けがリソースに適用されるタイミングについて」を参照してください。

Systems Manager の関連付けの使用

このセクションでは、AWS Systems Manager コンソール、AWS Command Line Interface (AWS CLI)、および AWS Tools for PowerShell を使用して State Manager 関連付けを作成し管理する方法について説明します。

トピック

- State Manager 関連付けのターゲットとレート制御について

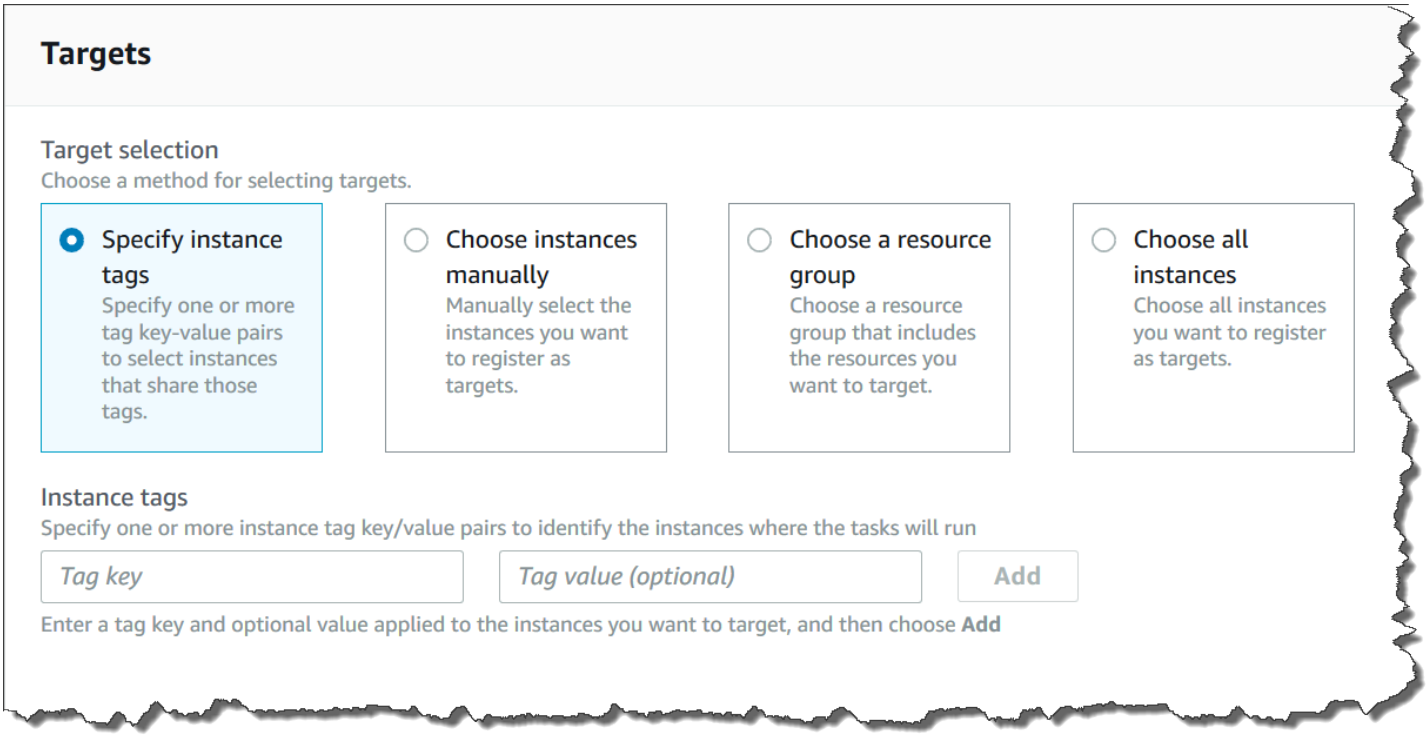
- 関連付けの作成
- 関連付けの編集と新しいバージョンの作成
- 関連付けを削除する
- 関連付けで Auto Scaling グループを実行する
- 関連付けの履歴の表示
- IAM を使用して関連付けを操作する

State Manager 関連付けのターゲットとレート制御について

このトピックでは、スケジュールされた時間に関連付けを実行するノードの数を制御しながら、数十または数百のノードに関連付けをデプロイするのに役立つ State Manager の機能について説明します。State Manager は AWS Systems Manager のツールです。

ターゲットの使用について

State Manager 関連付けを作成するときは、ここに示すように Systems Manager コンソールの [Targets] (ターゲット) セクションで、関連付けを設定するノードを選択します。



AWS Command Line Interface (AWS CLI) などのコマンドラインツールを使用して関連付けを作成する場合は、`targets` パラメータを指定します。ノードをターゲットにすると、個々のノード ID を指定または選択しなくても、数十、数百、数千のノードに関連付けを設定できます。

各マネージドノードは、最大 20 件の関連付けの対象にすることができます。

State Manager では、関連付けの作成時に以下のターゲットオプションが提供されます。

タグを指定する

このオプションを使用して、ノードに割り当てられているタグキーと (必要に応じて) タグ値を指定します。このリクエストを実行すると、システムは指定されたタグキーと値に一致するすべてのノードを検出し、関連付けの作成を試みます。複数のタグ値を指定した場合、関連付けはそれらのタグ値の少なくとも 1 つを持つすべてのノードをターゲットとします。システムは、最初に関連付けを作成すると、その関連付けを実行します。この最初の実行後、システムは指定されたスケジュールに従って関連付けを実行します。

新しいノードを作成し、指定したタグキーと値をそれらのノードに割り当てると、システムは関連付けを自動的に適用し、すぐに実行した後、スケジュールに従って実行します。これは、関連付けがコマンドまたはポリシードキュメントを使用する場合に適用され、関連付けが Automation ランブックを使用する場合は適用されません。指定したタグをノードから削除すると、システムはそれらのノードで関連付けを実行しなくなります。

> **Note**
>
> オートメーションランブックを State Manager と共に使用していて、タグ付けの制限により特定の目標を達成できない場合は、Amazon EventBridge で自動化ランブックを使用することを検討してください。詳細については、「EventBridge イベントに基づくオートメーションを実行する」を参照してください。State Manager でのオートメーションランブックの使用の詳細については、「State Manager 関連付けでのオートメーションのスケジュール設定」を参照してください。

ベストプラクティスとして、コマンドまたはポリシードキュメントを使用する関連付けを作成する際にタグを使用することをお勧めします。Auto Scaling グループを実行するための関連付けを作成する際にも、タグを使用することをお勧めします。詳細については、「関連付けで Auto Scaling グループを実行する」を参照してください。

> **Note**
>
> 以下の情報に注意してください。
>
> - AWS Management Consoleでノードをターゲットとする関連付けを作成するときにタグを使用する場合、自動関連付けには 1 つのタグキーのみ、コマンド関連付けには 5 つのタグ

キーを指定できます。関連付けに指定されたすべてのタグキーが、現時点でノードに割り当てられている必要があります。割り当てられていない場合、State Manager はノードを関連付けのターゲットにできません。

- コンソールを使用していて、かつ、ノードをターゲットとするときに自動関連付けには複数のタグキー、コマンド関連付けには 5 つのタグキーを使用する場合は、それらのタグキーを AWS Resource Groups グループに割り当ててからそのグループにノードを追加します。その後、State Manager 関連付けを作成する際に、[ターゲット] リストで [リソースグループ] オプションを選択できます。
- AWS CLI を使用して、最大 5 個のタグキーを指定できます。AWS CLI を使用する場合は、`create-association` コマンドで指定されたすべてのタグキーがノードに現在割り当てられている必要があります。割り当てられていない場合、State Manager はノードを関連付けのターゲットにできません。

ノードを手動で選択する

このオプションを使用して、関連付けを作成するノードを手動で選択します。[Instances] (インスタンス) ペインに、現在の AWS アカウント と AWS リージョン 内にあるすべての Systems Manager マネージドノードが表示されます。任意の数のノードを手動で選択できます。システムは、最初に関連付けを作成すると、その関連付けを実行します。この最初の実行後、システムは指定されたスケジュールに従って関連付けを実行します。

> **Note**
>
> 表示されるはずのマネージドノードが表示されない場合は、トラブルシューティングのヒントについて「マネージドノードの可用性のトラブルシューティング」を参照してください。

リソースグループの選択

このオプションを使用して、AWS Resource Groups タグベースまたは AWS CloudFormation スタックベースのクエリによって返されるすべてのノードに関連付けを作成します。

関連付けでリソースグループをターゲットにする際の詳細は以下のとおりです。

- 新しいノードをグループに追加すると、システムは自動的にそのノードを、リソースグループをターゲットにする関連付けにマッピングします。システムは、変更を検出すると、ノードに関連付

けを適用します。この最初の実行後、システムは指定されたスケジュールに従って関連付けを実行します。

- リソースグループをターゲットとする関連付けを作成し、そのグループの `AWS::SSM::ManagedInstance` リソースタイプが指定されていた場合、設計上、関連付けはハイブリッドおよびマルチクラウド環境で Amazon Elastic Compute Cloud (Amazon EC2) インスタンスと非 EC2 ノードの両方で実行されます。

  逆の場合も同様です。リソースグループをターゲットとする関連付けを作成し、そのグループの `AWS::EC2::Instance` リソースタイプが指定されていた場合、設計上、関連付けはハイブリッドおよびマルチクラウド環境の非 EC2 ノードと (Amazon EC2) インスタンスの両方で実行されます。
- リソースグループをターゲットとする関連付けを作成する場合、リソースグループには 5 つ以上のタグキー、または 1 つのタグキーに対して指定されている値以上のタグキーを割り当てらることはできません。リソースグループにこれらの条件のいずれかがタグとキーに適用される場合、関連付けの実行は失敗し、`InvalidTarget` エラーが返されます。
- タグを使用してリソースグループをターゲットにする関連付けを作成する場合、タグ値に [(空の値)] オプションを選択することはできません。
- リソースグループを削除すると、そのグループのすべてのインスタンスで関連付けが実行されなくなります。ベストプラクティスとして、グループをターゲットにする関連付けを削除します。
- 1 つの関連付けについて、ターゲットにできるのは 1 つのリソースグループだけです。複数のグループまたはネストされたグループはサポートされません。
- 関連付けを作成した後、State Manager によって関連付けはリソースグループのリソースに関する情報で定期的に更新されます。リソースグループに新しいリソースを追加する場合、システムによって新しいリソースに関連付けが適用されるスケジュールは、いくつかの要因によって異なります。関連付けのステータスは、Systems Manager コンソールの State Manager ページで確認できます。

> **Warning**
>
> Amazon EC2 インスタンスのリソースグループをターゲットにする関連付けを作成するアクセス許可を有する AWS Identity and Access Management (IAM) ユーザー、グループ、または ロールは、自動的にグループ内のすべてのインスタンスのルートレベルを制御することができます。信頼された管理者のみが関連付けの作成を許可されるようにしてください。

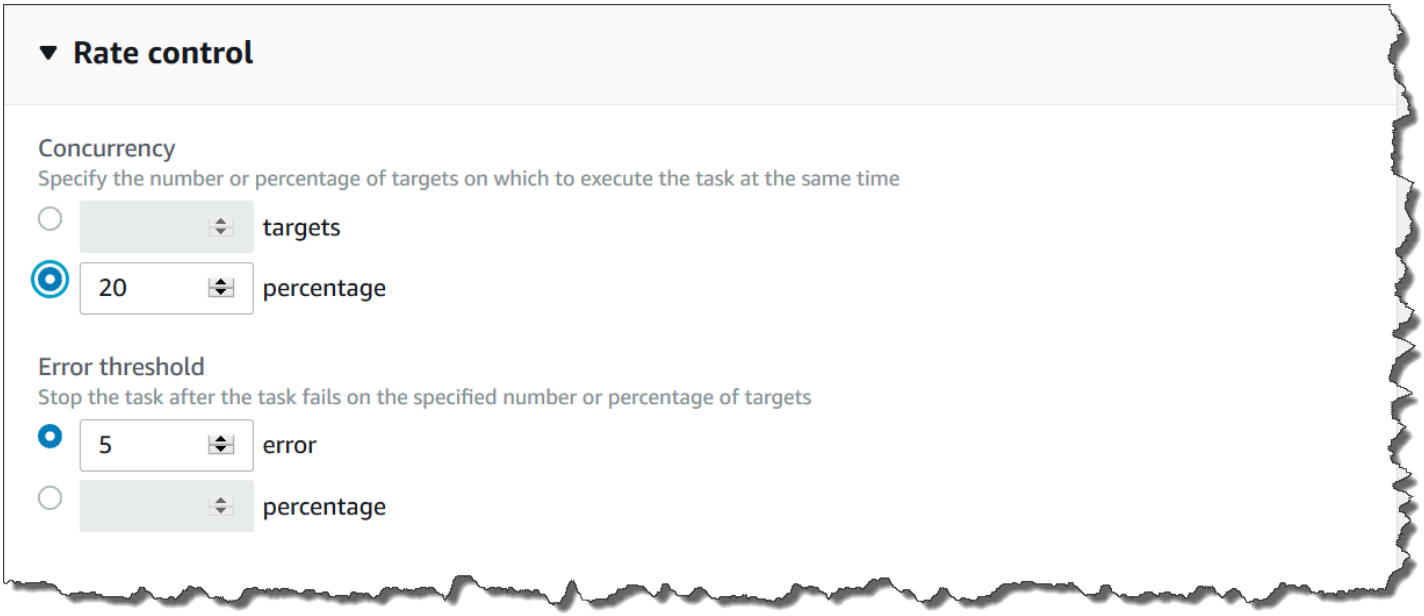
Resource Groups の詳細については、AWS Resource Groups ユーザーガイドの「AWS Resource Groups とは」を参照してください。

すべてのノードを選択する

このオプションを使用して、現在の AWS アカウント と AWS リージョン 内にあるすべてのノードをターゲットにします。このリクエストを実行すると、システムは現在の AWS アカウント と AWS リージョン 内にあるすべてのノードを検出し、関連付けの作成を試みます。システムは、最初に関連付けを作成すると、その関連付けを実行します。この最初の実行後、システムは指定されたスケジュールに従って関連付けを実行します。新しいノードを作成すると、システムは自動的に関連付けを適用し、すぐに実行した後、スケジュールに従って実行します。

レート制御の使用

同時実行値とエラーしきい値を指定することで、ノードでの関連付けの実行を制御できます。同時実行値には、関連付けを同時に実行できるノードの数を指定します。関連付けの実行の失敗回数がある値を上回ると、その関連付けが設定された各ノードに、Systems Manager が関連付けの実行を停止するコマンドを送信します。エラーしきい値には、その値を指定します。このコマンドは、次のスケジュールされた実行まで関連付けの実行を停止します。同時実行数とエラーのしきい値機能は、まとめてレート制御と呼ばれます。



同時実行

同時実行数は、一度に特定の数のノードだけが関連付けを処理できるよう指定することで、ノードへの影響を制限するのに役立ちます。ノードの絶対数 (20 など) またはノードのターゲットセットの割合 (10% など) を指定できます。

State Manager 同時実行数には次の制限と制約があります。

- ターゲットを使用して関連付けを作成することを選択した場合に、同時実行値を指定しないと、State Manager は最大同時実行数を自動的に 50 ノードにします。
- 同時実行数を使用する関連付けが実行されているときに、ターゲット基準に一致する新しいノードがオンラインになると、同時実行値を超えていない場合、新しいノードは関連付けを実行します。同時実行値を超えた場合、現在の関連付けの実行期間中、ノードは無視されます。ノードでは、次のスケジュールされた期間中に同時実行数の要件に適合している間は、関連付けが実行されます。
- 同時実行数を使用する関連付けを更新する場合に、更新されるときに 1 つまたは複数のノードがその関連付けを処理しているときは、関連付けを実行しているすべてのノードで完了となります。開始されていない関連付けは停止されます。実行中の関連付けが完了すると、関連付けが更新されたため、すべてのターゲットノードですぐに関連付けが再実行されます。関連付けが再び実行されると、同時実行数の値が適用されます。

エラーしきい値

関連付けの実行の失敗回数がある値を上回ると、その関連付けが設定された各ノードに、Systems Manager がコマンドを送信します。エラーしきい値には、その値を指定します。このコマンドは、次のスケジュールされた実行まで関連付けの実行を停止します。エラーの絶対数 (10 など) またはターゲットセットのパーセント数 (10% など) を指定できます。

たとえば、エラーの絶対数として 3 を指定した場合、4 番目のエラーが返されると、State Manager は停止コマンドを送信します。0 を指定すると、最初のエラー結果が返された後に State Manager は停止コマンドを送信します。

50 件の関連付けに対して 10% のエラーしきい値を指定した場合、6 番目のエラーが返されると、State Manager は停止コマンドを送信します。エラーのしきい値に達したときにすでに実行中の関連付けについては完了されますが、これらの関連付けのいくつかは失敗する可能性があります。エラーしきい値に指定された数より多くのエラーが発生しないようにするには、[同時実行数] 値を 1 に設定して、関連付けを 1 つずつ進めるようにします。

State Manager エラーしきい値には以下の制限と制約があります。

- エラーしきい値は、現在の間隔で適用されます。
- ステップレベルの詳細を含む各エラーに関する情報は、関連付け履歴に記録されます。
- ターゲットを使用して関連付けを作成することを選択したが エラーしきい値を指定しない場合、State Manager は 100% のエラーのしきい値を自動的に適用します。

関連付けの作成

AWS Systems Manager のツールである State Manager は、AWS リソースを定義された状態に保ち、設定のずれを軽減するのに役立ちます。これを行うために、State Manager は関連付けを使用します。関連付けとは、AWS リソースに割り当てる設定です。この設定では、リソースで維持したい状態を定義します。例えば、関連付けでは、アンチウイルスソフトウェアがマネージドノードにインストールされて実行されている必要があることや、特定のポートを閉じる必要があることなどを指定できます。

関連付けでは、設定を適用するスケジュールと、関連付けのターゲットを指定します。例えば、アンチウイルスソフトウェアに関する関連付けが AWS アカウントのすべてのマネージドノードで 1 日に 1 回実行されるとします。ソフトウェアがノードにインストールされていない場合、関連付けによって State Manager にインストールするように指示することができます。ソフトウェアがインストールされていてもサービスが実行されていない場合、関連付けによって State Manager にサービスを開始するように指示することができます。

> **Warning**
>
> 関連付けを作成するときは、関連付けのターゲットとしてマネージドノードの AWS リソースグループを選択できます。AWS Identity and Access Management (IAM) ユーザー、グループ、またはロールに、マネージドノードのリソースグループをターゲットとする関連付けを作成するアクセス許可がある場合、そのユーザー、グループ、またはロールは、自動的にグループ内のすべてのノードをルートレベルで制御することができます。信頼された管理者のみに関連付けの作成を許可するようにしてください。

関連付けのターゲットとレート制御

関連付けでは、関連付けを受け取るマネージドノードやターゲットも指定します。State Manager には、マネージドノードをターゲットにし、それらのターゲットに関連付けをデプロイする方法を制御するのに役立ついくつかの機能があります。ターゲットとレート制御の詳細については、「State Manager 関連付けのターゲットとレート制御について」を参照してください。

関連付けのタグ付け

AWS CLI や AWS Tools for PowerShell などのコマンドラインツールを使用して、関連付けを作成するときには、タグを割り当てることができます。Systems Manager コンソールを使用して関連付けにタグを追加することはできません。

関連付けの実行

デフォルトでは、関連付けを作成した直後に、定義したスケジュールに従って State Manager が関連付けを実行します。

また、システムは、次の規則に従って関連付けを実行することもできます。

- State Manager は関連付けを、指定されたノードまたはターゲットになっているノードすべてに対して、ある期間内に実行しようとします。
- 期間中に関連付けが実行されない場合 (例えば、同時実行値によって一度に関連付けを処理できるノード数が制限されたため)、State Manager は次の期間に関連付けを実行しようとします。
- State Manager は関連付けの設定、ターゲットノード、ドキュメント、またはパラメータが変更された後に、関連付けを実行します。詳細については、関連付けがリソースに適用されるタイミングについてを参照してください。
- State Manager は、すべてのスキップされた間隔の履歴を記録します。[Execution History (実行履歴)] タブで履歴を表示できます。

関連付けのスケジュール

関連付けを 10 時間ごとなどの基本的な間隔で実行するようにスケジュールすることも、カスタム cron と rate の式を使用してより高度なスケジュールを作成することもできます。また、関連付けを初めて作成するときに実行されないようにすることもできます。

関連付けを作成した後、cron 式または rate 式を使用する

標準の cron 式または rate 式の他に、State Manager はまた、関連付けを実行する曜日、および月の n 番目の日を指定する番号記号 (#) を含む cron 式もサポートしています。毎月、第 3 火曜日の 23:30 UTC に cron スケジュールを実行する例を次に示します。

```
cron(30 23 ? * TUE#3 *)
```

毎月第 2 木曜日の深夜 UTC に実行する例を次に示します。

```
cron(0 0 ? * THU#2 *)
```

State Manager はまた、月の最後の X 曜日を示す (L) 記号もサポートしています。毎月、最後の火曜日の深夜 UTC に cron スケジュールを実行する例を次に示します。

```
cron(0 0 ? * 3L *)
```

パッチした火曜日の 2 日後に関連付けを実行するなど、関連付けを実行するタイミングをさらに制御するには、オフセットを指定できます。オフセットでは、関連付けの実行がスケジュールされてい

る日の後に待機する日数を定義します。例えば、cron スケジュールを `cron(0 0 ? * THU#2 *)` とした場合、[Schedule offset] (スケジュールのオフセット) フィールドで番号 3 を指定して、その月の第 2 木曜日の後の毎週日曜日に関連付けを実行できます。

> **Note**
>
> オフセットを使用するには、コンソールの [次に指定した Cron の間隔でのみ関連付けを適用する] オプションを選択するか、コマンドラインから `ApplyOnlyAtCronInterval` パラメータを指定する必要があります。これらのオプションのいずれかをアクティブにすると、関連付けを作成した後、State Manager がすぐに実行されないようにできます。

cron 式と rate 式の詳細については、「リファレンス: Systems Manager の Cron 式および rate 式」を参照してください。

関連付けを作成する (コンソール)

次の手順では、Systems Manager コンソールを使用して、State Manager の関連付けを作成する方法について説明します。

> **Note**
>
> 以下の情報に注意してください。
>
> - この手順は、`Command` または `Policy` ドキュメントのどちらかを使用してマネージドノードをターゲットにする関連付けの作成方法を説明しています。Automation ランブックを使用してノードまたは他のタイプの AWS リソースをターゲットにする関連付けを作成する方法については、「State Manager 関連付けでのオートメーションのスケジュール設定」を参照してください。
> - 関連付けを作成するときに、AWS Management Consoleを使用して、最大 5 個のタグキーを指定できます。関連付けに指定されたすべてのタグキーが、現在ノードに割り当てられている必要があります。割り当てられていない場合、State Manager はノードを関連付けのターゲットにできません。

State Manager の関連付けを作成するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。

2. ナビゲーションペインで、[State Manager] を選択します。
3. [Create association] を選択します。
4. [Name (名前)] フィールドで名前を指定します。
5. [Document (ドキュメント)] リストで、ドキュメント名の横にあるオプションを選択します。ドキュメントタイプをメモしておきます。この手順は、`Command` および `Policy` ドキュメントに適用されます。オートメーションランブックを使用する関連付けの作成については、「State Manager 関連付けでのオートメーションのスケジュール設定」を参照してください。

   > **Important**
   >
   > ドキュメントが別のアカウントから共有されている場合、State Manager は新しいバージョンのドキュメントを使用する関連付けの実行をサポートしません。Systems Manager コンソールに新しいバージョンが処理されたことが示されていても、別のアカウントから共有される場合、State Manager は常にドキュメントの `default` バージョンを実行します。別なアカウントから共有されたドキュメントの新しいバージョンを使用して関連付けを実行する場合、ドキュメントバージョンを `default` に設定する必要があります。

6. [Parameters (パラメータ)] で、必要な入力パラメータを指定します。
7. (オプション) モニタリング用の関連付けに適用する CloudWatch アラームを選択します。

   > **Note**
   >
   > このステップに関する以下の情報に注意してください。
   >
   > - アラームリストには最大 100 個のアラームが表示されます。リストにアラームが表示されない場合は、AWS Command Line Interface を使用して関連付けを作成してください。詳細については、「関連付けの作成 (コマンドライン)」を参照してください。
   > - CloudWatch アラームをコマンドにアタッチするには、関連付けを作成する IAM プリンシパルに `iam:createServiceLinkedRole` アクションの権限が必要です。CloudWatch アラームの詳細については、「Amazon CloudWatch でのアラームの使用」を参照してください。
   > - アラームがアクティブ化されると、保留中のコマンド呼び出しまたはオートメーションは実行されません。

8. [Targets (ターゲット)] で、オプションを選択します。ターゲットの使用については、「State Manager 関連付けのターゲットとレート制御について」を参照してください。

> **Note**
>
> 新しいターゲットノードが検出されたときに、Automation ランブックで作成された関連付けを適用するには、特定の条件が満たされている必要があります。詳細については、「Automation ランブックによるターゲット更新について」を参照してください。

9. [Specify schedule (スケジュールの指定)] セクションで、[On Schedule (スケジュールあり)] または [No schedule (スケジュールなし)] を選択します。[On Schedule (スケジュールあり)] を選択した場合は、関連付けの cron または rate スケジュールを作成するためのボタンを使用します。

   作成直後に関連付けを実行しない場合は、[Apply association only at the next specified Cron interval (次に指定した Cron の間隔でのみ関連付けを適用する)] を選択します。

10. (オプション) [Schedule offset] (スケジュールオフセット) フィールドで、1～6 の数値を指定します。

11. [詳細オプション] セクションで、[コンプライアンスの重要度] を使用して関連付けの重大度を選択し、[Change Calendar] を使用して関連付けの変更カレンダーを選択します。

    コンプライアンスレポートには、ここで指定した重要度と共に関連付けの状態が準拠しているか準拠していないかが表示されます。詳細については、「State Manager 関連付けのコンプライアンスについて」を参照してください。

    変更カレンダーによって、関連付けが実行されるタイミングが決まります。カレンダーが閉じている場合、関連付けは適用されません。カレンダーが開いている場合は、それに応じて関連付けが実行されます。詳細については、「AWS Systems Manager Change Calendar」を参照してください。

12. [Rate control] (レート制御) セクションで、複数のノードでの関連付けの実行方法を制御するオプションを選択します。レート制御については、「State Manager 関連付けのターゲットとレート制御について」を参照してください。

    [Concurrency (同時実行数)] セクションでオプションを選択します。

    - [targets (ターゲット)] を選択して、関連付けを同時に実行できるターゲットの絶対数を入力します。
    - [percentage (パーセント値)] を選択して、関連付けを同時に実行できるターゲットセットのパーセント値を入力します。

[Error threshold (エラーのしきい値)] セクションでオプションを選択します。

- State Manager が追加ターゲットでの関連付けの実行を停止する前に、[errors (エラー)] を選択して許可されるエラーの絶対数を入力します。
- State Manager が追加ターゲットでの関連付けの実行を停止する前に、[percentage (パーセンテージ)] を選択して許可されるエラーの割合を入力します。

13. (オプション) [出力オプション] で、コマンド出力をファイルに保存するには、[S3 への出力の書き込みを有効にします] ボックスをオンにします。ボックスにバケット名とプレフィックス (フォルダ) 名を入力してください。

> **Note**
>
> S3 バケットにデータを書き込む機能を許可する S3 アクセス許可は、このタスクを実行する IAM ユーザーのものではなく、マネージドノードに割り当てられたインスタンスプロファイルのものです。詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」または「ハイブリッド環境に IAM サービスロールを作成する」を参照してください。さらに、指定された S3 バケットが別の AWS アカウント にある場合は、マネージドノードに関連付けられたインスタンスプロファイルまたは IAM サービスロールに、そのバケットへの書き込みに必要なアクセス許可があることを確認してください。

以下は、関連付けのために Amazon S3 出力をオンにするために必要な最小限のアクセス許可です。IAM ポリシーをアタッチすることで、アカウント内の個々のユーザーまたはロールへのアクセスをさらに制限することができます。最低でも、Amazon EC2 インスタンスプロファイルには、`AmazonSSMManagedInstanceCore` 管理ポリシーと次のインラインポリシーを持つ IAM ロールがある必要があります。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:PutObjectAcl"
```

```
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
        }
    ]
}
```

最小限のアクセス許可を得るには、エクスポート先の Amazon S3 バケットに Amazon S3 コンソールで定義されたデフォルト設定が必要です。Amazon S3 バケットの作成の詳細については、Amazon S3 ユーザーガイドの「バケットの作成」を参照してください。

> **Note**
>
> 関連付けの実行中に SSM ドキュメントによって開始される API オペレーションは、AWS CloudTrail でログ記録されません。

14. [関連付けの作成] を選択します。

> **Note**
>
> 作成した関連付けを削除すると、関連付けはそのターゲットで実行されなくなります。

関連付けの作成 (コマンドライン)

以下の手順では、AWS CLI (Linux または Windows の場合) または Tools for PowerShell を使用して、State Manager の関連付けを作成する方法について説明します。このセクションには、ターゲットとレート制御の使用方法を示すいくつかの例が含まれています。ターゲットとレート制御を使用すると、これらの関連付けの実行を制御しながら、関連付けを数十または数百のノードに割り当てることができます。ターゲットとレート制御の詳細については、「State Manager 関連付けのターゲットとレート制御について」を参照してください。

> **Important**
>
> この手順は、`Command` または `Policy` ドキュメントのどちらかを使用してマネージドノードをターゲットにする関連付けの作成方法を説明しています。Automation ランブックを使用してノードまたは他のタイプの AWS リソースをターゲットにする関連付けを作成する方法については、「State Manager 関連付けでのオートメーションのスケジュール設定」を参照してください。

[開始する前に]

targets パラメータは、指定した Key、Value の組み合わせを使用してノードをターゲットにする検索条件の配列です。targets パラメータを使用して数十または数百のノードで関連付けを作成する場合は、手順を開始する前に以下のターゲット設定オプションを確認してください。

ID を指定して特定のノードをターゲットにする

```
--targets Key=InstanceIds,Values=instance-id-1,instance-id-2,instance-id-3
```

```
--targets
 Key=InstanceIds,Values=i-02573cafcfEXAMPLE,i-0471e04240EXAMPLE,i-07782c72faEXAMPLE
```

タグを使用してインスタンスをターゲットにする

```
--targets Key=tag:tag-key,Values=tag-value-1,tag-value-2,tag-value-3
```

```
--targets Key=tag:Environment,Values=Development,Test,Pre-production
```

AWS Resource Groups を使用してノードをターゲットにする

```
--targets Key=resource-groups:Name,Values=resource-group-name
```

```
--targets Key=resource-groups:Name,Values=WindowsInstancesGroup
```

現在の AWS アカウント と AWS リージョン のすべてのインスタンスをターゲットに設定する

```
--targets Key=InstanceIds,Values=*
```

> **Note**
>
> 以下の情報に注意してください。
>
> - ドキュメントが別のアカウントから共有されている場合、State Manager は新しいバージョンのドキュメントを使用する関連付けの実行をサポートしません。Systems Manager コンソールに新しいバージョンが処理されたことが示されていても、別のアカウントから共有される場合、State Manager は常にドキュメントの default バージョンを実行しま

す。別なアカウントから共有されたドキュメントの新しいバージョンを使用して関連付けを実行する場合、ドキュメントバージョンを `default` に設定する必要があります。

- AWS CLI を使用して、最大 5 個のタグキーを指定できます。AWS CLI を使用する場合は、`create-association` コマンドで指定されたすべてのタグキーがノードに現在割り当てられている必要があります。割り当てられていない場合、State Manager はノードを関連付けのターゲットにできません。
- 関連付けを作成するときは、スケジュールの実行時を指定します。cron または rate 式を使用して、スケジュールを指定します。cron 式と rate 式の詳細については、「関連付けのための cron および rate 式」を参照してください。
- 新しいターゲットノードが検出されたときに、Automation ランブックで作成された関連付けを適用するには、特定の条件が満たされている必要があります。詳細については、「Automation ランブックによるターゲット更新について」を参照してください。

関連付けを作成するには

1. まだ AWS CLI または AWS Tools for PowerShell をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」および「AWS Tools for PowerShell のインストール」を参照してください。

2. 以下の形式を使用して、関連付けを作成する State Manager コマンドを作成します。各*##########*をユーザー自身の情報に置き換えます。

   Linux & macOS

```
aws ssm create-association \
    --name document_name \
    --document-version version_of_document_applied \
    --instance-id instances_to_apply_association_on \
    --parameters (if any) \
    --targets target_options \
    --schedule-expression "cron_or_rate_expression" \
    --apply-only-at-cron-interval required_parameter_for_schedule_offsets \
    --schedule-offset number_between_1_and_6 \
    --output-location s3_bucket_to_store_output_details \
    --association-name association_name \
    --max-errors a_number_of_errors_or_a_percentage_of_target_set \
    --max-concurrency a_number_of_instances_or_a_percentage_of_target_set \
```

```
    --compliance-severity severity_level \
    --calendar-names change_calendar_names \
    --target-locations aws_region_or_account \
    --tags "Key=tag_key,Value=tag_value"
```

Windows

```
aws ssm create-association ^
    --name document_name ^
    --document-version version_of_document_applied ^
    --instance-id instances_to_apply_association_on ^
    --parameters (if any) ^
    --targets target_options ^
    --schedule-expression "cron_or_rate_expression" ^
    --apply-only-at-cron-interval required_parameter_for_schedule_offsets ^
    --schedule-offset number_between_1_and_6 ^
    --output-location s3_bucket_to_store_output_details ^
    --association-name association_name ^
    --max-errors a_number_of_errors_or_a_percentage_of_target_set ^
    --max-concurrency a_number_of_instances_or_a_percentage_of_target_set ^
    --compliance-severity severity_level ^
    --calendar-names change_calendar_names ^
    --target-locations aws_region_or_account ^
    --tags "Key=tag_key,Value=tag_value"
```

PowerShell

```
New-SSMAssociation `
    -Name document_name `
    -DocumentVersion version_of_document_applied `
    -InstanceId instances_to_apply_association_on `
    -Parameters (if any) `
    -Target target_options `
    -ScheduleExpression "cron_or_rate_expression" `
    -ApplyOnlyAtCronInterval required_parameter_for_schedule_offsets `
    -ScheduleOffSet number_between_1_and_6 `
    -OutputLocation s3_bucket_to_store_output_details `
    -AssociationName association_name `
    -MaxError  a_number_of_errors_or_a_percentage_of_target_set
    -MaxConcurrency a_number_of_instances_or_a_percentage_of_target_set `
    -ComplianceSeverity severity_level `
    -CalendarNames change_calendar_names `
    -TargetLocations aws_region_or_account `
```

```
    -Tags "Key=tag_key,Value=tag_value"
```

次の例では、"Environment,Linux" でタグ付けされたノードで関連付けを作成します。関連付けは AWS-UpdateSSMAgent ドキュメントを使用して、毎週日曜日の午前 2 時 (UTC) にターゲットノード上の SSM Agent を更新します。この関連付けが同時に実行されるのは、常に最大 10 ノードです。また、エラー数が 5 を超えた場合、この実行期間内では、関連付けがそれ以降のノードで実行されなくなります。コンプライアンスレポートでは、この関連付けについて「中」の重要度レベルが割り当てられます。

Linux & macOS

```
aws ssm create-association \
  --association-name Update_SSM_Agent_Linux \
  --targets Key=tag:Environment,Values=Linux \
  --name AWS-UpdateSSMAgent  \
  --compliance-severity "MEDIUM" \
  --schedule-expression "cron(0 2 ? * SUN *)" \
  --max-errors "5" \
  --max-concurrency "10"
```

Windows

```
aws ssm create-association ^
  --association-name Update_SSM_Agent_Linux ^
  --targets Key=tag:Environment,Values=Linux ^
  --name AWS-UpdateSSMAgent  ^
  --compliance-severity "MEDIUM" ^
  --schedule-expression "cron(0 2 ? * SUN *)" ^
  --max-errors "5" ^
  --max-concurrency "10"
```

PowerShell

```
New-SSMAssociation `
  -AssociationName Update_SSM_Agent_Linux `
  -Name AWS-UpdateSSMAgent `
  -Target @{
      "Key"="tag:Environment"
      "Values"="Linux"
    } `
```

```
  -ComplianceSeverity MEDIUM `
  -ScheduleExpression "cron(0 2 ? * SUN *)" `
  -MaxConcurrency 10 `
  -MaxError 5
```

次の例では、ワイルドカード値 (*) を指定してノード ID をターゲットにしています。これにより、Systems Manager は現在の AWS アカウント と AWS リージョン 内にあるすべてのノードに関連付けを作成できます。この関連付けが同時に実行されるのは、常に最大 10 ノードです。また、エラー数が 5 を超えた場合、この実行期間内では、関連付けがそれ以降のノードで実行されなくなります。コンプライアンスレポートでは、この関連付けについて「中」の重要度レベルが割り当てられます。この関連付けでは、スケジュールオフセットが使用されます。つまり、指定された cron スケジュールの 2 日後に実行されます。また、ApplyOnlyAtCronInterval パラメータも含まれています。これは、スケジュールオフセットの使用に必要であり、関連付けが作成された直後に実行されないように指定しています。

Linux & macOS

```
aws ssm create-association \
  --association-name Update_SSM_Agent_Linux \
  --name "AWS-UpdateSSMAgent" \
  --targets "Key=instanceids,Values=*" \
  --compliance-severity "MEDIUM" \
  --schedule-expression "cron(0 2 ? * SUN#2 *)" \
  --apply-only-at-cron-interval \
  --schedule-offset 2 \
  --max-errors "5" \
  --max-concurrency "10" \
```

Windows

```
aws ssm create-association ^
  --association-name Update_SSM_Agent_Linux ^
  --name "AWS-UpdateSSMAgent" ^
  --targets "Key=instanceids,Values=*" ^
  --compliance-severity "MEDIUM" ^
  --schedule-expression "cron(0 2 ? * SUN#2 *)" ^
  --apply-only-at-cron-interval ^
  --schedule-offset 2 ^
  --max-errors "5" ^
```

```
  --max-concurrency "10" ^
  --apply-only-at-cron-interval
```

PowerShell

```
New-SSMAssociation `
  -AssociationName Update_SSM_Agent_All `
  -Name AWS-UpdateSSMAgent `
  -Target @{
      "Key"="InstanceIds"
      "Values"="*"
    } `
  -ScheduleExpression "cron(0 2 ? * SUN#2 *)" `
  -ApplyOnlyAtCronInterval `
  -ScheduleOffset 2 `
  -MaxConcurrency 10 `
  -MaxError 5 `
  -ComplianceSeverity MEDIUM `
  -ApplyOnlyAtCronInterval
```

次の例では、リソースグループでノードの関連付けを作成します。グループの名前は「HR-Department」です。関連付けは AWS-UpdateSSMAgent ドキュメントを使用して、毎週日曜日の午前 2 時 (UTC) にターゲットノード上の SSM Agent を更新します。この関連付けが同時に実行されるのは、常に最大 10 ノードです。また、エラー数が 5 を超えた場合、この実行期間内では、関連付けがそれ以降のノードで実行されなくなります。コンプライアンスレポートでは、この関連付けについて「中」の重要度レベルが割り当てられます。この関連付けは、指定された cron スケジュールで実行されます。作成直後に関連付けは実行されません。

Linux & macOS

```
aws ssm create-association \
  --association-name Update_SSM_Agent_Linux \
  --targets Key=resource-groups:Name,Values=HR-Department \
  --name AWS-UpdateSSMAgent  \
  --compliance-severity "MEDIUM" \
  --schedule-expression "cron(0 2 ? * SUN *)" \
  --max-errors "5" \
  --max-concurrency "10" \
  --apply-only-at-cron-interval
```

Windows

```
aws ssm create-association ^
  --association-name Update_SSM_Agent_Linux ^
  --targets Key=resource-groups:Name,Values=HR-Department ^
  --name AWS-UpdateSSMAgent  ^
  --compliance-severity "MEDIUM" ^
  --schedule-expression "cron(0 2 ? * SUN *)" ^
  --max-errors "5" ^
  --max-concurrency "10" ^
  --apply-only-at-cron-interval
```

PowerShell

```
New-SSMAssociation `
  -AssociationName Update_SSM_Agent_Linux `
  -Name AWS-UpdateSSMAgent `
  -Target @{
      "Key"="resource-groups:Name"
      "Values"="HR-Department"
    } `
  -ScheduleExpression "cron(0 2 ? * SUN *)" `
  -MaxConcurrency 10 `
  -MaxError 5 `
  -ComplianceSeverity MEDIUM `
  -ApplyOnlyAtCronInterval
```

次の例では、特定のノード ID でタグ付けされたノードで実行される関連付けを作成します。関連付けは、変更カレンダーが開いているときに、SSM Agent ドキュメントを使用して、ターゲットノードの SSM Agent を更新します。関連付けは、実行時にカレンダーの状態をチェックします。カレンダーが起動時に閉じられ、関連付けが 1 回だけ実行された場合、関連付けの実行ウィンドウが過ぎているため、再度実行されません。カレンダーが開いている場合は、それに応じて関連付けが実行されます。

> **Note**
>
> 変更カレンダーを閉じているときに関連付けが作用するタグまたはリソースグループに新しいノードを追加すると、変更カレンダーが開いたときにその関連付けがそれらのノードに適用されます。

Linux & macOS

```
aws ssm create-association \
  --association-name CalendarAssociation \
  --targets "Key=instanceids,Values=i-0cb2b964d3e14fd9f" \
  --name AWS-UpdateSSMAgent  \
  --calendar-names "arn:aws:ssm:us-east-1:123456789012:document/testCalendar1" \
  --schedule-expression "rate(1day)"
```

Windows

```
aws ssm create-association ^
  --association-name CalendarAssociation ^
  --targets "Key=instanceids,Values=i-0cb2b964d3e14fd9f" ^
  --name AWS-UpdateSSMAgent  ^
  --calendar-names "arn:aws:ssm:us-east-1:123456789012:document/testCalendar1" ^
  --schedule-expression "rate(1day)"
```

PowerShell

```
New-SSMAssociation `
  -AssociationName CalendarAssociation `
  -Target @{
      "Key"="tag:instanceids"
      "Values"="i-0cb2b964d3e14fd9f"
    } `
  -Name AWS-UpdateSSMAgent `
  -CalendarNames "arn:aws:ssm:us-east-1:123456789012:document/testCalendar1" `
  -ScheduleExpression "rate(1day)"
```

次の例では、特定のノード ID でタグ付けされたノードで実行される関連付けを作成します。関連付けは、SSM Agent ドキュメントを使用して、毎週日曜日の午前 2 時にターゲットノードで SSM Agent を更新します。この関連付けは、変更カレンダーが開いているときに、指定された cron スケジュールでのみ実行されます。関連付けが作成されると、カレンダーの状態がチェックされます。カレンダーが閉じている場合、関連付けは適用されません。関連付けを適用する間隔が日曜日の午前 2 時に開始されると、関連付けはカレンダーが開いているかどうかをチェックします。カレンダーが開いている場合は、それに応じて関連付けが実行されます。

> **Note**
>
> 変更カレンダーを閉じているときに関連付けが作用するタグまたはリソースグループに新しいノードを追加すると、変更カレンダーが開いたときにその関連付けがそれらのノードに適用されます。

Linux & macOS

```
aws ssm create-association \
  --association-name MultiCalendarAssociation \
  --targets "Key=instanceids,Values=i-0cb2b964d3e14fd9f" \
  --name AWS-UpdateSSMAgent  \
  --calendar-names "arn:aws:ssm:us-east-1:123456789012:document/testCalendar1"
 "arn:aws:ssm:us-east-2:123456789012:document/testCalendar2" \
  --schedule-expression "cron(0 2 ? * SUN *)"
```

Windows

```
aws ssm create-association ^
  --association-name MultiCalendarAssociation ^
  --targets "Key=instanceids,Values=i-0cb2b964d3e14fd9f" ^
  --name AWS-UpdateSSMAgent  ^
  --calendar-names "arn:aws:ssm:us-east-1:123456789012:document/testCalendar1"
 "arn:aws:ssm:us-east-2:123456789012:document/testCalendar2" ^
  --schedule-expression "cron(0 2 ? * SUN *)"
```

PowerShell

```
New-SSMAssociation `
```

```
  -AssociationName MultiCalendarAssociation `
  -Name AWS-UpdateSSMAgent `
  -Target @{
      "Key"="tag:instanceids"
      "Values"="i-0cb2b964d3e14fd9f"
    } `
  -CalendarNames "arn:aws:ssm:us-east-1:123456789012:document/testCalendar1"
"arn:aws:ssm:us-east-2:123456789012:document/testCalendar2" `
  -ScheduleExpression "cron(0 2 ? * SUN *)"
```

> **Note**
>
> 作成した関連付けを削除すると、関連付けはそのターゲットで実行されなくなります。また、apply-only-at-cron-interval パラメータを指定した場合は、このオプションをリセットできます。これを行うには、コマンドラインから関連付けを更新するときに no-apply-only-at-cron-interval パラメータを指定します。このパラメータは、関連付けの更新直後に、指定された間隔に従って関連付けを適用します。

関連付けの編集と新しいバージョンの作成

State Manager の関連付けを編集して、新しい名前、スケジュール、重大度レベル、ターゲット、またはその他の値を指定できます。SSM Command タイプのドキュメントに基づく関連付けについては、コマンドの出力を Amazon Simple Storage Service (Amazon S3) バケットに書き込むことも選択できます。関連付けを編集した後、State Manager で新しいバージョンが作成されます。編集後、次の手順で説明しているように、複数のバージョンを表示できます。

> **Note**
>
> 新しいターゲットノードが検出されたときに、Automation ランブックで作成された関連付けを適用するには、特定の条件が満たされている必要があります。詳細については、「Automation ランブックによるターゲット更新について」を参照してください。

次の手順では、Systems Manager コンソール、AWS Command Line Interface (AWS CLI)、および AWS Tools for PowerShell (Tools for PowerShell) を使用して、関連付けの新しいバージョンを編集および作成する方法について説明します。

> **Important**
>
> ドキュメントが別のアカウントから共有されている場合、State Manager は、そのドキュメントの新しいバージョンを使用する関連付けの実行をサポートしません。Systems Manager コンソールに新しいバージョンが処理されたことが表示されている場合でも、別のアカウントから共有されているときは、State Manager は、常にドキュメントの `default` バージョンを実行します。別なアカウントから共有されたドキュメントの新しいバージョンを使用して関連付けを実行する場合、ドキュメントバージョンを `default` に設定する必要があります。

関連付けを編集する (コンソール)

次の手順では、Systems Manager コンソールを使用して、関連付けの新しいバージョンを編集および作成する方法について説明します。

> **Note**
>
> Automation ランブックではなく、SSM Command ドキュメントを使用する関連付けの場合、この手順では既存の Amazon S3 バケットへの書き込みアクセス権が必要になります。Amazon S3 を初めて使用する場合は、Amazon S3 の使用料金が発生することに留意してください。バケットを作成する方法については、「バケットの作成」を参照してください。

State Manager の関連付けを編集するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[State Manager] を選択します。
3. 既存の関連付けを選択してから、[編集] を選択します。
4. 現在の要件を満たすように関連付けを再設定します。

   `Command` および `Policy` ドキュメントを使用した関連付けのオプションについては、「関連付けの作成」を参照してください。Automation ランブックを使用した関連付けのオプションについては、「State Manager 関連付けでのオートメーションのスケジュール設定」を参照してください。

5. [Save changes] (変更の保存) をクリックします。
6. (オプション) 関連付け情報を表示するには、[関連付け] ページで編集した関連付けの名前を選択してから、[バージョン] タブを選択します。システムが、作成および編集した関連付けの各バージョンを一覧表示します。
7. (オプション) SSM Command ドキュメントに基づく関連付けの出力を表示するには、次の手順を実行します。

   a. Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。

   b. コマンド出力の保存先として指定した Amazon S3 バケットの名前を選択し、関連付けを実行したノードの ID を使用して名前を付けたフォルダを選択します (出力の保存先としてバケット内のフォルダを選択した場合は、最初にそのフォルダを開きます)。

   c. `awsrunPowerShell` フォルダで数レベルをドリルダウンして、`stdout` ファイルを見つけます。

   d. [Open] または [Download] を選択してホスト名を表示します。

関連付けを編集する (コマンドライン)

次の手順では、AWS CLI (Linux または Windows の場合) または AWS Tools for PowerShell を使用して、関連付けの新しいバージョンを編集および作成する方法について説明します。

State Manager の関連付けを編集するには

1. まだ AWS CLI または AWS Tools for PowerShell をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」および「AWS Tools for PowerShell のインストール」を参照してください。
2. 既存の State Manager 関連付けの新しいバージョンを編集および作成するコマンドを作成するには、次の形式を使用します。各##############をユーザー自身の情報に置き換えます。

   > **Important**
   >
   > `update-association` を呼び出す場合、システムはリクエストのすべてのオプションパラメータを削除し、それらのパラメータにおいて関連付けを null 値で上書きします。これは仕様です。パラメータを変更しない場合でも、呼び出しのオプションパラメータをすべて指定する必要があります。これには `--name` パラメータが含まれます。このアクションを呼び出す前に、`describe-association` API オペレーションを呼び出し

て、update-association コールに必要なすべてのオプションパラメータをメモしておくことをお勧めします。

Linux & macOS

```
aws ssm update-association \
    --name document_name \
    --document-version version_of_document_applied \
    --instance-id instances_to_apply_association_on \
    --parameters (if any) \
    --targets target_options \
    --schedule-expression "cron_or_rate_expression" \
    --schedule-offset "number_between_1_and_6" \
    --output-location s3_bucket_to_store_output_details \
    --association-name association_name \
    --max-errors a_number_of_errors_or_a_percentage_of_target_set \
    --max-concurrency a_number_of_instances_or_a_percentage_of_target_set \
    --compliance-severity severity_level \
    --calendar-names change_calendar_names \
    --target-locations aws_region_or_account
```

Windows

```
aws ssm update-association ^
    --name document_name ^
    --document-version version_of_document_applied ^
    --instance-id instances_to_apply_association_on ^
    --parameters (if any) ^
    --targets target_options ^
    --schedule-expression "cron_or_rate_expression" ^
    --schedule-offset "number_between_1_and_6" ^
    --output-location s3_bucket_to_store_output_details ^
    --association-name association_name ^
    --max-errors a_number_of_errors_or_a_percentage_of_target_set ^
    --max-concurrency a_number_of_instances_or_a_percentage_of_target_set ^
    --compliance-severity severity_level ^
    --calendar-names change_calendar_names ^
    --target-locations aws_region_or_account
```

PowerShell

```
Update-SSMAssociation `
    -Name document_name `
    -DocumentVersion version_of_document_applied `
    -InstanceId instances_to_apply_association_on `
    -Parameters (if any) `
    -Target target_options `
    -ScheduleExpression "cron_or_rate_expression" `
    -ScheduleOffset "number_between_1_and_6" `
    -OutputLocation s3_bucket_to_store_output_details `
    -AssociationName association_name `
    -MaxError  a_number_of_errors_or_a_percentage_of_target_set
    -MaxConcurrency a_number_of_instances_or_a_percentage_of_target_set `
    -ComplianceSeverity severity_level `
    -CalendarNames change_calendar_names `
    -TargetLocations aws_region_or_account
```

次の例では、既存の関連付けを更新して名前を TestHostnameAssociation2 に変更します。新しい関連付けバージョンは 1 時間ごとに実行され、コマンドの出力を指定された Amazon S3 バケットに書き込みます。

Linux & macOS

```
aws ssm update-association \
  --association-id 8dfe3659-4309-493a-8755-01234EXAMPLE \
  --association-name TestHostnameAssociation2 \
  --parameters commands="echo Association" \
  --output-location S3Location='{OutputS3Region=us-
east-1,OutputS3BucketName=amzn-s3-demo-bucket,OutputS3KeyPrefix=logs}' \
  --schedule-expression "cron(0 */1 * * ? *)"
```

Windows

```
aws ssm update-association ^
  --association-id 8dfe3659-4309-493a-8755-01234EXAMPLE ^
  --association-name TestHostnameAssociation2 ^
  --parameters commands="echo Association" ^
  --output-location S3Location='{OutputS3Region=us-
east-1,OutputS3BucketName=amzn-s3-demo-bucket,OutputS3KeyPrefix=logs}' ^
```

```
  --schedule-expression "cron(0 */1 * * ? *)"
```

PowerShell

```
Update-SSMAssociation `
  -AssociationId b85ccafe-9f02-4812-9b81-01234EXAMPLE `
  -AssociationName TestHostnameAssociation2 `
  -Parameter @{"commands"="echo Association"} `
  -S3Location_OutputS3BucketName amzn-s3-demo-bucket `
  -S3Location_OutputS3KeyPrefix logs `
  -S3Location_OutputS3Region us-east-1 `
  -ScheduleExpression "cron(0 */1 * * ? *)"
```

次の例では、既存の関連付けを更新して名前を CalendarAssociation に変更します。新しい関連付けは、カレンダーが開いているときに実行され、指定された Amazon S3 バケットにコマンド出力を書き込みます。

Linux & macOS

```
aws ssm update-association \
  --association-id 8dfe3659-4309-493a-8755-01234EXAMPLE \
  --association-name CalendarAssociation \
  --parameters commands="echo Association" \
  --output-location S3Location='{OutputS3Region=us-
east-1,OutputS3BucketName=amzn-s3-demo-bucket,OutputS3KeyPrefix=logs}' \
  --calendar-names "arn:aws:ssm:us-east-1:123456789012:document/testCalendar2"
```

Windows

```
aws ssm update-association ^
  --association-id 8dfe3659-4309-493a-8755-01234EXAMPLE ^
  --association-name CalendarAssociation ^
  --parameters commands="echo Association" ^
  --output-location S3Location='{OutputS3Region=us-
east-1,OutputS3BucketName=amzn-s3-demo-bucket,OutputS3KeyPrefix=logs}' ^
  --calendar-names "arn:aws:ssm:us-east-1:123456789012:document/testCalendar2"
```

PowerShell

```
Update-SSMAssociation `
```

```
  -AssociationId b85ccafe-9f02-4812-9b81-01234EXAMPLE `
  -AssociationName CalendarAssociation `
  -AssociationName OneTimeAssociation `
  -Parameter @{"commands"="echo Association"} `
  -S3Location_OutputS3BucketName amzn-s3-demo-bucket `
  -CalendarNames "arn:aws:ssm:us-east-1:123456789012:document/testCalendar2"
```

次の例では、既存の関連付けを更新して名前を MultiCalendarAssociation に変更します。新しい関連付けは、カレンダーが開いているときに実行され、指定された Amazon S3 バケットにコマンド出力を書き込みます。

Linux & macOS

```
aws ssm update-association \
  --association-id 8dfe3659-4309-493a-8755-01234EXAMPLE \
  --association-name MultiCalendarAssociation \
  --parameters commands="echo Association" \
  --output-location S3Location='{OutputS3Region=us-
east-1,OutputS3BucketName=amzn-s3-demo-bucket,OutputS3KeyPrefix=logs}' \
  --calendar-names "arn:aws:ssm:us-east-1:123456789012:document/testCalendar1"
 "arn:aws:ssm:us-east-2:123456789012:document/testCalendar2"
```

Windows

```
aws ssm update-association ^
  --association-id 8dfe3659-4309-493a-8755-01234EXAMPLE ^
  --association-name MultiCalendarAssociation ^
  --parameters commands="echo Association" ^
  --output-location S3Location='{OutputS3Region=us-
east-1,OutputS3BucketName=amzn-s3-demo-bucket,OutputS3KeyPrefix=logs}' ^
  --calendar-names "arn:aws:ssm:us-east-1:123456789012:document/testCalendar1"
 "arn:aws:ssm:us-east-2:123456789012:document/testCalendar2"
```

PowerShell

```
Update-SSMAssociation `
  -AssociationId b85ccafe-9f02-4812-9b81-01234EXAMPLE `
  -AssociationName MultiCalendarAssociation `
  -Parameter @{"commands"="echo Association"} `
  -S3Location_OutputS3BucketName amzn-s3-demo-bucket `
```

```
  -CalendarNames "arn:aws:ssm:us-east-1:123456789012:document/testCalendar1"
 "arn:aws:ssm:us-east-2:123456789012:document/testCalendar2"
```

3. 関連付けの新しいバージョンを表示するには、次のコマンドを実行します。

Linux & macOS

```
aws ssm describe-association \
  --association-id b85ccafe-9f02-4812-9b81-01234EXAMPLE
```

Windows

```
aws ssm describe-association ^
  --association-id b85ccafe-9f02-4812-9b81-01234EXAMPLE
```

PowerShell

```
Get-SSMAssociation `
  -AssociationId b85ccafe-9f02-4812-9b81-01234EXAMPLE | Select-Object *
```

システムが以下のような情報を返します。

Linux & macOS

```
{
    "AssociationDescription": {
        "ScheduleExpression": "cron(0 */1 * * ? *)",
        "OutputLocation": {
            "S3Location": {
                "OutputS3KeyPrefix": "logs",
                "OutputS3BucketName": "amzn-s3-demo-bucket",
                "OutputS3Region": "us-east-1"
            }
        },
        "Name": "AWS-RunPowerShellScript",
        "Parameters": {
            "commands": [
                "echo Association"
            ]
        },
        "LastExecutionDate": 1559316400.338,
```

```
        "Overview": {
            "Status": "Success",
            "DetailedStatus": "Success",
            "AssociationStatusAggregatedCount": {}
        },
        "AssociationId": "b85ccafe-9f02-4812-9b81-01234EXAMPLE",
        "DocumentVersion": "$DEFAULT",
        "LastSuccessfulExecutionDate": 1559316400.338,
        "LastUpdateAssociationDate": 1559316389.753,
        "Date": 1559314038.532,
        "AssociationVersion": "2",
        "AssociationName": "TestHostnameAssociation2",
        "Targets": [
            {
                "Values": [
                    "Windows"
                ],
                "Key": "tag:Environment"
            }
        ]
    }
}
```

Windows

```
{
    "AssociationDescription": {
        "ScheduleExpression": "cron(0 */1 * * ? *)",
        "OutputLocation": {
            "S3Location": {
                "OutputS3KeyPrefix": "logs",
                "OutputS3BucketName": "amzn-s3-demo-bucket",
                "OutputS3Region": "us-east-1"
            }
        },
        "Name": "AWS-RunPowerShellScript",
        "Parameters": {
            "commands": [
                "echo Association"
            ]
        },
        "LastExecutionDate": 1559316400.338,
        "Overview": {
```

```
            "Status": "Success",
            "DetailedStatus": "Success",
            "AssociationStatusAggregatedCount": {}
        },
        "AssociationId": "b85ccafe-9f02-4812-9b81-01234EXAMPLE",
        "DocumentVersion": "$DEFAULT",
        "LastSuccessfulExecutionDate": 1559316400.338,
        "LastUpdateAssociationDate": 1559316389.753,
        "Date": 1559314038.532,
        "AssociationVersion": "2",
        "AssociationName": "TestHostnameAssociation2",
        "Targets": [
            {
                "Values": [
                    "Windows"
                ],
                "Key": "tag:Environment"
            }
        ]
    }
}
```

PowerShell

```
AssociationId                : b85ccafe-9f02-4812-9b81-01234EXAMPLE
AssociationName              : TestHostnameAssociation2
AssociationVersion           : 2
AutomationTargetParameterName :
ComplianceSeverity           :
Date                         : 5/31/2019 2:47:18 PM
DocumentVersion              : $DEFAULT
InstanceId                   :
LastExecutionDate            : 5/31/2019 3:26:40 PM
LastSuccessfulExecutionDate  : 5/31/2019 3:26:40 PM
LastUpdateAssociationDate    : 5/31/2019 3:26:29 PM
MaxConcurrency               :
MaxErrors                    :
Name                         : AWS-RunPowerShellScript
OutputLocation               :
 Amazon.SimpleSystemsManagement.Model.InstanceAssociationOutputLocation
Overview                     :
 Amazon.SimpleSystemsManagement.Model.AssociationOverview
```

```
Parameters                    : {[commands,
 Amazon.Runtime.Internal.Util.AlwaysSendList`1[System.String]]}
ScheduleExpression            : cron(0 */1 * * ? *)
Status                        :
Targets                       : {tag:Environment}
```

関連付けを削除する

AWS Systems Manager コンソールを使用して関連付けを削除するには、次の手順に従います。

関連付け提案を削除するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[State Manager] を選択します。
3. 関連付けを選択し、[削除] を選択します。

AWS Systems Manager コンソールから自動化を実行することで、1 回のオペレーションで複数の関連付けを削除できます。削除するアソシエーションを複数選択すると、State Manager はアソシエーション ID を入力パラメータ値として入力した状態で自動化ランブックの開始ページを起動します。

1 回のオペレーションで複数の関連付けを削除するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[State Manager] を選択します。
3. 削除するそれぞれの関連付けを選択し、[削除] を選択します。
4. (オプション) [追加入力パラメータ] 領域で、実行中に自動化に使用するロールの Amazon リソースネーム (ARN) を選択します。新しい IAM ロールを作成するには、[作成] を選択します。
5. [Submit] を選択します。

関連付けで Auto Scaling グループを実行する

関連付けを使用して Auto Scaling グループを実行する際のベストプラクティスは、タグターゲットを使用することです。タグを使用しないと、関連付けの制限に達する可能性があります。

すべてのノードに同じキーと値でタグ付けされている場合、Auto Scaling グループを実行するために必要な関連付けは 1 つだけです。以下の手順では、このような関連付けを作成する方法について説明します。

Auto Scaling グループを実行する関連付けを作成するには

1. Auto Scaling グループ内のすべてのノードに、同じキーと値でタグ付けされていることを確認します。ノードのタグ付けの詳細については、「AWS Auto Scaling ユーザーガイド」の「Tagging Auto Scaling groups and instances」(Auto Scaling グループとインスタンスにタグを付ける) を参照してください 。
2. Systems Manager の関連付けの使用 の手順を使用して、関連付けを作成します。

   コンソールで作業している場合は、[ターゲット] フィールドで [インスタンスタグを指定] を選択します。[インスタンスタグ] で、Auto Scaling グループのタグキーと値を入力します。

   AWS Command Line Interface (AWS CLI) を使用している場合は、`--targets Key=tag:tag-key,Values=tag-value` と指定します。キーと値はノードにタグ付けされたものと一致させます。

関連付けの履歴の表示

DescribeAssociationExecutions API オペレーションを使用して、特定の関連付け ID のすべての実行を表示できます。このオペレーションを使用して、State Manager の関連付けのステータス、詳細なステータス、結果、最終実行時間、および詳細情報を確認します。State Manager は AWS Systems Manager のツールです。この API オペレーションには、指定する条件に従って関連付けを見つけるのに役立つフィルターも含まれています。例えば、正確な日時を指定し、GREATER_THAN フィルターを使用して、指定の日時より後に処理された実行を表示できます。

例えば、関連付けの実行が失敗した場合、DescribeAssociationExecutionTargets API オペレーションを使用して、特定の実行を詳細にドリルダウンすることができます。このオペレーションにより、ノード ID など関連付けが実行されたリソース、およびさまざまな関連付けステータスが表示されます。これにより、どのリソースまたはノードで関連付けの実行に失敗したかを確認できます。リソース ID を使用して、コマンドのどのステップが失敗したかを示すコマンド実行の詳細を表示できます。

このセクションの例には、StartAssociationsOnce API オペレーションを使用して、作成時に関連付けを 1 回実行する方法についての情報も含まれています。この API オペレーションを失敗した関連付けの実行の調査に使用できます。関連付けが失敗した場合は、リソースを変更して直ちに関連付けを実行して、リソースの変更によって関連付けが正常に実行されるかどうかを確認できます。

> **Note**
>
> 関連付けの実行中に SSM ドキュメントによって開始される API オペレーションは、AWS CloudTrail で口グ記録されません。

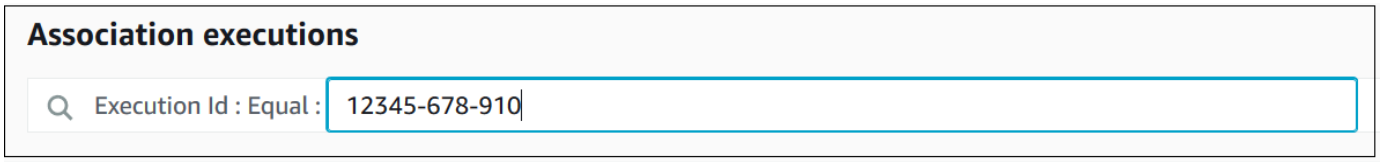
関連付けの履歴の表示 (コンソール)

次の手順を使用して、特定の関連付け ID の実行履歴を表示し、1 つ以上のリソースの実行の詳細を表示します。

特定の関連付け ID の実行履歴を表示するには

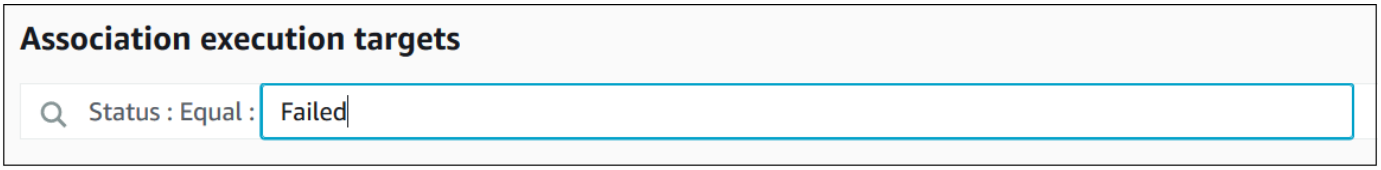
1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. State Manager を選択してください。
3. [Association id (アソシエーション ID)] フィールドで、履歴を表示する関連付けを選択します。
4. [View details (詳細を表示)] ボタンを選択します。
5. [Execution history (実行履歴の表示)] タブを選択します。
6. リソースレベルの実行の詳細を表示する関連付けを選択します。たとえば、ステータスが [Failed (失敗)] と表示される関連付けを選択します。これにより、関連付けの実行に失敗したノードの実行の詳細を表示できます。

   検索ボックスのフィルターを使用して、詳細を表示する実行を見つけます。

7. 実行 ID を選択します。[Association execution targets (関連付け実行ターゲット)] ページが開きます。このページには、関連付けを実行したすべてのリソースが表示されます。
8. リソースに関する固有の情報を表示するリソース ID を選択します。

   検索ボックスのフィルターを使用して、詳細を表示するリソースを見つけます。

9. 実行に失敗した関連付けを調査する場合は、[Apply association now] (関連付けを今すぐ適用) ボタンを使用して、作成時に関連付けを 1 回実行できます。関連付けの実行に失敗したリソースで変更をした後、ナビゲーションブレッドクラムで、[Association ID (関連 ID)] リンクを選択します。
10. [Apply association now (関連付けを今すぐ適用)] ボタンを選択します。実行が完了したら、関連付けの実行が成功したことを確認します。

関連付けの履歴の表示 (コマンドライン)

次の手順では、Linux または Windows の場合 AWS Command Line Interface (AWS CLI) または AWS Tools for PowerShell を使用して特定の関連付け ID の実行履歴を表示する方法について説明します。これに続いて、この手順では、1 つ以上のリソースの実行の詳細を表示する方法について説明します。

特定の関連付け ID の実行履歴を表示するには

1. まだ AWS CLI または AWS Tools for PowerShell をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」および「AWS Tools for PowerShell のインストール」を参照してください。
2. 以下のコマンドを実行して、特定の関連付け ID の実行を一覧表示します。

   Linux & macOS

```
aws ssm describe-association-executions \
  --association-id ID \
  --filters Key=CreatedTime,Value="2018-04-10T19:15:38.372Z",Type=GREATER_THAN
```

> **Note**
>
> このコマンドには、特定の日時以降に実行された実行のみに結果を限定するフィルタが含まれています。特定の関連付け ID のすべての実行を表示するには、`--filters` パラメータおよび `Key=CreatedTime,Value="2018-04-10T19:15:38.372Z",Type=GREATER_THAN` 値を削除します。

Windows

```
aws ssm describe-association-executions ^
  --association-id ID ^
  --filters Key=CreatedTime,Value="2018-04-10T19:15:38.372Z",Type=GREATER_THAN
```

> **Note**
>
> このコマンドには、特定の日時以降に実行された実行のみに結果を限定するフィルタが含まれています。特定の関連付け ID のすべての実行を表示するには、--filters パラメータおよび Key=CreatedTime,Value="2018-04-10T19:15:38.372Z",Type=GREATER_THAN 値を削除します。

PowerShell

```
Get-SSMAssociationExecution `
  -AssociationId ID `
  -Filter
 @{"Key"="CreatedTime";"Value"="2019-06-01T19:15:38.372Z";"Type"="GREATER_THAN"}
```

> **Note**
>
> このコマンドには、特定の日時以降に実行された実行のみに結果を限定するフィルタが含まれています。特定の関連付け ID のすべての実行を表示するには、-Filter パラメータおよび @{"Key"="CreatedTime";"Value"="2019-06-01T19:15:38.372Z";"Type"="GREAT 値を削除します。

システムが以下のような情報をレスポンスします。

Linux & macOS

```
{
   "AssociationExecutions":[
```

```
      {
         "Status":"Success",
         "DetailedStatus":"Success",
         "AssociationId":"c336d2ab-09de-44ba-8f6a-6136cEXAMPLE",
         "ExecutionId":"76a5a04f-caf6-490c-b448-92c02EXAMPLE",
         "CreatedTime":1523986028.219,
         "AssociationVersion":"1"
      },
      {
         "Status":"Success",
         "DetailedStatus":"Success",
         "AssociationId":"c336d2ab-09de-44ba-8f6a-6136cEXAMPLE",
         "ExecutionId":"791b72e0-f0da-4021-8b35-f95dfEXAMPLE",
         "CreatedTime":1523984226.074,
         "AssociationVersion":"1"
      },
      {
         "Status":"Success",
         "DetailedStatus":"Success",
         "AssociationId":"c336d2ab-09de-44ba-8f6a-6136cEXAMPLE",
         "ExecutionId":"ecec60fa-6bb0-4d26-98c7-140308EXAMPLE",
         "CreatedTime":1523982404.013,
         "AssociationVersion":"1"
      }
   ]
}
```

Windows

```
{
   "AssociationExecutions":[
      {
         "Status":"Success",
         "DetailedStatus":"Success",
         "AssociationId":"c336d2ab-09de-44ba-8f6a-6136cEXAMPLE",
         "ExecutionId":"76a5a04f-caf6-490c-b448-92c02EXAMPLE",
         "CreatedTime":1523986028.219,
         "AssociationVersion":"1"
      },
      {
         "Status":"Success",
         "DetailedStatus":"Success",
         "AssociationId":"c336d2ab-09de-44ba-8f6a-6136cEXAMPLE",
```

```
         "ExecutionId":"791b72e0-f0da-4021-8b35-f95dfEXAMPLE",
         "CreatedTime":1523984226.074,
         "AssociationVersion":"1"
      },
      {
         "Status":"Success",
         "DetailedStatus":"Success",
         "AssociationId":"c336d2ab-09de-44ba-8f6a-6136cEXAMPLE",
         "ExecutionId":"ecec60fa-6bb0-4d26-98c7-140308EXAMPLE",
         "CreatedTime":1523982404.013,
         "AssociationVersion":"1"
      }
   ]
}
```

PowerShell

```
AssociationId         : c336d2ab-09de-44ba-8f6a-6136cEXAMPLE
AssociationVersion    : 1
CreatedTime           : 8/18/2019 2:00:50 AM
DetailedStatus        : Success
ExecutionId           : 76a5a04f-caf6-490c-b448-92c02EXAMPLE
LastExecutionDate     : 1/1/0001 12:00:00 AM
ResourceCountByStatus : {Success=1}
Status                : Success

AssociationId         : c336d2ab-09de-44ba-8f6a-6136cEXAMPLE
AssociationVersion    : 1
CreatedTime           : 8/11/2019 2:00:54 AM
DetailedStatus        : Success
ExecutionId           : 791b72e0-f0da-4021-8b35-f95dfEXAMPLE
LastExecutionDate     : 1/1/0001 12:00:00 AM
ResourceCountByStatus : {Success=1}
Status                : Success

AssociationId         : c336d2ab-09de-44ba-8f6a-6136cEXAMPLE
AssociationVersion    : 1
CreatedTime           : 8/4/2019 2:01:00 AM
DetailedStatus        : Success
ExecutionId           : ecec60fa-6bb0-4d26-98c7-140308EXAMPLE
LastExecutionDate     : 1/1/0001 12:00:00 AM
ResourceCountByStatus : {Success=1}
Status                : Success
```

1 つ以上のフィルターを使用して、結果を制限することもできます。次の例では、特定の日時以前に実行されたすべての関連付けが返されます。

Linux & macOS

```
aws ssm describe-association-executions \
  --association-id ID \
  --filters Key=CreatedTime,Value="2018-04-10T19:15:38.372Z",Type=LESS_THAN
```

Windows

```
aws ssm describe-association-executions ^
  --association-id ID ^
  --filters Key=CreatedTime,Value="2018-04-10T19:15:38.372Z",Type=LESS_THAN
```

PowerShell

```
Get-SSMAssociationExecution `
  -AssociationId 14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE `
  -Filter
 @{"Key"="CreatedTime";"Value"="2019-06-01T19:15:38.372Z";"Type"="LESS_THAN"}
```

次の場合、特定の日時以降に正常に実行されたすべての関連付けが返されます。

Linux & macOS

```
aws ssm describe-association-executions \
  --association-id ID \
  --filters Key=CreatedTime,Value="2018-04-10T19:15:38.372Z",Type=GREATER_THAN
 Key=Status,Value=Success,Type=EQUAL
```

Windows

```
aws ssm describe-association-executions ^
  --association-id ID ^
  --filters Key=CreatedTime,Value="2018-04-10T19:15:38.372Z",Type=GREATER_THAN
 Key=Status,Value=Success,Type=EQUAL
```

PowerShell

```
Get-SSMAssociationExecution `
  -AssociationId 14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE `
  -Filter @{
      "Key"="CreatedTime";
      "Value"="2019-06-01T19:15:38.372Z";
      "Type"="GREATER_THAN"
    },
    @{
      "Key"="Status";
      "Value"="Success";
      "Type"="EQUAL"
    }
```

3. 特定の実行のすべてのターゲットを表示するには、次のコマンドを実行します。

Linux & macOS

```
aws ssm describe-association-execution-targets \
  --association-id ID \
  --execution-id ID
```

Windows

```
aws ssm describe-association-execution-targets ^
  --association-id ID ^
  --execution-id ID
```

PowerShell

```
Get-SSMAssociationExecutionTarget `
  -AssociationId 14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE `
  -ExecutionId 76a5a04f-caf6-490c-b448-92c02EXAMPLE
```

1 つ以上のフィルターを使用して、結果を制限することもできます。次の例では、特定の関連付けの実行に失敗したすべてのターゲットに関する情報が返されます。

Linux & macOS

```
aws ssm describe-association-execution-targets \
  --association-id ID \
  --execution-id ID \
  --filters Key=Status,Value="Failed"
```

Windows

```
aws ssm describe-association-execution-targets ^
  --association-id ID ^
  --execution-id ID ^
  --filters Key=Status,Value="Failed"
```

PowerShell

```
Get-SSMAssociationExecutionTarget `
  -AssociationId 14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE `
  -ExecutionId 76a5a04f-caf6-490c-b448-92c02EXAMPLE `
  -Filter @{
      "Key"="Status";
      "Value"="Failed"
    }
```

次の例では、関連付けの実行に失敗した特定のマネージドノードに関する情報が返されます。

Linux & macOS

```
aws ssm describe-association-execution-targets \
  --association-id ID \
  --execution-id ID \
  --filters Key=Status,Value=Failed Key=ResourceId,Value="i-02573cafcfEXAMPLE"
 Key=ResourceType,Value=ManagedInstance
```

Windows

```
aws ssm describe-association-execution-targets ^
  --association-id ID ^
  --execution-id ID ^
```

```
  --filters Key=Status,Value=Failed Key=ResourceId,Value="i-02573cafcfEXAMPLE"
 Key=ResourceType,Value=ManagedInstance
```

PowerShell

```
Get-SSMAssociationExecutionTarget `
  -AssociationId 14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE `
  -ExecutionId 76a5a04f-caf6-490c-b448-92c02EXAMPLE `
  -Filter @{
      "Key"="Status";
      "Value"="Success"
    },
    @{
      "Key"="ResourceId";
      "Value"="i-02573cafcfEXAMPLE"
    },
    @{
      "Key"="ResourceType";
      "Value"="ManagedInstance"
    }
```

4. 実行に失敗した関連付けを調査する場合、StartAssociationsOnce API オペレーションを使用して、関連付けを直ちに 1 回のみ実行できます。関連付けの実行に失敗したリソースを変更した後、関連付けをすぐに 1 回のみ実行する場合、次のコマンドを実行します。

   Linux & macOS

   ```
   aws ssm start-associations-once \
     --association-id ID
   ```

   Windows

   ```
   aws ssm start-associations-once ^
     --association-id ID
   ```

   PowerShell

   ```
   Start-SSMAssociationsOnce `
     -AssociationId ID
   ```

IAM を使用して関連付けを操作する

AWS Systems Manager のツールである State Manager は、ターゲットを使用して、関連付けを設定するインスタンスを選択します。元々、関連付けはドキュメント名 (Name) とインスタンス ID (InstanceId) を指定して作成されました。これで、ドキュメントとインスタンスまたはマネージドノードの間の関連付けが作成されました。これらのパラメータによって識別に使用される関連付け。これらのパラメータは廃止されましたが、引き続きサポートされます。リソース instance と managed-instance は Name および InstanceId を使用してアクションにリソースとして追加されました。

AWS Identity and Access Management (IAM) ポリシー適用の動作は、指定されたリソースのタイプによって異なります。State Manager オペレーションのリソースは、渡された要求に基づいてのみ適用されます。State Manager は、アカウント内のリソースのプロパティのディープチェックを実行しません。リクエストパラメータに指定されたポリシーリソースが含まれている場合、リクエストはポリシーリソースに対してのみ検証されます。例えば、リソースブロックでインスタンスを指定すると、リクエストが InstanceId パラメータを使用する場合にポリシーが適用されます。アカウント内の各リソースの Targets パラメータは、InstanceId に対してチェックされません。

以下は、混乱を招く動作の例です。

- DescribeAssociation、DeleteAssociation、UpdateAssociation は instance、managed-instance、および documentリソースを使用して、関連付けを参照する非推奨の方法を指定します。これには、InstanceId 非推奨パラメータで作成されたすべての関連付けが含まれます。
- CreateAssociation、 CreateAssociationBatch、および UpdateAssociation は、instance および managed-instance のリソースを使用して、関連付けを参照する非推奨の方法を指定します。これには、InstanceId 非推奨パラメータで作成されたすべての関連付けが含まれます。document のリソースタイプは、非推奨の関連付けを参照する方法の一部であり、関連付けの実際のプロパティです。つまり、ドキュメント名に基づいて、Create アクションと Update アクションの両方に対して、Allow または Deny のアクセス許可を持つ IAM ポリシーを作成できます。

Systems Manager と IAM ポリシーを使用する方法の詳細については、サービス許可リファレンスの「AWS Systems Manager のためのアイデンティティおよびアクセス管理」または「AWS Systems Manager のアクション、リソース、および条件キー」を参照してください。

MOF ファイルを実行する関連付けの作成

Managed Object Format (MOF) ファイルを実行すると、AWS-ApplyDSCMofs SSM ドキュメントを使用して、AWS Systems Manager のツールである State Manager によって Windows Server マネージドインノードに目的の状態を適用できます。AWS-ApplyDSCMofs ドキュメントには 2 つの実行モードがあります。最初のモードでは関連付けを設定して、マネージドノードが特定の MOF ファイルで定義されている目的の状態であるかどうかをスキャンおよびレポートできます。2 番目のモードでは MOF ファイルを実行して、MOF ファイルで定義されているリソースやその値に基づいてノードの設定を変更できます。AWS-ApplyDSCMofs ドキュメントを使用すると、Amazon Simple Storage Service (Amazon S3)、ローカル共有、または HTTPS ドメインを持つ安全なウェブサイトから MOF 設定ファイルをダウンロードして実行できます。

State Manager は、各関連付け実行中の各 MOF ファイルの実行状態を記録、報告します。State Manager はコンプライアンスイベントとして各 MOF ファイルの出力実行も報告し、AWS Systems Manager Compliance ページで確認できます。

MOF ファイルの実行は、Windows PowerShell Desired State Configuration (PowerShell DSC) で構築されています。PowerShell DSC は、Windows システムの設定、デプロイ、および管理で使用される宣言型のプラットフォームです。PowerShell DSC を使用すると、管理者は DSC 設定と呼ばれる、シンプルなテキストドキュメントで、サーバーの設定方法を記述できます。PowerShell DSC 設定は、何をするかを示しますがどうやって行うかは説明していない特殊な PowerShell スクリプトです。設定を実行すると MOF ファイルが生成されます。MOF ファイルは、1 台以上のサーバーに適用でき、それらのサーバーに必要な設定がなされています。PowerShell DSC リソースは実際の設定を強制する作業を行います。詳細については、「Windows PowerShell Desired State Configuration の概要」を参照してください。

トピック

- Amazon S3 を使用してアーティファクトを保存する
- MOF ファイルで認証情報を解決する
- MOF ファイルでトークンを使用する
- MOF ファイルを実行する関連付けを作成するための前提条件
- MOF ファイルを実行する関連付けの作成
- MOF ファイルを実行する関連付けを作成する際の問題のトラブルシューティング
- DSC リソースコンプライアンスの詳細の表示

Amazon S3 を使用してアーティファクトを保存する

Amazon S3 を使用して PowerShell モジュール、MOF ファイル、コンプライアンスレポート、またはステータスレポートを保存している場合、AWS Systems Manager SSM Agent で使用される AWS Identity and Access Management (IAM) ロールには、バケットに対する `GetObject` および `ListBucket` 許可が必要です。これらのアクセス許可を指定しない場合、システムにより「アクセスが拒否されました」エラーが返されます。Amazon S3 でのアーティファクトの保存に関する重要な情報を次に示します。

- バケットが他の AWS アカウント にある場合は、アカウント (または IAM ロール) に `GetObject` および `ListBucket` アクセス許可を付与するバケットリソースポリシーを作成します。
- カスタム DSC リソースを使用する場合は、Amazon S3 バケットからこれらのリソースをダウンロードできます。PowerShell ギャラリーから自動的にインストールすることもできます。
- Amazon S3 をモジュールのソースとして使用している場合は、*ModuleName_ModuleVersion*.zip という大文字と小文字が区別される形式の Zip ファイルとしてモジュールをアップロードします。例: MyModule_1.0.0.zip。
- すべてのファイルは、バケットルートに存在する必要があります。フォルダ構造はサポートされていません。

MOF ファイルで認証情報を解決する

認証情報は AWS Secrets Manager または AWS Systems Manager Parameter Store を使用して解決されます。これにより、認証情報の自動更新を設定します。これにより、DSC は MOF を再デプロイせずに、サーバーに認証情報を自動的に伝達することもできます。

設定で AWS Secrets Manager シークレットを使用するには、ユーザー名は認証情報が含まれるシークレットの SecretId または SecretARN で、PSCredential オブジェクトを作成します。パスワードには任意の値を指定できます。値は無視されます。次に例を示します。

```
Configuration MyConfig
{
   $ss = ConvertTo-SecureString -String 'a_string' -AsPlaintext -Force
   $credential = New-Object PSCredential('a_secret_or_ARN', $ss)

    Node localhost
    {
       File file_name
       {
           DestinationPath = 'C:\MyFile.txt'
```

```
            SourcePath = '\\FileServer\Share\MyFile.txt'
            Credential = $credential
        }
    }
}
```

設定データの PsAllowPlaintextPassword 設定を使用して、MOF をコンパイルします。認証情報にはラベルのみが含まれているため、これは問題ありません。

Secrets Manager で、IAM 管理ポリシー、および必要に応じて Secret Resource Policy (存在する場合) で GetSecretValue アクセス権がノードにあることを確認します。DSC を使用するには、シークレットは次の形式である必要があります。

```
{ 'Username': 'a_name', 'Password': 'a_password' }
```

このシークレットには、他のプロパティ (ローテーションに使用されるプロパティなど) を含められますが、少なくともユーザー名とパスワードのプロパティが必要です。

ここで、2 つの異なるをユーザー名とパスワードを持ち、ローテーション AWS Lambda 関数間で反転するマルチユーザーローテーションメソッドを使用することをお勧めします。この方法では、ローテーション中にユーザーをロックするリスクを排除しつつ複数のアクティブなアカウントを持てます。

MOF ファイルでトークンを使用する

トークンを使用すると、MOF をコンパイルした後にリソースプロパティ値を変更することもできます。これにより、類似の設定を必要とする複数のサーバーで共通の MOF ファイルを再利用できます。

トークン置換は、String 型のリソースプロパティに対してのみ機能します。ただし、リソースにネストされた CIM ノードプロパティがある場合、その CIM ノードの String プロパティからもトークンを解決します。数字または配列にはトークン置換を使用することはできません。

たとえば、xComputerManagement リソースを使用している場合に、DSC を使用してコンピュータの名前を変更するシナリオを考えてみましょう。通常はそのマシン専用の MOF ファイルが必要になります。ただし、トークンのサポートにより、単一の MOF ファイルを作成して、すべてのノードに適用できます。ComputerName プロパティでは、コンピュータ名を MOF にハードコーディングする代わりに、インスタンスタグタイプトークンを使用できます。この値は MOF 解析中に解決されます。次の例を参照してください。

```
Configuration MyConfig
```

```
{
    xComputer Computer
    {
        ComputerName = '{tag:ComputerName}'
    }
}
```

次に、Systems Manager コンソールのマネージドノード、または Amazon EC2 コンソールの Amazon Elastic Compute Cloud (Amazon EC2) タグのいずれかに、タグを設定します。ドキュメントを実行すると、スクリプトは {tag:ComputerName} トークンをインスタンスタグの値に置き換えます。

次の例に示すように、複数のタグを 1 つのプロパティに結合することもできます。

```
Configuration MyConfig
{
    File MyFile
    {
        DestinationPath = '{env:TMP}\{tag:ComputerName}'
        Type = 'Directory'
    }
}
```

トークンは、以下の 5 種類を使用できます。

- タグ: Amazon EC2 またはマネージドノードタグ。
- tagb64: これはタグと同じですが、システムは base64 を使用して値をデコードします。これによりタグの値に特殊文字を使用できます。
- env: 環境変数を解決します。
- ssm: Parameter Store 値。String 型および SecureString 型のみサポートされています。
- tagssm: これはタグと同じですが、ノードにタグが設定されていない場合、システムは、同じ名前の Systems Manager パラメータから値を解決しようとします。これが便利なのは、"デフォルトのグローバル値" が必要だが、1 つのノード (例えば、1 ボックスのデプロイ) で上書きできるようにする場合です。

`ssm` トークンタイプを使用する Parameter Store の例を以下に示します。

```
File MyFile
{
```

```
    DestinationPath = "C:\ProgramData\ConnectionData.txt"
    Content = "{ssm:%servicePath%/ConnectionData}"
}
```

トークンは MOF ファイルを一般的かつ再利用可能にすることで、冗長性のあるコードを削減する上で重要な役割を果たします。サーバー固有の MOF ファイルを避けられる場合は、MOF 構築サービスは必要ありません。MOF 構築サービスを使用すると、MOF がコンパイルされたときにビルドサーバーにインストールされているモジュールバージョンが異なるため、コストが増大し、プロビジョニング時間が遅くなり、グループ化されたノード間の設定がずれるリスクが増大します。

MOF ファイルを実行する関連付けを作成するための前提条件

MOF ファイルを実行する関連付けを作成する前に、マネージドノードが次の前提条件を満たしていることを確認します。

- Windows PowerShell バージョン 5.0 以降。詳細については、Microsoft.com の「Windows PowerShell のシステム要件」を参照してください。
- AWS Tools for Windows PowerShell バージョン 3.3.261.0 以降
- SSM Agent バージョン 2.2 以降。

MOF ファイルを実行する関連付けの作成

MOF ファイルを実行する関連付けを作成するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[State Manager] を選択します。
3. [State Manager] を選択してから、[関連付けの作成] を選択します。
4. [Name (名前)] フィールドで名前を指定します。これはオプションですが推奨されます。名前は、関連付け作成時の目的を理解する助けになります。名前にはスペースを使用できません。
5. [Document (ドキュメント)] リストで、[**AWS-ApplyDSCMofs**] を選択します。
6. [Parameters (パラメータ)] セクションで、必須およびオプションの入力パラメータを選択して指定します。

    a. [Mofs To Apply (適用する Mof)]: この関連付けが実行されるときに実行する 1 つまたは複数の MOF ファイルを指定します。MOF ファイルのリストを区切るには、カンマを使用します。MOF ファイルの検索では、以下のオプションを指定できます。

- Amazon S3 バケット名。バケット名には小文字を使用する必要があります。以下の形式を使用して、この情報を指定できます。

  ```
  s3:amzn-s3-demo-bucket:MOF_file_name.mof
  ```

  AWS リージョン を指定する場合は、次の形式を使用します。

  ```
  s3:bucket_Region:amzn-s3-demo-bucket:MOF_file_name.mof
  ```

- 安全なウェブサイト。以下の形式を使用して、この情報を指定できます。

  ```
  https://domain_name/MOF_file_name.mof
  ```

  以下はその例です。

  ```
  https://www.example.com/TestMOF.mof
  ```

- ローカル共有のファイルシステム。以下の形式を使用して、この情報を指定できます。

  ```
  \server_name\shared_folder_name\MOF_file_name.mof
  ```

  以下はその例です。

  ```
  \StateManagerAssociationsBox\MOFs_folder\MyMof.mof
  ```

b. [Service Path (サービスパス)]: (オプション) サービスパスは、レポートおよびステータス情報を書き込む Amazon S3 バケットのプレフィックスです。または、サービスパスは、Parameter Store パラメータベースのタグのパスです。パラメータベースのタグを解決する場合、システムは {ssm:%servicePath%/*parameter_name*} を使用して servicePath 値をパラメータ名に挿入します。たとえば、サービスパスが "WebServers/Production" の場合、システムはパラメータを WebServers/Production/*parameter_name* として解決します。これは、同じアカウントで複数の環境を実行している場合に便利です。

c. [Report Bucket Name (レポートバケット名)]: (オプション) コンプライアンスデータを書き込む Amazon S3 バケットの名前を入力します。レポートは JSON 形式で、このバケットに保存されます。

> **Note**
>
> バケット名の前に、バケットが配置されているリージョンのプレフィックスを付けることができます。例: us-west-2:MyMOFBucket。us-east-1 を含まない特定のリージョンの Amazon S3 エンドポイントのプロキシを使用している場合、バケット名にリージョンのプレフィックスを付けます。バケット名にプレフィックスがない場合は、us-east-1 エンドポイントを使用してバケットリージョンが自動的に検出されます。

d. Mof Operation Mode: **`AWS-ApplyDSCMofs`** の関連付けを実行するときの State Manager の動作を選択します。

- [Apply] (適用): 準拠していないノード設定を修正します。
- [ReportOnly]: ノードの設定を修正しませんが、代わりにすべてのコンプライアンスデータをログに記録し、準拠していないノードをレポートします。

e. [Status Bucket Name (ステータスバケット名)]: (オプション) MOF 実行ステータス情報を書き込む Amazon S3 バケットの名前を入力します。これらのステータスレポートは、最新のコンプライアンスを実行したノードのシングルトンの概要です。つまり、次回関連付けが MOF ファイルで実行されるとレポートが上書きされることを意味します。

> **Note**
>
> バケット名の前に、バケットが配置されているリージョンのプレフィックスを付けることができます。例えば、`us-west-2:amzn-s3-demo-bucket` のようにします。us-east-1 を含まない特定のリージョンの Amazon S3 エンドポイントのプロキシを使用している場合、バケット名にリージョンのプレフィックスを付けます。バケット名のプレフィックスが付いていない場合、us-east-1 エンドポイントを使用してバケットリージョンが自動的に検出されます。

f. [Module Source Bucket Name (モジュールソースバケット名)]: (オプション) PowerShell モジュールファイルが格納されている Amazon S3 バケットの名前を入力します。[None] (なし) を指定した場合、次のオプションの [Allow PS Gallery Module Source] (PS ギャラリーモジュールソースを許可) で [True] を選択します。

> **Note**
>
> バケット名の前に、バケットが配置されているリージョンのプレフィックスを付けることができます。例えば、`us-west-2:amzn-s3-demo-bucket` のようにします。us-east-1 を含まない特定のリージョンの Amazon S3 エンドポイントのプロキシを使用している場合、バケット名にリージョンのプレフィックスを付けます。バケット名のプレフィックスが付いていない場合、us-east-1 エンドポイントを使用してバケットリージョンが自動的に検出されます。

g. [Allow PS Gallery Module Source]: (オプション) https://www.powershellgallery.com/ から PowerShell モジュールをダウンロードする場合は True を選択します。[False] を選択した場合、前のオプション [ModuleSourceBucketName] のソースを指定します。

h. [Proxy Uri]: (オプション) このオプションを使用して、プロキシサーバーから MOF ファイルをダウンロードします。

i. [Reboot Behavior]: (オプション) MOF ファイルの実行に再起動が必要な場合は、以下のいずれかの再起動の動作を指定します。

- [AfterMof]: すべての MOF の実行完了後にノードを再起動します。複数の MOF 実行が再起動をリクエストしても、システムはすべての MOF 実行が完了して再起動するまで待機します。
- [Immediately] (即時): MOF 実行がリクエストするたびにノードを再起動します。再起動をリクエストする複数の MOF ファイルを実行する場合、ノードは複数回再起動します。
- [Never] (しない): MOF 実行が明示的に再起動をリクエストしても、ノードは再起動されません。

j. [Use Computer Name For Reporting] (レポートにコンピュータの名前を使用): (オプション) このオプションを有効にすると、コンプライアンス情報をレポートするときにコンピュータの名前を使用します。デフォルト値は [false] です。つまり、システムはコンプライアンス情報をレポートするときにノード ID を使用します。

k. [Enable VerboseLogging] (VerboseLogging を有効にする): (オプション) 初めての MOF ファイルのデプロイ時には、詳細ログ記録を有効にすることをお勧めします。

> **Important**
>
> 詳細ログ記録を有効にすると、標準の関連付けの実行ログ記録より多くのデータを Amazon S3 バケットに書き込みます。その結果、パフォーマンスが低下

し、Amazon S3 のストレージ費用が増加する場合があります。ストレージサイズの問題を軽減するには、Amazon S3 バケットに対してライフサイクルポリシーを有効にすることをお勧めします。詳細については、Amazon Simple Storage Service ユーザーガイドの「S3 バケットのライフサイクルポリシーを作成する方法を教えてください」を参照してください。

l. [Enable Debug Logging] (デバッグログの有効化): (オプション) MOF 障害のトラブルシューティングを行うために、デバッグログを有効にすることをお勧めします。また、通常の使用ではこのオプションを非アクティブ化することをお勧めします。

> **Important**
>
> デバッグログ記録を有効にすると、標準の関連付けの実行ログ記録より多くのデータを Amazon S3 バケットに書き込みます。その結果、パフォーマンスが低下し、Amazon S3 のストレージ費用が増加する場合があります。ストレージサイズの問題を軽減するには、Amazon S3 バケットに対してライフサイクルポリシーを有効にすることをお勧めします。詳細については、Amazon Simple Storage Service ユーザーガイドの「S3 バケットのライフサイクルポリシーを作成する方法を教えてください」を参照してください。

m. [Compliance Type (コンプライアンスタイプ)]: (オプション) コンプライアンス情報をレポートするときに使用するコンプライアンスタイプを指定します。デフォルトのコンプライアンスタイプは [Custom:DSC] です。MOF ファイルを実行する複数の関連付けを作成する場合は、各関連付けに異なるコンプライアンスタイプを指定します。指定していない場合、[Custom:DSC] を使用する追加の各関連付けが既存のコンプライアンスデータを上書きします。

n. [Pre Reboot Script]: (オプション) 再起動が必要な設定がある場合に実行するスクリプトを指定します。再起動する前に、スクリプトが実行されます。このスクリプトは 1 行にする必要があります。追加の行はセミコロンで区切ります。

7. [Targets (ターゲット)] セクションで、[タグの指定] または [インスタンスの手動選択] を選択します。タグを使用してターゲットリソースを選択した場合は、タグキーとタグ値をフィールドに入力します。ターゲットの使用の詳細については、「State Manager 関連付けのターゲットとレート制御について」を参照してください。

8. [Specify schedule (スケジュールの指定)] セクションで、[On Schedule (スケジュールあり)] または [No schedule (スケジュールなし)] を選択します。[On Schedule (スケジュールあり)] を選択した場合、関連付けの cron または rate スケジュールを作成するためのボタンを使用します。

9. [Advanced options (アドバンスドオプション)] セクションで、以下の操作を行います。

   - [Compliance severity (コンプライアンスの重要度)] で、関連付けの重要度レベルを選択します。コンプライアンスレポートには、ここで指定した重要度と共に関連付けの状態が準拠しているか準拠していないかが表示されます。詳細については、「State Manager 関連付けのコンプライアンスについて」を参照してください。

10. [Rate control] (レート制御) セクションで、マネージドノードのフリート全体の State Manager 関連付けを実行するためのオプションを設定します。これらのパラメータの詳細については、State Manager 関連付けのターゲットとレート制御についてを参照してください。

    [Concurrency (同時実行数)] セクションでオプションを選択します。

    - [targets (ターゲット)] を選択して、関連付けを同時に実行できるターゲットの絶対数を入力します。
    - [percentage (パーセント値)] を選択して、関連付けを同時に実行できるターゲットセットのパーセント値を入力します。

    [Error threshold (エラーのしきい値)] セクションでオプションを選択します。

    - State Manager が追加ターゲットでの関連付けの実行を停止する前に、[errors (エラー)] を選択して許可されるエラーの絶対数を入力します。
    - State Manager が追加ターゲットでの関連付けの実行を停止する前に、[percentage (パーセンテージ)] を選択して許可されるエラーの割合を入力します。

11. (オプション) [出力オプション] で、コマンド出力をファイルに保存するには、[S3 への出力の書き込みを有効にします] ボックスをオンにします。ボックスにバケット名とプレフィックス (フォルダ) 名を入力してください。

    > **Note**
    >
    > S3 バケットにデータを書き込む機能を許可する S3 アクセス許可は、このタスクを実行する IAM ユーザーのものではなく、マネージドノードに割り当てられたインスタンスプロファイルのものです。詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」または「ハイブリッド環境に IAM サービスロールを作成する」を参照してください。さらに、指定された S3 バケットが別の AWS アカウント にある場合は、マネージドノードに関連付けられたインスタンスプロファイルまたは IAM

サービスロールに、そのバケットへの書き込みに必要なアクセス許可があることを確認してください。

12. [関連付けの作成] を選択します。

State Manager は、指定されたノードまたはターゲットで関連付けを作成してすぐに実行します。最初の実行後、関連付けは定義したスケジュールと以下のルールに従って間隔を空けて実行されます。

- State Manager は、期間の開始時にオンラインのノードには関連付けを実行し、オフラインのノードはスキップします。
- State Manager は、期間中に設定されたすべてのノードで関連付けを実行しようとします。
- 期間中に関連付けが実行されない場合 (例えば、同時実行値によって一度に関連付けを処理できるノード数が制限されたため)、State Manager は次の期間に関連付けを実行しようとします。
- State Manager は、すべてのスキップされた間隔の履歴を記録します。[Execution History (実行履歴)] タブで履歴を表示できます。

> **Note**
>
> `AWS-ApplyDSCMofs` は、Systems Manager のコマンドドキュメントです。つまり、AWS Systems Manager のツールである Run Command を使用してこのドキュメントを実行することもできます。詳細については、「AWS Systems Manager Run Command」を参照してください。

MOF ファイルを実行する関連付けを作成する際の問題のトラブルシューティング

このセクションには、MOF ファイルを実行する関連付けの作成に関する問題のトラブルシューティングに役立つ情報が収められています。

拡張ログ記録を有効にする

トラブルシューティングの最初のステップとして、拡張ログ記録を有効にします。具体的には次の操作を行います。

1. 関連付けが Amazon S3 または Amazon CloudWatch Logs (CloudWatch) のいずれかにコマンド出力を書き込むように設定されていることを確認します。
2. [Enable Verbose Logging (詳細ログ記録の有効化)] パラメータを True に設定します。

3. [Enable Debug Logging (デバッグログの有効化)] パラメータを True に設定します。

詳細とデバッグの口グ記録をオンにすると、[Stdout] 出力ファイルにはスクリプトの実行に関する詳細が含まれます。この出力ファイルは、失敗したスクリプトを特定するの役立ちます。[Stderr] 出力ファイルにはスクリプトの実行中に発生したエラーが含まれています。

MOF ファイルを実行する関連付けの作成する際のよくある問題

このセクションでは、MOF ファイルを実行する関連付けを作成する際に発生する可能性のある一般的な問題の情報と、これらの問題をトラブルシューティングする手順を説明します。

MOF が適用されませんでした

State Manager がノードへの関連付けの適用に失敗した場合は、まず Stderr 出力ファイルを確認します。このファイルは、問題の根本的な原因を理解する助けになります。また、以下についても確認してください。

- ノードに、MOF に関連するすべての Amazon S3 バケットに必要なアクセス許可があること。具体的には次のとおりです。
  - [s3:GetObject permissions]: これはプライベート Amazon S3 バケット内の MOF ファイルおよび Amazon S3 バケット内のカスタムモジュールに必要です。
  - [s3:PutObject permission]: これはコンプライアンスレポートおよびコンプライアンスのステータスを Amazon S3 バケットに書き込むために必要です。
- タグを使用している場合は、ノードに必要な IAM ポリシーがあることを確認します。タグを使用するには、インスタンスの IAM ロールに `ec2:DescribeInstances` および `ssm:ListTagsForResource` アクションを許可するポリシーが必要です。
- ノードに想定されているタグ、または SSM パラメータが割り当てられていることを確認します。
- タグまたは SSM パラメータが間違っていないことを確認します。
- MOF をノードでローカルに適用してみて、MOF ファイル自体に問題はないことを確認します。

MOF が失敗したように見えたが、Systems Manager の実行は成功した

`AWS-ApplyDSCMofs` ドキュメントが正常に実行された場合、Systems Manager の実行ステータスには [Success (成功)] と表示されます。このステータスには、MOF ファイルの設定要件に対するノードのコンプライアンスステータスは反映されていません。ノードのコンプライアンスステータスを確認するには、コンプライアンスレポートを確認します。JSON レポートは、Amazon S3 Report Bucket で表示できます。これは、Run Command および State Manager の実行に適用されます。ま

た、State Manager の場合は、[Systems Manager Compliance] ページでコンプライアンスの詳細を表示できます。

Stderr states: サービスに到達した際の名前解決の失敗

このエラーは、スクリプトがリモートサービスに到達できないことを示しています。ほとんどの場合、スクリプトは Amazon S3 に到達できません。この問題は、スクリプトがドキュメントパラメータで指定されている Amazon S3 バケットにコンプライアンスレポートまたはコンプライアンスステータスを書き込もうとするときによく発生します。通常、このエラーはコンピューティング環境で許可リストが含まれるファイアウォールまたは透過プロキシを使用したときに発生します。この問題を解決するには。

- すべての Amazon S3 バケットのパラメータにリージョン固有のバケット構文を使用します。たとえば、[Mofs to Apply] パラメータは次の形式にする必要があります。

  s3:*bucket-region*:*amzn-s3-demo-bucket*:*mof-file-name*.mof。

  以下はその例です。 `s3:us-west-2:amzn-s3-demo-bucket:my-mof.mof`

  レポート、ステータス、およびモジュールのソースバケット名は次の形式にする必要があります。

  bucket-region:*amzn-s3-demo-bucket*。次に例を示します。`us-west-1:amzn-s3-demo-bucket;`
- リージョン固有の構文でも問題が解決しない場合は、ターゲットのノードが希望するリージョンの Amazon S3 にアクセスできることを確認します。これを確認するには。
  1. 適切な Amazon S3 リージョンで、Amazon S3 のエンドポイント名を見つけます。詳細については、「Amazon Web Services 全般のリファレンス」の「Amazon S3 サービスエンドポイント」を参照してください。
  2. ターゲットノードにログオンして、次の ping コマンドを実行します。

     ```
     ping s3.s3-region.amazonaws.com
     ```

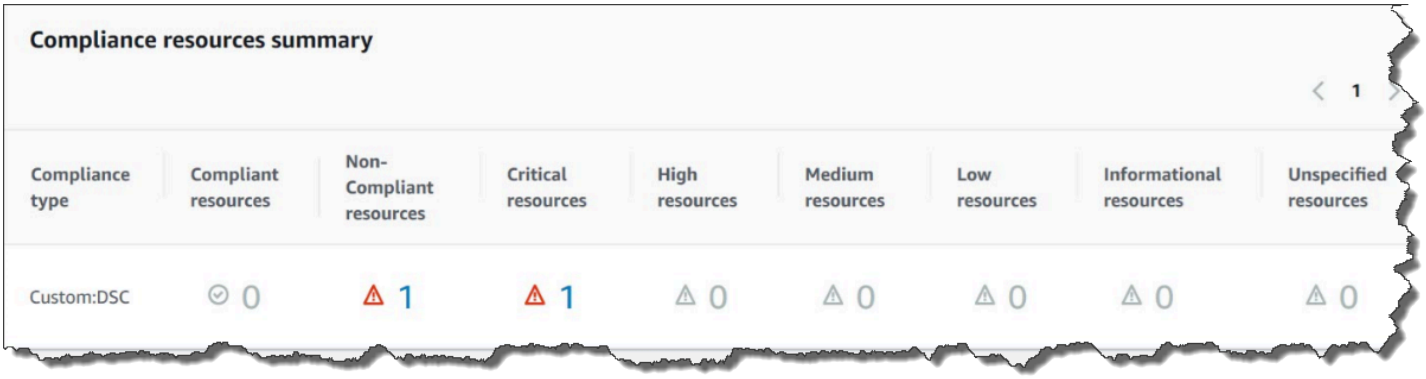
     ping が失敗した場合は、Amazon S3 がダウンしているか、ファイアウォール/透過プロキシが Amazon S3 のリージョンへのアクセスをブロックしているか、ノードがインターネットにアクセスできないかのいずれかです。

DSC リソースコンプライアンスの詳細の表示

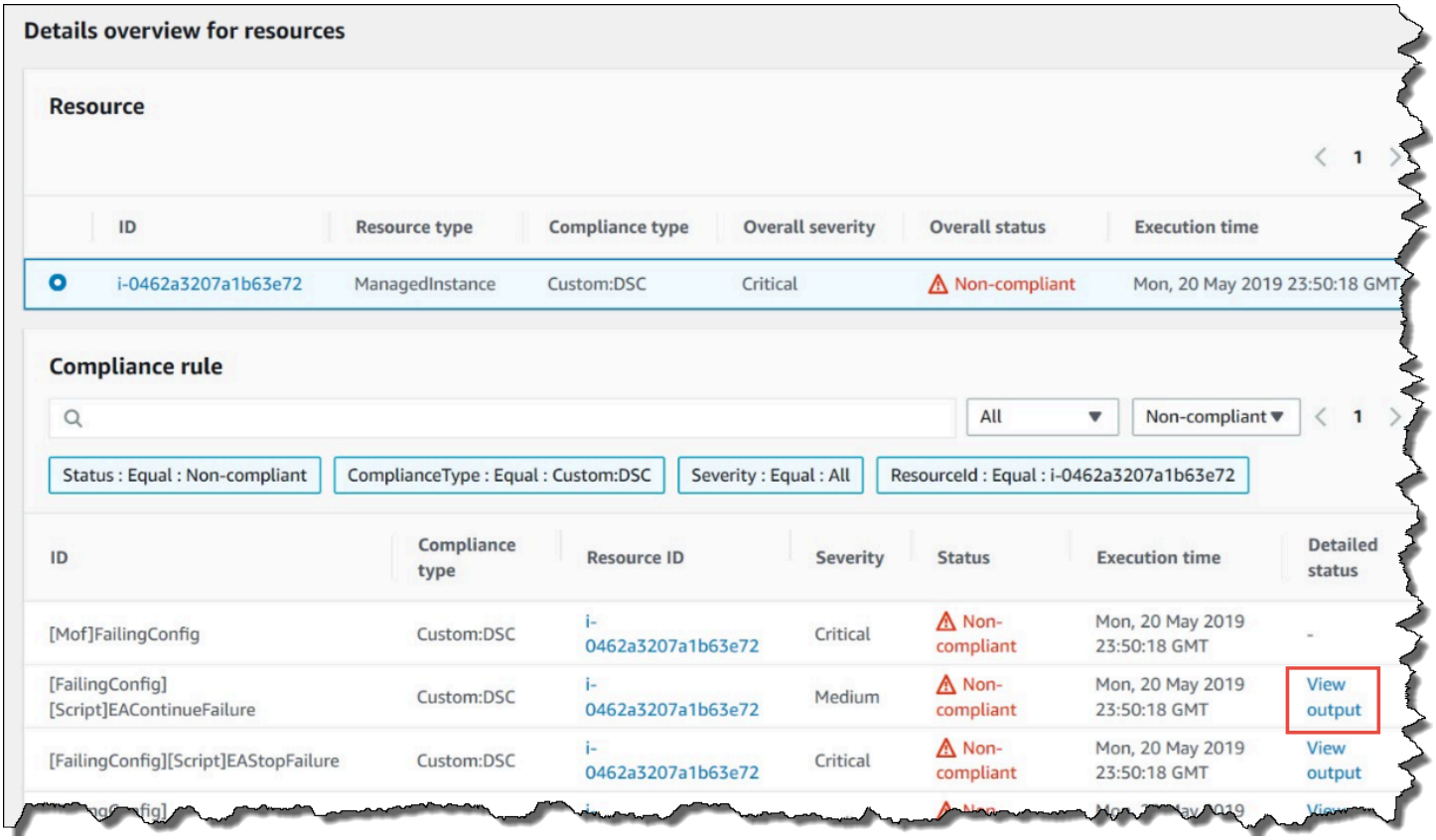
Systems Manager は、AWS-ApplyDSCMofs ドキュメントを実行したときに指定した Amazon S3 Status Bucket に DSC リソース障害に関するコンプライアンス情報をキャプチャします。Amazon S3 バケット内の DSC リソース障害に関する情報を検索するには、時間がかかる場合があります。代わりに、この情報を [Systems Manager Compliance] ページで表示できます。

[コンプライアンスリソースの概要] セクションには、失敗したリソース数が表示されます。次の例では、[ComplianceType] は [Custom:DSC] であり、1 つのリソースは準拠していません。

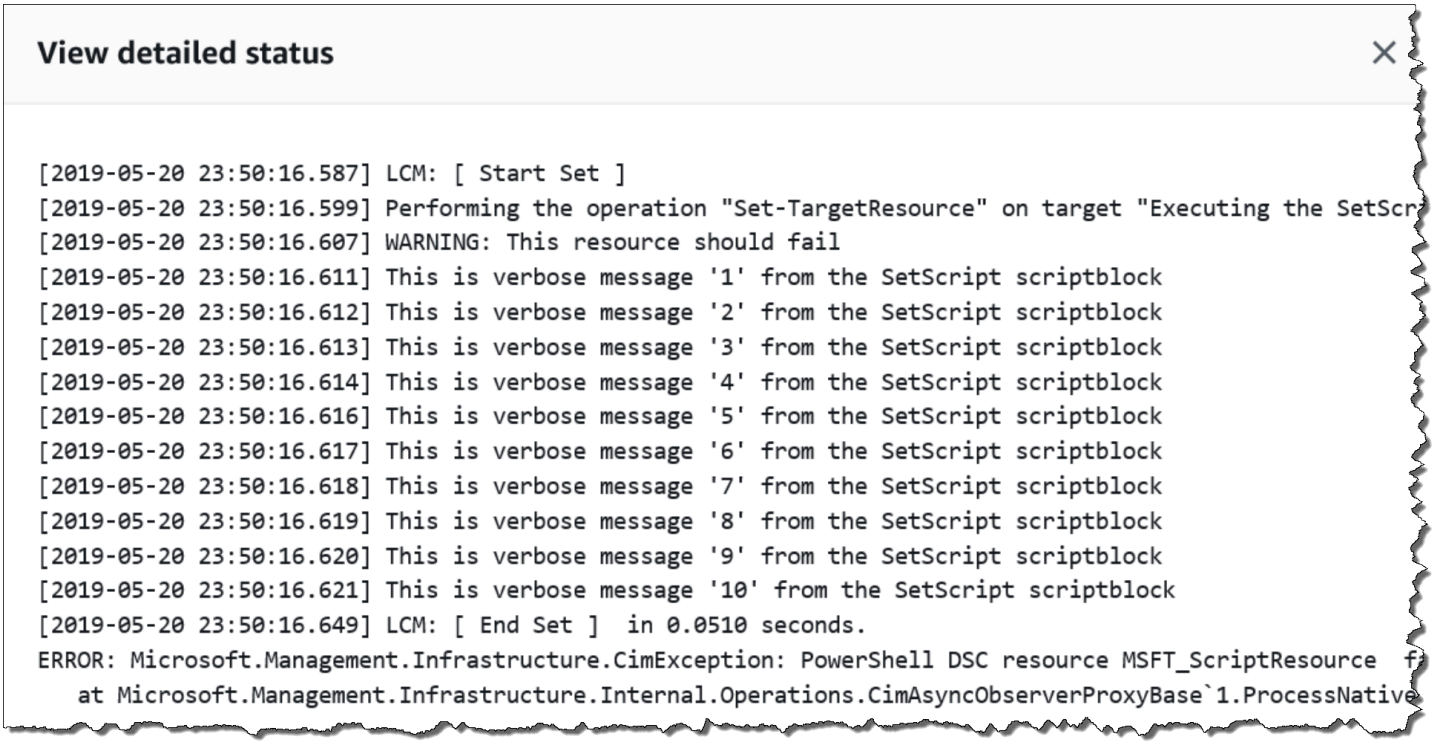
> **Note**
>
> カスタム: DSC は、AWS-ApplyDSCMofs ドキュメントのデフォルトの ComplianceType 値です。この値はカスタマイズすることができます。



[Details overview for resources] (リソースの詳細概要) セクションには、非準拠の DSC リソースを含む AWS リソースに関する情報が表示されます。このセクションには、MOF 名、スクリプト実行ステップ、および (該当する場合) 詳細な状況情報を表示するための [View output (出力の表示)] リンクも含まれています。



[出力の表示] リンクには、詳細ステータスの最後の 4,000 文字が表示されます。Systems Manager は、最初の要素としてまず例外を表示した後、詳細メッセージを検索して、4,000 文字のクォータに達するまで先頭に追加して表示します。このプロセスでは、例外がスローされる前に出力されたログメッセージが表示されます。表示されるメッセージは、トラブルシューティングに最もよく関連しています。



コンプライアンス情報の表示方法については、「AWS Systems Manager のコンプライアンス」を参照してください。

コンプライアンスレポートに影響する状況

State Manager の関連付けに失敗した場合、準拠データは報告されません。具体的には、MOF で処理できない場合は関連付けに失敗するため、Systems Manager はコンプライアンス項目をレポートしません。例えば、ノードにアクセス許可が付与されていない Amazon S3 バケットの MOF を Systems Manager でダウンロードしようとすると、関連付けは失敗し、コンプライアンスデータはレポートされません。

2 つめの MOF のリソースに失敗した場合、Systems Manager はコンプライアンスデータをレポートしません。例えば、MOF が存在しないドライブにファイルを作成しようとすると、AWS-ApplyDSCMofs ドキュメントは完全に処理できるため、Systems Manager は準拠をレポートします。これは、関連付けが正常に実行されたことを意味します。

Ansible プレイブックを実行する関連付けの作成

AWS-ApplyAnsiblePlaybooks SSM ドキュメントを使用して、Ansible プレイブックを実行する State Manager の関連付けを作成できます。State Manager は AWS Systems Manager のツールです。このドキュメントには、プレイブックを実行するための以下の利点があります。

- 複雑なプレイブックの実行のサポート
- GitHub と Amazon Simple Storage Service (Amazon S3) からのプレイブックのダウンロードをサポート
- 圧縮されたプレイブック構造のサポート
- 高度なログ記録
- プレイブックがバンドルされているときに実行するプレイブックを指定する機能

> **Note**
>
> Systems Manager には、Ansible プレイブックを実行する State Manager の関連付けを作成できる、AWS-RunAnsiblePlaybook と AWS-ApplyAnsiblePlaybooks という 2 つの SSM ドキュメントが含まれています。AWS-RunAnsiblePlaybook ドキュメントは廃止されました。これは、従来の目的のために Systems Manager で引き続き使用できます。ここで説明する機能強化のため、AWS-ApplyAnsiblePlaybooks ドキュメントを使用することをお勧めします。
>
> Ansible プレイブックを実行する関連付けは、macOS ではサポートされていません。

複雑なプレイブックの実行のサポート

AWS-ApplyAnsiblePlaybooks ドキュメントは、指定されたメインプレイブックを実行する前に、ファイル構造全体をローカルディレクトリにコピーするため、バンドルされた複雑なプレイブックをサポートします。ソースプレイブックは、Zip ファイルまたはディレクトリ構造で提供できます。Zip ファイルまたはディレクトリは、GitHub または Amazon S3 に保存できます。

GitHub からのプレイブックのダウンロードのサポート

AWS-ApplyAnsiblePlaybooks ドキュメントでは、aws:downloadContent プラグインを使用してプレイブックファイルをダウンロードします。ファイルは、単一のファイルで GitHub に保存することも、結合された一連のプレイブックファイルとして保存することもできます。GitHub からコンテンツをダウンロードするには、GitHub リポジトリに関する情報を JSON 形式で指定します。以下はその例です。

```
{
   "owner":"TestUser",
   "repository":"GitHubTest",
   "path":"scripts/python/test-script",
   "getOptions":"branch:master",
```

```
    "tokenInfo":"{{ssm-secure:secure-string-token}}"
}
```

Amazon S3 からのプレイブックのダウンロードのサポート

Ansible プレイブックは、単一の .zip ファイルまたはディレクトリ構造として Amazon S3 に保存およびダウンロードすることもできます。Amazon S3 からコンテンツをダウンロードするには、ファイルへのパスを指定します。これらはその 2 つの例です。

例 1: 特定のプレイブックファイルをダウンロードする

```
{
    "path":"https://s3.amazonaws.com/amzn-s3-demo-bucket/playbook.yml"
}
```

例 2: ディレクトリの内容をダウンロードする

```
{
    "path":"https://s3.amazonaws.com/amzn-s3-demo-bucket/ansible/webservers/"
}
```

> **Important**
>
> Amazon S3 を指定する場合は、マネージドノードの AWS Identity and Access Management (IAM) インスタンスプロファイルに S3 バケットのアクセス許可が含まれている必要があります。詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」を参照してください。

圧縮されたプレイブック構造のサポート

AWS-ApplyAnsiblePlaybooks ドキュメントを使用すると、圧縮された .zip ファイルをダウンロードしたバンドルで実行できます。ドキュメントは、ダウンロードしたファイルに .zip 形式の圧縮ファイルが含まれているかどうかを確認します。.zip が見つかった場合、ドキュメントは自動的にファイルを解凍し、指定された Ansible 自動化を実行します。

高度なログ記録

AWS-ApplyAnsiblePlaybooks ドキュメントには、さまざまなレベルのログ記録を指定するためのオプションのパラメータが含まれています。詳細度が低い場合は -v、中程度の場合は -vv または -

vvv、デバッグレベルのログ記録の場合は -vvvv を指定します。これらのオプションは、Ansible の詳細オプションに直接マッピングされます。

プレイブックがバンドルされているときに実行するプレイブックを指定する機能

AWS-ApplyAnsiblePlaybooks ドキュメントには、複数のプレイブックがバンドルされている場合に実行するプレイブックを指定するための必須パラメータが含まれています。このオプションでは、さまざまなユースケースをサポートするためにプレイブックを実行するための柔軟性が得られます。

インストールされている依存関係について

[InstallDependencies] パラメータに [True] を指定すると、Systems Manager は次の依存関係がノードにインストールされていることを確認します。

- Ubuntu Server/Debian Server: Apt-get (パッケージ管理)、Python 3、Ansible、Unzip
- Amazon Linux: Ansible
- RHEL: Python 3、Ansible、Unzip

1 つまたは複数のこれらの依存関係が見つからない場合は、Systems Manager によって自動的にインストールされます。

Ansible プレイブックを実行する関連付けを作成する (コンソール)

以下の手順では、Systems Manager コンソールを使用し、AWS-ApplyAnsiblePlaybooks ドキュメントを使って Ansible プレイブックを実行する State Manager の関連付けを作成する方法について説明します。

Ansible プレイブックを実行する関連付けを作成するには (コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[State Manager] を選択します。
3. [State Manager] を選択してから、[関連付けの作成] を選択します。
4. [名前] に、関連付けの目的を思い出すのに役立つ名前を指定します。
5. [Document (ドキュメント)] リストで、[**AWS-ApplyAnsiblePlaybooks**] を選択します。
6. [パラメータ] セクションの [ソースタイプ] リストで、[GitHub] または [S3] を選択します。

GitHub

[GitHub] を選択した場合は、リポジトリ情報を次の形式で指定します。

```
{
   "owner":"user_name",
   "repository":"name",
   "path":"path_to_directory_or_playbook_to_download",
   "getOptions":"branch:branch_name",
   "tokenInfo":"{{(Optional)_token_information}}"
}
```

S3

[S3] を選択した場合は、パス情報を次の形式で指定します。

```
{
   "path":"https://s3.amazonaws.com/path_to_directory_or_playbook_to_download"
}
```

7. [依存関係のインストール] にオプションを選択します。
8. （オプション）[プレイブックファイル] にファイル名を入力します。Zip ファイルにプレイブックが含まれている場合は、Zip ファイルへの相対パスを指定します。
9. (オプション) [追加の変数] に、実行時に State Manager から Ansible に送信する変数を入力します。
10. （オプション）[チェック] にオプションを選択します。
11. （オプション）[詳細] にオプションを選択します。
12. [Targets (ターゲット)] で、オプションを選択します。ターゲットの使用については、「State Manager 関連付けのターゲットとレート制御について」を参照してください。
13. [Specify schedule (スケジュールの指定)] セクションで、[On schedule(スケジュールあり)] または [No schedule (スケジュールなし)] を選択します。[On Schedule (スケジュールあり)] を選択した場合は、関連付けの cron または rate スケジュールを作成するためのボタンを使用します。
14. [詳細オプション] セクションの [Compliance severity (コンプライアンスの重要度)] で、関連付けの重要度レベルを選択します。コンプライアンスレポートには、ここで指定した重要度と共に関連付けの状態が準拠しているか準拠していないかが表示されます。詳細については、「State Manager 関連付けのコンプライアンスについて」を参照してください。

15. [Rate control] (レート制御) セクションで、マネージドノードのフリート全体の State Manager 関連付けを実行するためのオプションを設定します。レート制御の使用については、「State Manager 関連付けのターゲットとレート制御について」を参照してください。

    [Concurrency (同時実行数)] セクションでオプションを選択します。

    - [targets (ターゲット)] を選択して、関連付けを同時に実行できるターゲットの絶対数を入力します。
    - [percentage (パーセント値)] を選択して、関連付けを同時に実行できるターゲットセットのパーセント値を入力します。

    [Error threshold (エラーのしきい値)] セクションでオプションを選択します。

    - State Manager が追加ターゲットでの関連付けの実行を停止する前に、[errors (エラー)] を選択して許可されるエラーの絶対数を入力します。
    - State Manager が追加ターゲットでの関連付けの実行を停止する前に、[percentage (パーセンテージ)] を選択して許可されるエラーの割合を入力します。
16. (オプション) [出力オプション] で、コマンド出力をファイルに保存するには、[S3 への出力の書き込みを有効にします] ボックスをオンにします。ボックスにバケット名とプレフィックス (フォルダ) 名を入力してください。

    > **Note**
    >
    > S3 バケットにデータを書き込む機能を許可する S3 アクセス許可は、このタスクを実行する IAM ユーザーのものではなく、マネージドノードに割り当てられたインスタンスプロファイルのものです。詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」または「ハイブリッド環境に IAM サービスロールを作成する」を参照してください。さらに、指定された S3 バケットが別の AWS アカウント にある場合は、マネージドノードに関連付けられたインスタンスプロファイルまたは IAM サービスロールに、そのバケットへの書き込みに必要なアクセス許可があることを確認してください。
17. [関連付けの作成] を選択します。

> **Note**
>
> タグを使用して 1 つまたは複数のターゲットノードで関連付けを作成した後、ノードからタグを削除すると、そのノードは関連付けを実行しなくなります。ノードは State Manager ドキュメントから関連付けを解除されます。

Ansible プレイブックを実行する関連付けを作成する (CLI)

以下の手順では、AWS Command Line Interface (AWS CLI) を使用し、`AWS-ApplyAnsiblePlaybooks` ドキュメントを使って Ansible プレイブックを実行する State Manager の関連付けを作成する方法について説明します。

Ansible プレイブックを実行する関連付けを作成するには (CLI)

1. まだ AWS Command Line Interface (AWS CLI) をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」を参照してください。

2. タグを使ってノードをターゲットにし、Ansible プレイブックを実行する関連付けを作成する場合は、次のいずれかのコマンドを実行します。各*###############*をユーザー自身の情報に置き換えます。コマンド (A) は、ソースタイプとして GitHub を指定します。コマンド (B) は、ソースタイプとして Amazon S3 を指定します。

   (A) GitHub ソース

   Linux & macOS

```
aws ssm create-association --name "AWS-ApplyAnsiblePlaybooks" \
    --targets Key=tag:TagKey,Values=TagValue \
    --parameters '{"SourceType":["GitHub"],"SourceInfo":
["{\"owner\":\"owner_name\", \"repository\": \"name\",
 \"getOptions\": \"branch:master\"}"],"InstallDependencies":
["True_or_False"],"PlaybookFile":["file_name.yml"],"ExtraVariables":["key/
value_pairs_separated_by_a_space"],"Check":["True_or_False"],"Verbose":["-v,-
vv,-vvv, or -vvvv"],"TimeoutSeconds":["3600"]}' \
    --association-name "name" \
    --schedule-expression "cron_or_rate_expression"
```

Windows

```
aws ssm create-association --name "AWS-ApplyAnsiblePlaybooks" ^
    --targets Key=tag:TagKey,Values=TagValue ^
    --parameters '{"SourceType":["GitHub"],"SourceInfo":
["{\"owner\":\"owner_name\", \"repository\": \"name\",
 \"getOptions\": \"branch:master\"}"],"InstallDependencies":
["True_or_False"],"PlaybookFile":["file_name.yml"],"ExtraVariables":["key/
value_pairs_separated_by_a_space"],"Check":["True_or_False"],"Verbose":["-v,-
vv,-vvv, or -vvvv"], "TimeoutSeconds":["3600"]}' ^
    --association-name "name" ^
    --schedule-expression "cron_or_rate_expression"
```

以下はその例です。

```
aws ssm create-association --name "AWS-ApplyAnsiblePlaybooks" \
    --targets "Key=tag:OS,Values=Linux" \
    --parameters '{"SourceType":["GitHub"],"SourceInfo":["{\"owner\":
\"ansibleDocumentTest\", \"repository\": \"Ansible\", \"getOptions\":
 \"branch:master\"}"],"InstallDependencies":["True"],"PlaybookFile":["hello-world-
playbook.yml"],"ExtraVariables":["SSM=True"],"Check":["False"],"Verbose":["-v"]}' \
    --association-name "AnsibleAssociation" \
    --schedule-expression "cron(0 2 ? * SUN *)"
```

(B) S3 ソース

Linux & macOS

```
aws ssm create-association --name "AWS-ApplyAnsiblePlaybooks" \
    --targets Key=tag:TagKey,Values=TagValue \
    --parameters '{"SourceType":["S3"],"SourceInfo":["{\"path\":\"https://
s3.amazonaws.com/
path_to_Zip_file,_directory,_or_playbook_to_download\"}"],"InstallDependencies":
["True_or_False"],"PlaybookFile":["file_name.yml"],"ExtraVariables":["key/
value_pairs_separated_by_a_space"],"Check":["True_or_False"],"Verbose":["-v,-
vv,-vvv, or -vvvv"]}' \
    --association-name "name" \
    --schedule-expression "cron_or_rate_expression"
```

Windows

```
aws ssm create-association --name "AWS-ApplyAnsiblePlaybooks" ^
    --targets Key=tag:TagKey,Values=TagValue ^
    --parameters '{"SourceType":["S3"],"SourceInfo":["{\"path\":\"https://
s3.amazonaws.com/
path_to_Zip_file,_directory,_or_playbook_to_download\"}"],"InstallDependencies":
["True_or_False"],"PlaybookFile":["file_name.yml"],"ExtraVariables":["key/
value_pairs_separated_by_a_space"],"Check":["True_or_False"],"Verbose":["-v,-
vv,-vvv, or -vvvv"]}' ^
    --association-name "name" ^
    --schedule-expression "cron_or_rate_expression"
```

以下はその例です。

```
aws ssm create-association --name "AWS-ApplyAnsiblePlaybooks" \
    --targets "Key=tag:OS,Values=Linux" \
    --parameters '{"SourceType":["S3"],"SourceInfo":["{\"path\":\"https://
s3.amazonaws.com/amzn-s3-demo-bucket/playbook.yml\"}"],"InstallDependencies":
["True"],"PlaybookFile":["playbook.yml"],"ExtraVariables":["SSM=True"],"Check":
["False"],"Verbose":["-v"]}' \
    --association-name "AnsibleAssociation" \
    --schedule-expression "cron(0 2 ? * SUN *)"
```

> **Note**
>
> State Manager の関連付けは、すべての cron および rate 式をサポートしていません。関連付けの cron および rate 式の作成の詳細については、「リファレンス: Systems Manager の Cron 式および rate 式」を参照してください。

システムはノードで関連付けを作成し、状態を即時に適用しようとします。

3. 作成した関連付けの最新のステータスを表示するには、次のコマンドを実行します。

```
aws ssm describe-association --association-id "ID"
```

Chef recipe を実行する関連付けの作成

AWS-ApplyChefRecipes SSM ドキュメントを使用して、Chef recipe を実行する State Manager の関連付けを作成できます。State Manager は AWS Systems Manager のツールです。AWS-ApplyChefRecipes SSM ドキュメントを使用して Linux ベースのSystems Manager マネージドノードをターゲットにすることができます。このドキュメントには、Chef recipe の実行に関して次の利点があります。

- Chef の複数のリリース (Chef 11 から Chef 18) をサポートします。
- ターゲットノードに Chef クライアントソフトウェアを自動的にインストールします。
- オプションで、ターゲットノードの Systems Manager コンプライアンスチェックを実行し、コンプライアンスチェックの結果を Amazon Simple Storage Service (Amazon S3) バケットに保存します。
- ドキュメントの 1 回の実行で複数のクックブックと recipe を実行します。
- オプションで、recipe を why-run モードで実行して、どの recipe がターゲットノードに変更を加えるかを、変更せずに確認します。
- オプションで、カスタム JSON 属性を chef-client 実行に適用します。
- オプションで、指定した場所に保存されているソースファイルからカスタム JSON 属性を適用します。

Git、GitHub、HTTP、または Amazon S3 バケットを、AWS-ApplyChefRecipes ドキュメントで指定する Chef のクックブックと recipe のダウンロードソースとして使用できます。

> **Note**
>
> Chef recipe を実行する関連付けは、macOS ではサポートされていません。

入門

AWS-ApplyChefRecipes ドキュメントを作成する前に、Chef クックブックとクックブックリポジトリを準備します。使用する Chef クックブックがまだない場合は、AWS に用意されているテスト用の HelloWorld クックブックを使用して開始できます。デフォルトでは、AWS-ApplyChefRecipes ドキュメントは既にこのクックブックを指しています。クックブックは、次のディレクトリ構造と同様にセットアップする必要があります。以下の例では、jenkins および nginx は Chef ウェブサイトの Chef Supermarket で入手可能な Chef クックブックの例です。

AWS は、Chef Supermarket ウェブサイトのクックブックを正式にサポートすることはできませんが、その多くは AWS-ApplyChefRecipes ドキュメントで使用できます。コミュニティクックブックをテストするときに確認する基準の例を次に示します。

- クックブックは、ターゲットとする Systems Manager マネージドノードの Linux ベースのオペレーティングシステムをサポートしている必要があります。
- クックブックは、使用する Chef クライアントバージョン (Chef 11 から Chef 18) に対して有効である必要があります。
- クックブックは Chef Infra Client と互換性があるため、Chef サーバーは必要ありません。

Chef.io ウェブサイトにアクセスできることを確認し、Systems Manager ドキュメント (SSM ドキュメント) の実行時に実行リストに指定したクックブックをインストールできるようにします。ネストされた cookbooks フォルダはサポートされていますが、必須ではありません。クックブックはルートレベルに直接保存できます。

```
<Top-level directory, or the top level of the archive file (ZIP or tgz or tar.gz)>
    ### cookbooks (optional level)
        ### jenkins
        #   ### metadata.rb
        #   ### recipes
        ### nginx
            ### metadata.rb
            ### recipes
```

Important

Chef recipe を実行する State Manager の関連付けを作成する前に注意すべき点は、[Chef クライアントのバージョン] の値を None に設定していないと、ドキュメントを実行したときに、Chef クライアントソフトウェアが Systems Manager マネージドノードにインストールされることです。このオペレーションでは、Chef のインストールスクリプトを使用して、ユーザーに代わって Chef コンポーネントをインストールします。AWS-ApplyChefRecipes ドキュメントを実行する前に、Chef ソフトウェアの使用に適用されるライセンス条項など、適用される法的要件を企業が準拠していることを確認してください。詳細については、Chef のウェブサイトを参照してください。

Systems Manager は、コンプライアンスレポートを S3 バケットや Systems Manager コンソールに配信したり、Systems Manager API コマンドに応答してコンプライアンス結果を利用できるように

したりできます。Systems Manager コンプライアンスレポートを実行するには、Systems Manager マネージドノードにアタッチされたインスタンスプロファイルに、S3 バケットへ書き込むためのアクセス許可が必要です。インスタンスプロファイルには、Systems Manager `PutComplianceItem` API を使用するためのアクセス許可が必要です。Systems Manager のコンプライアンスの詳細については、「AWS Systems Manager のコンプライアンス」を参照してください。

ドキュメント実行のログ記録

State Manager の関連付けを使用してSystems Manager ドキュメント (SSM ドキュメント) を実行する場合、ドキュメント実行の出力を選択するように関連付けを設定し、その出力を Amazon S3 または Amazon CloudWatch Logs (CloudWatch Logs) に送信できます。関連付けの実行が終了したときのトラブルシューティングを容易にするために、コマンド出力を Amazon S3 バケットまたは CloudWatch Logs に書き込むように関連付けが設定されていることを確認します。詳細については、「Systems Manager の関連付けの使用」を参照してください。

recipe の実行時におけるターゲットへの JSON 属性の適用

Chef クライアントの JSON 属性を指定して、関連付けの実行中にターゲットノードに適用できます。関連付けを設定する際には、Raw JSON を指定することも、Amazon S3 に保存されている JSON ファイルへのパスを指定することもできます。

recipe 自体を変更せずに recipe の実行方法をカスタマイズする場合は、JSON 属性を使用します。次に例を示します。

- 少数の属性の上書き

  カスタム JSON を使用すると、軽微な違いに対応するために recipe の複数のバージョンを維持する必要がなくなります。
- 変数の値の指定

  カスタム JSON を使用して、実行ごとに変更される可能性のある値を指定します。例えば、Chef クックブックで支払いを受け付けるサードパーティアプリケーションを設定する場合、カスタム JSON を使用してエンドポイントの支払い URL を指定できます。

Raw JSON での属性の指定

Chef recipe のカスタム JSON 属性を指定するために使用できる形式の例を次に示します。

```
{"filepath":"/tmp/example.txt", "content":"Hello, World!"}
```

JSON ファイルへのパスの指定

Chef recipe のカスタム JSON 属性へのパスを指定するために使用できる形式の例を次に示します。

```
{"sourceType":"s3", "sourceInfo":"someS3URL1"}, {"sourceType":"s3",
 "sourceInfo":"someS3URL2"}
```

Git をクックブックのソースとして使用する

AWS-ApplyChefRecipes ドキュメントは、aws:downloadContent プラグインを使用して Chef クックブックをダウンロードします。Git からコンテンツをダウンロードするには、次の例で示すように、Git リポジトリに関する情報を JSON 形式で指定します。各 *example-resource-placeholder* を、ユーザー自身の情報に置き換えます。

```
{
   "repository":"GitCookbookRepository",
   "privateSSHKey":"{{ssm-secure:ssh-key-secure-string-parameter}}",
   "skipHostKeyChecking":"false",
   "getOptions":"branch:refs/head/main",
   "username":"{{ssm-secure:username-secure-string-parameter}}",
   "password":"{{ssm-secure:password-secure-string-parameter}}"
}
```

クックブックのソースとして GitHub を使用する

AWS-ApplyChefRecipes ドキュメントは、aws:downloadContent プラグインを使用してクックブックをダウンロードします。GitHub からコンテンツをダウンロードするには、次の例で示すように、GitHub リポジトリに関する情報を JSON 形式で指定します。各 *example-resource-placeholder* を、ユーザー自身の情報に置き換えます。

```
{
   "owner":"TestUser",
   "repository":"GitHubCookbookRepository",
   "path":"cookbooks/HelloWorld",
   "getOptions":"branch:refs/head/main",
   "tokenInfo":"{{ssm-secure:token-secure-string-parameter}}"
}
```

クックブックのソースとして HTTP を使用する

Chef クックブックは、単一の .zip や tar.gz ファイル、あるいはディレクトリ構造としてカスタム HTTP の場所に保存できます。HTTP からコンテンツをダウンロードするには、次の例のように、ファイルまたはディレクトリへのパスを JSON 形式で指定します。各 *example-resource-placeholder* を、ユーザー自身の情報に置き換えます。

```
{
   "url":"https://my.website.com/chef-cookbooks/HelloWorld.zip",
   "allowInsecureDownload":"false",
   "authMethod":"Basic",
   "username":"{{ssm-secure:username-secure-string-parameter}}",
   "password":"{{ssm-secure:password-secure-string-parameter}}"
}
```

Amazon S3 をクックブックソースとして使用する

Chef クックブックは、単一の .zip や tar.gz ファイル、あるいはディレクトリ構造として Amazon S3 に保存およびダウンロードすることもできます。Amazon S3 からコンテンツをダウンロードするには、次の例のように、ファイルへのパスを JSON 形式で指定します。各 *example-resource-placeholder* を、ユーザー自身の情報に置き換えます。

例 1: 特定のクックブックをダウンロードする

```
{
   "path":"https://s3.amazonaws.com/chef-cookbooks/HelloWorld.zip"
}
```

例 2: ディレクトリの内容をダウンロードする

```
{
   "path":"https://s3.amazonaws.com/chef-cookbooks-test/HelloWorld"
}
```

> **Important**
>
> Amazon S3 を指定した場合、マネージドノードの AWS Identity and Access Management (IAM) インスタンスプロファイルを AmazonS3ReadOnlyAccess ポリシーで設定する必要があります。詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」を参照してください。

Chef recipe を実行する関連付けを作成する (コンソール)

以下の手順では、Systems Manager コンソールを使用し、AWS-ApplyChefRecipes ドキュメントを使って Chef クックブックを実行する State Manager の関連付けを作成する方法について説明します。

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[State Manager] を選択します。
3. [State Manager] を選択してから、[関連付けの作成] を選択します。
4. [Name (名前)] に、関連付けの目的を思い出すのに役立つ名前を入力します。
5. [Document (ドキュメント)] リストで、[**AWS-ApplyChefRecipes**] を選択します。
6. [パラメータ] の [ソースタイプ] で、Git、GitHub、HTTP、または S3 のいずれかを選択します。
7. [ソース情報] で、ステップ 6 で選択した [ソースタイプ] に適切な形式を使用してクックブックのソース情報を入力します。詳細については、以下の各トピックを参照してください。
   - the section called “Git をクックブックのソースとして使用する”
   - the section called “クックブックのソースとして GitHub を使用する”
   - the section called “クックブックのソースとして HTTP を使用する”
   - the section called “Amazon S3 をクックブックソースとして使用する”
8. [Run list] (リストの実行) で、実行する recipe を次の形式で一覧表示します。各 recipe はカンマで区切ります。コンマの後にスペースを入れないでください。各 *example-resource-placeholder* を、ユーザー自身の情報に置き換えます。

   ```
   recipe[cookbook-name1::recipe-name],recipe[cookbook-name2::recipe-name]
   ```
9. (オプション) Chef クライアントからターゲットノードに渡すカスタム JSON 属性を指定します。
   a. [JSON 属性のコンテンツ] で、Chef クライアントからターゲットノードに渡す属性を追加します。
   b. [JSON 属性のソース] で、Chef クライアントからターゲットノードに渡す属性へのパスを追加します。

   詳細については、「the section called “recipe の実行時におけるターゲットへの JSON 属性の適用”」を参照してください。

10. [Chef クライアントバージョン] には、Chef のバージョンを指定します。有効な値は、11 ~ 18、または None です。11 から 18 まで (両端の値を含む) の数値を指定すると、Systems Manager はターゲットノードに正しい Chef クライアントバージョンをインストールします。None を指定すると、Systems Manager はドキュメントの recipe を実行する前にターゲットノードに Chef クライアントをインストールしません。
11. (オプション) [Chef クライアント引数] には、使用している Chef のバージョンでサポートされている追加の引数を指定します。サポートされている引数の詳細については、Chef クライアントを実行しているノードで `chef-client -h` を実行してください。
12. (オプション) recipe を実行する場合に、ターゲットノードを実際に変更せずに、ターゲットノードに対して行われる変更を表示するには、[Why-run] をオンにします。
13. [Compliance severity (コンプライアンスの重要度)] で、レポートする Systems Manager コンプライアンスの結果の重要度を選択します。コンプライアンスレポートには、ここで指定した重要度と共に関連付けの状態が準拠しているか準拠していないかが表示されます。コンプライアンスレポートは、[Compliance report bucket (コンプライアンスレポートバケット)] パラメータの値として指定する S3 バケットに保存されます (ステップ 14)。コンプライアンスの詳細については、このガイドの「コンプライアンスの詳細について」を参照してください。

    コンプライアンススキャンでは、Chef recipe で指定された設定とノードリソース間のずれを測定します。有効な値は `Critical`、`High`、`Medium`、`Low`、`Informational`、`Unspecified`、`None` です。コンプライアンスレポートをスキップするには、`None` を選択します。
14. [コンプライアンスタイプ] で、結果をレポートするコンプライアンスタイプを指定します。有効な値は、State Manager の関連付けについては `Association`、または `Custom:`*`custom-type`* です。デフォルト値は `Custom:Chef` です。
15. [コンプライアンスレポートバケット] に、リソース設定やコンプライアンスの結果など、このドキュメントで実行されるすべての Chef 実行に関する情報を保存する S3 バケットの名前を入力します。
16. [Rate control] (レート制御) で、マネージドノードのフリート全体に State Manager の関連付けを実行するためのオプションを設定します。レート制御の使用については、「State Manager 関連付けのターゲットとレート制御について」を参照してください。

    [Concurrency (同時実行)] で、次のいずれかのオプションを選択します。

    - [targets (ターゲット)] を選択して、関連付けを同時に実行できるターゲットの絶対数を入力します。

- [percentage (パーセント値)] を選択して、関連付けを同時に実行できるターゲットセットのパーセント値を入力します。

[Error threshold (エラーのしきい値)] で、オプションを選択します。

- State Manager が追加ターゲットでの関連付けの実行を停止する前に、[errors (エラー)] を選択して許可されるエラーの絶対数を入力します。
- State Manager が追加ターゲットでの関連付けの実行を停止する前に、[percentage (パーセンテージ)] を選択して許可されるエラーの割合を入力します。

17. (オプション) [出力オプション] で、コマンド出力をファイルに保存するには、[S3 への出力の書き込みを有効にします] ボックスをオンにします。ボックスにバケット名とプレフィックス (フォルダ) 名を入力してください。

> **Note**
>
> S3 バケットにデータを書き込む機能を許可する S3 アクセス許可は、このタスクを実行する IAM ユーザーのものではなく、マネージドノードに割り当てられたインスタンスプロファイルのものです。詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」または「ハイブリッド環境に IAM サービスロールを作成する」を参照してください。さらに、指定された S3 バケットが別の AWS アカウント にある場合は、マネージドノードに関連付けられたインスタンスプロファイルまたは IAM サービスロールに、そのバケットへの書き込みに必要なアクセス許可があることを確認してください。

18. [関連付けの作成] を選択します。

Chef recipe を実行する関連付けの作成 (CLI)

以下の手順では、AWS Command Line Interface (AWS CLI) を使用して、`AWS-ApplyChefRecipes` ドキュメントを使用し、Chef クックブックを実行する State Manager の関連付けを作成する方法について説明します。

1. まだ AWS Command Line Interface (AWS CLI) をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」を参照してください。

2. 次のコマンドのいずれかを実行して、指定されたタグを持つターゲットノードで Chef クックブックを実行する関連付けを作成します。クックブックのソースタイプとオペレーティングシステムに適したコマンドを使用します。各 *example-resource-placeholder* を、ユーザー自身の情報に置き換えます。

   a. Git ソース

      Linux & macOS

```
aws ssm create-association --name "AWS-ApplyChefRecipes" \
    --targets Key=tag:TagKey,Values=TagValue \
    --parameters '{"SourceType":["Git"],"SourceInfo":["{\"repository\":
\"repository-name\", \"getOptions\": \"branch:branch-name\", \"username
\": \"{{ ssm-secure:username-secure-string-parameter }}\", \"password\":
 \"{{ ssm-secure:password-secure-string-parameter }}\"}"], "RunList":
["{\"recipe[cookbook-name-1::recipe-name]\", \"recipe[cookbook-
name-2::recipe-name]\"}"], "JsonAttributesContent": ["{custom-json-
content}"], "JsonAttributesSources": "{\"sourceType\":\"s3\", \"sourceInfo
\":\"s3-bucket-endpoint-1\"}, {\"sourceType\":\"s3\", \"sourceInfo\":
\"s3-bucket-endpoint-2\"}", "ChefClientVersion": ["version-number"],
 "ChefClientArguments":["{chef-client-arguments}"], "WhyRun": boolean,
 "ComplianceSeverity": ["severity-value"], "ComplianceType":
 ["Custom:Chef"], "ComplianceReportBucket": ["s3-bucket-name"]}' \
    --association-name "name" \
    --schedule-expression "cron-or-rate-expression"
```

      Windows

```
aws ssm create-association --name "AWS-ApplyChefRecipes" ^
    --targets Key=tag:TagKey,Values=TagValue ^
    --parameters '{"SourceType":["Git"],"SourceInfo":["{\"repository\":
\"repository-name\", \"getOptions\": \"branch:branch-name\", \"username
\": \"{{ ssm-secure:username-secure-string-parameter }}\", \"password\":
 \"{{ ssm-secure:password-secure-string-parameter }}\"}"], "RunList":
["{\"recipe[cookbook-name-1::recipe-name]\", \"recipe[cookbook-
name-2::recipe-name]\"}"], "JsonAttributesContent": ["{custom-json}"],
 "JsonAttributesSources": "{\"sourceType\":\"s3\", \"sourceInfo\":
\"s3-bucket-endpoint-1\"}, {\"sourceType\":\"s3\", \"sourceInfo\":
\"s3-bucket-endpoint-2\"}", "ChefClientVersion": ["version-number"],
 "ChefClientArguments":["{chef-client-arguments}"], "WhyRun": boolean,
 "ComplianceSeverity": ["severity-value"], "ComplianceType":
 ["Custom:Chef"], "ComplianceReportBucket": ["s3-bucket-name"]}' ^
```

```
    --association-name "name" ^
    --schedule-expression "cron-or-rate-expression"
```

b. GitHub ソース

Linux & macOS

```
aws ssm create-association --name "AWS-ApplyChefRecipes" \
    --targets Key=tag:TagKey,Values=TagValue \
    --parameters '{"SourceType":["GitHub"],"SourceInfo":["{\"owner\":
\"owner-name\", \"repository\": \"name\", \"path\": \"path-to-directory-
or-cookbook-to-download\", \"getOptions\": \"branch:branch-name\"}"],
 "RunList":["{\"recipe[cookbook-name-1::recipe-name]\", \"recipe[cookbook-
name-2::recipe-name]\"}"], "JsonAttributesContent": ["{custom-json}"],
 "ChefClientVersion": ["version-number"], "ChefClientArguments":["{chef-
client-arguments}"], "WhyRun": boolean, "ComplianceSeverity": ["severity-
value"], "ComplianceType": ["Custom:Chef"], "ComplianceReportBucket": ["s3-
bucket-name"]}' \
    --association-name "name" \
    --schedule-expression "cron-or-rate-expression"
```

Windows

```
aws ssm create-association --name "AWS-ApplyChefRecipes" ^
    --targets Key=tag:TagKey,Values=TagValue \
    --parameters '{"SourceType":["GitHub"],"SourceInfo":["{\"owner\":
\"owner-name\", \"repository\": \"name\", \"path\": \"path-to-directory-
or-cookbook-to-download\", \"getOptions\": \"branch:branch-name\"}"],
 "RunList":["{\"recipe[cookbook-name-1::recipe-name]\", \"recipe[cookbook-
name-2::recipe-name]\"}"], "JsonAttributesContent": ["{custom-json}"],
 "ChefClientVersion": ["version-number"], "ChefClientArguments":["{chef-
client-arguments}"], "WhyRun": boolean, "ComplianceSeverity": ["severity-
value"], "ComplianceType": ["Custom:Chef"], "ComplianceReportBucket": ["s3-
bucket-name"]}' ^
    --association-name "name" ^
    --schedule-expression "cron-or-rate-expression"
```

以下はその例です。

Linux & macOS

```
aws ssm create-association --name "AWS-ApplyChefRecipes" \
    --targets Key=tag:OS,Values=Linux \
    --parameters '{"SourceType":["GitHub"],"SourceInfo":["{\"owner
\":\"ChefRecipeTest\", \"repository\": \"ChefCookbooks\", \"path
\": \"cookbooks/HelloWorld\", \"getOptions\": \"branch:master
\"}"], "RunList":["{\"recipe[HelloWorld::HelloWorldRecipe]\",
 \"recipe[HelloWorld::InstallApp]\"}"], "JsonAttributesContent":
 ["{\"state\": \"visible\",\"colors\": {\"foreground\": \"light-blue
\",\"background\": \"dark-gray\"}}"], "ChefClientVersion": ["14"],
 "ChefClientArguments":["{--fips}"], "WhyRun": false, "ComplianceSeverity":
 ["Medium"], "ComplianceType": ["Custom:Chef"], "ComplianceReportBucket":
 ["ChefComplianceResultsBucket"]}' \
    --association-name "MyChefAssociation" \
    --schedule-expression "cron(0 2 ? * SUN *)"
```

Windows

```
aws ssm create-association --name "AWS-ApplyChefRecipes" ^
    --targets Key=tag:OS,Values=Linux ^
    --parameters '{"SourceType":["GitHub"],"SourceInfo":["{\"owner
\":\"ChefRecipeTest\", \"repository\": \"ChefCookbooks\", \"path
\": \"cookbooks/HelloWorld\", \"getOptions\": \"branch:master
\"}"], "RunList":["{\"recipe[HelloWorld::HelloWorldRecipe]\",
 \"recipe[HelloWorld::InstallApp]\"}"], "JsonAttributesContent":
 ["{\"state\": \"visible\",\"colors\": {\"foreground\": \"light-blue
\",\"background\": \"dark-gray\"}}"], "ChefClientVersion": ["14"],
 "ChefClientArguments":["{--fips}"], "WhyRun": false, "ComplianceSeverity":
 ["Medium"], "ComplianceType": ["Custom:Chef"], "ComplianceReportBucket":
 ["ChefComplianceResultsBucket"]}' ^
    --association-name "MyChefAssociation" ^
    --schedule-expression "cron(0 2 ? * SUN *)"
```

c. HTTP ソース

Linux & macOS

```
aws ssm create-association --name "AWS-ApplyChefRecipes" \
    --targets Key=tag:TagKey,Values=TagValue \
    --parameters '{"SourceType":["HTTP"],"SourceInfo":["{\"url\":\"url-
to-zip-file|directory|cookbook\", \"authMethod\": \"auth-method\",
```

```
 \"username\": \"{{ ssm-secure:username-secure-string-parameter }}\",
 \"password\": \"{{ ssm-secure:password-secure-string-parameter }}\"}"],
 "RunList":["{\"recipe[cookbook-name-1::recipe-name]\", \"recipe[cookbook-
name-2::recipe-name]\"}"], "JsonAttributesContent": ["{custom-json-
content}"], "JsonAttributesSources": "{\"sourceType\":\"s3\", \"sourceInfo
\":\"s3-bucket-endpoint-1\"}, {\"sourceType\":\"s3\", \"sourceInfo\":
\"s3-bucket-endpoint-2\"}", "ChefClientVersion": ["version-number"],
 "ChefClientArguments":["{chef-client-arguments}"], "WhyRun": boolean,
 "ComplianceSeverity": ["severity-value"], "ComplianceType":
 ["Custom:Chef"], "ComplianceReportBucket": ["s3-bucket-name"]}' \
    --association-name "name" \
    --schedule-expression "cron-or-rate-expression"
```

Windows

```
aws ssm create-association --name "AWS-ApplyChefRecipes" ^
    --targets Key=tag:TagKey,Values=TagValue ^
    --parameters '{"SourceType":["HTTP"],"SourceInfo":["{\"url\":\"url-
to-zip-file|directory|cookbook\", \"authMethod\": \"auth-method\",
 \"username\": \"{{ ssm-secure:username-secure-string-parameter }}\",
 \"password\": \"{{ ssm-secure:password-secure-string-parameter }}\"}"],
 "RunList":["{\"recipe[cookbook-name-1::recipe-name]\", \"recipe[cookbook-
name-2::recipe-name]\"}"], "JsonAttributesContent": ["{custom-json-
content}"], "JsonAttributesSources": "{\"sourceType\":\"s3\", \"sourceInfo
\":\"s3-bucket-endpoint-1\"}, {\"sourceType\":\"s3\", \"sourceInfo\":
\"s3-bucket-endpoint-2\"}", "ChefClientVersion": ["version-number"],
 "ChefClientArguments":["{chef-client-arguments}"], "WhyRun": boolean,
 "ComplianceSeverity": ["severity-value"], "ComplianceType":
 ["Custom:Chef"], "ComplianceReportBucket": ["s3-bucket-name"]}' \
    --association-name "name" ^
    --schedule-expression "cron-or-rate-expression"
```

d. Amazon S3 ソース

Linux & macOS

```
aws ssm create-association --name "AWS-ApplyChefRecipes" \
    --targets Key=tag:TagKey,Values=TagValue \
    --parameters '{"SourceType":["S3"],"SourceInfo":["{\"path\":\"https://
s3.amazonaws.com/path_to_Zip_file,_directory,_or_cookbook_to_download\"}"],
 "RunList":["{\"recipe[cookbook_name1::recipe_name]\",
 \"recipe[cookbook_name2::recipe_name]\"}"], "JsonAttributesContent":
 ["{Custom_JSON}"], "ChefClientVersion": ["version_number"],
```

```
 "ChefClientArguments":["{chef_client_arguments}"], "WhyRun": true_or_false,
 "ComplianceSeverity": ["severity_value"], "ComplianceType":
 ["Custom:Chef"], "ComplianceReportBucket": ["amzn-s3-demo-bucket"]}' \
    --association-name "name" \
    --schedule-expression "cron_or_rate_expression"
```

Windows

```
aws ssm create-association --name "AWS-ApplyChefRecipes" ^
    --targets Key=tag:TagKey,Values=TagValue ^
    --parameters '{"SourceType":["S3"],"SourceInfo":["{\"path\":\"https://
s3.amazonaws.com/path_to_Zip_file,_directory,_or_cookbook_to_download\"}"],
 "RunList":["{\"recipe[cookbook_name1::recipe_name]\",
 \"recipe[cookbook_name2::recipe_name]\"}"], "JsonAttributesContent":
 ["{Custom_JSON}"], "ChefClientVersion": ["version_number"],
 "ChefClientArguments":["{chef_client_arguments}"], "WhyRun": true_or_false,
 "ComplianceSeverity": ["severity_value"], "ComplianceType":
 ["Custom:Chef"], "ComplianceReportBucket": ["amzn-s3-demo-bucket"]}' ^
    --association-name "name" ^
    --schedule-expression "cron_or_rate_expression"
```

以下はその例です。

Linux & macOS

```
aws ssm create-association --name "AWS-ApplyChefRecipes" \
    --targets "Key=tag:OS,Values= Linux" \
    --parameters '{"SourceType":["S3"],"SourceInfo":["{\"path
\":\"https://s3.amazonaws.com/amzn-s3-demo-bucket/HelloWorld
\"}"], "RunList":["{\"recipe[HelloWorld::HelloWorldRecipe]\",
 \"recipe[HelloWorld::InstallApp]\"}"], "JsonAttributesContent":
 ["{\"state\": \"visible\",\"colors\": {\"foreground\": \"light-blue
\",\"background\": \"dark-gray\"}}"], "ChefClientVersion": ["14"],
 "ChefClientArguments":["{--fips}"], "WhyRun": false, "ComplianceSeverity":
 ["Medium"], "ComplianceType": ["Custom:Chef"], "ComplianceReportBucket":
 ["ChefComplianceResultsBucket"]}' \
    --association-name "name" \
    --schedule-expression "cron(0 2 ? * SUN *)"
```

Windows

```
aws ssm create-association --name "AWS-ApplyChefRecipes" ^
    --targets "Key=tag:OS,Values= Linux" ^
    --parameters '{"SourceType":["S3"],"SourceInfo":["{\"path
\":\"https://s3.amazonaws.com/amzn-s3-demo-bucket/HelloWorld
\"}"], "RunList":["{\"recipe[HelloWorld::HelloWorldRecipe]\",
 \"recipe[HelloWorld::InstallApp]\"}"], "JsonAttributesContent":
 ["{\"state\": \"visible\",\"colors\": {\"foreground\": \"light-blue
\",\"background\": \"dark-gray\"}}"], "ChefClientVersion": ["14"],
 "ChefClientArguments":["{--fips}"], "WhyRun": false, "ComplianceSeverity":
 ["Medium"], "ComplianceType": ["Custom:Chef"], "ComplianceReportBucket":
 ["ChefComplianceResultsBucket"]}' ^
    --association-name "name" ^
    --schedule-expression "cron(0 2 ? * SUN *)"
```

システムは関連付けを作成し、指定した cron または rate 式によって妨げられない限り、システムはターゲットノードで関連付けを実行します。

> **Note**
>
> State Manager の関連付けは、すべての cron および rate 式をサポートしていません。関連付けの cron および rate 式の作成の詳細については、「リファレンス: Systems Manager の Cron 式および rate 式」を参照してください。

3. 作成した関連付けのステータスを表示するには、次のコマンドを実行します。

```
aws ssm describe-association --association-id "ID"
```

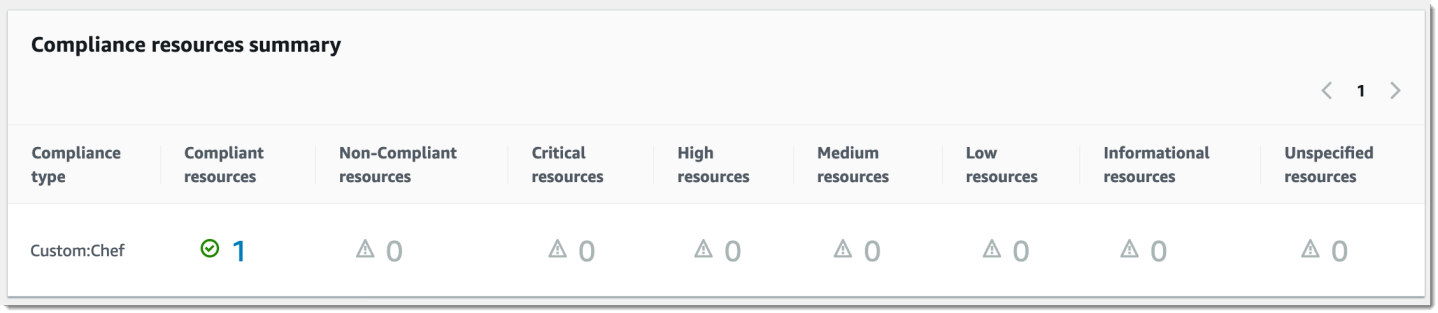
Chef リソースコンプライアンスの詳細の表示

Systems Manager は、AWS-ApplyChefRecipes ドキュメントの実行時に指定した Amazon S3 の [コンプライアンスレポートバケット] 値で、Chef で管理されているリソースに関するコンプライアンス情報をキャプチャします。S3 バケット内の Chef リソース障害に関する情報を検索するには、時間がかかる場合があります。代わりに、この情報を [Systems Manager Compliance] ページに表示できます。

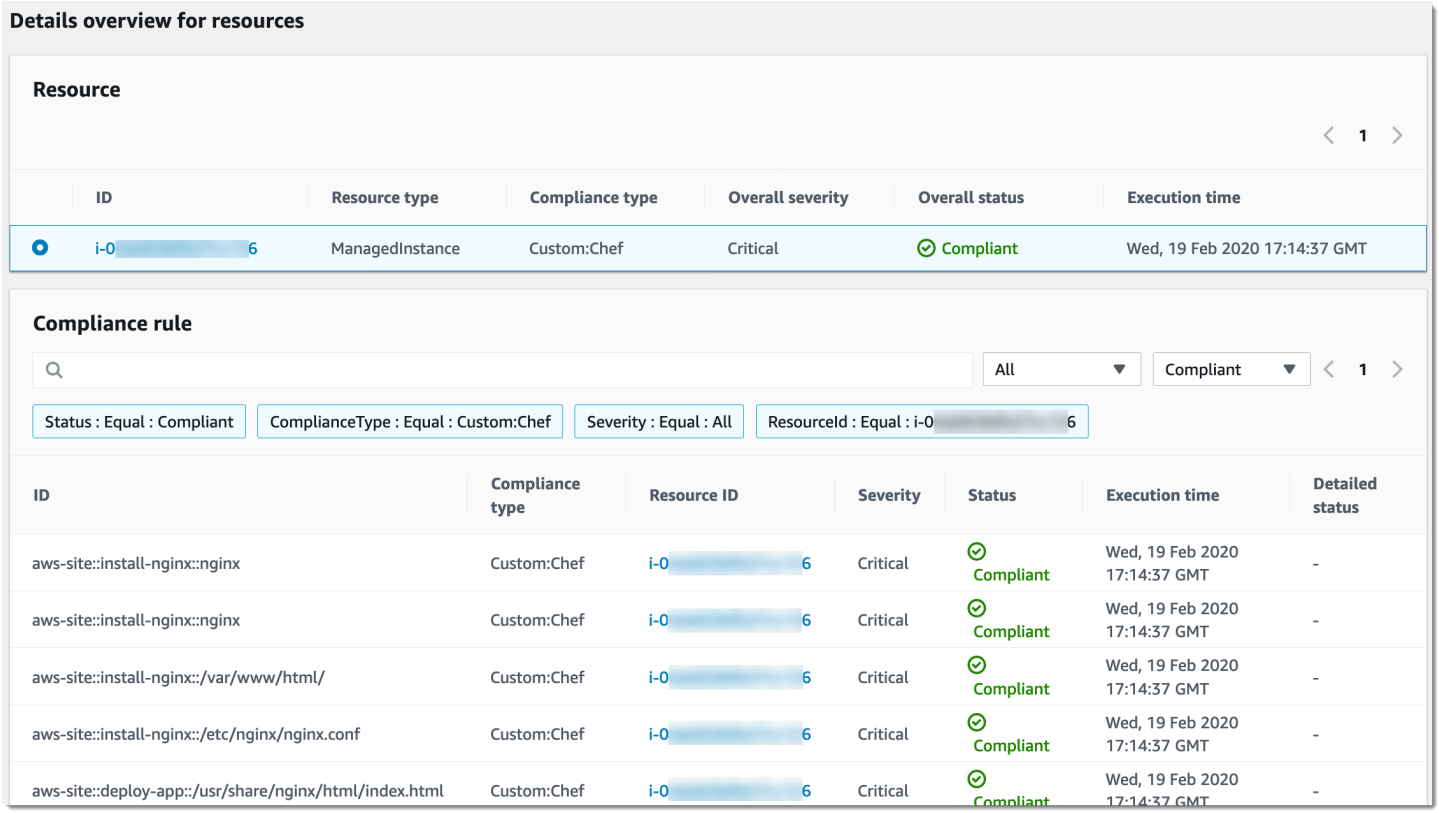
Systems Manager コンプライアンススキャンを使用すると、最新の Chef 実行で作成またはチェックされたマネージドノード上のリソースに関する情報を収集できます。リソースには、ファイル、ディレクトリ、systemd サービス、yum パッケージ、テンプレート化されたファイル、gem パッケージ、依存クックブックなどが含まれます。

[コンプライアンスリソースの概要] セクションには、失敗したリソース数が表示されます。次の例では、[ComplianceType] は [Custom:Chef] であり、1 つのリソースは準拠していません。

> **Note**
>
> Custom:Chef は、AWS-ApplyChefRecipes ドキュメントのデフォルトの ComplianceType 値です。この値はカスタマイズすることができます。



[Details overview for resources] (リソースの詳細の概要) セクションには、準拠していない AWS リソースに関する情報が表示されます。このセクションには、コンプライアンスが実行された Chef リソースタイプ、問題の重要度、コンプライアンスのステータス、および詳細情報へのリンク (該当する場合) も含まれます。



[出力の表示] には、詳細ステータスの最後の 4,000 文字が表示されます。Systems Manager は、最初の要素としてまず例外を表示した後、詳細メッセージを検索して、4,000 文字のクォータに達するまで表示します。このプロセスでは、例外がスローされる前に出力されたログメッセージが表示されます。表示されるメッセージは、トラブルシューティングに最もよく関連しています。

コンプライアンス情報の表示方法については、「AWS Systems Manager のコンプライアンス」を参照してください。

> **Important**
>
> State Manager の関連付けが失敗すると、コンプライアンスデータはレポートされません。例えば、Systems Manager が、ノードにアクセス許可が付与されていない S3 バケットから Chef クックブックをダウンロードしようとすると、関連付けは失敗し、Systems Manager でコンプライアンスデータはレポートされません。

チュートリアル: AWS CLI で SSM Agent を自動的に更新する

以下の手順では、AWS Command Line Interface を使用して State Manager の関連付けを作成するプロセスを説明します。関連付けにより、ユーザーが指定したスケジュールに従って SSM Agent エー

ジェントを自動的に更新できます。SSM Agent の詳細については、「「SSM Agent」 の使用」を参照してください。コンソールを使用して SSM Agent の更新スケジュールをカスタマイズするには、「SSM Agent の自動更新」を参照してください。

SSM Agent の更新に関する通知を受け取るには、GitHub の「SSM Agent リリースノート」ページをサブスクライブします。

[開始する前に]

次の手順を完了する前に、Systems Manager 用に設定されている実行中の Amazon Elastic Compute Cloud (Amazon EC2) インスタンス (Linux、macOS または Windows Server) が少なくとも 1 つあることを確認します。詳細については、「AWS Systems Manager のマネージドノードのセットアップ」を参照してください。

AWS CLI または AWS Tools for Windows PowerShell を使用して関連付けを作成する場合は、次の例に示すように `--Targets` パラメータを使用してインスタンスをターゲットにします。`--InstanceID` パラメータは使用しないでください。`--InstanceID` パラメータはレガシーパラメータです。

SSM Agent を自動的に更新するための関連付けを作成するには

1. まだ AWS Command Line Interface (AWS CLI) をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」を参照してください。

2. Amazon Elastic Compute Cloud (Amazon EC2) タグを使用してインスタンスをターゲットにして関連付けを作成するには、以下のコマンドを実行します。各##############をユーザー自身の情報に置き換えます。`Schedule` パラメータは、毎週日曜日の午前 2:00 に関連付けを実行するようスケジュールを設定します。(UTC)

   State Manager の関連付けは、すべての cron および rate 式をサポートしていません。関連付けの cron および rate 式の作成の詳細については、「リファレンス: Systems Manager の Cron 式および rate 式」を参照してください。

   Linux & macOS

```
aws ssm create-association \
--targets Key=tag:tag_key,Values=tag_value \
--name AWS-UpdateSSMAgent \
```

```
--schedule-expression "cron(0 2 ? * SUN *)"
```

Windows

```
aws ssm create-association ^
--targets Key=tag:tag_key,Values=tag_value ^
--name AWS-UpdateSSMAgent ^
--schedule-expression "cron(0 2 ? * SUN *)"
```

インスタンス ID をカンマ区切りのリストで指定すると、複数のインスタンスを対象にすることができます。

Linux & macOS

```
aws ssm create-association \
--targets Key=instanceids,Values=instance_ID,instance_ID,instance_ID \
--name AWS-UpdateSSMAgent \
--schedule-expression "cron(0 2 ? * SUN *)"
```

Windows

```
aws ssm create-association ^
--targets Key=instanceids,Values=instance_ID,instance_ID,instance_ID ^
--name AWS-UpdateSSMAgent ^
--schedule-expression "cron(0 2 ? * SUN *)"
```

更新したい SSM Agent のバージョンを指定できます。

Linux & macOS

```
aws ssm create-association \
--targets Key=instanceids,Values=instance_ID,instance_ID,instance_ID \
--name AWS-UpdateSSMAgent \
--schedule-expression "cron(0 2 ? * SUN *)" \
--parameters version=ssm_agent_version_number
```

Windows

```
aws ssm create-association ^
```

```
--targets Key=instanceids,Values=instance_ID,instance_ID,instance_ID ^
--name AWS-UpdateSSMAgent ^
--schedule-expression "cron(0 2 ? * SUN *)" ^
--parameters version=ssm_agent_version_number
```

システムが以下のような情報を返します。

```
{
    "AssociationDescription": {
        "ScheduleExpression": "cron(0 2 ? * SUN *)",
        "Name": "AWS-UpdateSSMAgent",
        "Overview": {
            "Status": "Pending",
            "DetailedStatus": "Creating"
        },
        "AssociationId": "123.............",
        "DocumentVersion": "$DEFAULT",
        "LastUpdateAssociationDate": 1504034257.98,
        "Date": 1504034257.98,
        "AssociationVersion": "1",
        "Targets": [
            {
                "Values": [
                    "TagValue"
                ],
                "Key": "tag:TagKey"
            }
        ]
    }
}
```

システムは、インスタンス上で関連付けを作成し、作成後に状態を適用することを試みます。関連付けのステータスは Pending と表示されます。

3. 作成した関連付けの最新のステータスを表示するには、次のコマンドを実行します。

```
aws ssm list-associations
```

インスタンスで最新バージョンの SSM Agent が実行されていない場合、ステータスは Failed になります。新しいバージョンの SSM Agent が公開されると、関連付けによって自動的に新しいエージェントがインストールされ、ステータスが Success と表示されます。

チュートリアル: Windows Server の EC2 インスタンスで PV ドライバーを自動的に更新する

Amazon Windows Amazon Machine Images (AMIs) には、仮想ハードウェアにアクセスできるようにするためのドライバー一式が含まれています。このようなドライバーは、インスタンスストアと Amazon Elastic Block Store (Amazon EBS) ボリュームをデバイスにマッピングするために、Amazon Elastic Compute Cloud (Amazon EC2) によって使用されます。Windows Server の EC2 インスタンスの安定性とパフォーマンスを向上させるため、最新のドライバーをインストールすることをお勧めします。PV ドライバーの詳細については、「AWS PV ドライバー」を参照してください。

以下のチュートリアルでは、ドライバーが利用可能になると自動的に新しい AWS PV ドライバーをダウンロードしてインストールするよう State Manager の関連付けを設定する方法を説明します。State Manager は AWS Systems Manager のツールです。

[開始する前に]

次の手順を実行する前に、Systems Manager に設定されている Windows Server の実行中の Amazon EC2 インスタンスが少なくとも 1 つあることを確認します。詳細については、「AWS Systems Manager のマネージドノードのセットアップ」を参照してください。

PV ドライバーを自動的に更新する State Manager の関連付けを作成するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[State Manager] を選択します。
3. [アソシエーションを作成する] を選択してください。
4. [名前] フィールドに、関連付けを説明する名前を入力します。
5. [ドキュメント] リストで、`AWS-ConfigureAWSPackage`[] を選択します。
6. [パラメータ] エリアで、次を実行します。
   - [Action] で、[Install] を選択します。
   - [インストールタイプ] で、[アンインストールと再インストール] を選択してください。

> **Note**
>
> このパッケージは、インプレースアップグレードに対応していません。アンインストールしてから再インストールする必要があります。

- [名前] に**AWSPVDriver**と入力してください。

[バージョン] と [追加の引数] には何も入力する必要はありません。

7. [ターゲット] セクションで、タグの指定、インスタンスやエッジデバイスの手動選択、リソースグループの指定により、このオペレーションを実行するマネージドノードを選択します。

> **Tip**
>
> 表示されるはずのマネージドノードが表示されない場合は、トラブルシューティングのヒントについて「マネージドノードの可用性のトラブルシューティング」を参照してください。

> **Note**
>
> タグを使用してインスタンスを対象にし、Linux インスタンスにマッピングされるタグを指定する場合、関連付けは Windows インスタンスでは成功しますが、Linux インスタンスでは失敗します。関連付けの全体的なステータスは Failed と表示されます。

8. [スケジュールの指定] エリアで、設定したスケジュールに従って関連付けを実行するか、1 回だけ実行するかを選択します。更新された PV ドライバーは年間数回リリースされるため、必要に応じて月に 1 回実行するよう関連付けをスケジュールできます。
9. [詳細オプション] エリアの [コンプライアンスの重要度] で、関連付けの重要度レベルを選択します。コンプライアンスレポートには、ここで指定した重要度と共に関連付けの状態が準拠しているか準拠していないかが表示されます。詳細については、「State Manager 関連付けのコンプライアンスについて」を参照してください。
10. [レート制御] の場合:

- [同時実行数] の場合、コマンドを同時に実行するマネージドノードの数または割合を指定します。

> **Note**
>
> マネージドノードに適用されるタグを指定するか、AWS リソースグループを指定してターゲットを選択し、ターゲットとなるマネージドノードの数が不明な場合は、割合を指定してドキュメントを同時に実行できるターゲットの数を制限します。

- [エラーのしきい値] で、ノードの数または割合のいずれかで失敗した後、他のマネージドノードでのコマンドの実行をいつ停止するか指定します。例えば、3 つのエラーを指定した場合、4 番目のエラーが受信されると、システムマネージャー はコマンドの送信を停止します。コマンドを処理しているマネージドノードもエラーを送信する可能性があります。

11. (オプション) [出力オプション] で、コマンド出力をファイルに保存するには、[S3 への出力の書き込みを有効にします] ボックスをオンにします。ボックスにバケット名とプレフィックス (フォルダ) 名を入力してください。

> **Note**
>
> S3 バケットにデータを書き込む機能を許可する S3 アクセス許可は、このタスクを実行する IAM ユーザーのものではなく、マネージドノードに割り当てられたインスタンスプロファイルのものです。詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」または「ハイブリッド環境に IAM サービスロールを作成する」を参照してください。さらに、指定された S3 バケットが別の AWS アカウント にある場合は、マネージドノードに関連付けられたインスタンスプロファイルまたは IAM サービスロールに、そのバケットへの書き込みに必要なアクセス許可があることを確認してください。

12. (オプション) [CloudWatch アラーム] セクションの [アラーム名] で、モニタリングのための関連付けに適用する CloudWatch アラームを選択します。

> **Note**
>
> このステップに関する以下の情報に注意してください。
>
> - アラームリストには最大 100 個のアラームが表示されます。リストにアラームが表示されない場合は、AWS Command Line Interface を使用して関連付けを作成してください。詳細については、「関連付けの作成 (コマンドライン)」を参照してください。
> - CloudWatch アラームをコマンドにアタッチするには、関連付けを作成する IAM プリンシパルに `iam:createServiceLinkedRole` アクションの権限が必要で

す。CloudWatch アラームの詳細については、「Amazon CloudWatch でのアラームの使用」を参照してください。

- アラームがアクティブ化されると、保留中のコマンド呼び出しまたはオートメーションは実行されません。

13. [関連付けを作成する] を選択してから、[閉じる] を選択してください。システムはインスタンスで関連付けを作成し、状態を即時に適用します。

    Windows Server 用の 1 つ以上の Amazon EC2 インスタンスで関連付けを作成した場合、ステータスは [Success (成功)] に変わります。インスタンスが Systems Manager 用に設定されていない場合、または誤って Linux インスタンスを対象にした場合、ステータスは [Failed] と表示されます。

    ステータスが [Failed (失敗)] である場合、関連付け ID を選択し、[Resources (リソース)] タブを選択して、Windows Server の EC2 インスタンス上で関連付けが正常に作成されたことを確認します。Windows Server の EC2 インスタンスのステータスが [Failed] と表示されている場合は、インスタンスで SSM Agent が実行されていることを確認し、インスタンスが Systems Manager の AWS Identity and Access Management (IAM) ロールで設定されていることを確認します。詳細については、「組織用の Systems Manager 統合コンソールのセットアップ」を参照してください。

AWS Systems Manager 変更管理ツール

AWS Systems Manager は、AWS リソースを変更するための次のツールを提供します。

トピック

- AWS Systems Manager Automation
- AWS Systems Manager Change Calendar
- AWS Systems Manager Change Manager
- AWS Systems Manager ドキュメント
- AWS Systems Manager Maintenance Windows
- AWS Systems Manager Quick Setup

AWS Systems Manager Automation

Automation は、AWS のサービス (Amazon Elastic Compute Cloud (Amazon EC2)、Amazon Relational Database Service (Amazon RDS)、Amazon Redshift、Amazon Simple Storage Service (Amazon S3) など) でのメンテナンス、デプロイ、および修復に関する一般的なタスクを簡素化するための AWS Systems Manager のツールです。オートメーションを開始するには、Systems Manager コンソールを開きます。ナビゲーションペインで [オートメーション] を選択します。

オートメーションは、AWS リソースを大規模にデプロイ、設定、管理のための、自動化されたソリューションを構築するのに役立ちます。オートメーションを使用すると、自動化の同時実行性をきめ細かく制御できます。同時実行のターゲットにするリソースの数や、オートメーションを停止する前に許容可能なエラーの発生数を指定することが可能です。

オートメーションの使用開始時に役立てていただけるよう、AWS では、いくつかの事前定義済みランブックを開発および保守しています。これら定義済みランブックでは、ユースケースに応じてさまざまなタスクを実行できます。あるいは、カスタムのランブックを作成すれば、独自のニーズを満たすこともできます。オートメーションの進行状況とステータスをモニタリングするには、Systems Manager オートメーションコンソールを使用するか、任意のコマンドラインツールを使用します。オートメーションは Amazon EventBridge とも統合されており、大規模なイベント駆動型アーキテクチャを構築するのに役立ちます。

オートメーションには組織にとってどのようなメリットがありますか?

オートメーションには、次のようなメリットがあります。

- ランブックコンテンツ用のスクリプトサポート

  `aws:executeScript` アクションを使用することで、Python ならびに PowerShell のカスタム関数を、ランブックから直接実行できます。カスタムのランブックを作成することで、オートメーションで用意されたアクションではサポートされていない各種のタスクを完了できるようになるので、柔軟性が大きく向上します。同時に、ランブックのロジックをより詳細に制御できるようになります。このアクションの使用方法と、既存の自動ソリューションの改善にどのように役立つかについては、「オートメーションランブックのオーサリング」でサンプルを参照してください。
- 一元的な場所から複数の AWS アカウント および AWS リージョン 内のオートメーションを実行する

  管理者は Systems Manager コンソールから、複数のアカウントとリージョンにわたって、リソースに対してオートメーションを実行できます。
- 運用のための強化されたセキュリティ

管理者は一元的な場所から、ランブックへのアクセスを許可したり取り消したりできます。AWS Identity and Access Management (IAM) ポリシーのみを使用することで、組織内でオートメーションを使用できる個々のユーザーまたはグループを指定したり、これらのユーザーがアクセスできるランブックを制御することができます。

- 一般的な IT タスクを自動化する

  一般的なタスクを自動化することで、運用効率の向上、組織内での標準化の実施、オペレータが起こすエラー数の削減に役立ちます。例えば、AWS CloudFormation テンプレートを使用してデプロイされたリソースを更新するには、`AWS-UpdateCloudFormationStackWithApproval` ランブックが使用できます。更新には新しいテンプレートが適用されます。更新開始前に 1 人以上のユーザーの承認をリクエストするように自動化を設定できます。

- 分裂したタスクを一括で安全に実行する

  オートメーションには、同時実行数やエラー数のしきい値を指定することで、フリート全体でオートメーションのデプロイを制御するための、レート制御機能などが含まれています。レート制御機能の操作については、「自動オペレーションを大規模に実行する」を参照してください。

- 複雑なタスクを合理化する

  オートメーションでは、Golden Amazon Machine Images (AMIs) の作成など、複雑で時間のかかるタスクを合理化するための、事前定義済みランブックが利用できます。例えば、`AWS-UpdateLinuxAmi` および `AWS-UpdateWindowsAmi` ランブックを使用して、ソース AMI から Golden AMIs を作成できます。これらのランブックにより、更新が適用される前後にカスタムスクリプトを実行できます。また、特定のソフトウェアパッケージをインストールに含めたり、除外したりもできます。これらのランブックの使用例については、「チュートリアル」を参照してください。

- 入力での制約を定義する

  オートメーションが特定の入力パラメータについて受け入れる値の範囲を、カスタムランブックで定義し制限することができます。例えば、`allowedPattern` では、定義した正規表現に一致する値のみを、入力パラメータから受け入れます。入力パラメータに対し `allowedValues` を指定していると、ランブックで指定した値のみが受け入れられます。

- オートメーションアクションからの出力を Amazon CloudWatch Logs に ログ記録する

  組織の運用上またはセキュリティ上の要件を満たすために、ランブック内で実行されるスクリプトの記録が必要となることがあります。CloudWatch Logs を使用すると、さまざまな AWS のサービス からのログファイルについて、モニタリング、保存、アクセスが行えま

す。aws:executeScript アクションからの出力を CloudWatch Logs のロググループに送信し、デバッグやトラブルシューティングの目的に使用できます。ログデータは、KMS キーを使用した AWS KMS 暗号化の有無にかかわらずロググループに送信できます。詳細については、「CloudWatch Logs を使用した自動アクション出力のログ記録」を参照してください。

- Amazon EventBridge との統合

  オートメーションは、Amazon EventBridge ルール内で target 型としてサポートされます。つまり、イベントを使用してランブックをトリガーすることが可能です。詳細については、Amazon EventBridge を使用して Systems Manager イベントをモニタリングするおよびリファレンス: Systems Manager 用の Amazon EventBridge イベントパターンとタイプを参照してください。

- 組織のベストプラクティスを共有する

  リソース管理、運用タスクその他のベストプラクティスをランブックで定義すると、アカウントとリージョン間でそれを共有できます。

オートメーションはどのようなユーザーに適していますか?

- 大規模な運用における効率の向上、手動による介入が原因で起きるエラー数の削減、一般的な問題の解決にかかる時間の短縮を希望される、すべての AWS のお客様にご利用いただけます。
- デプロイおよび設定タスクを自動化しようとするインフラストラクチャの専門家。
- 一般的な問題の確実な解決、トラブルシューティングの効率向上、および反復処理の削減を希望する管理者。
- 通常手動で実行しているタスクの自動化を目指すユーザー。

オートメーションとは何ですか?

オートメーションは、ランブックで定義されているすべてのタスクを含んでおり、オートメーションサービスによって実行されます。オートメーションでは、次のコンポーネントを使用して自動化を実行します。

概念	詳細
オートメーションランブック	Systems Manager Automation ランブックでは、オートメーション (Systems Manager がマネージドノードと AWS リソースに対して実行するアクション) を定義します。オートメー

概念	詳細
	ションには、いくつかのランブックが事前に定義されており、1 つ以上の Amazon EC2 インスタンスの再起動や、Amazon Machine Image (AMI) の作成といった一般的なタスクを実行する際に使用することができます。独自のランブックを作成することもできます。ランブックは YAML や JSON を使用し、これらにはユーザーが指定するステップおよびパラメータが含まれています。ステップは順番に実行されます。詳細については、「独自のランブックの作成」を参照してください。 ランブックは、`Automation` 、`Command`、`Policy` ドキュメントとは異なり、`Session` タイプの Systems Manager ドキュメントです。ランブックは、スキーマバージョン 0.3 をサポートしています。Command ドキュメントは、スキーマバージョン 1.2、2.0、または 2.2 を使用します。ポリシードキュメントは、スキーマバージョン 2.0 以降を使用します。
自動化アクション	ランブックで定義されているオートメーションには、1 つ以上のステップが含まれています。各ステップは、特定のオペレーションに関連付けられます。このアクションは、ステップの入力、動作、出力を決定します。ステップは、ランブックの `mainSteps` セクションで定義されます。オートメーションは、20 種類の異なるアクションタイプをサポートしています。詳細については、「Systems Manager Automation アクションのリファレンス」を参照してください。

概念	詳細
オートメーションクォータ	各 AWS アカウント は、100 個のオートメーションを同時に実行できます。これには、子オートメーション (別のオートメーションによって開始されるオートメーション) とレート制御のオートメーションが含まれます。この数を超えるオートメーションを実行しようとすると、Systems Manager からキューに対して追加のオートメーションが行われ、保留中のステータスが表示されます。このクォータは、適応型同時実行を使用して調整できます。詳細については「オートメーションで同時実行のニーズに対する適応を許可する」を参照してください。オートメーションの実行に関する詳細は「Systems Manager Automation を使用した自動オペレーションを実行する」を参照してください。
オートメーションキューのクォータ	同時オートメーションの制限よりも多くのオートメーションを実行しようとすると、後続のオートメーションがキューに追加されます。各 AWS アカウント は、5,000 個のオートメーションをキューに入れることができます。オートメーションが完了 (または終了状態に到達) すると、キューの最初のオートメーションが開始されます。

概念	詳細
レート制御のオートメーションクォータ	各 AWS アカウント は、25 個のレート制御のオートメーションを同時に実行できます。同時レート制御のオートメーション制限よりも多くのレート制御のオートメーションを実行しようとすると、Systems Manager は後続のレート制御のオートメーションをキューに追加し、保留中のステータスが表示されます。レート制御のオートメーション実行の詳細については、「自動オペレーションを大規模に実行する」を参照してください。
レート制御のオートメーションキューのクォータ	同時レート制御のオートメーション制限よりも多くのオートメーションを実行しようとすると、後続のオートメーションがキューに追加されます。各 AWS アカウント は、1,000 個のレート制御のオートメーションをキューに入れることができます。オートメーションが完了 (または終了状態に到達) すると、キューの最初のオートメーションが開始されます。

トピック

- オートメーションの設定
- Systems Manager Automation を使用した自動オペレーションを実行する
- 承認が必要なオートメーションを実行する
- 自動オペレーションを大規模に実行する
- 複数の AWS リージョン とアカウントでのオートメーションの実行
- EventBridge イベントに基づくオートメーションを実行する
- オートメーションを段階的に実行する
- State Manager 関連付けでのオートメーションのスケジュール設定
- メンテナンスウィンドウによるオートメーションのスケジュール設定
- Systems Manager Automation アクションのリファレンス
- 独自のランブックの作成

- Systems Manager Automation ランブックのリファレンス
- チュートリアル
- Systems Manager Automation が返すステータスについて学ぶ
- Systems Manager Automation のトラブルシューティング

オートメーションの設定

AWS Systems Manager のツールである Automation をセットアップするには、Automation サービスへのユーザーアクセスを検証し、サービスがリソースでアクションを実行できるように、状況に応じてロールを設定する必要があります。また、オートメーションの設定で、適応同時実行モードにオプトインしておくことをお勧めします。適応同時実行では、オートメーションのクォータが、ニーズに合わせて自動的にスケーリングされます。詳細については、「オートメーションで同時実行のニーズに対する適応を許可する」を参照してください。

AWS Systems Manager 自動化への適切なアクセスを確保するために、次のユーザーおよびサービスロールの要件を確認します。

ランブックへのユーザーアクセスの確認

ランブックを使用するアクセス許可があることを確認します。ユーザー、グループ、ロールに管理者権限が割り当てられている場合は、Systems Manager Automation にアクセスできます。管理者権限がない場合は、管理者に `AmazonSSMFullAccess` マネージドポリシーの割り当てを依頼するか、ユーザー、グループ、ロールに同等のアクセス許可を付与するポリシーの割り当てを依頼してください。

> **Important**
>
> IAM ポリシー `AmazonSSMFullAccess` は、Systems Manager のアクションにアクセス許可を付与します。ただし、一部のランブックでは、ランブック `AWS-ReleaseElasticIP` などの他のサービスに対するアクセス許可が必要であり、これには `ec2:ReleaseAddress` に対する IAM アクセス許可が必要です。したがって、ランブックで実行されたアクションを確認し、ユーザー、グループ、ロールに、ランブックに含まれるアクションを実行するために必要なアクセス許可が割り当てられていることを確認する必要があります。

オートメーションのサービスロール（ロールを引き受ける）アクセスの設定

オートメーションは、サービスロール（または継承ロール）のコンテキストで開始できます。これにより、サービスがユーザーに代わってアクションを実行できるようになります。継承ロールを指定しない場合、オートメーションは、オートメーションを呼び出したユーザーのコンテキストを使用します。

ただし、次の条件では、自動化にサービスロールを指定する必要があります。

- リソースに対するユーザーのアクセス許可は制限するが、そのユーザーに昇格された許可を必要とするオートメーションを実行させる場合があるとします。このシナリオでは、昇格されたアクセス許可を持つサービスロールを作成して、このユーザーにオートメーションの実行を許可できます。
- ランブックを実行する Systems Manager State Manager の関連付けを作成する場合。
- 実行時間が 12 時間を超えると予想されるオペレーションがある場合。
- `aws:executeScript` アクションを使用して AWS API オペレーションを呼び出したり、AWS リソースを操作する Amazon が所有していないランブックを実行している場合。詳細については、ランブックを使用するためのアクセス許可 を参照してください。

自動化のためのサービスロールを作成する必要がある場合、次のいずれかのメソッドを使用できます。

トピック

- AWS CloudFormation を使用して Automation 用のサービスロールを作成する
- コンソールを使用して Automation 用のサービスロールを作成する
- オートメーションで同時実行のニーズに対する適応を許可する
- オートメーションの変更管理の実装

AWS CloudFormation を使用して Automation 用のサービスロールを作成する

AWS Systems Manager のツールである Automation のサービスロールは AWS CloudFormation テンプレートから作成できます。サービスロールを作成したら、パラメータ `AutomationAssumeRole` を使用してランブックでサービスロールを指定できます。

AWS CloudFormation を使用してサービスロールを作成する

AWS CloudFormation を使用して Systems Manager Automation に必要な AWS Identity and Access Management (IAM) ロールを作成するには、次の手順に従います。

必須の IAM ロールを作成するには

1. AWS-SystemsManager-AutomationServiceRole.zip ファイルをダウンロードして解凍します。このファイルには、AWS-SystemsManager-AutomationServiceRole.yaml AWS CloudFormation テンプレートファイルが含まれています。
2. https://console.aws.amazon.com/cloudformation で AWS CloudFormation コンソール を開きます。
3. [Create Stack] を選択します。
4. [Specify template (テンプレートの指定)] セクションで、[Upload a template file (テンプレートファイルのアップロード)] を選択します。
5. [参照] を選択して、AWS-SystemsManager-AutomationServiceRole.yaml AWS CloudFormation テンプレートファイルを選択します。
6. [Next] を選択します。
7. [Specify stack details (スタックの詳細の指定)] ページの [Stack Name (スタック名)] フィールドに名前を入力します。
8. [Configure stack options (スタックオプションの設定)] ページでは何も選択する必要はありません。[Next] を選択します。
9. [Review (確認)] ページで、下にスクロールして、[I acknowledge that AWS CloudFormation might create IAM resources] オプションを選択します。
10. [Create] を選択します。

CloudFormation は、[CREATE_IN_PROGRESS] ステータスを約 3 分間表示します。スタックが作成され、ロールを使用できる状態になると、ステータスが [CREATE_COMPLETE] に変わります。

> **Important**
>
> AWS Identity and Access Management (IAM) サービスロールを使用して他のサービスを呼び出す自動化ワークフローを実行する場合は、それらのサービスを呼び出すためのアクセス許可をサービスロールに設定する必要がある点に注意してください。この要件は、AWS-ConfigureS3BucketLogging、AWS-CreateDynamoDBBackup、AWS-RestartEC2Instance ランブックなど、すべての AWS オートメーションランブック (AWS-* ランブック) に適用されます。この要件は、他のサービスを呼び出すアクションを使用して他の AWS のサービスを呼び出すように作成したカスタムオートメーションランブックにも適用されます。例えば、aws:executeAwsApi、aws:createStack、または aws:copyImage のアクションを使用する場合は、それらのサービスを呼び出すためのアク

セス許可を持つサービスロールを設定します。ロールに IAM インラインポリシーを追加することで、他の AWS のサービスへのアクセス許可を有効にできます。詳細については、「(オプション) 他の AWS のサービス を呼び出すためのオートメーションインラインポリシーまたはカスタマー管理ポリシーを追加する」を参照してください。

自動化のロール情報をコピーする

次の手順を使用して、AWS CloudFormation コンソールから自動化サービスロールの情報をコピーします。ランブックを使用するときは、これらのロールを指定する必要があります。

> **Note**
>
> `AWS-UpdateLinuxAmi` または `AWS-UpdateWindowsAmi` ランブックを実行する場合は、この手順を使ってロール情報をコピーする必要はありません。これらのランブックには、すでにデフォルト値として指定されている必要なロールがあります。これらのランブックで指定されているロールは、IAM 管理ポリシーを使用します。

ロール名をコピーするには

1. https://console.aws.amazon.com/cloudformation で AWS CloudFormation コンソール を開きます。
2. 前の手順で作成したオートメーション [スタック名] を選択します。
3. [Resources] タブを選択します。
4. [AutomationServiceRole] リンクの [Physical ID] を選択します。IAM コンソールが、オートメーションサービスロールの概要を開きます。
5. [ロール ARN] の横にある Amazon リソースネーム (ARN) をコピーします。ARN は次のようになります。`arn:aws:iam::12345678:role/AutomationServiceRole`
6. ARN を後で使用するテキストファイルに貼り付けます。

これで、自動化用サービスロールの設定が完了しました。ランブックでオートメーションサービスロール ARN を使用できるようになりました。

コンソールを使用して Automation 用のサービスロールを作成する

AWS Systems Manager のツールである Automation のサービスロールを作成する必要がある場合、次のいずれかのタスクを完了します。オートメーションにサービスロールが必要な場合の詳細については、「オートメーションの設定」を参照してください 。

タスク

- タスク 1: 自動化のサービスロールを作成する
- タスク 2: iam:PassRole ポリシーをオートメーションロールにアタッチする

タスク 1: 自動化のサービスロールを作成する

次の手順を使用して、Systems Manager Automation のサービスロールを作成 (または、ロールを継承) します。

> **Note**
>
> このロールは、`AWS-CreateManagedLinuxInstance` ランブックなどのランブックでも使用できます。ランブックでこのロール、または AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN) を使用すると、オートメーションにより新しいインスタンスの起動やユーザーに代わってアクションを実行するなどのアクションをお客様の環境で実行できます。

IAM ロールを作成し、Automation がそのロールを引き受けることを許可します。

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. ナビゲーションペインで ロール を選択し、続いて ロールを作成する を選択します。
3. [Select type of trusted entity] (信頼されたエンティティの種類を選択) の下で、[AWS service] (AWS サービス) を選択します。
4. [Choose a use case (ユースケースの選択)] セクションで、[Systems Manager] を選択し、[Next: Permissions (次へ: アクセス許可)] を選択します。
5. [Attached permissions policy] ページで [AmazonSSMAutomationRole] を検索して選択したら、[Next: Review] を選択します。
6. [Review (確認)] ページの [Role name (ロール名)] ボックスに名前を入力し、続いて説明を入力します。
7. [ロールの作成] を選択します。ロールページが再度表示されます。

8. ロール ページで作成したロールを選択して、概要 ページを開きます。[ロール名] と [ロール ARN] を書き留めます。ロール ARN は、次の手順で iam:PassRole ポリシーを IAM アカウントにアタッチするときに指定します。ランブックでロール名と ARN を指定することもできます。

> **Note**
>
> `AmazonSSMAutomationRole` ポリシーは、アカウント内の一部の AWS Lambda 関数に Automation ロールのアクセス許可を割り当てます。これらの関数は「Automation」で始まります。Lambda 関数で Automation を使用する予定の場合、Lambda ARN には以下の形式を使用する必要があります。
> `"arn:aws:lambda:*:*:function:Automation*"`
> この形式を使用していない ARN を持つ既存の Lambda 関数がある場合、オートメーションロールに追加で AWSLambdaRole ポリシーなどの Lambda ポリシーをアタッチする必要があります。追加のポリシーまたはロールは、内の Lambda 関数へのより広範なアクセスを許可する必要がありますAWS アカウント

サービスロールを作成した後は、クロスサービスの混乱による代理の問題を防ぐために、信頼ポリシーを修正するようにお勧めします。「混乱した代理」問題は、アクションを実行するためのアクセス許可を持たないエンティティが、より特権のあるエンティティにアクションの実行を強制できてしまう場合に生じる、セキュリティ上の問題です。AWS では、サービス間でのなりすましによって、混乱した代理問題が発生する場合があります。サービス間でのなりすましは、1 つのサービス (呼び出し元サービス) が、別のサービス (呼び出し対象サービス) を呼び出すときに発生する可能性があります。呼び出し元サービスは、本来ならアクセスすることが許可されるべきではない方法でその許可を使用して、別のお客様のリソースに対する処理を実行するように操作される場合があります。これを防ぐため、AWS では、アカウントのリソースへのアクセス権が付与されたサービスプリンシパルで、すべてのサービスのデータを保護するために役立つツールを提供しています。

リソースポリシー内の `aws:SourceArn` と `aws:SourceAccount` のグローバル条件コンテキストキーを使用して、リソースについてオートメーションが別のサービスに付与するアクセス許可を、制限することをお勧めします。Amazon S3 バケットの ARN などのアカウント ID が、`aws:SourceArn` 値に含まれていない場合、アクセス許可を制限するためには、これら両方のグローバル条件コンテキストキーを使用する必要があります。同じポリシーステートメントでこれらのグローバル条件コンテキストキーの両方を使用し、アカウント ID に`aws:SourceArn` の値が含まれていない場合、`aws:SourceAccount` 値と `aws:SourceArn` 値の中のアカウントには、同じアカウント ID を使用する必要があります。クロスサービスのアクセスにリソースを 1 つだけ関連付けたい場合は、`aws:SourceArn` を使用します。そのアカウント内のリソー

スをクロスサービスの使用に関連付けることを許可する場合は、aws:SourceAccount を使用します。aws:SourceArn の値は、オートメーション実行の ARN である必要があります。リソースの ARN 全体が不明または複数のリソースを指定する場合、ARN の未知部分にワイルドカード *が付いた aws:SourceArn グローバルコンテキスト条件キー を使用します。例えば、arn:aws:ssm:*:123456789012:automation-execution/* と指定します。

以下の例はオートメーション用に aws:SourceArn と aws:SourceAccount のグローバル条件コンテキストキーを使用して「混乱した使節の問題」を防止する方法を示します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "ssm.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:ssm:*:123456789012:automation-execution/*"
        }
      }
    }
  ]
}
```

ロールの信頼ポリシーを変更するには

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. ナビゲーションペインで [Roles] (ロール) を選択します。
3. アカウントのロールのリストから、オートメーションのサービスロールの名前を選択します。
4. [Trust relationships] タブを選択し、続いて [Edit trust relationship] を選択します。
5. オートメーション用の aws:SourceArn と aws:SourceAccount のグローバル条件コンテキストキーを使用して「混乱した代理の問題」を防止するために信頼ポリシーを修正します。

6. [Update Trust Policy] (信頼ポリシーの更新) をクリックし、変更を保存します。

(オプション) 他の AWS のサービス を呼び出すためのオートメーションインラインポリシーまたはカスタマー管理ポリシーを追加する

IAM サービスロールを使用して他の AWS のサービスを呼び出すオートメーションを実行する場合は、それらのサービスを呼び出すためのアクセス許可をサービスロールに設定する必要があります。この要件は、`AWS-ConfigureS3BucketLogging`、`AWS-CreateDynamoDBBackup`、`AWS-RestartEC2Instance` ランブックなど、すべての AWS オートメーションランブック (`AWS-*` ランブック) に適用されます。この要件は、他のサービスを呼び出すアクションを使用して他の AWS のサービスを呼び出すように作成したカスタムランブックにも適用されます。たとえば、`aws:executeAwsApi`、`aws:CreateStack`、または `aws:copyImage` などのアクションを使用する場合は、それらのサービスを呼び出すためのアクセス許可を持つサービスロールを設定する必要があります。ロールに IAM インラインポリシーまたはカスタマー管理ポリシーを追加することで、他の AWS のサービス へのアクセス許可を有効にできます。

ユーザーまたはロールのインラインポリシーを埋め込むには (IAM コンソール)

1. AWS Management Console にサインインして、IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. ナビゲーションペインで [Roles (ロール)] を選択します。
3. リストで編集するロールの名前を選択します。
4. [Permissions] タブを選択します。
5. [アクセス許可の追加] ドロップダウンで、[ポリシーをアタッチする] または [インラインポリシーの作成] を選択します。
6. [ポリシーをアタッチする] を選択した場合、追加するポリシーの横にあるチェックボックスを選択して [アクセス許可の追加] を選択します。
7. [ポリシーの作成] を選択し、[JSON] タブを選択します。
8. 呼び出す AWS のサービスの JSON ポリシードキュメントを入力します。JSON ポリシードキュメントの 2 つの例を以下に示します。

   Amazon S3 PutObject と GetObject の例

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

```
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
        }
    ]
}
```

Amazon EC2 CreateSnapshot と DescribeSnapShots の例

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshot",
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action":"ec2:DescribeSnapshots",
         "Resource":"*"
      }
   ]
}
```

IAM ポリシー言語の詳細については、IAM ユーザーガイドの「IAM JSON ポリシーリファレンス」を参照してください。

9. 完了したら、[ポリシーの確認] を選択します。構文エラーがある場合は、Policy Validator (ポリシー検証) によってレポートされます。
10. [ポリシーの確認] ページで、作成するポリシーの [名前] を入力します。ポリシーの [概要] を確認して、ポリシーで許可されている権限を確認します。次に [ポリシーの作成] を選択して作業を保存します。
11. インラインポリシーを作成した後は、自動的にロールに埋め込まれます。

タスク 2: iam:PassRole ポリシーをオートメーションロールにアタッチする

以下の手順を使用して、`iam:PassRole` ポリシーを Automation サービスロールにアタッチします。これにより、自動化を実行する際に、Automation サービスによって他のサービスまたは Systems Manager ツールにロールが渡されるようになります。

iam:PassRole ポリシーを自動化ロールにアタッチするには

1. 作成したロールの [Summary] ページで [Permissions] タブを選択します。
2. [Add inline policy] を選択します。
3. [ポリシーの作成] ページの [Visual editor] (ビジュアルエディタ) タブを選択します。
4. [サービス]、[IAM] の順に選択します。
5. [アクションの選択] を選択します。
6. [Filter actions (フィルタアクション)] テキストボックスに「**`PassRole`**」と入力し、[PassRole] オプションを選択します。
7. [リソース] を選択します。[Specific] (固有) が選択されていることを確認し、[Add ARN] (ARN の追加) を選択します。
8. [Specify ARN for role] (ロールの ARN の指定) フィールドに、タスク 1 の終わりでコピーした自動化ロールの ARN を貼り付けます。システムによって、[アカウント] と [Role name with path (ロール名とパス)] フィールドが入力されます。

   > **Note**
   >
   > オートメーションサービスロールで IAM インスタンスプロファイルロールを EC2 インスタンスにアタッチする場合は、IAM インスタンスプロファイルロールの ARN を追加する必要があります。これにより、オートメーションサービスロールが IAM インスタンスプロファイルのロールをターゲット EC2 インスタンスに渡すことができます。

9. [Add] (追加) をクリックします。
10. [Review policy (ポリシーの確認)] を選択します。
11. [Review Policy (ポリシーの確認)] ページに名前を入力し、[Create Policy (ポリシーの作成)] を選択します。

オートメーションで同時実行のニーズに対する適応を許可する

オートメーションのデフォルトでは、一度に最大 100 個の自動化処理を同時実行できます。またオートメーションには、同時実行される自動化のクォータを自動的に調整するためのオプション設定も用意されています。このオプションを設定することで、同時実行される自動化処理のクォータを、使用可能なリソースに応じて最大で 500 個まで増やすことができます。

> **Note**
>
> オートメーションが API オペレーションを呼び出す場合、ターゲットに合わせて適応的にスケーリングした際に、スロットリングに関する例外が発生する可能性があります。適応的な同時実行を有効にして自動化を実行していて、定期的なスロットリング例外が発生する場合には、API オペレーションのクォータの増加をリクエストする必要も生じます。

AWS Management Console を使用して適応同時実行をオンにするには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで [オートメーション] を選択します。
3. [設定] タブを選択してから、[編集] を選択します。
4. [Enable adaptive concurrency] (適応同時実行を有効にする) の横にあるチェックボックスをオンにします。
5. [Save] を選択します。

コマンドラインを使用して適応同時実行をオンにするには

- AWS CLI または Tools for Windows PowerShell を開き、次のコマンドを実行して、リクエスト元のリージョンのアカウントのために適応同時実行をオンにします。

  Linux & macOS

  ```
  aws ssm update-service-setting \
      --setting-id /ssm/automation/enable-adaptive-concurrency \
      --setting-value True
  ```

Windows

```
aws ssm update-service-setting ^
    --setting-id /ssm/automation/enable-adaptive-concurrency ^
    --setting-value True
```

PowerShell

```
Update-SSMServiceSetting `
    -SettingId "/ssm/automation/enable-adaptive-concurrency" `
    -SettingValue "True"
```

オートメーションの変更管理の実装

デフォルトのオートメーションでは、日付と時刻の制約なしにランブックを使用できます。オートメーションを Change Calendar と統合することで、AWS アカウント のすべてのオートメーションに変更管理を実装できます。この設定では、アカウントの AWS Identity and Access Management (IAM) プリンシパルは、変更カレンダーで許可されている期間にのみオートメーションを実行できます。Change Calendar での作業の詳細については、「「Change Calendar」 の使用」を参照してください。

変更管理を有効にするには (コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで [オートメーション] を選択します。
3. [設定] タブを選択してから、[編集] を選択します。
4. [Change Calendar の統合を有効にする] の横にあるチェックボックスをオンにします。
5. [変更カレンダーの選択] ドロップダウンリストで、オートメーションに適用する変更カレンダーを選択します。
6. [保存] を選択します。

Systems Manager Automation を使用した自動オペレーションを実行する

デフォルトでは、オートメーションを実行すると、オートメーションはオートメーションを開始したユーザーのコンテキストで実行されます。例えば、 ユーザーが管理者のアクセス許可を持っている

場合、オートメーションは、管理者のアクセス許可とオートメーションで設定されているリソースに対するフルアクセスを使用して実行されます。セキュリティのベストプラクティスとして、オートメーションは、AmazonSSMAutomationRole 管理ポリシーで設定されている IAM サービスロール (継承ロールとも呼ばれる) を使用して実行することをお勧めします。さまざまなランブックを使用するために、継承ロールに IAM ポリシーを追加する必要がある場合があります。IAM サービスロールを使用したオートメーションの実行は、委任管理者と呼ばれます。

サービスロールを使用すると、AWS リソースに対してオートメーションを実行することはできますが、オートメーションを実行したユーザーによる、それらのリソースに対するアクセスは制限されます (またはアクセスできません)。例えば、サービスロールを設定後、オートメーションでそのロールを使用して、1 つ以上の Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを再起動できます。Automation は AWS Systems Manager のツールです。オートメーションによってインスタンスは再起動されますが、ユーザーがそのサービスロールを使用して、そのインスタンスにアクセスすることはできません。

オートメーションを実行する際、ランタイムでサービスロールを指定するか、カスタムのランブックを作成して、ランブックで直接サービスロールを指定することができます。ランタイム時またはランブックでサービスロールを指定した場合、サービスは、指定したサービスロールのコンテキストで実行されます。サービスロールを指定しない場合、システムは、ユーザーのコンテキストで一時セッションを作成し、オートメーションを実行します。

> **Note**
>
> オートメーションを 12 時間以上実行する場合は、サービスロールを指定する必要があります。ユーザーのコンテキストで長時間稼働するオートメーションを開始すると、ユーザーの一時セッションの有効期限は 12 時間後に切れます。

委任管理者は、AWS リソースの昇格されたセキュリティと制御を保証します。また、アクションは複数の IAM リソースではなく、主要サービスロールのリソースに対して実行されているため、監査プロセスを強化することができます。

[開始する前に]

次の手順を完了する前に、IAM サービスロールを作成し、AWS Systems Manager のツールである Automation への信頼関係を設定する必要があります。詳細については、「タスク 1: 自動化のサービスロールを作成する」を参照してください。

次の手順では、Systems Manager コンソールまたは任意のコマンドラインツールを使用してシンプルなオートメーションを実行する方法を説明します。

シンプルなオートメーションを実行する (コンソール)

次の手順では、Systems Manager コンソールを使用してシンプルなオートメーションを実行する方法を説明します。

シンプルなオートメーションを実行するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[オートメーション]、[オートメーションの実行] の順に選択します。
3. [Automation document (自動化ドキュメント)] リストで、ランブックを選択します。[Document categories (ドキュメントカテゴリ)] ペインで 1 つ以上のオプションを選択して、目的に応じて SSM ドキュメントをフィルタリングします。自分が所有するランブックを表示するには、[Owned by me (自分が所有)] タブを選択します。自分のアカウントと共有されているランブックを表示するには、[Shared with me (共有ファイル)] タブを選択します。すべてのランブックを表示するには、[すべてのドキュメント] タブを選択します。

   > **Note**
   >
   > ランブックの名前を選択すると、ランブックに関する情報を表示できます。

4. [Document details (ドキュメントの詳細)] セクションで、[Document version (ドキュメントのバージョン)] が実行するバージョンに設定されていることを確認します。システムには、次のバージョンのオプションが含まれています。

   - [ランタイムのデフォルトバージョン]: 自動化ランブックが定期的に更新され、新しいデフォルトバージョンが割り当てられている場合は、このオプションを選択します。
   - [ランタイムの最新バージョン]: 自動化ランブックが定期的に更新され、直前に更新されたバージョンを実行する場合は、このオプションを選択します。
   - [1 (デフォルト)]: ドキュメントの最初のバージョンを実行するには、このオプションを選択します。これはデフォルト設定です。

5. [Next] を選択します。
6. [Execution Mode (実行モード)] セクションで、[Simple execution (シンプルな実行)] を選択します。

7. [Input parameters (入力パラメータ)] セクションで、必要な入力を指定します。必要に応じて、[AutomationAssumeRole] リストから IAM サービスロールを選択できます。
8. (オプション) モニタリング用のオートメーションに適用する CloudWatch アラームを選択します。CloudWatch アラームをオートメーションにアタッチするには、コマンドを実行する IAM プリンシパルに `iam:createServiceLinkedRole` アクションの権限が必要です。CloudWatch アラームの詳細については、「Amazon CloudWatch でのアラームの使用」を参照してください。アラームが作動すると、オートメーションは停止されます。AWS CloudTrail を使用する場合、トレイルに API コールが表示されます。
9. [Execute] を選択します。

オートメーションのステータスがコンソールに表示されます。オートメーションの実行に失敗した場合は、「Systems Manager Automation のトラブルシューティング」を参照してください。

シンプルなオートメーションを実行する (コマンドライン)

次の手順では、AWS CLI (Linux または Windows) または AWS Tools for PowerShell を使用してシンプルなオートメーションを実行する方法を説明します。

シンプルなオートメーションを実行するには

1. まだ AWS CLI または AWS Tools for PowerShell をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」および「AWS Tools for PowerShell のインストール」を参照してください。
2. 以下のコマンドを実行して、シンプルなオートメーションを開始します。各*##########*をユーザー自身の情報に置き換えます。

   Linux & macOS

   ```
   aws ssm start-automation-execution \
       --document-name runbook name \
       --parameters runbook parameters
   ```

   Windows

   ```
   aws ssm start-automation-execution ^
       --document-name runbook name ^
   ```

```
    --parameters runbook parameters
```

PowerShell

```
Start-SSMAutomationExecution `
  -DocumentName runbook name `
  -Parameter runbook parameters
```

ランブック AWS-RestartEC2Instance を使用して指定した EC2 インスタンスを再起動する例を次に示します。

Linux & macOS

```
aws ssm start-automation-execution \
    --document-name "AWS-RestartEC2Instance" \
    --parameters "InstanceId=i-02573cafcfEXAMPLE"
```

Windows

```
aws ssm start-automation-execution ^
    --document-name "AWS-RestartEC2Instance" ^
    --parameters "InstanceId=i-02573cafcfEXAMPLE"
```

PowerShell

```
Start-SSMAutomationExecution `
  -DocumentName AWS-RestartEC2Instance `
  -Parameter @{"InstanceId"="i-02573cafcfEXAMPLE"}
```

システムが以下のような情報を返します。

Linux & macOS

```
{
    "AutomationExecutionId": "4105a4fc-f944-11e6-9d32-0123456789ab"
}
```

Windows

```
{
    "AutomationExecutionId": "4105a4fc-f944-11e6-9d32-0123456789ab"
}
```

PowerShell

```
4105a4fc-f944-11e6-9d32-0123456789ab
```

3. 次のコマンドを実行してオートメーションのステータスを取得します。

Linux & macOS

```
aws ssm describe-automation-executions \
    --filter "Key=ExecutionId,Values=4105a4fc-f944-11e6-9d32-0123456789ab"
```

Windows

```
aws ssm describe-automation-executions ^
    --filter "Key=ExecutionId,Values=4105a4fc-f944-11e6-9d32-0123456789ab"
```

PowerShell

```
Get-SSMAutomationExecutionList | `
  Where {$_.AutomationExecutionId -eq "4105a4fc-f944-11e6-9d32-0123456789ab"}
```

システムが以下のような情報を返します。

Linux & macOS

```
{
    "AutomationExecutionMetadataList": [
        {
            "AutomationExecutionStatus": "InProgress",
            "CurrentStepName": "stopInstances",
            "Outputs": {},
            "DocumentName": "AWS-RestartEC2Instance",
            "AutomationExecutionId": "4105a4fc-f944-11e6-9d32-0123456789ab",
```

```
            "DocumentVersion": "1",
            "ResolvedTargets": {
                "ParameterValues": [],
                "Truncated": false
            },
            "AutomationType": "Local",
            "Mode": "Auto",
            "ExecutionStartTime": 1564600648.159,
            "CurrentAction": "aws:changeInstanceState",
            "ExecutedBy": "arn:aws:sts::123456789012:assumed-role/Administrator/
Admin",
            "LogFile": "",
            "Targets": []
        }
    ]
}
```

Windows

```
{
    "AutomationExecutionMetadataList": [
        {
            "AutomationExecutionStatus": "InProgress",
            "CurrentStepName": "stopInstances",
            "Outputs": {},
            "DocumentName": "AWS-RestartEC2Instance",
            "AutomationExecutionId": "4105a4fc-f944-11e6-9d32-0123456789ab",
            "DocumentVersion": "1",
            "ResolvedTargets": {
                "ParameterValues": [],
                "Truncated": false
            },
            "AutomationType": "Local",
            "Mode": "Auto",
            "ExecutionStartTime": 1564600648.159,
            "CurrentAction": "aws:changeInstanceState",
            "ExecutedBy": "arn:aws:sts::123456789012:assumed-role/Administrator/
Admin",
            "LogFile": "",
            "Targets": []
        }
    ]
}
```

PowerShell

```
AutomationExecutionId       : 4105a4fc-f944-11e6-9d32-0123456789ab
AutomationExecutionStatus   : InProgress
AutomationType              : Local
CurrentAction               : aws:changeInstanceState
CurrentStepName             : startInstances
DocumentName                : AWS-RestartEC2Instance
DocumentVersion             : 1
ExecutedBy                  : arn:aws:sts::123456789012:assumed-role/
Administrator/Admin
ExecutionEndTime            : 1/1/0001 12:00:00 AM
ExecutionStartTime          : 7/31/2019 7:17:28 PM
FailureMessage              :
LogFile                     :
MaxConcurrency              :
MaxErrors                   :
Mode                        : Auto
Outputs                     : {}
ParentAutomationExecutionId :
ResolvedTargets             :
 Amazon.SimpleSystemsManagement.Model.ResolvedTargets
Target                      :
TargetMaps                  : {}
TargetParameterName         :
Targets                     : {}
```

承認が必要なオートメーションを実行する

次の手順では、AWS Systems Manager コンソールおよび AWS Command Line Interface (AWS CLI) を使用して、シンプルな実行によりオートメーションを実行する方法について説明します。オートメーションは、オートメーションアクション `aws:approve` を使用します。これにより、指定されたプリンシパルがアクションを承認または拒否するまで、オートメーションは一時停止します。このオートメーションは、現在のユーザーのコンテキストで実行します。これは、ランブックおよびこのランブックが呼び出すアクションを使用するアクセス許可がある限り、追加の IAM アクセス許可を設定する必要がないことを意味しています。IAM での管理者アクセス許可がある場合、このオランブックを実行するアクセス許可を既に保持しています。

開始する前に

ランブックで必要とされる標準入力に加えて、aws:approve アクションは以下の 2 つのパラメータを必要とします。

- 承認者のリスト。承認者のリストには、ユーザー名またはユーザー ARN の形式の承認者を少なくとも 1 人含める必要があります。複数の承認者が提供されている場合は、対応する最小承認数もランブック内で指定する必要があります。
- Amazon Simple Notification Service (Amazon SNS) のトピック ARN Amazon SNS トピック名は、Automation で始まる必要があります。

この手順では、承認リクエストを配信するために必要な Amazon SNS トピックが既に作成されていることを前提としています。詳細については、Amazon Simple Notification Service デベロッパーガイドの「トピックの作成」を参照してください。

承認者によるオートメーションの実行 (コンソール)

承認者を使用してオートメーションを実行するには

次の手順では、Systems Manager コンソールを使用して承認者がシンプルなオートメーションを実行する方法を説明します。

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[オートメーション]、[オートメーションの実行] の順に選択します。
3. [Automation document (自動化ドキュメント)] リストで、ランブックを選択します。[Document categories (ドキュメントカテゴリ)] ペインで 1 つ以上のオプションを選択して、目的に応じて SSM ドキュメントをフィルタリングします。自分が所有するランブックを表示するには、[Owned by me (自分が所有)] タブを選択します。自分のアカウントと共有されているランブックを表示するには、[Shared with me (共有ファイル)] タブを選択します。すべてのランブックを表示するには、[すべてのドキュメント] タブを選択します。

   > **Note**
   >
   > ランブックの名前を選択すると、ランブックに関する情報を表示できます。

4. [Document details (ドキュメントの詳細)] セクションで、[Document version (ドキュメントのバージョン)] が実行するバージョンに設定されていることを確認します。システムには、次のバージョンのオプションが含まれています。

- [ランタイムのデフォルトバージョン]: 自動化ランブックが定期的に更新され、新しいデフォルトバージョンが割り当てられている場合は、このオプションを選択します。
- [ランタイムの最新バージョン]: 自動化ランブックが定期的に更新され、直前に更新されたバージョンを実行する場合は、このオプションを選択します。
- [1 (デフォルト)]: ドキュメントの最初のバージョンを実行するには、このオプションを選択します。これはデフォルト設定です。

5. [Next] を選択します。
6. [Execute automation document (自動化ドキュメントの実行)] ページで、[Simple execution (シンプルな実行)] を選択します。
7. [Input Parameters (入力パラメータ)] セクションで、必須の入力パラメータを指定します。

   例えば、**`AWS-StartEC2InstanceWithApproval`** ランブックを選択した場合は、[InstanceId] パラメータにインスタンス ID を指定または選択する必要があります。
8. [承認者] セクションで、自動化アクションの承認者のユーザー名またはユーザー ARN を指定します。
9. [SNSTopicARN] セクションで、承認通知の送信に使用する SNS トピックの ARN を指定します。SNS トピック名は Automation で始まる必要があります。
10. 必要に応じて、[AutomationAssumeRole] リストから IAM サービスロールを選択できます。100 を超えるアカウントとリージョンをターゲットにする場合は、`AWS-SystemsManager-AutomationAdministrationRole` を指定する必要があります。
11. [Execute automation] を選択します。

指定された承認者は、オートメーションを承認または却下するための詳細を含む Amazon SNS 通知を受け取ります。この承認アクションは発行日から 7 日間有効で、Systems Manager コンソールまたは AWS Command Line Interface (AWS CLI) を使用して発行できます。

オートメーションを承認することを選択した場合、オートメーションは指定されたランブックに含まれているステップを実行し続けます。オートメーションのステータスがコンソールに表示されます。オートメーションの実行に失敗した場合は、「Systems Manager Automation のトラブルシューティング」を参照してください。

オートメーションを許可または拒否するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。

2. ナビゲーションペインで、[Automation (オートメーション)] を選択し、前の手順で実行したオートメーションを選択します。
3. [Actions (アクション)] を選択して、[Approve/Deny (承認/拒否)] を選択します。
4. [Approve (承認)] または [Deny (拒否)]を選択し、オプションでコメントを入力します。
5. [Submit] (送信) をクリックします。

承認者によるオートメーションの実行 (コマンドライン)

次の手順では、AWS CLI (Linux または Windowsで) または AWS Tools for PowerShell を使用して承認者がオートメーションを実行する方法を説明します。

承認者を使用してオートメーションを実行するには

1. まだ AWS CLI または AWS Tools for PowerShell をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」および「AWS Tools for PowerShell のインストール」を参照してください。
2. 次のコマンドを実行して、承認者によりオートメーションを実行します。各##########をユーザー自身の情報に置き換えます。[Document name (文書名)] セクションで、オートメーションアクション `aws:approve` を含むランブックを指定します。

   `Approvers` には、アクションの承認者のユーザー名またはユーザー ARN を指定します。`SNSTopic` に、承認通知の送信に使用する SNS トピック の ARN を指定します。Amazon SNS トピック名は、`Automation` で始まる必要があります。

   > **Note**
   >
   > 承認者および SNS トピックのパラメータ値の特定の名前は、選択したランブック内で指定されている値によって異なります。

   Linux & macOS

   ```
   aws ssm start-automation-execution \
       --document-name "AWS-StartEC2InstanceWithApproval" \
   ```

```
    --parameters
 "InstanceId=i-02573cafcfEXAMPLE,Approvers=arn:aws:iam::123456789012:role/
Administrator,SNSTopicArn=arn:aws:sns:region:123456789012:AutomationApproval"
```

Windows

```
aws ssm start-automation-execution ^
    --document-name "AWS-StartEC2InstanceWithApproval" ^
    --parameters
 "InstanceId=i-02573cafcfEXAMPLE,Approvers=arn:aws:iam::123456789012:role/
Administrator,SNSTopicArn=arn:aws:sns:region:123456789012:AutomationApproval"
```

PowerShell

```
Start-SSMAutomationExecution `
    -DocumentName AWS-StartEC2InstanceWithApproval `
    -Parameters @{
        "InstanceId"="i-02573cafcfEXAMPLE"
        "Approvers"="arn:aws:iam::123456789012:role/Administrator"
        "SNSTopicArn"="arn:aws:sns:region:123456789012:AutomationApproval"
    }
```

システムが以下のような情報を返します。

Linux & macOS

```
{
    "AutomationExecutionId": "df325c6d-b1b1-4aa0-8003-6cb7338213c6"
}
```

Windows

```
{
    "AutomationExecutionId": "df325c6d-b1b1-4aa0-8003-6cb7338213c6"
}
```

PowerShell

```
df325c6d-b1b1-4aa0-8003-6cb7338213c6
```

オートメーションを承認するには

- オートメーションを承認するには、次のコマンドを実行します。各##############をユーザー自身の情報に置き換えます。

  Linux & macOS

  ```
  aws ssm send-automation-signal \
      --automation-execution-id "df325c6d-b1b1-4aa0-8003-6cb7338213c6" \
      --signal-type "Approve" \
      --payload "Comment=your comments"
  ```

  Windows

  ```
  aws ssm send-automation-signal ^
      --automation-execution-id "df325c6d-b1b1-4aa0-8003-6cb7338213c6" ^
      --signal-type "Approve" ^
      --payload "Comment=your comments"
  ```

  PowerShell

  ```
  Send-SSMAutomationSignal `
      -AutomationExecutionId df325c6d-b1b1-4aa0-8003-6cb7338213c6 `
      -SignalType Approve `
      -Payload @{"Comment"="your comments"}
  ```

  コマンドが成功した場合、出力はありません。

オートメーションを拒否するには

- オートメーションを拒否するには、次のコマンドを実行します。各##############をユーザー自身の情報に置き換えます。

  Linux & macOS

  ```
  aws ssm send-automation-signal \
      --automation-execution-id "df325c6d-b1b1-4aa0-8003-6cb7338213c6" \
      --signal-type "Deny" \
      --payload "Comment=your comments"
  ```

Windows

```
aws ssm send-automation-signal ^
    --automation-execution-id "df325c6d-b1b1-4aa0-8003-6cb7338213c6" ^
    --signal-type "Deny" ^
    --payload "Comment=your comments"
```

PowerShell

```
Send-SSMAutomationSignal `
    -AutomationExecutionId df325c6d-b1b1-4aa0-8003-6cb7338213c6 `
    -SignalType Deny `
    -Payload @{"Comment"="your comments"}
```

コマンドが成功した場合、出力はありません。

自動オペレーションを大規模に実行する

AWS Systems Manager オートメーションを使用すると、ターゲットを使用して AWS リソースのフリートで自動化処理を実行できます。さらに、同時実行値とエラーのしきい値を指定することで、フリート全体のオートメーションのデプロイを制御することができます。同時実行数とエラーのしきい値機能は、まとめてレート制御と呼ばれます。同時実行値は、オートメーションを同時に実行できるリソースの数を決定します。オートメーションには、オプトインできる適応同時実行モードも用意されています。適応同時実行では、同時実行される自動化処理数のクオータが、100 個から最大 500 個まで自動的にスケーリングされます。エラーのしきい値は、Systems Manager がオートメーションの他のリソースへの送信を停止するまでの、オートメーションの失敗の許容量を決定します。

同時実行とエラーしきい値の詳細については、「オートメーションを大規模に制御する」を参照してください。ターゲットの詳細については、「オートメーションのターゲットのマッピング」を参照してください。

以下の手順で、Systems Manager コンソールおよび AWS Command Line Interface (AWS CLI) を使用して、適応同時実行を有効化する方法、ならびに、ターゲットおよびレート制御を使用したオートメーションの実行方法について説明します。

ターゲットとレート制御を使用してオートメーションを実行する (コンソール)

次の手順では、Systems Manager コンソールを使用してターゲットおよびレート制御により、シンプルなオートメーションを実行する方法を説明します。

ターゲットとレート制御を使用してオートメーションを実行するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[オートメーション]、[オートメーションの実行] の順に選択します。
3. [Automation document (自動化ドキュメント)] リストで、ランブックを選択します。[Document categories (ドキュメントカテゴリ)] ペインで 1 つ以上のオプションを選択して、目的に応じて SSM ドキュメントをフィルタリングします。自分が所有するランブックを表示するには、[Owned by me (自分が所有)] タブを選択します。自分のアカウントと共有されているランブックを表示するには、[Shared with me (共有ファイル)] タブを選択します。すべてのランブックを表示するには、[すべてのドキュメント] タブを選択します。

   > **Note**
   >
   > ランブックの名前を選択すると、ランブックに関する情報を表示できます。

4. [Document details (ドキュメントの詳細)] セクションで、[Document version (ドキュメントのバージョン)] が実行するバージョンに設定されていることを確認します。システムには、次のバージョンのオプションが含まれています。

   - [ランタイムのデフォルトバージョン]: 自動化ランブックが定期的に更新され、新しいデフォルトバージョンが割り当てられている場合は、このオプションを選択します。
   - [ランタイムの最新バージョン]: 自動化ランブックが定期的に更新され、直前に更新されたバージョンを実行する場合は、このオプションを選択します。
   - [1 (デフォルト)]: ドキュメントの最初のバージョンを実行するには、このオプションを選択します。これはデフォルト設定です。

5. [Next] を選択します。
6. [Execution Mode (実行モード)] セクションで [Rate Control (レート制御)] を選択します。ターゲットとレート制御を使用する場合は、このモードまたは [Multi-account and Region (マルチアカウントとリージョン)] を使用する必要があります。
7. [Targets (ターゲット)] セクションで、オートメーションを実行する AWS リソースをどのようにターゲットにするかを選択します。これらのオプションは必須です。

a. [Parameter (パラメータ)] リストを使用してパラメータを選択します。[Parameter (パラメータ)] リストの項目は、この手順の開始時に選択した自動化ドキュメントのランブックによって決まります。パラメータを選択して、自動化ワークフローが実行されるリソースの種類を定義します。

b. [Targets (ターゲット)] リストを使用して、リソースをターゲットにする方法を選択します。

   i. パラメータ値を使用してターゲットリソースを選択した場合は、[Input parameters (パラメータの入力)] セクションで選択したパラメータのパラメータ値を入力します。

   ii. AWS Resource Groups を使用してターゲットリソースを選択した場合、[Resource Group (リソースグループ)] リストからグループの名前を選択します。

   iii. タグを使用してターゲットリソースを選択した場合は、タグキーと (オプションとして) タグ値をフィールドに入力します。[Add] (追加) をクリックします。

   iv. 現在の AWS アカウント および AWS リージョン にあるすべてのインスタンスでオートメーションランブックを実行する場合、[All instances (すべてのインスタンス)] を選択します。

8. [Input parameters (入力パラメータ)] セクションで、必要な入力を指定します。必要に応じて、[AutomationAssumeRole] リストから IAM サービスロールを選択できます。

> **Note**
>
> [Input parameters (入力パラメータ)] セクションでオプションを選択する必要はありません。これは、タグまたはリソースグループを使用してリソースをターゲットとしたためです。例えば、`AWS-RestartEC2Instance` ランブックを選択した場合、[Input parameters (入力パラメータ)] セクションでインスタンス ID を指定または選択する必要はありません。オートメーションの実行では、指定したタグまたはリソースグループを使用してインスタンスを再起動します。

9. [Rate control (レート制御)] セクションのオプションを使用して、各アカウントとリージョンのペア内でオートメーションを実行できる AWS リソースの数を制限します。

   [Concurrency (同時実行数)] セクションでオプションを選択します。

   - [targets (ターゲット)] を選択して、自動化ワークフローを同時に実行できるターゲットの絶対数を入力します。

- [percentage (パーセント値)] を選択して、自動化ワークフローを同時に実行できるターゲットセットのパーセント値を入力します。

10. [Error threshold (エラーのしきい値)] セクションでオプションを選択します。

    - [errors (エラー)] を選択して、自動化が他のリソースへのワークフローの送信を停止するまでに許容されるエラーの絶対数を入力します。
    - [percentage (パーセント値)] を選択して、自動化が他のリソースへのワークフローの送信を停止するまでに許容されるエラーのパーセント値を入力します。

11. (オプション) モニタリング用のオートメーションに適用する CloudWatch アラームを選択します。CloudWatch アラームをオートメーションにアタッチするには、コマンドを実行する IAM プリンシパルに `iam:createServiceLinkedRole` アクションの権限が必要です。CloudWatch アラームの詳細については、「Amazon CloudWatch でのアラームの使用」を参照してください。アラームが作動すると、オートメーションは停止されます。AWS CloudTrail を使用する場合、トレイルに API コールが表示されます。

12. [Execute] を選択します。

レート制御のオートメーションによって開始されたオートメーションを表示するには、ナビゲーションペインで [オートメーション] を選択し、[Show child automations (子オートメーションを表示)] を選択します。

ターゲットとレート制御を使用してオートメーションを実行する (コマンドライン)

次の手順では、AWS CLI (Linux または Windows) または AWS Tools for PowerShell を使用して、ターゲットとレート制御でオートメーションを実行する方法を説明します。

ターゲットとレート制御を使用してオートメーションを実行するには

1. まだ AWS CLI または AWS Tools for PowerShell をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」および「AWS Tools for PowerShell のインストール」を参照してください。

2. ドキュメントのリストを表示するには、次のコマンドを実行します。

   Linux & macOS

   ```
   aws ssm list-documents
   ```

Windows

```
aws ssm list-documents
```

PowerShell

```
Get-SSMDocumentList
```

使用するランブックの名前を書き留めます。

3. 以下のコマンドを実行して、ランブックの詳細を表示します。詳細を表示するランブックの*[runbook name]* (ランブック名) を置き換えます。さらに、--target-parameter-name オプションに使用するパラメータ名 (例: InstanceId) を書き留めます。このパラメータは、オートメーションが実行されるリソースのタイプを決定します。

   Linux & macOS

   ```
   aws ssm describe-document \
       --name runbook name
   ```

   Windows

   ```
   aws ssm describe-document ^
       --name runbook name
   ```

   PowerShell

   ```
   Get-SSMDocumentDescription `
       -Name runbook name
   ```

4. 実行するターゲットとレート制御オプションを使用するコマンドを作成します。各##########をユーザー自身の情報に置き換えます。

   タグを使用したターゲット設定

   Linux & macOS

   ```
   aws ssm start-automation-execution \
       --document-name runbook name \
   ```

```
    --targets Key=tag:key name,Values=value \
    --target-parameter-name parameter name \
    --parameters "input parameter name=input parameter value,input parameter 2
 name=input parameter 2 value" \
    --max-concurrency 10 \
    --max-errors 25%
```

Windows

```
aws ssm start-automation-execution ^
    --document-name runbook name ^
    --targets Key=tag:key name,Values=value ^
    --target-parameter-name parameter name ^
    --parameters "input parameter name=input parameter value,input parameter 2
 name=input parameter 2 value" ^
    --max-concurrency 10 ^
    --max-errors 25%
```

PowerShell

```
$Targets = New-Object Amazon.SimpleSystemsManagement.Model.Target
$Targets.Key = "tag:key name"
$Targets.Values = "value"

Start-SSMAutomationExecution `
    DocumentName "runbook name" `
    -Targets $Targets `
    -TargetParameterName "parameter name" `
    -Parameter @{"input parameter name"="input parameter value";"input parameter
 2 name"="input parameter 2 value"} `
    -MaxConcurrency "10" `
    -MaxError "25%"
```

パラメータ値を使用したターゲット設定

Linux & macOS

```
aws ssm start-automation-execution \
    --document-name runbook name \
    --targets Key=ParameterValues,Values=value,value 2,value 3 \
    --target-parameter-name parameter name \
```

```
    --parameters "input parameter name=input parameter value" \
    --max-concurrency 10 \
    --max-errors 25%
```

Windows

```
aws ssm start-automation-execution ^
    --document-name runbook name ^
    --targets Key=ParameterValues,Values=value,value 2,value 3 ^
    --target-parameter-name parameter name ^
    --parameters "input parameter name=input parameter value" ^
    --max-concurrency 10 ^
    --max-errors 25%
```

PowerShell

```
$Targets = New-Object Amazon.SimpleSystemsManagement.Model.Target
$Targets.Key = "ParameterValues"
$Targets.Values = "value","value 2","value 3"

Start-SSMAutomationExecution `
    -DocumentName "runbook name" `
    -Targets $Targets `
    -TargetParameterName "parameter name" `
    -Parameter @{"input parameter name"="input parameter value"} `
    -MaxConcurrency "10" `
    -MaxError "25%"
```

AWS Resource Groups を使用したターゲット設定

Linux & macOS

```
aws ssm start-automation-execution \
    --document-name runbook name \
    --targets Key=ResourceGroup,Values=Resource group nname \
    --target-parameter-name parameter name \
    --parameters "input parameter name=input parameter value" \
    --max-concurrency 10 \
    --max-errors 25%
```

Windows

```
aws ssm start-automation-execution ^
    --document-name runbook name ^
    --targets Key=ResourceGroup,Values=Resource group name ^
    --target-parameter-name parameter name ^
    --parameters "input parameter name=input parameter value" ^
    --max-concurrency 10 ^
    --max-errors 25%
```

PowerShell

```
$Targets = New-Object Amazon.SimpleSystemsManagement.Model.Target
$Targets.Key = "ResourceGroup"
$Targets.Values = "Resource group name"

Start-SSMAutomationExecution `
    -DocumentName "runbook name" `
    -Targets $Targets `
    -TargetParameterName "parameter name" `
    -Parameter @{"input parameter name"="input parameter value"} `
    -MaxConcurrency "10" `
    -MaxError "25%"
```

現在の AWS アカウント と AWS リージョン で、Amazon EC2 インスタンスをターゲットにする

Linux & macOS

```
aws ssm start-automation-execution \
    --document-name runbook name \
    --targets "Key=AWS::EC2::Instance,Values=*"  \
    --target-parameter-name instanceId \
    --parameters "input parameter name=input parameter value" \
    --max-concurrency 10 \
    --max-errors 25%
```

Windows

```
aws ssm start-automation-execution ^
```

```
    --document-name runbook name ^
    --targets Key=AWS::EC2::Instance,Values=* ^
    --target-parameter-name instanceId ^
    --parameters "input parameter name=input parameter value" ^
    --max-concurrency 10 ^
    --max-errors 25%
```

PowerShell

```
$Targets = New-Object Amazon.SimpleSystemsManagement.Model.Target
$Targets.Key = "AWS::EC2::Instance"
$Targets.Values = "*"

Start-SSMAutomationExecution `
    -DocumentName "runbook name" `
    -Targets $Targets `
    -TargetParameterName "instanceId" `
    -Parameter @{"input parameter name"="input parameter value"} `
    -MaxConcurrency "10" `
    -MaxError "25%"
```

コマンドによって実行 ID が返されます。この ID をクリップボードにコピーします。この ID を使用して、オートメーションの状態を表示できます。

Linux & macOS

```
{
    "AutomationExecutionId": "a4a3c0e9-7efd-462a-8594-01234EXAMPLE"
}
```

Windows

```
{
    "AutomationExecutionId": "a4a3c0e9-7efd-462a-8594-01234EXAMPLE"
}
```

PowerShell

```
a4a3c0e9-7efd-462a-8594-01234EXAMPLE
```

5. 以下のコマンドを実行して、オートメーションを表示します。各*########## ID* をユーザー自身の情報に置き換えます。

   Linux & macOS

   ```
   aws ssm describe-automation-executions \
       --filter Key=ExecutionId,Values=automation execution ID
   ```

   Windows

   ```
   aws ssm describe-automation-executions ^
       --filter Key=ExecutionId,Values=automation execution ID
   ```

   PowerShell

   ```
   Get-SSMAutomationExecutionList | `
       Where {$_.AutomationExecutionId -eq "automation execution ID"}
   ```

6. オートメーションの進捗の詳細を表示するには、以下のコマンドを実行します。各*########## ID* をユーザー自身の情報に置き換えます。

   Linux & macOS

   ```
   aws ssm get-automation-execution \
       --automation-execution-id automation execution ID
   ```

   Windows

   ```
   aws ssm get-automation-execution ^
       --automation-execution-id automation execution ID
   ```

   PowerShell

   ```
   Get-SSMAutomationExecution `
       -AutomationExecutionId automation execution ID
   ```

   システムが以下のような情報を返します。

Linux & macOS


```
{
    "AutomationExecution": {
        "StepExecutionsTruncated": false,
        "AutomationExecutionStatus": "Success",
        "MaxConcurrency": "1",
        "Parameters": {},
        "MaxErrors": "1",
        "Outputs": {},
        "DocumentName": "AWS-StopEC2Instance",
        "AutomationExecutionId": "a4a3c0e9-7efd-462a-8594-01234EXAMPLE",
        "ResolvedTargets": {
            "ParameterValues": [
                "i-02573cafcfEXAMPLE"
            ],
            "Truncated": false
        },
        "ExecutionEndTime": 1564681619.915,
        "Targets": [
            {
                "Values": [
                    "DEV"
                ],
                "Key": "tag:ENV"
            }
        ],
        "DocumentVersion": "1",
        "ExecutionStartTime": 1564681576.09,
        "ExecutedBy": "arn:aws:sts::123456789012:assumed-role/Administrator/
Admin",
        "StepExecutions": [
            {
                "Inputs": {
                    "InstanceId": "i-02573cafcfEXAMPLE"
                },
                "Outputs": {},
                "StepName": "i-02573cafcfEXAMPLE",
                "ExecutionEndTime": 1564681619.093,
                "StepExecutionId": "86c7b811-3896-4b78-b897-01234EXAMPLE",
                "ExecutionStartTime": 1564681576.836,
                "Action": "aws:executeAutomation",
                "StepStatus": "Success"
```

```
            }
        ],
        "TargetParameterName": "InstanceId",
        "Mode": "Auto"
    }
}
```

Windows

```
{
    "AutomationExecution": {
        "StepExecutionsTruncated": false,
        "AutomationExecutionStatus": "Success",
        "MaxConcurrency": "1",
        "Parameters": {},
        "MaxErrors": "1",
        "Outputs": {},
        "DocumentName": "AWS-StopEC2Instance",
        "AutomationExecutionId": "a4a3c0e9-7efd-462a-8594-01234EXAMPLE",
        "ResolvedTargets": {
            "ParameterValues": [
                "i-02573cafcfEXAMPLE"
            ],
            "Truncated": false
        },
        "ExecutionEndTime": 1564681619.915,
        "Targets": [
            {
                "Values": [
                    "DEV"
                ],
                "Key": "tag:ENV"
            }
        ],
        "DocumentVersion": "1",
        "ExecutionStartTime": 1564681576.09,
        "ExecutedBy": "arn:aws:sts::123456789012:assumed-role/Administrator/
Admin",
        "StepExecutions": [
            {
                "Inputs": {
                    "InstanceId": "i-02573cafcfEXAMPLE"
                },
```

```
                "Outputs": {},
                "StepName": "i-02573cafcfEXAMPLE",
                "ExecutionEndTime": 1564681619.093,
                "StepExecutionId": "86c7b811-3896-4b78-b897-01234EXAMPLE",
                "ExecutionStartTime": 1564681576.836,
                "Action": "aws:executeAutomation",
                "StepStatus": "Success"
            }
        ],
        "TargetParameterName": "InstanceId",
        "Mode": "Auto"
    }
}
```

PowerShell

```
AutomationExecutionId       : a4a3c0e9-7efd-462a-8594-01234EXAMPLE
AutomationExecutionStatus   : Success
CurrentAction               :
CurrentStepName             :
DocumentName                : AWS-StopEC2Instance
DocumentVersion             : 1
ExecutedBy                  : arn:aws:sts::123456789012:assumed-role/
Administrator/Admin
ExecutionEndTime            : 8/1/2019 5:46:59 PM
ExecutionStartTime          : 8/1/2019 5:46:16 PM
FailureMessage              :
MaxConcurrency              : 1
MaxErrors                   : 1
Mode                        : Auto
Outputs                     : {}
Parameters                  : {}
ParentAutomationExecutionId :
ProgressCounters            :
ResolvedTargets             :
 Amazon.SimpleSystemsManagement.Model.ResolvedTargets
StepExecutions              : {i-02573cafcfEXAMPLE}
StepExecutionsTruncated     : False
Target                      :
TargetLocations             : {}
TargetMaps                  : {}
TargetParameterName         : InstanceId
Targets                     : {tag:Name}
```

> **Note**
>
> コンソールで、オートメーションのステータスをモニタリングすることもできます。[Automation executions (オートメーション実行)] リストで、先ほど開始した実行を選択し、[Execution steps (実行ステップ)] タブを選択します。このタブには、オートメーションアクションのステータスが表示されます。

オートメーションのターゲットのマッピング

`Targets` パラメータを使用すると、オートメーションの対象リソースを素早く定義できます。例えば、マネージドインスタンスを再起動するオートメーションを実行する場合は、コンソールで多数のインスタンス ID を手動で選択したりコマンドで入力したりする代わりに、`Targets` パラメータを使用して Amazon Elastic Compute Cloud (Amazon EC2) タグを指定しインスタンスをターゲティングできます。

ターゲットを使用するオートメーションを実行すると、AWS Systems Manager はターゲットごとに子 Automation を作成します。例えば、タグを指定して Amazon Elastic Block Store (Amazon EBS) ボリュームをターゲットに設定し、それらのタグが 100 の Amazon EBS ボリュームに解決された場合、Systems Manager は 100 の子オートメーションを作成します。親 Automation は、すべての子 Automation が最終状態に達すると完了します。

> **Note**
>
> 実行時に指定する `input parameters` (コンソールの [Input parameters (入力パラメータ)] セクション、またはコマンドラインの `parameters` オプションを使用) は、すべての子 Automation によって自動的に処理されます。

タグ、リソースグループ、およびパラメータ値を使用して、オートメーションのリソースをターゲットにすることができます。さらに、`TargetMaps` オプションを使用すると、コマンドラインまたはファイルから複数のパラメータ値を指定できます。次のセクションでは、これらの各ターゲティングオプションについて詳しく説明します。

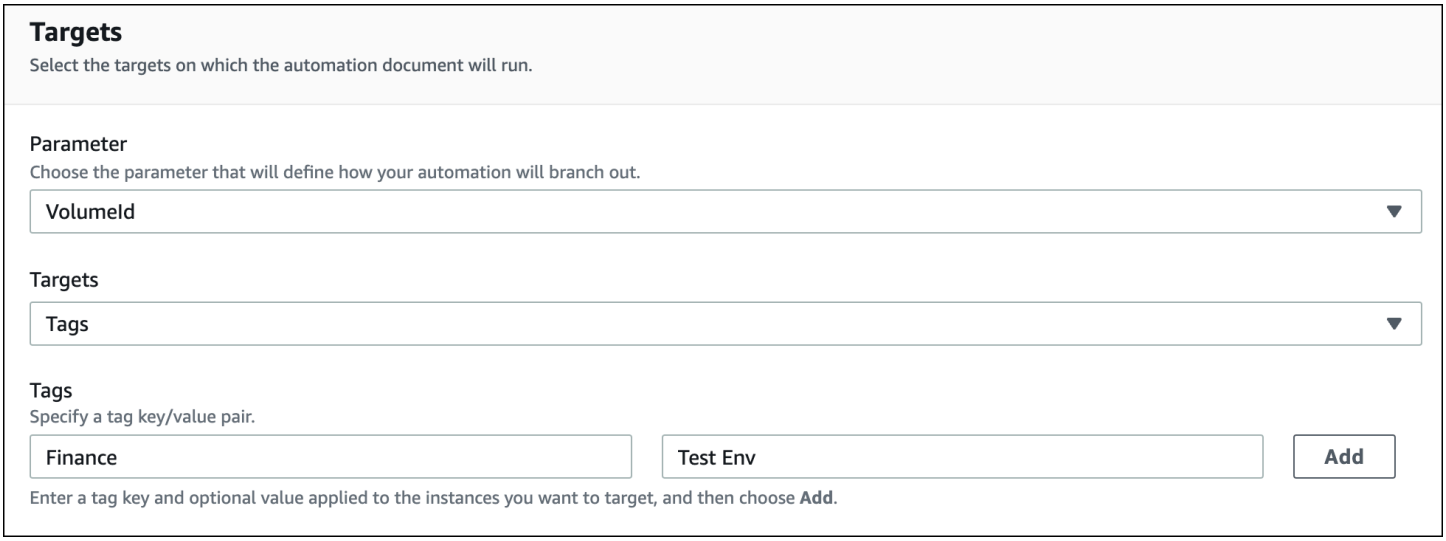
タグをターゲットにする

オートメーションのターゲットとして、1 つのタグを指定できます。Amazon Elastic Compute Cloud (Amazon EC2) および Amazon Relational Database Service (Amazon RDS) インスタンス、Amazon

Elastic Block Store (Amazon EBS) ボリュームとスナップショット、Resource Groups、Amazon Simple Storage Service (Amazon S3) バケットなどの多くの AWS リソースはタグをサポートしています。タグをターゲットにすることにより、AWS リソースに対するオートメーションをすばやく実行できます。タグは、Operating_System:Linux や Department:Finance などのキーと値のペアです。特定の名前をリソースに割り当てる場合は、「名前」という単語をキーとして使用し、リソースの名前を値として使用することもできます。

オートメーションのターゲットとしてタグを指定する場合は、ターゲットパラメータも指定します。ターゲットパラメータは、`TargetParameterName` オプションを使用します。ターゲットパラメータを選択することで、オートメーションが実行されるリソースのタイプを定義します。タグで指定するターゲットパラメータは、ランブックで定義された有効なパラメータでなければなりません。たとえば、タグを使用して多数の EC2 インスタンスをターゲットにする場合は、`InstanceId` ターゲットパラメータを選択します。このパラメータを選択すると、インスタンスがオートメーションのリソースタイプとして定義されます。カスタムランブックを作成するときは、[ターゲットタイプ]を `/AWS::EC2::Instance` に指定して、インスタンスのみが使用されるようにする必要があります。そうしなければ、同じタグを持つすべてのリソースがターゲットになります。タグ付きのインスタンスをターゲットにする際に、終了したインスタンスが含まれる場合があります。

次のスクリーンショットでは、`AWS-DetachEBSVolume` ランブックを使用しています。論理ターゲットパラメータは `VolumeId` です。



`AWS-DetachEBSVolume` ランブックには、`/AWS::EC2::Volume` に設定された [Target type (ターゲットの種類)] という特別なプロパティも含まれています。これは、タグキーペア `Finance:TestEnv` が異なるタイプのリソース (EC2 インスタンス、Amazon EBS ボリューム、Amazon EBS スナップショットなど) を返す場合、Amazon EBS ボリュームのみが使用されることを意味します。

Important

ターゲットのパラメータ名では大文字と小文字が区別されます。AWS Command Line Interface (AWS CLI) または AWS Tools for Windows PowerShell を使用してオートメーションを実行する場合は、ランブックで定義されているとおり、ターゲットパラメータ名を正確に入力する必要があります。指定しないと、システムは `InvalidAutomationExecutionParametersException` エラーを返します。DescribeDocument API オペレーションを使用すると、特定のランブックで使用可能なターゲットパラメータに関する情報を表示できます。次に、`AWS-DeleteSnapshot` ドキュメントに関する情報を提供する AWS CLI コマンドの例を示します。

```
aws ssm describe-document \
    --name AWS-DeleteSnapshot
```

さらに、タグを使用してリソースをターゲットにする AWS CLI コマンドの例を示します。

例 1: Amazon EC2 インスタンスを再起動するために、キーと値のペアを使用してタグをターゲットにする

この例では、Department のキーと HumanResources の値でタグ付けされたすべての Amazon EC2 インスタンスを再起動します。ターゲットパラメータは、ランブックの InstanceId パラメータを使用します。この例では、Automation サービスロール (引き受けロール) を使用して、自動化を実行するための追加のパラメータを使用しています。

```
aws ssm start-automation-execution \
    --document-name AWS-RestartEC2Instance \
    --targets Key=tag:Department,Values=HumanResources \
    --target-parameter-name InstanceId \
    --parameters "AutomationAssumeRole=arn:aws:iam::111122223333:role/
AutomationServiceRole"
```

例 2: Amazon EBS スナップショットを削除するために、キーと値のペアを使用してタグをターゲットにする

以下の例では、`AWS-DeleteSnapshot` ランブックを使用して、Name キーと、January2018Backups 値のすべてのスナップショットを削除します。ターゲットのパラメータは、VolumeId パラメータを使用します。

```
aws ssm start-automation-execution \
    --document-name AWS-DeleteSnapshot \
    --targets Key=tag:Name,Values=January2018Backups \
    --target-parameter-name VolumeId
```

AWS Resource Groups をターゲットにする

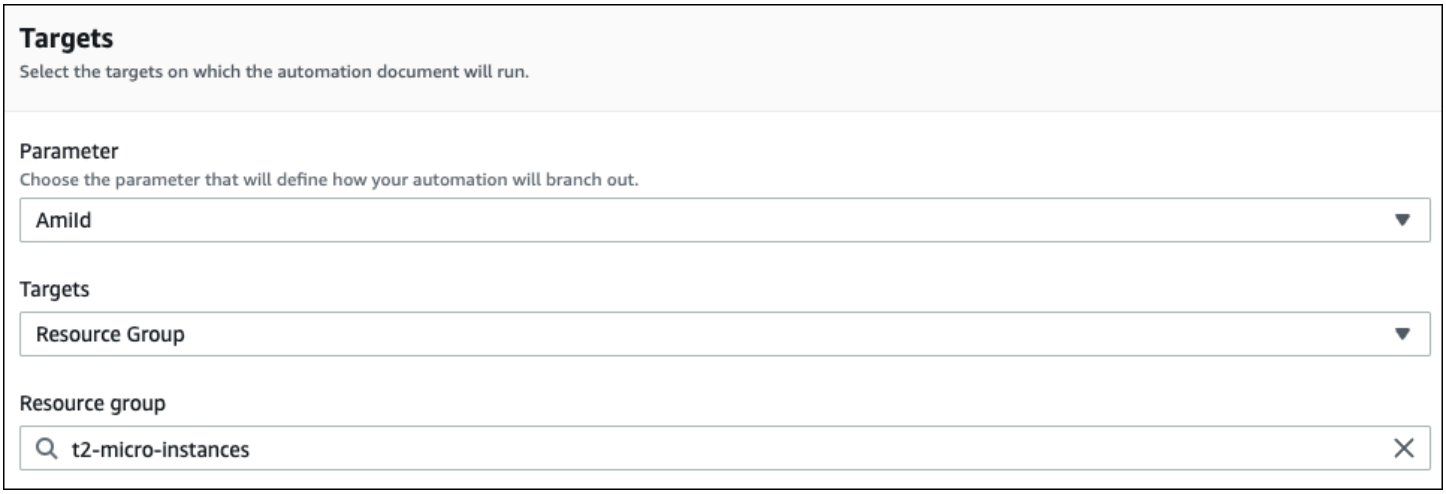
オートメーションのターゲットとして、1 つの AWS リソースグループを指定できます。Systems Manager は、ターゲットリソースグループ内のすべてのオブジェクトに対して子オートメーションを作成します。

たとえば、リソースグループの 1 つに PatchedAMI という名前が付けられているとします。この Resource Group には、定期的にパッチ適用される 25 個の Windows Amazon Machine Images (AMIs) のリストが含まれています。`AWS-CreateManagedWindowsInstance` ランブックを使用し、この Resource Group をターゲットとするオートメーションを実行すると、Systems Manager は 25 個の AMIs ごとに子オートメーションを作成します。つまり、PatchedAMIs Resource Group をターゲットとすることで、オートメーションはパッチを適用した AMIs のリストから 25 個のインスタンスを作成します。親オートメーションは、すべての子オートメーションが処理を完了するか、最終状態に達すると完了します。

次の AWS CLI コマンドは、PatchAMI リソースグループの例に適用されます。このコマンドは、`--target-parameter-name` オプションの AmiId パラメータを受け取ります。このコマンドには、各 AMI から作成するインスタンスのタイプを定義する追加のパラメータは含まれていません。`AWS-CreateManagedWindowsInstance` ランブックはデフォルトで t2.medium インスタンスタイプになっているため、このコマンドは Windows Server に 25 個の t2.medium Amazon EC2 インスタンスを作成します。

```
aws ssm start-automation-execution \
    --document-name AWS-CreateManagedWindowsInstance \
    --targets Key=ResourceGroup,Values=PatchedAMIs  \
    --target-parameter-name AmiId
```

次のコンソールの例では、t2-micro-instances というリソースグループを使用しています。



パラメータ値のターゲット設定

パラメータ値をターゲットにすることもできます。ParameterValues をキーとして入力し、オートメーションを実行する特定のリソース値を入力します。複数の値を指定すると、Systems Manager は指定された各値に対して子オートメーションを実行します。

たとえば、ランブックに instanceID パラメーターが含まれているとします。オートメーションを実行するときに [InstanceID] パラメータの値を指定すると、Systems Manager は指定された各インスタンス ID 値に対して子オートメーションを実行します。オートメーションが指定された各インスタンスの実行を終了するか、オートメーションが失敗した場合、親オートメーションは完了します。最大 50 個のパラメータ値を対象にすることができます。

次の例では、AWS-CreateImage ランブックを使用します 指定されたターゲットパラメータ名は InstanceId です。キーは ParameterValues を使用します。値は 2 つの Amazon EC2 インスタンス ID です。このコマンドは、インスタンスごとにオートメーションを作成し、各インスタンスから AMI を生成します。

```
aws ssm start-automation-execution
    --document-name AWS-CreateImage \
    --target-parameter-name InstanceId \
    --targets Key=ParameterValues,Values=i-02573cafcfEXAMPLE,i-0471e04240EXAMPLE
```

> **Note**
>
> AutomationAssumeRole は有効なパラメータではありません。パラメータ値をターゲットにするオートメーションを実行するときは、この項目を選択しないでください。

パラメータ値マップをターゲットにする

TargetMaps オプションは、ParameterValues をターゲットにする機能を拡張します。コマンドラインで TargetMaps を使用すると、パラメータ値の配列を入力できます。コマンドラインでは、最大 50 のパラメータ値を指定できます。50 を超えるパラメータ値を指定するコマンドを実行する場合は、値を JSON ファイルに入力できます。その後、コマンドラインからファイルを呼び出すことができます。

> **Note**
>
> コンソールでは、TargetMaps オプションはサポートされていません。

コマンドで TargetMaps オプションを使用して複数のパラメータ値を指定するには、次の形式を使用します。各*###############*をユーザー自身の情報に置き換えます。

```
aws ssm start-automation-execution \
    --document-name runbook name \
    --target-maps “parameter=value, parameter 2=value, parameter 3=value”  “parameter
 4=value, parameter 5=value, parameter 6=value”
```

TargetMaps オプションに 50 以上のパラメータ値を入力する場合は、次の JSON 形式を使用してファイル内の値を指定します。JSON ファイルを使用すると、複数のパラメータ値を提供する際の読みやすさも向上します。

```
[

    {“parameter”: "value", “parameter 2”: "value", “parameter 3”: "value"},

    {“parameter 4”: "value", “parameter 5”: "value", "parameter 6": "value"}

]
```

.json ファイル拡張子でこのファイルを保存します。次のコマンドを使用してファイルを呼び出すことができます。各*###############*をユーザー自身の情報に置き換えます。

```
aws ssm start-automation-execution \
    --document-name runbook name \
    --parameters input parameters \
```

```
    --target-maps path to file/file name.json
```

またはバケットからデータを読み取るアクセス権限を持っている限り、Amazon Simple Storage Service (Amazon S3) バケットからファイルをダウンロードすることもできます。次のコマンド形式を使用します。各##############をユーザー自身の情報に置き換えます。

```
aws ssm start-automation-execution \
    --document-name runbook name \
    --target-maps http://amzn-s3-demo-bucket.s3.amazonaws.com/file_name.json
```

以下は、TargetMaps オプションを理解するのに役立つシナリオの例です。このシナリオでは、ユーザーは異なる AMIs から異なるタイプの Amazon EC2 インスタンスを作成する必要があります。このタスクを実行するには、AMI_Testing という名前のランブックを作成します。このランブックでは、instanceType と imageId の 2 つの入力パラメータを定義しています。

```
{
  "description": "AMI Testing",
  "schemaVersion": "0.3",
  "assumeRole": "{{assumeRole}}",
  "parameters": {
    "assumeRole": {
      "type": "String",
      "description": "Role under which to run the automation",
      "default": ""
    },
    "instanceType": {
      "type": "String",
      "description": "Type of EC2 Instance to launch for this test"
    },
    "imageId": {
      "type": "String",
      "description": "Source AMI id from which to run instance"
    }
  },
  "mainSteps": [
    {
      "name": "runInstances",
      "action": "aws:runInstances",
      "maxAttempts": 1,
      "onFailure": "Abort",
      "inputs": {
        "ImageId": "{{imageId}}",
```

```
        "InstanceType": "{{instanceType}}",
        "MinInstanceCount": 1,
        "MaxInstanceCount": 1
      }
    }
  ],
  "outputs": [
    "runInstances.InstanceIds"
  ]
}
```

次に、ユーザーは AMI_instance_types.json という名前のファイルで次のターゲットパラメータ値を指定します。

```
[
  {
    "instanceType" : ["t2.micro"],
    "imageId" : ["ami-b70554c8"]
  },
  {
    "instanceType" : ["t2.small"],
    "imageId" : ["ami-b70554c8"]
  },
  {
    "instanceType" : ["t2.medium"],
    "imageId" : ["ami-cfe4b2b0"]
  },
  {
    "instanceType" : ["t2.medium"],
    "imageId" : ["ami-cfe4b2b0"]
  },
  {
    "instanceType" : ["t2.medium"],
    "imageId" : ["ami-cfe4b2b0"]
  }
]
```

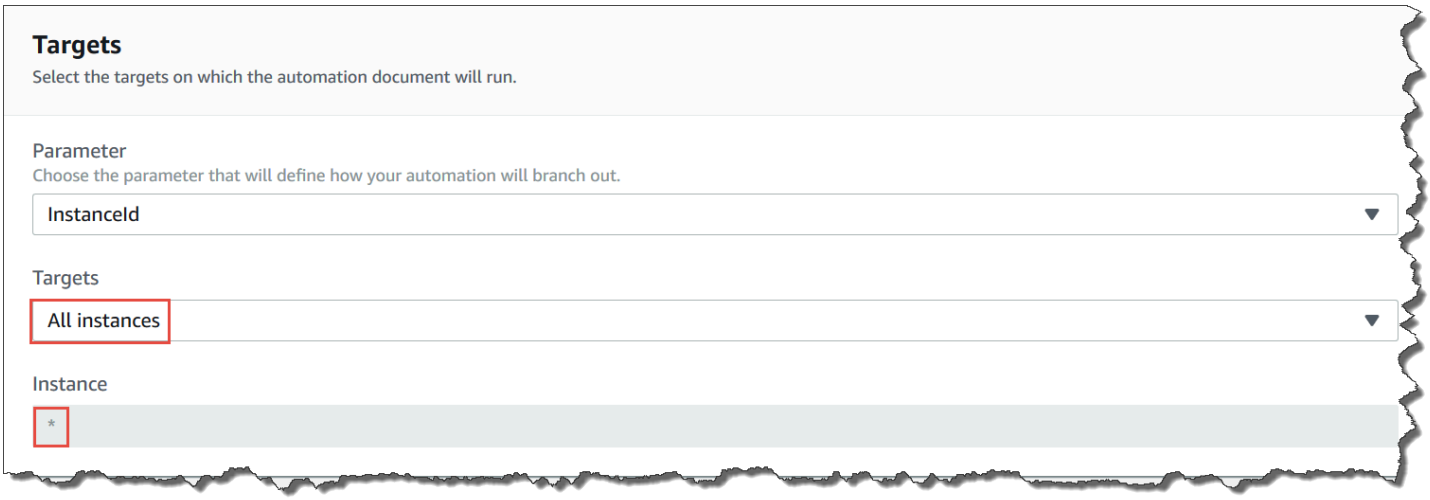
ユーザーはオートメーションを実行し、次のコマンドを実行して AMI_instance_types.json で定義された 5 つの EC2 インスタンスを作成できます。

```
aws ssm start-automation-execution \
    --document-name AMI_Testing \
```

```
    --target-parameter-name imageId \
    --target-maps file:///home/TestUser/workspace/runinstances/AMI_instance_types.json
```

すべての Amazon EC2 インスタンスをターゲットにする

[ターゲット] リストで [すべてのインスタンス] をクリックすることにより、現在の AWS アカウントと AWS リージョン のすべての Amazon EC2 インスタンスで自動化を実行できます。例えば、AWS アカウント と現在の AWS リージョン にあるすべての Amazon EC2 インスタンスを再起動する場合は、**AWS-RestartEC2Instance** ランブックを選択した上で、[ターゲット] のリストから [すべてのインスタンス] を選択します。



[すべてのインスタンス] を選択すると、[インスタンス] フィールドにアスタリスク (*) が入力され、フィールドを変更できなくなります (フィールドはグレー表示されます)。また、Systems Manager では、[入力パラメータ] フィールドの [InstanceId] フィールドを変更できなくなります。すべてのインスタンスをターゲットにするよう選択する場合、これらのフィールドが変更できなくなることは想定される動作となります。

オートメーションを大規模に制御する

同時実行値とエラーのしきい値を指定することで、AWS リソースのフリート全体でオートメーションのデプロイを制御できます。同時実行数とエラーのしきい値は、まとめてレート制御と呼ばれます。

同時実行

Concurrency (同時実行) を使用すると、オートメーションを同時に実行できるリソースの数を指定できます。同時実行数は、オートメーションを処理する際のリソースへの影響やダウンタイムを制限するのに役立ちます。リソースの絶対数 (20 など) またはターゲットセットのパーセント数 (10% など) を指定できます。

キューシステムにより、オートメーションは 1 つのリソースに送信され、この最初の呼び出しが完了するのを待ってから、さらに 2 つのリソースにオートメーションが送信されます。同時実行値の値に達するまで、システムはオートメーションをより多くのリソースに指数関数的に送信します。

エラーしきい値

エラーしきい値を使用すると、AWS Systems Manager が他のリソースへオートメーションの送信を停止するまでの、オートメーションの失敗の許容量を決定できます。エラーの絶対数 (10 など) またはターゲットセットのパーセント数 (10% など) を指定できます。

たとえば、エラーの絶対数として 3 を指定すると、4 番目のエラーを受信した際に、システムはオートメーションの実行を停止します。値として 0 を指定した場合、最初のエラー結果が返されると、システムから他のターゲットでオートメーションが実行されなくなります。

たとえば、50 のインスタンスにオートメーションを送信し、エラーしきい値を 10% に設定した場合、5 番目のエラーが受信されると、システムから他のインスタンスにコマンドが送信されなくなります。エラーのしきい値に達したときに既にオートメーションを実行中の呼び出しについては、完了を許可されますが、これらのオートメーションも失敗する可能性があります。エラーのしきい値に指定された数より多くのエラーが発生しないようにする必要がある場合は、[Concurrency (同時実行数)] 値を 1 に設定して、オートメーションを 1 つずつ進めるようにします。

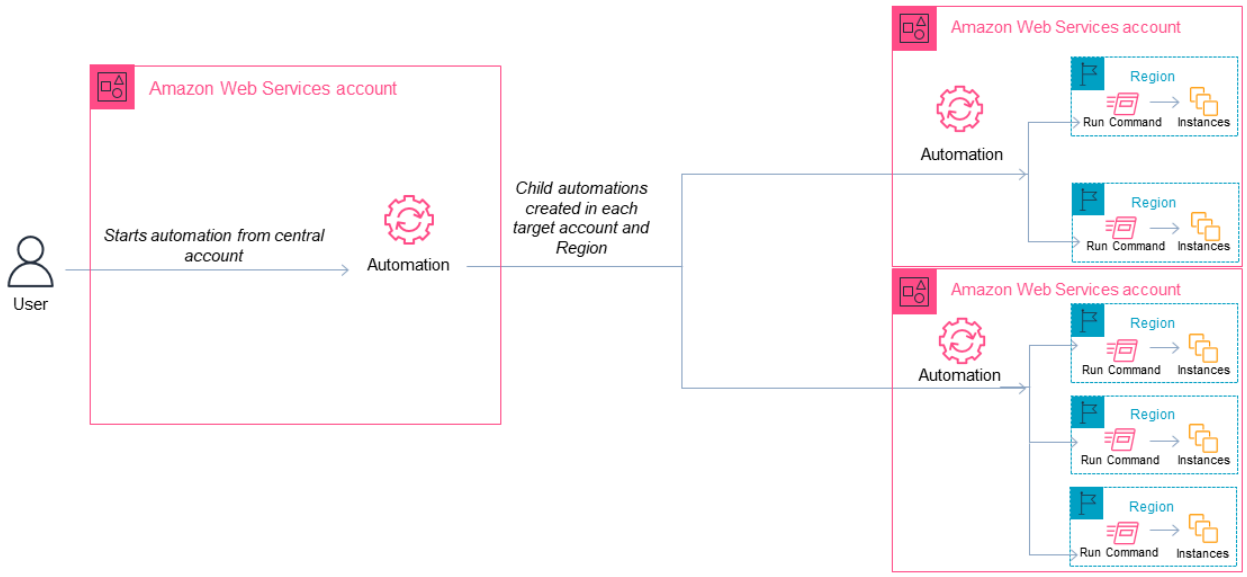
複数の AWS リージョン とアカウントでのオートメーションの実行

中央アカウントから、複数の AWS リージョン および AWS アカウント または AWS Organizations 組織単位 (OU) で AWS Systems Manager オートメーションを実行することができます。Automation は AWS Systems Manager のツールです。複数のリージョンやアカウント、または OU でオートメーションを実行すると、AWS リソースの管理に必要な時間が短縮され、コンピューティング環境のセキュリティが強化されます。

例えば、オートメーションランブックを使用して次を実行できます。

- パッチ適用とセキュリティ更新を一元的に実装します。
- VPC 設定や Amazon S3 バケットポリシーでコンプライアンスの問題を修正します。
- Amazon Elastic Compute Cloud (Amazon EC2) EC2 インスタンスなどのリソースを、大規模に管理します。

次の図は、中央アカウントから、複数のリージョンおよびアカウントで `AWS-RestartEC2Instances` ランブックを実行しているユーザーの例を示しています。オートメーションは、対象のリージョンおよびアカウントで指定されたタグを使用してインスタンスを検索します。



オートメーション用の中央アカウントを選択する

OU 全体でオートメーションを実行する場合、中央アカウントには OU 内のすべてのアカウントを一覧表示する権限が必要です。これは、委任された管理者アカウントまたは組織の管理アカウントからのみ可能です。AWS Organizations ベストプラクティスに従い、委任された管理者アカウントを使用することをお勧めします。AWS Organizations ベストプラクティスの詳細については、「AWS Organizations ユーザーガイド」の「管理アカウントのベストプラクティス」を参照してください。Systems Manager 用に委任された管理者アカウントを作成するには、次の例のように、`register-delegated-administrator` コマンドと AWS CLI を使用できます。

```
aws organizations register-delegated-administrator \
    --account-id delegated admin account ID \
    --service-principal ssm.amazonaws.com
```

AWS Organizations で管理されていない複数のアカウントでオートメーションを実行したい場合は、オートメーション管理専用のアカウントを作成することをお勧めします。すべてのクロスアカウントオートメーションを専用アカウントから実行すると、IAM 権限管理やトラブルシューティング作業が簡単になり、運用と管理が分離されます。この方法は、AWS Organizations を使用し、OU ではなく個々のアカウントのみを対象とする場合にも推奨されます。

オートメーション実行の仕組み

複数のリージョンとアカウント、または OU でオートメーションを実行すると、次のように動作します。

1. オートメーション中央アカウントとして設定するアカウントにサインインします。
2. このトピックの マルチリージョンおよびマルチアカウントのオートメーションのための管理アカウントアクセス許可の設定 手順を使用して、次の IAM ロールを作成します。
   - **AWS-SystemsManager-AutomationAdministrationRole** - このロールは、複数のアカウントと OU でオートメーションを実行するアクセス許可をユーザーに付与します。
   - **AWS-SystemsManager-AutomationExecutionRole** - このロールは、ターゲットアカウントでオートメーションを実行するアクセス許可をユーザーに付与します。
3. オートメーションを実行するランブック、リージョン、およびアカウント、または OU を選択します。

> **Note**
>
> ターゲット OU に目的のアカウントが含まれていることを確認します。カスタムランブックを選択した場合は、ランブックをすべてのターゲットアカウントと共有する必要があります。ランブック共有の詳細については、「SSM ドキュメントの共有」を参照してください。共有ランブックの使用については、「共有 SSM ドキュメントを使用する」を参照してください。

4. オートメーションを実行します。

> **Note**
>
> 複数のリージョン、アカウント、または OU でオートメーションを実行する場合、プライマリアカウントから実行するオートメーションによって、各ターゲットアカウントの子オートメーションが開始されます。プライマリアカウントのオートメーションには、ターゲットアカウントそれぞれに `aws:executeAutomation` ステップがあります。

5. AWS Systems Manager コンソール、または AWS CLI から GetAutomationExecution、DescribeAutomationStepExecutions、および DescribeAutomationExecutions API オペレーションを使用して、オートメーションの進行状況をモニタリングします。プライマリアカウントのオートメーションのステップの出力は、子オートメーションの `AutomationExecutionId` になります。ターゲットアカウントで作成された子

オートメーションの出力を表示するには、リクエストで適切なアカウント、リージョン、および AutomationExecutionId を指定してください。

マルチリージョンおよびマルチアカウントのオートメーションのための管理アカウントアクセス許可の設定

を使用して、Systems Manager Automation のマルチリージョンおよびマルチアカウントのオートメーションに必要な IAM ロールを作成するには、次の手順に従いますAWS CloudFormation ここでは、**AWS-SystemsManager-AutomationAdministrationRole** ロールの作成方法について説明します。オートメーション中央アカウントでこのロールを作成するだけで済みます。この手順では、**AWS-SystemsManager-AutomationExecutionRole** ロールの作成方法についても説明します。マルチリージョンおよびマルチアカウントのオートメーションを実行するために、ターゲットとするすべてのアカウントでこのロールを作成する必要があります。AWS CloudFormation StackSet を使用して、マルチリージョンおよびマルチアカウントのオートメーションを実行するターゲットとするアカウントに **AWS-SystemsManager-AutomationExecutionRole** ロールを作成することをお勧めします。

AWS CloudFormation を使用してマルチリージョンおよびマルチアカウントのオートメーションに必要な IAM 管理ロールを作成するには

1. AWS-SystemsManager-AutomationAdministrationRole.zip をダウンロードして、解凍します。または、アカウントが AWS Organizations AWS-SystemsManager-AutomationAdministrationRole (org).zip によって管理されている場合は。このファイルには、AWS-SystemsManager-AutomationAdministrationRole.yaml AWS CloudFormation テンプレートファイルが含まれています。
2. https://console.aws.amazon.com/cloudformation で AWS CloudFormation コンソール を開きます。
3. [Create stack] を選択します。
4. [Specify template] (テンプレートの指定) セクションで、[Upload a template] (テンプレートのアップロード)] を選択します。
5. [Choose file] (ファイルを選択) を選択して、AWS-SystemsManager-AutomationAdministrationRole.yaml AWS CloudFormation テンプレートファイルを選択します。
6. [Next] を選択します。
7. [Specify stack details (スタックの詳細の指定)] ページの [Stack Name (スタック名)] フィールドに名前を入力します。

8. [Next] を選択します。
9. [Configure stack options] (スタックオプションの設定) ページで、使用するオプションの値を入力します。[Next] を選択します。
10. [確認] ページをスクロールダウンして、[AWS CloudFormation がカスタム名で IAM リソースを作成する可能性があることを承認します] オプションを選択します。
11. [スタックの作成] を選択してください。

AWS CloudFormation は、[CREATE_IN_PROGRESS] の状態を約 3 分間表示します。状態が [CREATE_COMPLETE] に変わります。

マルチリージョンおよびマルチアカウントのオートメーションを実行するために、ターゲットとするすべてのアカウントで以下の手順を繰り返す必要があります。

AWS CloudFormation を使用してマルチリージョンおよびマルチアカウントのオートメーションに必要な IAM オートメーションロールを作成するには

1. AWS-SystemsManager-AutomationExecutionRole.zipをダウンロードします。または、アカウントが AWS Organizations AWS-SystemsManager-AutomationExecutionRole(org).zip によって管理されている場合は。このファイルには、`AWS-SystemsManager-AutomationExecutionRole.yaml` AWS CloudFormation テンプレートファイルが含まれています。
2. https://console.aws.amazon.com/cloudformation で AWS CloudFormation コンソール を開きます。
3. [Create stack] を選択します。
4. [Specify template] (テンプレートの指定) セクションで、[Upload a template] (テンプレートのアップロード)] を選択します。
5. [Choose file] (ファイルを選択) を選択して、`AWS-SystemsManager-AutomationExecutionRole.yaml` AWS CloudFormation テンプレートファイルを選択します。
6. [Next] を選択します。
7. [Specify stack details (スタックの詳細の指定)] ページの [Stack Name (スタック名)] フィールドに名前を入力します。
8. [Parameters] (パラメータ) セクションの [AdminAccountId] フィールドに、オートメーション中央アカウントの ID を入力します。

9. AWS Organizations 環境でこのロールを設定する場合、[OrganizationID] というセクションには別のフィールドがあります。AWS 組織の ID を入力します。
10. [Next] を選択します。
11. [Configure stack options] (スタックオプションの設定) ページで、使用するオプションの値を入力します。[Next] を選択します。
12. [確認] ページをスクロールダウンして、[AWS CloudFormation がカスタム名で IAM リソースを作成する可能性があることを承認します] オプションを選択します。
13. [スタックの作成] を選択してください。

AWS CloudFormation は、[CREATE_IN_PROGRESS] の状態を約 3 分間表示します。状態が [CREATE_COMPLETE] に変わります。

複数のリージョンとアカウントでのオートメーションを実行する (コンソール)

次の手順では、Systems Manager コンソールを使用して、オートメーション管理アカウントから複数のリージョンおよびアカウントでオートメーションを実行する方法を説明します。

開始する前に

次の手順を完了する前に、次の情報を書き留めます。

- マルチリージョンまたはマルチアカウントのオートメーションの実行に使用するユーザーまたはロールには、`AWS-SystemsManager-AutomationAdministrationRole` ロールの `iam:PassRole` アクセス許可が必要です。
- AWS アカウントオートメーションを実行する ID または OU。
- オートメーションを実行する Systems Manager でサポートされているリージョン。
- オートメーションを実行するタグキーとタグ値、またはリソースグループの名前。

複数のリージョンとアカウントでオートメーションを実行する

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[オートメーション]、[オートメーションの実行] の順に選択します。
3. [Automation document (自動化ドキュメント)] リストで、ランブックを選択します。[Document categories (ドキュメントカテゴリ)] ペインで 1 つ以上のオプションを選択して、目的に応じて SSM ドキュメントをフィルタリングします。自分が所有するランブックを表示するには、[Owned by me (自分が所有)] タブを選択します。自分のアカウントと共有されているランブック

を表示するには、[Shared with me (共有ファイル)] タブを選択します。すべてのランブックを表示するには、[すべてのドキュメント] タブを選択します。

> **Note**
>
> ランブックの名前を選択すると、ランブックに関する情報を表示できます。

4. [Document details (ドキュメントの詳細)] セクションで、[Document version (ドキュメントのバージョン)] が実行するバージョンに設定されていることを確認します。システムには、次のバージョンのオプションが含まれています。

   - [ランタイムのデフォルトバージョン]: 自動化ランブックが定期的に更新され、新しいデフォルトバージョンが割り当てられている場合は、このオプションを選択します。
   - [ランタイムの最新バージョン]: 自動化ランブックが定期的に更新され、直前に更新されたバージョンを実行する場合は、このオプションを選択します。
   - [1 (デフォルト)]: ドキュメントの最初のバージョンを実行するには、このオプションを選択します。これはデフォルト設定です。

5. [Next] を選択します。
6. [Execute automation document (自動化ドキュメントの実行)] ページで、[Multi-account and Region (複数のアカウントとリージョン)] を選択します。
7. [Target accounts and Regions] (ターゲットのアカウントとリージョン) セクションで、[Accounts and organizational (OU)] (アカウントおよび組織 (OU)) フィールドを使用して、オートメーションを実行する別の AWS アカウント または AWS 組織単位 (OU) を指定します。カンマで複数のアカウントまたは OU を区切ります。
8. AWS リージョン リストを使用して、1 つ以上のリージョンを選択してオートメーションを実行します。
9. [Multi-Region and account rate control (複数のリージョンとアカウントのレート制御)] オプションを使用して、オートメーションを、限定された数のリージョンで実行されている限られた数のアカウントに制限します。これらのオプションは、オートメーションの実行が可能な AWS リソースの数を制限するわけではありません。

   a. [Location (account-Region pair) concurrency (場所 (アカウントとリージョンのペア) の同時実行)] セクションで、複数のアカウントとリージョンで同時に実行できるオートメーションの数を制限するオプションを選択します。例えば、4 つの AWS リージョン にある、5 つの AWS アカウント でオートメーションを実行すると、Systems Manager は合計 20 のアカウントとリージョンのペアでオートメーションを実行します。このオプションを使用

して、オートメーションが 2 つのアカウントとリージョンのペアで同時に実行されるように、絶対数 (**2** など) を指定することができます。または、同時に実行できるアカウントとリージョンのペアのパーセント値を指定することもできます。例えば、20 のアカウントとリージョンのペアに 20% と指定すると、オートメーションは同時に最大 5 つのアカウントとリージョンのペアで実行されます。

- [targets (ターゲット)] を選択して、オートメーションを同時に実行できるアカウントとリージョンのペアの絶対数を入力します。
- [percent (パーセント)] を選択して、オートメーションを同時に実行できるアカウントとリージョンのペアの合計数のパーセント値を入力します。

b. [Error threshold (エラーのしきい値)] セクションでオプションを選択します。

- [errors (エラー)] を選択して、オートメーションが他のリソースへのオートメーションの送信を停止するまでに許容されるエラーの絶対数を入力します。
- [percent (パーセント)] を選択して、オートメーションが他のリソースへのオートメーションの送信を停止するまでに許容されるエラーのパーセント値を入力します。

10. [Targets (ターゲット)] セクションで、オートメーションを実行する AWS リソースをどのようにターゲットにするかを選択します。これらのオプションは必須です。

a. [Parameter (パラメータ)] リストを使用してパラメータを選択します。[Parameter (パラメータ)] リストの項目は、この手順の開始時に選択した自動化ドキュメントのランブックによって決まります。パラメータを選択して、自動化ワークフローが実行されるリソースの種類を定義します。

b. [Targets (ターゲット)] リストを使用して、リソースをターゲットにする方法を選択します。

i. パラメータ値を使用してターゲットリソースを選択した場合は、[Input parameters (パラメータの入力)] セクションで選択したパラメータのパラメータ値を入力します。

ii. AWS Resource Groups を使用してターゲットリソースを選択した場合、[Resource Group (リソースグループ)] リストからグループの名前を選択します。

iii. タグを使用してターゲットリソースを選択した場合は、タグキーと (オプションとして) タグ値をフィールドに入力します。[Add] (追加) をクリックします。

iv. 現在の AWS アカウント および AWS リージョン にあるすべてのインスタンスでオートメーションランブックを実行する場合、[All instances (すべてのインスタンス)] を選択します。

11. [Input parameters (入力パラメータ)] セクションで、必要な入力を指定します。AutomationAssumeRole リストから `AWS-SystemsManager-AutomationAdministrationRole` IAM サービスロールを選択します。

    > **Note**
    >
    > [Input parameters (入力パラメータ)] セクションでオプションを選択する必要はありません。これは、タグまたはリソースグループを使用して複数のリージョンおよびアカウントのリソースをターゲットとしたためです。例えば、`AWS-RestartEC2Instance` ランブックを選択した場合、[Input parameters (入力パラメータ)] セクションでインスタンス ID を指定または選択する必要はありません。オートメーションでは、指定したタグを使用してインスタンスを再起動します。

12. (オプション) モニタリング用のオートメーションに適用する CloudWatch アラームを選択します。CloudWatch アラームをオートメーションにアタッチするには、コマンドを実行する IAM プリンシパルに `iam:createServiceLinkedRole` アクションの権限が必要です。CloudWatch アラームの詳細については、「Amazon CloudWatch でのアラームの使用」を参照してください。アラームがアクティブになると、自動化は実行されず、定義したすべての `0nCancel` ステップが実行されます。AWS CloudTrail を使用する場合、トレイルに API コールが表示されます。

13. [Rate control (レート制御)] セクションのオプションを使用して、各アカウントとリージョンのペア内でオートメーションを実行できる AWS リソースの数を制限します。

    [Concurrency (同時実行数)] セクションでオプションを選択します。

    - [targets (ターゲット)] を選択して、自動化ワークフローを同時に実行できるターゲットの絶対数を入力します。
    - [percentage (パーセント値)] を選択して、自動化ワークフローを同時に実行できるターゲットセットのパーセント値を入力します。

14. [Error threshold (エラーのしきい値)] セクションでオプションを選択します。

    - [errors (エラー)] を選択して、自動化が他のリソースへのワークフローの送信を停止するまでに許容されるエラーの絶対数を入力します。
    - [percentage (パーセント値)] を選択して、自動化が他のリソースへのワークフローの送信を停止するまでに許容されるエラーのパーセント値を入力します。

15. [Execute] を選択します。

複数のリージョンとアカウントでの自動化を実行する (コマンドライン)

次の手順では、AWS CLI (Linux または Windows) または AWS Tools for PowerShell を使用して、オートメーション管理アカウントから複数のリージョンおよびアカウントでオートメーションを実行する方法を説明します。

開始する前に

次の手順を完了する前に、次の情報を書き留めます。

- AWS アカウントオートメーションを実行する ID または OU。
- オートメーションを実行する Systems Manager でサポートされているリージョン。
- オートメーションを実行するタグキーとタグ値、またはリソースグループの名前。

複数のリージョンとアカウントでオートメーションを実行する

1. まだ AWS CLI または AWS Tools for PowerShell をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」および「AWS Tools for PowerShell のインストール」を参照してください。
2. 次のフォーマットを使用して、複数のリージョンとアカウントでオートメーションを実行するコマンドを作成します。各###############をユーザー自身の情報に置き換えます。

   Linux & macOS

   ```
   aws ssm start-automation-execution \
           --document-name runbook name \
           --parameters AutomationAssumeRole=arn:aws:iam::management account
    ID:role/AWS-SystemsManager-AutomationAdministrationRole \
           --target-parameter-name parameter name \
           --targets Key=tag key,Values=value \
           --target-locations Accounts=account ID,account ID
    2,Regions=Region,Region 2,ExecutionRoleName=AWS-SystemsManager-
   AutomationExecutionRole
   ```

   Windows

   ```
   aws ssm start-automation-execution ^
           --document-name runbook name ^
   ```

```
        --parameters AutomationAssumeRole=arn:aws:iam::management account
 ID:role/AWS-SystemsManager-AutomationAdministrationRole ^
        --target-parameter-name parameter name ^
        --targets Key=tag key,Values=value ^
        --target-locations Accounts=account ID,account ID
 2,Regions=Region,Region 2,ExecutionRoleName=AWS-SystemsManager-
AutomationExecutionRole
```

PowerShell

```
$Targets = New-Object Amazon.SimpleSystemsManagement.Model.Target
    $Targets.Key = "tag key"
    $Targets.Values = "value"

    Start-SSMAutomationExecution `
        -DocumentName "runbook name" `
        -Parameter @{
        "AutomationAssumeRole"="arn:aws:iam::management account ID:role/AWS-
SystemsManager-AutomationAdministrationRole" } `
        -TargetParameterName "parameter name" `
        -Target $Targets `
        -TargetLocation @{
        "Accounts"="account ID","account ID 2";
        "Regions"="Region","Region 2";
        "ExecutionRoleName"="AWS-SystemsManager-AutomationExecutionRole" }
```

次にいくつかの例を示します。

例 1: この例では、AWS Organizations 組織全体の 3 つのリージョンで EC2 インスタンスを再起動します。これを行うには、組織のルート ID をターゲットにして、子 OU を含めます。

Linux & macOS

```
aws ssm start-automation-execution \
        --document-name "AWS-RestartEC2Instance" \
        --target-parameter-name InstanceId \
        --targets '[{"Key":"AWS::EC2::Instance","Values":["*"]}]' \
        --target-locations '[{
            "Accounts": ["r-example"],
            "IncludeChildOrganizationUnits": true,
            "Regions": ["us-east-1", "us-east-2", "us-west-2"]
```

```
        }]'
```

Windows

```
aws ssm start-automation-execution \
        --document-name "AWS-RestartEC2Instance" ^
        --target-parameter-name InstanceId ^
        --targets '[{"Key":"AWS::EC2::Instance","Values":["*"]}]' ^
        --target-locations '[{
            "Accounts": ["r-example"],
            "IncludeChildOrganizationUnits": true,
            "Regions": ["us-east-1", "us-east-2", "us-west-2"]
        }]'
```

PowerShell

```
Start-SSMAutomationExecution `
        -DocumentName "AWS-RestartEC2Instance" `
        -TargetParameterName "InstanceId" `
        -Targets '[{"Key":"AWS::EC2::Instance","Values":["*"]}]'
        -TargetLocation @{
            "Accounts"="r-example";
            "Regions"="us-east-1", "us-east-2", "us-west-2";
            "IncludeChildOrganizationUnits"=true}
```

例 2: この例では、異なるアカウントおよびリージョンの特定の EC2 インスタンスを再起動します。

Linux & macOS

```
aws ssm start-automation-execution \
        --document-name "AWS-RestartEC2Instance" \
        --target-parameter-name InstanceId \
        --target-locations '[{
            "Accounts": ["123456789012"],
            "Targets": [{
                "Key":"ParameterValues",
                "Values":["i-02573cafcfEXAMPLE", "i-0471e04240EXAMPLE"]
            }],
            "TargetLocationMaxConcurrency": "100%",
            "Regions": ["us-east-1"]
```

```
        }, {
            "Accounts": ["987654321098"],
            "Targets": [{
                "Key":"ParameterValues",
                "Values":["i-07782c72faEXAMPLE"]
            }],
            "TargetLocationMaxConcurrency": "100%",
            "Regions": ["us-east-2"]
        }]'
```

Windows

```
aws ssm start-automation-execution ^
        --document-name "AWS-RestartEC2Instance" ^
        --target-parameter-name InstanceId ^
        --target-locations '[{
            "Accounts": ["123456789012"],
            "Targets": [{
                "Key":"ParameterValues",
                "Values":["i-02573cafcfEXAMPLE", "i-0471e04240EXAMPLE"]
            }],
            "TargetLocationMaxConcurrency": "100%",
            "Regions": ["us-east-1"]
        }, {
            "Accounts": ["987654321098"],
            "Targets": [{
                "Key":"ParameterValues",
                "Values":["i-07782c72faEXAMPLE"]
            }],
            "TargetLocationMaxConcurrency": "100%",
            "Regions": ["us-east-2"]
        }]'
```

PowerShell

```
Start-SSMAutomationExecution `
        -DocumentName "AWS-RestartEC2Instance" `
        -TargetParameterName "InstanceId" `
        -Targets '[{"Key":"AWS::EC2::Instance","Values":["*"]}]'
        -TargetLocation @({
            "Accounts"="123456789012",
            "Targets"= @{
                "Key":"ParameterValues",
```

```
                "Values":["i-02573cafcfEXAMPLE", "i-0471e04240EXAMPLE"]
            },
            "TargetLocationMaxConcurrency"="100%",
            "Regions"=["us-east-1"]
        }, {
            "Accounts"="987654321098",
            "Targets": @{
                "Key":"ParameterValues",
                "Values":["i-07782c72faEXAMPLE"]
            },
            "TargetLocationMaxConcurrency": "100%",
            "Regions"=["us-east-2"]
        })
```

例 3: この例では、123456789012 および 987654321098 リージョンにある us-east-2 アカウントと us-west-1 アカウントの EC2 インスタンスを再起動します。インスタンスは Env-PROD のキーペア値でタグ付けされている必要があります。

Linux & macOS

```
aws ssm start-automation-execution \
        --document-name AWS-RestartEC2Instance \
        --parameters AutomationAssumeRole=arn:aws:iam::123456789012:role/AWS-
SystemsManager-AutomationAdministrationRole \
        --target-parameter-name InstanceId \
        --targets Key=tag:Env,Values=PROD \
        --target-locations Accounts=123456789012,987654321098,Regions=us-
east-2,us-west-1,ExecutionRoleName=AWS-SystemsManager-AutomationExecutionRole
```

Windows

```
aws ssm start-automation-execution ^
        --document-name AWS-RestartEC2Instance ^
        --parameters AutomationAssumeRole=arn:aws:iam::123456789012:role/AWS-
SystemsManager-AutomationAdministrationRole ^
        --target-parameter-name InstanceId ^
        --targets Key=tag:Env,Values=PROD ^
        --target-locations Accounts=123456789012,987654321098,Regions=us-
east-2,us-west-1,ExecutionRoleName=AWS-SystemsManager-AutomationExecutionRole
```

PowerShell

```
$Targets = New-Object Amazon.SimpleSystemsManagement.Model.Target
    $Targets.Key = "tag:Env"
    $Targets.Values = "PROD"

    Start-SSMAutomationExecution `
        -DocumentName "AWS-RestartEC2Instance" `
        -Parameter @{
        "AutomationAssumeRole"="arn:aws:iam::123456789012:role/AWS-
SystemsManager-AutomationAdministrationRole" } `
        -TargetParameterName "InstanceId" `
        -Target $Targets `
        -TargetLocation @{
        "Accounts"="123456789012","987654321098";
        "Regions"="us-east-2","us-west-1";
        "ExecutionRoleName"="AWS-SystemsManager-AutomationExecutionRole" }
```

例 4: この例では、123456789012 リージョンにある 987654321098 アカウントと eu-central-1 アカウントの EC2 インスタンスを再起動します。これらのインスタンスは、prod-instances AWS リソースグループのメンバーである必要があります。

Linux & macOS

```
aws ssm start-automation-execution \
        --document-name AWS-RestartEC2Instance \
        --parameters AutomationAssumeRole=arn:aws:iam::123456789012:role/AWS-
SystemsManager-AutomationAdministrationRole \
        --target-parameter-name InstanceId \
        --targets Key=ResourceGroup,Values=prod-instances \
        --target-locations Accounts=123456789012,987654321098,Regions=eu-
central-1,ExecutionRoleName=AWS-SystemsManager-AutomationExecutionRole
```

Windows

```
aws ssm start-automation-execution ^
        --document-name AWS-RestartEC2Instance ^
        --parameters AutomationAssumeRole=arn:aws:iam::123456789012:role/AWS-
SystemsManager-AutomationAdministrationRole ^
        --target-parameter-name InstanceId ^
```

```
        --targets Key=ResourceGroup,Values=prod-instances ^
        --target-locations Accounts=123456789012,987654321098,Regions=eu-
central-1,ExecutionRoleName=AWS-SystemsManager-AutomationExecutionRole
```

PowerShell

```
$Targets = New-Object Amazon.SimpleSystemsManagement.Model.Target
    $Targets.Key = "ResourceGroup"
    $Targets.Values = "prod-instances"

    Start-SSMAutomationExecution `
        -DocumentName "AWS-RestartEC2Instance" `
        -Parameter @{
        "AutomationAssumeRole"="arn:aws:iam::123456789012:role/AWS-
SystemsManager-AutomationAdministrationRole" } `
        -TargetParameterName "InstanceId" `
        -Target $Targets `
        -TargetLocation @{
        "Accounts"="123456789012","987654321098";
        "Regions"="eu-central-1";
        "ExecutionRoleName"="AWS-SystemsManager-AutomationExecutionRole" }
```

例 5: この例では、ou-1a2b3c-4d5e6c AWS 組織単位 (OU) の EC2 インスタンスを再起動します。インスタンスは us-west-1 および us-west-2 リージョンにあります。これらのインスタンスは、WebServices AWS リソースグループのメンバーである必要があります。

Linux & macOS

```
aws ssm start-automation-execution \
        --document-name AWS-RestartEC2Instance \
        --parameters AutomationAssumeRole=arn:aws:iam::123456789012:role/AWS-
SystemsManager-AutomationAdministrationRole \
        --target-parameter-name InstanceId \
        --targets Key=ResourceGroup,Values=WebServices \
        --target-locations Accounts=ou-1a2b3c-4d5e6c,Regions=us-west-1,us-
west-2,ExecutionRoleName=AWS-SystemsManager-AutomationExecutionRole
```

Windows

```
aws ssm start-automation-execution ^
        --document-name AWS-RestartEC2Instance ^
```

```
        --parameters AutomationAssumeRole=arn:aws:iam::123456789012:role/AWS-
SystemsManager-AutomationAdministrationRole ^
        --target-parameter-name InstanceId ^
        --targets Key=ResourceGroup,Values=WebServices ^
        --target-locations Accounts=ou-1a2b3c-4d5e6c,Regions=us-west-1,us-
west-2,ExecutionRoleName=AWS-SystemsManager-AutomationExecutionRole
```

PowerShell

```
$Targets = New-Object Amazon.SimpleSystemsManagement.Model.Target
    $Targets.Key = "ResourceGroup"
    $Targets.Values = "WebServices"

    Start-SSMAutomationExecution `
        -DocumentName "AWS-RestartEC2Instance" `
        -Parameter @{
        "AutomationAssumeRole"="arn:aws:iam::123456789012:role/AWS-
SystemsManager-AutomationAdministrationRole" } `
        -TargetParameterName "InstanceId" `
        -Target $Targets `
        -TargetLocation @{
        "Accounts"="ou-1a2b3c-4d5e6c";
        "Regions"="us-west-1";
        "ExecutionRoleName"="AWS-SystemsManager-AutomationExecutionRole" }
```

システムは以下のような情報を返します。

Linux & macOS

```
{
        "AutomationExecutionId": "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE"
    }
```

Windows

```
{
        "AutomationExecutionId": "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE"
    }
```

PowerShell

```
4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE
```

3. 以下のコマンドを実行して、オートメーションの詳細を表示します。*[Automation execution ID]* (オートメーション実行 ID) をユーザー自身の情報に置き換えます。

Linux & macOS

```
aws ssm describe-automation-executions \
        --filters Key=ExecutionId,Values=automation execution ID
```

Windows

```
aws ssm describe-automation-executions ^
        --filters Key=ExecutionId,Values=automation execution ID
```

PowerShell

```
Get-SSMAutomationExecutionList | `
        Where {$_.AutomationExecutionId -eq "automation execution ID"}
```

4. 以下のコマンドを実行して、オートメーションの進行状況の詳細を表示します。

Linux & macOS

```
aws ssm get-automation-execution \
        --automation-execution-id 4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE
```

Windows

```
aws ssm get-automation-execution ^
        --automation-execution-id 4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE
```

PowerShell

```
Get-SSMAutomationExecution `
        -AutomationExecutionId a4a3c0e9-7efd-462a-8594-01234EXAMPLE
```

> **Note**
>
> コンソールで、オートメーションのステータスをモニタリングすることもできます。[Automation executions (オートメーション実行)] リストで、先ほど開始した実行を選択し、[Execution steps (実行ステップ)] タブを選択します。このタブには、オートメーションアクションのステータスが表示されます。

詳細情報

AWS Systems Manager Automation を使用した集中型マルチアカウントおよびマルチリージョンパッチ

EventBridge イベントに基づくオートメーションを実行する

ランブックを Amazon EventBridge イベントのターゲットとして指定することで、オートメーションを開始できます。オートメーションは、スケジュールに従って、または特定の AWS システムイベントが発生したときに開始できます。たとえば、インスタンスの起動時にインスタンスにソフトウェアをインストールする BootStrapInstances というランブックを作成するとします。BootStrapInstances ランブック (および対応するオートメーション) を EventBridge イベントのターゲットとして指定するには、まず新しい EventBridge ルールを作成します。(ルール例は次のとおりです: Service name: EC2、Event Type: EC2 Instance State-change Notification、Specific state(s): running、Any instance。) 次に、以下の手順により、EventBridge コンソールおよび AWS Command Line Interface (AWS CLI) を使用し、BootStrapInstances ランブックをイベントのターゲットに指定します。新しいインスタンスが起動すると、システムによってオートメーションが実行されソフトウェアがインストールされます。

ランブックの作成の詳細については、「独自のランブックの作成」を参照してください。

ランブックを使用する EventBridge イベントを作成する (コンソール)

ランブックを EventBridge イベントのターゲットとして設定するには、以下の手順を使用します。

EventBridge イベントルールのターゲットとしてランブックを設定するには

1. Amazon EventBridge コンソール (https://console.aws.amazon.com/events/) を開きます。
2. ナビゲーションペインで ルール] を選択します。

3. [ルールの作成] を選択します。
4. ルールの名前と説明を入力します。

   ルールには同じリージョン内および同じイベントバス上の別のルールと同じ名前を付けることはできません。
5. [イベントバス] で、このルールに関連付けるイベントバスを選択します。このルールを使用して、自分の AWS アカウント の一致するイベントに応答する場合は、[default] (デフォルト) を選択します。アカウントの AWS のサービスで発生したイベントは、常にアカウントのデフォルトのイベントバスに移動します。
6. ルールをトリガーする方法を選択します。

... に基づきルールを作成するには	手順	
イベント	a. [ルールタイプ] で、[イベントパターンを持つルール] を選択してください。 b. [Next] を選択します。 c. [Event source] (イベントソース) で、[AWS events or EventBridge partner events] (イベントまたは EventBridge パートナーイベント) を選択してください。 d. [Event pattern] (イベントパターン) セクションで次のいずれかを実行します。 • テンプレートを使用してイベントパターンを作成するには、[Event pattern form] (イベントパターンのフォーム) を選択	

... に基づきルールを作成するには	手順	
	し、[Event source] (イベントソース)、[AWS service]、[Event type] (イベントタイプ) を選択します。イベントタイプとして [All Events] (すべてのイベント) を選択した場合、AWS のサービスによって出力されるすべてのイベントがルールに一致します。 テンプレートをカスタマイズするには、[Custom pattern (JSON editor)] (カスタムパターン (JSON エディタ)) を選択して変更します。 • カスタムイベントパターンを使用するには、[Custom pattern (JSON editor)] (カスタムパターン (JSON エディタ)) を選択し、イベントパターンを作成します。	

... に基づきルールを作成するには	手順	
スケジュール	a. [Rule type] (ルールタイプ) では、[Schedule] (スケジュール) を選択します。 b. [Next] を選択します。 c. [Schedule pattern] (スケジュールパターン) では、次のいずれかを実行します。 • Cron 式を使用してスケジュールを定義するには、午前 8 時など、特定の時間に実行されるきめ細かいスケジュールを選択します。毎月最初の月曜日の PST に、cron 式を入力します。 • rate 式を使用してスケジュールを定義するには、10 分ごとなど、通常レートで実行されるスケジュールを選択し、rate 式を入力します。	

7. [Next] を選択します。
8. [ターゲットタイプ] で、[AWS のサービス] を選択します。
9. [Select a target] (ターゲットを選択) では、[Systems Manager オートメーション] を選択します。
10. [Document (ドキュメント)] で、ターゲットが呼び出されたときに使用するランブックを選択します。

11. [Configure automation parameter(s)] (自動化パラメータの設定) を展開して、デフォルトのパラメータ値 (使用可能な場合) のままにするか、独自の値を入力します。

> **Note**
>
> ターゲットを作成するには、各必須パラメータの値を指定する必要があります。指定しない場合、ルールは作成されますが、実行はされません。

12. 多くのターゲットタイプでは、EventBridge はターゲットにイベントを送信するためのアクセス許可が必要です。これらの場合、EventBridge は、イベントの実行に必要な IAM ロールを作成できます。次のいずれかを行います :

    - 自動的に IAM ロールを作成するには、この特定のリソースに対して新しいロールを作成するを選択します。
    - 以前に作成した IAM ロールを使用するには、[Use existing role] (既存のロールの使用) を選択し、ドロップダウンから既存のロールを選択します。EventBridge を含むように IAM ロールの信頼ポリシーを更新する必要がある場合があります。以下に例を示します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "events.amazonaws.com",
                    "ssm.amazonaws.com"
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

13. [Next] を選択します。
14. (オプション) ルールに 1 つ以上のタグを入力します。詳細については、Amazon EventBridge ユーザーガイドの「Amazon EventBridge リソースのタグ付け」を参照してください 。
15. [Next] を選択します。

16. ルールの詳細を確認し、ルールの作成 を選択します。

ランブックを使用する EventBridge イベントの作成 (コマンドライン)

次の手順では、AWS CLI (Linux または Windows の場合) または AWS Tools for PowerShell を使用して、EventBridge イベントルールを作成し、ランブックをターゲットとして設定する方法を説明します。

ランブックを EventBridge イベントルールのターゲットとして設定するには

1. まだ AWS CLI または AWS Tools for PowerShell をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」および「AWS Tools for PowerShell のインストール」を参照してください。
2. 新しい EventBridge イベントルールを指定するコマンドを作成します。各##############をユーザー自身の情報に置き換えます。

   スケジュールに基づいてトリガー

   Linux & macOS

   ```
   aws events put-rule \
   --name "rule name" \
   --schedule-expression "cron or rate expression"
   ```

   Windows

   ```
   aws events put-rule ^
   --name "rule name" ^
   --schedule-expression "cron or rate expression"
   ```

   PowerShell

   ```
   Write-CWERule `
   -Name "rule name" `
   -ScheduleExpression "cron or rate expression"
   ```

   次の例では、毎日午前 9:00 (UTC) に開始される EventBridge イベントルールを作成します。

Linux & macOS

```
aws events put-rule \
--name "DailyAutomationRule" \
--schedule-expression "cron(0 9 * * ? *)"
```

Windows

```
aws events put-rule ^
--name "DailyAutomationRule" ^
--schedule-expression "cron(0 9 * * ? *)"
```

PowerShell

```
Write-CWERule `
-Name "DailyAutomationRule" `
-ScheduleExpression "cron(0 9 * * ? *)"
```

イベントに基づいてトリガー

Linux & macOS

```
aws events put-rule \
--name "rule name" \
--event-pattern "{\"source\":[\"aws.service\"],\"detail-type\":[\"service event
 detail type\"]}"
```

Windows

```
aws events put-rule ^
--name "rule name" ^
--event-pattern "{\"source\":[\"aws.service\"],\"detail-type\":[\"service event
 detail type\"]}"
```

PowerShell

```
Write-CWERule `
-Name "rule name" `
```

```
-EventPattern '{"source":["aws.service"],"detail-type":["service event detail
 type"]}'
```

次の例では、リージョン内の任意の EC2 インスタンスの状態が変更されたときに開始される EventBridge イベントルールを作成します。

Linux & macOS

```
aws events put-rule \
--name "EC2InstanceStateChanges" \
--event-pattern "{\"source\":[\"aws.ec2\"],\"detail-type\":[\"EC2 Instance
 State-change Notification\"]}"
```

Windows

```
aws events put-rule ^
--name "EC2InstanceStateChanges" ^
--event-pattern "{\"source\":[\"aws.ec2\"],\"detail-type\":[\"EC2 Instance
 State-change Notification\"]}"
```

PowerShell

```
Write-CWERule `
-Name "EC2InstanceStateChanges" `
-EventPattern '{"source":["aws.ec2"],"detail-type":["EC2 Instance State-change
 Notification"]}'
```

このコマンドでは、次のような新しい EventBridge ルールの詳細が返されます。

Linux & macOS

```
{
"RuleArn": "arn:aws:events:us-east-1:123456789012:rule/automationrule"
}
```

Windows

```
{
"RuleArn": "arn:aws:events:us-east-1:123456789012:rule/automationrule"
```

```
}
```

PowerShell

```
arn:aws:events:us-east-1:123456789012:rule/EC2InstanceStateChanges
```

3. ステップ 2 で作成した EventBridge イベントルールのターゲットとして、ランブックを指定するコマンドを作成します。各*##############*をユーザー自身の情報に置き換えます。

Linux & macOS

```
aws events put-targets \
--rule rule name \
--targets '{"Arn": " arn:aws:ssm:region:account ID:automation-definition/runbook
 name","Input":"{\"Message\":[\"{\\\"Key\\\":\\\"key name\\\",\\\"Values\\\":[\\
\"value\\\"]}\"]}","Id": "target ID","RoleArn": "arn:aws:iam::123456789012:role/
service-role/EventBridge service role"}'
```

Windows

```
aws events put-targets ^
--rule rule name ^
--targets '{"Arn": "arn:aws:ssm:region:account ID:automation-definition/runbook
 name","Input":"{\"Message\":[\"{\\\"Key\\\":\\\"key name\\\",\\\"Values\\\":[\\
\"value\\\"]}\"]}","Id": "target ID","RoleArn": "arn:aws:iam::123456789012:role/
service-role/EventBridge service role"}'
```

PowerShell

```
$Target = New-Object Amazon.CloudWatchEvents.Model.Target
$Target.Id = "target ID"
$Target.Arn = "arn:aws:ssm:region:account ID:automation-definition/runbook name"
$Target.RoleArn = "arn:aws:iam::123456789012:role/service-role/EventBridge
 service role"
$Target.Input = '{"input parameter":["value"],"AutomationAssumeRole":
["arn:aws:iam::123456789012:role/AutomationServiceRole"]}'

Write-CWETarget `
-Rule "rule name" `
-Target $Target
```

次の例では、ランブック AWS-StartEC2Instance を使用して指定されたインスタンス ID を起動する EventBridge イベントターゲットを作成します。

Linux & macOS

```
aws events put-targets \
--rule DailyAutomationRule \
--targets '{"Arn": "arn:aws:ssm:region:*:automation-definition/AWS-
StartEC2Instance","Input":"{\"InstanceId\":[\"i-02573cafcfEXAMPLE\"],
\"AutomationAssumeRole\":[\"arn:aws:iam::123456789012:role/AutomationServiceRole
\"]}","Id": "Target1","RoleArn": "arn:aws:iam::123456789012:role/service-role/
AWS_Events_Invoke_Start_Automation_Execution_1213609520"}'
```

Windows

```
aws events put-targets ^
--rule DailyAutomationRule ^
--targets '{"Arn": "arn:aws:ssm:region:*:automation-definition/AWS-
StartEC2Instance","Input":"{\"InstanceId\":[\"i-02573cafcfEXAMPLE\"],
\"AutomationAssumeRole\":[\"arn:aws:iam::123456789012:role/AutomationServiceRole
\"]}","Id": "Target1","RoleArn": "arn:aws:iam::123456789012:role/service-role/
AWS_Events_Invoke_Start_Automation_Execution_1213609520"}'
```

PowerShell

```
$Target = New-Object Amazon.CloudWatchEvents.Model.Target
$Target.Id = "Target1"
$Target.Arn = "arn:aws:ssm:region:*:automation-definition/AWS-StartEC2Instance"
$Target.RoleArn = "arn:aws:iam::123456789012:role/service-role/
AWS_Events_Invoke_Start_Automation_Execution_1213609520"
$Target.Input = '{"InstanceId":["i-02573cafcfEXAMPLE"],"AutomationAssumeRole":
["arn:aws:iam::123456789012:role/AutomationServiceRole"]}'

Write-CWETarget `
-Rule "DailyAutomationRule" `
-Target $Target
```

システムが以下のような情報を返します。

Linux & macOS

```
{
"FailedEntries": [],
"FailedEntryCount": 0
}
```

Windows

```
{
"FailedEntries": [],
"FailedEntryCount": 0
}
```

PowerShell

PowerShell のコマンドが成功した場合、出力はありません。

オートメーションを段階的に実行する

次の手順では、AWS Systems Manager コンソール、AWS Command Line Interface (AWS CLI) を使用して、手動実行モードでオートメーションを実行する方法を説明します。手動実行モードを使用すると、オートメーションは Waiting の状態で開始し、各ステップの間で Waiting の状態で一時停止します。これにより、オートメーションをいつ進めるかを制御できます。続行する前にステップの結果を確認する必要がある場合に役立ちます。

このオートメーションは、現在のユーザーのコンテキストで実行します。これは、ランブックおよびこのランブックが呼び出すアクションを使用するアクセス許可がある限り、追加の IAM アクセス許可を設定する必要がないことを意味しています。IAM での管理者権限がある場合、このオートメーションを実行するアクセス許可を既に保持しています。

オートメーションをステップごとに実行する (コンソール)

次の手順は、Systems Manager コンソールを使用してオートメーションをステップごとに手動で実行する方法を説明します。

オートメーションをステップごとに実行するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[オートメーション]、[オートメーションの実行] の順に選択します。
3. [Automation document (自動化ドキュメント)] リストで、ランブックを選択します。[Document categories (ドキュメントカテゴリ)] ペインで 1 つ以上のオプションを選択して、目的に応じて SSM ドキュメントをフィルタリングします。自分が所有するランブックを表示するには、[Owned by me (自分が所有)] タブを選択します。自分のアカウントと共有されているランブックを表示するには、[Shared with me (共有ファイル)] タブを選択します。すべてのランブックを表示するには、[すべてのドキュメント] タブを選択します。

   > **Note**
   >
   > ランブックの名前を選択すると、ランブックに関する情報を表示できます。

4. [Document details (ドキュメントの詳細)] セクションで、[Document version (ドキュメントのバージョン)] が実行するバージョンに設定されていることを確認します。システムには、次のバージョンのオプションが含まれています。

   - [ランタイムのデフォルトバージョン]: 自動化ランブックが定期的に更新され、新しいデフォルトバージョンが割り当てられている場合は、このオプションを選択します。
   - [ランタイムの最新バージョン]: 自動化ランブックが定期的に更新され、直前に更新されたバージョンを実行する場合は、このオプションを選択します。
   - [1 (デフォルト)]: ドキュメントの最初のバージョンを実行するには、このオプションを選択します。これはデフォルト設定です。

5. [Next] を選択します。
6. [Execution Mode (実行モード)] セクションで、[Manual execution (手動実行)] を選択します。
7. [Input parameters (入力パラメータ)] セクションで、必要な入力を指定します。必要に応じて、[AutomationAssumeRole] リストから IAM サービスロールを選択できます。
8. [Execute] を選択します。
9. オートメーションの最初のステップを開始する準備ができたとき、[Execute this step (このステップを実行)] を選択します。オートメーションは1 ステップだけ進み、この手順のステップ 3 で選択したランブックで指定した後続のステップを実行する前に一時停止します。ランブックに複数のステップがある場合は、オートメーションを続行するために各ステップに対して

[Execute this step (このステップを実行)] を選択する必要があります。[Execute this step (このステップを実行)] を選択するたびに、アクションが実行されます。

> **Note**
>
> オートメーションのステータスがコンソールに表示されます。オートメーションでステップの実行に失敗した場合は、「Systems Manager Automation のトラブルシューティング」を参照してください。

10. ランブックで指定されているすべてのステップを完了したら、[Complete and view results (完了して結果を表示)] を選択してオートメーションを終了し、結果を表示します。

オートメーションをステップごとに実行する (コマンドライン)

次の手順は、AWS CLI (Linux の場合、Windows の場合は macOS) または AWS Tools for PowerShell 使用して、オートメーションをステップごとに手動で実行する方法を説明しています。

オートメーションをステップごとに実行するには

1. まだ AWS CLI または AWS Tools for PowerShell をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」および「AWS Tools for PowerShell のインストール」を参照してください。
2. 以下のコマンドを実行して、オートメーションを手動で開始します。各##############をユーザー自身の情報に置き換えます。

   Linux & macOS

   ```
   aws ssm start-automation-execution \
       --document-name runbook name \
       --mode Interactive \
       --parameters runbook parameters
   ```

   Windows

   ```
   aws ssm start-automation-execution ^
       --document-name runbook name ^
       --mode Interactive ^
   ```

```
    --parameters runbook parameters
```

PowerShell

```
Start-SSMAutomationExecution `
    -DocumentName runbook name `
    -Mode Interactive `
    -Parameter runbook parameters
```

ランブック AWS-RestartEC2Instance を使用して指定した EC2 インスタンスを再起動する例を次に示します。

Linux & macOS

```
aws ssm start-automation-execution \
    --document-name "AWS-RestartEC2Instance" \
    --mode Interactive \
    --parameters "InstanceId=i-02573cafcfEXAMPLE"
```

Windows

```
aws ssm start-automation-execution ^
    --document-name "AWS-RestartEC2Instance" ^
    --mode Interactive ^
    --parameters "InstanceId=i-02573cafcfEXAMPLE"
```

PowerShell

```
Start-SSMAutomationExecution `
    -DocumentName AWS-RestartEC2Instance `
    -Mode Interactive
    -Parameter @{"InstanceId"="i-02573cafcfEXAMPLE"}
```

システムが以下のような情報を返します。

Linux & macOS

```
{
    "AutomationExecutionId": "ba9cd881-1b36-4d31-a698-0123456789ab"
```

```
}
```

Windows

```
{
    "AutomationExecutionId": "ba9cd881-1b36-4d31-a698-0123456789ab"
}
```

PowerShell

```
ba9cd881-1b36-4d31-a698-0123456789ab
```

3. オートメーションの最初のステップを開始する準備が整ったら、次のコマンドを実行します。各*###############*をユーザー自身の情報に置き換えます。オートメーションは1 ステップだけ進み、この手順のステップ 1 で選択したランブックで指定した後続のステップを実行する前に一時停止します。ランブックに複数のステップがある場合は、オートメーションを続行するために各ステップに対して次のコマンドを実行する必要があります。

   Linux & macOS

   ```
   aws ssm send-automation-signal \
       --automation-execution-id ba9cd881-1b36-4d31-a698-0123456789ab \
       --signal-type StartStep \
       --payload StepName="stopInstances"
   ```

   Windows

   ```
   aws ssm send-automation-signal ^
       --automation-execution-id ba9cd881-1b36-4d31-a698-0123456789ab ^
       --signal-type StartStep ^
       --payload StepName="stopInstances"
   ```

   PowerShell

   ```
   Send-SSMAutomationSignal `
       -AutomationExecutionId ba9cd881-1b36-4d31-a698-0123456789ab `
       -SignalType StartStep
       -Payload @{"StepName"="stopInstances"}
   ```

コマンドが成功した場合、出力はありません。

4. 次のコマンドを実行して、オートメーションにおける各ステップ実行のステータスを取得します。

Linux & macOS

```
aws ssm describe-automation-step-executions \
    --automation-execution-id ba9cd881-1b36-4d31-a698-0123456789ab
```

Windows

```
aws ssm describe-automation-step-executions ^
    --automation-execution-id ba9cd881-1b36-4d31-a698-0123456789ab
```

PowerShell

```
Get-SSMAutomationStepExecution `
    -AutomationExecutionId ba9cd881-1b36-4d31-a698-0123456789ab
```

システムが以下のような情報を返します。

Linux & macOS

```
{
    "StepExecutions": [
        {
            "StepName": "stopInstances",
            "Action": "aws:changeInstanceState",
            "ExecutionStartTime": 1557167178.42,
            "ExecutionEndTime": 1557167220.617,
            "StepStatus": "Success",
            "Inputs": {
                "DesiredState": "\"stopped\"",
                "InstanceIds": "[\"i-02573cafcfEXAMPLE\"]"
            },
            "Outputs": {
                "InstanceStates": [
                    "stopped"
```

```
                ]
            },
            "StepExecutionId": "654243ba-71e3-4771-b04f-0123456789ab",
            "OverriddenParameters": {},
            "ValidNextSteps": [
                "startInstances"
            ]
        },
        {
            "StepName": "startInstances",
            "Action": "aws:changeInstanceState",
            "ExecutionStartTime": 1557167273.754,
            "ExecutionEndTime": 1557167480.73,
            "StepStatus": "Success",
            "Inputs": {
                "DesiredState": "\"running\"",
                "InstanceIds": "[\"i-02573cafcfEXAMPLE\"]"
            },
            "Outputs": {
                "InstanceStates": [
                    "running"
                ]
            },
            "StepExecutionId": "8a4a1e0d-dc3e-4039-a599-0123456789ab",
            "OverriddenParameters": {}
        }
    ]
}
```

Windows

```
{
    "StepExecutions": [
        {
            "StepName": "stopInstances",
            "Action": "aws:changeInstanceState",
            "ExecutionStartTime": 1557167178.42,
            "ExecutionEndTime": 1557167220.617,
            "StepStatus": "Success",
            "Inputs": {
                "DesiredState": "\"stopped\"",
                "InstanceIds": "[\"i-02573cafcfEXAMPLE\"]"
            },
```

```
            "Outputs": {
                "InstanceStates": [
                    "stopped"
                ]
            },
            "StepExecutionId": "654243ba-71e3-4771-b04f-0123456789ab",
            "OverriddenParameters": {},
            "ValidNextSteps": [
                "startInstances"
            ]
        },
        {
            "StepName": "startInstances",
            "Action": "aws:changeInstanceState",
            "ExecutionStartTime": 1557167273.754,
            "ExecutionEndTime": 1557167480.73,
            "StepStatus": "Success",
            "Inputs": {
                "DesiredState": "\"running\"",
                "InstanceIds": "[\"i-02573cafcfEXAMPLE\"]"
            },
            "Outputs": {
                "InstanceStates": [
                    "running"
                ]
            },
            "StepExecutionId": "8a4a1e0d-dc3e-4039-a599-0123456789ab",
            "OverriddenParameters": {}
        }
    ]
}
```

PowerShell

```
Action: aws:changeInstanceState
ExecutionEndTime     : 5/6/2019 19:45:46
ExecutionStartTime   : 5/6/2019 19:45:03
FailureDetails       :
FailureMessage       :
Inputs               : {[DesiredState, "stopped"], [InstanceIds,
 ["i-02573cafcfEXAMPLE"]]}
IsCritical           : False
IsEnd                : False
```

```
MaxAttempts          : 0
NextStep             :
OnFailure            :
Outputs              : {[InstanceStates,
 Amazon.Runtime.Internal.Util.AlwaysSendList`1[System.String]]}
OverriddenParameters : {}
Response             :
ResponseCode         :
StepExecutionId      : 8fcc9641-24b7-40b3-a9be-0123456789ab
StepName             : stopInstances
StepStatus           : Success
TimeoutSeconds       : 0
ValidNextSteps       : {startInstances}
```

5. 選択したランブック内のすべての指定されているステップが終了したら、次のコマンドを実行してオートメーションを完了します。各*###############*をユーザー自身の情報に置き換えます。

   Linux & macOS

   ```
   aws ssm stop-automation-execution \
       --automation-execution-id ba9cd881-1b36-4d31-a698-0123456789ab \
       --type Complete
   ```

   Windows

   ```
   aws ssm stop-automation-execution ^
       --automation-execution-id ba9cd881-1b36-4d31-a698-0123456789ab ^
       --type Complete
   ```

   PowerShell

   ```
   Stop-SSMAutomationExecution `
       -AutomationExecutionId ba9cd881-1b36-4d31-a698-0123456789ab `
       -Type Complete
   ```

   コマンドが成功した場合、出力はありません。

State Manager 関連付けでのオートメーションのスケジュール設定

ランブックと State Manager との関連付けを作成することにより、オートメーションを開始できます。State Manager は AWS Systems Manager のツールです。ランブックと State Manager との関連付けを作成することにより、異なるタイプの AWS リソースをターゲットにすることができます。たとえば、以下のような、AWS リソースに目的の状態を強制する関連付けを作成できます。

- Amazon Elastic Compute Cloud (Amazon EC2) インスタンスに Systems Manager ロールをアタッチして、マネージドインスタンスにします。
- セキュリティグループに Ingress ルールと Egress ルールを適用します。
- Amazon DynamoDB バックアップを作成または削除します。
- Amazon Elastic Block Store (Amazon EBS) スナップショットを作成または削除します。
- Amazon Simple Storage Service (Amazon S3) バケットの読み取りおよび書き込みのアクセス許可をオフにします。
- マネージドインスタンスと Amazon Relational Database Service (Amazon RDS) インスタンスを開始、再起動、または停止します。
- Linux、macOS、Window AMIs にパッチを適用します。

次の手順により、AWS Systems Manager コンソールおよび AWS Command Line Interface (AWS CLI) を使用してオートメーションを実行する State Manager 関連付けを作成します。関連付けに関する一般的な情報と、SSM `Command` ドキュメントまたは SSM `Policy` ドキュメントを使用する関連付けの作成については、「関連付けの作成」を参照してください。

[開始する前に]

State Manager を使用してオートメーションを実行する前に、以下の重要な詳細に注意してください。

- ランブックを使用する関連付けを作成する前に、AWS Systems Manager のツールである Automation に必要なアクセス許可を設定したことを確認してください。詳細については、「オートメーションの設定」を参照してください。
- ランブックを使用する State Manager 関連付けは、AWS アカウント で同時に実行されるオートメーションの最大数に反映されます。同時に最大 100 のオートメーションを実行できます。詳細については、「Amazon Web Services 全般のリファレンス」の「System Manager Service Quotas」を参照してください。

- オートメーションを実行する場合、State Manager は AWS CloudTrail のオートメーションによって開始された API オペレーションをログ記録しません。
- Systems Manager は、サービスにリンクされたロールを自動的に作成します。これにより、State Manager が Systems Manager Automation API オペレーションを呼び出すアクセス許可を持つようにします。必要に応じて AWS CLI または AWS Tools for PowerShell から次のコマンドを実行し、ユーザー自身がサービスにリンクされたロールを作成できます。

  Linux & macOS

  ```
  aws iam create-service-linked-role \
  --aws-service-name ssm.amazonaws.com
  ```

  Windows

  ```
  aws iam create-service-linked-role ^
  --aws-service-name ssm.amazonaws.com
  ```

  PowerShell

  ```
  New-IAMServiceLinkedRole `
  -AWSServiceName ssm.amazonaws.com
  ```

  サービスにリンクされたロールの詳細については、「Systems Manager のサービスにリンクされたロールの使用」を参照してください。

オートメーションを実行する関連付けを作成する (コンソール)

次の手順では、Systems Manager コンソールを使用して、オートメーションを実行する State Manager の関連付けを作成する方法について説明します。

オートメーションを実行する State Manager 関連付けを作成するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[State Manager] を選択し、[Create association (関連付けの作成)] を選択します。
3. [Name (名前)] フィールドで名前を指定します。これはオプションですが推奨されます。

4. [Document (ドキュメント)] リストで、ランブックを選択します。検索バーを使用して [Document type : Equal : Automation] ランブックでフィルタリングします。検索バーの右側にある数字を使用して、さらに多くのランブックを表示できます。

   > **Note**
   >
   > ランブックの名前を選択すると、ランブックに関する情報を表示できます。

5. ターゲットのリソース ID を指定して 1 つ以上のターゲットで自動化を実行するには、[Simple execution (シンプルな実行)] を選択します。タグや AWS などのターゲット設定のオプションを指定して AWS Resource Groups リソースのフリート全体で自動化を実行するには、[Rate control (レート制御)]を選択します。同時実行とエラーのしきい値を指定することによって、リソース全体でオートメーションの操作を制御することもできます。

   [Rate control (レート制御)] を選択した場合は [Targets (ターゲット)] セクションが表示されます。

6. [Targets (ターゲット)] セクションで、リソースをターゲットとするメソッドを選択します。

   a. (必須) [Parameter (パラメータ)] リストでパラメータを選択します。[Parameter (パラメータ)] リストの項目は、この手順の開始時に選択したランブックのパラメータによって決まります。パラメータを選択することで、オートメーションが実行されるリソースのタイプを定義します。

   b. (必須) [Targets (ターゲット)] リストで、リソースをターゲットとするメソッドを選択します。

      - [Resource Group (リソースグループ)]: [Resource Group (リソースグループ)] リストからのグループの名前を選択します。ランブックでの AWS Resource Groups のターゲット設定の詳細については、「AWS Resource Groups をターゲットにする」を参照してください。
      - [Tags (タグ)]: 表示されたフィールドにタグキーと (オプションで) タグ値を入力します。[Add] (追加) をクリックします。ランブックでのタグのターゲット設定の詳細については、「タグをターゲットにする」を参照してください。
      - [Parameter Values (パラメータ値)]: [Input parameters (入力パラメータ)] セクションに値を入力します。複数の値を指定すると、Systems Manager は指定された各値に対して子オートメーションを実行します。

たとえば、ランブックに instanceID パラメーターが含まれているとします。オートメーションを実行するときに [InstanceID] パラメータの値を指定すると、Systems Manager は指定された各インスタンス ID 値に対して子オートメーションを実行します。オートメーションが指定された各インスタンスの実行を終了するか、オートメーションが失敗した場合、親オートメーションは完了します。最大 50 個のパラメータ値を対象にすることができます。ランブックでのパラメータ値のターゲット設定の詳細については、「パラメータ値のターゲット設定」を参照してください。

7. [Input Parameters (入力パラメータ)] セクションで、必須の入力パラメータを指定します。

   タグまたはリソースグループを使用してターゲットリソースを選択した場合は、[Input parameters (入力パラメータ)] セクションでオプションを選択する必要はありません。例えば、`AWS-RestartEC2Instance` ランブックを選択し、タグを使用してインスタンスのターゲットを選択した場合、[Input parameters (入力パラメータ)] セクションでインスタンス ID を指定または選択する必要はありません。オートメーションでは、指定したタグを使用してインスタンスを再起動します。

   > **Important**
   >
   > [AutomationAssumeRole] フィールドでロール ARN を指定する必要があります。State Manager は、継承されたロールを使用しランブックで指定されている AWS のサービスを呼び出し、お客様に代わってオートメーション関連付けを実行します。

8. 定期的に関連付けを実行する場合は、[Specify schedule (スケジュールを指定)] セクションで [On Schedule (スケジュール通り)] を選択します。このオプションを選択した場合は、提供されているオプションを使用して、Cron 式または Rate 式を使用してスケジュールを作成します。State Manager 用のCron 式と Rate 式の詳細については、関連付けのための cron および rate 式 を参照してください。

   > **Note**
   >
   > Rate 式は、ランブックを使用する State Manager 関連付けに適したスケジューリングメカニズムです。Rate 式を使用すると、オートメーションの同時実行の最大数に達した場合に、関連付けを実行する際の柔軟性が高まります。Rate スケジュールを使用すると、Systems Manager は、同時オートメーションが最大に達してスロットルされたという通知を受け取った後で、オートメーションを再試行できます。

関連付けを 1 回だけ実行する場合は、[No schedule (スケジュールなし)] を選択します。

9. (オプション) [Rate Control] (レート制御) セクションで、[Concurrency] (同時実行数) および [Error threshold] (エラーのしきい値) オプションを選択して、AWS リソース全体のオートメーションのデプロイを制御できます。

   a. [Concurrency (同時実行数)] セクションでオプションを選択します。

      - [targets (ターゲット)] を選択して、オートメーションを同時に実行できるターゲットの絶対数を入力します。
      - [percentage (パーセント値)] を選択して、オートメーションを同時に実行できるターゲットセットのパーセント値を入力します。

   b. [Error threshold (エラーのしきい値)] セクションでオプションを選択します。

      - [errors (エラー)] を選択して、オートメーションが他のリソースへのオートメーションの送信を停止するまでに許容されるエラーの絶対数を入力します。
      - [percentage (パーセント値)] を選択して、オートメーションが他のリソースへのオートメーションの送信を停止するまでに許容されるエラーのパーセント値を入力します。

   オートメーションでターゲットとレート制御を使用する方法の詳細については、「自動オペレーションを大規模に実行する」を参照してください。

10. [関連付けの作成] を選択します。

> **Important**
>
> 関連付けを作成すると、関連付けはただちに指定されたターゲットに対して実行されます。その後、選択された Cron 式または Rate 式に基づいて関連付けが実行されます。[No schedule (スケジュールなし)] を選択した場合、関連付けは再び実行されません。

オートメーションワークフローを実行する関連付けを作成する (コマンドライン)

以下の手順では、AWS CLI (Linux または Windows) または AWS Tools for PowerShell を使用して、オートメーションを実行する State Manager 関連付けを作成する方法について説明します。

[開始する前に]

次の手順を完了する前に、ランブックの実行に必要な許可を含む IAM サービスロールを作成し、AWS Systems Manager のツールである Automation の信頼関係を設定していることを確認してください。詳細については、「タスク 1: 自動化のサービスロールを作成する」を参照してください。

オートメーションを実行する関連付けを作成するには

1. まだ AWS CLI または AWS Tools for PowerShell をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」および「AWS Tools for PowerShell のインストール」を参照してください。
2. ドキュメントのリストを表示するには、次のコマンドを実行します。

   Linux & macOS

   ```
   aws ssm list-documents
   ```

   Windows

   ```
   aws ssm list-documents
   ```

   PowerShell

   ```
   Get-SSMDocumentList
   ```

   関連付けに使用するランブックの名前を記録します。
3. 以下のコマンドを実行して、ランブックの詳細を表示します。次のコマンドで、*[Runbook name]* (ランブック名) をユーザー自身の情報に置き換えます。

   Linux & macOS

   ```
   aws ssm describe-document \
   --name runbook name
   ```

   InstanceId オプションに使用するパラメータ名 (例: --automation-target-parameter-name) を書き留めます。このパラメータは、オートメーションが実行されるリソースのタイプを決定します。

Windows

```
aws ssm describe-document ^
--name runbook name
```

InstanceId オプションに使用するパラメータ名 (例: --automation-target-parameter-name) を書き留めます。このパラメータは、オートメーションが実行されるリソースのタイプを決定します。

PowerShell

```
Get-SSMDocumentDescription `
-Name runbook name
```

InstanceId オプションに使用するパラメータ名 (例: AutomationTargetParameterName) を書き留めます。このパラメータは、オートメーションが実行されるリソースのタイプを決定します。

4. State Manager 関連付けを使用してオートメーションを実行するコマンドを作成します。各##########をユーザー自身の情報に置き換えます。

タグを使用したターゲット設定

Linux & macOS

```
aws ssm create-association \
--association-name association name \
--targets Key=tag:key name,Values=value \
--name runbook name \
--parameters AutomationAssumeRole=arn:aws:iam::123456789012:role/
RunbookAssumeRole \
--automation-target-parameter-name target parameter \
--schedule "cron or rate expression"
```

> **Note**
>
> AWS CLI を使用して関連付けを作成する場合は、--targets パラメータを使用して、インスタンスを関連付けのターゲットにします。--instance-id パラメー

タは使用しないでください。--instance-id パラメータはレガシーパラメータです。

Windows

```
aws ssm create-association ^
--association-name association name ^
--targets Key=tag:key name,Values=value ^
--name runbook name ^
--parameters AutomationAssumeRole=arn:aws:iam::123456789012:role/
RunbookAssumeRole ^
--automation-target-parameter-name target parameter ^
--schedule "cron or rate expression"
```

> **Note**
>
> AWS CLI を使用して関連付けを作成する場合は、--targets パラメータを使用して、インスタンスを関連付けのターゲットにします。--instance-id パラメータは使用しないでください。--instance-id パラメータはレガシーパラメータです。

PowerShell

```
$Targets = New-Object Amazon.SimpleSystemsManagement.Model.Target
$Targets.Key = "tag:key name"
$Targets.Values = "value"

New-SSMAssociation `
-AssociationName "association name" `
-Target $Targets `
-Name "runbook name" `
-Parameters @{
"AutomationAssumeRole"="arn:aws:iam::123456789012:role/RunbookAssumeRole" } `
-AutomationTargetParameterName "target parameter" `
-ScheduleExpression "cron or rate expression"
```

> **Note**
>
> AWS Tools for PowerShell を使用して関連付けを作成する場合は、Target パラメータを使用して、インスタンスを関連付けのターゲットにします。InstanceId パラメータは使用しないでください。InstanceId パラメータはレガシーパラメータです。

パラメータ値を使用したターゲット設定

Linux & macOS

```
aws ssm create-association \
--association-name association name \
--targets Key=ParameterValues,Values=value,value 2,value 3 \
--name runbook name \
--parameters AutomationAssumeRole=arn:aws:iam::123456789012:role/
RunbookAssumeRole \
--automation-target-parameter-name target parameter \
--schedule "cron or rate expression"
```

Windows

```
aws ssm create-association ^
--association-name association name ^
--targets Key=ParameterValues,Values=value,value 2,value 3 ^
--name runbook name ^
--parameters AutomationAssumeRole=arn:aws:iam::123456789012:role/
RunbookAssumeRole ^
--automation-target-parameter-name target parameter ^
--schedule "cron or rate expression"
```

PowerShell

```
$Targets = New-Object Amazon.SimpleSystemsManagement.Model.Target
$Targets.Key = "ParameterValues"
$Targets.Values = "value","value 2","value 3"

New-SSMAssociation `
-AssociationName "association name" `
```

```
-Target $Targets `
-Name "runbook name" `
-Parameters @{
"AutomationAssumeRole"="arn:aws:iam::123456789012:role/RunbookAssumeRole"} `
-AutomationTargetParameterName "target parameter" `
-ScheduleExpression "cron or rate expression"
```

AWS Resource Groups を使用したターゲット設定

Linux & macOS

```
aws ssm create-association \
--association-name association name \
--targets Key=ResourceGroup,Values=resource group name \
--name runbook name \
--parameters AutomationAssumeRole=arn:aws:iam::123456789012:role/
RunbookAssumeRole \
--automation-target-parameter-name target parameter \
--schedule "cron or rate expression"
```

Windows

```
aws ssm create-association ^
--association-name association name ^
--targets Key=ResourceGroup,Values=resource group name ^
--name runbook name ^
--parameters AutomationAssumeRole=arn:aws:iam::123456789012:role/
RunbookAssumeRole ^
--automation-target-parameter-name target parameter ^
--schedule "cron or rate expression"
```

PowerShell

```
$Targets = New-Object Amazon.SimpleSystemsManagement.Model.Target
$Targets.Key = "ResourceGroup"
$Targets.Values = "resource group name"

New-SSMAssociation `
-AssociationName "association name" `
-Target $Targets `
-Name "runbook name" `
```

```
-Parameters @{
"AutomationAssumeRole"="arn:aws:iam::123456789012:role/RunbookAssumeRole"} `
-AutomationTargetParameterName "target parameter" `
-ScheduleExpression "cron or rate expression"
```

複数のアカウントとリージョンをターゲットにする

Linux & macOS

```
aws ssm create-association \
--association-name association name \
--targets Key=ResourceGroup,Values=resource group name \
--name runbook name \
--parameters AutomationAssumeRole=arn:aws:iam::123456789012:role/
RunbookAssumeRole \
--automation-target-parameter-name target parameter \
--schedule "cron or rate expression" \
--target-locations
 Accounts=111122223333,444455556666,444455556666,Regions=region,region
```

Windows

```
aws ssm create-association ^
--association-name association name ^
--targets Key=ResourceGroup,Values=resource group name ^
--name runbook name ^
--parameters AutomationAssumeRole=arn:aws:iam::123456789012:role/
RunbookAssumeRole ^
--automation-target-parameter-name target parameter ^
--schedule "cron or rate expression" ^
--target-locations
 Accounts=111122223333,444455556666,444455556666,Regions=region,region
```

PowerShell

```
$Targets = New-Object Amazon.SimpleSystemsManagement.Model.Target
$Targets.Key = "ResourceGroup"
$Targets.Values = "resource group name"

New-SSMAssociation `
-AssociationName "association name" `
```

```
-Target $Targets `
-Name "runbook name" `
-Parameters @{
"AutomationAssumeRole"="arn:aws:iam::123456789012:role/RunbookAssumeRole"} `
-AutomationTargetParameterName "target parameter" `
-ScheduleExpression "cron or rate expression" `
-TargetLocations @{
    "Accounts"=["111122223333,444455556666,444455556666"],
    "Regions"=["region,region"]
```

このコマンドでは、次のような新しい関連付けの詳細が返されます。

Linux & macOS

```
{
"AssociationDescription": {
    "ScheduleExpression": "cron(0 7 ? * MON *)",
    "Name": "AWS-StartEC2Instance",
    "Parameters": {
        "AutomationAssumeRole": [
            "arn:aws:iam::123456789012:role/RunbookAssumeRole"
        ]
    },
    "Overview": {
        "Status": "Pending",
        "DetailedStatus": "Creating"
    },
    "AssociationId": "1450b4b7-bea2-4e4b-b340-01234EXAMPLE",
    "DocumentVersion": "$DEFAULT",
    "AutomationTargetParameterName": "InstanceId",
    "LastUpdateAssociationDate": 1564686638.498,
    "Date": 1564686638.498,
    "AssociationVersion": "1",
    "AssociationName": "CLI",
    "Targets": [
        {
            "Values": [
                "DEV"
            ],
            "Key": "tag:ENV"
        }
    ]
```

```
}
}
```

Windows

```
{
"AssociationDescription": {
    "ScheduleExpression": "cron(0 7 ? * MON *)",
    "Name": "AWS-StartEC2Instance",
    "Parameters": {
        "AutomationAssumeRole": [
            "arn:aws:iam::123456789012:role/RunbookAssumeRole"
        ]
    },
    "Overview": {
        "Status": "Pending",
        "DetailedStatus": "Creating"
    },
    "AssociationId": "1450b4b7-bea2-4e4b-b340-01234EXAMPLE",
    "DocumentVersion": "$DEFAULT",
    "AutomationTargetParameterName": "InstanceId",
    "LastUpdateAssociationDate": 1564686638.498,
    "Date": 1564686638.498,
    "AssociationVersion": "1",
    "AssociationName": "CLI",
    "Targets": [
        {
            "Values": [
                "DEV"
            ],
            "Key": "tag:ENV"
        }
    ]
}
}
```

PowerShell

```
Name                 : AWS-StartEC2Instance
InstanceId           :
Date                 : 8/1/2019 7:31:38 PM
Status.Name          :
Status.Date          :
```

```
Status.Message        :
Status.AdditionalInfo :
```

> **Note**
>
> タグを使用して 1 つ以上のターゲットインスタンスで関連付けを作成した後インスタンスからタグを削除すると、そのインスタンスは関連付けを実行しなくなります。インスタンスは State Manager ドキュメントから関連付けを解除されます。

State Manager 関連付けによって実行されるトラブルシューティングのオートメーション

Systems Manager Automation は、リージョンごと、アカウントごとに 100 の同時オートメーションの制限、1,000 のキューに入れられたオートメーションの制限を適用します。ランブックを使用する State Manager 関連付けのステータスが [Failed] (失敗) となっており、ステータス詳細が [AutomationExecutionLimitExceeded] の場合、オートメーションの数が上限に達している可能性があります。その結果、Systems Manager はオートメーションを制限します。この問題を解決するには、以下の手順を実行します。

- 別の Rate 式または Cron 式を使用して関連付けます。たとえば、関連付けが 30 分ごとに実行されるようにスケジュールされている場合は、1〜2 時間ごとに実行されるように式を変更します。
- ステータスが [Pending (保留中)] の既存のオートメーションを削除します。これらのオートメーションを削除すると、現在のキューがクリアされます。

メンテナンスウィンドウによるオートメーションのスケジュール設定

ランブックをメンテナンスウィンドウの登録済みタスクとして設定することで、オートメーションを開始できます。ランブックを登録済みタスクとして登録することにより、メンテナンスウィンドウはスケジュールされたメンテナンス期間中にオートメーションを実行します。

例えば、メンテナンスウィンドウのターゲットとして登録されたインスタンスの Amazon Machine Image (AMI) を作成する `CreateAMI` という名前のランブックを作成するとします。`CreateAMI` ランブック (および対応するオートメーション) をメンテナンスウィンドウの登録済みタスクとして指定するには、まずメンテナンスウィンドウを作成してターゲットを登録します。次に、以下の手順を使用して、メンテナンスウィンドウ内で登録済みタスクとして `CreateAMI` ドキュメントを指定します。スケジュールされた期間中にメンテナンスウィンドウが開始されると、システムはオートメーションを実行し、登録されたターゲットの AMI を作成します。

オートメーションランブックの作成については、「独自のランブックの作成」を参照してください。Automation は AWS Systems Manager のツールです。

以下の手順を使用し、AWS Systems Manager コンソール、AWS Command Line Interface (AWS CLI)、または AWS Tools for Windows PowerShell を使用して、オートメーションをメンテナンスウィンドウの登録済みタスクとして設定します。

オートメーションタスクをメンテナンスウィンドウに登録する (コンソール)

次の手順では、Systems Manager コンソールを使用して、オートメーションをメンテナンスウィンドウの登録済みタスクとして設定する方法を説明します。

開始する前に

次の手順を完了する前に、メンテナンスウィンドウを作成し、少なくとも 1 つのターゲットを登録する必要があります。詳細については、次の手順を参照してください。

- コンソールを使用してメンテナンスウィンドウを作成する.
- コンソールを使用してメンテナンスウィンドウにターゲットを割り当てる

メンテナンスウィンドウの登録されたタスクとしてオートメーションを設定するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. 左側のナビゲーションペインで、[Maintenance Windows] を選択してから、自動化タスクの登録に使用するメンテナンスウィンドウを選択します。
3. [Actions] を選択します。次に、[Register Automation task (オートメーションタスクの登録)] を選択して、ランブックを使用してターゲット上でオートメーションを選択して実行します。
4. [Name (名前)] に、タスクの名前を入力します。
5. [説明] に説明を入力します。
6. [Document (ドキュメント)] で、実行するタスクを定義するランブックを選択します。
7. [Document version (ドキュメントのバージョン)] で、使用するランブックのバージョンを選択します。
8. [Task priority (タスクの優先度)] で、このタスクの優先度を指定します。1 が最高の優先度です。メンテナンスウィンドウのタスクは、優先度順にスケジュールされ、優先度が同じタスクは並行してスケジュールされます。

9. [Targets (ターゲット)] セクションで、リソース上でタスクを実行するランブックを選択した場合は、タグを指定するか、インスタンスを手動で選択して、このオートメーションを実行するターゲットを特定します。

> **Note**
>
> ターゲットではなく入力パラメータを介してリソースを渡す場合は、メンテナンスウィンドウターゲットを指定する必要はありません。
> 多くの場合、オートメーションタスクのターゲットを明示的に指定する必要はありません。例えば、`AWS-UpdateLinuxAmi` ランブックを使用して Linux 用の Amazon Machine Image (AMI) を更新するためのオートメーションタイプのタスクを作成するとします。このタスクが実行されると、AMI は最新の利用可能な Linux ディストリビューションパッケージと Amazon ソフトウェアを反映して更新されます。AMI から作成した新しいインスタンスには、これらの更新がインストール済みです。更新する AMI の ID はランブックの入力パラメータで指定されるため、メンテナンスウィンドウタスクでターゲットを再度指定する必要はありません。

ターゲットを必要としないメンテナンスウィンドウタスクについては、the section called “ターゲットのないメンテナンスウィンドウタスクを登録” を参照してください。

10. (オプション) [レートの制御] で、以下の操作を行います。

> **Note**
>
> 実行中のタスクでターゲットが指定されていない場合は、レートコントロールを指定する必要はありません。

- [Concurrency (同時実行数)] には、オートメーションを同時に実行するターゲットの数または割合 (%) を指定します。

  タグのキーと値のペアを選択してターゲットを選択し、選択したタグを使用するターゲットの数がわからない場合は、割合を指定して同時に実行できるオートメーションの数を制限します。

  メンテナンスウィンドウが実行されると、ターゲットごとに新しいオートメーションが開始されます。1 つのにつき 100 の同時オートメーションの制限がありますAWS アカウント 100 個

を超える同時実行率を指定した場合、100 個を超える同時オートメーションはオートメーションキューに自動的に追加されます。詳細については、「Amazon Web Services 全般のリファレンス」の「System Manager Service Quotas」を参照してください。

- [Error threshold (エラーしきい値)] には、ターゲットの失敗後に他のターゲットでオートメーションの実行を停止するタイミングを、ターゲットの数または割合によって指定します。例えば、3 つのエラーを指定した場合、4 番目のエラーが受信されると Systems Manager はオートメーションの実行を停止します。まだオートメーションを処理しているターゲットもエラーを送信する可能性があります。

11. [Input Parameters (入力パラメータ)] セクションで、ランブックのパラメータを指定します。ランブックの場合、システムによって一部の値が自動的に設定されます。これらの値はそのままにすることも置き換えることもできます。

> **Important**
>
> ランブックの場合、オプションでオートメーションの引き受けロールを指定できます。このパラメータにロールを指定しない場合、オートメーションは、ステップ 11 で選択したメンテナンスウィンドウサービスロールを継承します。そのため、選択したメンテナンスウィンドウサービスロールに、ランブック内で定義されているアクションを実行するための適切な AWS Identity and Access Management (IAM) アクセス許可があることを確認する必要があります。
>
> 例えば、Systems Manager のサービスにリンクされたロールには、ランブック `ec2:CreateSnapshot` を実行するために必要な IAM アクセス許可 `AWS-CopySnapshot` がありません。このシナリオでは、カスタムのメンテナンスウィンドウサービスロールを使用するか、または `ec2:CreateSnapshot` アクセス許可を持つ自動化継承ロールを指定する必要があります。詳細については、オートメーションの設定 を参照してください。

12. [IAM service role] (IAM サービスロール) 領域でロールを選択し、Systems Manager がオートメーションを開始するためのアクセス許可を付与します。

    メンテナンスウィンドウのタスク用にサービスロールを作成するには、「Maintenance Windows を設定する」を参照してください。

13. [Register Automation task (自動化タスクの登録)] を選択します。

オートメーションタスクをメンテナンスウィンドウに登録する (コマンドライン)

次の手順では、AWS CLI (Linux または Windows) または AWS Tools for PowerShell を使用して、オートメーションをメンテナンスウィンドウの登録済みタスクとして設定する方法を説明します。

開始する前に

次の手順を完了する前に、メンテナンスウィンドウを作成し、少なくとも 1 つのターゲットを登録する必要があります。詳細については、次の手順を参照してください。

- ステップ 1: AWS CLI を使用してメンテナンスウィンドウを作成する.
- ステップ 2: AWS CLI を使用してメンテナンスウィンドウにターゲットノードを登録する

メンテナンスウィンドウの登録されたタスクとしてオートメーションを設定するには

1. まだ AWS CLI または AWS Tools for PowerShell をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」および「AWS Tools for PowerShell のインストール」を参照してください。

2. オートメーションをメンテナンスウィンドウの登録済みタスクとして設定するコマンドを作成します。各###############をユーザー自身の情報に置き換えます。

   Linux & macOS

```
aws ssm register-task-with-maintenance-window \
--window-id window ID \
--name task name \
--task-arn runbook name \
--targets Key=targets,Values=value \
--service-role-arn IAM role arn \
--task-type AUTOMATION \
--task-invocation-parameters task parameters \
--priority task priority \
--max-concurrency 10% \
--max-errors 5
```

> **Note**
>
> AWS CLI を使用してオートメーションを登録済みタスクとして設定する場合、--Task-Invocation-Parameters パラメータを使用して、実行時にタスクに渡すパラメータを指定します。--Task-Parameters パラメータは使用しないでください。--Task-Parameters パラメータはレガシーパラメータです。
> ターゲットが指定されていないメンテナンスウィンドウタスクの場合、--max-errors と --max-concurrency の値は指定できません。代わりに、システムはプレースホルダ値として 1 を挿入します。これは describe-maintenance-window-tasks や get-maintenance-window-task などのコマンドへのレスポンスで報告されることがあります。これらの値は、タスクの実行には影響しないため、無視できます。
> ターゲットを必要としないメンテナンスウィンドウタスクについては、ターゲットのないメンテナンスウィンドウタスクを登録 を参照してください。

Windows

```
aws ssm register-task-with-maintenance-window ^
--window-id window ID ^
--name task name ^
--task-arn runbook name ^
--targets Key=targets,Values=value ^
--service-role-arn IAM role arn ^
--task-type AUTOMATION ^
--task-invocation-parameters task parameters ^
--priority task priority ^
--max-concurrency 10% ^
--max-errors 5
```

> **Note**
>
> AWS CLI を使用してオートメーションを登録済みタスクとして設定する場合、--task-invocation-parameters パラメータを使用して、実行時にタスクに渡すパラメータを指定します。--task-parameters パラメータは使用しないでください。--task-parameters パラメータはレガシーパラメータです。
> ターゲットが指定されていないメンテナンスウィンドウタスクの場合、--max-errors と --max-concurrency の値は指定できません。代わりに、システムは

プレースホルダ値として 1 を挿入します。これは describe-maintenance-window-tasks や get-maintenance-window-task などのコマンドへのレスポンスで報告されることがあります。これらの値は、タスクの実行には影響しないため、無視できます。ターゲットを必要としないメンテナンスウィンドウタスクについては、ターゲットのないメンテナンスウィンドウタスクを登録 を参照してください。

PowerShell

```
Register-SSMTaskWithMaintenanceWindow `
-WindowId window ID `
-Name "task name" `
-TaskArn "runbook name" `
-Target @{ Key="targets";Values="value" } `
-ServiceRoleArn "IAM role arn" `
-TaskType "AUTOMATION" `
-Automation_Parameter @{ "task parameter"="task parameter value"} `
-Priority task priority `
-MaxConcurrency 10% `
-MaxError 5
```

> **Note**
>
> AWS Tools for PowerShell を使用してオートメーションを登録済みタスクとして設定する場合、-Automation_Parameter パラメータを使用して、タスクの実行時にタスクに渡すパラメータを指定します。-TaskParameters パラメータは使用しないでください。-TaskParameters パラメータはレガシーパラメータです。
> ターゲットが指定されていないメンテナンスウィンドウタスクの場合、-MaxError と -MaxConcurrency の値は指定できません。代わりに、システムはプレースホルダ値として 1 を挿入します。これは Get-SSMMaintenanceWindowTaskList や Get-SSMMaintenanceWindowTask などのコマンドへのレスポンスで報告されることがあります。これらの値は、タスクの実行には影響しないため、無視できます。ターゲットを必要としないメンテナンスウィンドウタスクについては、ターゲットのないメンテナンスウィンドウタスクを登録 を参照してください。

次の例では、優先度 1 のメンテナンスウィンドウの登録済みタスクとしてオートメーションを設定します。また、ターゲットレスメンテナンスウィンドウタスクの --targets、--max-

errors、--max-concurrency オプションの省略についても説明します。オートメーションは AWS-StartEC2Instance ランブックおよび指定されたオートメーション継承ロールを使用して、メンテナンスウィンドウにターゲットとして登録済みの EC2 インスタンスを起動します。メンテナンスウィンドウは、所定の時点で最大 5 個のインスタンスでオートメーションを同時に実行します。また、エラー数が 1 を超えた場合、この登録済みタスクは特定の間隔で、それ以上のインスタンスで実行されなくなります。

Linux & macOS

```
aws ssm register-task-with-maintenance-window \
--window-id mw-0c50858d01EXAMPLE \
--name StartEC2Instances \
--task-arn AWS-StartEC2Instance \
--service-role-arn arn:aws:iam::123456789012:role/MaintenanceWindowRole \
--task-type AUTOMATION \
--task-invocation-parameters "{\"Automation\":{\"Parameters\":{\"InstanceId\":
[\"{{TARGET_ID}}\"],\"AutomationAssumeRole\":[\"arn:aws:iam::123456789012:role/
AutomationAssumeRole\"]}}}" \
--priority 1
```

Windows

```
aws ssm register-task-with-maintenance-window ^
--window-id mw-0c50858d01EXAMPLE ^
--name StartEC2Instances ^
--task-arn AWS-StartEC2Instance ^
--service-role-arn arn:aws:iam::123456789012:role/MaintenanceWindowRole ^
--task-type AUTOMATION ^
--task-invocation-parameters "{\"Automation\":{\"Parameters\":{\"InstanceId\":
[\"{{TARGET_ID}}\"],\"AutomationAssumeRole\":[\"arn:aws:iam::123456789012:role/
AutomationAssumeRole\"]}}}" ^
--priority 1
```

PowerShell

```
Register-SSMTaskWithMaintenanceWindow `
-WindowId mw-0c50858d01EXAMPLE `
-Name "StartEC2" `
-TaskArn "AWS-StartEC2Instance" `
-ServiceRoleArn "arn:aws:iam::123456789012:role/MaintenanceWindowRole" `
-TaskType "AUTOMATION" `
```

```
-Automation_Parameter
 @{ "InstanceId"="{{TARGET_ID}}";"AutomationAssumeRole"="arn:aws:iam::123456789012:role/
AutomationAssumeRole" } `
-Priority 1
```

このコマンドでは、次のような新しい登録済みタスクの詳細が返されます。

Linux & macOS

```
{
"WindowTaskId": "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE"
}
```

Windows

```
{
"WindowTaskId": "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE"
}
```

PowerShell

```
4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE
```

3. 登録済みタスクを表示するには、次のコマンドを実行します。*[Maintenance windows ID]* (メンテナンスウィンドウ ID) をユーザー自身の情報に置き換えます。

Linux & macOS

```
aws ssm describe-maintenance-window-tasks \
--window-id maintenance window ID
```

Windows

```
aws ssm describe-maintenance-window-tasks ^
--window-id maintenance window ID
```

PowerShell

```
Get-SSMMaintenanceWindowTaskList `
```

```
-WindowId maintenance window ID
```

システムが以下のような情報を返します。

Linux & macOS

```
{
"Tasks": [
    {
        "ServiceRoleArn": "arn:aws:iam::123456789012:role/
MaintenanceWindowRole",
        "MaxErrors": "1",
        "TaskArn": "AWS-StartEC2Instance",
        "MaxConcurrency": "1",
        "WindowTaskId": "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE",
        "TaskParameters": {},
        "Priority": 1,
        "WindowId": "mw-0c50858d01EXAMPLE",
        "Type": "AUTOMATION",
        "Targets": [
        ],
        "Name": "StartEC2"
    }
]
}
```

Windows

```
{
"Tasks": [
    {
        "ServiceRoleArn": "arn:aws:iam::123456789012:role/
MaintenanceWindowRole",
        "MaxErrors": "1",
        "TaskArn": "AWS-StartEC2Instance",
        "MaxConcurrency": "1",
        "WindowTaskId": "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE",
        "TaskParameters": {},
        "Priority": 1,
        "WindowId": "mw-0c50858d01EXAMPLE",
        "Type": "AUTOMATION",
        "Targets": [
```

```
        ],
        "Name": "StartEC2"
    }
]
}
```

PowerShell

```
Description    :
LoggingInfo    :
MaxConcurrency : 5
MaxErrors      : 1
Name           : StartEC2
Priority       : 1
ServiceRoleArn : arn:aws:iam::123456789012:role/MaintenanceWindowRole
Targets        : {}
TaskArn        : AWS-StartEC2Instance
TaskParameters : {}
Type           : AUTOMATION
WindowId       : mw-0c50858d01EXAMPLE
WindowTaskId   : 4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE
```

Systems Manager Automation アクションのリファレンス

このリファレンスでは、オートメーションランブックで指定できるAutomation アクションについて説明します。Automation は AWS Systems Manager のツールです。これらのアクションは他のタイプの Systems Manager (SSM) ドキュメントでは使用できません。SSM の他のドキュメントタイプのプラグインについては、「コマンドドキュメントプラグインリファレンス」を参照してください。

Systems Manager Automation は、オートエアコンランブックで定義されたステップを実行します。各ステップは、特定のオペレーションに関連付けられます。このアクションは、ステップの入力、動作、出力を決定します。ステップは、ランブックの `mainSteps` セクションで定義されます。

アクションまたはステップの出力を指定する必要はありません。出力は、ステップに関係付けられるアクションで事前判断されます。Runbook でステップ入力を指定すると、前のステップの 1 つあるいは複数の出力を参照できます。たとえば、`aws:runInstances` の出力は後続の `aws:runCommand` アクションで利用できます。Runbook の `Output` セクションで前のステップの出力を参照することもできます。

Important

AWS Identity and Access Management (IAM) サービスロールを使用して他のサービスを呼び出す自動化ワークフローを実行する場合は、それらのサービスを呼び出すためのアクセス許可をサービスロールに設定する必要がある点に注意してください。この要件は、`AWS-ConfigureS3BucketLogging`、`AWS-CreateDynamoDBBackup`、`AWS-RestartEC2Instance` ランブックなど、すべての AWS オートメーションランブック (`AWS-*` ランブック) に適用されます。この要件は、他のサービスを呼び出すアクションを使用して他の AWS のサービスを呼び出すように作成したカスタムオートメーションランブックにも適用されます。例えば、`aws:executeAwsApi`、`aws:createStack`、または `aws:copyImage` のアクションを使用する場合は、それらのサービスを呼び出すためのアクセス許可を持つサービスロールを設定します。ロールに IAM インラインポリシーを追加することで、他の AWS のサービスへのアクセス許可を有効にできます。詳細については、「(オプション) 他の AWS のサービス を呼び出すためのオートメーションインラインポリシーまたはカスタマー管理ポリシーを追加する」を参照してください。

トピック

- すべてのアクションで共有されるプロパティ
- aws:approve - 手動承認のためにオートメーションを一時停止する
- aws:assertAwsResourceProperty – AWS リソースの状態またはイベントの状態をアサートする
- aws:branch – 条件付きオートメーションステップを実行する
- aws:changeInstanceState – インスタンスの状態を変更またはアサートする
- aws:copyImage — Amazon Machine Image のコピーまたは暗号化
- aws:createImage – Amazon マシンイメージ (AMI) を作成する
- aws:createStack – AWS CloudFormation スタックを作成する
- aws:createTags – AWS リソースのタグを作成する
- aws:deleteImage – Amazon Machine Image を削除する
- aws:deleteStack – AWS CloudFormation スタックを削除する
- aws:executeAutomation – 別のオートメーションを実行する
- aws:executeAwsApi — AWS API オペレーションの呼び出しと実行
- aws:executeScript – スクリプトを実行する
- aws:executeStateMachine – AWS Step Functions ステートマシンを実行する

- aws:invokeWebhook – オートメーションのウェブフック統合を呼び出す
- aws:invokeLambdaFunction – AWS Lambda 関数を呼び出す
- aws:loop — オートメーション内のステップを反復処理します。
- aws:pause – オートメーションを一時停止する
- aws:runCommand – マネージドインスタンスでコマンドを実行する
- aws:runInstances – Amazon EC2 インスタンスの起動
- aws:sleep – オートメーションを遅らせる
- aws:updateVariable — ランブック変数の値を更新します。
- aws:waitForAwsResourceProperty – AWS リソースプロパティを待つ
- オートメーションシステム変数

すべてのアクションで共有されるプロパティ

共通プロパティは、すべてのアクションで見つかるパラメータまたはオプションです。一部のオプションは、ステップの動作を定義します。たとえば、ステップが完了するまで待機する時間や、ステップが失敗した場合の対処方法などです。以下のプロパティは、すべてのアクションに共通です。

description

ランブックまたはステップの目的を説明するために提供する情報。

タイプ: 文字列

必須: いいえ

name

Runbook のすべてのステップ名にわたって一意でなければならない識別子。

タイプ: 文字列

使用できるパターン: [a-zA-Z0-9_]+$

必須: はい

action

ステップが実行するアクションの名前です。aws:runCommand – マネージドインスタンスでコマンドを実行する はここで指定できるアクションの例です。このドキュメントは、使用可能なすべてのアクションの詳細情報を提供します。

型: 文字列

必須: はい

maxAttempts

ステップが失敗した場合は再試行する回数。指定した値が 1 より大きい場合、すべての再試行が失敗するまでステップは失敗したと見なされません。デフォルト値は 1 です。

タイプ: 整数

必須: いいえ

timeoutSeconds

ステップのタイムアウト値。タイムアウトが達したときに maxAttempts の値が 1 以上の場合、すべての再試行が実行されるまでこのステップはタイムアウトとは見なされません。

タイプ: 整数

必須: いいえ

onFailure

失敗時にオートメーションを中止するか、続行するか、別のステップに移行するかを示します。このオプションのデフォルト値は中止です。

型: 文字列

有効な値: Abort | Continue | step:*step_name*

必須: いいえ

onCancel

ユーザーがオートメーションをキャンセルした場合に、オートメーションがどのステップに進むべきかを示します。Automation は、最大で 2 分間、キャンセルワークフローを実行します。

型: 文字列

有効な値: Abort | step:*step_name*

必須: いいえ

onCancel プロパティでは、次のアクションへの移動はサポートされていません。

- aws:approve
- aws:copyImage

- aws:createImage
- aws:createStack
- aws:createTags
- aws:loop
- aws:pause
- aws:runInstances
- aws:sleep

isEnd

このオプションでは、特定のステップの最後にオートメーションを停止します。ステップが失敗または成功した場合に、オートメーションが停止します。デフォルト値は false です。

タイプ: ブール値

有効な値: true | false

必須: いいえ

nextStep

ステップを正常に完了した後に、次に処理するオートメーションのステップを指定します。

型: 文字列

必須: いいえ

isCritical

自動化の正常な完了のために、ステップを critical として指定します。この指定のステップが失敗した場合、自動化は自動化の失敗の最終的なステータスをレポートします。このプロパティは、ステップで明示的に定義した場合のみ評価されます。ステップで onFailure プロパティが Continue に設定されている場合、値はデフォルトで false になります。それ以外の場合、このオプションのデフォルト値は true です。

タイプ: ブール値

有効な値: true | false

必須: いいえ

inputs

アクション固有のプロパティ。

型: マップ

必須: はい

例

```
---
description: "Custom Automation Example"
schemaVersion: '0.3'
assumeRole: "{{ AutomationAssumeRole }}"
parameters:
  AutomationAssumeRole:
    type: String
    description: "(Required) The ARN of the role that allows Automation to perform
      the actions on your behalf. If no role is specified, Systems Manager Automation
      uses your IAM permissions to run this runbook."
    default: ''
  InstanceId:
      type: String
      description: "(Required) The Instance Id whose root EBS volume you want to
 restore the latest Snapshot."
      default: ''
mainSteps:
- name: getInstanceDetails
  action: aws:executeAwsApi
  onFailure: Abort
  inputs:
    Service: ec2
    Api: DescribeInstances
    InstanceIds:
    - "{{ InstanceId }}"
  outputs:
    - Name: availabilityZone
      Selector: "$.Reservations[0].Instances[0].Placement.AvailabilityZone"
      Type: String
    - Name: rootDeviceName
      Selector: "$.Reservations[0].Instances[0].RootDeviceName"
      Type: String
  nextStep: getRootVolumeId
- name: getRootVolumeId
  action: aws:executeAwsApi
  maxAttempts: 3
  onFailure: Abort
```

```
  inputs:
    Service: ec2
    Api: DescribeVolumes
    Filters:
    -  Name: attachment.device
       Values: ["{{ getInstanceDetails.rootDeviceName }}"]
    -  Name: attachment.instance-id
       Values: ["{{ InstanceId }}"]
  outputs:
    - Name: rootVolumeId
      Selector: "$.Volumes[0].VolumeId"
      Type: String
  nextStep: getSnapshotsByStartTime
- name: getSnapshotsByStartTime
  action: aws:executeScript
  timeoutSeconds: 45
  onFailure: Abort
  inputs:
    Runtime: python3.8
    Handler: getSnapshotsByStartTime
    InputPayload:
      rootVolumeId : "{{ getRootVolumeId.rootVolumeId }}"
    Script: |-
      def getSnapshotsByStartTime(events,context):
        import boto3

        #Initialize client
        ec2 = boto3.client('ec2')
        rootVolumeId = events['rootVolumeId']
        snapshotsQuery = ec2.describe_snapshots(
          Filters=[
            {
              "Name": "volume-id",
              "Values": [rootVolumeId]
            }
          ]
        )
        if not snapshotsQuery['Snapshots']:
          noSnapshotFoundString = "NoSnapshotFound"
          return { 'noSnapshotFound' : noSnapshotFoundString }
        else:
          jsonSnapshots = snapshotsQuery['Snapshots']
          sortedSnapshots = sorted(jsonSnapshots, key=lambda k: k['StartTime'],
 reverse=True)
```

```
          latestSortedSnapshotId = sortedSnapshots[0]['SnapshotId']
          return { 'latestSnapshotId' : latestSortedSnapshotId }
  outputs:
  - Name: Payload
    Selector: $.Payload
    Type: StringMap
  - Name: latestSnapshotId
    Selector: $.Payload.latestSnapshotId
    Type: String
  - Name: noSnapshotFound
    Selector: $.Payload.noSnapshotFound
    Type: String
  nextStep: branchFromResults
- name: branchFromResults
  action: aws:branch
  onFailure: Abort
  onCancel: step:startInstance
  inputs:
    Choices:
    - NextStep: createNewRootVolumeFromSnapshot
      Not:
        Variable: "{{ getSnapshotsByStartTime.noSnapshotFound }}"
        StringEquals: "NoSnapshotFound"
  isEnd: true
- name: createNewRootVolumeFromSnapshot
  action: aws:executeAwsApi
  onFailure: Abort
  inputs:
    Service: ec2
    Api: CreateVolume
    AvailabilityZone: "{{ getInstanceDetails.availabilityZone }}"
    SnapshotId: "{{ getSnapshotsByStartTime.latestSnapshotId }}"
  outputs:
    - Name: newRootVolumeId
      Selector: "$.VolumeId"
      Type: String
  nextStep: stopInstance
- name: stopInstance
  action: aws:executeAwsApi
  onFailure: Abort
  inputs:
    Service: ec2
    Api: StopInstances
    InstanceIds:
```

```
    - "{{ InstanceId }}"
  nextStep: verifyVolumeAvailability
- name: verifyVolumeAvailability
  action: aws:waitForAwsResourceProperty
  timeoutSeconds: 120
  inputs:
    Service: ec2
    Api: DescribeVolumes
    VolumeIds:
    - "{{ createNewRootVolumeFromSnapshot.newRootVolumeId }}"
    PropertySelector: "$.Volumes[0].State"
    DesiredValues:
    - "available"
  nextStep: verifyInstanceStopped
- name: verifyInstanceStopped
  action: aws:waitForAwsResourceProperty
  timeoutSeconds: 120
  inputs:
    Service: ec2
    Api: DescribeInstances
    InstanceIds:
    - "{{ InstanceId }}"
    PropertySelector: "$.Reservations[0].Instances[0].State.Name"
    DesiredValues:
    - "stopped"
  nextStep: detachRootVolume
- name: detachRootVolume
  action: aws:executeAwsApi
  onFailure: Abort
  isCritical: true
  inputs:
    Service: ec2
    Api: DetachVolume
    VolumeId: "{{ getRootVolumeId.rootVolumeId }}"
  nextStep: verifyRootVolumeDetached
- name: verifyRootVolumeDetached
  action: aws:waitForAwsResourceProperty
  timeoutSeconds: 30
  inputs:
    Service: ec2
    Api: DescribeVolumes
    VolumeIds:
    - "{{ getRootVolumeId.rootVolumeId }}"
    PropertySelector: "$.Volumes[0].State"
```

```
    DesiredValues:
    - "available"
  nextStep: attachNewRootVolume
- name: attachNewRootVolume
  action: aws:executeAwsApi
  onFailure: Abort
  inputs:
    Service: ec2
    Api: AttachVolume
    Device: "{{ getInstanceDetails.rootDeviceName }}"
    InstanceId: "{{ InstanceId }}"
    VolumeId: "{{ createNewRootVolumeFromSnapshot.newRootVolumeId }}"
  nextStep: verifyNewRootVolumeAttached
- name: verifyNewRootVolumeAttached
  action: aws:waitForAwsResourceProperty
  timeoutSeconds: 30
  inputs:
    Service: ec2
    Api: DescribeVolumes
    VolumeIds:
    - "{{ createNewRootVolumeFromSnapshot.newRootVolumeId }}"
    PropertySelector: "$.Volumes[0].Attachments[0].State"
    DesiredValues:
    - "attached"
  nextStep: startInstance
- name: startInstance
  action: aws:executeAwsApi
  onFailure: Abort
  inputs:
    Service: ec2
    Api: StartInstances
    InstanceIds:
    - "{{ InstanceId }}"
```

aws:approve - 手動承認のためにオートメーションを一時停止する

指定されたプリンシパルによってアクションか承認または拒否されるまで、一時的にオートメーションを停止します。必要な承認数が得られると、オートメーションが再開されます。Runbook の mainSteps セクションの任意の場所に承認ステップを挿入できます。

> **Note**
>
> このアクションは、マルチアカウントとリージョンオートメーションをサポートしていません。このアクションのデフォルトのタイムアウトは 7 日間 (604800 秒) で、最大値は 30 日間 (2592000 秒) です。timeoutSeconds ステップで aws:approve パラメータを指定して、タイムアウトを制限または延長することができます。

次の例では、1 つの承認者がアクションを許可または拒否するまで、aws:approve アクションによって一時的にオートメーションが停止します。承認されると、オートメーションはシンプルな PowerShell コマンドを実行します。

YAML

```
---
description: RunInstancesDemo1
schemaVersion: '0.3'
assumeRole: "{{ assumeRole }}"
parameters:
  assumeRole:
    type: String
  message:
    type: String
mainSteps:
- name: approve
  action: aws:approve
  timeoutSeconds: 1000
  onFailure: Abort
  inputs:
    NotificationArn: arn:aws:sns:us-east-2:12345678901:AutomationApproval
    Message: "{{ message }}"
    MinRequiredApprovals: 1
    Approvers:
    - arn:aws:iam::12345678901:user/AWS-User-1
- name: run
  action: aws:runCommand
  inputs:
    InstanceIds:
    - i-1a2b3c4d5e6f7g
    DocumentName: AWS-RunPowerShellScript
    Parameters:
      commands:
```

```
      - date
```

JSON

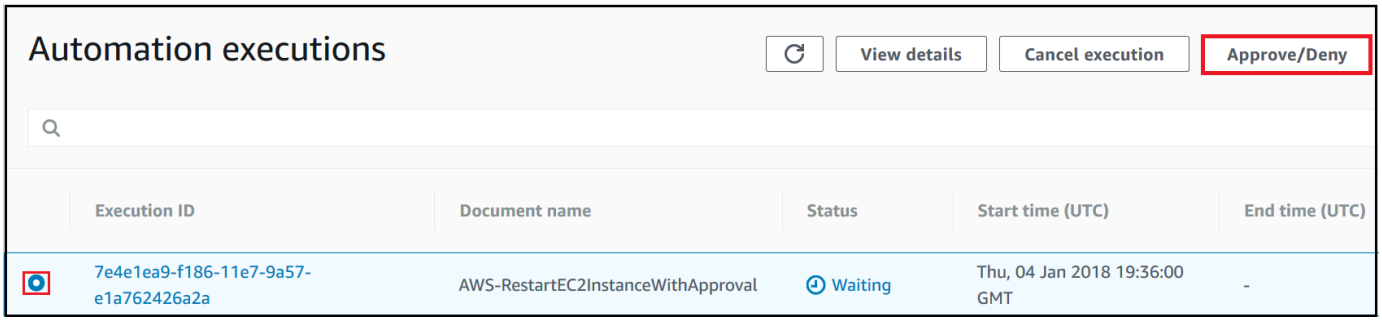
```
{
   "description":"RunInstancesDemo1",
   "schemaVersion":"0.3",
   "assumeRole":"{{ assumeRole }}",
   "parameters":{
      "assumeRole":{
         "type":"String"
      },
      "message":{
         "type":"String"
      }
   },
   "mainSteps":[
      {
         "name":"approve",
         "action":"aws:approve",
         "timeoutSeconds":1000,
         "onFailure":"Abort",
         "inputs":{
            "NotificationArn":"arn:aws:sns:us-
east-2:12345678901:AutomationApproval",
            "Message":"{{ message }}",
            "MinRequiredApprovals":1,
            "Approvers":[
               "arn:aws:iam::12345678901:user/AWS-User-1"
            ]
         }
      },
      {
         "name":"run",
         "action":"aws:runCommand",
         "inputs":{
            "InstanceIds":[
               "i-1a2b3c4d5e6f7g"
            ],
            "DocumentName":"AWS-RunPowerShellScript",
            "Parameters":{
               "commands":[
                  "date"
```

```
                ]
            }
        }
    }
]
}
```

コンソールで承認を待機中の自動化を承認または拒否できます。

待機中の自動化を許可または拒否するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで [オートメーション] を選択します。
3. ステータスが [待機中] の自動化の横にあるオプションを選択します。



4. [Approve/Deny] (承認/拒否) を選択します。
5. 自動化の詳細を確認します。
6. [承認] または [拒否] を選択し、オプションでコメントを入力して、[送信] を選択します。

入力例

YAML

```
NotificationArn: arn:aws:sns:us-west-1:12345678901:Automation-ApprovalRequest
Message: Please approve this step of the Automation.
MinRequiredApprovals: 3
Approvers:
- IamUser1
- IamUser2
- arn:aws:iam::12345678901:user/IamUser3
```

```
- arn:aws:iam::12345678901:role/IamRole
```

JSON

```
{
   "NotificationArn":"arn:aws:sns:us-west-1:12345678901:Automation-ApprovalRequest",
   "Message":"Please approve this step of the Automation.",
   "MinRequiredApprovals":3,
   "Approvers":[
      "IamUser1",
      "IamUser2",
      "arn:aws:iam::12345678901:user/IamUser3",
      "arn:aws:iam::12345678901:role/IamRole"
   ]
}
```

NotificationArn

オートメーションの承認のための Amazon Simple Notification Service (Amazon SNS) トピックの Amazon リソースネーム (ARN)。Runbook で aws:approve ステップを指定すると、オートメーションステップを承認または拒否する必要があることを知らせるメッセージが、このトピックに送信されます。Amazon SNS トピックのタイトルは「Automation」というプレフィックスをつける必要があります。

型: 文字列

必須: いいえ

メッセージ

承認リクエストが送信されるときに Amazon SNS トピックに含める情報。メッセージの最大長は 4096 文字です。

型: 文字列

必須: いいえ

MinRequiredApprovals

オートメーションが再開されるために必要な承認の最小数。値を指定しない場合、システムによるデフォルトは 1 です。このパラメータの値は、正の数にする必要があります。このパラメータの値は、Approvers パラメータで定義された承認者の数を超えることはできません。

タイプ: 整数

必須: いいえ

Approvers

アクションを承認または拒否できる AWS の認証プリンシパルのリスト。承認者の最大数は 10 です。プリンシパルは、次のいずれかの形式を使用して指定できます。

- ユーザー名
- ユーザー ARN
- IAM ロール ARN
- IAM 継承ロール ARN

タイプ: StringList

必須: はい

EnhancedApprovals

Change Manager テンプレートにのみ使用される入力。アクションを承認または拒否できる AWS 認証済みプリンシパルのリスト、IAM プリンシパルのタイプ、および承認者の最小数。以下に例を示します。

```
schemaVersion: "0.3"
emergencyChange: false
autoApprovable: false
mainSteps:
    - name: ApproveAction1
    action: aws:approve
    timeoutSeconds: 604800
    inputs:
        Message: Please approve this change request
        MinRequiredApprovals: 3
        EnhancedApprovals:
        Approvers:
            - approver: John Stiles
            type: IamUser
            minRequiredApprovals: 0
            - approver: Ana Carolina Silva
            type: IamUser
            minRequiredApprovals: 0
            - approver: GroupOfThree
```

```
            type: IamGroup
            minRequiredApprovals: 0
            - approver: RoleOfTen
            type: IamRole
            minRequiredApprovals: 0
```

タイプ: StringList

必須: はい

出力

ApprovalStatus

ステップの承認ステータス。ステータスは、Approved、Rejected、または Waiting のいずれかです。Waiting は自動化が承認者の入力を待っていることを意味します。

型: 文字列

ApproverDecisions

各承認者の承認状況を含む JSON マップです。

タイプ: MapList

aws:assertAwsResourceProperty – AWS リソースの状態またはイベントの状態をアサートする

aws:assertAwsResourceProperty アクションを使用すると、特定の Automation ステップの、特定のリソース状態またはイベント状態をアサートできます。

このアクションの使用例については、「その他のランブックの例」を参照してください。

入力

入力は、選択した API オペレーションによって定義されます。

YAML

```
action: aws:assertAwsResourceProperty
```

```
inputs:
  Service: The official namespace of the service
  Api: The API operation or method name
  API operation inputs or parameters: A value
  PropertySelector: Response object
  DesiredValues:
  - Desired property values
```

JSON

```
{
  "action": "aws:assertAwsResourceProperty",
  "inputs": {
    "Service":"The official namespace of the service",
    "Api":"The API operation or method name",
    "API operation inputs or parameters":"A value",
    "PropertySelector": "Response object",
    "DesiredValues": [
      "Desired property values"
    ]
  }
}
```

サービス

実行する API オペレーションを含む AWS のサービスの名前空間。例えば、Systems Manager の名前空間は ssm です。Amazon EC2 の名前空間は ec2 です。サポートされている AWS のサービスの名前空間のリストは、 AWS CLI コマンドリファレンスの「Available Services (利用可能なサービス)」セクションを参照してください。

型: 文字列

必須: はい

Api

実行する API オペレーションの名前。API オペレーション (メソッド) は、以下の「サービスリファレンス」ページの左側のナビゲーションでサービスを選択することで表示できます。呼び出すサービスの [Client (クライアント)] セクションでメソッドを選択します。例えば、Amazon Relational Database Service (Amazon RDS) のすべての API オペレーション (メソッド) は、Amazon RDS メソッドのページに一覧表示されます。

型: 文字列

必須: はい

API オペレーション入力

1 つ以上の API オペレーションを入力します。使用できる入力 (パラメータ) は、以下の「サービスリファレンス」ページの左側のナビゲーションでサービスを選択することで表示できます。呼び出すサービスの [Client (クライアント)] セクションでメソッドを選択します。例えば、Amazon RDS のすべてのメソッドは、Amazon RDS メソッドページに一覧表示されています。describe_db_instances メソッドを選択し、下にスクロールして、[DBInstanceIdentifier]、[Name (名前)]、および [Values (値)] などの使用可能なパラメータを表示します。複数の入力を指定するには、次の形式を使用します。

YAML

```
inputs:
  Service: The official namespace of the service
  Api: The API operation name
  API input 1: A value
  API Input 2: A value
  API Input 3: A value
```

JSON

```
"inputs":{
      "Service":"The official namespace of the service",
      "Api":"The API operation name",
      "API input 1":"A value",
      "API Input 2":"A value",
      "API Input 3":"A value"
}
```

型: 選択した API オペレーションによって決まります

必須: はい

PropertySelector

応答オブジェクト内の特定の属性への JSONPath。レスポンスオブジェクトは、以下の「サービスリファレンス」ページの左側のナビゲーションでサービスを選択することで表示できます。呼び出すサービスの [Client (クライアント)] セクションでメソッドを選択します。例え

ば、Amazon RDS のすべてのメソッドは、Amazon RDS メソッドページに一覧表示されています。describe_db_instances メソッドを選択し、[Response Structure (レスポンス構造)] セクションまで下にスクロールします。[DBInstances] は応答オブジェクトとして表示されます。

型: 文字列

必須: はい

DesiredValues

予定の状態、またはオートメーションを継続する状態。ブール値を指定する場合は、True または False などのように大文字を使用する必要があります。

タイプ: StringList

必須: はい

aws:branch – 条件付きオートメーションステップを実行する

aws:branch アクションを使用すると、1 つのステップでさまざまな選択肢を評価し、その評価結果に基づいてランブックの別のステップにジャンプする、動的なオートメーションを作成できます。

ステップの aws:branch アクションを指定する場合、オートメーションが評価する必要のある Choices を指定します。Choices は、Runbook の Parameters セクションで指定した値、または前述のステップの出力として生成された動的値のいずれかをベースにすることができます。自動化は、ブール式を使用して各選択肢を評価します。最初の選択肢が true である場合、オートメーションはその選択肢に指定されたステップにジャンプします。最初の選択肢が false の場合、オートメーションは次の選択肢を評価します。オートメーションは、選択肢が true になるまで、各選択肢の評価を続けます。オートメーションは、true の選択肢に指定されたステップにジャンプします。

true の選択肢がない場合、オートメーションはステップに default 値が含まれているかどうかを確認します。デフォルト値は、true の選択肢がない場合にオートメーションがジャンプするステップを定義します。ステップに default 値が指定されていない場合、オートメーションはランブックの次のステップを処理します。

aws:branch アクションは、And、Not、および Or 演算子の組み合わせを使用して複雑な選択肢の評価をサポートします。サンプルのランブックや、さまざまな演算子を使用する例を含む aws:branch の使用方法については、「ランブックでの条件文の使用」を参照してください。

入力

ステップに 1 つ以上の Choices を指定します。Choices は、Runbook の Parameters セクションで指定した値、または前述のステップの出力として生成された動的値のいずれかをベースにすることができます。ここでは、パラメータを評価する YAML サンプルを示します。

```
mainSteps:
- name: chooseOS
  action: aws:branch
  inputs:
    Choices:
    - NextStep: runWindowsCommand
      Variable: "{{Name of a parameter defined in the Parameters section. For example:
 OS_name}}"
      StringEquals: windows
    - NextStep: runLinuxCommand
      Variable: "{{Name of a parameter defined in the Parameters section. For example:
 OS_name}}"
      StringEquals: linux
    Default:
      sleep3
```

前のステップからの出力を評価する YAML サンプルを示します。

```
mainSteps:
- name: chooseOS
  action: aws:branch
  inputs:
    Choices:
    - NextStep: runPowerShellCommand
      Variable: "{{Name of a response object. For example: GetInstance.platform}}"
      StringEquals: Windows
    - NextStep: runShellCommand
      Variable: "{{Name of a response object. For example: GetInstance.platform}}"
      StringEquals: Linux
    Default:
      sleep3
```

選択肢

次のステップを決定し処理する際に、自動化が評価する 1 つ以上の式。選択肢はブール式を使用して評価されます。各選択肢は、次のオプションを定義する必要があります。

- NextStep: 指定された選択肢が true である場合に処理する、Runbook の次のステップ。

- Variable: Runbook の `Parameters` セクションで定義されているパラメータの名前を指定します。または、Runbook の前述のステップからの出力オブジェクトを指定します。`aws:branch` の変数作成の詳細については、「出力変数の作成について」を参照してください。
- Operation: 選択肢を評価するために使用される基準。`aws:branch` アクションは、次の操作をサポートします。

  文字列演算子

  - StringEquals
  - EqualsIgnoreCase
  - StartsWith
  - EndsWith
  - Contains

  数値演算子

  - NumericEquals
  - NumericGreater
  - NumericLesser
  - NumericGreaterOrEquals
  - NumericLesser
  - NumericLesserOrEquals

  ブール演算子

  - BooleanEquals

  > **Important**
  > ランブックを作成すると、システムはランブック内の各オペレーションを検証します。オペレーションがサポートされていない場合は、ランブックの作成時にエラーが返されます。

デフォルト

true の `Choices` がない場合にオートメーションがジャンプするステップの名前。

オペレーション

型: 文字列

必須: いいえ

> **Note**
>
> aws:branch アクションは、And、Or、および Not 演算子をサポートします。演算子を使用する aws:branch の例については、「ランブックでの条件文の使用」を参照してください。

aws:changeInstanceState – インスタンスの状態を変更またはアサートする

インスタンスの状態を変更またはアサートします。

このアクションは、アサートモードで使用できます (API は実行して状態を変更することはしませんが、インスタンスが目的の状態であることを検証します)。アサートモードを使用するには、CheckStateOnly パラメータを true に設定します。このモードは、Windows で Sysprep (バックグラウンドで長期に実行できる非同期コマンド) を実行するときに役立ちます。Amazon Machine Image (AMI) を作成する前に、インスタンスが停止していることを確認できます。

> **Note**
>
> このアクションのデフォルトのタイムアウト値は 3600 秒 (1 時間) です。timeoutSeconds ステップで aws:changeInstanceState パラメータを指定して、タイムアウトを制限または延長することができます。

Input (入力)

YAML

```
name: stopMyInstance
action: aws:changeInstanceState
maxAttempts: 3
timeoutSeconds: 3600
onFailure: Abort
inputs:
  InstanceIds:
  - i-1234567890abcdef0
  CheckStateOnly: true
```

```
  DesiredState: stopped
```

JSON

```
{
    "name":"stopMyInstance",
    "action": "aws:changeInstanceState",
    "maxAttempts": 3,
    "timeoutSeconds": 3600,
    "onFailure": "Abort",
    "inputs": {
        "InstanceIds": ["i-1234567890abcdef0"],
        "CheckStateOnly": true,
        "DesiredState": "stopped"
    }
}
```

InstanceIds

インスタンスの ID。

タイプ: StringList

必須: はい

CheckStateOnly

false の場合、インスタンスの状態は目的の状態に設定されます。true の場合、ポーリングを使用して目的の状態をアサートします。

デフォルト: `false`

タイプ: ブール値

必須: いいえ

DesiredState

目的の状態。`running` に設定されている場合、このアクションは Amazon EC2 の状態が `Running`、インスタンスの状態が `OK`、および完了する前にシステム状態が `OK` になるのを待ちます。

型: 文字列

有効な値: `running` | `stopped` | `terminated`

必須: はい

Force

設定した場合、インスタンスが強制的に停止されます。インスタンスによって、ファイルシステムキャッシュまたはファイルシステムメタデータがフラッシュされることはありません。このオプションを使用する場合は、ファイルシステムのチェックと修復の手順を手動で実行する必要があります。このオプションは Windows Server の EC2 インスタンスにはお勧めしません。

タイプ: ブール値

必須: いいえ

AdditionalInfo

リザーブド。

型: 文字列

必須: いいえ

出力

なし

`aws:copyImage` — Amazon Machine Image のコピーまたは暗号化

任意の AWS リージョン から現在のリージョンに Amazon Machine Image (AMI) をコピーします。このアクションでは、新しい AMI を暗号化することもできます。

入力

このアクションでは、ほとんどの `CopyImage` パラメータがサポートされています。詳細については、「CopyImage」を参照してください。

次の例では、ソウルリージョンで AMI のコピーを作成します (`SourceImageID`: ami-0fe10819. `SourceRegion`: ap-northeast-2)。新しい AMI が、Automation アクションを開始したリージョンにコピーされます。オプションの `Encrypted` フラグが `true` に設定されているため、コピーされた AMI は暗号化されます。

YAML

```
name: createEncryptedCopy
action: aws:copyImage
maxAttempts: 3
onFailure: Abort
inputs:
  SourceImageId: ami-0fe10819
  SourceRegion: ap-northeast-2
  ImageName: Encrypted Copy of LAMP base AMI in ap-northeast-2
  Encrypted: true
```

JSON

```
{
    "name": "createEncryptedCopy",
    "action": "aws:copyImage",
    "maxAttempts": 3,
    "onFailure": "Abort",
    "inputs": {
        "SourceImageId": "ami-0fe10819",
        "SourceRegion": "ap-northeast-2",
        "ImageName": "Encrypted Copy of LAMP base AMI in ap-northeast-2",
        "Encrypted": true
    }
}
```

SourceRegion

ソース AMI が存在するリージョン。

型: 文字列

必須: はい

SourceImageId

ソースリージョンからコピーする AMI ID。

型: 文字列

必須: はい

ImageName

新しいイメージの名前。

型: 文字列

必須: はい

ImageDescription

ターゲットイメージの説明。

型: 文字列

必須: いいえ

暗号化された

ターゲット AMI を暗号化します。

タイプ: ブール値

必須: いいえ

KmsKeyId

コピーオペレーション中にイメージのスナップショットを暗号化するときに使用する AWS KMS key の Amazon リソースネーム (ARN)。詳細については、「CopyImage」を参照してください。

型: 文字列

必須: いいえ

ClientToken

リクエストのべき等のために割り当てる一意の識別子 (大文字と小文字を区別)。詳細については、「CopyImage」を参照してください。

型: 文字列

必須: いいえ

出力

ImageId

コピーされたイメージの ID。

ImageState

コピーされたイメージの状態。

有効な値: `available` | `pending` | `failed`

aws:createImage – Amazon マシンイメージ (AMI) を作成する

実行中、停止中、または停止済みのインスタンスから Amazon Machine Image (AMI) を作成し、`ImageState` が `available` になるまでポーリングします。

入力

このアクションでは、次の `CreateImage` パラメータがサポートされています。詳細については、「CreateImage」を参照してください

YAML

```
name: createMyImage
action: aws:createImage
maxAttempts: 3
onFailure: Abort
inputs:
  InstanceId: i-1234567890abcdef0
  ImageName: AMI Created on{{global:DATE_TIME}}
  NoReboot: true
  ImageDescription: My newly created AMI
```

JSON

```
{
    "name": "createMyImage",
    "action": "aws:createImage",
    "maxAttempts": 3,
    "onFailure": "Abort",
    "inputs": {
        "InstanceId": "i-1234567890abcdef0",
        "ImageName": "AMI Created on{{global:DATE_TIME}}",
        "NoReboot": true,
        "ImageDescription": "My newly created AMI"
    }
}
```

InstanceId

インスタンスの ID。

型: 文字列

必須: はい

ImageName

イメージの名前。

型: 文字列

必須: はい

ImageDescription

イメージの説明。

型: 文字列

必須: いいえ

NoReboot

ブールリテラルです。

デフォルトでは、Amazon Elastic Compute Cloud (Amazon EC2) はインスタンスをシャットダウンして再起動してからイメージを作成します。再起動しないオプションが `true` に設定されている場合、Amazon EC2 はイメージの作成前にインスタンスをシャットダウンしません。このオプションを使用すると、作成したイメージのファイルシステムの完全性は保証できません。

AMI を作成した後、そのイメージからインスタンスを実行しない場合、まず、`aws:changeInstanceState` – インスタンスの状態を変更またはアサートする アクションを使用してインスタンスを停止します。次に、[NoReboot] オプションを `true` に設定して、この `aws:createImage` アクションを使用します。

タイプ: ブール値

必須: いいえ

BlockDeviceMappings

インスタンスのブロックデバイス。

型: マップ

必須: いいえ

出力

ImageId

新しく作成したイメージの ID。

タイプ: 文字列。

ImageState

イメージの現在の状態。この状態が available の場合、イメージは正常に登録されており、インスタンスの作成に使用できます。

型: 文字列

aws:createStack – AWS CloudFormation スタックを作成する

テンプレートから AWS CloudFormation スタックを作成します。

CloudFormation スタックの作成に関する補足情報については、AWS CloudFormation API リファレンスの「CreateStack」を参照してください。

Input (入力)

YAML

```
name: makeStack
action: aws:createStack
maxAttempts: 1
onFailure: Abort
inputs:
  Capabilities:
  - CAPABILITY_IAM
  StackName: myStack
  TemplateURL: http://s3.amazonaws.com/amzn-s3-demo-bucket/myStackTemplate
  TimeoutInMinutes: 5
  Parameters:
    - ParameterKey: LambdaRoleArn
      ParameterValue: "{{LambdaAssumeRole}}"
    - ParameterKey: createdResource
      ParameterValue: createdResource-{{automation:EXECUTION_ID}}
```

JSON

```
{
    "name": "makeStack",
    "action": "aws:createStack",
    "maxAttempts": 1,
    "onFailure": "Abort",
    "inputs": {
        "Capabilities": [
            "CAPABILITY_IAM"
        ],
        "StackName": "myStack",
        "TemplateURL": "http://s3.amazonaws.com/amzn-s3-demo-bucket/
myStackTemplate",
        "TimeoutInMinutes": 5,
        "Parameters": [
          {
            "ParameterKey": "LambdaRoleArn",
            "ParameterValue": "{{LambdaAssumeRole}}"
          },
          {
            "ParameterKey": "createdResource",
            "ParameterValue": "createdResource-{{automation:EXECUTION_ID}}"
          }
    }
}
```

機能

CloudFormation が特定のスタックを作成する前に指定する値のリスト。一部のスタックテンプレートには、 のアクセス許可に影響するリソースが含まれますAWS アカウント このようなスタックの場合は、このパラメータを指定して、それらの機能を明示的に認識する必要があります。

有効な値は、CAPABILITY_IAM、CAPABILITY_NAMED_IAM、および CAPABILITY_AUTO_EXPAND です。

CAPABILITY_IAM および CAPABILITY_NAMED_IAM

IAM リソースがある場合、どちらの機能でも指定できます。カスタム名を持つ IAM リソースがある場合は、CAPABILITY_NAMED_IAM を指定する必要があります。このパラメータを指定しな

い場合、このアクションは InsufficientCapabilities エラーを返します。次のリソースでは、CAPABILITY_IAM または CAPABILITY_NAMED_IAM を指定する必要があります。

- AWS::IAM::AccessKey
- AWS::IAM::Group
- AWS::IAM::InstanceProfile
- AWS::IAM::Policy
- AWS::IAM::Role
- AWS::IAM::User
- AWS::IAM::UserToGroupAddition

スタックテンプレートにこのリソースが含まれている場合、これらに関連付けられるすべてのアクセス許可を確認して、必要時にはそのアクセス許可を編集することが推奨されます。

詳細については、「AWS CloudFormation テンプレートの IAM リソースの承認」を参照してください。

CAPABILITY_AUTO_EXPAND

一部のテンプレートにはマクロが含まれています。マクロはテンプレート上でカスタム処理を実行します。これには検索して置換操作のような単純なアクションからテンプレート全体の広範な変換までが含まれます。このためユーザーは通常、実際にスタックを作成する前に、マクロによって発生した変更を確認できるように、処理済みのテンプレートから変更セットを作成します。スタックテンプレートに 1 つ以上のマクロが含まれており、変更セットの結果を確認せずに、処理されたテンプレートから直接スタックを作成することを選択する場合、この機能を確認する必要があります。

詳細については、「AWS CloudFormation ユーザーガイド」の「AWS CloudFormation マクロを使用したテンプレートのカスタム処理の実行」を参照してください。

型: 文字列の配列

有効な値: CAPABILITY_IAM | CAPABILITY_NAMED_IAM | CAPABILITY_AUTO_EXPAND

必須: いいえ

ClientRequestToken

この CreateStack リクエストの一意の識別子。このステップで、maxAttempts に 1 より大きい値を設定する場合、このトークンを指定します。このトークンを指定することによって、同じ名前で新しいスタックの作成を試行していないことを CloudFormation が認識します。

型: 文字列

必須: いいえ

長さの制限: 最小長は 1 です。最大長は 128 です。

パターン: [a-zA-Z0-9][-a-zA-Z0-9]*

DisableRollback

スタックの作成に失敗した場合にスタックのロールバックをオフにするために、true を設定します。

条件付き: DisableRollback パラメータ、あるいは OnFailure パラメータのどちらかを指定できますが、両方を指定することはできません。

デフォルト: false

タイプ: ブール値

必須: いいえ

NotificationARNs

スタック関連イベントを発行する Amazon Simple Notification Service (Amazon SNS) トピックの ARN。Amazon SNS コンソール (https://console.aws.amazon.com/sns/v3/home) を使用して SNS トピック ARN を検索できます。

型: 文字列の配列

配列メンバー: 5 つの項目の最大数。

必須: いいえ

OnFailure

スタックの作成に失敗した場合に実行するアクションを決定します。DO_NOTHING、ROLLBACK または DELETE を指定する必要があります。

条件付き: OnFailure パラメータ、あるいは DisableRollback パラメータのどちらかを指定できますが、両方を指定することはできません。

デフォルト: ROLLBACK

型: 文字列

有効な値: DO_NOTHING | ROLLBACK | DELETE

必須: いいえ

パラメータ

スタック用の入力パラメータを指定する Parameter 構造のリスト。詳細については、「パラメータ」データタイプを参照してください。

タイプ:「パラメータ」オブジェクトの配列

必須: いいえ

ResourceTypes

作成したこのスタックアクションで動作するアクセス許可があるテンプレートリソースの種類。たとえば、AWS::EC2::Instance、AWS::EC2::*、または Custom::*MyCustomInstance* などです。次の構文を使用して、テンプレートリソースの種類を記述します。

- すべての AWS リソース用:

```
AWS::*
```

- すべてのカスタムリソース用:

```
Custom::*
```

- 特定のカスタムリソース用:

```
Custom::logical_ID
```

- 特定の AWS のサービスのすべてのリソース用:

```
AWS::service_name::*
```

- 特定の AWS リソース用:

```
AWS::service_name::resource_logical_ID
```

リソースの種類のリストに作成しているリソースが含まれていない場合、スタックの作成は失敗します。デフォルトでは、CloudFormation によりすべてのリソースタイプにアクセス許可が付与されます。IAM は、IAM ポリシーで CloudFormation 固有の条件キーにこのパラメータを使用し

ます。詳細については、「AWS Identity and Access Management を使用したユーザーアクセスの制御」を参照してください。

型: 文字列の配列

長さの制限: 最小長は 1 です。最大長は 256 です。

必須: いいえ

RoleARN

CloudFormation がスタックを作成するために引き受ける IAM ロールの Amazon リソースネーム (ARN)。CloudFormation は、ユーザーに代わって呼び出しを行うために、このロールの認証情報を使用します。CloudFormation は、このスタックにおけるこれからのすべてのオペレーションにこのロールを常に使用します。ユーザーにこのスタックで操作できるアクセス許可がある限り、ユーザーに渡す許可がない場合でも、CloudFormation はこのロールを使用します。ロールに最小限の特権が付与されていることを確認してください。

値を指定しない場合、CloudFormation は以前にこのスタックに関連付けられたロールを使用します。利用できるロールがない場合、CloudFormation はユーザー認証情報から生成される一時セッションを使用します。

型: 文字列

長さの制限: 最小長は 20 です。最大長は 2048 です。

必須: いいえ

StackName

スタックに関連付けられた名前。この名前は、作成しているスタックのリージョン内で一意であることが必要です。

> **Note**
>
> スタック名には、英数字 (大文字と小文字が区別されます) とハイフンのみを使用できます。先頭の文字はアルファベット文字である必要があります。また、128 文字より長くすることはできません。

型: 文字列

必須: はい

StackPolicyBody

スタックポリシー本文を含む構造。詳細については、「スタックのリソースが更新されないようにする」を参照してください。

条件付き: StackPolicyBody パラメータ、あるいは StackPolicyURL パラメータのどちらかを指定できますが、両方を指定することはできません。

型: 文字列

長さの制限: 最小長は 1 です。最大長は 16384 です。

必須: いいえ

StackPolicyURL

スタックポリシーを含むファイルの場所。URL は、スタックと同じリージョンにある S3 バケット内のポリシーを指定する必要があります。スタックポリシーに許可される最大のファイルサイズは 16 KB になります。

条件付き: StackPolicyBody パラメータ、あるいは StackPolicyURL パラメータのどちらかを指定できますが、両方を指定することはできません。

型: 文字列

長さの制限: 最小長は 1 です。最大長は 1350 です。

必須: いいえ

タグ

このスタックに関連付るキー値のペア。また、CloudFormation はスタックで作成されたリソースにこれらのタグを伝達します。最大で 10 個のタグを指定できます。

タイプ: 「タグ」オブジェクトの配列

必須: いいえ

TemplateBody

最少長が 1 バイトで最大長が 51,200 バイトのテンプレート本文がある構造。詳細については、「テンプレートの分析」を参照してください。

条件付き: TemplateBody パラメータ、あるいは TemplateURL パラメータのどちらかを指定できますが、両方を指定することはできません。

型: 文字列

長さの制限: 最小長は 1 です。

必須: いいえ

TemplateURL

テンプレート本文を含むファイルの場所。URL は、S3 バケット内にあるテンプレートを指定する必要があります。テンプレートに許可される最大サイズは 460,800 バイトです。詳細については、「テンプレートの分析」を参照してください。

条件付き: TemplateBody パラメータ、あるいは TemplateURL パラメータのどちらかを指定できますが、両方を指定することはできません。

型: 文字列

長さの制限: 最小長は 1 です。最大長は 1,024 です。

必須: いいえ

TimeoutInMinutes

スタックステータスが CREATE_FAILED になるまでに経過できる時間数。DisableRollback が設定されない、あるいは false に設定されている場合、スタックはロールバックされます。

タイプ: 整数

有効な範囲: 最小値 は 1 です。

必須 : いいえ

出力

StackId

スタックの一意の識別子です。

型: 文字列

StackStatus

スタックの現在のステータス。

型: 文字列

有効な値: CREATE_IN_PROGRESS | CREATE_FAILED | CREATE_COMPLETE | ROLLBACK_IN_PROGRESS | ROLLBACK_FAILED | ROLLBACK_COMPLETE | DELETE_IN_PROGRESS | DELETE_FAILED | DELETE_COMPLETE | UPDATE_IN_PROGRESS | UPDATE_COMPLETE_CLEANUP_IN_PROGRESS | UPDATE_COMPLETE | UPDATE_ROLLBACK_IN_PROGRESS | UPDATE_ROLLBACK_FAILED | UPDATE_ROLLBACK_COMPLETE_CLEANUP_IN_PROGRESS | UPDATE_ROLLBACK_COMPLETE | REVIEW_IN_PROGRESS

必須: はい

StackStatusReason

スタックステータスに関連付けられる成功あるいは失敗のメッセージ。

型: 文字列

必須: いいえ

詳細については、「CreateStack」を参照してください

セキュリティに関する考慮事項

aws:createStack アクションを使用できる前に、IAM オートメーションが継承するロールに次のポリシーを割り当てる必要があります。継承ロールの詳細については、「タスク 1: 自動化のサービスロールを作成する」を参照してください。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "sqs:*",
            "cloudformation:CreateStack",
            "cloudformation:DescribeStacks"
         ],
         "Resource":"*"
      }
   ]
}
```

aws:createTags – AWS リソースのタグを作成する

Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは AWS Systems Manager マネージドインスタンスの新しいタグを作成します。

入力

このアクションでは、ほとんどの Amazon EC2 `CreateTags` パラメータと Systems Manager `AddTagsToResource` パラメータがサポートされています。詳細については、「CreateTags」および「AddTagsToResource」を参照してください。

次の例は、Amazon Machine Image (AMI) とインスタンスに、特定の部門の本番稼働用リソースとしてタグを付ける方法を示しています。

YAML

```
name: createTags
action: aws:createTags
maxAttempts: 3
onFailure: Abort
inputs:
  ResourceType: EC2
  ResourceIds:
  - ami-9a3768fa
  - i-02951acd5111a8169
  Tags:
  - Key: production
    Value: ''
  - Key: department
    Value: devops
```

JSON

```
{
    "name": "createTags",
    "action": "aws:createTags",
    "maxAttempts": 3,
    "onFailure": "Abort",
    "inputs": {
        "ResourceType": "EC2",
        "ResourceIds": [
            "ami-9a3768fa",
```

```
            "i-02951acd5111a8169"
        ],
        "Tags": [
            {
                "Key": "production",
                "Value": ""
            },
            {
                "Key": "department",
                "Value": "devops"
            }
        ]
    }
}
```

ResourceIds

タグを付けるリソースの ID。リソースタイプが「EC2」でない場合、このフィールドは 1 つの項目のみを含むことができます。

型: 文字列のリスト

必須: はい

タグ

リソースに関連付けるタグ。

型: マップのリスト

必須: はい

ResourceType

タグを付けるリソースのタイプ。指定しない場合は、デフォルト値の「EC2」が使用されます。

型: 文字列

必須: いいえ

有効な値: `EC2` | `ManagedInstance` | `MaintenanceWindow` | `Parameter`

出力

なし

aws:deleteImage – Amazon Machine Image を削除する

指定された Amazon Machine Image (AMI) およびすべての関連するスナップショットを削除します。

入力

このアクションでは 1 つのパラメータのみがサポートされています。詳細については、DeregisterImage と DeleteSnapshot のドキュメントを参照してください。

YAML

```
name: deleteMyImage
action: aws:deleteImage
maxAttempts: 3
timeoutSeconds: 180
onFailure: Abort
inputs:
  ImageId: ami-12345678
```

JSON

```
{
    "name": "deleteMyImage",
    "action": "aws:deleteImage",
    "maxAttempts": 3,
    "timeoutSeconds": 180,
    "onFailure": "Abort",
    "inputs": {
        "ImageId": "ami-12345678"
    }
}
```

ImageId

削除するイメージの ID。

型: 文字列

必須: はい

出力

なし

`aws:deleteStack` – AWS CloudFormation スタックを削除する

AWS CloudFormation スタックを削除します。

Input (入力)

YAML

```
name: deleteStack
action: aws:deleteStack
maxAttempts: 1
onFailure: Abort
inputs:
  StackName: "{{stackName}}"
```

JSON

```
{
   "name":"deleteStack",
   "action":"aws:deleteStack",
   "maxAttempts":1,
   "onFailure":"Abort",
   "inputs":{
      "StackName":"{{stackName}}"
   }
}
```

ClientRequestToken

この DeleteStack リクエストの一意な識別子。お客様が同じ名前のスタックを削除しようとしていないと CloudFormation に認識させるためにリクエストを再試行する場合は、このトークンを指定します。DeleteStack リクエストを再試行して、CloudFormation がリクエストを受信したことを確認できます。

型: 文字列

長さの制限: 最小長は 1 です。最大長は 128 です。

パターン: [a-zA-Z][a-zA-Z0-9]*

必須: いいえ

RetainResources.member.N

この入力は、DELETE_FAILED 状態にあるスタックにのみ適用されます。お客様が保持したいリソースの論理リソース ID のリストです。削除中、CloudFormation はスタックを削除しますが、保持したリソースは削除しません。

空白でない S3 バケットなど、削除できないリソースは残すと便利ですが、スタックの削除が必要な場合もあります。

型: 文字列の配列

必須: いいえ

RoleARN

CloudFormation がスタックを作成するために引き受ける AWS Identity and Access Management (IAM) ロールの Amazon リソースネーム (ARN)。CloudFormation は、ユーザーに代わって呼び出しを行うために、このロールの認証情報を使用します。CloudFormation は、このスタックにおけるこれからのすべてのオペレーションにこのロールを常に使用します。ユーザーにこのスタックで操作できるアクセス許可がある限り、ユーザーに渡す許可がない場合でも、CloudFormation はこのロールを使用します。ロールに最小限の特権が付与されていることを確認してください。

値を指定しない場合、CloudFormation は以前にこのスタックに関連付けられたロールを使用します。利用できるロールがない場合、CloudFormation はユーザー認証情報から生成される一時セッションを使用します。

型: 文字列

長さの制限: 最小長は 20 です。最大長は 2048 です。

必須: いいえ

StackName

スタックと関連付けられている名前または一意のスタック ID。

型: 文字列

必須: はい

セキュリティに関する考慮事項

aws:deleteStack アクションを使用できる前に、IAM オートメーションが継承するロールに次のポリシーを割り当てる必要があります。継承ロールの詳細については、「タスク 1: 自動化のサービスロールを作成する」を参照してください。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "sqs:*",
            "cloudformation:DeleteStack",
            "cloudformation:DescribeStacks"
         ],
         "Resource":"*"
      }
   ]
}
```

aws:executeAutomation – 別のオートメーションを実行する

セカンダリの Runbook を呼び出して、セカンダリのオートメーションを実行します。このアクションを使用すると、最も一般的な操作のための Runbook を作成でき、オートメーションを実行するときにこれらの Runbook を参照できます。このアクションでは、同じような Runbook で重複したステップが不要になり、 Runbook を簡素化できます。

セカンダリのオートメーションは、プライマリのオートメーションを開始したユーザーのコンテキストで実行されます。つまり、セカンダリオートメーションでは、最初のオートメーションを開始したユーザーと同じ AWS Identity and Access Management (IAM) ロールまたはユーザーが使用されます。

> **Important**
>
> 継承ロール (iam:passRole ポリシーを使用するロール) を使用するセカンダリオートメーションでパラメータを指定する場合、プライマリオートメーションを開始したユーザーまたはロールには、セカンダリオートメーションで指定されたロールの継承を渡すアクセス許可が必要です。自動化のロールの継承のセットアップについては、「コンソールを使用して Automation 用のサービスロールを作成する」を参照してください。

Input (入力)

YAML

```
name: Secondary_Automation
action: aws:executeAutomation
maxAttempts: 3
timeoutSeconds: 3600
onFailure: Abort
inputs:
  DocumentName: secondaryAutomation
  RuntimeParameters:
    instanceIds:
    - i-1234567890abcdef0
```

JSON

```
{
   "name":"Secondary_Automation",
   "action":"aws:executeAutomation",
   "maxAttempts":3,
   "timeoutSeconds":3600,
   "onFailure":"Abort",
   "inputs":{
      "DocumentName":"secondaryAutomation",
      "RuntimeParameters":{
         "instanceIds":[
            "i-1234567890abcdef0"
         ]
      }
   }
}
```

DocumentName

ステップ中に実行するセカンダリ Runbook の名前。同じ AWS アカウント 内のランブックの場合は、ランブック名を指定します。別の AWS アカウント により共有されたランブックの場合は、ランブックの Amazon リソースネーム (ARN) を指定します。共有ランブックの使用については、「共有 SSM ドキュメントを使用する」を参照してください。

型: 文字列

必須: はい

DocumentVersion

実行するセカンダリ Runbook のバージョン。指定しない場合、Automation はデフォルトの Runbook バージョンで実行されます。

型: 文字列

必須: いいえ

MaxConcurrency

並列してこのタスクを実行できるターゲットの最大数。10 などの数値や、10% などの割合を指定できます。

タイプ: 文字列。

必須: いいえ

MaxErrors

追加のターゲットでオートメーションの実行を停止するまでに許容されるエラー数。エラーの絶対数 (10 など) またはターゲットセットのパーセント数 (10% など) を指定できます。たとえば、3 を指定すると、4 番目のエラーを受信した際に、システムはオートメーションの実行を停止します。値として 0 を指定した場合、最初のエラー結果が返されると、システムから他のターゲットでオートメーションが実行されなくなります。50 のリソースでオートメーションを実行し、`MaxErrors` を 10% に設定した場合、6 番目のエラーを受信すると、システムは追加ターゲットでオートメーションの実行を停止します。

`MaxErrors` のしきい値に達した時点で既に実行中のオートメーションについては完了を許可されますが、一部のオートメーションは失敗する可能性があります。失敗したオートメーションが指定された `MaxErrors` を上回っていないことを確認する必要がある場合は、`MaxConcurrency` を 1 に設定し、オートメーションが一度に 1 つずつ行われるようにします。

タイプ: 文字列。

必須: いいえ

RuntimeParameters

セカンダ Runbook の実行に必要なパラメータ。マッピングでは次の形式を使用します: {"parameter1" : "value1", "parameter2" : "value2" }

型: マップ

必須: いいえ

[タグ]

リソースに割り当てるオプションのメタデータ。オートメーション用に最大 5 つのタグを指定できます。

タイプ: MapList

必須: いいえ

TargetLocations

ロケーションとは、オートメーションを実行する AWS リージョン や AWS アカウント の組み合わせです。1 つ以上の項目を指定する必要があります。指定可能な最大数は 100 個です。このパラメータの値を指定すると、出力は親オートメーションには返されません。必要に応じて、子オートメーションから出力を取得するために、API オペレーションを後続で呼び出す必要があります。

タイプ: MapList

必須: いいえ

TargetMaps

ターゲットリソースに対するドキュメントパラメータのキー値マッピングのリスト。`Targets` と `TargetMaps` の両方を一緒に指定することはできません。

タイプ: MapList

必須: いいえ

TargetParameterName

レート制御されたオートメーションのターゲットリソースとして使用されるパラメータの名前。`Targets` を指定する場合は必須です。

タイプ: 文字列。

必須: いいえ

ターゲット

ターゲットリソースへのキー値マッピングのリスト。`TargetParameterName` を指定する場合は必須です。

タイプ: MapList

必須: いいえ

Output

Output

セカンダリオートメーションによって生成される出力。この出力は、次の形式を使って参照できます: ############.Output

タイプ: StringList

以下はその例です。

```
- name: launchNewWindowsInstance
  action: 'aws:executeAutomation'
  onFailure: Abort
  inputs:
    DocumentName: launchWindowsInstance
  nextStep: getNewInstanceRootVolume
- name: getNewInstanceRootVolume
  action: 'aws:executeAwsApi'
  onFailure: Abort
  inputs:
    Service: ec2
    Api: DescribeVolumes
    Filters:
    - Name: attachment.device
      Values:
      - /dev/sda1
    - Name: attachment.instance-id
      Values:
      - '{{launchNewWindowsInstance.Output}}'
  outputs:
  - Name: rootVolumeId
    Selector: '$.Volumes[0].VolumeId'
    Type: String
  nextStep: snapshotRootVolume
- name: snapshotRootVolume
  action: 'aws:executeAutomation'
  onFailure: Abort
  inputs:
    DocumentName: AWS-CreateSnapshot
    RuntimeParameters:
```

```
    VolumeId:
    - '{{getNewInstanceRootVolume.rootVolumeId}}'
    Description:
    - 'Initial root snapshot for {{launchNewWindowsInstance.Output}}'
```

ExecutionId

セカンダリオートメーションの ID。

型: 文字列

ステータス

セカンダリオートメーションのステータス。

タイプ: 文字列

`aws:executeAwsApi` — AWS API オペレーションの呼び出しと実行

AWS API オペレーションを呼び出し、実行します。API 操作のほとんどはサポートされていますが、すべての API オペレーションがテストされているわけではありません。GetObject オペレーションなどのストリーミング API オペレーションはサポートされていません。使用する API オペレーションがストリーミングオペレーションかどうかわからない場合は、サービスの「Boto3」ドキュメントを参照して、API でストリーミング入力または出力が必要かどうかを確認してください。このアクションで使用される Boto3 のバージョンは定期的に更新されます。ただし、新しい Boto3 バージョンのリリース後、変更がこのアクションに反映されるまでに最大で数週間かかる場合があります。各 `aws:executeAwsApi` アクションは、最大 25 秒間実行できます。このアクションの使用例については、「その他のランブックの例」を参照してください。

入力

入力は、選択した API オペレーションによって定義されます。

YAML

```
action: aws:executeAwsApi
inputs:
  Service: The official namespace of the service
  Api: The API operation or method name
  API operation inputs or parameters: A value
outputs: # These are user-specified outputs
- Name: The name for a user-specified output key
  Selector: A response object specified by using jsonpath format
```

```
  Type: The data type
```

JSON

```
{
   "action":"aws:executeAwsApi",
   "inputs":{
      "Service":"The official namespace of the service",
      "Api":"The API operation or method name",
      "API operation inputs or parameters":"A value"
   },
   "outputs":[ These are user-specified outputs
      {
         "Name":"The name for a user-specified output key",
         "Selector":"A response object specified by using JSONPath format",
         "Type":"The data type"
      }
   ]
}
```

サービス

実行する API オペレーションを含む AWS のサービスの名前空間。サポートされている AWS のサービスの名前空間のリストは、AWS SDK for Python (Boto3) の利用可能なサービスを参照してください。名前空間は、[クライアント] セクションにあります。例えば、Systems Manager の名前空間は `ssm` です。Amazon Elastic Compute Cloud (Amazon EC2) の名前空間は、`ec2` です。

型: 文字列

必須: はい

Api

実行する API オペレーションの名前。API オペレーション (メソッド) は、以下の「サービスリファレンス」ページの左側のナビゲーションでサービスを選択することで表示できます。呼び出すサービスの [Client (クライアント)] セクションでメソッドを選択します。例えば、Amazon Relational Database Service (Amazon RDS) のすべての API オペレーション (メソッド) は、Amazon RDS メソッドのページに一覧表示されます。

型: 文字列

必須: はい

API オペレーション入力

1 つ以上の API オペレーションを入力します。使用できる入力 (パラメータ) は、以下の「サービスリファレンス」ページの左側のナビゲーションでサービスを選択することで表示できます。呼び出すサービスの [Client (クライアント)] セクションでメソッドを選択します。例えば、Amazon RDS のすべてのメソッドは、Amazon RDS メソッドページに一覧表示されています。describe_db_instances メソッドを選択し、下にスクロールして、[DBInstanceIdentifier]、[Name (名前)]、および [Values (値)] などの使用可能なパラメータを表示します。

YAML

```
inputs:
  Service: The official namespace of the service
  Api: The API operation name
  API input 1: A value
  API Input 2: A value
  API Input 3: A value
```

JSON

```
"inputs":{
      "Service":"The official namespace of the service",
      "Api":"The API operation name",
      "API input 1":"A value",
      "API Input 2":"A value",
      "API Input 3":"A value"
}
```

型: 選択した API オペレーションによって決まります

必須: はい

出力

出力は、選択した API オペレーションからの応答に基づいてユーザーによって指定されます。

名前

出力の名前。

型: 文字列

必須: はい

Selector

応答オブジェクト内の特定の属性への JSONPath。レスポンスオブジェクトは、以下の「サービスリファレンス」ページの左側のナビゲーションでサービスを選択することで表示できます。呼び出すサービスの [Client (クライアント)] セクションでメソッドを選択します。例えば、Amazon RDS のすべてのメソッドは、Amazon RDS メソッドページに一覧表示されています。describe_db_instances メソッドを選択し、[Response Structure (レスポンス構造)] セクションまで下にスクロールします。[DBInstances] は応答オブジェクトとして表示されます。

型: 整数型、ブール型、文字列型、StringList、StringMap、または MapList

必須: はい

タイプ

レスポンス要素のデータ型。

型: 可変

必須: はい

`aws:executeScript` – スクリプトを実行する

指定されたランタイムとハンドラを使用して、提供された Python または PowerShell スクリプトを実行します。各 `aws:executeScript` アクションは、最大 600 秒 (10 分) 実行できます。`timeoutSeconds` ステップで `aws:executeScript` パラメータを指定して、タイムアウトを制限または延長することができます。

関数でリターンステートメントを使用して、出力ペイロードに出力を追加します。`aws:executeScript` アクションの出力の定義例については、「例 2: スクリプト化されたランブック」を参照してください。ランブック内にある `aws:executeScript` アクションからの出力は、指定した Amazon CloudWatch Logs ロググループに送信することもできます。詳しくは、「CloudWatch Logs を使用した自動アクション出力のログ記録」を参照してください。

`aws:executeScript` アクションからの出力を CloudWatch Logs に送信する場合、または `aws:executeScript` アクションに指定するスクリプトが AWS API オペレーションを呼び出す場合、ランブックを実行するには AWS Identity and Access Management (IAM) サービスロール (または引き受けロール) が常に必要です。

`aws:executeScript` アクションには、次のプレインストールされた PowerShell Core モジュールが含まれています。

- Microsoft.PowerShell.Host
- Microsoft.PowerShell.Management
- Microsoft.PowerShell.Security
- Microsoft.PowerShell.Utility
- PackageManagement
- PowerShellGet

プレインストールされていない PowerShell Core モジュールを使用するには、次のコマンドに示すように、スクリプトで `-Force` フラグを使用してモジュールをインストールする必要があります。`AWSPowerShell.NetCore` モジュールはサポートされていません。インストールするモジュールの *`ModuleName`* を置き換えます。

```
Install-Module ModuleName -Force
```

スクリプトで PowerShell Core コマンドレットを使用するには、次のコマンドに示すように、`AWS.Tools` モジュールを使用することをお勧めします。各*`##############`*をユーザー自身の情報に置き換えます。

- Amazon S3 コマンドレット。

```
Install-Module AWS.Tools.S3 -Force
Get-S3Bucket -BucketName amzn-s3-demo-bucket
```

- Amazon EC2 コマンドレット。

```
Install-Module AWS.Tools.EC2 -Force
Get-EC2InstanceStatus -InstanceId instance-id
```

- 共通またはサービスに依存しない AWS Tools for Windows PowerShell コマンドレット。

```
Install-Module AWS.Tools.Common -Force
Get-AWSRegion
```

スクリプトで PowerShell Core コマンドレットを使用するだけでなく、新しいオブジェクトを初期化する場合は、次のコマンドに示すように、モジュールもインポートする必要があります。

```
Install-Module AWS.Tools.EC2 -Force
```

```
Import-Module AWS.Tools.EC2

$tag = New-Object Amazon.EC2.Model.Tag
$tag.Key = "Tag"
$tag.Value = "TagValue"

New-EC2Tag -Resource i-02573cafcfEXAMPLE -Tag $tag
```

AWS.Tools モジュールのインストールとインポートの例、およびランブックにある PowerShell Core コマンドレットの使用例については、「オートメーションランブックのビジュアルデザインエクスペリエンス」を参照してください 。

Input

スクリプトを実行するために必要な情報を入力します。各###############をユーザー自身の情報に置き換えます。

> **Note**
>
> Python スクリプトの添付ファイルは、.py ファイルでも、スクリプトを含む .zip ファイルでもかまいません。PowerShell スクリプトは .zip ファイルに保存する必要があります。

YAML

```
action: "aws:executeScript"
inputs:
 Runtime: runtime
 Handler: "functionName"
 InputPayload:
  scriptInput: '{{parameterValue}}'
 Script: |-
   def functionName(events, context):
   ...
 Attachment: "scriptAttachment.zip"
```

JSON

```
{
    "action": "aws:executeScript",
```

```
    "inputs": {
        "Runtime": "runtime",
        "Handler": "functionName",
        "InputPayload": {
            "scriptInput": "{{parameterValue}}"
        },
        "Attachment": "scriptAttachment.zip"
    }
}
```

ランタイム

提供されたスクリプトを実行するために使用されるランタイム言語。aws:executeScript は Python 3.7 (python3.7)、Python 3.8 (python3.8)、Python 3.9 (python3.9)、Python 3.10 (python3.10)、Python 3.11 (python3.11)、PowerShell Core 6.0 (dotnetcore2.1)、PowerShell 7.0 (dotnetcore3.1) スクリプトをサポートしています。

サポートされる値: **python3.7** | **python3.8** | **python3.9** | **python3.10** | **python3.11** | **PowerShell Core 6.0** | **PowerShell 7.0**

タイプ: 文字列

必須: はい

> **Note**
>
> Python ランタイムの場合、環境は 512MB のメモリと 512MB のディスク容量を提供します。PowerShell ランタイムの場合、環境は 1,024 MB のメモリと 512 MB のディスク容量を提供します。

Handler

関数の名前。ハンドラで定義された関数に、events と context の 2 つのパラメータがあることを確認する必要があります。PowerShell ランタイムはこのパラメータをサポートしていません。

タイプ: 文字列

必須: はい (Python) | サポートされていません (PowerShell)

InputPayload

ハンドラの最初のパラメータに渡される JSON または YAML オブジェクト。これは、スクリプトに入力データを渡すために使用できます。

型: 文字列

必須: いいえ

Python

```
description: Tag an instance
schemaVersion: '0.3'
assumeRole: '{{AutomationAssumeRole}}'
parameters:
    AutomationAssumeRole:
        type: String
        description: '(Required) The Amazon Resource Name (ARN) of the IAM role
 that allows Automation to perform the actions on your behalf. If no role is
 specified, Systems Manager Automation uses your IAM permissions to operate this
 runbook.'
    InstanceId:
        type: String
        description: (Required) The ID of the EC2 instance you want to tag.
mainSteps:
  - name: tagInstance
    action: 'aws:executeScript'
    inputs:
        Runtime: "python3.11"
        Handler: tagInstance
        InputPayload:
            instanceId: '{{InstanceId}}'
        Script: |-
          def tagInstance(events,context):
            import boto3

            #Initialize client
            ec2 = boto3.client('ec2')
            instanceId = events['instanceId']
            tag = {
                "Key": "Env",
                "Value": "ExamplePython"
            }
            print(f"Adding tag {tag} to instance id {instanceId}")
```

```
            ec2.create_tags(
                Resources=[instanceId],
                Tags=[tag]
            )
            return tag
    outputs:
      - Type: String
        Name: TagKey
        Selector: $.Payload.Key
outputs:
  - tagInstance.TagKey
```

PowerShell

```
description: Tag an instance
schemaVersion: '0.3'
assumeRole: '{{AutomationAssumeRole}}'
parameters:
  AutomationAssumeRole:
    type: String
    description: (Required) The Amazon Resource Name (ARN) of the IAM role
 that allows Automation to perform the actions on your behalf. If no role is
 specified, Systems Manager Automation uses your IAM permissions to operate this
 runbook.
  InstanceId:
    type: String
    description: (Required) The ID of the EC2 instance you want to tag.
mainSteps:
  - name: tagInstance
    action: aws:executeScript
    isEnd: true
    inputs:
      Runtime: PowerShell 7.0
      InputPayload:
        instanceId: '{{InstanceId}}'
      Script: |-
        Install-Module AWS.Tools.EC2 -Force
        Import-Module AWS.Tools.EC2

        $input = $env:InputPayload | ConvertFrom-Json

        $tag = New-Object Amazon.EC2.Model.Tag
        $tag.Key = "Env"
```

```
        $tag.Value = "ExamplePowerShell"

        Write-Information "Adding tag key: $($tag.Key) and value: $($tag.Value)
 to instance id $($input.instanceId)"
        New-EC2Tag -Resource $input.instanceId -Tag $tag

        return $tag
    outputs:
      - Type: String
        Name: TagKey
        Selector: $.Payload.Key
outputs:
  - tagInstance.TagKey
```

Script

オートメーションで実行する埋め込みスクリプト。

タイプ: 文字列

必須: いいえ (Python) | はい (PowerShell)

Attachment

アクションによって呼び出すことができるスタンドアロンスクリプトファイルまたは .zip ファイルの名前。`Attachments` のリクエストパラメータで指定したドキュメント添付ファイルの `Name` と同じ値を指定します。詳細については、「AWS Systems Manager API リファレンス」の「Attachments」(アタッチメント) を参照してください。アタッチメントを使用してスクリプトを提供する場合は、ランブックのトップレベル要素にある `files` セクションも定義する必要があります。詳しくは、「スキーマバージョン 0.3」を参照してください。

Python 用のファイルを呼び出すには、`filename.method_name` の `Handler` 形式を使用します。

> **Note**
>
> Python スクリプトの添付ファイルは、.py ファイルでも、スクリプトを含む .zip ファイルでもかまいません。PowerShell スクリプトは .zip ファイルに保存する必要があります。

添付ファイルに Python ライブラリを含める場合は、各モジュールディレクトリに空の `__init__.py` ファイルを追加することをお勧めします。これにより、スクリプトコンテンツ内の添付ファイルのライブラリからモジュールをインポートできます。例: `from library import module`

型: 文字列

必須: いいえ

Output

ペイロード

関数によって返されるオブジェクトの JSON 形式です。最大 100KB が返されます。リストを出力する場合、最大 100 個の項目が返されます。

`aws:executeStateMachine` – AWS Step Functions ステートマシンを実行する

AWS Step Functions ステートマシンを実行します。

Input (入力)

このアクションでは、Step Functions StartExecution API オペレーションのほとんどのパラメータがサポートされています。

必要な AWS Identity and Access Management (IAM) アクセス許可

- `states:DescribeExecution`
- `states:StartExecution`
- `states:StopExecution`

YAML

```
name: executeTheStateMachine
action: aws:executeStateMachine
inputs:
  stateMachineArn: StateMachine_ARN
  input: '{"parameters":"values"}'
  name: name
```

JSON

```
{
    "name": "executeTheStateMachine",
    "action": "aws:executeStateMachine",
    "inputs": {
        "stateMachineArn": "StateMachine_ARN",
        "input": "{\"parameters\":\"values\"}",
        "name": "name"
    }
}
```

stateMachineArn

Step Functions ステートマシンの Amazon Resource Name (ARN)。

型: 文字列

必須: はい

name

実行の名前。

型: 文字列

必須: いいえ

input

実行に必要な JSON 入力データを含む文字列。

型: 文字列

必須: いいえ

出力

このアクションでは、以下の出力が事前に定義されています。

executionArn

実行の ARN。

型: 文字列

input

実行の入力データ (JSON) を含む文字列。このデータ長は、ペイロードのサイズにより制約を受け、UTF-8 エンコーディングによりバイト数で表現されます。

型: 文字列

name

実行の名前。

型: 文字列

output

実行の出力データ (JSON)。このデータ長は、ペイロードのサイズにより制約を受け、UTF-8 エンコーディングによりバイト数で表現されます。

型: 文字列

startDate

実行が開始された日付。

型: 文字列

stateMachineArn

実行されたステートマシンの ARN。

型: 文字列

status

実行に関する現在の状態。

型: 文字列

stopDate

実行がすでに終了している場合の、その実行が停止した日付。

型: 文字列

`aws:invokeWebhook` – オートメーションのウェブフック統合を呼び出す

オートメーションでウェブフック統合を指定して呼び出します。オートメーションのランブックの作成については、「Automation 向けのウェブフック統合の作成」を参照してください。

> **Note**
>
> `aws:invokeWebhook` アクションを使用するには、ユーザーまたはサービスロールが、以下のアクションを許可している必要があります。
>
> - ssm:GetParameter
> - kms:Decrypt
>
> AWS Key Management Service (AWS KMS) `Decrypt` オペレーションに対するアクセス許可が必要になるのは、カスタマー管理キーを使用して統合のパラメータを暗号化する場合のみです。

入力

呼び出すオートメーション統合の情報を入力します。

YAML

```
action: "aws:invokeWebhook"
inputs:
 IntegrationName: "exampleIntegration"
 Body: "Request body"
```

JSON

```
{
    "action": "aws:invokeWebhook",
    "inputs": {
        "IntegrationName": "exampleIntegration",
        "Body": "Request body"
    }
}
```

IntegrationName

オートメーション統合の名前。例えば、exampleIntegration と指定します。指定できるのは、既に存在している統合のみです。

タイプ: 文字列。

必須: はい

[Body] (本文)

ウェブフック統合が呼び出された際に送信するペイロード。

タイプ: 文字列。

必須: いいえ

出力

レスポンス

ウェブフックプロバイダーの応答から受信したテキスト。

ResponseCode

ウェブフックプロバイダーの応答から受信した HTTP ステータスコード。

aws:invokeLambdaFunction – AWS Lambda 関数を呼び出す

指定した AWS Lambda 関数を呼び出します。

> **Note**
>
> 各 aws:invokeLambdaFunction アクションは、最大 300 秒 (5 分) 実行できます。timeoutSeconds ステップで aws:invokeLambdaFunction パラメータを指定して、タイムアウトを制限または延長することができます。

Input

このアクションでは、Lambda サービスのほとんどの呼び出しパラメータがサポートされています。詳細については、「起動」を参照してください。

YAML

```
name: invokeMyLambdaFunction
action: aws:invokeLambdaFunction
maxAttempts: 3
timeoutSeconds: 120
onFailure: Abort
inputs:
  FunctionName: MyLambdaFunction
```

JSON

```
{
    "name": "invokeMyLambdaFunction",
    "action": "aws:invokeLambdaFunction",
    "maxAttempts": 3,
    "timeoutSeconds": 120,
    "onFailure": "Abort",
    "inputs": {
        "FunctionName": "MyLambdaFunction"
    }
}
```

FunctionName

Lambda 関数の名前。必須の関数です。

型: 文字列

必須: はい

Qualifier

関数のバージョンまたはエイリアス名。

型: 文字列

必須: いいえ

InvocationType

呼び出しタイプ。デフォルト値は RequestResponse です。

型: 文字列

有効な値: `Event` | `RequestResponse` | `DryRun`

必須: いいえ

LogType

デフォルト値が `Tail` の場合、呼び出しタイプは `RequestResponse` である必要があります。Lambda は、Lambda 関数で生成されたログデータの最後の 4 KB を base64 でエンコードして返します。

型: 文字列

有効な値: `None` | `Tail`

必須: いいえ

ClientContext

クライアント固有の情報。

必須: いいえ

InputPayload

ハンドラの最初のパラメータに渡される JSON または YAML オブジェクト。この入力を使用して、関数にデータを渡すことができます。この入力は、従来の `Payload` 入力よりもより高い柔軟性とサポート性を提供します。アクションで `InputPayload` と `Payload` の両方を定義する場合、`InputPayload` が優先され、`Payload` 値は使用されません。

型: StringMap

必須: いいえ

ペイロード

ハンドラの最初のパラメータに渡される JSON 文字列。これを使用して、関数に入力データを渡すことができます。追加機能では `InputPayload` 入力を使用することをお勧めします。

タイプ: 文字列

必須: いいえ

Output

StatusCode

HTTP ステータスコード

FunctionError

エラーが存在する場合、関数の実行中にエラーが発生したことを示します。エラーの詳細は、レスポンスペイロードに含まれています。

LogResult

Lambda 関数の呼び出しに対して base64 でエンコードされたログ。ログが存在するのは、呼び出しタイプが RequestResponse で、ログがリクエストされた場合のみです。

Payload

Lambda 関数によって返されるオブジェクトの JSON 形式。ペイロードは、呼び出しタイプが RequestResponse の場合にのみ存在します。

以下は、aws:invokeLambdaFunction アクションから出力を参照する方法を示した AWS-PatchInstanceWithRollback ランブックの一部です。

YAML

```
- name: IdentifyRootVolume
  action: aws:invokeLambdaFunction
  inputs:
    FunctionName: "IdentifyRootVolumeLambda-{{automation:EXECUTION_ID}}"
    Payload: '{"InstanceId": "{{InstanceId}}"}'
- name: PrePatchSnapshot
  action: aws:executeAutomation
  inputs:
    DocumentName: "AWS-CreateSnapshot"
    RuntimeParameters:
      VolumeId: "{{IdentifyRootVolume.Payload}}"
      Description: "ApplyPatchBaseline restoration case contingency"
```

JSON

```
{
    "name": "IdentifyRootVolume",
    "action": "aws:invokeLambdaFunction",
```

```
    "inputs": {
      "FunctionName": "IdentifyRootVolumeLambda-{{automation:EXECUTION_ID}}",
      "Payload": "{\"InstanceId\": \"{{InstanceId}}\"}"
    }
  },
  {
    "name": "PrePatchSnapshot",
    "action": "aws:executeAutomation",
    "inputs": {
      "DocumentName": "AWS-CreateSnapshot",
      "RuntimeParameters": {
        "VolumeId": "{{IdentifyRootVolume.Payload}}",
        "Description": "ApplyPatchBaseline restoration case contingency"
      }
    }
  }
```

aws:loop — オートメーション内のステップを反復処理します。

このアクションは、オートメーションランブック内のステップのサブセットを反復処理します。do while または for each スタイルループを選択できます。do while ループを作成するには、LoopCondition 入力パラメーターを使用します。for each ループを作成するには、Iterators と IteratorDataType 入力パラメーターを使用します。aws:loop アクションを使用するときは、Iterators または LoopCondition 入力パラメータのみを指定してください。最大反復回数は 100 です。

onCancel プロパティを使用できるのは、ループ内で定義されたステップのみです。onCancel プロパティは aws:loop アクションではサポートされていません。aws:loop アクションに onFailure プロパティを使用することはできますが、これが使用されるのは、ステップを失敗させる予期しないエラーが発生した場合のみです。ループ内のステップに onFailure プロパティを定義すると、aws:loop アクションがこれらのプロパティを継承し、失敗した場合に適切に対応します。

例

さまざまなタイプのループアクションの作成方法の例を以下に示します。

do while

```
name: RepeatMyLambdaFunctionUntilOutputIsReturned
action: aws:loop
```

```
inputs:
    Steps:
    - name: invokeMyLambda
        action: aws:invokeLambdaFunction
        inputs:
        FunctionName: LambdaFunctionName
        outputs:
        - Name: ShouldRetry
            Selector: $.Retry
            Type: Boolean
    LoopCondition:
        Variable: "{{ invokeMyLambda.ShouldRetry }}"
        BooleanEquals: true
    MaxIterations: 3
```

for each

```
name: stopAllInstancesWithWaitTime
action: aws:loop
inputs:
    Iterators: "{{ DescribeInstancesStep.InstanceIds }}"
    IteratorDataType: "String"
    Steps:
    - name: stopOneInstance
        action: aws:changeInstanceState
        inputs:
        InstanceIds:
            - "{{stopAllInstancesWithWaitTime.CurrentIteratorValue}}"
        CheckStateOnly: false
        DesiredState: stopped
    - name: wait10Seconds
        action: aws:sleep
        inputs:
        Duration: PT10S
```

入力

入力は次のとおりです。

イテレーター

ステップを反復処理する項目のリスト。最大反復回数は 100 です。

タイプ: StringList

必須：いいえ

イテレータ/データタイプ

Iterators のデータ型を指定するオプションのパラメータ。このパラメータの値は、Iterators 入力パラメータとともに提供できます。このパラメータ値と Iterators を指定しない場合、LoopCondition パラメータ値を指定する必要があります。

型: 文字列

有効な値: ブール値 | 整数 | 文字列 | StringMap

デフォルト: 文字列

必須：いいえ

ループ条件

Variable と評価する演算子条件で構成されます。このパラメータ値を指定しない場合、Iterators と IteratorDataType パラメータ値を指定する必要があります。And、Not と Or 演算子の組み合わせを使用して、複雑な演算子の評価を使用できます。条件はループ内のステップが完了した後に評価されます。条件が true で、MaxIterations 値に達していない場合は、ループ内のステップが再び実行されます。オペレータの条件は以下のとおりです。

文字列演算子

- StringEquals
- EqualsIgnoreCase
- StartsWith
- EndsWith
- Contains

数値演算子

- NumericEquals
- NumericGreater
- NumericLesser
- NumericGreaterOrEquals
- NumericLesser
- NumericLesserOrEquals

ブール演算子

- BooleanEquals

型: StringMap

必須：いいえ

最大反復回数

ループ内のステップの最大実行回数。この入力に指定された値に達すると、LoopCondition が true でも、または Iterators パラメータにオブジェクトが残っていても、ループの実行は停止します。

型: 整数

有効な値: 1 ~ 100

必須：いいえ

ステップ

ループで実行するステップのリスト。これらはネストされたランブックのように機能します。これらのステップでは、{{loopStepName.CurrentIteratorValue}} 構文を使用して for each ループの現在のイテレーター値にアクセスできます。{{loopStepName.CurrentIteration}} 構文を使用して、両方のループタイプの現在の反復の整数値にアクセスすることもできます。

タイプ: ステップのリスト

必須: はい

出力

CurrentIteration

現在のループ反復を整数で表したもの。反復値は 1 から始まります。

型: 整数

現在のイテレータ値

現在のイテレータの値を文字列で表したもの。この出力は for each ループ内にのみ存在します。

型: 文字列

aws:pause – オートメーションを一時停止する

このアクションは、オートメーションを一時停止します。一時停止されると、オートメーションのステータスは [待機中] になります。オートメーションを続行するには、Resume シグナルタイプの SendAutomationSignal API オペレーションを使用します。ワークフローをよりきめ細かく制御する場合、aws:sleep または aws:approve アクションを使用することをお勧めします。

> **Note**
>
> このアクションのデフォルトのタイムアウトは 7 日間 (604800 秒) で、最大値は 30 日間 (2592000 秒) です。timeoutSeconds ステップで aws:pause パラメータを指定して、タイムアウトを制限または延長することができます。

Input

入力は次のとおりです。

YAML

```
name: pauseThis
action: aws:pause
timeoutSeconds: 1209600
inputs: {}
```

JSON

```
{
    "name": "pauseThis",
    "action": "aws:pause",
    "timeoutSeconds": "1209600",
    "inputs": {}
}
```

Output

なし

aws:runCommand – マネージドインスタンスでコマンドを実行する

指定されたコマンドを実行します。

> **Note**
>
> オートメーションは、1 つの AWS Systems Manager Run Command アクションの出力のみをサポートします。Runbook には、複数の Run Command アクションを含めることができますが、出力がサポートされるのは一度に 1 つのアクションに対してのみです。

Input

このアクションでは、ほとんどの Send Command パラメータがサポートされています。詳細については、「SendCommand」を参照してください。

YAML

```
- name: checkMembership
  action: 'aws:runCommand'
  inputs:
    DocumentName: AWS-RunPowerShellScript
    InstanceIds:
      - '{{InstanceIds}}'
    Parameters:
      commands:
        - (Get-WmiObject -Class Win32_ComputerSystem).PartOfDomain
```

JSON

```
{
    "name": "checkMembership",
    "action": "aws:runCommand",
    "inputs": {
        "DocumentName": "AWS-RunPowerShellScript",
        "InstanceIds": [
            "{{InstanceIds}}"
        ],
        "Parameters": {
            "commands": [
                "(Get-WmiObject -Class Win32_ComputerSystem).PartOfDomain"
            ]
```

```
        }
    }
}
```

DocumentName

コマンドタイプドキュメントの所有者が、お客様または AWS の場合は、ドキュメントの名前を指定します。別の AWS アカウント から共有されたドキュメントを使用している場合は、そのドキュメントの Amazon リソースネーム (ARN) を指定します。共有ドキュメントの使用方法については、「共有 SSM ドキュメントを使用する」を参照してください。

型: 文字列

必須: はい

InstanceIds

コマンドを実行するインスタンス ID です。最大 50 の ID を指定できます。

インスタンス ID の代わりに擬似パラメータ {{RESOURCE_ID}} を使用して、ターゲットグループ内のすべてのインスタンスでコマンドを実行することもできます。擬似パラメーターの詳細については、「メンテナンスウィンドウのタスクを登録する際の疑似パラメータの使用」を参照してください。

他に、Targets パラメータを使用して、コマンドをインスタンスのフリートに送信する方法もあります。Targets パラメータは、Amazon Elastic Compute Cloud (Amazon EC2) タグを受け入れます。Targets パラメータの使用方法の詳細については、「コマンドを大規模に実行する」を参照してください。

タイプ: StringList

必須: いいえ (InstanceId を指定しない場合、または {{RESOURCE_ID}} 擬似パラメータを使用する場合は、Targets パラメータを指定する必要があります)。

ターゲット

指定した Key、Value の組み合わせを使用してインスタンスを対象とする検索条件の配列です。呼び出しにインスタンス ID を 1 つも指定しない場合は、Targets が必要です。Targets パラメータの使用方法の詳細については、「コマンドを大規模に実行する」を参照してください。

タイプ: MapList (リスト内のマップのスキーマはオブジェクトと一致する必要があります)。詳細については、AWS Systems Manager API リファレンスの「ターゲット」を参照してください。

必須: いいえ (Targets を指定しない場合は、InstanceId を指定するか、{{RESOURCE_ID}} 擬似パラメータを使用する必要があります)。

次に例を示します。

YAML

```
- name: checkMembership
  action: aws:runCommand
  inputs:
    DocumentName: AWS-RunPowerShellScript
    Targets:
      - Key: tag:Stage
        Values:
          - Gamma
          - Beta
      - Key: tag-key
        Values:
          - Suite
    Parameters:
      commands:
        - (Get-WmiObject -Class Win32_ComputerSystem).PartOfDomain
```

JSON

```
{
    "name": "checkMembership",
    "action": "aws:runCommand",
    "inputs": {
        "DocumentName": "AWS-RunPowerShellScript",
        "Targets": [
            {
                "Key": "tag:Stage",
                "Values": [
                    "Gamma", "Beta"
                ]
            },
            {
                "Key": "tag:Application",
                "Values": [
                    "Suite"
                ]
            }
        ],
```

```
        "Parameters": {
            "commands": [
                "(Get-WmiObject -Class Win32_ComputerSystem).PartOfDomain"
            ]
        }
    }
}
```

パラメータ

ドキュメントに指定されている必須およびオプションのパラメータ。

型: マップ

必須: いいえ

CloudWatchOutputConfig

Amazon CloudWatch Logs にコマンド出力を送信するための設定オプション。CloudWatch Logs へのコマンド出力送信の詳細については、「Run Command の Amazon CloudWatch Logs の設定」を参照してください。

タイプ: StringMap (マップのスキーマはオブジェクトと一致する必要があります。 詳細については、AWS Systems Manager API リファレンスの「CloudWatchOutputConfig」を参照してください)。

必須: いいえ

次に例を示します。

YAML

```
- name: checkMembership
  action: aws:runCommand
  inputs:
    DocumentName: AWS-RunPowerShellScript
    InstanceIds:
      - "{{InstanceIds}}"
    Parameters:
      commands:
        - "(Get-WmiObject -Class Win32_ComputerSystem).PartOfDomain"
    CloudWatchOutputConfig:
      CloudWatchLogGroupName: CloudWatchGroupForSSMAutomationService
```

```
      CloudWatchOutputEnabled: true
```

JSON

```
{
    "name": "checkMembership",
    "action": "aws:runCommand",
    "inputs": {
        "DocumentName": "AWS-RunPowerShellScript",
        "InstanceIds": [
            "{{InstanceIds}}"
        ],
        "Parameters": {
            "commands": [
                "(Get-WmiObject -Class Win32_ComputerSystem).PartOfDomain"
            ]
        },
        "CloudWatchOutputConfig" : {
                "CloudWatchLogGroupName":
 "CloudWatchGroupForSSMAutomationService",
                "CloudWatchOutputEnabled": true
        }
    }
}
```

コメント

コマンドに関するユーザー定義情報。

型: 文字列

必須: いいえ

DocumentHash

ドキュメントのハッシュ。

型: 文字列

必須: いいえ

DocumentHashType

ハッシュの種類。

型: 文字列

有効な値: Sha256 | Sha1

必須: いいえ

NotificationConfig

通知を送信するための設定。

必須: いいえ

OutputS3BucketName

コマンド出力の応答を保存する S3 バケットの名前。マネージドノードには、S3 バケットが出力を正常にログに記録するためのアクセス許可が必要です。

タイプ: 文字列

必須: いいえ

OutputS3KeyPrefix

プレフィックス。

型: 文字列

必須: いいえ

ServiceRoleArn

AWS Identity and Access Management (IAM) ロールの ARN。

型: 文字列

必須: いいえ

TimeoutSeconds

インスタンスの AWS Systems Manager SSM Agent にコマンドが配信されるまで待機する時間 (秒単位)。指定した値に達する前にインスタンスで SSM Agent がコマンドを受信しなかった場合、コマンドのステータスは Delivery Timed Out に変わります。

タイプ: 整数

必須: いいえ

有効な値: 30 ~ 2592000

Output

CommandId

コマンドの ID。

ステータス

コマンドのステータス。

ResponseCode

コマンドのレスポンスコード。実行するドキュメントに複数のステップがある場合、この出力の値は返されません。

Output

コマンドの出力。コマンドでタグまたは複数のインスタンスをターゲットにした場合、出力値は返されません。`GetCommandInvocation` および `ListCommandInvocations` API オペレーションを使用して、個々のインスタンスの出力を取得できます。

`aws:runInstances` – Amazon EC2 インスタンスの起動

新しい Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを起動します。

入力

このアクションでは、ほとんどの API パラメータがサポートされています。詳細については、RunInstances API ドキュメントを参照してください。

YAML

```
name: launchInstance
action: aws:runInstances
maxAttempts: 3
timeoutSeconds: 1200
onFailure: Abort
inputs:
  ImageId: ami-12345678
```

```
  InstanceType: t2.micro
  MinInstanceCount: 1
  MaxInstanceCount: 1
  IamInstanceProfileName: myRunCmdRole
  TagSpecifications:
  - ResourceType: instance
    Tags:
    - Key: LaunchedBy
      Value: SSMAutomation
    - Key: Category
      Value: HighAvailabilityFleetHost
```

JSON

```
{
   "name":"launchInstance",
   "action":"aws:runInstances",
   "maxAttempts":3,
   "timeoutSeconds":1200,
   "onFailure":"Abort",
   "inputs":{
      "ImageId":"ami-12345678",
      "InstanceType":"t2.micro",
      "MinInstanceCount":1,
      "MaxInstanceCount":1,
      "IamInstanceProfileName":"myRunCmdRole",
      "TagSpecifications":[
         {
            "ResourceType":"instance",
            "Tags":[
               {
                  "Key":"LaunchedBy",
                  "Value":"SSMAutomation"
               },
               {
                  "Key":"Category",
                  "Value":"HighAvailabilityFleetHost"
               }
            ]
         }
      ]
   }
}
```

AdditionalInfo

リザーブド。

型: 文字列

必須: いいえ

BlockDeviceMappings

インスタンスのブロックデバイス。

型: MapList

必須: いいえ

ClientToken

リクエストの多重実行を禁止するための識別子。

型: 文字列

必須: いいえ

DisableApiTermination

インスタンス API の終了をオンまたはオフにします。

タイプ: ブール値

必須: いいえ

EbsOptimized

Amazon Elastic Block Store (Amazon EBS) 最適化をオンまたはオフにします。

タイプ: ブール値

必須: いいえ

IamInstanceProfileArn

インスタンスの AWS Identity and Access Management (IAM) インスタンスプロファイルの Amazon リソースネーム (ARN)。

型: 文字列

必須: いいえ

IamInstanceProfileName

インスタンスの IAM インスタンスプロファイルの名前。

型: 文字列

必須: いいえ

ImageId

Amazon Machine Image (AMI) の ID。

型: 文字列

必須: はい

InstanceInitiatedShutdownBehavior

システムのシャットダウン時にインスタンスを停止するか終了するかを示します。

型: 文字列

必須: いいえ

InstanceType

インスタンスタイプ。

> **Note**
>
> インスタンスタイプの値が指定されていない場合は、インスタンスタイプ m1.small を使用します。

型: 文字列

必須: いいえ

KernelId

カーネルの ID。

型: 文字列

必須: いいえ

KeyName

キーペアの名前。

型: 文字列

必須: いいえ

MaxInstanceCount

起動するインスタンスの最大数。

型: 文字列

必須: いいえ

MetadataOptions

インスタンスのメタデータオプション。詳細については、「InstanceMetadataOptionsRequest」を参照してください。

型: StringMap

必須 : いいえ

MinInstanceCount

起動するインスタンスの最小数。

型: 文字列

必須: いいえ

Monitoring

詳細モニタリングをオンまたはオフにします。

タイプ: ブール値

必須: いいえ

NetworkInterfaces

ネットワークインターフェイス。

型: MapList

必須: いいえ

Placement

インスタンスのプレイスメント。

型: StringMap

必須: いいえ

PrivateIpAddress

プライマリ IPv4 アドレス。

型: 文字列

必須: いいえ

RamdiskId

RAM ディスクの ID。

型: 文字列

必須: いいえ

SecurityGroupIds

インスタンスのセキュリティグループの ID。

タイプ: StringList

必須: いいえ

SecurityGroups

インスタンスのセキュリティグループの名前。

タイプ: StringList

必須: いいえ

SubnetId

サブネット ID。

型: 文字列

必須: いいえ

TagSpecifications

タグは、起動中のリソースに適用されます。起動時にインスタンスとボリュームにのみタグを付けることができます。指定されたタグは、すべてのインスタンス、または起動時に作成されたボリュームに適用されます。インスタンスを起動した後にタグを付けるには、aws:createTags – AWS リソースのタグを作成する アクションを使用します。

タイプ: MapList (詳細については、「TagSpecification」を参照してください)。

必須: いいえ

UserData

文字列リテラル値として渡されるスクリプト。リテラル値を入力する場合、Base64 エンコードである必要があります。

型: 文字列

必須: いいえ

出力

InstanceIds

インスタンスの ID。

InstanceStates

インスタンスの現在の状態。

aws:sleep – オートメーションを遅らせる

特定の時間数のオートメーションの遅延。このアクションは、国際標準化機構 (ISO) 8601 に日付と時刻形式を使用します。日付と時刻形式の詳細については、「ISO 8601」を参照してください。

入力

指定する時間でオートメーションを遅延することができます。

YAML

```
name: sleep
action: aws:sleep
inputs:
  Duration: PT10M
```

JSON

```
{
   "name":"sleep",
   "action":"aws:sleep",
   "inputs":{
      "Duration":"PT10M"
   }
}
```

また、指定された日付や時間までオートメーションを遅延することもできます。指定した日付と時刻が経過すると、アクションはすぐに処理されます。

YAML

```
name: sleep
action: aws:sleep
inputs:
  Timestamp: '2020-01-01T01:00:00Z'
```

JSON

```
{
    "name": "sleep",
    "action": "aws:sleep",
    "inputs": {
        "Timestamp": "2020-01-01T01:00:00Z"
    }
}
```

> **Note**
>
> 自動化は、最大で 604,799 秒 (7 日間) までの遅延をサポートします。

duration

ISO 8601 の時間。負の時間を指定することはできません。

型: 文字列

必須: いいえ

タイムスタンプ

ISO 8601 のタイムスタンプ。このパラメータ値を指定しない場合、Duration パラメータ値を指定する必要があります。

型: 文字列

必須: いいえ

出力

なし

aws:updateVariable — ランブック変数の値を更新します。

このアクションはランブック変数の値を更新します。値のデータ型は、更新元となる可変のデータ型に一致する必要があります。データ型変換はサポートされていません。onCancel プロパティは aws:updateVariable アクションではサポートされていません。

入力

入力は次のとおりです。

YAML

```
name: updateStringList
```

```
action: aws:updateVariable
inputs:
    Name: variable:variable name
    Value:
    - "1"
    - "2"
```

JSON

```
{
    "name": "updateStringList",
    "action": "aws:updateVariable",
    "inputs": {
        "Name": "variable:variable name",
        "Value": ["1","2"]
    }
}
```

名前

値の更新元となる変数の名前。次の形式を使用する必要があります。variable:*variable name*

型: 文字列

必須: はい

値

変数に代入する新しい値。値は、変数のデータ型に一致する必要があります。データ型変換はサポートされていません。

型: ブール値 | 整数 | マップリスト | 文字列 | 文字列リスト | 文字列マップ

必須: はい

制約:

- マップリストには、最大数は 200 項目まで格納できます。
- キーの長さは、最小長は 1、最大長は 50 です。
- 文字列リストには、最小で 0 個のアイテムから最大で 50 個のアイテムを指定できます。

- 文字列の長さは、最小長は 1、最大長は 512 です。

出力

なし

aws:waitForAwsResourceProperty – AWS リソースプロパティを待つ

aws:waitForAwsResourceProperty アクションにより、続行する前にオートメーションが特定のリソース状態またはイベント状態を待てるようにします。このアクションの使用例については、「その他のランブックの例」を参照してください。

> **Note**
>
> このアクションのデフォルトのタイムアウト値は 3600 秒 (1 時間) です。timeoutSeconds ステップで aws:waitForAwsResourceProperty パラメータを指定して、タイムアウトを制限または延長することができます。このアクションの使用方法の詳細と例については、「ランブックでのタイムアウトの処理」を参照してください。

入力

入力は、選択した API オペレーションによって定義されます。

YAML

```
action: aws:waitForAwsResourceProperty
inputs:
  Service: The official namespace of the service
  Api: The API operation or method name
  API operation inputs or parameters: A value
  PropertySelector: Response object
  DesiredValues:
  - Desired property value
```

JSON

```
{
  "action": "aws:waitForAwsResourceProperty",
```

```
  "inputs": {
    "Service":"The official namespace of the service",
    "Api":"The API operation or method name",
    "API operation inputs or parameters":"A value",
    "PropertySelector": "Response object",
    "DesiredValues": [
      "Desired property value"
    ]
  }
}
```

サービス

実行する API オペレーションを含む AWS のサービスの名前空間。たとえば、AWS Systems Manager の名前空間は、ssm となります。Amazon Elastic Compute Cloud (Amazon EC2) の名前空間は、ec2 です。サポートされている AWS のサービスの名前空間のリストは、AWS CLI コマンドリファレンスの「Available Services (利用可能なサービス)」セクションを参照してください。

型: 文字列

必須: はい

Api

実行する API オペレーションの名前。API オペレーション (メソッド) は、以下の「サービスリファレンス」ページの左側のナビゲーションでサービスを選択することで表示できます。呼び出すサービスの [Client (クライアント)] セクションでメソッドを選択します。例えば、Amazon Relational Database Service (Amazon RDS) のすべての API オペレーション (メソッド) は、Amazon RDS メソッドのページに一覧表示されます。

型: 文字列

必須: はい

API オペレーション入力

1 つ以上の API オペレーションを入力します。使用できる入力 (パラメータ) は、以下の「サービスリファレンス」ページの左側のナビゲーションでサービスを選択することで表示できます。呼び出すサービスの [Client (クライアント)] セクションでメソッドを選択します。例えば、Amazon RDS のすべてのメソッドは、Amazon RDS メソッドページに一覧表示されていま

す。describe_db_instances メソッドを選択し、下にスクロールして、[DBInstanceIdentifier]、[Name (名前)]、および [Values (値)] などの使用可能なパラメータを表示します。

YAML

```
inputs:
  Service: The official namespace of the service
  Api: The API operation name
  API input 1: A value
  API Input 2: A value
  API Input 3: A value
```

JSON

```
"inputs":{
      "Service":"The official namespace of the service",
      "Api":"The API operation name",
      "API input 1":"A value",
      "API Input 2":"A value",
      "API Input 3":"A value"
}
```

型: 選択した API オペレーションによって決まります

必須: はい

PropertySelector

応答オブジェクト内の特定の属性への JSONPath。レスポンスオブジェクトは、以下の「サービスリファレンス」ページの左側のナビゲーションでサービスを選択することで表示できます。呼び出すサービスの [Client (クライアント)] セクションでメソッドを選択します。例えば、Amazon RDS のすべてのメソッドは、Amazon RDS メソッドページに一覧表示されています。describe_db_instances メソッドを選択し、[Response Structure (レスポンス構造)] セクションまで下にスクロールします。[DBInstances] は応答オブジェクトとして表示されます。

型: 文字列

必須: はい

DesiredValues

予定の状態、またはオートメーションを継続する状態。

タイプ: MapList、StringList

必須: はい

オートメーションシステム変数

AWS Systems Manager オートメーションランブックでは、以下の変数が使用されます。これらの変数の使用例については、`AWS-UpdateWindowsAmi` Runbook の JSON ソースを参照してください。

`AWS-UpdateWindowsAmi` ランブックの JSON ソースを表示するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[ドキュメント] を選択します。
3. ドキュメントリストで、検索バーまたは検索バーの右側にある数字のいずれかを使用して、ランブック **`AWS-UpdateWindowsAmi`** を選択します。
4. [Content] タブを選択します。

システム変数

オートメーションランブックでは、以下のシステム変数がサポートされています。

変数	詳細
`global:ACCOUNT_ID`	オートメーションを実行するユーザーまたはロールの AWS アカウント ID です。
`global:DATE`	yyyy-MM-dd 形式の日付 (実行時)。
`global:DATE_TIME`	yyyy-MM-dd_HH.mm.ss 形式の日時 (実行時)。
`global:AWS_PARTITION`	リソースが置かれているパーティションです。標準 AWS リージョン の場合、パーティションは `aws` です。他のパーティションのリソースについては、パーティションは `aws-`*`partitionname`* です。例えば、AWS GovCloud (米国西部) リージョンのリソースのパーティションは `aws-us-gov` です。

変数	詳細
global:REGION	Runbook が実行されるリージョン。たとえば、us-east-2 です。

オートメーション変数

オートメーションランブックでは、以下の Automation 変数がサポートされています。

変数	詳細
automation:EXECUTION_ID	現在のオートメーションに割り当てられた一意の識別子 例えば、1a2b3c-1a2b3c-1a2b3c-1a2b3c1a2b3c1a2b3c と指定します。

トピック

- 用語
- サポートされるシナリオ
- サポートされないシナリオ

用語

以下の用語では、変数とパラメータの解決方法について説明します。

用語	定義	例
定数 ARN	変数を含まない有効な Amazon リソースネーム (ARN)。	arn:aws:iam::123456789012:role/roleName
Runbook パラメータ	Runbook レベル (instanceId など) で定義されたパラメータ。このパラメータは基本的な文字列置換で使用されま	{ "description": "Create Image Demo", "version": "0.3",

用語	定義	例
	す。その値は Start Execution 時に渡されます。	<pre>"assumeRole": "*Your_Automation_Assume_Role_ARN* ", "parameters":{ **"instanceId": { "type": "String", "description": "Instance to create image from"** } }</pre>

用語	定義	例
システム変数	Runbook のいずれかの部分が評価されたときに Runbook に代入される一般的な変数。	"activities": [{ "id": "copyImage", "activityType": "AWS-CopyImage", "maxAttempts": 1, "onFailure": "Continue", "inputs": { "ImageName": "{{imageName}}", "SourceImageId": "{{sourceImageId}}", "SourceRegion": "{{sourceRegion}}", "Encrypted": true, "ImageDescription": "Test CopyImage Description created on **{{global:DATE}}** " } }]

用語	定義	例

Automation 変数	Runbook のいずれかの部分が評価されたときに Runbook に代入される、オートメーションに関連した変数。	{
		"name": "runFixedCmds",
		"action": "aws:runCommand",
		"maxAttempts": 1,
		"onFailure": "Continue",
		"inputs": {
		"DocumentName": "AWS-RunPowerShellScript",
		"InstanceIds": [
		"{{LaunchInstance.InstanceIds}}"
		],
		"Parameters": {
		"commands": [
		"dir",
		"date",
		"“{{outputFormat}}” -f “left”,”right”,”{{global:DATE}}”,” **{{automation:EXECUTION_ID}}** ”
		]
		}
		}
		}

用語	定義	例
Systems Manager パラメータ	AWS Systems Manager Parameter Store 内で定義された変数。ステップ入力で直接参照することはできません。パラメータにアクセスするにはアクセス許可が必要な場合があります。	description: Launch new Windows test instance schemaVersion: '0.3' assumeRole: '{{AutomationAssumeRole}}' parameters: AutomationAssumeRole: type: String default: '' description: >- (Required) The ARN of the role that allows Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses your IAM permissions to run this runbook. LatestAmi: type: String default: >- {{ssm:/aws/service/ami-windows-latest/Windows_Server-2016-English-Full-Base}} description: The latest Windows Server 2016 AMI queried from the public parameter. mainSteps: - name: launchInstance action: 'aws:runInstances' maxAttempts: 3

用語	定義	例
		timeoutSeconds: 1200 onFailure: Abort inputs: ImageId: '{{LatestAmi}}' ...

サポートされるシナリオ

シナリオ	コメント	例
作成時の一定 ARN assumeRole 。	権限付与チェックが実行されて、呼び出し元ユーザーが assumeRole の委譲を許可されていることが確認されます。	{ "description": "Test all Automation resolvable parameters", "schemaVersion": "0.3", "assumeRole": ***"arn:aws:iam::123456789012:role/roleName"*** , "parameters": { ...
オートメーションの開始時に、AssumeRole に与えられる Runbook のパラメータ。	Runbook のパラメータリストで定義する必要があります。	{ "description": "Test all Automation resolvable parameters", "schemaVersion": "0.3", "assumeRole": **"{{dynamicARN}}"** , "parameters": { ...

シナリオ	コメント	例

開始時に Runbook パラメータに渡される値	お客様がパラメータに使用する値を指定します。開始時に渡される入力は、Runbook のパラメータリストで定義する必要があります。	<pre>...
		"parameters": {
		    "amiId": {
		      "type": "String",
		      "default":
		 "*ami-12345678* ",
		      "description":
		 "list of commands to
		 run as part of first
		 step"
		    },
		...</pre>
		Start Automation Execution への入力には {"amiId" : ["*ami-12345678* "] } を含めます。

シナリオ	コメント	例

ランブックコンテンツ内で参照される Systems Manager パラメータ。	変数は、顧客のアカウント内に存在するか、パブリックにアクセス可能なパラメータであり、Runbook の AssumeRole に変数へのアクセスがあります。作成時にチェックが実行されて、AssumeRole が変数にアクセスできることが確認されます。パラメータは、ステップ入力で直接参照することはできません。	```
		...
		parameters:
		    LatestAmi:
		    type: String
		    default: >-
		      {{ssm:/aws/
		service/ami-wind
		ows-latest/Windows
		_Server-2016-English-
		Full-Base}}
		    description: The
		 latest Windows Server
		 2016 AMI queried from
		 the public parameter.
		mainSteps:
		  - name: launchIns
		tance
		    action: 'aws:runI
		nstances'
		    maxAttempts: 3
		    timeoutSeconds:
		 1200
		    onFailure: Abort
		    inputs:
		      ImageId: '{{Latest
		Ami}}'
		...
		``

シナリオ	コメント	例

ステップ定義内で参照されるシステム変数	オートメーションが開始されると、システム変数が Runbook に代入されます。Runbook に挿入される値は、代入時の変数の値に対して相対的になります。たとえば、ステップ 1 で挿入される時間変数の値は、ステップの実行にかかる時間のため、ステップ 3 で挿入される時間変数の値とは異なります。システム変数は、ランブックのパラメータリストで設定する必要はありません。	<pre>...
		  "mainSteps": [
		    {
		      "name": "RunSomeCommands",
		      "action": "aws:runCommand",
		      "maxAttempts": 1,
		      "onFailure": "Continue",
		      "inputs": {
		        "DocumentName": "AWS:RunPowerShell",
		        "InstanceIds": ["{{LaunchInstance.InstanceIds}}"],
		        "Parameters": {
		            "commands" : [
		                "echo {The time is now {{global:DATE_TIME}}}"
		            ]
		        }
		    }
		}, ...</pre>

シナリオ	コメント	例

ステップ定義内で参照される自動化の変数	Automation 変数は、ランブックのパラメータリストで設定する必要はありません。サポートされる Automation 変数は automation:EXECUTION_ID のみです。	```
		...
		"mainSteps": [
		    {
		      "name": "invokeLambdaFunction",
		      "action": "aws:invokeLambdaFunction",
		      "maxAttempts": 1,
		      "onFailure": "Continue",
		      "inputs": {
		        "FunctionName": "Hello-World-LambdaFunction",
		
		"Payload" : "{ "executionId" : "{{automation:EXECUTION_ID}}" }"
		      }
		    }
		...
		``

シナリオ	コメント	例

次のステップ定義内からの前のステップの出力の参照	これはパラメータのリダイレクトです。前のステップの出力は、構文 {{stepName.OutputName}} を使用して参照されます。この構文は、お客様がランブックのパラメータに対して使用することはできません。これは、参照ステップの実行時に解決されます。ランブックのパラメータリストでは設定されません。	```
		...
		"mainSteps": [
		    {
		      "name": "LaunchInstance",
		      "action": "aws:runInstances",
		      "maxAttempts": 1,
		      "onFailure": "Continue",
		      "inputs": {
		        "ImageId": "{{amiId}}",
		        "MinInstanceCount": 1,
		        "MaxInstanceCount": 2
		      }
		    },
		    {
		      "name":"changeState",
		      "action": "aws:changeInstanceState",
		      "maxAttempts": 1,
		      "onFailure": "Continue",
		      "inputs": {
		        "InstanceIds": ["{{LaunchInstance.InstanceIds}}"],
		        "DesiredState": "terminated"
		      }
		    }
		
		...
		``

サポートされないシナリオ

シナリオ	コメント	例

作成時に `assumeRole` に渡される Systems Manager パラメータ	サポート外。	`...`
		
		`{`
		`  "description":`
		`"Test all Automation`
		`resolvable parameter`
		`s",`
		`  "schemaVersion":`
		`"0.3",`
		`  "assumeRole":`
		`"{{ssm:administrato`
		`rRoleARN}}  ",`
		`  "parameters": {`
		
		`...`

ステップ入力で直接参照される Systems Manager パラメータ。	作成時に `InvalidDocumentContent` 例外を返します。	`...`
		`mainSteps:`
		`  - name: launchIns`
		`tance`
		`    action: 'aws:runI`
		`nstances'`
		`    maxAttempts: 3`
		`    timeoutSeconds:`
		`1200`
		`    onFailure: Abort`
		`    inputs:`
		`      ImageId: '{{ssm:/`
		`aws/service/ami-win`
		`dows-latest/Window`
		`s_Server-2016-Engl`
		`ish-Full-Base}}'`
		`...`

シナリオ	コメント	例
変数によるステップの定義	Runbook 内のステップの定義は変数によって構成されます。	... "mainSteps": [{ "name": "LaunchInstance", "action": "aws:runInstances", "**{{attemptModel}}** ": 1, "onFailure": "Continue", "inputs": { "ImageId": "*ami-12345678* ", "MinInstanceCount": 1, "MaxInstanceCount": 2 } ... User supplies input : { "attemptModel" : "**minAttempts** " }

シナリオ	コメント	例
Runbook パラメータの相互参照	ユーザーは開始時に入力パラメータとして、Runbook 内の別のパラメータへの参照を渡します。	... "parameters": { "amiId": { "type": "String", "default": "ami-7f2e6015 ", "description": "list of commands to run as part of first step" }, "alternateAmiId": { "type": "String", "description": "The alternate AMI to try if this first fails". "default" : "{{amiId}}" }, ...

シナリオ	コメント	例
複数レベルの展開	Runbook で、変数の名前に評価される変数を定義します。これは、変数区切り記号 ({{ }}) 内にあり、変数/パラメータの値に展開されます。	... "parameters": { "*firstParameter* ": { "type": "String", "default": "param2", "description": "The parameter to reference" }, "*secondParameter* ": { "type": "String", "default" : "echo {Hello world}", "description": "What to run" } }, "mainSteps": [{ "name": "runFixedCmds", "action": "aws:runCommand", "maxAttempts": 1, "onFailure": "Continue", "inputs": { "DocumentName": "AWS-RunPowerShellScript", "InstanceIds" : "{{LaunchInstance.InstanceIds}}", "Parameters": { "commands": ["{{ ***{{firstParameter}}*** }}"] }

シナリオ	コメント	例
		``` ... Note: The customer intention here would be to run a command of "echo {Hello world}" ```

シナリオ	コメント	例
別の変数タイプである Runbook ステップからの出力の参照	ユーザーは前のRunbook ステップからの出力を後続のステップ内で参照します。出力は、後続のステップのアクションの要件を満たしていない変数タイプです。	... mainSteps: - name: getImageId action: aws:execu teAwsApi inputs: Service: ec2 Api: DescribeImages Filters: - Name: "name" Values: - "{{ImageName}}" outputs: - Name: ImageIdList Selector: "$.Images " Type: "StringList" - name: copyMyImages action: aws:copyImage maxAttempts: 3 onFailure: Abort inputs: SourceImageId: {{getImageId.Image IdList}} SourceRegion: ap- northeast-2 ImageName: Encrypted Copies of LAMP base AMI in ap- northeast-2 Encrypted: true ... Note: You must provide the type required by the Automation action. In this case, aws:copyI mage requires a "String" type variable but the preceding step

シナリオ	コメント	例
		outputs a "StringList" type variable.

独自のランブックの作成

オートメーションランブックは、オートメーションの実行時にマネージドインスタンスおよびその他の AWS リソースで Systems Manager が実行するアクションを定義します。Automation は AWS Systems Manager のツールです。ランブックには、順次実行されるステップが 1 つ以上含まれています。各ステップは、1 つのアクションを中心に構築されます。1 つのステップからの出力は、後のステップで入力として使用できます。

これらのアクションとそのステップを実行するプロセスは、オートメーションと呼ばれます。

ランブックでサポートされているアクションタイプを使用すると、AWS 環境でのさまざまなオペレーションを自動化できます。たとえば、`executeScript` アクションタイプを使用すると、Python または PowerShell スクリプトをランブックに直接埋め込むことができます。(カスタムランブックを作成するときは、スクリプトをインラインで追加するか、S3 バケットまたはローカルマシンからアタッチできます)。AWS CloudFormation および `createStack` アクションタイプを使用すると、`deleteStack` リソースの管理を自動化できます。また、`executeAwsApi` アクションタイプを使用すると、ステップは AWS リソースの作成または削除、他のプロセスの開始、通知の開始など、任意の AWS のサービスで任意の API オペレーションを実行できます。

オートメーションでサポートされている 20 種類のアクションタイプの一覧については、「Systems Manager Automation アクションのリファレンス」を参照してください。

AWS Systems Manager Automation では、1 つ以上の Amazon Elastic Compute Cloud (Amazon EC2) インスタンスの再起動や、Amazon Machine Image (AMI) の作成といった一般的なタスクを実行する際に使用することができる事前定義されたステップを含むいくつかのランブックが用意されています。また、独自のランブックを作成して他の AWS アカウント と共有したり、すべての Automation ユーザーに公開したりすることもできます。

ランブックは YAML または JSON を使用して記述されます。ただし、Systems Manager Automation コンソールの [Document Builder (ドキュメントビルダー)] を使用すると、ネイティブの JSON または YAML で作成しなくても、ランブックを作成できます。

> **Important**
>
> AWS Identity and Access Management (IAM) サービスロールを使用して他のサービスを呼び出す自動化ワークフローを実行する場合は、それらのサービスを呼び出すためのアクセス許可をサービスロールに設定する必要がある点に注意してください。この要件は、`AWS-ConfigureS3BucketLogging`、`AWS-CreateDynamoDBBackup`、`AWS-RestartEC2Instance` ランブックなど、すべての AWS オートメーションランブック (`AWS-*` ランブック) に適用されます。この要件は、他のサービスを呼び出すアクションを使用して他の AWS のサービスを呼び出すように作成したカスタムオートメーションランブックにも適用されます。例えば、`aws:executeAwsApi`、`aws:createStack`、または `aws:copyImage` のアクションを使用する場合は、それらのサービスを呼び出すためのアクセス許可を持つサービスロールを設定します。ロールに IAM インラインポリシーを追加することで、他の AWS のサービスへのアクセス許可を有効にできます。詳細については、「(オプション) 他の AWS のサービス を呼び出すためのオートメーションインラインポリシーまたはカスタマー管理ポリシーを追加する」を参照してください。

ランブックで指定できるアクションまたはプラグインに関する情報を表示するには、「Systems Manager Automation アクションのリファレンス」を参照してください。

AWS Toolkit for Visual Studio Code を使用してランブックを作成する方法については、 AWS Toolkit for Visual Studio Code ユーザーガイドの「Systems Manager Automation ドキュメントの使用」を参照してください。

ビジュアルデザイナーを使用したカスタムランブックの作成については、「オートメーションランブックのビジュアルデザインエクスペリエンス」を参照してください。

目次

- オートメーションランブックのビジュアルデザインエクスペリエンス
  - 開始する前に
  - ビジュアルデザインエクスペリエンスのインターフェースの概要
    - アクションブラウザー
    - キャンバス
    - フォーム
    - キーボードショートカット
  - ビジュアルデザインエクスペリエンスの活用

        - ランブックワークフローを作成する
        - ランブックを作成する
        - ランブックを更新する
        - ランブックのエクスポート
    - アクションの入力と出力を構成する
        - アクションの入力データを提供する。
        - アクションの出力データを定義します。
    - ビジュアルデザインエクスペリエンスによるエラー処理
        - エラー発生時にアクションを再試行してください。
        - タイムアウト
        - 失敗したアクション
        - キャンセルされたアクション
        - 重要なアクション
        - アクションを終了する
    - チュートリアル: ビジュアルデザインエクスペリエンスを使用したランブックの作成
        - ステップ 1: ビジュアルデザインエクスペリエンスに移動
        - ステップ 2: ワークフローを作成する
        - ステップ 3: 自動生成されたコードを確認する
        - ステップ 4: 新しいランブックを実行する
        - ステップ 5 : クリーンアップ
- オートメーションランブックのオーサリング
    - ユースケースの特定
    - 開発環境をセットアップする
    - ランブックコンテンツの開発
    - 例 1: 親子のランブックの作成
        - 子ランブックの作成
        - 親ランブックの作成
    - 例 2: スクリプト化されたランブック
    - その他のランブックの例
        - VPC アーキテクチャと Microsoft Active Directory ドメインコントローラーのデプロイ

        - 最新のスナップショットからルートボリュームを復元する
        - AMI とクロスリージョンコピーの作成
- AWS リソースを設定する入力パラメーターの作成
- ランブック作成のためのドキュメントビルダーの使用
    - ドキュメントビルダーを使用してランブックを作成する
    - スクリプトを実行するランブックを作成する
- ランブックでのスクリプトの使用
    - ランブックを使用するためのアクセス許可
    - スクリプトをランブックに追加する
    - ランブックのスクリプト制約
- ランブックでの条件文の使用
    - aws:branch アクションの使用
        - ランブック aws:branch でのステップの作成
            - 出力変数の作成について
        - aws:branch ランブックの例
        - 演算子を使用した複雑な分岐オートメーションの作成
    - 条件オプションの使用例
- アクション出力の入力としての使用
    - ランブックでの JSONPath の使用
- Automation 向けのウェブフック統合の作成
    - 統合の作成 (コンソール)
    - 統合の作成 (コマンドライン)
    - 統合用のウェブフックの作成
- ランブックでのタイムアウトの処理

オートメーションランブックのビジュアルデザインエクスペリエンス

AWS Systems Manager 自動化は、自動化ランブックの作成に役立つローコードのビジュアルデザイン体験を提供します。ビジュアルデザインエクスペリエンスでは、独自のコードを追加できるドラッグアンドドロップインターフェイスが提供されるため、ランブックをより簡単に作成および編集できます。ビジュアルデザインのエクスペリエンスを使用すると、次のことを実行できます。

- 条件ステートメント
- アクションごとに入力と出力をどのようにフィルタリングまたは変換するかを制御します。
- エラー処理を設定する。
- 新しいランブックを試作する。
- AWS Toolkit for Visual Studio Code を使用したローカル開発の出発点として、プロトタイプランブックを使用してください。

ランブックを作成または編集すると、オートメーションコンソールからビジュアルデザインエクスペリエンスにアクセスできます。ランブックを作成すると、ビジュアルデザインによって作業が検証され、コードが自動生成されます。ローカル開発または 用に生成されたコードをレビューまたはエクスポートできます。完了したら、ランブックを保存して実行し、Systems Manager Automation コンソールで結果を調べることができます。

開始する前に

ビジュアルデザインエクスペリエンスを使用するには、AWS アカウント、および使用したいリソースに対して正しい許可を提供する認証情報が必要になります。

ビジュアルデザインエクスペリエンスでは、オートメーションは Amazon CodeGuru Security と統合され、Python スクリプトのセキュリティポリシー違反や脆弱性を検出するのに役立ちます。この機能を `aws:executeScript` アクションに使用するには、AWS Identity and Access Management (IAM) ポリシーに以下の権限が含まれている必要があります。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "codeguru-security:CreateUploadUrl",
                "codeguru-security:CreateScan",
                "codeguru-security:GetScan",
                "codeguru-security:GetFindings"
            ]
        }
    ]
}
```

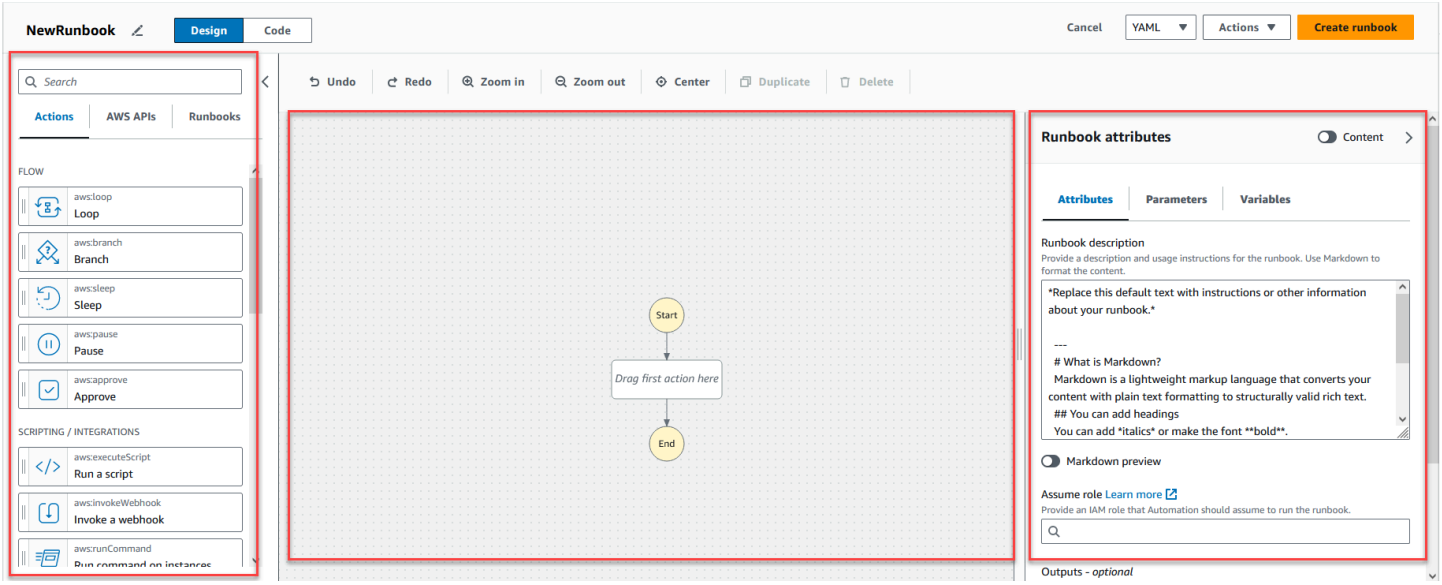
トピック

- ビジュアルデザインエクスペリエンスのインターフェースの概要
- ビジュアルデザインエクスペリエンスの活用
- アクションの入力と出力を構成する
- ビジュアルデザインエクスペリエンスによるエラー処理
- チュートリアル: ビジュアルデザインエクスペリエンスを使用したランブックの作成

ビジュアルデザインエクスペリエンスのインターフェースの概要

Systems Manager Automation のビジュアルデザインエクスペリエンスは、自動化ランブックの作成に役立つローコードのビジュアルワークフローデザイナーです。

インターフェースコンポーネントの概要を使って、ビジュアルデザインエクスペリエンスについて理解しましょう。



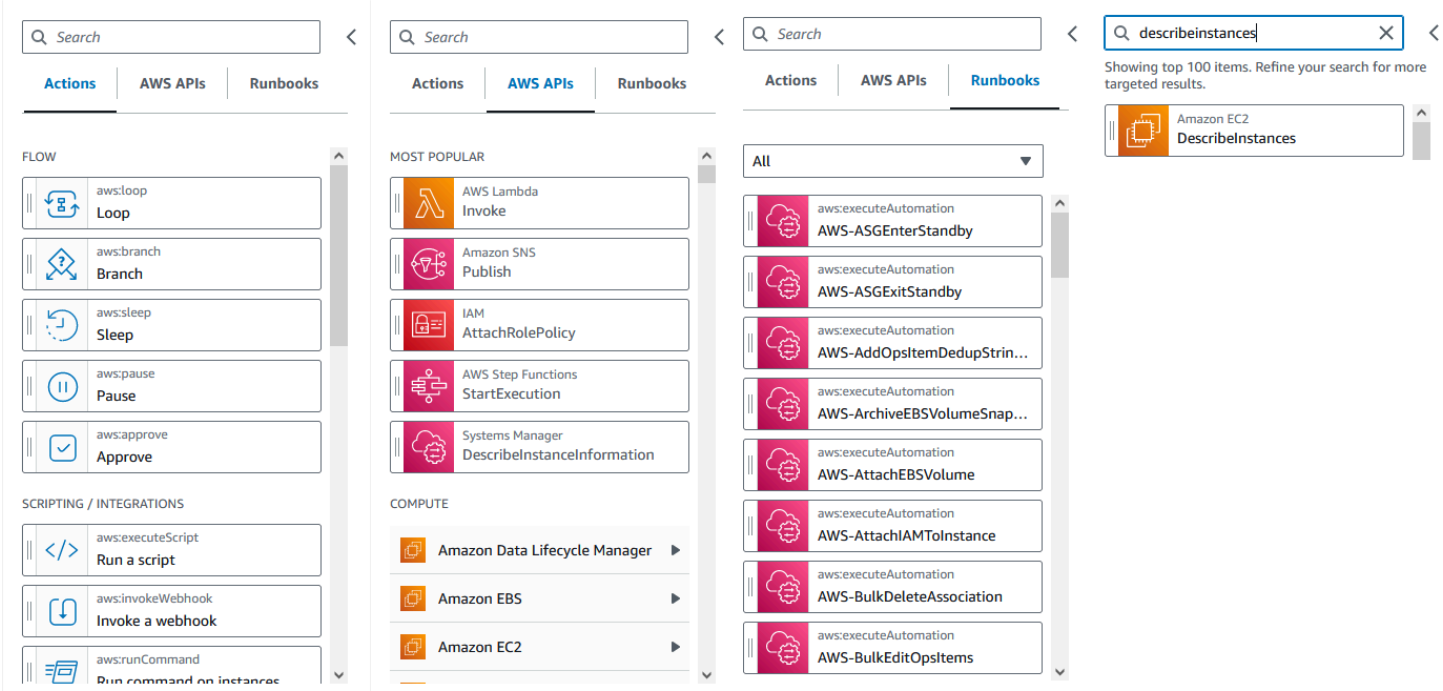
- [アクション] ブラウザーには [アクション]、[AWSAPI]、[ランブック] タブがあります。
- [キャンバス] は、状態をワークフローのグラフにドラッグアンドドロップし、状態の順序を変更し、状態を選択して、状態を設定または表示に選択します。
- [フォーム] パネルでは、キャンバス上で選択した任意のアクションのプロパティを表示および編集できます。[コンテンツ] トグルを選択すると、現在選択されているアクションが強調表示された状態でランブックの YAML または JSON が表示されます。

[Info] (情報) リンクは、ヘルプが必要になるとコンテキスト情報を含むパネルを開きます。これらのパネルには、Systems Manager Automationドキュメントの関連トピックへのリンクも含まれます。

アクションブラウザー

[アクション] ブラウザーから、アクションを選択してワークフローグラフにドラッグアンドドロップできます。すべての状態を検索するには、[アクション] ブラウザー上部の検索フィールドを使用します。[アクション] ブラウザーには以下のタブがあります。

- [アクション] タブには、キャンバス内のランブックワークフローグラフにドラッグアンドドロップできるオートメーションアクションのリストが表示されます。
- AWS[アクション] タブには、キャンバス内のワークフローグラフにドラッグアンドドロップできる AWS API のリストが表示されます。
- [ランブック] タブには、さまざまなユースケースに使用できるビルディングブロックとして、すぐに使える再利用可能なランブックがいくつか用意されています。例えば、ランブックを使用すると、同じアクションを再作成しなくても、ワークフロー内の Amazon EC2 インスタンスで一般的な修正タスクを実行できます。

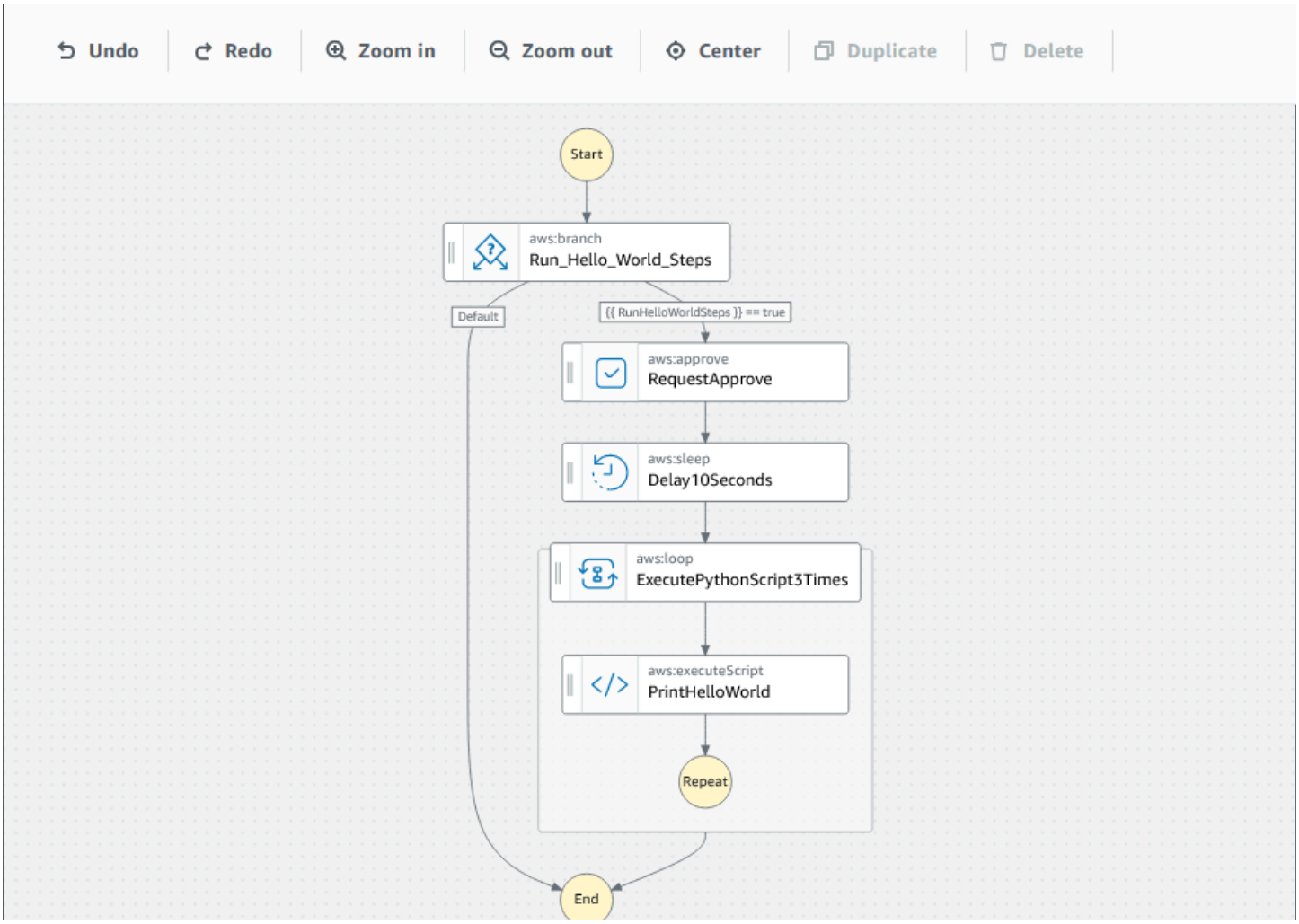


キャンバス

ワークフローに追加する状態を選択した後、キャンバスにドラッグし、ワークフローのグラフにドロップします。状態をドラッグアンドドロップして、ワークフローの別の場所に移動することもできます。ワークフローが複雑な場合は、キャンバスパネルでワークフローをすべて表示できない場合が

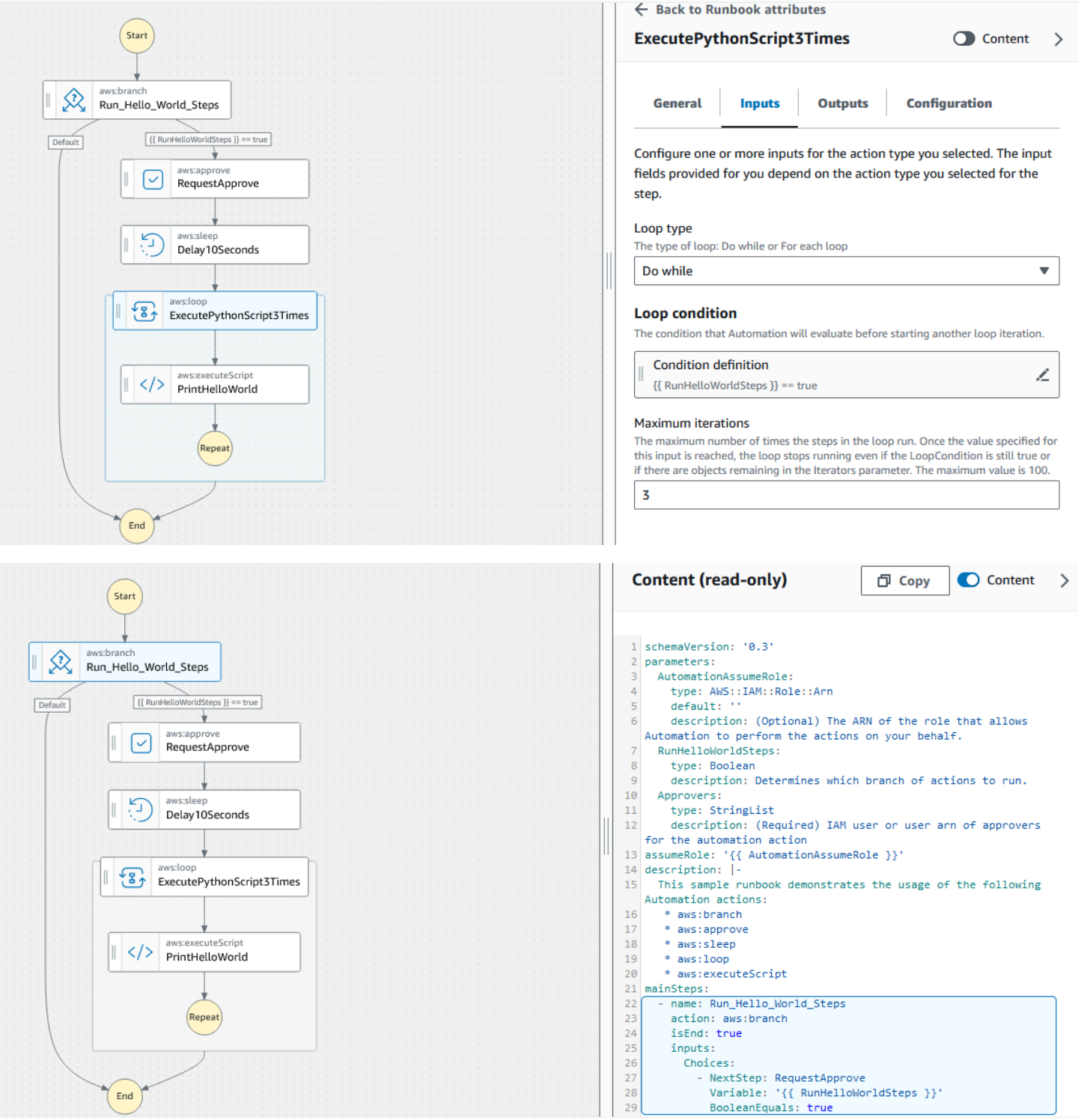
あります。キャンバスの上部にあるコントロールを使用して、拡大/縮小します。ワークフローのグラフのさまざまな部分を表示するには、キャンバスでワークフローのグラフをドラッグします。

[アクション] ブラウザーから、アクションを選択してランブックワークフローグラフにドラッグアンドドロップできます。ラインはワークフローのどこに配置されるかを示します。状態の順序を変更するには、ワークフロー内の別の場所にドラッグします。新しいワークフロー状態がワークフローに追加され、そのコードが自動生成されます。



フォーム

ランブックワークフローにアクションを追加したら、そのアクションをユースケースに合わせて設定できます。設定したいアクションを選択すると、[フォーム] パネルにそのパラメータとオプションが表示されます。[コンテンツ] トグルを選択すると、YAML コードまたは JSON コードを表示することもできます。選択した状態に関連付けられているコードがハイライトされます。



キーボードショートカット

ビジュアルデザインエクスペリエンスは、次の表に示すキーボードショートカットをサポートします。

機能	ショートカット
直前のオペレーションを元に戻す	Ctrl+Z
直前のオペレーションをやり直す	Ctrl+Shift+Z

機能ドショートカット

Alt + 矢印フローをキャンバスの中央に配置する

機能	ショートカット
選択した状態をすべて削除する	Backspace

機能一覧

ショートカットキー

選択した状態をすべて削除する

Ctrl+D (選択した状態を複製する)

ビジュアルデザインエクスペリエンスの活用

ビジュアルデザインエクスペリエンスを使用してランブックワークフローを作成、編集、実行する方法を学習します。ワークフローの準備ができたら、ワークフローをエクスポートできます。ビジュアルデザインエクスペリエンスを使用して、ラピッドプロトタイプ作成を行うこともできます。

ランブックワークフローを作成する

1. Systems Manager Automation コンソールにサインインします。
2. [ランブックの作成] を選択します。
3. [名前] ボックスに、ランブックの名前を入力します。例:*MyNewRunbook*
4. [デザイン] と [コード] トグルの横にある鉛筆アイコンを選択し、ランブックの名前を入力します。

これで、新しいランブックのワークフローをデザインできます。

ランブックを作成する

ビジュアルデザインエクスペリエンスを使用してランブックワークフローをデザインするには、[アクション] ブラウザーからキャンバスにオートメーションアクションをドラッグし、ランブックのワークフロー内の目的の場所に配置します。また、ワークフロー内の別の場所にドラッグして、ワークフローのアクションを並べ替えることができます。アクションをキャンバスにドラッグすると、ワークフロー内でドロップできる場所にラインが表示されます。キャンバスにアクションがドロップされると、そのコードが自動生成され、ランブックのコンテンツ内に追加されます。

追加したいアクションの名前がわかっている場合は、[アクション] ブラウザの上部にある検索ボックスを使用して、アクションを検索します。

アクションをキャンバスにドロップしたら、右側の [フォーム] パネルを使用してアクションを設定します。このパネルには、キャンバスに配置した各オートメーションアクションまたは API アクションの [一般]、[入力]、[出力]、および [設定]タブがあります。例えば、[一般] タブは次のセクションで構成されています。

- [ステップ名] はステップを識別します。ステップ名に一意の値を指定します。
- [説明] は、アクションがランブックのワークフローで何をしているのかを説明するのに役立ちます。

[入力] タブには、アクションによって異なるフィールドがあります。例えば、aws:executeScript オートメーションアクションには以下のセクションがあります。

- [ランタイム] は、指定されたスクリプトの実行に使用する言語です。
- [ハンドラー] は、関数の名前です。ハンドラで定義された関数に、events と context の 2 つのパラメータがあることを確認する必要があります。PowerShell ランタイムはこのパラメータをサポートしていません。
- [スクリプト] は、ワークフローで実行する埋め込みスクリプトです。
- (オプション) [添付ファイルは]、アクションによって呼び出せるスタンドアロンスクリプトまたは.zip ファイル用です。このパラメータは、JSON ランブックでは必須です。

[出力] タブは、アクションから出力する値を指定するのに役立ちます。ワークフローの後のアクションで出力値を参照したり、アクションからの出力を生成してログに記録したりできます。すべてのアクションがアウトプットをサポートしているわけではないため、すべてのアクションに [出力] タブがあるわけではありません。例えば、aws:pause アクションは出力をサポートしていません。出力をサポートするアクションの場合、[出力] タブは次のセクションで構成されます。

- [名前] は出力値に使用される名前です。出力はワークフローの後のアクションで参照できます。
- [セレクター] は、"$." から始まる JSONPath 式文字列で、JSON 要素内の 1 つまたは複数のコンポーネントを選択するために使用されます。
- [タイプ] は出力値のデータ型です。例えば、String または Integer データタイプと入力します。

[設定] タブには、すべてのオートメーションアクションで使用できるプロパティとオプションが含まれています。アクションには次のセクションがあります。

- [最大試行数] プロパティは、失敗した場合にアクションが再試行される回数です。
- [タイムアウト秒] プロパティは、アクションのタイムアウト値を指定します。
- [致命的か] プロパティは、アクションが失敗したためにオートメーション全体が停止するかどうかを決定します。
- [次のステップ] プロパティは、ランブック内でオートメーションが次に実行するアクションを決定します。
- [失敗時] プロパティは、アクションが失敗した場合にオートメーションがランブックで次に実行するアクションを決定します。

- [キャンセル時] プロパティは、アクションがユーザーによってキャンセルされた場合に、オートメーションがランブックで次に実行するアクションを決定します。

アクションを削除するには、キャンバスの上にあるツールバーの Backspace を使用するか、右クリックして [アクションを削除] を選択します。

ワークフローが大きくなると、キャンバスに収まらない場合があります。ワークフローがキャンバスに収まるようにするには、以下のオプションのいずれかを実行します。

- サイドパネルのコントロールを使用して、パネルのサイズを変更するか、パネルを閉じます。
- キャンバスの上部にあるコントロールを使用して、ワークフローのグラフをズームインまたはズームアウトします。

ランブックを更新する

ランブックの新しいバージョンを作成することで、既存のランブックワークフローを更新できます。ランブックを更新するには、ビジュアルデザインエクスペリエンスを使用するか、コードを直接編集します。既存のランブックを更新するには、以下の手順に従います。

1. Systems Manager Automation コンソールにサインインします。
2. 更新するランブックを選択します。
3. [Create new version (新しいバージョンの作成)] を選択します。
4. ビジュアルデザインエクスペリエンスには、コードペインとビジュアルワークフローペインの 2 つのペインがあります。ビジュアルワークフローペインで [デザイン] を選択して、ビジュアルデザインエクスペリエンスでワークフローを編集します。完了したら、[新しいバージョンを作成] を選択して変更を保存し、終了します。
5. (オプション) コードペインを使用して、YAML または JSON のランブックコンテンツを編集します。

ランブックのエクスポート

ランブックのワークフロー YAML または JSON コード、およびワークフローのグラフをエクスポートするには、以下の手順に従います。

1. [ドキュメント] コンソールでランブックを選択します。
2. [Create new version (新しいバージョンの作成)] を選択します。

3. [アクション] ドロップダウンで、グラフとランブックのどちらをエクスポートするか、またどの形式を好むかを選択します。

アクションの入力と出力を構成する

各オートメーションアクションは、受け取った入力に基づいて応答します。ほとんどの場合、出力を後続のアクションに渡します。ビジュアルデザインエクスペリエンスでは、[フォーム] パネルの [入力] タブと [出力] タブでアクションの入出力データを設定できます。

オートメーションアクションの出力を定義および使用する方法の詳細については、「アクション出力の入力としての使用」を参照してください。

アクションの入力データを提供する。

各オートメーションアクションには、値を指定する必要がある入力が 1 つ以上あります。アクションの入力に指定する値は、アクションが受け付けるデータ型と形式によって決まります。例えば、`aws:sleep` アクションの入力には、ISO 8601 形式の文字列値が `Duration` 入力に必要です。

通常、ランブックのワークフローでは、後続のアクションで使用したい出力を返すアクションを使用します。ランブックのワークフローでエラーが発生しないように、入力値が正しいことを確認することが重要です。入力値も重要です。入力値によって、アクションが期待どおりの出力を返すかどうかが決まるからです。例えば、`aws:executeAwsApi` アクションを使用するときは、API 操作に適切な値を指定していることを確認する必要があります。

アクションの出力データを定義します。

オートメーションアクションの中には、定義した操作を実行した後に出力を返すものもあります。出力を返すアクションには、出力が事前に定義されているか、ユーザーが出力を定義できるものがあります。例えば、`aws:createImage` アクションには `ImageId` と `ImageState` を返す出力があらかじめ定義されています。これとは対照的に、`aws:executeAwsApi` アクションでは、指定した API オペレーションから必要な出力を定義できます。そのため、1 回の API オペレーションから 1 つ以上の値を返して、後続のアクションで使用できます。

オートメーションアクションの独自の出力を定義するには、出力の名前、データ型、出力値を指定する必要があります。引き続き `aws:executeAwsApi` アクションを例として使用するために、Amazon EC2 から `DescribeInstances` API オペレーションを呼び出しているとしましょう。この例では、Amazon EC2 インスタンスの `State` を返す、あるいは出力し、その出力に基づいてランブックのワークフローを分岐させたいと考えています。**`InstanceState`** 出力に名前を付けることを選択し、そのデータ型 **`String`** を使用します。

出力の実際の値を定義するプロセスは、アクションによって異なります。例えば、aws:executeScript アクションを使用している場合は、出力にデータを提供するために関数内で return ステートメントを使用する必要があります。aws:executeAwsApi、aws:waitForAwsResourceProperty、aws:assertAwsResourcePrope などのアクションでは、Selector が必要です。Selector、または一部のアクションで参照されるような PropertySelector は、API オペレーションからの JSON レスポンスを処理するために使用される JSONPath 文字列です。出力に正しい値を選択できるように、API オペレーションからの JSON レスポンスオブジェクトがどのように構造化されているかを理解することが重要です。前述の DescribeInstances API オペレーションを使用する場合は、次の JSON レスポンスの例を参照してください。

```
{
  "reservationSet": {
    "item": {
      "reservationId": "r-1234567890abcdef0",
      "ownerId": 123456789012,
      "groupSet": "",
      "instancesSet": {
        "item": {
          "instanceId": "i-1234567890abcdef0",
          "imageId": "ami-bff32ccc",
          "instanceState": {
            "code": 16,
            "name": "running"
          },
          "privateDnsName": "ip-192-168-1-88.eu-west-1.compute.internal",
          "dnsName": "ec2-54-194-252-215.eu-west-1.compute.amazonaws.com",
          "reason": "",
          "keyName": "my_keypair",
          "amiLaunchIndex": 0,
          "productCodes": "",
          "instanceType": "t2.micro",
          "launchTime": "2018-05-08T16:46:19.000Z",
          "placement": {
            "availabilityZone": "eu-west-1c",
            "groupName": "",
            "tenancy": "default"
          },
          "monitoring": {
            "state": "disabled"
          },
          "subnetId": "subnet-56f5f000",
```

```
          "vpcId": "vpc-11112222",
          "privateIpAddress": "192.168.1.88",
          "ipAddress": "54.194.252.215",
          "sourceDestCheck": true,
          "groupSet": {
            "item": {
              "groupId": "sg-e4076000",
              "groupName": "SecurityGroup1"
            }
          },
          "architecture": "x86_64",
          "rootDeviceType": "ebs",
          "rootDeviceName": "/dev/xvda",
          "blockDeviceMapping": {
            "item": {
              "deviceName": "/dev/xvda",
              "ebs": {
                "volumeId": "vol-1234567890abcdef0",
                "status": "attached",
                "attachTime": "2015-12-22T10:44:09.000Z",
                "deleteOnTermination": true
              }
            }
          },
          "virtualizationType": "hvm",
          "clientToken": "xMcwG14507example",
          "tagSet": {
            "item": {
              "key": "Name",
              "value": "Server_1"
            }
          },
          "hypervisor": "xen",
          "networkInterfaceSet": {
            "item": {
              "networkInterfaceId": "eni-551ba000",
              "subnetId": "subnet-56f5f000",
              "vpcId": "vpc-11112222",
              "description": "Primary network interface",
              "ownerId": 123456789012,
              "status": "in-use",
              "macAddress": "02:dd:2c:5e:01:69",
              "privateIpAddress": "192.168.1.88",
              "privateDnsName": "ip-192-168-1-88.eu-west-1.compute.internal",
```

```
              "sourceDestCheck": true,
              "groupSet": {
                "item": {
                  "groupId": "sg-e4076000",
                  "groupName": "SecurityGroup1"
                }
              },
              "attachment": {
                "attachmentId": "eni-attach-39697adc",
                "deviceIndex": 0,
                "status": "attached",
                "attachTime": "2018-05-08T16:46:19.000Z",
                "deleteOnTermination": true
              },
              "association": {
                "publicIp": "54.194.252.215",
                "publicDnsName": "ec2-54-194-252-215.eu-west-1.compute.amazonaws.com",
                "ipOwnerId": "amazon"
              },
              "privateIpAddressesSet": {
                "item": {
                  "privateIpAddress": "192.168.1.88",
                  "privateDnsName": "ip-192-168-1-88.eu-west-1.compute.internal",
                  "primary": true,
                  "association": {
                    "publicIp": "54.194.252.215",
                    "publicDnsName": "ec2-54-194-252-215.eu-
west-1.compute.amazonaws.com",
                    "ipOwnerId": "amazon"
                  }
                }
              },
              "ipv6AddressesSet": {
                "item": {
                  "ipv6Address": "2001:db8:1234:1a2b::123"
                }
              }
            }
          },
          "iamInstanceProfile": {
            "arn": "arn:aws:iam::123456789012:instance-profile/AdminRole",
            "id": "ABCAJEDNCAA64SSD123AB"
          },
          "ebsOptimized": false,
```

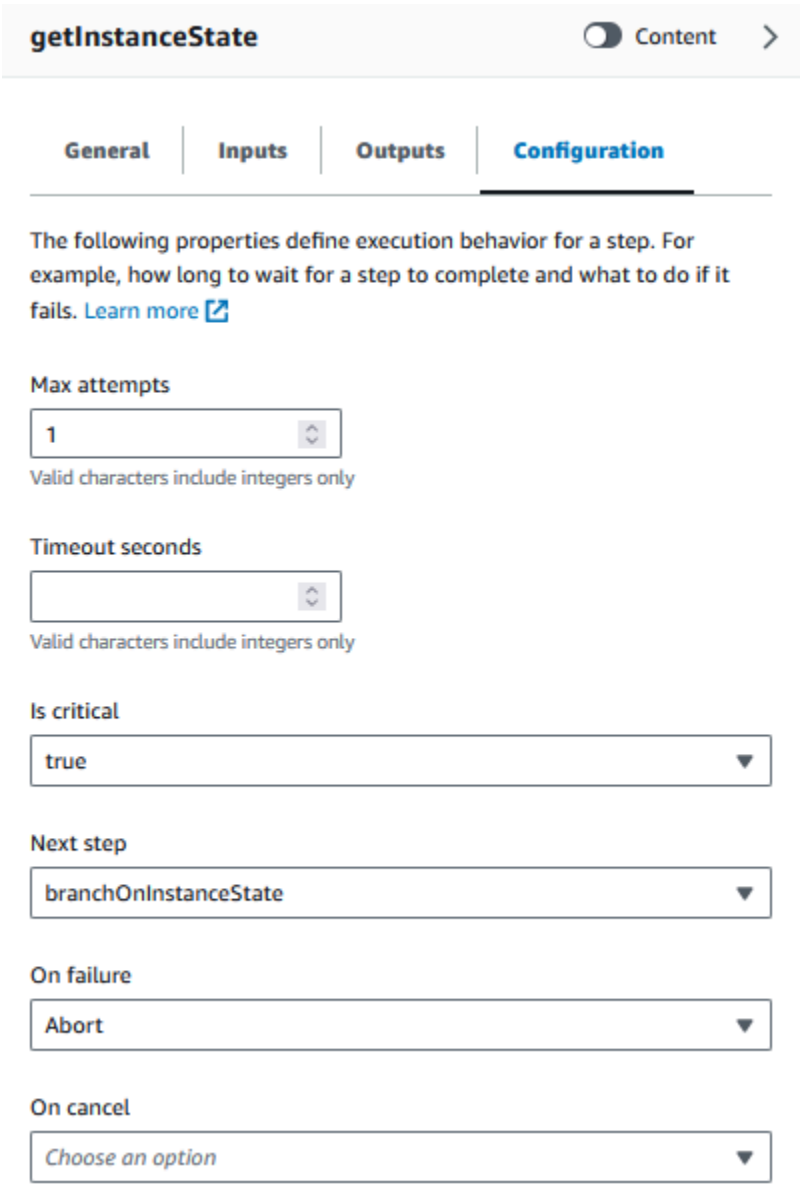
```
          "cpuOptions": {
            "coreCount": 1,
            "threadsPerCore": 1
          }
        }
      }
    }
  }
}
```

JSON レスポンスオブジェクトでは、State インスタンスは Instances オブジェクトにネストされ、次いで Reservations オブジェクトにネストされます。State インスタンスの値を返すには、Selector に文字列 (**$.Reservations[0].Instances[0].State.Name**) を使用して、その値を出力に使用できるようにします。

ランブックのワークフローの後続アクションで出力値を参照するには、次の形式を使用します: {{ *StepName*.*NameOfOutput* }}。例えば、**{{ GetInstanceState.InstanceState }}** と指定します。ビジュアルデザインエクスペリエンスでは、入力のドロップダウンを使用して、後続のアクションで使用する出力値を選択できます。後続のアクションで出力を使用する場合、出力のデータ型は入力のデータ型と一致する必要があります。この例では、InstanceState 出力は、String です。したがって、その値を後続のアクションの入力で使用するには、入力が String を受け入れる必要があります。

ビジュアルデザインエクスペリエンスによるエラー処理

デフォルトでは、アクションがエラーを報告すると、オートメーションはランブックのワークフローを完全に停止します。これは、すべてのアクションの onFailure プロパティのデフォルト値が Abort であるためです。ランブックのワークフローでオートメーションがエラーを処理する方法を設定できます。エラー処理を設定した場合でも、一部のエラーによって実行が失敗する可能性があります。詳細については、「Systems Manager Automation のトラブルシューティング」を参照してください。ビジュアルデザインエクスペリエンスでは、[設定] パネルでエラー処理を設定します。



エラー発生時にアクションを再試行してください。

エラーが発生した場合にアクションを再試行するには、[最大試行数] プロパティに値を指定します。デフォルト値は 1 です。指定した値が 1 より大きい場合、すべての再試行が失敗するまでステップは失敗したと見なされません。

タイムアウト

アクションのタイムアウトを設定して、アクションが失敗するまでの最大実行秒数を設定できます。タイムアウトを設定するには、アクションが失敗するまでのアクションの待機秒数を [タイムアウト秒数] プロパティに入力します。タイムアウトが達したときにアクションの値が `Max attempts` 以上の場合、すべての再試行が実行されるまでこのステップはタイムアウトとは見なされません。

失敗したアクション

デフォルトでは、アクションが失敗すると、オートメーションはランブックのワークフローを完全に停止します。ランブック内のアクションの [失敗時] プロパティに代替値を指定することで、この動作を変更できます。ワークフローをランブックの次のステップに進めたい場合は、[続行] を選択します。ワークフローをランブック内の別の後続ステップにジャンプさせたい場合は、[ステップ] を選択し、ステップの名前を入力します。

キャンセルされたアクション

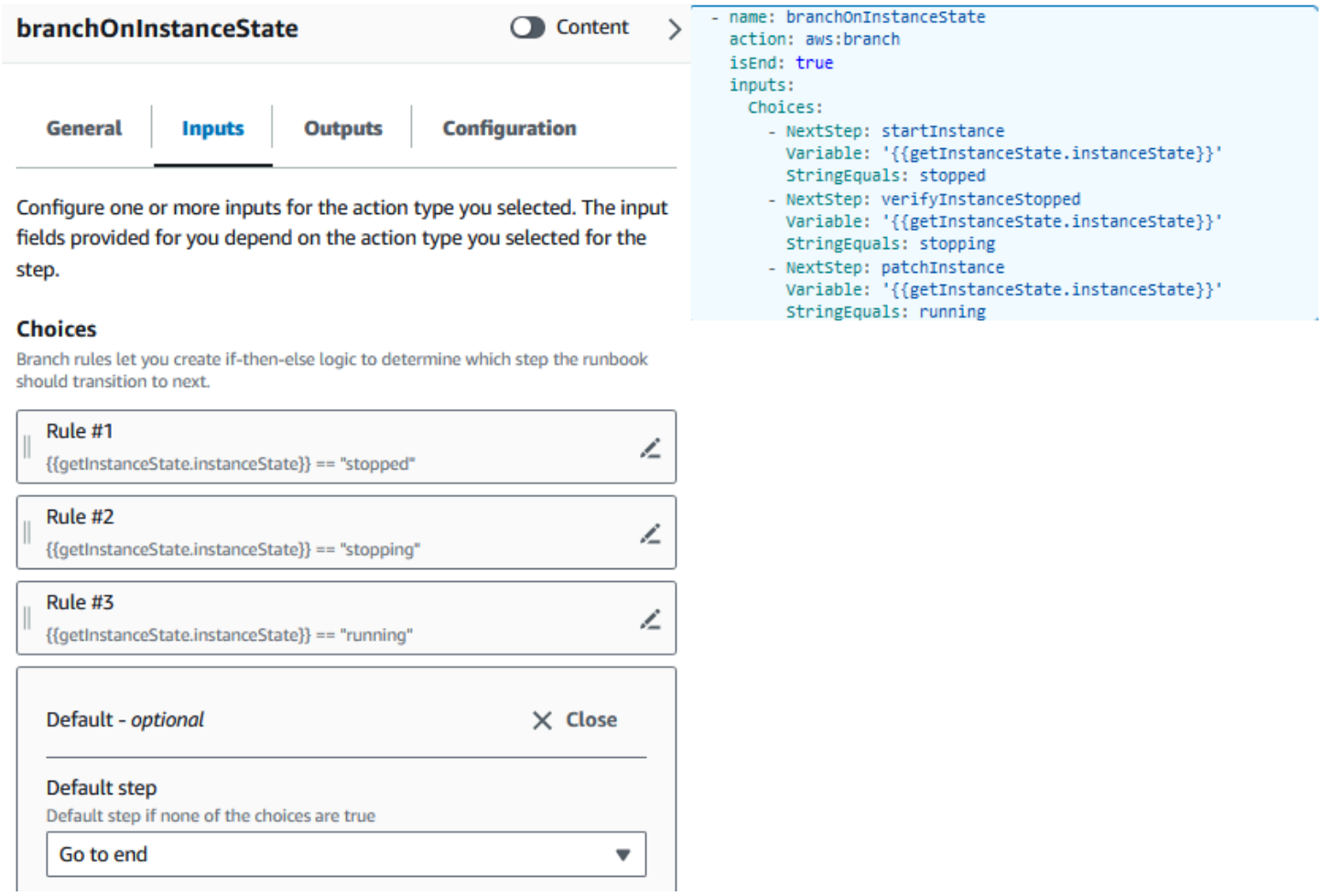
デフォルトでは、アクションがユーザーによってキャンセルされると、オートメーションはランブックのワークフローを完全に停止します。ランブック内のアクションの [キャンセル時] プロパティに代替値を指定することで、この動作を変更できます。ワークフローをランブック内の別の後続ステップにジャンプさせたい場合は、[ステップ] を選択し、ステップの名前を入力します。

重要なアクション

アクションをクリティカルとして指定できます。クリティカルアクションによってオートメーションの全体的なレポートステータスが決まります。この指定のステップが失敗した場合、オートメーションは、他のアクションの成功の有無にかかわらず、失敗の最終的なステータスを `Failed` としてレポートします。アクションをクリティカルとして設定するには、[クリティカルですか] プロパティのデフォルト値を [真] のままにします。

アクションを終了する

[停止ですか] プロパティでは、指定されたアクションの最後にオートメーションを停止します。このプロパティのデフォルト値は `false` です。アクションにこのプロパティを設定すると、アクションが成功するか失敗するかに関わらず、オートメーションは停止します。このプロパティは、予期しない入力値や未定義の入力値を処理する `aws:branch` アクションで最もよく使用されます。次の例は、`running`、`stopping` または `stopped` のどちらかのインスタンス状態を想定しているランブックを示しています。インスタンスの状態が異なる場合、自動化は終了します。



チュートリアル: ビジュアルデザインエクスペリエンスを使用したランブックの作成

このチュートリアルでは、Systems Manager Automation が提供するビジュアルデザインエクスペリエンスを使用した作業の基本について学習します。ビジュアルデザインエクスペリエンスでは、複数のアクションを使用するランブックを作成できます。ドラッグアンドドロップ機能を使用して、キャンバス上のアクションを整理します。また、これらのアクションを検索、選択、設定することもできます。次に、ランブックのワークフロー用に自動生成された YAML コードを表示したり、ビジュアルデザインエクスペリエンスを終了したり、ランブックを実行したり、実行の詳細を確認したりできます。

このチュートリアルでは、ランブックを更新して新しいバージョンを表示する方法も説明します。チュートリアルを最後までやると、クリーンアップステップを実行し、ランブックを削除します。

このチュートリアルを完了すると、ビジュアルデザインエクスペリエンスを使用してランブックを作成する方法がわかります。また、ランブックを更新、実行、削除する方法もわかります。

> **Note**
>
> このチュートリアルを開始する前に、オートメーションの設定 を完了していることを確認してください。

トピック

- ステップ 1: ビジュアルデザインエクスペリエンスに移動
- ステップ 2: ワークフローを作成する
- ステップ 3: 自動生成されたコードを確認する
- ステップ 4: 新しいランブックを実行する
- ステップ 5 : クリーンアップ

ステップ 1: ビジュアルデザインエクスペリエンスに移動

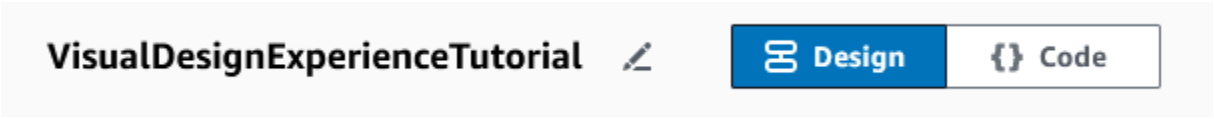
1. Systems Manager オートメーションコンソールにサインインします。
2. [オートメーションを作成] を選択してランブックを保存します。

ステップ 2: ワークフローを作成する

ビジュアルデザインエクスペリエンスでは、ワークフローはランブックをキャンバス上にグラフィカルに表示したものです。ビジュアルデザインエクスペリエンスを使用して、ランブックの個々のアクションを定義、設定、および検証できます。

ワークフローを作成するには

1. [デザイン] と [コード] トグルの横にある鉛筆アイコンを選択し、ランブックの名前を入力します。このチュートリアルでは、**VisualDesignExperienceTutorial** と入力します。

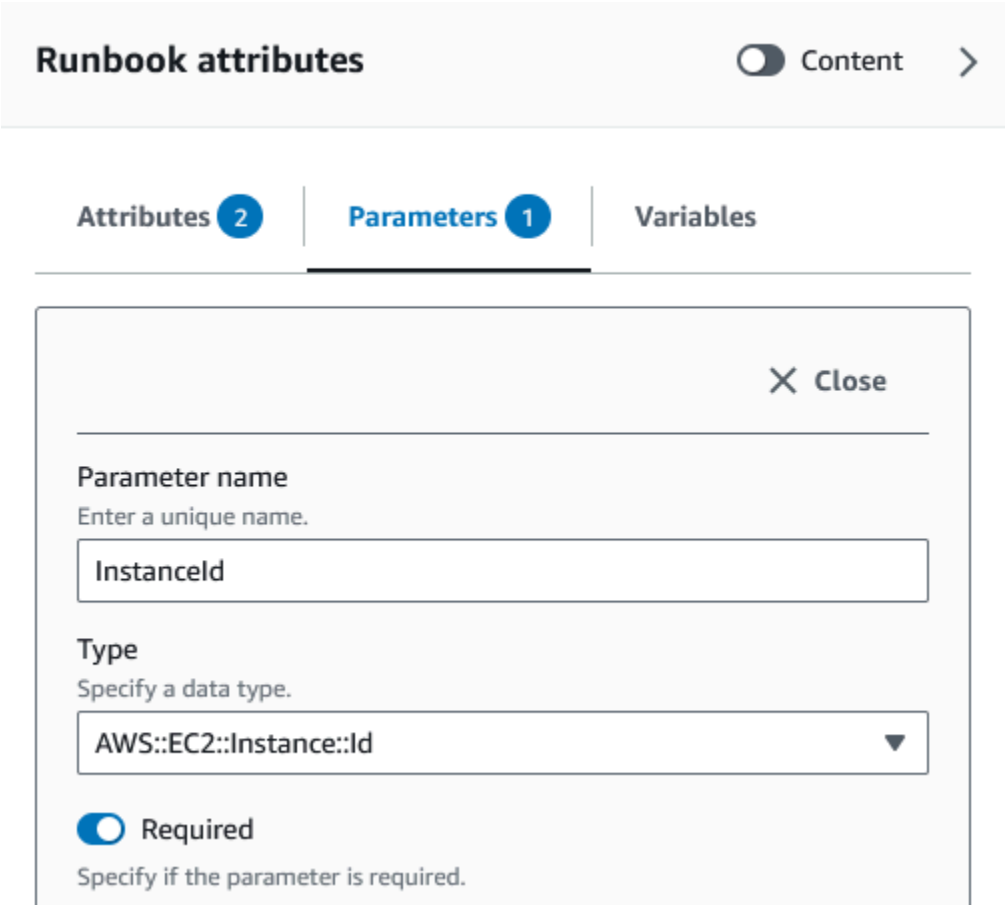


2. [フォーム] パネルの [ドキュメント属性] セクションで、[入力パラメーター] ドロップダウンを展開し、[パラメーターを追加] を選択します。

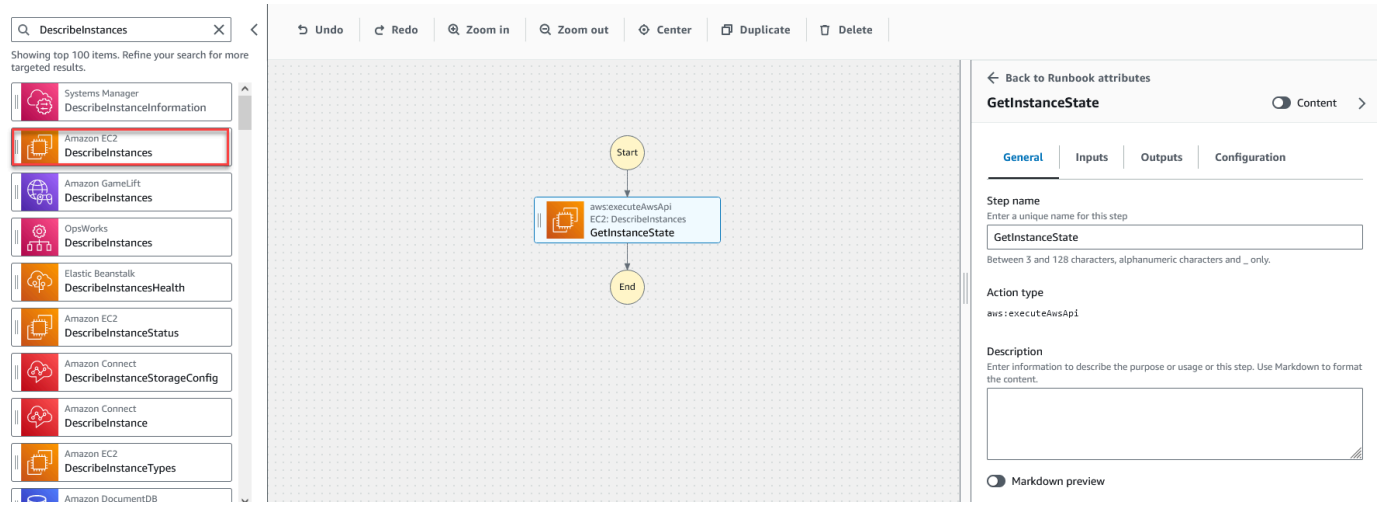
   a. [パラメータ名] セクションに「**InstanceId**」と入力します。

   b. [タイプ] ドロップダウンで、[AWS:: EC2:: インスタンス] を選択します。

c. [必須] トグルを選択します。



3. [AWSAPI] ブラウザで検索バーに「**DescribeInstances**」と入力します。
4. [Amazon EC2 — DescribeInstances] アクションを空のキャンバスにドラッグします。
5. [名前] に値を入力します。このチュートリアルでは、名として **GetInstanceState** を使用します。



a. [その他の入力] ドロップダウンを展開し、[入力名] フィールドに「**InstanceIds**」と入力します。

b. [入力] タブを選択します。

c. [入力値] フィールドで、**InstanceId** 文書入力を選択します。これは、プロシージャの最初に作成した入力パラメータの値を参照します。DescribeInstances アクションの InstanceIds 入力は StringList 値を受け入れるため、InstanceId 入力を角括弧で囲む必要があります。[入力値] の YAML は **['{{ InstanceId }}']** と一致する必要があります。

d. [出力] タブで [出力を追加] を選択し、[名前] フィールドに **InstanceState** を入力します。

e. [セレクター] フィールドに、**$.Reservations[0].Instances[0].State.Name** と入力します。

f. [タイプ] ドロップダウンで [文字列] を選択します。

6. [アクション] ブラウザーから [ブランチ] アクションをドラッグし、**GetInstanceState** ステップの下にドロップします。

7. [名前] に値を入力します。このチュートリアルでは、名前 **BranchOnInstanceState** を使用します。

   分岐ロジックを定義するには、次の手順を実行します。

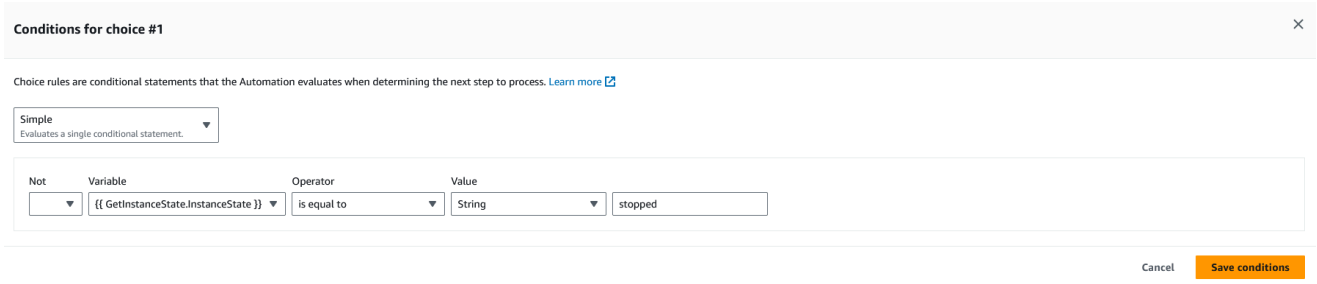
   a. **Branch** キャンバス上の状態を選択します。次に、[入力] と [選択肢] で鉛筆アイコンを選択し、[ルール #1] を編集します。

   b. [条件を追加] を選択します。

   c. [ルール #1 の条件] ダイアログボックスで、[変数] ドロップダウンから **GetInstanceState.InstanceState** ステップ出力を選択します。

d. [演算子] で、[次と等しい] を選択します。

e. [値] には、ドロップダウンリストから [文字列] を選択します。**stopped** と入力します。



f. [条件を保存] を選択します。

g. [新しいルールを追加] を選択します。

h. [ルール #2] の [条件を追加] を選択します。

i. [ルール #2 の条件] ダイアログボックスで、[変数] ドロップダウンから **GetInstanceState.InstanceState** ステップ出力を選択します。

j. [演算子] で、[次と等しい] を選択します。

k. [値] には、ドロップダウンリストから [文字列] を選択します。**stopping** と入力します。

l. [条件を保存] を選択します。

m. [新しいルールを追加] を選択します。

n. [ルール #3] で [条件を追加] を選択します。

o. [ルール #3 の条件] ダイアログボックスで、[変数] ドロップダウンから **GetInstanceState.InstanceState** ステップ出力を選択します。

p. [演算子] で、[次と等しい] を選択します。

q. [値] には、ドロップダウンリストから [文字列] を選択します。**running** と入力します。

r. [条件を保存] を選択します。

s. [デフォルトルール] で、[デフォルトステップ] の [最後まで進む] を選択します。

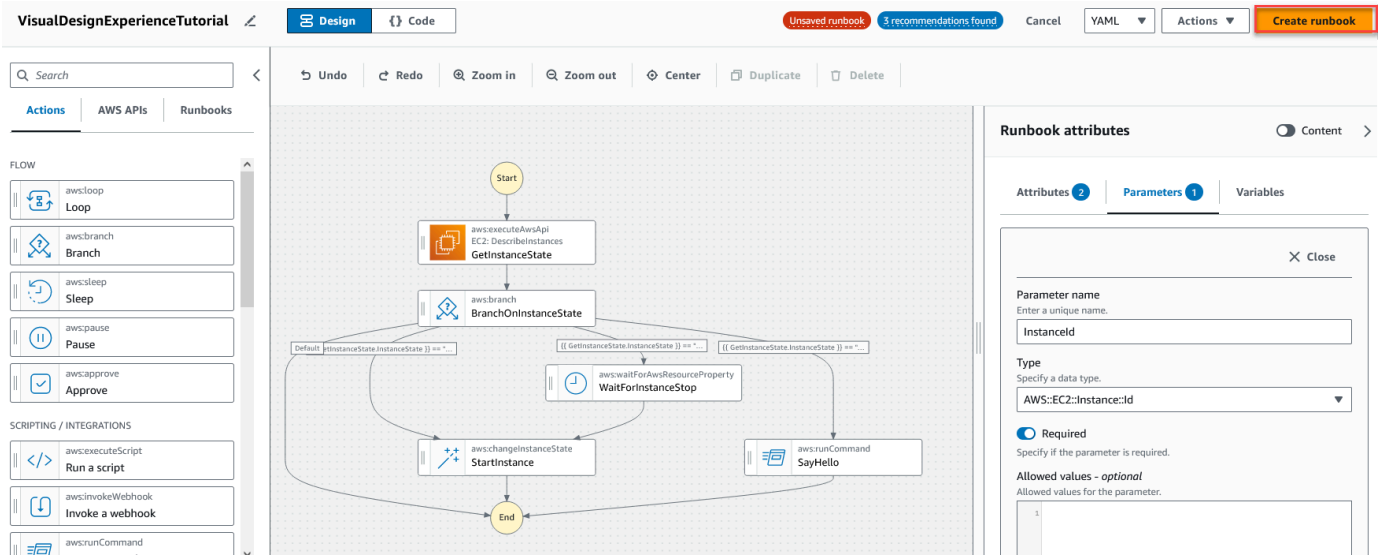
8. {{ GetInstanceState.InstanceState }} == "stopped" 条件の下にある空の [インスタンス状態を変更] アクションを、空の [ここにドラッグ] ボックスにドラッグします。

a. [ステップ名] には、と入力します。**StartInstance**

b. [入力] タブの [インスタンス ID] で、ドロップダウンから [InstanceId] ドキュメントの入力値を選択します。

c. [希望する状態] には **running** を指定します。

9. {{ GetInstanceState.InstanceState }} == "stopping" 条件の下にある空の [AWSリソースを待つ] アクションを、空の [ここにドラッグ] ボックスにドラッグします。
10. [名前] に値を入力します。このチュートリアルでは、名前 **WaitForInstanceStop** を使用します。
    a. [サービス] フィールドには [Amazon EC2] を選択します。
    b. [API] フィールドでは、[DescribeInstances] を選択します。
    c. [プロパティセレクター] フィールドには、**$.Reservations[0].Instances[0].State.Name** と入力します。
    d. [希望値] パラメータには、**["stopped"]** と入力します。
    e. [WaitForInstanceStop] アクションの [設定] タブで、[次のステップ] ドロップダウンから [インスタンスを開始] を選択します。
11. {{ GetInstanceState.InstanceState }} == "running" 条件の下にある空の [インスタンスでコマンドを実行] アクションを、空の [ここにドラッグ] ボックスにドラッグします。
12. [ステップ名] には、と入力します。**SayHello**
    a. [入力] タブで、[ドキュメント名] パラメータに「**AWS-RunShellScript**」と入力します。
    b. [InstanceIds] については、ドロップダウンから [InstanceId] ドキュメントの入力値を選択します。
    c. [追加入力] ドロップダウンを展開し、[入力名] ドロップダウンで [パラメータ] を選択します。
    d. [値入力] フィールドに **{"commands": "echo 'Hello World'"}** を入力します。
13. 完成したランブックをキャンバスで確認し、[ランブック作成] を選択してチュートリアルランブックを保存します。



ステップ 3: 自動生成されたコードを確認する

[アクション] ブラウザーからキャンバスにアクションをドラッグアンドドロップすると、ビジュアルデザインエクスペリエンスによってランブックの YAML または JSON コンテンツがリアルタイムで自動的に作成されます。このコードは表示および編集できます。自動生成されたコードを表示するには、[デザイン] と [コード] トグルの [コード] を選択します。

ステップ 4: 新しいランブックを実行する

ランブックを作成したら、オートメーションを実行できます。

新しい自動化ランブックを実行するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[オートメーション]、[オートメーションの実行] の順に選択します。
3. [Automation document (自動化ドキュメント)] リストで、ランブックを選択します。[Document categories (ドキュメントカテゴリ)] ペインで 1 つ以上のオプションを選択して、目的に応じて SSM ドキュメントをフィルタリングします。自分が所有するランブックを表示するには、[Owned by me (自分が所有)] タブを選択します。自分のアカウントと共有されているランブックを表示するには、[Shared with me (共有ファイル)] タブを選択します。すべてのランブックを表示するには、[すべてのドキュメント] タブを選択します。

> **Note**
>
> ランブックの名前を選択すると、ランブックに関する情報を表示できます。

4. [Document details (ドキュメントの詳細)] セクションで、[Document version (ドキュメントのバージョン)] が実行するバージョンに設定されていることを確認します。システムには、次のバージョンのオプションが含まれています。

   - [ランタイムのデフォルトバージョン]: 自動化ランブックが定期的に更新され、新しいデフォルトバージョンが割り当てられている場合は、このオプションを選択します。
   - [ランタイムの最新バージョン]: 自動化ランブックが定期的に更新され、直前に更新されたバージョンを実行する場合は、このオプションを選択します。
   - [1 (デフォルト)]: ドキュメントの最初のバージョンを実行するには、このオプションを選択します。これはデフォルト設定です。

5. [Next] を選択します。
6. [オートメーションランブックの実行] セクションで、[シンプルな実行] を選択します。
7. [Input parameters (入力パラメータ)] セクションで、必要な入力を指定します。必要に応じて、[AutomationAssumeRole] リストから IAM サービスロールを選択できます。
8. (オプション) モニタリング用のオートメーションに適用する Amazon CloudWatch アラームを選択します。CloudWatch アラームをオートメーションにアタッチするには、コマンドを実行する IAM プリンシパルに `iam:createServiceLinkedRole` アクションの権限が必要です。CloudWatch アラームの詳細については、「Amazon CloudWatch でのアラームの使用」を参照してください。アラームが作動すると、オートメーションは停止されます。AWS CloudTrail を使用する場合、トレイルに API コールが表示されます。
9. [実行] を選択します。

ステップ 5 : クリーンアップ

ランブックを削除するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[ドキュメント] を選択します。
3. [自分が所有] タブを選択します。
4. [ビジュアルデザインエクスペリエンスチュートリアル] のランブックを探してください。

5. ドキュメントカードページのボタンを選択し、[アクション] ドロップダウンから [ドキュメントを削除] を選択します。

オートメーションランブックのオーサリング

AWS Systems Manager のツールである Automation の各ランブックは、オートメーションを定義します。オートメーションランブックは、オートメーション中に実行されるアクションを定義します。ランブックコンテンツでは、Systems Manager が管理対象インスタンスと AWS リソースで実行する入力パラメータ、出力、およびアクションを定義します。

Automation には、いくつかのランブックが事前に定義されており、1 つ以上の Amazon Elastic Compute Cloud (Amazon EC2) インスタンスの再起動や、Amazon Machine Image (AMI) の作成といった一般的なタスクを実行する際に使用することができます。ただし、ユースケースは、事前定義されたランブックの機能を超える場合があります。このような場合は、独自のランブックを作成し、必要に応じて変更することができます。

ランブックは、オートメーションアクション、それらのアクションのパラメータ、および指定した入力パラメータで構成されます。ランブックのコンテンツは YAML または JSON のいずれかで記述されています。YAML と JSON のどちらにも精通していない場合は、ビジュアルデザイナーを使用するか、独自のランブックを作成する前に、いずれかのマークアップ言語について学習することをお勧めします。ビジュアルデザイナーの詳細については、「オートメーションランブックのビジュアルデザインエクスペリエンス」を参照してください。

以降のセクションは、最初のランブックの作成に役立ちます。

ユースケースの特定

ランブック作成の最初のステップは、ユースケースの特定です。例えば、`AWS-CreateImage` ランブックを Amazon EC2 インスタンスのすべての本番環境で毎日実行するようにスケジューリングしたとします。月末に、イメージ数がリカバリーポイント用に必要な分を超えていると判断しました。今後は、Amazon EC2 インスタンスの AMI が新しく作成されるたびに、最も古い AMI から削除したいと考えました。これを行うには、次の処理を実行するランブックを新規作成します。

1. `aws:createImage` アクションを実行して、イメージの説明でインスタンス ID を指定します。
2. `aws:waitForAwsResourceProperty` アクションを実行して、`available` になるまでイメージの状態をポーリングします。
3. イメージの状態が `available` になると、`aws:executeScript` アクションがカスタム Python スクリプトを実行し、Amazon EC2 インスタンスに関連付けられている全イメージの ID を収集し

ます。スクリプトは、作成時に指定したイメージ記述のインスタンス ID を使用して、フィルタリングによってこれを実行します。次にスクリプトは、イメージの creationDate に基づいてイメージ ID のリストをソートし、最も古い AMI の ID を出力します。

4. 最後に、aws:deleteImage アクションが実行され、前のステップで出力された ID を使用して、最も古い AMI が削除されます。

このシナリオでは、既に AWS-CreateImage ランブックを使用してはいたものの、ユースケースではさらなる柔軟性が必要であることがわかりました。ランブックとオートメーションアクションが重複する可能性があるため、これは一般的な状況です。結果として、ユースケースに対処するために使用するランブックやアクションを調整する必要がある場合があります。

例えば、aws:executeScript と aws:invokeLambdaFunction のアクションでは、どちらでもオートメーションの一部としてカスタムスクリプトを実行できます。この 2 つの間では、サポートされているランタイム言語が追加されているため、aws:invokeLambdaFunction の方を選ぶことにになるかもしれません。ただし、スクリプトコンテンツを YAML ランブックで直接作成でき、スクリプトコンテンツを JSON ランブックの添付ファイルとして提供できるため、aws:executeScript の方がよいこともあります。また、aws:executeScript のほうが AWS Identity and Access Management (IAM) のセットアップという観点からはよりシンプルであるという点も検討すべきかもしれません。AutomationAssumeRole で提供されるアクセス許可を使用するため、aws:executeScript では、追加の AWS Lambda 関数の実行ロールは必要ありません。

特定のシナリオでは、あるアクションが別のアクションよりも柔軟性、または追加機能を提供する可能性があります。したがって、使用するランブックまたはアクションで使用可能な入力パラメータを確認して、ユースケースとプリファレンスに最適なものを判断することをお勧めします。

開発環境をセットアップする

ユースケースと、ランブックで使用する事前定義済みのランブックまたはオートメーションアクションを特定したら、ランブックのコンテンツ用に開発環境をセットアップします。ランブックコンテンツを開発するには、Systems Manager ドキュメントコンソールよりも AWS Toolkit for Visual Studio Code を使用することを推奨します。

Toolkit for VS Code は、Visual Studio Code (VS Code) のオープンソースの拡張機能であり、Systems Manager ドキュメントコンソールよりも多くの機能を提供します。便利な機能には、YAML と JSON の両方のスキーマ検証、オートメーションアクションタイプのスニペット、YAML と JSON の両方のさまざまなオプションのオートコンプリートのサポートなどがあります。

Toolkit for VS Code のインストールについては、AWS Toolkit for Visual Studio Code のインストールを参照してください。Toolkit for VS Code を使用してランブックを作成する方法については、AWS Toolkit for Visual Studio Code ユーザーガイドの「Systems Manager オートメーションドキュメントの使用」を参照してください。

ランブックコンテンツの開発

ユースケースを特定して環境をセットアップしたら、ランブック用のコンテンツを開発できます。ユースケースとプリファレンスは、ランブックコンテンツで使用するオートメーションアクションまたはランブックに大きく影響します。一部のアクションでは、同様のタスクを実行できる別のアクションと比較して、入力パラメータのサブセットのみがサポートされます。`aws:createImage` のように特定の出力を持つアクションがありますが、中には独自の出力 (`aws:executeAwsApi` など) を定義できるアクションもあります。

ランブックで特定のアクションを使用する方法がわからない場合は、Systems Manager Automation アクションのリファレンス のアクションに対応するエントリを見直すことをお勧めします。また、定義済みのランブックの内容を確認して、これらのアクションの使用方法の実例を確認することもお勧めします。ランブックの実際のアプリケーションの例については、その他のランブックの例 を参照してください。

ランブックのコンテンツが提供するシンプルさと柔軟性の違いを実証するために、以下のチュートリアルでは、Amazon EC2 インスタンスのグループに段階的にパッチを適用する方法の例を示します。

- the section called “例 1: 親子のランブックの作成” — この例では、2 つのランブックが親子関係で使用されています。親ランブックが、子ランブックのレート制御のオートメーションを開始します。
- the section called “例 2: スクリプト化されたランブック” — この例では、コンテンツを 1 つのランブックと判断してランブックでスクリプトを使用することにより、例 1 と同じタスクを実行する方法を示します。

例 1: 親子のランブックの作成

以下の例は、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのタグ付きグループに段階的にパッチを適用する 2 つのランブックを作成する方法を示しています。これらのランブックは、親ランブックを使用して子ランブックのレート制御のオートメーションを開始する、親子の関係で使用されます。レート制御のオートメーションの詳細については、「自動オペレーションを大規模に実行する」を参照してください。この例で使用されているオートメーションアクションの詳細については、「Systems Manager Automation アクションのリファレンス」を参照してください。

子ランブックの作成

このランブック例では、次のシナリオに対処します。Emily は AnyCompany Consultants, LLC のシステムエンジニアです。プライマリデータベースとセカンダリデータベースをホスティングしている Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのグループに対して、パッチ適用を設定する必要があります。アプリケーションはこれらのデータベースに 24 時間アクセスするため、データベースインスタンスのいずれかは常に利用可能でなければなりません。

彼女は、段階的にインスタンスにパッチを適用することが最善のアプローチであると判断しました。まずはデータベースインスタンスのプライマリグループにパッチが適用され、続いてデータベースインスタンスのセカンダリグループにパッチが適用される予定です。また、以前に停止したインスタンスを実行したままにすることで追加コストが発生しないように、Emily はパッチ適用されたインスタンスをパッチ適用前の元の状態に戻したいと考えています。

Emily は、インスタンスに関連付けられたタグによって、データベースインスタンスのプライマリグループとセカンダリグループを識別します。子ランブックのレート制御のオートメーションを開始する親ランブックを作成することにしました。これにより、データベースインスタンスのプライマリグループとセカンダリグループに関連付けられたタグをターゲットにし、子のオートメーションの同時実行を管理できます。パッチ適用に使用できる Systems Manager (SSM) ドキュメントを確認した後、`AWS-RunPatchBaseline` ドキュメントを選択します。この SSM ドキュメントを使用することで、同僚は、パッチ適用操作の完了後に、関連するパッチコンプライアンス情報を確認できます。

ランブックコンテンツの作成を開始するために、Emily は利用可能なオートメーションアクションを確認し、子ランブックのコンテンツの作成を次のように開始します。

1. まず、ランブックのスキーマの値と説明を提供し、子ランブックの入力パラメータを定義します。

   `AutomationAssumeRole` パラメータを使用すると、Emily とその同僚は、ランブックで彼らに代わってアクションを実行することをオートメーションに許可する既存の IAM ロールを使用できます。Emily は `InstanceId` パラメータを使用して、パッチを適用するインスタンスを決定します。オプションで、`Operation`、`RebootOption`、および `SnapshotId` パラメータを使用して、`AWS-RunPatchBaseline` のドキュメントパラメータに値を提供できます。これらのドキュメントパラメータに無効な値が提供されるのを防ぐために、必要に応じて `allowedValues` を定義します。

   YAML

   ```
   schemaVersion: '0.3'
   ```

```
description: 'An example of an Automation runbook that patches groups of Amazon
 EC2 instances in stages.'
assumeRole: '{{AutomationAssumeRole}}'
parameters:
  AutomationAssumeRole:
    type: String
    description: >-
      '(Optional) The Amazon Resource Name (ARN) of the IAM role that allows
 Automation to perform the
      actions on your behalf. If no role is specified, Systems Manager
      Automation uses your IAM permissions to operate this runbook.'
    default: ''
  InstanceId:
    type: String
    description: >-
      '(Required) The instance you want to patch.'
  SnapshotId:
    type: String
    description: '(Optional) The snapshot ID to use to retrieve a patch baseline
 snapshot.'
    default: ''
  RebootOption:
    type: String
    description: '(Optional) Reboot behavior after a patch Install operation. If
 you choose NoReboot and patches are installed, the instance is marked as non-
compliant until a subsequent reboot and scan.'
    allowedValues:
      - NoReboot
      - RebootIfNeeded
    default: RebootIfNeeded
  Operation:
    type: String
    description: '(Optional) The update or configuration to perform on the
 instance. The system checks if patches specified in the patch baseline are
 installed on the instance. The install operation installs patches missing from
 the baseline.'
    allowedValues:
      - Install
      - Scan
    default: Install
```

JSON

```
{
   "schemaVersion":"0.3",
   "description":"An example of an Automation runbook that patches groups of
 Amazon EC2 instances in stages.",
   "assumeRole":"{{AutomationAssumeRole}}",
   "parameters":{
      "AutomationAssumeRole":{
         "type":"String",
         "description":"(Optional) The Amazon Resource Name (ARN) of the IAM role
 that allows Automation to perform the actions on your behalf. If no role is
 specified, Systems Manager Automation uses your IAM permissions to operate this
 runbook.",
         "default":""
      },
      "InstanceId":{
         "type":"String",
         "description":"(Required) The instance you want to patch."
      },
      "SnapshotId":{
         "type":"String",
         "description":"(Optional) The snapshot ID to use to retrieve a patch
 baseline snapshot.",
         "default":""
      },
      "RebootOption":{
         "type":"String",
         "description":"(Optional) Reboot behavior after a patch Install
 operation. If you choose NoReboot and patches are installed, the instance is
 marked as non-compliant until a subsequent reboot and scan.",
         "allowedValues":[
            "NoReboot",
            "RebootIfNeeded"
         ],
         "default":"RebootIfNeeded"
      },
      "Operation":{
         "type":"String",
         "description":"(Optional) The update or configuration to perform on
 the instance. The system checks if patches specified in the patch baseline are
 installed on the instance. The install operation installs patches missing from
 the baseline.",
```

```
         "allowedValues":[
            "Install",
            "Scan"
         ],
         "default":"Install"
      }
   }
},
```

2. 最上位の要素が定義された状態で、Emily はランブックの mainSteps を構成するアクションの作成に進みます。最初のステップでは、aws:executeAwsApi アクションを使用して、InstanceId 出力パラメータで指定したターゲットインスタンスの現在の状態を出力します。このアクションの出力は、後のアクションで使用します。

   YAML

```
mainSteps:
  - name: getInstanceState
    action: 'aws:executeAwsApi'
    onFailure: Abort
    inputs:
      inputs:
      Service: ec2
      Api: DescribeInstances
      InstanceIds:
        - '{{InstanceId}}'
    outputs:
      - Name: instanceState
        Selector: '$.Reservations[0].Instances[0].State.Name'
        Type: String
    nextStep: branchOnInstanceState
```

   JSON

```
"mainSteps":[
      {
         "name":"getInstanceState",
         "action":"aws:executeAwsApi",
         "onFailure":"Abort",
         "inputs":{
            "inputs":null,
            "Service":"ec2",
            "Api":"DescribeInstances",
```

```
            "InstanceIds":[
               "{{InstanceId}}"
            ]
         },
         "outputs":[
            {
               "Name":"instanceState",
               "Selector":"$.Reservations[0].Instances[0].State.Name",
               "Type":"String"
            }
         ],
         "nextStep":"branchOnInstanceState"
      },
```

3. Emily は、手動で開始してパッチを適用する必要があるすべてのインスタンスの元の状態を追跡するのではなく、前のアクションの出力を使用して、ターゲットインスタンスの状態に基づいてオートメーションを分岐します。こうすることで、aws:branch アクションで定義される条件に応じてオートメーションで異なるステップを実行し、手動による介入なしにオートメーションの全体的な効率を向上させることができます。

   インスタンスの状態がすでに running の場合、aws:runCommand アクションを使用する AWS-RunPatchBaseline ドキュメントで、インスタンスにパッチを適用しオートメーションが進められます。

   インスタンスの状態が stopping の場合、オートメーションは aws:waitForAwsResourceProperty アクションを使用して stopped 状態になるまでインスタンスにポーリングし、executeAwsApi アクションを使用してインスタンスを起動し、インスタンスにパッチを適用する前に running の状態になるまでインスタンスにポーリングします。

   インスタンスの状態が stopped の場合、自動化によってインスタンスが起動され、インスタンスが running 状態になるまでポーリングしてから、同じアクションを使用してインスタンスにパッチを適用します。

   YAML

```
- name: branchOnInstanceState
    action: 'aws:branch'
    onFailure: Abort
    inputs:
      Choices:
        - NextStep: startInstance
          Variable: '{{getInstanceState.instanceState}}'
```

```
          StringEquals: stopped
        - NextStep: verifyInstanceStopped
          Variable: '{{getInstanceState.instanceState}}'
          StringEquals: stopping
        - NextStep: patchInstance
          Variable: '{{getInstanceState.instanceState}}'
          StringEquals: running
    isEnd: true
  - name: startInstance
    action: 'aws:executeAwsApi'
    onFailure: Abort
    inputs:
      Service: ec2
      Api: StartInstances
      InstanceIds:
        - '{{InstanceId}}'
    nextStep: verifyInstanceRunning
  - name: verifyInstanceRunning
    action: 'aws:waitForAwsResourceProperty'
    timeoutSeconds: 120
    inputs:
      Service: ec2
      Api: DescribeInstances
      InstanceIds:
        - '{{InstanceId}}'
      PropertySelector: '$.Reservations[0].Instances[0].State.Name'
      DesiredValues:
        - running
    nextStep: patchInstance
  - name: verifyInstanceStopped
    action: 'aws:waitForAwsResourceProperty'
    timeoutSeconds: 120
    inputs:
      Service: ec2
      Api: DescribeInstances
      InstanceIds:
        - '{{InstanceId}}'
      PropertySelector: '$.Reservations[0].Instances[0].State.Name'
      DesiredValues:
        - stopped
      nextStep: startInstance
  - name: patchInstance
    action: 'aws:runCommand'
    onFailure: Abort
```

```
    timeoutSeconds: 5400
    inputs:
      DocumentName: 'AWS-RunPatchBaseline'
      InstanceIds:
      - '{{InstanceId}}'
      Parameters:
        SnapshotId: '{{SnapshotId}}'
        RebootOption: '{{RebootOption}}'
        Operation: '{{Operation}}'
```

JSON

```
{
         "name":"branchOnInstanceState",
         "action":"aws:branch",
         "onFailure":"Abort",
         "inputs":{
            "Choices":[
               {
                  "NextStep":"startInstance",
                  "Variable":"{{getInstanceState.instanceState}}",
                  "StringEquals":"stopped"
               },
               {
                  "Or":[
                     {
                        "Variable":"{{getInstanceState.instanceState}}",
                        "StringEquals":"stopping"
                     }
                  ],
                  "NextStep":"verifyInstanceStopped"
               },
               {
                  "NextStep":"patchInstance",
                  "Variable":"{{getInstanceState.instanceState}}",
                  "StringEquals":"running"
               }
            ]
         },
         "isEnd":true
      },
      {
         "name":"startInstance",
```

```
            "action":"aws:executeAwsApi",
            "onFailure":"Abort",
            "inputs":{
               "Service":"ec2",
               "Api":"StartInstances",
               "InstanceIds":[
                  "{{InstanceId}}"
               ]
            },
            "nextStep":"verifyInstanceRunning"
         },
         {
            "name":"verifyInstanceRunning",
            "action":"aws:waitForAwsResourceProperty",
            "timeoutSeconds":120,
            "inputs":{
               "Service":"ec2",
               "Api":"DescribeInstances",
               "InstanceIds":[
                  "{{InstanceId}}"
               ],
               "PropertySelector":"$.Reservations[0].Instances[0].State.Name",
               "DesiredValues":[
                  "running"
               ]
            },
            "nextStep":"patchInstance"
         },
         {
            "name":"verifyInstanceStopped",
            "action":"aws:waitForAwsResourceProperty",
            "timeoutSeconds":120,
            "inputs":{
               "Service":"ec2",
               "Api":"DescribeInstances",
               "InstanceIds":[
                  "{{InstanceId}}"
               ],
               "PropertySelector":"$.Reservations[0].Instances[0].State.Name",
               "DesiredValues":[
                  "stopped"
               ],
               "nextStep":"startInstance"
            }
```

```
      },
      {
         "name":"patchInstance",
         "action":"aws:runCommand",
         "onFailure":"Abort",
         "timeoutSeconds":5400,
         "inputs":{
            "DocumentName":"AWS-RunPatchBaseline",
            "InstanceIds":[
               "{{InstanceId}}"
            ],
            "Parameters":{
               "SnapshotId":"{{SnapshotId}}",
               "RebootOption":"{{RebootOption}}",
               "Operation":"{{Operation}}"
            }
         }
      },
```

4. パッチ適用操作が完了した後、Emily は、オートメーションがターゲットインスタンスをオートメーション開始前と同じ状態に戻すようにしたいと考えています。これは、最初のアクションでの出力を再び使用して行います。オートメーションは、aws:branch アクションを使用してターゲットインスタンスの元の状態に基づいて分岐します。インスタンスが以前 running 以外の状態にあった場合、インスタンスは停止します。インスタンスの状態が running であれば、オートメーションが終了します。

   YAML

```
- name: branchOnOriginalInstanceState
    action: 'aws:branch'
    onFailure: Abort
    inputs:
      Choices:
        - NextStep: stopInstance
          Not:
            Variable: '{{getInstanceState.instanceState}}'
            StringEquals: running
    isEnd: true
  - name: stopInstance
    action: 'aws:executeAwsApi'
    onFailure: Abort
    inputs:
      Service: ec2
```

```
      Api: StopInstances
      InstanceIds:
        - '{{InstanceId}}'
```

JSON

```
{
        "name":"branchOnOriginalInstanceState",
        "action":"aws:branch",
        "onFailure":"Abort",
        "inputs":{
           "Choices":[
              {
                 "NextStep":"stopInstance",
                 "Not":{
                    "Variable":"{{getInstanceState.instanceState}}",
                    "StringEquals":"running"
                 }
              }
           ]
        },
        "isEnd":true
     },
     {
        "name":"stopInstance",
        "action":"aws:executeAwsApi",
        "onFailure":"Abort",
        "inputs":{
           "Service":"ec2",
           "Api":"StopInstances",
           "InstanceIds":[
              "{{InstanceId}}"
           ]
        }
     }
  ]
}
```

5. Emily は完成した子ランブックコンテンツをレビューし、ターゲットインスタンスと同じ AWS アカウント と AWS リージョン でランブックを作成します。これで、親ランブックのコンテンツの作成を続行する準備が整いました。完成した子ランブックのコンテンツは次のとおりです。

YAML

```
schemaVersion: '0.3'
description: 'An example of an Automation runbook that patches groups of Amazon
 EC2 instances in stages.'
assumeRole: '{{AutomationAssumeRole}}'
parameters:
  AutomationAssumeRole:
    type: String
    description: >-
      '(Optional) The Amazon Resource Name (ARN) of the IAM role that allows
 Automation to perform the
      actions on your behalf. If no role is specified, Systems Manager
      Automation uses your IAM permissions to operate this runbook.'
    default: ''
  InstanceId:
    type: String
    description: >-
      '(Required) The instance you want to patch.'
  SnapshotId:
    type: String
    description: '(Optional) The snapshot ID to use to retrieve a patch baseline
 snapshot.'
    default: ''
  RebootOption:
    type: String
    description: '(Optional) Reboot behavior after a patch Install operation. If
 you choose NoReboot and patches are installed, the instance is marked as non-
compliant until a subsequent reboot and scan.'
    allowedValues:
      - NoReboot
      - RebootIfNeeded
    default: RebootIfNeeded
  Operation:
    type: String
    description: '(Optional) The update or configuration to perform on the
 instance. The system checks if patches specified in the patch baseline are
 installed on the instance. The install operation installs patches missing from
 the baseline.'
    allowedValues:
      - Install
      - Scan
    default: Install
```

```
mainSteps:
  - name: getInstanceState
    action: 'aws:executeAwsApi'
    onFailure: Abort
    inputs:
      inputs:
      Service: ec2
      Api: DescribeInstances
      InstanceIds:
        - '{{InstanceId}}'
    outputs:
      - Name: instanceState
        Selector: '$.Reservations[0].Instances[0].State.Name'
        Type: String
    nextStep: branchOnInstanceState
  - name: branchOnInstanceState
    action: 'aws:branch'
    onFailure: Abort
    inputs:
      Choices:
        - NextStep: startInstance
          Variable: '{{getInstanceState.instanceState}}'
          StringEquals: stopped
        - Or:
            - Variable: '{{getInstanceState.instanceState}}'
              StringEquals: stopping
          NextStep: verifyInstanceStopped
        - NextStep: patchInstance
          Variable: '{{getInstanceState.instanceState}}'
          StringEquals: running
    isEnd: true
  - name: startInstance
    action: 'aws:executeAwsApi'
    onFailure: Abort
    inputs:
      Service: ec2
      Api: StartInstances
      InstanceIds:
        - '{{InstanceId}}'
    nextStep: verifyInstanceRunning
  - name: verifyInstanceRunning
    action: 'aws:waitForAwsResourceProperty'
    timeoutSeconds: 120
    inputs:
```

```
      Service: ec2
      Api: DescribeInstances
      InstanceIds:
        - '{{InstanceId}}'
      PropertySelector: '$.Reservations[0].Instances[0].State.Name'
      DesiredValues:
        - running
    nextStep: patchInstance
  - name: verifyInstanceStopped
    action: 'aws:waitForAwsResourceProperty'
    timeoutSeconds: 120
    inputs:
      Service: ec2
      Api: DescribeInstances
      InstanceIds:
        - '{{InstanceId}}'
      PropertySelector: '$.Reservations[0].Instances[0].State.Name'
      DesiredValues:
        - stopped
      nextStep: startInstance
  - name: patchInstance
    action: 'aws:runCommand'
    onFailure: Abort
    timeoutSeconds: 5400
    inputs:
      DocumentName: 'AWS-RunPatchBaseline'
      InstanceIds:
      - '{{InstanceId}}'
      Parameters:
        SnapshotId: '{{SnapshotId}}'
        RebootOption: '{{RebootOption}}'
        Operation: '{{Operation}}'
  - name: branchOnOriginalInstanceState
    action: 'aws:branch'
    onFailure: Abort
    inputs:
      Choices:
        - NextStep: stopInstance
          Not:
            Variable: '{{getInstanceState.instanceState}}'
            StringEquals: running
    isEnd: true
  - name: stopInstance
    action: 'aws:executeAwsApi'
```

```
    onFailure: Abort
    inputs:
      Service: ec2
      Api: StopInstances
      InstanceIds:
        - '{{InstanceId}}'
```

JSON

```
{
   "schemaVersion":"0.3",
   "description":"An example of an Automation runbook that patches groups of
 Amazon EC2 instances in stages.",
   "assumeRole":"{{AutomationAssumeRole}}",
   "parameters":{
      "AutomationAssumeRole":{
         "type":"String",
         "description":"'(Optional) The Amazon Resource Name (ARN) of the IAM
 role that allows Automation to perform the actions on your behalf. If no role is
 specified, Systems Manager Automation uses your IAM permissions to operate this
 runbook.'",
         "default":""
      },
      "InstanceId":{
         "type":"String",
         "description":"'(Required) The instance you want to patch.'"
      },
      "SnapshotId":{
         "type":"String",
         "description":"(Optional) The snapshot ID to use to retrieve a patch
 baseline snapshot.",
         "default":""
      },
      "RebootOption":{
         "type":"String",
         "description":"(Optional) Reboot behavior after a patch Install
 operation. If you choose NoReboot and patches are installed, the instance is
 marked as non-compliant until a subsequent reboot and scan.",
         "allowedValues":[
            "NoReboot",
            "RebootIfNeeded"
         ],
         "default":"RebootIfNeeded"
```

```
      },
      "Operation":{
         "type":"String",
         "description":"(Optional) The update or configuration to perform on
the instance. The system checks if patches specified in the patch baseline are
installed on the instance. The install operation installs patches missing from
the baseline.",
         "allowedValues":[
            "Install",
            "Scan"
         ],
         "default":"Install"
      }
   },
   "mainSteps":[
      {
         "name":"getInstanceState",
         "action":"aws:executeAwsApi",
         "onFailure":"Abort",
         "inputs":{
            "inputs":null,
            "Service":"ec2",
            "Api":"DescribeInstances",
            "InstanceIds":[
               "{{InstanceId}}"
            ]
         },
         "outputs":[
            {
               "Name":"instanceState",
               "Selector":"$.Reservations[0].Instances[0].State.Name",
               "Type":"String"
            }
         ],
         "nextStep":"branchOnInstanceState"
      },
      {
         "name":"branchOnInstanceState",
         "action":"aws:branch",
         "onFailure":"Abort",
         "inputs":{
            "Choices":[
               {
                  "NextStep":"startInstance",
```

```
                "Variable":"{{getInstanceState.instanceState}}",
                "StringEquals":"stopped"
             },
             {
                "Or":[
                   {
                      "Variable":"{{getInstanceState.instanceState}}",
                      "StringEquals":"stopping"
                   }
                ],
                "NextStep":"verifyInstanceStopped"
             },
             {
                "NextStep":"patchInstance",
                "Variable":"{{getInstanceState.instanceState}}",
                "StringEquals":"running"
             }
          ]
       },
       "isEnd":true
    },
    {
       "name":"startInstance",
       "action":"aws:executeAwsApi",
       "onFailure":"Abort",
       "inputs":{
          "Service":"ec2",
          "Api":"StartInstances",
          "InstanceIds":[
             "{{InstanceId}}"
          ]
       },
       "nextStep":"verifyInstanceRunning"
    },
    {
       "name":"verifyInstanceRunning",
       "action":"aws:waitForAwsResourceProperty",
       "timeoutSeconds":120,
       "inputs":{
          "Service":"ec2",
          "Api":"DescribeInstances",
          "InstanceIds":[
             "{{InstanceId}}"
          ],
```

```
            "PropertySelector":"$.Reservations[0].Instances[0].State.Name",
            "DesiredValues":[
               "running"
            ]
         },
         "nextStep":"patchInstance"
      },
      {
         "name":"verifyInstanceStopped",
         "action":"aws:waitForAwsResourceProperty",
         "timeoutSeconds":120,
         "inputs":{
            "Service":"ec2",
            "Api":"DescribeInstances",
            "InstanceIds":[
               "{{InstanceId}}"
            ],
            "PropertySelector":"$.Reservations[0].Instances[0].State.Name",
            "DesiredValues":[
               "stopped"
            ],
            "nextStep":"startInstance"
         }
      },
      {
         "name":"patchInstance",
         "action":"aws:runCommand",
         "onFailure":"Abort",
         "timeoutSeconds":5400,
         "inputs":{
            "DocumentName":"AWS-RunPatchBaseline",
            "InstanceIds":[
               "{{InstanceId}}"
            ],
            "Parameters":{
               "SnapshotId":"{{SnapshotId}}",
               "RebootOption":"{{RebootOption}}",
               "Operation":"{{Operation}}"
            }
         }
      },
      {
         "name":"branchOnOriginalInstanceState",
         "action":"aws:branch",
```

```
            "onFailure":"Abort",
            "inputs":{
               "Choices":[
                  {
                     "NextStep":"stopInstance",
                     "Not":{
                        "Variable":"{{getInstanceState.instanceState}}",
                        "StringEquals":"running"
                     }
                  }
               ]
            },
            "isEnd":true
         },
         {
            "name":"stopInstance",
            "action":"aws:executeAwsApi",
            "onFailure":"Abort",
            "inputs":{
               "Service":"ec2",
               "Api":"StopInstances",
               "InstanceIds":[
                  "{{InstanceId}}"
               ]
            }
         }
      ]
}
```

この例で使用されているオートメーションアクションの詳細については、「Systems Manager Automation アクションのリファレンス」を参照してください。

親ランブックの作成

この例のランブックのシナリオは、前のセクションで説明したシナリオと同じです。子ランブックを作成した Emily は、次のように親ランブックのコンテンツの作成を開始します。

1. まず、ランブックのスキーマの値と説明を提供し、親ランブックの入力パラメータを定義します。

   AutomationAssumeRole パラメータを使用すると、Emily とその同僚は、ランブックで彼らに代わってアクションを実行することをオートメーションに許可する既存の IAM ロールを使用でき

ます。Emily は PatchGroupPrimaryKey と PatchGroupPrimaryValue のパラメータを使用して、パッチを適用するデータベースインスタンスのプライマリグループに関連付けられたタグを指定します。PatchGroupSecondaryKey と PatchGroupSecondaryValue のパラメータを使用して、パッチを適用するデータベースインスタンスのセカンダリグループに関連付けられたタグを指定します。

YAML

```
description: 'An example of an Automation runbook that patches groups of Amazon
 EC2 instances in stages.'
schemaVersion: '0.3'
assumeRole: '{{AutomationAssumeRole}}'
parameters:
  AutomationAssumeRole:
    type: String
    description: '(Optional) The Amazon Resource Name (ARN) of the IAM role that
 allows Automation to perform the actions on your behalf. If no role is specified,
 Systems Manager Automation uses your IAM permissions to operate this runbook.'
    default: ''
  PatchGroupPrimaryKey:
    type: String
    description: '(Required) The key of the tag for the primary group of instances
 you want to patch.''
  PatchGroupPrimaryValue:
    type: String
    description: '(Required) The value of the tag for the primary group of
 instances you want to patch.'
  PatchGroupSecondaryKey:
    type: String
    description: '(Required) The key of the tag for the secondary group of
 instances you want to patch.'
  PatchGroupSecondaryValue:
    type: String
    description: '(Required) The value of the tag for the secondary group of
 instances you want to patch.'
```

JSON

```
{
   "schemaVersion": "0.3",
   "description": "An example of an Automation runbook that patches groups of
 Amazon EC2 instances in stages.",
   "assumeRole": "{{AutomationAssumeRole}}",
```

```
  "parameters": {
     "AutomationAssumeRole": {
        "type": "String",
        "description": "(Optional) The Amazon Resource Name (ARN) of the IAM
role that allows Automation to perform the actions on your behalf. If no role is
specified, Systems Manager Automation uses your IAM permissions to operate this
runbook.",
        "default": ""
     },
     "PatchGroupPrimaryKey": {
        "type": "String",
        "description": "(Required) The key of the tag for the primary group of
instances you want to patch."
     },
     "PatchGroupPrimaryValue": {
        "type": "String",
        "description": "(Required) The value of the tag for the primary group of
instances you want to patch."
     },
     "PatchGroupSecondaryKey": {
        "type": "String",
        "description": "(Required) The key of the tag for the secondary group of
instances you want to patch."
     },
     "PatchGroupSecondaryValue": {
        "type": "String",
        "description": "(Required) The value of the tag for the secondary group
of instances you want to patch."
     }
  }
},
```

2. 最上位の要素が定義された状態で、Emily はランブックの mainSteps を構成するアクションの作成に進みます。

   最初のアクションは、作成した子ランブックを使用してレート制御のオートメーションを開始します。この子ランブックは、PatchGroupPrimaryKey と PatchGroupPrimaryValue の入力パラメータで指定されるタグに関連付けられたインスタンスをターゲットしています。入力パラメータに指定された値を使用して、パッチを適用するデータベースインスタンスのプライマリグループに関連付けられたタグのキーと値を指定します。

   最初のオートメーションが完了すると、2 番目のアクションが子ランブックを使用して別のレート制御のオートメーションを開始します。この子ランブックは、PatchGroupSecondaryKey と

PatchGroupSecondaryValue の入力パラメータで指定されるタグに関連付けられたインスタンスをターゲットしています。入力パラメータに指定された値を使用して、パッチを適用するデータベースインスタンスのセカンダリグループに関連付けられたタグのキーと値を指定します。

YAML

```
mainSteps:
  - name: patchPrimaryTargets
    action: 'aws:executeAutomation'
    onFailure: Abort
    timeoutSeconds: 7200
    inputs:
      DocumentName: RunbookTutorialChildAutomation
      Targets:
        - Key: 'tag:{{PatchGroupPrimaryKey}}'
          Values:
            - '{{PatchGroupPrimaryValue}}'
      TargetParameterName: 'InstanceId'
  - name: patchSecondaryTargets
    action: 'aws:executeAutomation'
    onFailure: Abort
    timeoutSeconds: 7200
    inputs:
      DocumentName: RunbookTutorialChildAutomation
      Targets:
        - Key: 'tag:{{PatchGroupSecondaryKey}}'
          Values:
            - '{{PatchGroupSecondaryValue}}'
      TargetParameterName: 'InstanceId'
```

JSON

```
"mainSteps":[
      {
         "name":"patchPrimaryTargets",
         "action":"aws:executeAutomation",
         "onFailure":"Abort",
         "timeoutSeconds":7200,
         "inputs":{
            "DocumentName":"RunbookTutorialChildAutomation",
            "Targets":[
               {
                  "Key":"tag:{{PatchGroupPrimaryKey}}",
```

```
                  "Values":[
                     "{{PatchGroupPrimaryValue}}"
                  ]
               }
            ],
            "TargetParameterName":"InstanceId"
         }
      },
      {
         "name":"patchSecondaryTargets",
         "action":"aws:executeAutomation",
         "onFailure":"Abort",
         "timeoutSeconds":7200,
         "inputs":{
            "DocumentName":"RunbookTutorialChildAutomation",
            "Targets":[
               {
                  "Key":"tag:{{PatchGroupSecondaryKey}}",
                  "Values":[
                     "{{PatchGroupSecondaryValue}}"
                  ]
               }
            ],
            "TargetParameterName":"InstanceId"
         }
      }
   ]
}
```

3. Emily は完成した親ランブックコンテンツをレビューし、ターゲットインスタンスと同じ AWS アカウント と AWS リージョン でランブックを作成します。これで、ランブックをテストして、オートメーションが希望どおりに動作していることを確認してから、本番環境に実装する準備が整いました。完成した親ランブックのコンテンツは次のとおりです。

   YAML

```
description: An example of an Automation runbook that patches groups of Amazon EC2
 instances in stages.
schemaVersion: '0.3'
assumeRole: '{{AutomationAssumeRole}}'
parameters:
  AutomationAssumeRole:
    type: String
```

```
    description: '(Optional) The Amazon Resource Name (ARN) of the IAM role that
 allows Automation to perform the actions on your behalf. If no role is specified,
 Systems Manager Automation uses your IAM permissions to operate this runbook.'
    default: ''
  PatchGroupPrimaryKey:
    type: String
    description: (Required) The key of the tag for the primary group of instances
 you want to patch.
  PatchGroupPrimaryValue:
    type: String
    description: '(Required) The value of the tag for the primary group of
 instances you want to patch. '
  PatchGroupSecondaryKey:
    type: String
    description: (Required) The key of the tag for the secondary group of
 instances you want to patch.
  PatchGroupSecondaryValue:
    type: String
    description: '(Required) The value of the tag for the secondary group of
 instances you want to patch.  '
mainSteps:
  - name: patchPrimaryTargets
    action: 'aws:executeAutomation'
    onFailure: Abort
    timeoutSeconds: 7200
    inputs:
      DocumentName: RunbookTutorialChildAutomation
      Targets:
        - Key: 'tag:{{PatchGroupPrimaryKey}}'
          Values:
            - '{{PatchGroupPrimaryValue}}'
      TargetParameterName: 'InstanceId'
  - name: patchSecondaryTargets
    action: 'aws:executeAutomation'
    onFailure: Abort
    timeoutSeconds: 7200
    inputs:
      DocumentName: RunbookTutorialChildAutomation
      Targets:
        - Key: 'tag:{{PatchGroupSecondaryKey}}'
          Values:
            - '{{PatchGroupSecondaryValue}}'
      TargetParameterName: 'InstanceId'
```

JSON

```
{
   "description":"An example of an Automation runbook that patches groups of
 Amazon EC2 instances in stages.",
  "schemaVersion":"0.3",
  "assumeRole":"{{AutomationAssumeRole}}",
  "parameters":{
     "AutomationAssumeRole":{
        "type":"String",
        "description":"(Optional) The Amazon Resource Name (ARN) of the IAM role
 that allows Automation to perform the actions on your behalf. If no role is
 specified, Systems Manager Automation uses your IAM permissions to operate this
 runbook.",
        "default":""
     },
     "PatchGroupPrimaryKey":{
        "type":"String",
        "description":"(Required) The key of the tag for the primary group of
instances you want to patch."
     },
     "PatchGroupPrimaryValue":{
        "type":"String",
        "description":"(Required) The value of the tag for the primary group of
instances you want to patch. "
     },
     "PatchGroupSecondaryKey":{
        "type":"String",
        "description":"(Required) The key of the tag for the secondary group of
instances you want to patch."
     },
     "PatchGroupSecondaryValue":{
        "type":"String",
        "description":"(Required) The value of the tag for the secondary group of
instances you want to patch.  "
     }
  },
  "mainSteps":[
     {
        "name":"patchPrimaryTargets",
        "action":"aws:executeAutomation",
        "onFailure":"Abort",
        "timeoutSeconds":7200,
```

```
         "inputs":{
            "DocumentName":"RunbookTutorialChildAutomation",
            "Targets":[
               {
                  "Key":"tag:{{PatchGroupPrimaryKey}}",
                  "Values":[
                     "{{PatchGroupPrimaryValue}}"
                  ]
               }
            ],
            "TargetParameterName":"InstanceId"
         }
      },
      {
         "name":"patchSecondaryTargets",
         "action":"aws:executeAutomation",
         "onFailure":"Abort",
         "timeoutSeconds":7200,
         "inputs":{
            "DocumentName":"RunbookTutorialChildAutomation",
            "Targets":[
               {
                  "Key":"tag:{{PatchGroupSecondaryKey}}",
                  "Values":[
                     "{{PatchGroupSecondaryValue}}"
                  ]
               }
            ],
            "TargetParameterName":"InstanceId"
         }
      }
   ]
}
```

この例で使用されているオートメーションアクションの詳細については、「Systems Manager Automation アクションのリファレンス」を参照してください。

例 2: スクリプト化されたランブック

このランブック例では、次のシナリオに対処します。Emily は AnyCompany Consultants, LLC のシステムエンジニアです。彼女は先に、プライマリデータベースとセカンダリデータベースをホスティングする Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのパッチグループに対して、

親子関係で使用されるランブックを 2 つ作成しました。アプリケーションはこれらのデータベースに 24 時間アクセスするため、データベースインスタンスのいずれかは常に利用可能でなければなりません。

この要件に基づいて、彼女は AWS-RunPatchBaseline Systems Manager (SSM) ドキュメントを使用してインスタンスを段階的にパッチするソリューションを構築しました。この SSM ドキュメントを使用することで、同僚は、パッチ適用操作の完了後に、関連するパッチコンプライアンス情報を確認できます。

まずはデータベースインスタンスのプライマリグループにパッチが適用され、続いてデータベースインスタンスのセカンダリグループにパッチが適用されます。また、以前に停止したインスタンスを実行したままにすることで追加コストが発生しないように、Emily は、オートメーションがパッチ適用されたインスタンスをパッチ適用前の元の状態に戻したことを確認しました。Emily は、データベースインスタンスのプライマリグループとセカンダリグループに関連付けられたタグを使用して、パッチを適用する必要があるインスタンスを希望する順序で特定しました。

既存の自動ソリューションは機能しますが、可能であればソリューションを改善したいと考えています。ランブックコンテンツのメンテナンスを支援し、トラブルシューティングを容易にするため、オートメーションを 1 つのランブックにまとめて、入力パラメータの数を簡素化したいと考えています。また、複数の子オートメーションは作成しないようにしたいと考えています。

利用可能なオートメーションアクションを確認した後、Emily は、aws:executeScript アクションを使用すればソリューションをさらに改善し、カスタム Python スクリプトを実行できると判断しました。次のようにランブックのコンテンツの作成を開始しました。

1. まず、ランブックのスキーマの値と説明を提供し、親ランブックの入力パラメータを定義します。

   AutomationAssumeRole パラメータを使用すると、Emily とその同僚は、ランブックで彼らに代わってアクションを実行することをオートメーションに許可する既存の IAM ロールを使用できます。例 1 とは異なり、AutomationAssumeRole パラメータはオプションではなく必須になりました。このランブックには aws:executeScript アクションが含まれるため、AWS Identity and Access Management (IAM) サービスロール (または継承ロール) が常に必要です。アクションに指定された Python スクリプトの一部が AWS API オペレーションを呼び出すため、この要件が必要になります。

   Emily は PrimaryPatchGroupTag と SecondaryPatchGroupTag のパラメータを使用して、パッチを適用するデータベースインスタンスのプライマリグループとセカンダリグループに関連付けられたタグを指定します。必要な入力パラメータを単純化するために、例 1 のランブック

で使用したように複数の String パラメータを使用するのではなく、StringMap パラメータを使用することにしました。オプションで、Operation、RebootOption、および SnapshotId パラメータを使用して、AWS-RunPatchBaseline のドキュメントパラメータに値を提供できます。これらのドキュメントパラメータに無効な値が提供されるのを防ぐために、必要に応じて allowedValues を定義します。

YAML

```
description: 'An example of an Automation runbook that patches groups of Amazon
 EC2 instances in stages.'
schemaVersion: '0.3'
assumeRole: '{{AutomationAssumeRole}}'
parameters:
  AutomationAssumeRole:
    type: String
    description: '(Required) The Amazon Resource Name (ARN) of the IAM role that
 allows Automation to perform the actions on your behalf. If no role is specified,
 Systems Manager Automation uses your IAM permissions to operate this runbook.'
  PrimaryPatchGroupTag:
    type: StringMap
    description: '(Required) The tag for the primary group of instances you want
 to patch. Specify a key-value pair. Example: {"key" : "value"}'
  SecondaryPatchGroupTag:
    type: StringMap
    description: '(Required) The tag for the secondary group of instances you want
 to patch. Specify a key-value pair. Example: {"key" : "value"}'
  SnapshotId:
    type: String
    description: '(Optional) The snapshot ID to use to retrieve a patch baseline
 snapshot.'
    default: ''
  RebootOption:
    type: String
    description: '(Optional) Reboot behavior after a patch Install operation. If
 you choose NoReboot and patches are installed, the instance is marked as non-
compliant until a subsequent reboot and scan.'
    allowedValues:
      - NoReboot
      - RebootIfNeeded
    default: RebootIfNeeded
  Operation:
    type: String
```

```
   description: '(Optional) The update or configuration to perform on the
instance. The system checks if patches specified in the patch baseline are
installed on the instance. The install operation installs patches missing from
the baseline.'
   allowedValues:
     - Install
     - Scan
   default: Install
```

JSON

```
{
  "description":"An example of an Automation runbook that patches groups of
Amazon EC2 instances in stages.",
  "schemaVersion":"0.3",
  "assumeRole":"{{AutomationAssumeRole}}",
  "parameters":{
     "AutomationAssumeRole":{
        "type":"String",
        "description":"(Required) The Amazon Resource Name (ARN) of the IAM role
that allows Automation to perform the actions on your behalf. If no role is
specified, Systems Manager Automation uses your IAM permissions to operate this
runbook."
     },
     "PrimaryPatchGroupTag":{
        "type":"StringMap",
        "description":"(Required) The tag for the primary group of instances you
want to patch. Specify a key-value pair. Example: {\"key\" : \"value\"}"
     },
     "SecondaryPatchGroupTag":{
        "type":"StringMap",
        "description":"(Required) The tag for the secondary group of instances
you want to patch. Specify a key-value pair. Example: {\"key\" : \"value\"}"
     },
     "SnapshotId":{
        "type":"String",
        "description":"(Optional) The snapshot ID to use to retrieve a patch
baseline snapshot.",
        "default":""
     },
     "RebootOption":{
        "type":"String",
```

```
        "description":"(Optional) Reboot behavior after a patch Install
 operation. If you choose NoReboot and patches are installed, the instance is
 marked as non-compliant until a subsequent reboot and scan.",
        "allowedValues":[
           "NoReboot",
           "RebootIfNeeded"
        ],
        "default":"RebootIfNeeded"
     },
     "Operation":{
        "type":"String",
        "description":"(Optional) The update or configuration to perform on
 the instance. The system checks if patches specified in the patch baseline are
 installed on the instance. The install operation installs patches missing from
 the baseline.",
        "allowedValues":[
           "Install",
           "Scan"
        ],
        "default":"Install"
     }
   }
},
```

2. 最上位の要素が定義された状態で、Emily はランブックの mainSteps を構成するアクションの作成に進みます。最初のステップでは、PrimaryPatchGroupTag パラメータで指定されるタグに関連付けられたすべてのインスタンスの ID を収集し、インスタンス ID とインスタンスの現在の状態を含む StringMap パラメータを出力します。このアクションの出力は、後のアクションで使用します。

   script 入力パラメータは、JSON ランブックではサポートされていませんのでご注意ください。JSON ランブックでは、attachment 入力パラメータを使用してスクリプトコンテンツを指定する必要があります。

   YAML

```
mainSteps:
  - name: getPrimaryInstanceState
    action: 'aws:executeScript'
    timeoutSeconds: 120
    onFailure: Abort
    inputs:
      Runtime: python3.7
```

```
      Handler: getInstanceStates
      InputPayload:
        primaryTag: '{{PrimaryPatchGroupTag}}'
      Script: |-
        def getInstanceStates(events,context):
          import boto3

          #Initialize client
          ec2 = boto3.client('ec2')
          tag = events['primaryTag']
          tagKey, tagValue = list(tag.items())[0]
          instanceQuery = ec2.describe_instances(
          Filters=[
              {
                  "Name": "tag:" + tagKey,
                  "Values": [tagValue]
              }]
          )
          if not instanceQuery['Reservations']:
              noInstancesForTagString = "No instances found for specified tag."
              return({ 'noInstancesFound' : noInstancesForTagString })
          else:
              queryResponse = instanceQuery['Reservations']
              originalInstanceStates = {}
              for results in queryResponse:
                  instanceSet = results['Instances']
                  for instance in instanceSet:
                      instanceId = instance['InstanceId']
                      originalInstanceStates[instanceId] = instance['State']
['Name']
              return originalInstanceStates
    outputs:
      - Name: originalInstanceStates
        Selector: $.Payload
        Type: StringMap
    nextStep: verifyPrimaryInstancesRunning
```

JSON

```
"mainSteps":[
      {
         "name":"getPrimaryInstanceState",
         "action":"aws:executeScript",
```

```
         "timeoutSeconds":120,
         "onFailure":"Abort",
         "inputs":{
            "Runtime":"python3.7",
            "Handler":"getInstanceStates",
            "InputPayload":{
               "primaryTag":"{{PrimaryPatchGroupTag}}"
            },
            "Script":"..."
         },
         "outputs":[
            {
               "Name":"originalInstanceStates",
               "Selector":"$.Payload",
               "Type":"StringMap"
            }
         ],
         "nextStep":"verifyPrimaryInstancesRunning"
      },
```

3. Emily は、前のアクションの出力を別の aws:executeScript アクションで使用して、PrimaryPatchGroupTag パラメータで指定されたタグに関連付けられたすべてのインスタンスが running の状態にあることを検証します。

   インスタンスの状態がすでに running または shutting-down の場合、スクリプトは残りのインスタンスをループし続けます。

   インスタンスの状態が stopping の場合、スクリプトは stopped の状態になるまでインスタンスにポーリングし、インスタンスを起動します。

   インスタンスの状態が stopped の場合、スクリプトはインスタンスを起動します。

   YAML

```
- name: verifyPrimaryInstancesRunning
    action: 'aws:executeScript'
    timeoutSeconds: 600
    onFailure: Abort
    inputs:
      Runtime: python3.7
      Handler: verifyInstancesRunning
      InputPayload:
        targetInstances: '{{getPrimaryInstanceState.originalInstanceStates}}'
```

```
      Script: |-
        def verifyInstancesRunning(events,context):
          import boto3

          #Initialize client
          ec2 = boto3.client('ec2')
          instanceDict = events['targetInstances']
          for instance in instanceDict:
            if instanceDict[instance] == 'stopped':
                print("The target instance " + instance + " is stopped. The
 instance will now be started.")
                ec2.start_instances(
                    InstanceIds=[instance]
                    )
            elif instanceDict[instance] == 'stopping':
                print("The target instance " + instance + " is stopping. Polling
 for instance to reach stopped state.")
                while instanceDict[instance] != 'stopped':
                    poll = ec2.get_waiter('instance_stopped')
                    poll.wait(
                        InstanceIds=[instance]
                    )
                ec2.start_instances(
                    InstanceIds=[instance]
                )
            else:
              pass
    nextStep: waitForPrimaryRunningInstances
```

JSON

```
{
         "name":"verifyPrimaryInstancesRunning",
         "action":"aws:executeScript",
         "timeoutSeconds":600,
         "onFailure":"Abort",
         "inputs":{
            "Runtime":"python3.7",
            "Handler":"verifyInstancesRunning",
            "InputPayload":{

 "targetInstances":"{{getPrimaryInstanceState.originalInstanceStates}}"
            },
```

```
            "Script":"..."
         },
         "nextStep":"waitForPrimaryRunningInstances"
      },
```

4. Emily は、PrimaryPatchGroupTag パラメータで指定されたタグに関連付けられたすべてのインスタンスが開始されているか、もしくは既に running の状態にあることを検証します。次に、別のスクリプトを使用して、前のアクションで開始されたインスタンスも含め、すべてのインスタンスが running の状態に到達していることを確認します。

   YAML

```
- name: waitForPrimaryRunningInstances
    action: 'aws:executeScript'
    timeoutSeconds: 300
    onFailure: Abort
    inputs:
      Runtime: python3.7
      Handler: waitForRunningInstances
      InputPayload:
        targetInstances: '{{getPrimaryInstanceState.originalInstanceStates}}'
      Script: |-
        def waitForRunningInstances(events,context):
          import boto3

          #Initialize client
          ec2 = boto3.client('ec2')
          instanceDict = events['targetInstances']
          for instance in instanceDict:
              poll = ec2.get_waiter('instance_running')
              poll.wait(
                  InstanceIds=[instance]
              )
    nextStep: returnPrimaryTagKey
```

   JSON

```
{
         "name":"waitForPrimaryRunningInstances",
         "action":"aws:executeScript",
         "timeoutSeconds":300,
         "onFailure":"Abort",
         "inputs":{
```

```
            "Runtime":"python3.7",
            "Handler":"waitForRunningInstances",
            "InputPayload":{

 "targetInstances":"{{getPrimaryInstanceState.originalInstanceStates}}"
            },
            "Script":"..."
         },
         "nextStep":"returnPrimaryTagKey"
      },
```

5. Emilyは、さらに 2 つのスクリプトを使用して、PrimaryPatchGroupTag パラメータで指定された個々のキー String の値とのタグの値を返します。これらのアクションで返された値により、AWS-RunPatchBaseline ドキュメントの Targets パラメータに直接値を提供できます。その後、aws:runCommand アクションを使用する AWS-RunPatchBaseline ドキュメントで、インスタンスにパッチを適用しオートメーションが進められます。

   YAML

```
- name: returnPrimaryTagKey
    action: 'aws:executeScript'
    timeoutSeconds: 120
    onFailure: Abort
    inputs:
      Runtime: python3.7
      Handler: returnTagValues
      InputPayload:
        primaryTag: '{{PrimaryPatchGroupTag}}'
      Script: |-
        def returnTagValues(events,context):
          tag = events['primaryTag']
          tagKey = list(tag)[0]
          stringKey = "tag:" + tagKey
          return {'tagKey' : stringKey}
    outputs:
      - Name: Payload
        Selector: $.Payload
        Type: StringMap
      - Name: primaryPatchGroupKey
        Selector: $.Payload.tagKey
        Type: String
    nextStep: returnPrimaryTagValue
  - name: returnPrimaryTagValue
```

```
    action: 'aws:executeScript'
    timeoutSeconds: 120
    onFailure: Abort
    inputs:
      Runtime: python3.7
      Handler: returnTagValues
      InputPayload:
        primaryTag: '{{PrimaryPatchGroupTag}}'
      Script: |-
        def returnTagValues(events,context):
          tag = events['primaryTag']
          tagKey = list(tag)[0]
          tagValue = tag[tagKey]
          return {'tagValue' : tagValue}
    outputs:
      - Name: Payload
        Selector: $.Payload
        Type: StringMap
      - Name: primaryPatchGroupValue
        Selector: $.Payload.tagValue
        Type: String
    nextStep: patchPrimaryInstances
  - name: patchPrimaryInstances
    action: 'aws:runCommand'
    onFailure: Abort
    timeoutSeconds: 7200
    inputs:
      DocumentName: AWS-RunPatchBaseline
      Parameters:
        SnapshotId: '{{SnapshotId}}'
        RebootOption: '{{RebootOption}}'
        Operation: '{{Operation}}'
      Targets:
        - Key: '{{returnPrimaryTagKey.primaryPatchGroupKey}}'
          Values:
            - '{{returnPrimaryTagValue.primaryPatchGroupValue}}'
      MaxConcurrency: 10%
      MaxErrors: 10%
    nextStep: returnPrimaryToOriginalState
```

JSON

```
{
```

```
            "name":"returnPrimaryTagKey",
            "action":"aws:executeScript",
            "timeoutSeconds":120,
            "onFailure":"Abort",
            "inputs":{
               "Runtime":"python3.7",
               "Handler":"returnTagValues",
               "InputPayload":{
                  "primaryTag":"{{PrimaryPatchGroupTag}}"
               },
               "Script":"..."
            },
            "outputs":[
               {
                  "Name":"Payload",
                  "Selector":"$.Payload",
                  "Type":"StringMap"
               },
               {
                  "Name":"primaryPatchGroupKey",
                  "Selector":"$.Payload.tagKey",
                  "Type":"String"
               }
            ],
            "nextStep":"returnPrimaryTagValue"
         },
         {
            "name":"returnPrimaryTagValue",
            "action":"aws:executeScript",
            "timeoutSeconds":120,
            "onFailure":"Abort",
            "inputs":{
               "Runtime":"python3.7",
               "Handler":"returnTagValues",
               "InputPayload":{
                  "primaryTag":"{{PrimaryPatchGroupTag}}"
               },
               "Script":"..."
            },
            "outputs":[
               {
                  "Name":"Payload",
                  "Selector":"$.Payload",
                  "Type":"StringMap"
```

```
            },
            {
               "Name":"primaryPatchGroupValue",
               "Selector":"$.Payload.tagValue",
               "Type":"String"
            }
         ],
         "nextStep":"patchPrimaryInstances"
      },
      {
         "name":"patchPrimaryInstances",
         "action":"aws:runCommand",
         "onFailure":"Abort",
         "timeoutSeconds":7200,
         "inputs":{
            "DocumentName":"AWS-RunPatchBaseline",
            "Parameters":{
               "SnapshotId":"{{SnapshotId}}",
               "RebootOption":"{{RebootOption}}",
               "Operation":"{{Operation}}"
            },
            "Targets":[
               {
                  "Key":"{{returnPrimaryTagKey.primaryPatchGroupKey}}",
                  "Values":[
                     "{{returnPrimaryTagValue.primaryPatchGroupValue}}"
                  ]
               }
            ],
            "MaxConcurrency":"10%",
            "MaxErrors":"10%"
         },
         "nextStep":"returnPrimaryToOriginalState"
      },
```

6. パッチ適用操作が完了した後、Emily はオートメーションが、PrimaryPatchGroupTag パラメータで指定したタグに関連付けられたターゲットインスタンスを、オートメーション開始前と同じ状態に戻すようにしたいと考えています。これは、スクリプトの最初のアクションでの出力を再び使用して行います。ターゲットインスタンスの元の状態に基づいて、インスタンスが以前 running 以外の状態にあった場合、インスタンスは停止します。インスタンスの状態が running であれば、スクリプトは残りのインスタンスをループし続けます。

YAML

```
- name: returnPrimaryToOriginalState
    action: 'aws:executeScript'
    timeoutSeconds: 600
    onFailure: Abort
    inputs:
      Runtime: python3.7
      Handler: returnToOriginalState
      InputPayload:
        targetInstances: '{{getPrimaryInstanceState.originalInstanceStates}}'
      Script: |-
        def returnToOriginalState(events,context):
          import boto3

          #Initialize client
          ec2 = boto3.client('ec2')
          instanceDict = events['targetInstances']
          for instance in instanceDict:
            if instanceDict[instance] == 'stopped' or instanceDict[instance] ==
 'stopping':
                ec2.stop_instances(
                    InstanceIds=[instance]
                    )
            else:
              pass
    nextStep: getSecondaryInstanceState
```

JSON

```
{
         "name":"returnPrimaryToOriginalState",
         "action":"aws:executeScript",
         "timeoutSeconds":600,
         "onFailure":"Abort",
         "inputs":{
            "Runtime":"python3.7",
            "Handler":"returnToOriginalState",
            "InputPayload":{

 "targetInstances":"{{getPrimaryInstanceState.originalInstanceStates}}"
            },
            "Script":"..."
```

```
        },
        "nextStep":"getSecondaryInstanceState"
    },
```

7. PrimaryPatchGroupTag パラメータで指定したタグに関連付けられたインスタンスのパッチ適用操作は完了しました。これで、Emily はランブックコンテンツ内の以前のアクションをすべて複製し、SecondaryPatchGroupTag パラメータで指定したタグに関連付けられたインスタンスをターゲットにできるようになりました。

   YAML

```
- name: getSecondaryInstanceState
    action: 'aws:executeScript'
    timeoutSeconds: 120
    onFailure: Abort
    inputs:
      Runtime: python3.7
      Handler: getInstanceStates
      InputPayload:
        secondaryTag: '{{SecondaryPatchGroupTag}}'
      Script: |-
        def getInstanceStates(events,context):
          import boto3

          #Initialize client
          ec2 = boto3.client('ec2')
          tag = events['secondaryTag']
          tagKey, tagValue = list(tag.items())[0]
          instanceQuery = ec2.describe_instances(
          Filters=[
              {
                  "Name": "tag:" + tagKey,
                  "Values": [tagValue]
              }]
          )
          if not instanceQuery['Reservations']:
              noInstancesForTagString = "No instances found for specified tag."
              return({ 'noInstancesFound' : noInstancesForTagString })
          else:
              queryResponse = instanceQuery['Reservations']
              originalInstanceStates = {}
              for results in queryResponse:
                  instanceSet = results['Instances']
                  for instance in instanceSet:
```

```
                    instanceId = instance['InstanceId']
                    originalInstanceStates[instanceId] = instance['State']
['Name']
            return originalInstanceStates
    outputs:
      - Name: originalInstanceStates
        Selector: $.Payload
        Type: StringMap
    nextStep: verifySecondaryInstancesRunning
  - name: verifySecondaryInstancesRunning
    action: 'aws:executeScript'
    timeoutSeconds: 600
    onFailure: Abort
    inputs:
      Runtime: python3.7
      Handler: verifyInstancesRunning
      InputPayload:
        targetInstances: '{{getSecondaryInstanceState.originalInstanceStates}}'
      Script: |-
        def verifyInstancesRunning(events,context):
          import boto3

          #Initialize client
          ec2 = boto3.client('ec2')
          instanceDict = events['targetInstances']
          for instance in instanceDict:
            if instanceDict[instance] == 'stopped':
                print("The target instance " + instance + " is stopped. The
 instance will now be started.")
                ec2.start_instances(
                    InstanceIds=[instance]
                    )
            elif instanceDict[instance] == 'stopping':
                print("The target instance " + instance + " is stopping. Polling
 for instance to reach stopped state.")
                while instanceDict[instance] != 'stopped':
                    poll = ec2.get_waiter('instance_stopped')
                    poll.wait(
                        InstanceIds=[instance]
                    )
                ec2.start_instances(
                    InstanceIds=[instance]
                )
            else:
```

```
            pass
    nextStep: waitForSecondaryRunningInstances
  - name: waitForSecondaryRunningInstances
    action: 'aws:executeScript'
    timeoutSeconds: 300
    onFailure: Abort
    inputs:
      Runtime: python3.7
      Handler: waitForRunningInstances
      InputPayload:
        targetInstances: '{{getSecondaryInstanceState.originalInstanceStates}}'
      Script: |-
        def waitForRunningInstances(events,context):
          import boto3

          #Initialize client
          ec2 = boto3.client('ec2')
          instanceDict = events['targetInstances']
          for instance in instanceDict:
              poll = ec2.get_waiter('instance_running')
              poll.wait(
                  InstanceIds=[instance]
              )
    nextStep: returnSecondaryTagKey
  - name: returnSecondaryTagKey
    action: 'aws:executeScript'
    timeoutSeconds: 120
    onFailure: Abort
    inputs:
      Runtime: python3.7
      Handler: returnTagValues
      InputPayload:
        secondaryTag: '{{SecondaryPatchGroupTag}}'
      Script: |-
        def returnTagValues(events,context):
          tag = events['secondaryTag']
          tagKey = list(tag)[0]
          stringKey = "tag:" + tagKey
          return {'tagKey' : stringKey}
    outputs:
      - Name: Payload
        Selector: $.Payload
        Type: StringMap
      - Name: secondaryPatchGroupKey
```

```
        Selector: $.Payload.tagKey
        Type: String
    nextStep: returnSecondaryTagValue
  - name: returnSecondaryTagValue
    action: 'aws:executeScript'
    timeoutSeconds: 120
    onFailure: Abort
    inputs:
      Runtime: python3.7
      Handler: returnTagValues
      InputPayload:
        secondaryTag: '{{SecondaryPatchGroupTag}}'
      Script: |-
        def returnTagValues(events,context):
          tag = events['secondaryTag']
          tagKey = list(tag)[0]
          tagValue = tag[tagKey]
          return {'tagValue' : tagValue}
    outputs:
      - Name: Payload
        Selector: $.Payload
        Type: StringMap
      - Name: secondaryPatchGroupValue
        Selector: $.Payload.tagValue
        Type: String
    nextStep: patchSecondaryInstances
  - name: patchSecondaryInstances
    action: 'aws:runCommand'
    onFailure: Abort
    timeoutSeconds: 7200
    inputs:
      DocumentName: AWS-RunPatchBaseline
      Parameters:
        SnapshotId: '{{SnapshotId}}'
        RebootOption: '{{RebootOption}}'
        Operation: '{{Operation}}'
      Targets:
        - Key: '{{returnSecondaryTagKey.secondaryPatchGroupKey}}'
          Values:
          - '{{returnSecondaryTagValue.secondaryPatchGroupValue}}'
      MaxConcurrency: 10%
      MaxErrors: 10%
    nextStep: returnSecondaryToOriginalState
  - name: returnSecondaryToOriginalState
```

```
    action: 'aws:executeScript'
    timeoutSeconds: 600
    onFailure: Abort
    inputs:
      Runtime: python3.7
      Handler: returnToOriginalState
      InputPayload:
        targetInstances: '{{getSecondaryInstanceState.originalInstanceStates}}'
      Script: |-
        def returnToOriginalState(events,context):
          import boto3

          #Initialize client
          ec2 = boto3.client('ec2')
          instanceDict = events['targetInstances']
          for instance in instanceDict:
            if instanceDict[instance] == 'stopped' or instanceDict[instance] ==
 'stopping':
                ec2.stop_instances(
                    InstanceIds=[instance]
                    )
            else:
              pass
```

JSON

```
{
         "name":"getSecondaryInstanceState",
         "action":"aws:executeScript",
         "timeoutSeconds":120,
         "onFailure":"Abort",
         "inputs":{
            "Runtime":"python3.7",
            "Handler":"getInstanceStates",
            "InputPayload":{
               "secondaryTag":"{{SecondaryPatchGroupTag}}"
            },
            "Script":"..."
         },
         "outputs":[
            {
               "Name":"originalInstanceStates",
               "Selector":"$.Payload",
```

```
                "Type":"StringMap"
            }
        ],
        "nextStep":"verifySecondaryInstancesRunning"
    },
    {
        "name":"verifySecondaryInstancesRunning",
        "action":"aws:executeScript",
        "timeoutSeconds":600,
        "onFailure":"Abort",
        "inputs":{
            "Runtime":"python3.7",
            "Handler":"verifyInstancesRunning",
            "InputPayload":{

"targetInstances":"{{getSecondaryInstanceState.originalInstanceStates}}"
            },
            "Script":"..."
        },
        "nextStep":"waitForSecondaryRunningInstances"
    },
    {
        "name":"waitForSecondaryRunningInstances",
        "action":"aws:executeScript",
        "timeoutSeconds":300,
        "onFailure":"Abort",
        "inputs":{
            "Runtime":"python3.7",
            "Handler":"waitForRunningInstances",
            "InputPayload":{

"targetInstances":"{{getSecondaryInstanceState.originalInstanceStates}}"
            },
            "Script":"..."
        },
        "nextStep":"returnSecondaryTagKey"
    },
    {
        "name":"returnSecondaryTagKey",
        "action":"aws:executeScript",
        "timeoutSeconds":120,
        "onFailure":"Abort",
        "inputs":{
            "Runtime":"python3.7",
```

```
            "Handler":"returnTagValues",
            "InputPayload":{
               "secondaryTag":"{{SecondaryPatchGroupTag}}"
            },
            "Script":"..."
         },
         "outputs":[
            {
               "Name":"Payload",
               "Selector":"$.Payload",
               "Type":"StringMap"
            },
            {
               "Name":"secondaryPatchGroupKey",
               "Selector":"$.Payload.tagKey",
               "Type":"String"
            }
         ],
         "nextStep":"returnSecondaryTagValue"
      },
      {
         "name":"returnSecondaryTagValue",
         "action":"aws:executeScript",
         "timeoutSeconds":120,
         "onFailure":"Abort",
         "inputs":{
            "Runtime":"python3.7",
            "Handler":"returnTagValues",
            "InputPayload":{
               "secondaryTag":"{{SecondaryPatchGroupTag}}"
            },
            "Script":"..."
         },
         "outputs":[
            {
               "Name":"Payload",
               "Selector":"$.Payload",
               "Type":"StringMap"
            },
            {
               "Name":"secondaryPatchGroupValue",
               "Selector":"$.Payload.tagValue",
               "Type":"String"
            }
```

```
        ],
        "nextStep":"patchSecondaryInstances"
     },
     {
        "name":"patchSecondaryInstances",
        "action":"aws:runCommand",
        "onFailure":"Abort",
        "timeoutSeconds":7200,
        "inputs":{
           "DocumentName":"AWS-RunPatchBaseline",
           "Parameters":{
              "SnapshotId":"{{SnapshotId}}",
              "RebootOption":"{{RebootOption}}",
              "Operation":"{{Operation}}"
           },
           "Targets":[
              {
                 "Key":"{{returnSecondaryTagKey.secondaryPatchGroupKey}}",
                 "Values":[
                    "{{returnSecondaryTagValue.secondaryPatchGroupValue}}"
                 ]
              }
           ],
           "MaxConcurrency":"10%",
           "MaxErrors":"10%"
        },
        "nextStep":"returnSecondaryToOriginalState"
     },
     {
        "name":"returnSecondaryToOriginalState",
        "action":"aws:executeScript",
        "timeoutSeconds":600,
        "onFailure":"Abort",
        "inputs":{
           "Runtime":"python3.7",
           "Handler":"returnToOriginalState",
           "InputPayload":{

"targetInstances":"{{getSecondaryInstanceState.originalInstanceStates}}"
           },
           "Script":"..."
        }
     }
  ]
```

```
}
```

8. Emily は完成したスクリプトのランブックコンテンツをレビューし、ターゲットインスタンスと同じ AWS アカウント と AWS リージョン でランブックを作成します。これで、ランブックをテストして、オートメーションが希望どおりに動作していることを確認してから、本番環境に実装する準備が整いました。以下は、完成したスクリプト化されたランブックコンテンツです。

   YAML

```
description: An example of an Automation runbook that patches groups of Amazon EC2
 instances in stages.
schemaVersion: '0.3'
assumeRole: '{{AutomationAssumeRole}}'
parameters:
  AutomationAssumeRole:
    type: String
    description: '(Required) The Amazon Resource Name (ARN) of the IAM role that
 allows Automation to perform the actions on your behalf. If no role is specified,
 Systems Manager Automation uses your IAM permissions to operate this runbook.'
  PrimaryPatchGroupTag:
    type: StringMap
    description: '(Required) The tag for the primary group of instances you want
 to patch. Specify a key-value pair. Example: {"key" : "value"}'
  SecondaryPatchGroupTag:
    type: StringMap
    description: '(Required) The tag for the secondary group of instances you want
 to patch. Specify a key-value pair. Example: {"key" : "value"}'
  SnapshotId:
    type: String
    description: '(Optional) The snapshot ID to use to retrieve a patch baseline
 snapshot.'
    default: ''
  RebootOption:
    type: String
    description: '(Optional) Reboot behavior after a patch Install operation. If
 you choose NoReboot and patches are installed, the instance is marked as non-
compliant until a subsequent reboot and scan.'
    allowedValues:
      - NoReboot
      - RebootIfNeeded
    default: RebootIfNeeded
  Operation:
    type: String
```

```
    description: '(Optional) The update or configuration to perform on the
 instance. The system checks if patches specified in the patch baseline are
 installed on the instance. The install operation installs patches missing from
 the baseline.'
    allowedValues:
      - Install
      - Scan
    default: Install
mainSteps:
  - name: getPrimaryInstanceState
    action: 'aws:executeScript'
    timeoutSeconds: 120
    onFailure: Abort
    inputs:
      Runtime: python3.7
      Handler: getInstanceStates
      InputPayload:
        primaryTag: '{{PrimaryPatchGroupTag}}'
      Script: |-
        def getInstanceStates(events,context):
          import boto3

          #Initialize client
          ec2 = boto3.client('ec2')
          tag = events['primaryTag']
          tagKey, tagValue = list(tag.items())[0]
          instanceQuery = ec2.describe_instances(
          Filters=[
              {
                  "Name": "tag:" + tagKey,
                  "Values": [tagValue]
              }]
          )
          if not instanceQuery['Reservations']:
              noInstancesForTagString = "No instances found for specified tag."
              return({ 'noInstancesFound' : noInstancesForTagString })
          else:
              queryResponse = instanceQuery['Reservations']
              originalInstanceStates = {}
              for results in queryResponse:
                  instanceSet = results['Instances']
                  for instance in instanceSet:
                      instanceId = instance['InstanceId']
```

```
                    originalInstanceStates[instanceId] = instance['State']
['Name']
            return originalInstanceStates
    outputs:
      - Name: originalInstanceStates
        Selector: $.Payload
        Type: StringMap
    nextStep: verifyPrimaryInstancesRunning
  - name: verifyPrimaryInstancesRunning
    action: 'aws:executeScript'
    timeoutSeconds: 600
    onFailure: Abort
    inputs:
      Runtime: python3.7
      Handler: verifyInstancesRunning
      InputPayload:
        targetInstances: '{{getPrimaryInstanceState.originalInstanceStates}}'
      Script: |-
        def verifyInstancesRunning(events,context):
          import boto3

          #Initialize client
          ec2 = boto3.client('ec2')
          instanceDict = events['targetInstances']
          for instance in instanceDict:
            if instanceDict[instance] == 'stopped':
                print("The target instance " + instance + " is stopped. The
 instance will now be started.")
                ec2.start_instances(
                    InstanceIds=[instance]
                    )
            elif instanceDict[instance] == 'stopping':
                print("The target instance " + instance + " is stopping. Polling
 for instance to reach stopped state.")
                while instanceDict[instance] != 'stopped':
                    poll = ec2.get_waiter('instance_stopped')
                    poll.wait(
                        InstanceIds=[instance]
                    )
                ec2.start_instances(
                    InstanceIds=[instance]
                )
            else:
              pass
```

```
    nextStep: waitForPrimaryRunningInstances
  - name: waitForPrimaryRunningInstances
    action: 'aws:executeScript'
    timeoutSeconds: 300
    onFailure: Abort
    inputs:
      Runtime: python3.7
      Handler: waitForRunningInstances
      InputPayload:
        targetInstances: '{{getPrimaryInstanceState.originalInstanceStates}}'
      Script: |-
        def waitForRunningInstances(events,context):
          import boto3

          #Initialize client
          ec2 = boto3.client('ec2')
          instanceDict = events['targetInstances']
          for instance in instanceDict:
              poll = ec2.get_waiter('instance_running')
              poll.wait(
                  InstanceIds=[instance]
              )
    nextStep: returnPrimaryTagKey
  - name: returnPrimaryTagKey
    action: 'aws:executeScript'
    timeoutSeconds: 120
    onFailure: Abort
    inputs:
      Runtime: python3.7
      Handler: returnTagValues
      InputPayload:
        primaryTag: '{{PrimaryPatchGroupTag}}'
      Script: |-
        def returnTagValues(events,context):
          tag = events['primaryTag']
          tagKey = list(tag)[0]
          stringKey = "tag:" + tagKey
          return {'tagKey' : stringKey}
    outputs:
      - Name: Payload
        Selector: $.Payload
        Type: StringMap
      - Name: primaryPatchGroupKey
        Selector: $.Payload.tagKey
```

```
      Type: String
  nextStep: returnPrimaryTagValue
- name: returnPrimaryTagValue
  action: 'aws:executeScript'
  timeoutSeconds: 120
  onFailure: Abort
  inputs:
    Runtime: python3.7
    Handler: returnTagValues
    InputPayload:
      primaryTag: '{{PrimaryPatchGroupTag}}'
    Script: |-
      def returnTagValues(events,context):
        tag = events['primaryTag']
        tagKey = list(tag)[0]
        tagValue = tag[tagKey]
        return {'tagValue' : tagValue}
  outputs:
    - Name: Payload
      Selector: $.Payload
      Type: StringMap
    - Name: primaryPatchGroupValue
      Selector: $.Payload.tagValue
      Type: String
  nextStep: patchPrimaryInstances
- name: patchPrimaryInstances
  action: 'aws:runCommand'
  onFailure: Abort
  timeoutSeconds: 7200
  inputs:
    DocumentName: AWS-RunPatchBaseline
    Parameters:
      SnapshotId: '{{SnapshotId}}'
      RebootOption: '{{RebootOption}}'
      Operation: '{{Operation}}'
    Targets:
      - Key: '{{returnPrimaryTagKey.primaryPatchGroupKey}}'
        Values:
          - '{{returnPrimaryTagValue.primaryPatchGroupValue}}'
    MaxConcurrency: 10%
    MaxErrors: 10%
  nextStep: returnPrimaryToOriginalState
- name: returnPrimaryToOriginalState
  action: 'aws:executeScript'
```

```
    timeoutSeconds: 600
    onFailure: Abort
    inputs:
      Runtime: python3.7
      Handler: returnToOriginalState
      InputPayload:
        targetInstances: '{{getPrimaryInstanceState.originalInstanceStates}}'
      Script: |-
        def returnToOriginalState(events,context):
          import boto3

          #Initialize client
          ec2 = boto3.client('ec2')
          instanceDict = events['targetInstances']
          for instance in instanceDict:
            if instanceDict[instance] == 'stopped' or instanceDict[instance] ==
'stopping':
                ec2.stop_instances(
                    InstanceIds=[instance]
                    )
            else:
              pass
    nextStep: getSecondaryInstanceState
  - name: getSecondaryInstanceState
    action: 'aws:executeScript'
    timeoutSeconds: 120
    onFailure: Abort
    inputs:
      Runtime: python3.7
      Handler: getInstanceStates
      InputPayload:
        secondaryTag: '{{SecondaryPatchGroupTag}}'
      Script: |-
        def getInstanceStates(events,context):
          import boto3

          #Initialize client
          ec2 = boto3.client('ec2')
          tag = events['secondaryTag']
          tagKey, tagValue = list(tag.items())[0]
          instanceQuery = ec2.describe_instances(
          Filters=[
              {
                  "Name": "tag:" + tagKey,
```

```
                "Values": [tagValue]
            }]
        )
        if not instanceQuery['Reservations']:
            noInstancesForTagString = "No instances found for specified tag."
            return({ 'noInstancesFound' : noInstancesForTagString })
        else:
            queryResponse = instanceQuery['Reservations']
            originalInstanceStates = {}
            for results in queryResponse:
                instanceSet = results['Instances']
                for instance in instanceSet:
                    instanceId = instance['InstanceId']
                    originalInstanceStates[instanceId] = instance['State']
['Name']
            return originalInstanceStates
    outputs:
      - Name: originalInstanceStates
        Selector: $.Payload
        Type: StringMap
    nextStep: verifySecondaryInstancesRunning
  - name: verifySecondaryInstancesRunning
    action: 'aws:executeScript'
    timeoutSeconds: 600
    onFailure: Abort
    inputs:
      Runtime: python3.7
      Handler: verifyInstancesRunning
      InputPayload:
        targetInstances: '{{getSecondaryInstanceState.originalInstanceStates}}'
      Script: |-
        def verifyInstancesRunning(events,context):
          import boto3

          #Initialize client
          ec2 = boto3.client('ec2')
          instanceDict = events['targetInstances']
          for instance in instanceDict:
            if instanceDict[instance] == 'stopped':
                print("The target instance " + instance + " is stopped. The
 instance will now be started.")
                ec2.start_instances(
                    InstanceIds=[instance]
                    )
```

```
            elif instanceDict[instance] == 'stopping':
                print("The target instance " + instance + " is stopping. Polling
for instance to reach stopped state.")
                while instanceDict[instance] != 'stopped':
                    poll = ec2.get_waiter('instance_stopped')
                    poll.wait(
                        InstanceIds=[instance]
                    )
                ec2.start_instances(
                    InstanceIds=[instance]
                )
            else:
              pass
    nextStep: waitForSecondaryRunningInstances
  - name: waitForSecondaryRunningInstances
    action: 'aws:executeScript'
    timeoutSeconds: 300
    onFailure: Abort
    inputs:
      Runtime: python3.7
      Handler: waitForRunningInstances
      InputPayload:
        targetInstances: '{{getSecondaryInstanceState.originalInstanceStates}}'
      Script: |-
        def waitForRunningInstances(events,context):
          import boto3

          #Initialize client
          ec2 = boto3.client('ec2')
          instanceDict = events['targetInstances']
          for instance in instanceDict:
              poll = ec2.get_waiter('instance_running')
              poll.wait(
                  InstanceIds=[instance]
              )
    nextStep: returnSecondaryTagKey
  - name: returnSecondaryTagKey
    action: 'aws:executeScript'
    timeoutSeconds: 120
    onFailure: Abort
    inputs:
      Runtime: python3.7
      Handler: returnTagValues
      InputPayload:
```

```
        secondaryTag: '{{SecondaryPatchGroupTag}}'
      Script: |-
        def returnTagValues(events,context):
          tag = events['secondaryTag']
          tagKey = list(tag)[0]
          stringKey = "tag:" + tagKey
          return {'tagKey' : stringKey}
    outputs:
      - Name: Payload
        Selector: $.Payload
        Type: StringMap
      - Name: secondaryPatchGroupKey
        Selector: $.Payload.tagKey
        Type: String
    nextStep: returnSecondaryTagValue
  - name: returnSecondaryTagValue
    action: 'aws:executeScript'
    timeoutSeconds: 120
    onFailure: Abort
    inputs:
      Runtime: python3.7
      Handler: returnTagValues
      InputPayload:
        secondaryTag: '{{SecondaryPatchGroupTag}}'
      Script: |-
        def returnTagValues(events,context):
          tag = events['secondaryTag']
          tagKey = list(tag)[0]
          tagValue = tag[tagKey]
          return {'tagValue' : tagValue}
    outputs:
      - Name: Payload
        Selector: $.Payload
        Type: StringMap
      - Name: secondaryPatchGroupValue
        Selector: $.Payload.tagValue
        Type: String
    nextStep: patchSecondaryInstances
  - name: patchSecondaryInstances
    action: 'aws:runCommand'
    onFailure: Abort
    timeoutSeconds: 7200
    inputs:
      DocumentName: AWS-RunPatchBaseline
```

```
      Parameters:
        SnapshotId: '{{SnapshotId}}'
        RebootOption: '{{RebootOption}}'
        Operation: '{{Operation}}'
      Targets:
        - Key: '{{returnSecondaryTagKey.secondaryPatchGroupKey}}'
          Values:
          - '{{returnSecondaryTagValue.secondaryPatchGroupValue}}'
      MaxConcurrency: 10%
      MaxErrors: 10%
    nextStep: returnSecondaryToOriginalState
  - name: returnSecondaryToOriginalState
    action: 'aws:executeScript'
    timeoutSeconds: 600
    onFailure: Abort
    inputs:
      Runtime: python3.7
      Handler: returnToOriginalState
      InputPayload:
        targetInstances: '{{getSecondaryInstanceState.originalInstanceStates}}'
      Script: |-
        def returnToOriginalState(events,context):
          import boto3

          #Initialize client
          ec2 = boto3.client('ec2')
          instanceDict = events['targetInstances']
          for instance in instanceDict:
            if instanceDict[instance] == 'stopped' or instanceDict[instance] ==
 'stopping':
                ec2.stop_instances(
                    InstanceIds=[instance]
                    )
            else:
              pass
```

JSON

```
{
   "description":"An example of an Automation runbook that patches groups of
 Amazon EC2 instances in stages.",
   "schemaVersion":"0.3",
   "assumeRole":"{{AutomationAssumeRole}}",
```

```
  "parameters":{
     "AutomationAssumeRole":{
        "type":"String",
        "description":"(Required) The Amazon Resource Name (ARN) of the IAM role
that allows Automation to perform the actions on your behalf. If no role is
specified, Systems Manager Automation uses your IAM permissions to operate this
runbook."
     },
     "PrimaryPatchGroupTag":{
        "type":"StringMap",
        "description":"(Required) The tag for the primary group of instances you
want to patch. Specify a key-value pair. Example: {\"key\" : \"value\"}"
     },
     "SecondaryPatchGroupTag":{
        "type":"StringMap",
        "description":"(Required) The tag for the secondary group of instances
you want to patch. Specify a key-value pair. Example: {\"key\" : \"value\"}"
     },
     "SnapshotId":{
        "type":"String",
        "description":"(Optional) The snapshot ID to use to retrieve a patch
baseline snapshot.",
        "default":""
     },
     "RebootOption":{
        "type":"String",
        "description":"(Optional) Reboot behavior after a patch Install
operation. If you choose NoReboot and patches are installed, the instance is
marked as non-compliant until a subsequent reboot and scan.",
        "allowedValues":[
           "NoReboot",
           "RebootIfNeeded"
        ],
        "default":"RebootIfNeeded"
     },
     "Operation":{
        "type":"String",
        "description":"(Optional) The update or configuration to perform on
the instance. The system checks if patches specified in the patch baseline are
installed on the instance. The install operation installs patches missing from
the baseline.",
        "allowedValues":[
           "Install",
           "Scan"
```

```
        ],
        "default":"Install"
     }
  },
  "mainSteps":[
     {
        "name":"getPrimaryInstanceState",
        "action":"aws:executeScript",
        "timeoutSeconds":120,
        "onFailure":"Abort",
        "inputs":{
           "Runtime":"python3.7",
           "Handler":"getInstanceStates",
           "InputPayload":{
              "primaryTag":"{{PrimaryPatchGroupTag}}"
           },
           "Script":"..."
        },
        "outputs":[
           {
              "Name":"originalInstanceStates",
              "Selector":"$.Payload",
              "Type":"StringMap"
           }
        ],
        "nextStep":"verifyPrimaryInstancesRunning"
     },
     {
        "name":"verifyPrimaryInstancesRunning",
        "action":"aws:executeScript",
        "timeoutSeconds":600,
        "onFailure":"Abort",
        "inputs":{
           "Runtime":"python3.7",
           "Handler":"verifyInstancesRunning",
           "InputPayload":{

"targetInstances":"{{getPrimaryInstanceState.originalInstanceStates}}"
           },
           "Script":"..."
        },
        "nextStep":"waitForPrimaryRunningInstances"
     },
     {
```

```
        "name":"waitForPrimaryRunningInstances",
        "action":"aws:executeScript",
        "timeoutSeconds":300,
        "onFailure":"Abort",
        "inputs":{
           "Runtime":"python3.7",
           "Handler":"waitForRunningInstances",
           "InputPayload":{

"targetInstances":"{{getPrimaryInstanceState.originalInstanceStates}}"
           },
           "Script":"..."
        },
        "nextStep":"returnPrimaryTagKey"
     },
     {
        "name":"returnPrimaryTagKey",
        "action":"aws:executeScript",
        "timeoutSeconds":120,
        "onFailure":"Abort",
        "inputs":{
           "Runtime":"python3.7",
           "Handler":"returnTagValues",
           "InputPayload":{
              "primaryTag":"{{PrimaryPatchGroupTag}}"
           },
           "Script":"..."
        },
        "outputs":[
           {
              "Name":"Payload",
              "Selector":"$.Payload",
              "Type":"StringMap"
           },
           {
              "Name":"primaryPatchGroupKey",
              "Selector":"$.Payload.tagKey",
              "Type":"String"
           }
        ],
        "nextStep":"returnPrimaryTagValue"
     },
     {
        "name":"returnPrimaryTagValue",
```

```
         "action":"aws:executeScript",
         "timeoutSeconds":120,
         "onFailure":"Abort",
         "inputs":{
            "Runtime":"python3.7",
            "Handler":"returnTagValues",
            "InputPayload":{
               "primaryTag":"{{PrimaryPatchGroupTag}}"
            },
            "Script":"..."
         },
         "outputs":[
            {
               "Name":"Payload",
               "Selector":"$.Payload",
               "Type":"StringMap"
            },
            {
               "Name":"primaryPatchGroupValue",
               "Selector":"$.Payload.tagValue",
               "Type":"String"
            }
         ],
         "nextStep":"patchPrimaryInstances"
      },
      {
         "name":"patchPrimaryInstances",
         "action":"aws:runCommand",
         "onFailure":"Abort",
         "timeoutSeconds":7200,
         "inputs":{
            "DocumentName":"AWS-RunPatchBaseline",
            "Parameters":{
               "SnapshotId":"{{SnapshotId}}",
               "RebootOption":"{{RebootOption}}",
               "Operation":"{{Operation}}"
            },
            "Targets":[
               {
                  "Key":"{{returnPrimaryTagKey.primaryPatchGroupKey}}",
                  "Values":[
                     "{{returnPrimaryTagValue.primaryPatchGroupValue}}"
                  ]
               }
```

```
            ],
            "MaxConcurrency":"10%",
            "MaxErrors":"10%"
         },
         "nextStep":"returnPrimaryToOriginalState"
      },
      {
         "name":"returnPrimaryToOriginalState",
         "action":"aws:executeScript",
         "timeoutSeconds":600,
         "onFailure":"Abort",
         "inputs":{
            "Runtime":"python3.7",
            "Handler":"returnToOriginalState",
            "InputPayload":{

"targetInstances":"{{getPrimaryInstanceState.originalInstanceStates}}"
            },
            "Script":"..."
         },
         "nextStep":"getSecondaryInstanceState"
      },
      {
         "name":"getSecondaryInstanceState",
         "action":"aws:executeScript",
         "timeoutSeconds":120,
         "onFailure":"Abort",
         "inputs":{
            "Runtime":"python3.7",
            "Handler":"getInstanceStates",
            "InputPayload":{
               "secondaryTag":"{{SecondaryPatchGroupTag}}"
            },
            "Script":"..."
         },
         "outputs":[
            {
               "Name":"originalInstanceStates",
               "Selector":"$.Payload",
               "Type":"StringMap"
            }
         ],
         "nextStep":"verifySecondaryInstancesRunning"
      },
```

```
    {
       "name":"verifySecondaryInstancesRunning",
       "action":"aws:executeScript",
       "timeoutSeconds":600,
       "onFailure":"Abort",
       "inputs":{
          "Runtime":"python3.7",
          "Handler":"verifyInstancesRunning",
          "InputPayload":{

"targetInstances":"{{getSecondaryInstanceState.originalInstanceStates}}"
          },
          "Script":"..."
       },
       "nextStep":"waitForSecondaryRunningInstances"
    },
    {
       "name":"waitForSecondaryRunningInstances",
       "action":"aws:executeScript",
       "timeoutSeconds":300,
       "onFailure":"Abort",
       "inputs":{
          "Runtime":"python3.7",
          "Handler":"waitForRunningInstances",
          "InputPayload":{

"targetInstances":"{{getSecondaryInstanceState.originalInstanceStates}}"
          },
          "Script":"..."
       },
       "nextStep":"returnSecondaryTagKey"
    },
    {
       "name":"returnSecondaryTagKey",
       "action":"aws:executeScript",
       "timeoutSeconds":120,
       "onFailure":"Abort",
       "inputs":{
          "Runtime":"python3.7",
          "Handler":"returnTagValues",
          "InputPayload":{
             "secondaryTag":"{{SecondaryPatchGroupTag}}"
          },
          "Script":"..."
```

```
         },
         "outputs":[
            {
               "Name":"Payload",
               "Selector":"$.Payload",
               "Type":"StringMap"
            },
            {
               "Name":"secondaryPatchGroupKey",
               "Selector":"$.Payload.tagKey",
               "Type":"String"
            }
         ],
         "nextStep":"returnSecondaryTagValue"
      },
      {
         "name":"returnSecondaryTagValue",
         "action":"aws:executeScript",
         "timeoutSeconds":120,
         "onFailure":"Abort",
         "inputs":{
            "Runtime":"python3.7",
            "Handler":"returnTagValues",
            "InputPayload":{
               "secondaryTag":"{{SecondaryPatchGroupTag}}"
            },
            "Script":"..."
         },
         "outputs":[
            {
               "Name":"Payload",
               "Selector":"$.Payload",
               "Type":"StringMap"
            },
            {
               "Name":"secondaryPatchGroupValue",
               "Selector":"$.Payload.tagValue",
               "Type":"String"
            }
         ],
         "nextStep":"patchSecondaryInstances"
      },
      {
         "name":"patchSecondaryInstances",
```

```
         "action":"aws:runCommand",
         "onFailure":"Abort",
         "timeoutSeconds":7200,
         "inputs":{
            "DocumentName":"AWS-RunPatchBaseline",
            "Parameters":{
               "SnapshotId":"{{SnapshotId}}",
               "RebootOption":"{{RebootOption}}",
               "Operation":"{{Operation}}"
            },
            "Targets":[
               {
                  "Key":"{{returnSecondaryTagKey.secondaryPatchGroupKey}}",
                  "Values":[
                     "{{returnSecondaryTagValue.secondaryPatchGroupValue}}"
                  ]
               }
            ],
            "MaxConcurrency":"10%",
            "MaxErrors":"10%"
         },
         "nextStep":"returnSecondaryToOriginalState"
      },
      {
         "name":"returnSecondaryToOriginalState",
         "action":"aws:executeScript",
         "timeoutSeconds":600,
         "onFailure":"Abort",
         "inputs":{
            "Runtime":"python3.7",
            "Handler":"returnToOriginalState",
            "InputPayload":{

 "targetInstances":"{{getSecondaryInstanceState.originalInstanceStates}}"
            },
            "Script":"..."
         }
      }
   ]
}
```

この例で使用されているオートメーションアクションの詳細については、「Systems Manager Automation アクションのリファレンス」を参照してください。

その他のランブックの例

次のランブック例により、AWS Systems Manager オートメーションアクションを使用して、一般的なデプロイ、トラブルシューティング、および保守タスクを自動化する方法が確認できます。

> **Note**
>
> このセクションでは、運用上の特定のニーズをサポートするカスタムランブックを作成する方法を示すために、ランブックの例を提供しています。これらのランブックは、本番環境での使用を目的としていません。ただし、ユーザー自身で使用するためにカスタマイズすることはできます。

例

- VPC アーキテクチャと Microsoft Active Directory ドメインコントローラーのデプロイ
- 最新のスナップショットからルートボリュームを復元する
- AMI とクロスリージョンコピーの作成

VPC アーキテクチャと Microsoft Active Directory ドメインコントローラーのデプロイ

効率を高め、一般的なタスクを標準化するために、デプロイを自動化することができます。これは、定期的に複数のアカウントと に同じアーキテクチャをデプロイする場合に便利ですAWS リージョンまた、アーキテクチャのデプロイを自動化することで、アーキテクチャを手動でデプロイするときに発生する人為的エラーの発生率を減らすことができます。AWS Systems Managerオートメーションアクションが、これを実現するのに役立ちます。Automation は AWS Systems Manager のツールです。

次の AWS Systems Manager ランブックの例では、これらのアクションを実行します。

- ドメインコントローラーとして設定して EC2 インスタンスを起動する際に、Systems Manager Parameter Store を使用して、最新の Windows Server 2016 Amazon Machine Image (AMI) を取得します。Parameter Store は AWS Systems Manager のツールです。
- `aws:executeAwsApi` オートメーションアクションを使用して、複数の AWS API オペレーションを呼び出して VPC アーキテクチャを作成します。ドメインコントローラーインスタンスはプライベートサブネットで起動され、NAT ゲートウェイを使用してインターネットに接続されます。

これにより、インスタンスの SSM Agent は、必要な Systems Manager エンドポイントにアクセスできるようになります。

- aws:waitForAwsResourceProperty オートメーションアクションを使用して、前のアクションによって起動されたインスタンスが Online に対してAWS Systems Manager であることを確認します。
- aws:runCommand オートメーションアクションを使用して、Microsoft Active Directory ドメインコントローラーとして起動されるインスタンスを設定します。

YAML

```
---
description: Custom Automation Deployment Example
schemaVersion: '0.3'
parameters:
  AutomationAssumeRole:
    type: String
    default: ''
    description: >-
      (Optional) The ARN of the role that allows Automation to perform the
      actions on your behalf. If no role is specified, Systems Manager
      Automation uses your IAM permissions to run this runbook.
mainSteps:
  - name: getLatestWindowsAmi
    action: aws:executeAwsApi
    onFailure: Abort
    inputs:
      Service: ssm
      Api: GetParameter
      Name: >-
        /aws/service/ami-windows-latest/Windows_Server-2016-English-Full-Base
    outputs:
      - Name: amiId
        Selector: $.Parameter.Value
        Type: String
    nextStep: createSSMInstanceRole
  - name: createSSMInstanceRole
    action: aws:executeAwsApi
    onFailure: Abort
    inputs:
      Service: iam
```

```
          Api: CreateRole
          AssumeRolePolicyDocument: >-
            {"Version":"2012-10-17","Statement":[{"Effect":"Allow","Principal":
{"Service":["ec2.amazonaws.com"]},"Action":["sts:AssumeRole"]}]}
          RoleName: sampleSSMInstanceRole
        nextStep: attachManagedSSMPolicy
      - name: attachManagedSSMPolicy
        action: aws:executeAwsApi
        onFailure: Abort
        inputs:
          Service: iam
          Api: AttachRolePolicy
          PolicyArn: 'arn:aws:iam::aws:policy/service-role/
AmazonSSMManagedInstanceCore'
          RoleName: sampleSSMInstanceRole
        nextStep: createSSMInstanceProfile
      - name: createSSMInstanceProfile
        action: aws:executeAwsApi
        onFailure: Abort
        inputs:
          Service: iam
          Api: CreateInstanceProfile
          InstanceProfileName: sampleSSMInstanceRole
        outputs:
          - Name: instanceProfileArn
            Selector: $.InstanceProfile.Arn
            Type: String
        nextStep: addSSMInstanceRoleToProfile
      - name: addSSMInstanceRoleToProfile
        action: aws:executeAwsApi
        onFailure: Abort
        inputs:
          Service: iam
          Api: AddRoleToInstanceProfile
          InstanceProfileName: sampleSSMInstanceRole
          RoleName: sampleSSMInstanceRole
        nextStep: createVpc
      - name: createVpc
        action: aws:executeAwsApi
        onFailure: Abort
        inputs:
          Service: ec2
          Api: CreateVpc
          CidrBlock: 10.0.100.0/22
```

```
        outputs:
          - Name: vpcId
            Selector: $.Vpc.VpcId
            Type: String
        nextStep: getMainRtb
      - name: getMainRtb
        action: aws:executeAwsApi
        onFailure: Abort
        inputs:
          Service: ec2
          Api: DescribeRouteTables
          Filters:
            - Name: vpc-id
              Values:
                - '{{ createVpc.vpcId }}'
        outputs:
          - Name: mainRtbId
            Selector: '$.RouteTables[0].RouteTableId'
            Type: String
        nextStep: verifyMainRtb
      - name: verifyMainRtb
        action: aws:assertAwsResourceProperty
        onFailure: Abort
        inputs:
          Service: ec2
          Api: DescribeRouteTables
          RouteTableIds:
            - '{{ getMainRtb.mainRtbId }}'
          PropertySelector: '$.RouteTables[0].Associations[0].Main'
          DesiredValues:
            - 'True'
        nextStep: createPubSubnet
      - name: createPubSubnet
        action: aws:executeAwsApi
        onFailure: Abort
        inputs:
          Service: ec2
          Api: CreateSubnet
          CidrBlock: 10.0.103.0/24
          AvailabilityZone: us-west-2c
          VpcId: '{{ createVpc.vpcId }}'
        outputs:
          - Name: pubSubnetId
            Selector: $.Subnet.SubnetId
```

```
        Type: String
    nextStep: createPubRtb
  - name: createPubRtb
    action: aws:executeAwsApi
    onFailure: Abort
    inputs:
      Service: ec2
      Api: CreateRouteTable
      VpcId: '{{ createVpc.vpcId }}'
    outputs:
      - Name: pubRtbId
        Selector: $.RouteTable.RouteTableId
        Type: String
    nextStep: createIgw
  - name: createIgw
    action: aws:executeAwsApi
    onFailure: Abort
    inputs:
      Service: ec2
      Api: CreateInternetGateway
    outputs:
      - Name: igwId
        Selector: $.InternetGateway.InternetGatewayId
        Type: String
    nextStep: attachIgw
  - name: attachIgw
    action: aws:executeAwsApi
    onFailure: Abort
    inputs:
      Service: ec2
      Api: AttachInternetGateway
      InternetGatewayId: '{{ createIgw.igwId }}'
      VpcId: '{{ createVpc.vpcId }}'
    nextStep: allocateEip
  - name: allocateEip
    action: aws:executeAwsApi
    onFailure: Abort
    inputs:
      Service: ec2
      Api: AllocateAddress
      Domain: vpc
    outputs:
      - Name: eipAllocationId
        Selector: $.AllocationId
```

```
            Type: String
        nextStep: createNatGw
      - name: createNatGw
        action: aws:executeAwsApi
        onFailure: Abort
        inputs:
          Service: ec2
          Api: CreateNatGateway
          AllocationId: '{{ allocateEip.eipAllocationId }}'
          SubnetId: '{{ createPubSubnet.pubSubnetId }}'
        outputs:
          - Name: natGwId
            Selector: $.NatGateway.NatGatewayId
            Type: String
        nextStep: verifyNatGwAvailable
      - name: verifyNatGwAvailable
        action: aws:waitForAwsResourceProperty
        timeoutSeconds: 150
        inputs:
          Service: ec2
          Api: DescribeNatGateways
          NatGatewayIds:
            - '{{ createNatGw.natGwId }}'
          PropertySelector: '$.NatGateways[0].State'
          DesiredValues:
            - available
        nextStep: createNatRoute
      - name: createNatRoute
        action: aws:executeAwsApi
        onFailure: Abort
        inputs:
          Service: ec2
          Api: CreateRoute
          DestinationCidrBlock: 0.0.0.0/0
          NatGatewayId: '{{ createNatGw.natGwId }}'
          RouteTableId: '{{ getMainRtb.mainRtbId }}'
        nextStep: createPubRoute
      - name: createPubRoute
        action: aws:executeAwsApi
        onFailure: Abort
        inputs:
          Service: ec2
          Api: CreateRoute
          DestinationCidrBlock: 0.0.0.0/0
```

```
        GatewayId: '{{ createIgw.igwId }}'
        RouteTableId: '{{ createPubRtb.pubRtbId }}'
      nextStep: setPubSubAssoc
    - name: setPubSubAssoc
      action: aws:executeAwsApi
      onFailure: Abort
      inputs:
        Service: ec2
        Api: AssociateRouteTable
        RouteTableId: '{{ createPubRtb.pubRtbId }}'
        SubnetId: '{{ createPubSubnet.pubSubnetId }}'
    - name: createDhcpOptions
      action: aws:executeAwsApi
      onFailure: Abort
      inputs:
        Service: ec2
        Api: CreateDhcpOptions
        DhcpConfigurations:
          - Key: domain-name-servers
            Values:
              - '10.0.100.50,10.0.101.50'
          - Key: domain-name
            Values:
              - sample.com
      outputs:
        - Name: dhcpOptionsId
          Selector: $.DhcpOptions.DhcpOptionsId
          Type: String
      nextStep: createDCSubnet1
    - name: createDCSubnet1
      action: aws:executeAwsApi
      onFailure: Abort
      inputs:
        Service: ec2
        Api: CreateSubnet
        CidrBlock: 10.0.100.0/24
        AvailabilityZone: us-west-2a
        VpcId: '{{ createVpc.vpcId }}'
      outputs:
        - Name: firstSubnetId
          Selector: $.Subnet.SubnetId
          Type: String
      nextStep: createDCSubnet2
    - name: createDCSubnet2
```

```
      action: aws:executeAwsApi
      onFailure: Abort
      inputs:
        Service: ec2
        Api: CreateSubnet
        CidrBlock: 10.0.101.0/24
        AvailabilityZone: us-west-2b
        VpcId: '{{ createVpc.vpcId }}'
      outputs:
        - Name: secondSubnetId
          Selector: $.Subnet.SubnetId
          Type: String
      nextStep: createDCSecGroup
    - name: createDCSecGroup
      action: aws:executeAwsApi
      onFailure: Abort
      inputs:
        Service: ec2
        Api: CreateSecurityGroup
        GroupName: SampleDCSecGroup
        Description: Security Group for Sample Domain Controllers
        VpcId: '{{ createVpc.vpcId }}'
      outputs:
        - Name: dcSecGroupId
          Selector: $.GroupId
          Type: String
      nextStep: authIngressDCTraffic
    - name: authIngressDCTraffic
      action: aws:executeAwsApi
      onFailure: Abort
      inputs:
        Service: ec2
        Api: AuthorizeSecurityGroupIngress
        GroupId: '{{ createDCSecGroup.dcSecGroupId }}'
        IpPermissions:
          - FromPort: -1
            IpProtocol: '-1'
            IpRanges:
              - CidrIp: 0.0.0.0/0
                Description: Allow all traffic between Domain Controllers
      nextStep: verifyInstanceProfile
    - name: verifyInstanceProfile
      action: aws:waitForAwsResourceProperty
      maxAttempts: 5
```

```
        onFailure: Abort
        inputs:
          Service: iam
          Api: ListInstanceProfilesForRole
          RoleName: sampleSSMInstanceRole
          PropertySelector: '$.InstanceProfiles[0].Arn'
          DesiredValues:
            - '{{ createSSMInstanceProfile.instanceProfileArn }}'
        nextStep: iamEventualConsistency
      - name: iamEventualConsistency
        action: aws:sleep
        inputs:
          Duration: PT2M
        nextStep: launchDC1
      - name: launchDC1
        action: aws:executeAwsApi
        onFailure: Abort
        inputs:
          Service: ec2
          Api: RunInstances
          BlockDeviceMappings:
            - DeviceName: /dev/sda1
              Ebs:
                DeleteOnTermination: true
                VolumeSize: 50
                VolumeType: gp2
            - DeviceName: xvdf
              Ebs:
                DeleteOnTermination: true
                VolumeSize: 100
                VolumeType: gp2
          IamInstanceProfile:
            Arn: '{{ createSSMInstanceProfile.instanceProfileArn }}'
          ImageId: '{{ getLatestWindowsAmi.amiId }}'
          InstanceType: t2.micro
          MaxCount: 1
          MinCount: 1
          PrivateIpAddress: 10.0.100.50
          SecurityGroupIds:
            - '{{ createDCSecGroup.dcSecGroupId }}'
          SubnetId: '{{ createDCSubnet1.firstSubnetId }}'
          TagSpecifications:
            - ResourceType: instance
              Tags:
```

```
            - Key: Name
              Value: SampleDC1
      outputs:
        - Name: pdcInstanceId
          Selector: '$.Instances[0].InstanceId'
          Type: String
      nextStep: launchDC2
    - name: launchDC2
      action: aws:executeAwsApi
      onFailure: Abort
      inputs:
        Service: ec2
        Api: RunInstances
        BlockDeviceMappings:
          - DeviceName: /dev/sda1
            Ebs:
              DeleteOnTermination: true
              VolumeSize: 50
              VolumeType: gp2
          - DeviceName: xvdf
            Ebs:
              DeleteOnTermination: true
              VolumeSize: 100
              VolumeType: gp2
        IamInstanceProfile:
          Arn: '{{ createSSMInstanceProfile.instanceProfileArn }}'
        ImageId: '{{ getLatestWindowsAmi.amiId }}'
        InstanceType: t2.micro
        MaxCount: 1
        MinCount: 1
        PrivateIpAddress: 10.0.101.50
        SecurityGroupIds:
          - '{{ createDCSecGroup.dcSecGroupId }}'
        SubnetId: '{{ createDCSubnet2.secondSubnetId }}'
        TagSpecifications:
          - ResourceType: instance
            Tags:
              - Key: Name
                Value: SampleDC2
      outputs:
        - Name: adcInstanceId
          Selector: '$.Instances[0].InstanceId'
          Type: String
      nextStep: verifyDCInstanceState
```

```
      - name: verifyDCInstanceState
        action: aws:waitForAwsResourceProperty
        inputs:
          Service: ec2
          Api: DescribeInstanceStatus
          IncludeAllInstances: true
          InstanceIds:
            - '{{ launchDC1.pdcInstanceId }}'
            - '{{ launchDC2.adcInstanceId }}'
          PropertySelector: '$.InstanceStatuses..InstanceState.Name'
          DesiredValues:
            - running
        nextStep: verifyInstancesOnlineSSM
      - name: verifyInstancesOnlineSSM
        action: aws:waitForAwsResourceProperty
        timeoutSeconds: 600
        inputs:
          Service: ssm
          Api: DescribeInstanceInformation
          InstanceInformationFilterList:
            - key: InstanceIds
              valueSet:
                - '{{ launchDC1.pdcInstanceId }}'
                - '{{ launchDC2.adcInstanceId }}'
          PropertySelector: '$.InstanceInformationList..PingStatus'
          DesiredValues:
            - Online
        nextStep: installADRoles
      - name: installADRoles
        action: aws:runCommand
        inputs:
          DocumentName: AWS-RunPowerShellScript
          InstanceIds:
            - '{{ launchDC1.pdcInstanceId }}'
            - '{{ launchDC2.adcInstanceId }}'
          Parameters:
            commands: |-
              try {
                  Install-WindowsFeature -Name AD-Domain-Services -
IncludeManagementTools
              }
              catch {
                  Write-Error "Failed to install ADDS Role."
              }
```

```
        nextStep: setAdminPassword
      - name: setAdminPassword
        action: aws:runCommand
        inputs:
          DocumentName: AWS-RunPowerShellScript
          InstanceIds:
            - '{{ launchDC1.pdcInstanceId }}'
          Parameters:
            commands:
              - net user Administrator "sampleAdminPass123!"
        nextStep: createForest
      - name: createForest
        action: aws:runCommand
        inputs:
          DocumentName: AWS-RunPowerShellScript
          InstanceIds:
            - '{{ launchDC1.pdcInstanceId }}'
          Parameters:
            commands: |-
              $dsrmPass = 'sample123!' | ConvertTo-SecureString -asPlainText -Force
              try {
                  Install-ADDSForest -DomainName "sample.com" -DomainMode 6
 -ForestMode 6 -InstallDNS -DatabasePath "D:\NTDS" -SysvolPath "D:\SYSVOL" -
SafeModeAdministratorPassword $dsrmPass -Force
              }
              catch {
                  Write-Error $_
              }
              try {
                  Add-DnsServerForwarder -IPAddress "10.0.100.2"
              }
              catch {
                  Write-Error $_
              }
        nextStep: associateDhcpOptions
      - name: associateDhcpOptions
        action: aws:executeAwsApi
        onFailure: Abort
        inputs:
          Service: ec2
          Api: AssociateDhcpOptions
          DhcpOptionsId: '{{ createDhcpOptions.dhcpOptionsId }}'
          VpcId: '{{ createVpc.vpcId }}'
        nextStep: waitForADServices
```

```
      - name: waitForADServices
        action: aws:sleep
        inputs:
          Duration: PT1M
        nextStep: promoteADC
      - name: promoteADC
        action: aws:runCommand
        inputs:
          DocumentName: AWS-RunPowerShellScript
          InstanceIds:
            - '{{ launchDC2.adcInstanceId }}'
          Parameters:
            commands: |-
              ipconfig /renew
              $dsrmPass = 'sample123!' | ConvertTo-SecureString -asPlainText -Force
              $domAdminUser = "sample\Administrator"
              $domAdminPass = "sampleAdminPass123!" | ConvertTo-SecureString -
asPlainText -Force
              $domAdminCred = New-Object
 System.Management.Automation.PSCredential($domAdminUser,$domAdminPass)

              try {
                  Install-ADDSDomainController -DomainName "sample.com" -InstallDNS
 -DatabasePath "D:\NTDS" -SysvolPath "D:\SYSVOL" -SafeModeAdministratorPassword
 $dsrmPass -Credential $domAdminCred -Force
              }
              catch {
                  Write-Error $_
              }
```

JSON

```
   {
     "description": "Custom Automation Deployment Example",
     "schemaVersion": "0.3",
     "assumeRole": "{{ AutomationAssumeRole }}",
     "parameters": {
       "AutomationAssumeRole": {
         "type": "String",
         "description": "(Optional) The ARN of the role that allows Automation
 to perform the actions on your behalf. If no role is specified, Systems Manager
 Automation uses your IAM permissions to run this runbook.",
```

```
          "default": ""
        }
      },
      "mainSteps": [
        {
          "name": "getLatestWindowsAmi",
          "action": "aws:executeAwsApi",
          "onFailure": "Abort",
          "inputs": {
            "Service": "ssm",
            "Api": "GetParameter",
            "Name": "/aws/service/ami-windows-latest/Windows_Server-2016-English-
Full-Base"
          },
          "outputs": [
            {
              "Name": "amiId",
              "Selector": "$.Parameter.Value",
              "Type": "String"
            }
          ],
          "nextStep": "createSSMInstanceRole"
        },
        {
          "name": "createSSMInstanceRole",
          "action": "aws:executeAwsApi",
          "onFailure": "Abort",
          "inputs": {
            "Service": "iam",
            "Api": "CreateRole",
            "AssumeRolePolicyDocument": "{\"Version\":\"2012-10-17\",\"Statement\":
[{\"Effect\":\"Allow\",\"Principal\":{\"Service\":[\"ec2.amazonaws.com\"]},\"Action
\":[\"sts:AssumeRole\"]}]}",
            "RoleName": "sampleSSMInstanceRole"
          },
          "nextStep": "attachManagedSSMPolicy"
        },
        {
          "name": "attachManagedSSMPolicy",
          "action": "aws:executeAwsApi",
          "onFailure": "Abort",
          "inputs": {
            "Service": "iam",
            "Api": "AttachRolePolicy",
```

```
            "PolicyArn": "arn:aws:iam::aws:policy/service-role/
AmazonSSMManagedInstanceCore",
            "RoleName": "sampleSSMInstanceRole"
          },
          "nextStep": "createSSMInstanceProfile"
        },
        {
          "name": "createSSMInstanceProfile",
          "action":"aws:executeAwsApi",
          "onFailure": "Abort",
          "inputs": {
            "Service": "iam",
            "Api": "CreateInstanceProfile",
            "InstanceProfileName": "sampleSSMInstanceRole"
          },
          "outputs": [
            {
              "Name": "instanceProfileArn",
              "Selector": "$.InstanceProfile.Arn",
              "Type": "String"
            }
          ],
          "nextStep": "addSSMInstanceRoleToProfile"
        },
        {
          "name": "addSSMInstanceRoleToProfile",
          "action": "aws:executeAwsApi",
          "onFailure": "Abort",
          "inputs": {
            "Service": "iam",
            "Api": "AddRoleToInstanceProfile",
            "InstanceProfileName": "sampleSSMInstanceRole",
            "RoleName": "sampleSSMInstanceRole"
          },
          "nextStep": "createVpc"
        },
        {
          "name": "createVpc",
          "action": "aws:executeAwsApi",
          "onFailure": "Abort",
          "inputs": {
            "Service": "ec2",
            "Api": "CreateVpc",
            "CidrBlock": "10.0.100.0/22"
```

```
      },
      "outputs": [
        {
          "Name": "vpcId",
          "Selector": "$.Vpc.VpcId",
          "Type": "String"
        }

      "nextStep": "getMainRtb"
    },
    {
      "name": "getMainRtb",
      "action": "aws:executeAwsApi",
      "onFailure": "Abort",
      "inputs": {
        "Service": "ec2",
        "Api": "DescribeRouteTables",
        "Filters": [
          {
            "Name": "vpc-id",
            "Values": ["{{ createVpc.vpcId }}"]
          }
        ]
      },
      "outputs": [
        {
          "Name": "mainRtbId",
          "Selector": "$.RouteTables[0].RouteTableId",
          "Type": "String"
        }
      ],
      "nextStep": "verifyMainRtb"
    },
    {
      "name": "verifyMainRtb",
      "action": "aws:assertAwsResourceProperty",
      "onFailure": "Abort",
      "inputs": {
        "Service": "ec2",
        "Api": "DescribeRouteTables",
        "RouteTableIds": ["{{ getMainRtb.mainRtbId }}"],
        "PropertySelector": "$.RouteTables[0].Associations[0].Main",
        "DesiredValues": ["True"]
      },
```

```
      "nextStep": "createPubSubnet"
    },
    {
      "name": "createPubSubnet",
      "action": "aws:executeAwsApi",
      "onFailure": "Abort",
      "inputs": {
        "Service": "ec2",
        "Api": "CreateSubnet",
        "CidrBlock": "10.0.103.0/24",
        "AvailabilityZone": "us-west-2c",
        "VpcId": "{{ createVpc.vpcId }}"
      },
      "outputs":[
        {
          "Name": "pubSubnetId",
          "Selector": "$.Subnet.SubnetId",
          "Type": "String"
        }
      ],
      "nextStep": "createPubRtb"
    },
    {
      "name": "createPubRtb",
      "action": "aws:executeAwsApi",
      "onFailure": "Abort",
      "inputs": {
        "Service": "ec2",
        "Api": "CreateRouteTable",
        "VpcId": "{{ createVpc.vpcId }}"
      },
      "outputs": [
        {
          "Name": "pubRtbId",
          "Selector": "$.RouteTable.RouteTableId",
          "Type": "String"
        }
      ],
      "nextStep": "createIgw"
    },
    {
      "name": "createIgw",
      "action": "aws:executeAwsApi",
      "onFailure": "Abort",
```

```
        "inputs": {
          "Service": "ec2",
          "Api": "CreateInternetGateway"
        },
        "outputs": [
          {
            "Name": "igwId",
            "Selector": "$.InternetGateway.InternetGatewayId",
            "Type": "String"
          }
        ],
        "nextStep": "attachIgw"
      },
      {
        "name": "attachIgw",
        "action": "aws:executeAwsApi",
        "onFailure": "Abort",
        "inputs": {
          "Service": "ec2",
          "Api": "AttachInternetGateway",
          "InternetGatewayId": "{{ createIgw.igwId }}",
          "VpcId": "{{ createVpc.vpcId }}"
        },
        "nextStep": "allocateEip"
      },
      {
        "name": "allocateEip",
        "action": "aws:executeAwsApi",
        "onFailure": "Abort",
        "inputs": {
          "Service": "ec2",
          "Api": "AllocateAddress",
          "Domain": "vpc"
        },
        "outputs": [
          {
            "Name": "eipAllocationId",
            "Selector": "$.AllocationId",
            "Type": "String"
          }
        ],
        "nextStep": "createNatGw"
      },
      {
```

```
            "name": "createNatGw",
            "action": "aws:executeAwsApi",
            "onFailure": "Abort",
            "inputs": {
              "Service": "ec2",
              "Api": "CreateNatGateway",
              "AllocationId": "{{ allocateEip.eipAllocationId }}",
              "SubnetId": "{{ createPubSubnet.pubSubnetId }}"
            },
            "outputs":[
              {
                "Name": "natGwId",
                "Selector": "$.NatGateway.NatGatewayId",
                "Type": "String"
              }
            ],
            "nextStep": "verifyNatGwAvailable"
          },
          {
            "name": "verifyNatGwAvailable",
            "action": "aws:waitForAwsResourceProperty",
            "timeoutSeconds": 150,
            "inputs": {
              "Service": "ec2",
              "Api": "DescribeNatGateways",
              "NatGatewayIds": [
                "{{ createNatGw.natGwId }}"
              ],
              "PropertySelector": "$.NatGateways[0].State",
              "DesiredValues": [
                "available"
              ]
            },
            "nextStep": "createNatRoute"
          },
          {
            "name": "createNatRoute",
            "action": "aws:executeAwsApi",
            "onFailure": "Abort",
            "inputs": {
              "Service": "ec2",
              "Api": "CreateRoute",
              "DestinationCidrBlock": "0.0.0.0/0",
              "NatGatewayId": "{{ createNatGw.natGwId }}",
```

```
            "RouteTableId": "{{ getMainRtb.mainRtbId }}"
          },
          "nextStep": "createPubRoute"
        },
        {
          "name": "createPubRoute",
          "action": "aws:executeAwsApi",
          "onFailure": "Abort",
          "inputs": {
            "Service": "ec2",
            "Api": "CreateRoute",
            "DestinationCidrBlock": "0.0.0.0/0",
            "GatewayId": "{{ createIgw.igwId }}",
            "RouteTableId": "{{ createPubRtb.pubRtbId }}"
          },
          "nextStep": "setPubSubAssoc"
        },
        {
          "name": "setPubSubAssoc",
          "action": "aws:executeAwsApi",
          "onFailure": "Abort",
          "inputs": {
            "Service": "ec2",
            "Api": "AssociateRouteTable",
            "RouteTableId": "{{ createPubRtb.pubRtbId }}",
            "SubnetId": "{{ createPubSubnet.pubSubnetId }}"
          }
        },
        {
          "name": "createDhcpOptions",
          "action": "aws:executeAwsApi",
          "onFailure": "Abort",
          "inputs": {
            "Service": "ec2",
            "Api": "CreateDhcpOptions",
            "DhcpConfigurations": [
              {
                "Key": "domain-name-servers",
                "Values": ["10.0.100.50,10.0.101.50"]
              },
              {
                "Key": "domain-name",
                "Values": ["sample.com"]
              }
```

```
            ]
          },
          "outputs": [
            {
              "Name": "dhcpOptionsId",
              "Selector": "$.DhcpOptions.DhcpOptionsId",
              "Type": "String"
            }
          ],
          "nextStep": "createDCSubnet1"
        },
        {
          "name": "createDCSubnet1",
          "action": "aws:executeAwsApi",
          "onFailure": "Abort",
          "inputs": {
            "Service": "ec2",
            "Api": "CreateSubnet",
            "CidrBlock": "10.0.100.0/24",
            "AvailabilityZone": "us-west-2a",
            "VpcId": "{{ createVpc.vpcId }}"
          },
          "outputs": [
            {
              "Name": "firstSubnetId",
              "Selector": "$.Subnet.SubnetId",
              "Type": "String"
            }
          ],
          "nextStep": "createDCSubnet2"
        },
        {
          "name": "createDCSubnet2",
          "action": "aws:executeAwsApi",
          "onFailure": "Abort",
          "inputs": {
            "Service": "ec2",
            "Api": "CreateSubnet",
            "CidrBlock": "10.0.101.0/24",
            "AvailabilityZone": "us-west-2b",
            "VpcId": "{{ createVpc.vpcId }}"
          },
          "outputs": [
            {
```

```
            "Name": "secondSubnetId",
            "Selector": "$.Subnet.SubnetId",
            "Type": "String"
          }
        ],
        "nextStep": "createDCSecGroup"
      },
      {
        "name": "createDCSecGroup",
        "action": "aws:executeAwsApi",
        "onFailure": "Abort",
        "inputs": {
          "Service": "ec2",
          "Api": "CreateSecurityGroup",
          "GroupName": "SampleDCSecGroup",
          "Description": "Security Group for Example Domain Controllers",
          "VpcId": "{{ createVpc.vpcId }}"
        },
        "outputs": [
          {
            "Name": "dcSecGroupId",
            "Selector": "$.GroupId",
            "Type": "String"
          }
        ],
        "nextStep": "authIngressDCTraffic"
      },
      {
        "name": "authIngressDCTraffic",
        "action": "aws:executeAwsApi",
        "onFailure": "Abort",
        "inputs": {
          "Service": "ec2",
          "Api": "AuthorizeSecurityGroupIngress",
          "GroupId": "{{ createDCSecGroup.dcSecGroupId }}",
          "IpPermissions": [
            {
              "FromPort": -1,
              "IpProtocol": "-1",
              "IpRanges": [
                {
                  "CidrIp": "0.0.0.0/0",
                  "Description": "Allow all traffic between Domain Controllers"
                }
```

```
            ]
          }
        ]
      },
      "nextStep": "verifyInstanceProfile"
    },
    {
      "name": "verifyInstanceProfile",
      "action": "aws:waitForAwsResourceProperty",
      "maxAttempts": 5,
      "onFailure": "Abort",
      "inputs": {
        "Service": "iam",
        "Api": "ListInstanceProfilesForRole",
        "RoleName": "sampleSSMInstanceRole",
        "PropertySelector": "$.InstanceProfiles[0].Arn",
        "DesiredValues": [
          "{{ createSSMInstanceProfile.instanceProfileArn }}"
        ]
      },
      "nextStep": "iamEventualConsistency"
    },
    {
      "name": "iamEventualConsistency",
      "action": "aws:sleep",
      "inputs": {
        "Duration": "PT2M"
      },
      "nextStep": "launchDC1"
    },
    {
      "name": "launchDC1",
      "action": "aws:executeAwsApi",
      "onFailure": "Abort",
      "inputs": {
        "Service": "ec2",
        "Api": "RunInstances",
        "BlockDeviceMappings": [
          {
            "DeviceName": "/dev/sda1",
            "Ebs": {
              "DeleteOnTermination": true,
              "VolumeSize": 50,
              "VolumeType": "gp2"
```

```
            }
          },
          {
            "DeviceName": "xvdf",
            "Ebs": {
              "DeleteOnTermination": true,
              "VolumeSize": 100,
              "VolumeType": "gp2"
            }
          }
        ],
        "IamInstanceProfile": {
          "Arn": "{{ createSSMInstanceProfile.instanceProfileArn }}"
        },
        "ImageId": "{{ getLatestWindowsAmi.amiId }}",
        "InstanceType": "t2.micro",
        "MaxCount": 1,
        "MinCount": 1,
        "PrivateIpAddress": "10.0.100.50",
        "SecurityGroupIds": [
          "{{ createDCSecGroup.dcSecGroupId }}"
        ],
        "SubnetId": "{{ createDCSubnet1.firstSubnetId }}",
        "TagSpecifications": [
          {
            "ResourceType": "instance",
            "Tags": [
              {
                "Key": "Name",
                "Value": "SampleDC1"
              }
            ]
          }
        ]
      },
      "outputs": [
        {
          "Name": "pdcInstanceId",
          "Selector": "$.Instances[0].InstanceId",
          "Type": "String"
        }
      ],
      "nextStep": "launchDC2"
    },
```

```
        {
          "name": "launchDC2",
          "action": "aws:executeAwsApi",
          "onFailure": "Abort",
          "inputs": {
            "Service": "ec2",
            "Api": "RunInstances",
            "BlockDeviceMappings": [
              {
                "DeviceName": "/dev/sda1",
                "Ebs": {
                  "DeleteOnTermination": true,
                  "VolumeSize": 50,
                  "VolumeType": "gp2"
                }
              },
              {
                "DeviceName": "xvdf",
                "Ebs": {
                  "DeleteOnTermination": true,
                  "VolumeSize": 100,
                  "VolumeType": "gp2"
                }
              }
            ],
            "IamInstanceProfile": {
              "Arn": "{{ createSSMInstanceProfile.instanceProfileArn }}"
            },
            "ImageId": "{{ getLatestWindowsAmi.amiId }}",
            "InstanceType": "t2.micro",
            "MaxCount": 1,
            "MinCount": 1,
            "PrivateIpAddress": "10.0.101.50",
            "SecurityGroupIds": [
              "{{ createDCSecGroup.dcSecGroupId }}"
            ],
            "SubnetId": "{{ createDCSubnet2.secondSubnetId }}",
            "TagSpecifications": [
              {
                "ResourceType": "instance",
                "Tags": [
                  {
                    "Key": "Name",
                    "Value": "SampleDC2"
```

```
                }
              ]
            }
          ]
        },
        "outputs": [
          {
            "Name": "adcInstanceId",
            "Selector": "$.Instances[0].InstanceId",
            "Type": "String"
          }
        ],
        "nextStep": "verifyDCInstanceState"
      },
      {
        "name": "verifyDCInstanceState",
        "action": "aws:waitForAwsResourceProperty",
        "inputs": {
          "Service": "ec2",
          "Api": "DescribeInstanceStatus",
          "IncludeAllInstances": true,
          "InstanceIds": [
            "{{ launchDC1.pdcInstanceId }}",
            "{{ launchDC2.adcInstanceId }}"
          ],
          "PropertySelector": "$.InstanceStatuses[0].InstanceState.Name",
          "DesiredValues": [
            "running"
          ]
        },
        "nextStep": "verifyInstancesOnlineSSM"
      },
      {
        "name": "verifyInstancesOnlineSSM",
        "action": "aws:waitForAwsResourceProperty",
        "timeoutSeconds": 600,
        "inputs": {
          "Service": "ssm",
          "Api": "DescribeInstanceInformation",
          "InstanceInformationFilterList": [
            {
              "key": "InstanceIds",
              "valueSet": [
                "{{ launchDC1.pdcInstanceId }}",
```

```
                "{{ launchDC2.adcInstanceId }}"
              ]
            }
          ],
          "PropertySelector": "$.InstanceInformationList[0].PingStatus",
          "DesiredValues": [
            "Online"
          ]
        },
        "nextStep": "installADRoles"
      },
      {
        "name": "installADRoles",
        "action": "aws:runCommand",
        "inputs": {
          "DocumentName": "AWS-RunPowerShellScript",
          "InstanceIds": [
            "{{ launchDC1.pdcInstanceId }}",
            "{{ launchDC2.adcInstanceId }}"
          ],
          "Parameters": {
            "commands": [
              "try {",
              "  Install-WindowsFeature -Name AD-Domain-Services -
IncludeManagementTools",
              "}",
              "catch {",
              "  Write-Error \"Failed to install ADDS Role.\"",
              "}"
            ]
          }
        },
        "nextStep": "setAdminPassword"
      },
      {
        "name": "setAdminPassword",
        "action": "aws:runCommand",
        "inputs": {
          "DocumentName": "AWS-RunPowerShellScript",
          "InstanceIds": [
            "{{ launchDC1.pdcInstanceId }}"
          ],
          "Parameters": {
            "commands": [
```

```
                "net user Administrator \"sampleAdminPass123!\""
              ]
            }
          },
          "nextStep": "createForest"
        },
        {
          "name": "createForest",
          "action": "aws:runCommand",
          "inputs": {
            "DocumentName": "AWS-RunPowerShellScript",
            "InstanceIds": [
              "{{ launchDC1.pdcInstanceId }}"
            ],
            "Parameters": {
              "commands": [
                "$dsrmPass = 'sample123!' | ConvertTo-SecureString -asPlainText -
Force",
                "try {",
                "   Install-ADDSForest -DomainName \"sample.com\" -DomainMode 6 -
ForestMode 6 -InstallDNS -DatabasePath \"D:\\NTDS\" -SysvolPath \"D:\\SYSVOL\" -
SafeModeAdministratorPassword $dsrmPass -Force",
                "}",
                "catch {",
                "   Write-Error $_",
                "}",
                "try {",
                "   Add-DnsServerForwarder -IPAddress \"10.0.100.2\"",
                "}",
                "catch {",
                "   Write-Error $_",
                "}"
              ]
            }
          },
          "nextStep": "associateDhcpOptions"
        },
        {
          "name": "associateDhcpOptions",
          "action": "aws:executeAwsApi",
          "onFailure": "Abort",
          "inputs": {
            "Service": "ec2",
            "Api": "AssociateDhcpOptions",
```

```
            "DhcpOptionsId": "{{ createDhcpOptions.dhcpOptionsId }}",
            "VpcId": "{{ createVpc.vpcId }}"
          },
          "nextStep": "waitForADServices"
        },
        {
          "name": "waitForADServices",
          "action": "aws:sleep",
          "inputs": {
            "Duration": "PT1M"
          },
          "nextStep": "promoteADC"
        },
        {
          "name": "promoteADC",
          "action": "aws:runCommand",
          "inputs": {
            "DocumentName": "AWS-RunPowerShellScript",
            "InstanceIds": [
              "{{ launchDC2.adcInstanceId }}"
            ],
            "Parameters": {
              "commands": [
                "ipconfig /renew",
                "$dsrmPass = 'sample123!' | ConvertTo-SecureString -asPlainText -
Force",
                "$domAdminUser = \"sample\\Administrator\"",
                "$domAdminPass = \"sampleAdminPass123!\" | ConvertTo-SecureString -
asPlainText -Force",
                "$domAdminCred = New-Object
 System.Management.Automation.PSCredential($domAdminUser,$domAdminPass)",
                "try {",
                "   Install-ADDSDomainController -DomainName \"sample.com
\" -InstallDNS -DatabasePath \"D:\\NTDS\" -SysvolPath \"D:\\SYSVOL\" -
SafeModeAdministratorPassword $dsrmPass -Credential $domAdminCred -Force",
                "}",
                "catch {",
                "   Write-Error $_",
                "}"
              ]
            }
          }
        }
      ]
```

```
    }
```

最新のスナップショットからルートボリュームを復元する

ルートボリューム上のオペレーティングシステムは、さまざまな理由で破損する可能性があります。例えば、パッチ適用オペレーション後、カーネルまたはレジストリが破損しているため、インスタンスが正常に起動しない場合があります。パッチ適用操作の前に作成された最新のスナップショットからルートボリュームを復元するなどの一般的なトラブルシューティングタスクを自動化することで、ダウンタイムを短縮し、トラブルシューティング作業を迅速化できます。AWS Systems Manager オートメーションアクションが、これを実現するのに役立ちます。Automation は AWS Systems Manager のツールです。

次の AWS Systems Manager ランブックの例では、これらのアクションを実行します。

- `aws:executeAwsApi` オートメーションアクションを使用して、インスタンスのルートボリュームから詳細を取得します。
- `aws:executeScript` オートメーションアクションを使用して、ルートボリュームの最新のスナップショットを取得します。
- ルートボリュームのスナップショットが見つかった場合、`aws:branch` オートメーションアクションを使用して実行を続行します。

YAML

```
   ---
   description: Custom Automation Troubleshooting Example
   schemaVersion: '0.3'
   assumeRole: "{{ AutomationAssumeRole }}"
   parameters:
     AutomationAssumeRole:
       type: String
       description: "(Required) The ARN of the role that allows Automation to
perform
         the actions on your behalf. If no role is specified, Systems Manager
Automation
         uses your IAM permissions to use this runbook."
       default: ''
     InstanceId:
         type: String
```

```
        description: "(Required) The Instance Id whose root EBS volume you want to
restore the latest Snapshot."
        default: ''
   mainSteps:
   - name: getInstanceDetails
     action: aws:executeAwsApi
     onFailure: Abort
     inputs:
       Service: ec2
       Api: DescribeInstances
       InstanceIds:
       - "{{ InstanceId }}"
     outputs:
       - Name: availabilityZone
         Selector: "$.Reservations[0].Instances[0].Placement.AvailabilityZone"
         Type: String
       - Name: rootDeviceName
         Selector: "$.Reservations[0].Instances[0].RootDeviceName"
         Type: String
     nextStep: getRootVolumeId
   - name: getRootVolumeId
     action: aws:executeAwsApi
     onFailure: Abort
     inputs:
       Service: ec2
       Api: DescribeVolumes
       Filters:
       -  Name: attachment.device
          Values: ["{{ getInstanceDetails.rootDeviceName }}"]
       -  Name: attachment.instance-id
          Values: ["{{ InstanceId }}"]
     outputs:
       - Name: rootVolumeId
         Selector: "$.Volumes[0].VolumeId"
         Type: String
     nextStep: getSnapshotsByStartTime
   - name: getSnapshotsByStartTime
     action: aws:executeScript
     timeoutSeconds: 45
     onFailure: Abort
     inputs:
       Runtime: python3.8
       Handler: getSnapshotsByStartTime
       InputPayload:
```

```
          rootVolumeId : "{{ getRootVolumeId.rootVolumeId }}"
        Script: |-
          def getSnapshotsByStartTime(events,context):
            import boto3

            #Initialize client
            ec2 = boto3.client('ec2')
            rootVolumeId = events['rootVolumeId']
            snapshotsQuery = ec2.describe_snapshots(
              Filters=[
                {
                  "Name": "volume-id",
                  "Values": [rootVolumeId]
                }
              ]
            )
            if not snapshotsQuery['Snapshots']:
              noSnapshotFoundString = "NoSnapshotFound"
              return { 'noSnapshotFound' : noSnapshotFoundString }
            else:
              jsonSnapshots = snapshotsQuery['Snapshots']
              sortedSnapshots = sorted(jsonSnapshots, key=lambda k: k['StartTime'],
reverse=True)
              latestSortedSnapshotId = sortedSnapshots[0]['SnapshotId']
              return { 'latestSnapshotId' : latestSortedSnapshotId }
      outputs:
      - Name: Payload
        Selector: $.Payload
        Type: StringMap
      - Name: latestSnapshotId
        Selector: $.Payload.latestSnapshotId
        Type: String
      - Name: noSnapshotFound
        Selector: $.Payload.noSnapshotFound
        Type: String
      nextStep: branchFromResults
    - name: branchFromResults
      action: aws:branch
      onFailure: Abort
      inputs:
        Choices:
        - NextStep: createNewRootVolumeFromSnapshot
          Not:
            Variable: "{{ getSnapshotsByStartTime.noSnapshotFound }}"
```

```
            StringEquals: "NoSnapshotFound"
      isEnd: true
    - name: createNewRootVolumeFromSnapshot
      action: aws:executeAwsApi
      onFailure: Abort
      inputs:
        Service: ec2
        Api: CreateVolume
        AvailabilityZone: "{{ getInstanceDetails.availabilityZone }}"
        SnapshotId: "{{ getSnapshotsByStartTime.latestSnapshotId }}"
      outputs:
        - Name: newRootVolumeId
          Selector: "$.VolumeId"
          Type: String
      nextStep: stopInstance
    - name: stopInstance
      action: aws:executeAwsApi
      onFailure: Abort
      inputs:
        Service: ec2
        Api: StopInstances
        InstanceIds:
        - "{{ InstanceId }}"
      nextStep: verifyVolumeAvailability
    - name: verifyVolumeAvailability
      action: aws:waitForAwsResourceProperty
      timeoutSeconds: 120
      inputs:
        Service: ec2
        Api: DescribeVolumes
        VolumeIds:
        - "{{ createNewRootVolumeFromSnapshot.newRootVolumeId }}"
        PropertySelector: "$.Volumes[0].State"
        DesiredValues:
        - "available"
      nextStep: verifyInstanceStopped
    - name: verifyInstanceStopped
      action: aws:waitForAwsResourceProperty
      timeoutSeconds: 120
      inputs:
        Service: ec2
        Api: DescribeInstances
        InstanceIds:
        - "{{ InstanceId }}"
```

```
        PropertySelector: "$.Reservations[0].Instances[0].State.Name"
        DesiredValues:
        - "stopped"
      nextStep: detachRootVolume
    - name: detachRootVolume
      action: aws:executeAwsApi
      onFailure: Abort
      inputs:
        Service: ec2
        Api: DetachVolume
        VolumeId: "{{ getRootVolumeId.rootVolumeId }}"
      nextStep: verifyRootVolumeDetached
    - name: verifyRootVolumeDetached
      action: aws:waitForAwsResourceProperty
      timeoutSeconds: 30
      inputs:
        Service: ec2
        Api: DescribeVolumes
        VolumeIds:
        - "{{ getRootVolumeId.rootVolumeId }}"
        PropertySelector: "$.Volumes[0].State"
        DesiredValues:
        - "available"
      nextStep: attachNewRootVolume
    - name: attachNewRootVolume
      action: aws:executeAwsApi
      onFailure: Abort
      inputs:
        Service: ec2
        Api: AttachVolume
        Device: "{{ getInstanceDetails.rootDeviceName }}"
        InstanceId: "{{ InstanceId }}"
        VolumeId: "{{ createNewRootVolumeFromSnapshot.newRootVolumeId }}"
      nextStep: verifyNewRootVolumeAttached
    - name: verifyNewRootVolumeAttached
      action: aws:waitForAwsResourceProperty
      timeoutSeconds: 30
      inputs:
        Service: ec2
        Api: DescribeVolumes
        VolumeIds:
        - "{{ createNewRootVolumeFromSnapshot.newRootVolumeId }}"
        PropertySelector: "$.Volumes[0].Attachments[0].State"
        DesiredValues:
```

```
        - "attached"
      nextStep: startInstance
    - name: startInstance
      action: aws:executeAwsApi
      onFailure: Abort
      inputs:
        Service: ec2
        Api: StartInstances
        InstanceIds:
        - "{{ InstanceId }}"
```

JSON

```
   {
      "description": "Custom Automation Troubleshooting Example",
      "schemaVersion": "0.3",
      "assumeRole": "{{ AutomationAssumeRole }}",
      "parameters": {
         "AutomationAssumeRole": {
            "type": "String",
            "description": "(Required) The ARN of the role that allows Automation
to perform the actions on your behalf. If no role is specified, Systems Manager
Automation uses your IAM permissions to run this runbook.",
            "default": ""
         },
         "InstanceId": {
            "type": "String",
            "description": "(Required) The Instance Id whose root EBS volume you
want to restore the latest Snapshot.",
            "default": ""
         }
      },
      "mainSteps": [
         {
            "name": "getInstanceDetails",
            "action": "aws:executeAwsApi",
            "onFailure": "Abort",
            "inputs": {
               "Service": "ec2",
               "Api": "DescribeInstances",
               "InstanceIds": [
                  "{{ InstanceId }}"
```

```
            ]
         },
         "outputs": [
            {
               "Name": "availabilityZone",
               "Selector":
"$.Reservations[0].Instances[0].Placement.AvailabilityZone",
               "Type": "String"
            },
            {
               "Name": "rootDeviceName",
               "Selector": "$.Reservations[0].Instances[0].RootDeviceName",
               "Type": "String"
            }
         ],
         "nextStep": "getRootVolumeId"
      },
      {
         "name": "getRootVolumeId",
         "action": "aws:executeAwsApi",
         "onFailure": "Abort",
         "inputs": {
            "Service": "ec2",
            "Api": "DescribeVolumes",
            "Filters": [
               {
                  "Name": "attachment.device",
                  "Values": [
                     "{{ getInstanceDetails.rootDeviceName }}"
                  ]
               },
               {
                  "Name": "attachment.instance-id",
                  "Values": [
                     "{{ InstanceId }}"
                  ]
               }
            ]
         },
         "outputs": [
            {
               "Name": "rootVolumeId",
               "Selector": "$.Volumes[0].VolumeId",
               "Type": "String"
```

```
            }
         ],
         "nextStep": "getSnapshotsByStartTime"
      },
      {
         "name": "getSnapshotsByStartTime",
         "action": "aws:executeScript",
         "timeoutSeconds": 45,
         "onFailure": "Continue",
         "inputs": {
            "Runtime": "python3.8",
            "Handler": "getSnapshotsByStartTime",
            "InputPayload": {
               "rootVolumeId": "{{ getRootVolumeId.rootVolumeId }}"
            },
            "Attachment": "getSnapshotsByStartTime.py"
         },
         "outputs": [
            {
               "Name": "Payload",
               "Selector": "$.Payload",
               "Type": "StringMap"
            },
            {
               "Name": "latestSnapshotId",
               "Selector": "$.Payload.latestSnapshotId",
               "Type": "String"
            },
            {
               "Name": "noSnapshotFound",
               "Selector": "$.Payload.noSnapshotFound",
               "Type": "String"
            }
         ],
         "nextStep": "branchFromResults"
      },
      {
         "name": "branchFromResults",
         "action": "aws:branch",
         "onFailure": "Abort",
         "inputs": {
            "Choices": [
               {
                  "NextStep": "createNewRootVolumeFromSnapshot",
```

```
                    "Not": {
                       "Variable":
"{{ getSnapshotsByStartTime.noSnapshotFound }}",
                       "StringEquals": "NoSnapshotFound"
                    }
                 }
              ]
           },
           "isEnd": true
        },
        {
           "name": "createNewRootVolumeFromSnapshot",
           "action": "aws:executeAwsApi",
           "onFailure": "Abort",
           "inputs": {
              "Service": "ec2",
              "Api": "CreateVolume",
              "AvailabilityZone": "{{ getInstanceDetails.availabilityZone }}",
              "SnapshotId": "{{ getSnapshotsByStartTime.latestSnapshotId }}"
           },
           "outputs": [
              {
                 "Name": "newRootVolumeId",
                 "Selector": "$.VolumeId",
                 "Type": "String"
              }
           ],
           "nextStep": "stopInstance"
        },
        {
           "name": "stopInstance",
           "action": "aws:executeAwsApi",
           "onFailure": "Abort",
           "inputs": {
              "Service": "ec2",
              "Api": "StopInstances",
              "InstanceIds": [
                 "{{ InstanceId }}"
              ]
           },
           "nextStep": "verifyVolumeAvailability"
        },
        {
           "name": "verifyVolumeAvailability",
```

```
            "action": "aws:waitForAwsResourceProperty",
            "timeoutSeconds": 120,
            "inputs": {
               "Service": "ec2",
               "Api": "DescribeVolumes",
               "VolumeIds": [
                  "{{ createNewRootVolumeFromSnapshot.newRootVolumeId }}"
               ],
               "PropertySelector": "$.Volumes[0].State",
               "DesiredValues": [
                  "available"
               ]
            },
            "nextStep": "verifyInstanceStopped"
         },
         {
            "name": "verifyInstanceStopped",
            "action": "aws:waitForAwsResourceProperty",
            "timeoutSeconds": 120,
            "inputs": {
               "Service": "ec2",
               "Api": "DescribeInstances",
               "InstanceIds": [
                  "{{ InstanceId }}"
               ],
               "PropertySelector": "$.Reservations[0].Instances[0].State.Name",
               "DesiredValues": [
                  "stopped"
               ]
            },
            "nextStep": "detachRootVolume"
         },
         {
            "name": "detachRootVolume",
            "action": "aws:executeAwsApi",
            "onFailure": "Abort",
            "inputs": {
               "Service": "ec2",
               "Api": "DetachVolume",
               "VolumeId": "{{ getRootVolumeId.rootVolumeId }}"
            },
            "nextStep": "verifyRootVolumeDetached"
         },
         {
```

```
            "name": "verifyRootVolumeDetached",
            "action": "aws:waitForAwsResourceProperty",
            "timeoutSeconds": 30,
            "inputs": {
               "Service": "ec2",
               "Api": "DescribeVolumes",
               "VolumeIds": [
                  "{{ getRootVolumeId.rootVolumeId }}"
               ],
               "PropertySelector": "$.Volumes[0].State",
               "DesiredValues": [
                  "available"
               ]
            },
            "nextStep": "attachNewRootVolume"
         },
         {
            "name": "attachNewRootVolume",
            "action": "aws:executeAwsApi",
            "onFailure": "Abort",
            "inputs": {
               "Service": "ec2",
               "Api": "AttachVolume",
               "Device": "{{ getInstanceDetails.rootDeviceName }}",
               "InstanceId": "{{ InstanceId }}",
               "VolumeId": "{{ createNewRootVolumeFromSnapshot.newRootVolumeId }}"
            },
            "nextStep": "verifyNewRootVolumeAttached"
         },
         {
            "name": "verifyNewRootVolumeAttached",
            "action": "aws:waitForAwsResourceProperty",
            "timeoutSeconds": 30,
            "inputs": {
               "Service": "ec2",
               "Api": "DescribeVolumes",
               "VolumeIds": [
                  "{{ createNewRootVolumeFromSnapshot.newRootVolumeId }}"
               ],
               "PropertySelector": "$.Volumes[0].Attachments[0].State",
               "DesiredValues": [
                  "attached"
               ]
            },
```

```
            "nextStep": "startInstance"
         },
         {
            "name": "startInstance",
            "action": "aws:executeAwsApi",
            "onFailure": "Abort",
            "inputs": {
               "Service": "ec2",
               "Api": "StartInstances",
               "InstanceIds": [
                  "{{ InstanceId }}"
               ]
            }
         }
      ],
      "files": {
           "getSnapshotsByStartTime.py": {
               "checksums": {
                   "sha256": "sampleETagValue"
               }
           }
       }
   }
```

AMI とクロスリージョンコピーの作成

インスタンスの Amazon Machine Image (AMI) の作成は、バックアップと復旧で使用される一般的なプロセスです。災害対策アーキテクチャの一部として、AMI を別の AWS リージョン にコピーすることも選択できます。一般的なメンテナンスタスクを自動化することで、フェイルオーバーが必要な問題が発生した場合にダウンタイムを短縮できます。AWS Systems Managerオートメーションアクションが、これを実現するのに役立ちます。Automation は AWS Systems Manager のツールです。

次の AWS Systems Manager ランブックの例では、これらのアクションを実行します。

- `aws:executeAwsApi` オートメーションアクションを使用して、AMI を作成します。
- `aws:waitForAwsResourceProperty` オートメーションアクションを使用して、AMI の可用性を確認します。
- `aws:executeScript` オートメーションアクションを使用して、AMI を送信先リージョンにコピーします。

YAML

```
   ---
   description: Custom Automation Backup and Recovery Example
   schemaVersion: '0.3'
   assumeRole: "{{ AutomationAssumeRole }}"
   parameters:
     AutomationAssumeRole:
       type: String
       description: "(Required) The ARN of the role that allows Automation to
perform
         the actions on your behalf. If no role is specified, Systems Manager
Automation
         uses your IAM permissions to use this runbook."
       default: ''
     InstanceId:
       type: String
       description: "(Required) The ID of the EC2 instance."
       default: ''
   mainSteps:
   - name: createImage
     action: aws:executeAwsApi
     onFailure: Abort
     inputs:
       Service: ec2
       Api: CreateImage
       InstanceId: "{{ InstanceId }}"
       Name: "Automation Image for {{ InstanceId }}"
       NoReboot: false
     outputs:
       - Name: newImageId
         Selector: "$.ImageId"
         Type: String
     nextStep: verifyImageAvailability
   - name: verifyImageAvailability
     action: aws:waitForAwsResourceProperty
     timeoutSeconds: 600
     inputs:
       Service: ec2
       Api: DescribeImages
       ImageIds:
       - "{{ createImage.newImageId }}"
       PropertySelector: "$.Images[0].State"
```

```
        DesiredValues:
        - available
      nextStep: copyImage
    - name: copyImage
      action: aws:executeScript
      timeoutSeconds: 45
      onFailure: Abort
      inputs:
        Runtime: python3.8
        Handler: crossRegionImageCopy
        InputPayload:
          newImageId : "{{ createImage.newImageId }}"
        Script: |-
          def crossRegionImageCopy(events,context):
            import boto3

            #Initialize client
            ec2 = boto3.client('ec2', region_name='us-east-1')
            newImageId = events['newImageId']

            ec2.copy_image(
              Name='DR Copy for ' + newImageId,
              SourceImageId=newImageId,
              SourceRegion='us-west-2'
            )
```

JSON

```
   {
      "description": "Custom Automation Backup and Recovery Example",
      "schemaVersion": "0.3",
      "assumeRole": "{{ AutomationAssumeRole }}",
      "parameters": {
         "AutomationAssumeRole": {
            "type": "String",
            "description": "(Required) The ARN of the role that allows Automation
to perform\nthe actions on your behalf. If no role is specified, Systems Manager
Automation\nuses your IAM permissions to run this runbook.",
            "default": ""
         },
         "InstanceId": {
            "type": "String",
```

```
            "description": "(Required) The ID of the EC2 instance.",
            "default": ""
         }
      },
      "mainSteps": [
         {
            "name": "createImage",
            "action": "aws:executeAwsApi",
            "onFailure": "Abort",
            "inputs": {
               "Service": "ec2",
               "Api": "CreateImage",
               "InstanceId": "{{ InstanceId }}",
               "Name": "Automation Image for {{ InstanceId }}",
               "NoReboot": false
            },
            "outputs": [
               {
                  "Name": "newImageId",
                  "Selector": "$.ImageId",
                  "Type": "String"
               }
            ],
            "nextStep": "verifyImageAvailability"
         },
         {
            "name": "verifyImageAvailability",
            "action": "aws:waitForAwsResourceProperty",
            "timeoutSeconds": 600,
            "inputs": {
               "Service": "ec2",
               "Api": "DescribeImages",
               "ImageIds": [
                  "{{ createImage.newImageId }}"
               ],
               "PropertySelector": "$.Images[0].State",
               "DesiredValues": [
                  "available"
               ]
            },
            "nextStep": "copyImage"
         },
         {
            "name": "copyImage",
```

```
            "action": "aws:executeScript",
            "timeoutSeconds": 45,
            "onFailure": "Abort",
            "inputs": {
               "Runtime": "python3.8",
               "Handler": "crossRegionImageCopy",
               "InputPayload": {
                  "newImageId": "{{ createImage.newImageId }}"
               },
               "Attachment": "crossRegionImageCopy.py"
            }
         }
      ],
      "files": {
           "crossRegionImageCopy.py": {
               "checksums": {
                   "sha256": "sampleETagValue"
               }
           }
       }
   }
```

AWS リソースを設定する入力パラメーターの作成

Systems Manager のツールである Automation は、入力パラメータに対して定義したリソースタイプに一致する AWS リソースを AWS Management Consoleに入力します。リソースタイプと一致する AWS アカウント のリソースがドロップダウンリストに表示され、選択できます。Amazon Elastic Compute Cloud (Amazon EC2) インスタンス、Amazon Simple Storage Service (Amazon S3) バケット、および AWS Identity and Access Management (IAM) ロールに対して、入力パラメータを定義できます。サポートされているタイプ定義と、一致するリソースを検索するために使用される正規表現は次のとおりです。

- `AWS::EC2::Instance::Id` - `^m?i-([a-z0-9]{8}|[a-z0-9]{17})$`
- `List<AWS::EC2::Instance::Id>` - `^m?i-([a-z0-9]{8}|[a-z0-9]{17})$`
- `AWS::S3::Bucket::Name` - `^[0-9a-z][a-z0-9\\-\\.]{3,63}$`
- `List<AWS::S3::Bucket::Name>` - `^[0-9a-z][a-z0-9\\-\\.]{3,63}$`
- `AWS::IAM::Role::Arn` - `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12}:role/.*$`

- List<AWS::IAM::Role::Arn> - ^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam::[0-9]{12}:role/.*$

以下は、ランブックコンテンツで定義される入力パラメータタイプの例です。

YAML

```
description: Enables encryption on an Amazon S3 bucket
schemaVersion: '0.3'
assumeRole: '{{ AutomationAssumeRole }}'
parameters:
  BucketName:
    type: 'AWS::S3::Bucket::Name'
    description: (Required) The name of the Amazon S3 bucket you want to encrypt.
  SSEAlgorithm:
    type: String
    description: (Optional) The server-side encryption algorithm to use for the
 default encryption.
    default: AES256
  AutomationAssumeRole:
    type: 'AWS::IAM::Role::Arn'
    description: (Optional) The Amazon Resource Name (ARN) of the role that allows
 Automation to perform the actions on your behalf.
    default: ''
mainSteps:
  - name: enableBucketEncryption
    action: 'aws:executeAwsApi'
    inputs:
      Service: s3
      Api: PutBucketEncryption
      Bucket: '{{BucketName}}'
      ServerSideEncryptionConfiguration:
        Rules:
          - ApplyServerSideEncryptionByDefault:
              SSEAlgorithm: '{{SSEAlgorithm}}'
    isEnd: true
```

JSON

```
{
   "description": "Enables encryption on an Amazon S3 bucket",
   "schemaVersion": "0.3",
```

```
  "assumeRole": "{{ AutomationAssumeRole }}",
  "parameters": {
     "BucketName": {
        "type": "AWS::S3::Bucket::Name",
        "description": "(Required) The name of the Amazon S3 bucket you want to
encrypt."
     },
     "SSEAlgorithm": {
        "type": "String",
        "description": "(Optional) The server-side encryption algorithm to use for
the default encryption.",
        "default": "AES256"
     },
     "AutomationAssumeRole": {
        "type": "AWS::IAM::Role::Arn",
        "description": "(Optional) The Amazon Resource Name (ARN) of the role that
allows Automation to perform the actions on your behalf.",
        "default": ""
     }
  },
  "mainSteps": [
     {
        "name": "enableBucketEncryption",
        "action": "aws:executeAwsApi",
        "inputs": {
           "Service": "s3",
           "Api": "PutBucketEncryption",
           "Bucket": "{{BucketName}}",
           "ServerSideEncryptionConfiguration": {
              "Rules": [
                 {
                    "ApplyServerSideEncryptionByDefault": {
                       "SSEAlgorithm": "{{SSEAlgorithm}}"
                    }
                 }
              ]
           }
        },
        "isEnd": true
     }
  ]
}
```

ランブック作成のためのドキュメントビルダーの使用

AWS Systems Manager の公開ランブックが、AWS リソースで実行するすべてのアクションをサポートしない場合、独自のランブックを作成できます。カスタムランブックを作成するには、適切なオートメーションアクションを含むローカルの YAML または JSON 形式のファイルを手動で作成します。また別の方法として、Systems Manager Automation コンソールでドキュメントビルダーを使用し、カスタムランブックを構築することも可能です

ドキュメントビルダーを使用すると、JSON または YAML 構文を使用しなくても、オートメーションアクションをカスタムランブックに追加し、必要なパラメータを指定できます。ステップを追加してランブックを作成すると、追加したアクションが、Systems Manager がオートメーションの実行に使用できる YAML 形式に変換されます。

ランブックでは、マークアップ言語である Markdown の使用がサポートされています。これにより、wiki スタイルの説明をランブックやランブック内の個々のステップに追加できます。Markdown の使用に関する詳細については、「AWS での Markdown の使用」を参照してください。

ドキュメントビルダーを使用してランブックを作成する

開始する前に

ランブック内で使用できる他のさまざまなアクションについても、確認してみることをお勧めします。詳細については、「Systems Manager Automation アクションのリファレンス」を参照してください。

ドキュメントビルダーを使用してランブックを作成するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[ドキュメント] を選択します。
3. [Create automation (オートメーションを作成)] を選択します。
4. [名前] に、ランブックのわかりやすい名前を入力します。
5. [Document description (ドキュメントの説明)] に、ランブックのマークダウンスタイルの説明を入力します。ランブック、番号付きステップ、またはその他の種類の情報を使用してランブックを説明できます。コンテンツの書式設定については、デフォルトのテキストを参照してください。

> **Tip**
>
> [Hide preview (プレビューを非表示)] と [Show preview (プレビューを表示)] を切り替えて、作成時に説明の内容がどのように表示されるかを確認します。

6. （オプション）[Assume role (ロールの継承)] に、ユーザーに代わってアクションを実行するサービスロールの名前または ARN を入力します。ロールを指定しない場合、オートメーションはオートメーションを実行するユーザーのアクセス許可を使用します。

> **Important**
>
> `aws:executeScript` アクションを使用する Amazon が所有していないランブックの場合、ロールを指定する必要があります。詳細については、ランブックを使用するためのアクセス許可 を参照してください。

7. （オプション）[Outputs (出力)] に、このランブックを実行するための出力を入力して、他のプロセスで使用できるようにします。

   たとえば、ドキュメントが新しい AMI を作成する場合、["CreateImage.ImageId"] を指定し、この出力を使用して後続のオートメーションで新しいインスタンスを作成します。

8. （オプション）[Input parameters (入力パラメータ)] セクションを展開し、次の操作を行います。

   1. [Parameter name (パラメータ名)] に、作成するランブックパラメータのわかりやすい名前を入力します。
   2. [Type (タイプ)] で、パラメータのタイプ（`String` や `MapList` など）を選択します。
   3. [Required (必須)] で、次のいずれかの操作を行います。
      - ランタイムにこのランブックパラメータの値を指定する必要がある場合は、[Yes (はい)] を選択します。
      - パラメータが不要な場合は、[No (いいえ)] を選択し、（オプション）[Default value (デフォルト値)] にデフォルトのパラメータ値を入力します。
   4. [Description (説明)] に、ランブックパラメータの説明を入力します。

> **Note**
>
> ランブックパラメータをさらに追加するには、[Add a parameter (パラメータを追加)] を選択します。ランブックパラメータを削除するには、[X] (削除) ボタンを選択します。

9. (オプション) [Target type (ターゲットタイプ)] セクションを展開し、ターゲットタイプを選択して、オートメーションが実行できるリソースの種類を定義します。たとえば、EC2 インスタンスでランブックを使用するには、`/AWS::EC2::Instance` を選択します。

> **Note**
>
> 「`/`」の値を指定すると、ランブックはすべてのタイプのリソースで実行できます。有効なリソースタイプのリストについては、AWS CloudFormation ユーザーガイドの AWS リソースタイプのリファレンスをご参照ください。

10. (オプション) [Document tags (ドキュメントタグ)] セクションを展開し、ランブックに適用するタグキーと値のペアを 1 つ以上入力します。タグを使用すると、リソースの識別、整理、検索が容易になります。
11. [Step 1 (ステップ 1)] セクションで、次の情報を入力します。

    - [Step name (ステップ名)] に、オートメーションの最初のステップのわかりやすい名前を入力します。
    - [Action type (アクションタイプ)] で、このステップで使用するアクションタイプを選択します。

      使用可能なアクションタイプのリストと情報については、「Systems Manager Automation アクションのリファレンス」を参照してください。
    - [Description (説明)] に、オートメーションステップの説明を入力します。Markdown を使用してテキストの書式を設定できます。
    - 選択した [Action type (アクションタイプ)] に応じて、[Step inputs (ステップ入力)] セクションにアクションタイプに必要な入力を入力します。たとえば、アクション `aws:approve` を選択した場合は、`Approvers` プロパティの値を指定する必要があります。

      ステップ入力フィールドの詳細については、選択したアクションタイプの「Systems Manager Automation アクションのリファレンス」のエントリを参照してください。例: `aws:executeStateMachine` – AWS Step Functions ステートマシンを実行する。

- (オプション) [Additional inputs (追加入力)] で、ランブックに必要な追加の入力値を指定します。使用可能な入力タイプは、ステップで選択したアクションタイプによって異なります。（一部のアクションタイプには入力値が必要です）。

  > **Note**
  >
  > さらに入力を追加するには、[Add optional input (オプションの入力を追加)] を選択します。入力を削除するには、[X]（削除）ボタンを選択します。

- (オプション) [Outputs (入力)] に、このステップの出力を入力して、他のプロセスで使用できるようにします。

  > **Note**
  >
  > [Outputs (出力)] は、すべてのアクションタイプで使用できるわけではありません。

- (オプション) [Common properties (共通プロパティ)] セクションを展開し、すべてのオートメーションアクションに共通するアクションのプロパティを指定します。例えば、[Timeout seconds (タイムアウト秒)] には、ステップが停止するまでの実行時間を指定するための値を秒単位で指定できます。

  詳細については、「すべてのアクションで共有されるプロパティ」を参照してください。

> **Note**
>
> ステップをさらに追加するには、[Add step (ステップを追加)] を選択し、ステップを作成する手順を繰り返します。ステップを削除するには、[Remove step (ステップを削除)] を選択します。

12. [Create automation (オートメーションを作成)] を選択してランブックを保存します。

スクリプトを実行するランブックを作成する

次の手順で、AWS Systems Manager Automation コンソールでドキュメントビルダーを使用し、スクリプトを実行するためにカスタムランブックを作成する方法について説明します。

作成したランブックの最初のステップでは、スクリプトを実行して Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを起動します。2 番目のステップでは、インスタンスのステータス

チェックが ok に変更されるかどうかを監視する別のスクリプトが実行されます。次に、オートメーション実行の全体的なステータス Success が報告されます。

開始する前に

次の手順を完了していることを確認してください。

- 管理者権限を持っているか、または AWS Identity and Access Management (IAM) で Systems Manager にアクセスするための適切なアクセス許可が付与されていることを確認します。

  詳細については、ランブックへのユーザーアクセスの確認 を参照してください。
- AWS アカウント に Automation の IAM サービスロール (継承ロールとも呼ばれる) があることを確認します。このチュートリアルでは aws:executeScript アクションを使用するため、このロールが必要です。

  このロールの作成の詳細については、「オートメーションのサービスロール (ロールを引き受ける) アクセスの設定」を参照してください。

  [aws:executeScript] を実行するための IAM サービスロールの要件については、「ランブックを使用するためのアクセス許可」を参照してください。
- EC2 インスタンスを起動するアクセス許可があることを確認します。

  詳細については、「Amazon EC2 ユーザーガイド」の「IAM と Amazon EC2」を参照してください。

ドキュメントビルダーを使用してスクリプトを実行するためにカスタムランブックを作成するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[ドキュメント] を選択します。
3. [Create automation (オートメーションを作成)] を選択します。
4. [Name (名前)] に、ランブック **LaunchInstanceAndCheckStatus** のわかりやすい名前を入力します。
5. (オプション) [Document description (ドキュメントの説明)] で、Markdown を使用して、デフォルトのテキストをこのランブックの説明に置き換えます。以下はその例です。

```
##Title: LaunchInstanceAndCheckState
    -----
```

```
    **Purpose**: This runbook first launches an EC2 instance using the AMI
 ID provided in the parameter ```imageId```. The second step of this runbook
 continuously checks the instance status check value for the launched instance
 until the status ```ok``` is returned.

    ##Parameters:
    -----
    Name | Type | Description | Default Value
    ------------- | ------------- | ------------- | -------------
    assumeRole | String | (Optional) The ARN of the role that allows Automation to
 perform the actions on your behalf. | -
    imageId  | String | (Optional) The AMI ID to use for launching the instance.
 The default value uses the latest Amazon Linux AMI ID available. | {{ ssm:/aws/
service/ami-amazon-linux-latest/amzn-ami-hvm-x86_64-gp2 }}
```

6. [Assume role (継承ロール)] に、オートメーションのオートメーション (継承ロール) の IAM サービスロールの ARN を **arn:aws:iam::111122223333:role/AutomationServiceRole** の形式で入力します。AWS アカウント IDを 111122223333 に置き換えます。

   指定したロールは、オートメーションの開始に必要なアクセス許可を提供するために使用されます。

   > **Important**
   >
   > aws:executeScript アクションを使用する Amazon が所有していないランブックの場合、ロールを指定する必要があります。詳細については、ランブックを使用するためのアクセス許可 を参照してください。

7. [Input parameters (入力パラメータ)] を展開し、次の操作を行います。

   1. [Parameter name (パラメータ名)] に「**imageId**」と入力します。
   2. [Type (タイプ)] で、**String** を選択します。
   3. [Required (必須)] で、No を選択します。
   4. [Default value (デフォルト値)] に、次のように入力します。

      ```
      {{ ssm:/aws/service/ami-amazon-linux-latest/amzn-ami-hvm-x86_64-gp2 }}
      ```

> **Note**
>
> この値で、最新の Amazon Linux 1 Amazon Machine Image (AMI) ID を使用して Amazon EC2 インスタンスは起動します。別の AMI を使用する場合は、値を AMI ID に置き換えます。

5. [Description (説明)] に、次のように入力します。

```
(Optional) The AMI ID to use for launching the instance. The default value uses
 the latest released Amazon Linux AMI ID.
```

8. [Add a parameter (パラメータの追加)] を選択して 2 番目のパラメータ、**tagValue** を作成し、次のように入力します。

   1. [Parameter name (パラメータ名)] に「**tagValue**」と入力します。
   2. [Type (タイプ)] で、**String** を選択します。
   3. [Required (必須)] で、No を選択します。
   4. [Default value (デフォルト値)] に「**LaunchedBySsmAutomation**」と入力します。これにより、タグのキーペア値 `Name:LaunchedBySsmAutomation` がインスタンスに追加されます。
   5. [Description (説明)] に、次のように入力します。

```
(Optional) The tag value to add to the instance. The default value is
 LaunchedBySsmAutomation.
```

9. [Add a parameter (パラメータの追加)] を選択して 3 番目のパラメータ、**instanceType** を作成し、次の情報を入力します。

   1. [Parameter name (パラメータ名)] に「**instanceType**」と入力します。
   2. [Type (タイプ)] で、**String** を選択します。
   3. [Required (必須)] で、No を選択します。
   4. [Default value (デフォルト値)] に「**t2.micro**」と入力します。
   5. [Parameter description (パラメータの説明)] に、次のように入力します。

```
(Optional) The instance type to use for the instance. The default value is
 t2.micro.
```

10. [Target type (ターゲットタイプ)] を展開し、**"/"** を選択します。
11. (オプション) [Document tags (ドキュメントタグ)] を展開して、ランブックにリソースタグを適用します。[Tag key (タグキー)] に **Purpose** と入力し、[Tag value (タグ値)] に「**LaunchInstanceAndCheckState**」と入力します。
12. [Step 1 (ステップ 1)] セクションで、次のステップを実行します。

    1. [Step name (ステップ名)] に、オートメーションの最初のステップを表すわかりやすいステップ名を入力します: **LaunchEc2Instance**。
    2. [Action type (アクションタイプ)] で、[Run a script (スクリプトを実行)] (**aws:executeScript**) を選択します。
    3. [Description (説明)] に、次のようなオートメーションのステップの説明を入力します。

    ```
    **About This Step**

        This step first launches an EC2 instance using the ```aws:executeScript```
     action and the provided script.
    ```

    4. [入力] を展開します。
    5. [Runtime (ランタイム)] で、指定されたスクリプトの実行に使用するランタイム言語を選択します。
    6. [Handler (ハンドラ)] に「**launch_instance**」と入力します。これは、次のスクリプトで宣言された関数名です。

    > **Note**
    >
    > PowerShell では必須ではありません。

    7. [Script (スクリプト)] で、デフォルトのコンテンツを次のように置き換えます。スクリプトは、対応するランタイム値と一致するようにしてください。

    Python

    ```
    def launch_instance(events, context):
          import boto3
          ec2 = boto3.client('ec2')

          image_id = events['image_id']
          tag_value = events['tag_value']
          instance_type = events['instance_type']
    ```

```
    tag_config = {'ResourceType': 'instance', 'Tags': [{'Key':'Name',
 'Value':tag_value}]}

    res = ec2.run_instances(ImageId=image_id, InstanceType=instance_type,
 MaxCount=1, MinCount=1, TagSpecifications=[tag_config])

    instance_id = res['Instances'][0]['InstanceId']

    print('[INFO] 1 EC2 instance is successfully launched', instance_id)

    return { 'InstanceId' : instance_id }
```

PowerShell

```
Install-Module AWS.Tools.EC2 -Force
    Import-Module AWS.Tools.EC2

    $payload = $env:InputPayload | ConvertFrom-Json

    $imageid = $payload.image_id

    $tagvalue = $payload.tag_value

    $instanceType = $payload.instance_type

    $type = New-Object Amazon.EC2.InstanceType -ArgumentList $instanceType

    $resource = New-Object Amazon.EC2.ResourceType -ArgumentList 'instance'

    $tag = @{Key='Name';Value=$tagValue}

    $tagSpecs = New-Object Amazon.EC2.Model.TagSpecification

    $tagSpecs.ResourceType = $resource

    $tagSpecs.Tags.Add($tag)

    $res = New-EC2Instance -ImageId $imageId -MinCount 1 -MaxCount 1 -
InstanceType $type -TagSpecification $tagSpecs

    return @{'InstanceId'=$res.Instances.InstanceId}
```

8. [Additional inputs (追加入力)] を展開します。
9. [Input name (入力名)] で、[InputPayload] を選択します。[Input value (入力値)] に、次の YAML データを入力します。

```
image_id: "{{ imageId }}"
    tag_value: "{{ tagValue }}"
    instance_type: "{{ instanceType }}"
```

13. [Outputs (出力)] を展開し、次の操作を行います。
    - [Name (名前)] に **payload** と入力します。
    - [Selector (セレクタ)] に **$.Payload** と入力します。
    - [Type (タイプ)] で、StringMap を選択します。
14. [Add step (ステップを追加)] を選択して、ランブックに 2 番目のステップを追加します。2 番目のステップは、ステップ 1 で起動されたインスタンスのステータスをクエリし、返されるステータスが ok になるまで待機します。
15. [Step 2 (ステップ 2)] セクションで、次の操作を行います。
    1. [Step name (ステップ名)] に、オートメーションの 2 番目のステップを表すわかりやすい名前を入力します: **WaitForInstanceStatusOk**。
    2. [Action type (アクションタイプ)] で、[Run a script (スクリプトを実行)] (**aws:executeScript**) を選択します。
    3. [Description (説明)] に、次のようなオートメーションのステップの説明を入力します。

```
**About This Step**

   The script continuously polls the instance status check value for the
 instance launched in Step 1 until the ```ok``` status is returned.
```

    4. [Runtime (ランタイム)] では、提供されたスクリプトの実行に使用されるランタイム言語を選択します。
    5. [Handler (ハンドラ)] に「**poll_instance**」と入力します。これは、次のスクリプトで宣言された関数名です。

> **Note**
>
> PowerShell では必須ではありません。

6. [Script (スクリプト)] で、デフォルトのコンテンツを次のように置き換えます。スクリプトは、対応するランタイム値と一致するようにしてください。

   Python

```
def poll_instance(events, context):
      import boto3
      import time

      ec2 = boto3.client('ec2')

      instance_id = events['InstanceId']

      print('[INFO] Waiting for instance status check to report ok',
 instance_id)

      instance_status = "null"

      while True:
        res = ec2.describe_instance_status(InstanceIds=[instance_id])

        if len(res['InstanceStatuses']) == 0:
          print("Instance status information is not available yet")
          time.sleep(5)
          continue

        instance_status = res['InstanceStatuses'][0]['InstanceStatus']
['Status']

        print('[INFO] Polling to get status of the instance', instance_status)

        if instance_status == 'ok':
          break

        time.sleep(10)

      return {'Status': instance_status, 'InstanceId': instance_id}
```

   PowerShell

```
    Install-Module AWS.Tools.EC2 -Force
```

```
    $inputPayload = $env:InputPayload | ConvertFrom-Json

    $instanceId = $inputPayload.payload.InstanceId

    $status = Get-EC2InstanceStatus -InstanceId $instanceId

    while ($status.Status.Status -ne 'ok'){
       Write-Host 'Polling get status of the instance', $instanceId

       Start-Sleep -Seconds 5

       $status = Get-EC2InstanceStatus -InstanceId $instanceId
    }

    return @{Status = $status.Status.Status; InstanceId = $instanceId}
```

7. [Additional inputs (追加入力)] を展開します。
8. [Input name (入力名)] で、[InputPayload] を選択します。[Input value (入力値)] に、次のように入力します。

```
{{ LaunchEc2Instance.payload }}
```

16. [Create automation (オートメーションを作成)] を選択してランブックを保存します。

ランブックでのスクリプトの使用

オートメーションランブックは、オートメーションの一部としてスクリプトの実行をサポートします。Automation は AWS Systems Manager のツールです。ランブックを使用すると、スクリプトを実行するための独立したコンピューティング環境を作成せずに、AWS でスクリプトを直接実行できます。ランブックでは、承認などの他のオートメーションステップタイプとともにスクリプトステップを実行できるため、重要な状況やあいまいな状況に手動で介入できます。ランブックの `aws:executeScript` アクションからの出力を Amazon CloudWatch Logs に送信できます。詳細については、「CloudWatch Logs を使用した自動アクション出力の口グ記録」を参照してください。

ランブックを使用するためのアクセス許可

ランブックを使用するには、Systems Manager が AWS Identity and Access Management (IAM) ロールのアクセス許可を使用する必要があります。どのロールのアクセス許可を使用するかを判断するためにオートメーションが使用する方法は、いくつかの要因と、ステップで `aws:executeScript` アクションを使用するかどうかによって異なります。

aws:executeScript を使用しないランブックの場合、オートメーションは、次の 2 つのアクセス許可ソースのいずれかを使用します。

- ランブックで指定されているか、パラメータとして渡された IAM サービスロールまたは継承ロールのアクセス許可。
- IAM サービスロールが指定されていない場合は、オートメーションを開始したユーザーのアクセス許可。

ただし、ランブックのステップに aws:executeScript アクションが含まれている場合、アクションに指定されている Python スクリプトまたは PowerShell スクリプトが AWS API オペレーションを呼び出す場合は、IAM サービスロール (継承ロール) が常に必要です。オートメーションは、このロールを次の順序でチェックします。

- ランブックで指定されているか、パラメータとして渡された IAM サービスロールまたは継承ロールのアクセス許可。
- ロールが見つからない場合、オートメーションは aws:executeScript に指定された Python スクリプトまたは PowerShell スクリプトをアクセス許可なしで実行しようとします。スクリプトが AWS API オペレーション (Amazon EC2 CreateImage オペレーションなど) を呼び出している場合、または AWS リソース (EC2 インスタンスなど) に対して動作しようとしている場合、スクリプトを含むステップは失敗し、Systems Manager は失敗をレポートするエラーメッセージを返します。

スクリプトをランブックに追加する

スクリプトインラインをランブック内のステップの一部として含めることで、スクリプトをランブックに追加できます。スクリプトをランブックにアタッチするには、ローカルマシンからスクリプトをアップロードするか、スクリプトが配置されている Amazon Simple Storage Service (Amazon S3) バケットを指定します。スクリプトを実行するステップが完了すると、スクリプトの出力が JSON オブジェクトとして利用可能になり、ランブックの後続のステップの入力として使用できます。aws:executeScript アクションと、スクリプトのアタッチメントの使用方法の詳細については、「aws:executeScript – スクリプトを実行する」を参照してください。

ランブックのスクリプト制約

ランブックでは、5 つの添付ファイルの制限が適用されます。スクリプトは、Python スクリプト (.py)、PowerShell Core スクリプト (.ps1) の形式で、または .zip ファイル内のコンテンツとして添付できます。

ランブックでの条件文の使用

デフォルトでは、ランブックの mainSteps セクションで定義したステップは順番に実行されます。1 つのアクションが完了した後、mainSteps セクションで指定された次のアクションが開始されます。さらに、アクションが失敗した場合は、(デフォルトでは) オートメーション全体の実行に失敗します。このセクションで説明されている aws:branch オートメーションアクションおよびランブックオプションを使用すると、条件付き分岐を実行するオートメーションを作成できます。つまり、異なる選択肢を評価した後に異なるステップにジャンプするオートメーションを作成したり、ステップが完了したときに変更に動的に応答するオートメーションを作成することができます。動的オートメーションの作成に使用できるオプションのリストは次のとおりです。

- **aws:branch**: この自動化アクションを使用すると、1 つのステップで複数の選択肢を評価し、その評価結果に基づいてランブックの異なるステップにジャンプする動的オートメーションを作成できます。
- **nextStep**: このオプションは、ステップを正常に完了した後に、次に処理するオートメーションのステップを指定します。
- **isEnd**: このオプションでは、特定のステップの最後にオートメーションを停止します。このオプションのデフォルト値は false です。
- **isCritical**: このオプションはオートメーションの正常な完了のために、ステップを critical として指定します。この指定のステップが失敗した場合、オートメーションはオートメーションの失敗の最終的なステータスを Failed としてレポートします。このオプションのデフォルト値は true です。
- **onFailure**: このオプションは失敗時にオートメーションを中止するか、続行するか、または別のステップに移行するかを示します。このオプションのデフォルト値は中止です。

次のセクションでは、aws:branch オートメーションアクションについて説明します。nextStep、isEnd、isCritical、onFailure オプションの詳細については、「aws:branch ランブックの例」を参照してください。

aws:branch アクションの使用

aws:branch アクションは、オートメーションのための最も動的な条件分岐オプションを提供します。前述のとおり、このアクションによって、オートメーションで複数の条件を 1 つのステップで評価し、その評価の結果に基づいて新しいステップにジャンプすることができます。aws:branch アクションは、プログラミングで IF-ELIF-ELSE ステートメントのように機能します。

以下に、aws:branch ステップの YAML の例を示します。

```
- name: ChooseOSforCommands
  action: aws:branch
  inputs:
    Choices:
    - NextStep: runPowerShellCommand
      Variable: "{{GetInstance.platform}}"
      StringEquals: Windows
    - NextStep: runShellCommand
      Variable: "{{GetInstance.platform}}"
      StringEquals: Linux
    Default:
      PostProcessing
```

ステップの aws:branch アクションを指定する場合、オートメーションが評価する必要のある Choices を指定します。オートメーションは、ランブックの Choices セクションで指定したパラメータの値に基づいて、Parameters を評価できます。オートメーションは、前の手順の出力に基づいて Choices を評価することもできます。

自動化は、ブール式を使用して各選択肢を評価します。最初の選択肢が true であると判断された場合、オートメーションはその選択肢で指定されたステップにジャンプします。最初の選択肢が false であると判断された場合、オートメーションは次の選択肢を評価します。ステップに 3 つ以上の Choices が含まれている場合、オートメーションは、true である選択肢を評価するまで、各選択肢を順番に評価します。次に、オートメーションは、true の選択のために指定されたステップにジャンプします。

Choices である true がない場合、オートメーションはステップに Default 値が含まれているかどうかを確認します。Default 値は、true である選択肢がない場合にオートメーションがジャンプするステップを定義します。ステップに Default 値が指定されていない場合、オートメーションはランブックの次のステップを処理します。

以下は YAML の [chooseOSfromParameter] という名前の aws:branch ステップです。ステップには、2 つの Choices が含まれています。 (NextStep: runWindowsCommand) および (NextStep: runLinuxCommand)。オートメーションは、これらの Choices を評価して、適切なオペレーティングシステムで実行するコマンドを決定します。各選択肢の Variable は、{{OSName}} を使用します。これは、ランブック作成者がランブックの Parameters セクションで定義したパラメータです。

```
mainSteps:
- name: chooseOSfromParameter
```

```
  action: aws:branch
  inputs:
    Choices:
    - NextStep: runWindowsCommand
      Variable: "{{OSName}}"
      StringEquals: Windows
    - NextStep: runLinuxCommand
      Variable: "{{OSName}}"
      StringEquals: Linux
```

以下は YAML の [chooseOSfromOutput] という名前の aws:branch ステップです。ステップには、2 つの Choices が含まれています。 (NextStep: runPowerShellCommand) および (NextStep: runShellCommand)。オートメーションは、これらの Choices を評価して、適切なオペレーティングシステムで実行するコマンドを決定します。各選択肢の Variable は、{{GetInstance.platform}} を使用します。これは、ランブックの前のステップからの出力です。この例では Default というオプションも含まれています。オートメーションが両方の Choices を評価し 、どちらの選択肢も true である場合、オートメーションは PostProcessing というステップにジャンプします。

```
mainSteps:
- name: chooseOSfromOutput
  action: aws:branch
  inputs:
    Choices:
    - NextStep: runPowerShellCommand
      Variable: "{{GetInstance.platform}}"
      StringEquals: Windows
    - NextStep: runShellCommand
      Variable: "{{GetInstance.platform}}"
      StringEquals: Linux
    Default:
      PostProcessing
```

ランブック **aws:branch** でのステップの作成

ランブック aws:branch でステップを作成するときは、オートメーションが次にジャンプするステップを決定するために評価するChoices を定義します。前述のように、Choices はブール式を使用して評価されます。各選択肢は、次のオプションを定義する必要があります。

- NextStep : 指定された選択肢が true である場合に処理するランブックの次のステップ。

- Variable: ランブックの `Parameters` セクションで定義されているパラメータの名前を指定するか、`Variables` セクションで定義されている変数の名前を指定するか、前のステップからの出力オブジェクトを指定します。

  次の形式を使用して変数の値を指定します。

  `Variable: "{{variable name}}"`

  次の形式を使用してパラメータの値を指定します。

  `Variable: "{{parameter name}}"`

  次の形式を使用して出力オブジェクト変数を指定します。

  `Variable: "{{previousStepName.outputName}}"`

  > **Note**
  >
  > 出力変数の作成については、次のセクション「出力変数の作成について」でさらに詳しく説明します。

- Operation: `StringEquals: Linux` などの選択肢を評価するために使用される基準。`aws:branch` アクションは、次の操作をサポートします。

  文字列演算子

  - StringEquals
  - EqualsIgnoreCase
  - StartsWith
  - EndsWith
  - Contains

  数値演算子

  - NumericEquals
  - NumericGreater
  - NumericLesser
  - NumericGreaterOrEquals
  - NumericLesser

- NumericLesserOrEquals

ブール演算子

- BooleanEquals

> **Important**
>
> ランブックを作成すると、システムはランブック内の各オペレーションを検証します。オペレーションがサポートされていない場合は、ランブックの作成時にエラーが返されます。

- Default: Choices である true がない場合にオートメーションがジャンプするフォールバックステップを指定します。

> **Note**
>
> Default 値を指定しない場合は、isEnd オプションを指定できます。Choices である true がない場合、および Default 値が指定されていない場合は、オートメーションはステップの最後で停止します。

次のテンプレートを使用して、ランブックの aws:branch ステップを構築します。各##########をユーザー自身の情報に置き換えます。

YAML

```
mainSteps:
- name: step name
  action: aws:branch
  inputs:
    Choices:
    - NextStep: step to jump to if evaluation for this choice is true
      Variable: "{{parameter name or output from previous step}}"
      Operation type: Operation value
    - NextStep: step to jump to if evaluation for this choice is true
      Variable: "{{parameter name or output from previous step}}"
      Operation type: Operation value
    Default:
      step to jump to if all choices are false
```

JSON

```
{
   "mainSteps":[
      {
         "name":"a name for the step",
         "action":"aws:branch",
         "inputs":{
            "Choices":[
               {
                  "NextStep":"step to jump to if evaluation for this choice is
 true",
                  "Variable":"{{parameter name or output from previous step}}",
                  "Operation type":"Operation value"
               },
               {
                  "NextStep":"step to jump to if evaluation for this choice is
 true",
                  "Variable":"{{parameter name or output from previous step}}",
                  "Operation type":"Operation value"
               }
            ],
            "Default":"step to jump to if all choices are false"
         }
      }
   ]
}
```

出力変数の作成について

前のステップからの出力を参照する aws:branch 選択肢を作成するには、前のステップの名前と出力フィールドの名前を特定する必要があります。次に、以下の形式を使用して、ステップ名とフィールド名を結合します。

Variable: "{{*previousStepName.outputName*}}"

例えば、次の例の最初のステップは GetInstance という名前です。そして、outputs の下に、platform というフィールドがあります。2 番目のステップ (ChooseOSforCommands) では、作成者はプラットフォームフィールドからの出力を変数として参照しようとしています。変数を作成するには、単純にステップ名 (GetInstance) と出力フィールド名 (platform) を組み合わせて Variable: "{{*GetInstance.platform*}}" を作成します。

```
mainSteps:
- Name: GetInstance
  action: aws:executeAwsApi
  inputs:
    Service: ssm
    Api: DescribeInstanceInformation
    Filters:
    - Key: InstanceIds
      Values: ["{{ InstanceId }}"]
  outputs:
  - Name: myInstance
    Selector: "$.InstanceInformationList[0].InstanceId"
    Type: String
  - Name: platform
    Selector: "$.InstanceInformationList[0].PlatformType"
    Type: String
- name: ChooseOSforCommands
  action: aws:branch
  inputs:
    Choices:
    - NextStep: runPowerShellCommand
      Variable: "{{GetInstance.platform}}"
      StringEquals: Windows
    - NextStep: runShellCommand
      Variable: "{{GetInstance.platform}}"
      StringEquals: Linux
    Default:
      Sleep
```

前のステップと出力から *"Variable": "{{ describeInstance.Platform }}"* を作成する方法例を示します。

```
- name: describeInstance
  action: aws:executeAwsApi
  onFailure: Abort
  inputs:
    Service: ec2
    Api: DescribeInstances
    InstanceIds:
    - "{{ InstanceId }}"
  outputs:
  - Name: Platform
    Selector: "$.Reservations[0].Instances[0].Platform"
```

```
    Type: String
  nextStep: branchOnInstancePlatform
- name: branchOnInstancePlatform
  action: aws:branch
  inputs:
    Choices:
    - NextStep: runEC2RescueForWindows
      Variable: "{{ describeInstance.Platform }}"
      StringEquals: windows
    Default: runEC2RescueForLinux
```

aws:branch ランブックの例

以下に、aws:branch を使用するランブックの例をいくつか挙げます。

例 1: 出力変数で **aws:branch** を使用し、オペレーティングシステムの種類に基づいてコマンドを実行する

この例 (GetInstance) の最初の手順では、ランブック作成者は aws:executeAwsApi アクションを使用して、ssm DescribeInstanceInformation API オペレーションを呼び出します。作成者はこのアクションを使用して、インスタンスが使用しているオペレーティングシステムのタイプを判別します。aws:executeAwsApi アクションはインスタンス ID とプラットフォームタイプを出力します。

2 番目のステップ (ChooseOSforCommands) では、2 つの aws:branch (Choices) と (NextStep: runPowerShellCommand) を使用して NextStep: runShellCommand アクションを使用します。自動化は、前の手順 (Variable: "{{GetInstance.platform}}") の出力を使用して、インスタンスのオペレーティングシステムを評価します。オートメーションは、指定されたオペレーティングシステムのステップにジャンプします。

```
---
schemaVersion: '0.3'
assumeRole: "{{AutomationAssumeRole}}"
parameters:
  AutomationAssumeRole:
    default: ""
    type: String
mainSteps:
- name: GetInstance
  action: aws:executeAwsApi
  inputs:
    Service: ssm
```

```
    Api: DescribeInstanceInformation
  outputs:
  - Name: myInstance
    Selector: "$.InstanceInformationList[0].InstanceId"
    Type: String
  - Name: platform
    Selector: "$.InstanceInformationList[0].PlatformType"
    Type: String
- name: ChooseOSforCommands
  action: aws:branch
  inputs:
    Choices:
    - NextStep: runPowerShellCommand
      Variable: "{{GetInstance.platform}}"
      StringEquals: Windows
    - NextStep: runShellCommand
      Variable: "{{GetInstance.platform}}"
      StringEquals: Linux
    Default:
      Sleep
- name: runShellCommand
  action: aws:runCommand
  inputs:
    DocumentName: AWS-RunShellScript
    InstanceIds:
    - "{{GetInstance.myInstance}}"
    Parameters:
      commands:
      - ls
  isEnd: true
- name: runPowerShellCommand
  action: aws:runCommand
  inputs:
    DocumentName: AWS-RunPowerShellScript
    InstanceIds:
    - "{{GetInstance.myInstance}}"
    Parameters:
      commands:
      - ls
  isEnd: true
- name: Sleep
  action: aws:sleep
  inputs:
```

```
    Duration: PT3S
```

例 2: パラメータ変数で **aws:branch** を使用し、オペレーティングシステムの種類に基づいてコマンドを実行する

ランブック作成者は、parameters セクションのランブックの先頭にいくつかのパラメータオプションを定義します。1 つのパラメータの名前は OperatingSystemName です。最初のステップ (ChooseOS) では、2 つの aws:branch (Choices) と (NextStep: runWindowsCommand) を使用して NextStep: runLinuxCommand アクションを使用します。これらの Choices の変数は、パラメータセクション (Variable: "{{OperatingSystemName}}") で指定されたパラメータオプションを参照します。ユーザーがこのランブックを実行すると、実行時に OperatingSystemName の値を指定します 。オートメーションでは、Choices の評価時にランタイムパラメータが使用されます。オートメーションは、OperatingSystemName に指定されたランタイムパラメータに基づいて、指定されたオペレーティングシステムのステップにジャンプします。

```
---
schemaVersion: '0.3'
assumeRole: "{{AutomationAssumeRole}}"
parameters:
  AutomationAssumeRole:
    default: ""
    type: String
  OperatingSystemName:
    type: String
  LinuxInstanceId:
    type: String
  WindowsInstanceId:
    type: String
mainSteps:
- name: ChooseOS
  action: aws:branch
  inputs:
    Choices:
    - NextStep: runWindowsCommand
      Variable: "{{OperatingSystemName}}"
      StringEquals: windows
    - NextStep: runLinuxCommand
      Variable: "{{OperatingSystemName}}"
      StringEquals: linux
    Default:
      Sleep
- name: runLinuxCommand
```

```
  action: aws:runCommand
  inputs:
    DocumentName: "AWS-RunShellScript"
    InstanceIds:
    - "{{LinuxInstanceId}}"
    Parameters:
      commands:
      - ls
  isEnd: true
- name: runWindowsCommand
  action: aws:runCommand
  inputs:
    DocumentName: "AWS-RunPowerShellScript"
    InstanceIds:
    - "{{WindowsInstanceId}}"
    Parameters:
      commands:
      - date
  isEnd: true
- name: Sleep
  action: aws:sleep
  inputs:
    Duration: PT3S
```

演算子を使用した複雑な分岐オートメーションの作成

And ステップで Or、Not、および aws:branch 演算子を使用して、複雑な分岐オートメーションを作成できます。

"And" 演算子

選択肢の複数の変数を And にする場合は、true 演算子を使用します。次の例では、最初の選択肢に対して、インスタンスが running の状態で、Windows オペレーティングシステムを使用しているかどうかを評価します。これらの変数の両方が true と評価された場合、オートメーションは runPowerShellCommand ステップにジャンプします。1 つ以上の変数が false の場合、オートメーションは 2 番目の選択肢の変数を評価します。

```
mainSteps:
- name: switch2
  action: aws:branch
  inputs:
    Choices:
    - And:
```

```
      - Variable: "{{GetInstance.pingStatus}}"
        StringEquals: running
      - Variable: "{{GetInstance.platform}}"
        StringEquals: Windows
      NextStep: runPowerShellCommand

    - And:
      - Variable: "{{GetInstance.pingStatus}}"
        StringEquals: running
      - Variable: "{{GetInstance.platform}}"
        StringEquals: Linux
      NextStep: runShellCommand
    Default:
      sleep3
```

"OR" 演算子

選択肢の複数の変数のいずれかを true にする場合は、Or 演算子を使用します。次の例では、最初の選択は、パラメータ文字列が Windows であるかどうか、AWS Lambda ステップからの出力が true かどうかを評価します。これらの変数のどちらかが true であると判断された場合、オートメーションは RunPowerShellCommand ステップにジャンプします。両方の変数が false の場合、オートメーションは 2 番目の選択肢の変数を評価します。

```
- Or:
  - Variable: "{{parameter1}}"
    StringEquals: Windows
  - Variable: "{{BooleanParam1}}"
    BooleanEquals: true
  NextStep: RunPowershellCommand
- Or:
  - Variable: "{{parameter2}}"
    StringEquals: Linux
  - Variable: "{{BooleanParam2}}"
    BooleanEquals: true
  NextStep: RunShellScript
```

"Not" 演算子

変数が true でない場合に定義されたステップにジャンプする場合は、Not 演算子を使用します。次の例では、最初の選択肢は、パラメータ文字列が Not Linux かどうかを評価します。変数が Linux ではないと判断された場合、オートメーションは sleep2 ステップにジャンプします。最初の選択肢が Linux であると判断された場合、オートメーションは次の選択肢を評価します。

```
mainSteps:
- name: switch
  action: aws:branch
  inputs:
    Choices:
    - NextStep: sleep2
      Not:
        Variable: "{{testParam}}"
        StringEquals: Linux
    - NextStep: sleep1
      Variable: "{{testParam}}"
      StringEquals: Windows
    Default:
      sleep3
```

条件オプションの使用例

このセクションでは、ランブックで動的オプションを使用するさまざまな例について説明します。このセクションのそれぞれの例では、次のランブックを拡張します。このランブックには 2 つのアクションがあります。最初のアクションは InstallMsiPackage という名前です。aws:runCommand アクションを使用して、Windows Server インスタンスにアプリケーションをインストールします。2 番目のアクションは、TestInstall という名前です。このアクションは、aws:invokeLambdaFunction アクションを使用し、アプリケーションが正常にインストールされているかどうか、インストールされているアプリケーションのテストを実行します。ステップ 1 で onFailure: Abort を指定します。つまり、アプリケーションがインストールされなかった場合は、オートメーションの実行はステップ 2 より前で停止します。

例 1:2 つのリニアアクションがあるランブック

```
---
schemaVersion: '0.3'
description: Install MSI package and run validation.
assumeRole: "{{automationAssumeRole}}"
parameters:
  automationAssumeRole:
    type: String
    description: "(Required) Assume role."
  packageName:
    type: String
    description: "(Required) MSI package to be installed."
  instanceIds:
```

```
    type: String
    description: "(Required) Comma separated list of instances."
mainSteps:
- name: InstallMsiPackage
  action: aws:runCommand
  maxAttempts: 2
  onFailure: Abort
  inputs:
    InstanceIds:
    - "{{instanceIds}}"
    DocumentName: AWS-RunPowerShellScript
    Parameters:
      commands:
      - msiexec /i {{packageName}}
- name: TestInstall
  action: aws:invokeLambdaFunction
  maxAttempts: 1
  timeoutSeconds: 500
  inputs:
    FunctionName: TestLambdaFunction
...
```

onFailure オプションを使用し、別のステップにジャンプする動的オートメーションを作成する

次の例では、onFailure: step:*step name*、nextStep、および isEnd オプションを使用して、動的オートメーションを作成します。この例では、InstallMsiPackage アクションが失敗すると、自動化は PostFailure (onFailure: step:PostFailure) というアクションにジャンプし、インストールに失敗したイベントの何らかのアクションを実行する AWS Lambda 関数を実行します。インストールが成功した場合は、自動化は TestInstall アクション (nextStep: TestInstall) にジャンプします。TestInstall ステップと PostFailure ステップの両方で isEnd オプション (isEnd: true) を使用すると、これらのステップのいずれかが完了したときにオートメーションが終了します。

> **Note**
>
> isEnd セクションの最後のステップでの、mainSteps オプションの使用はオプションです。最後のステップが他のステップにジャンプしない場合、最後のステップのアクションの実行後にオートメーションは停止します。

例 2: 別のステップにジャンプする動的オートメーション

```
mainSteps
- name: InstallMsiPackage
  action: aws:runCommand
  onFailure: step:PostFailure
  maxAttempts: 2
  inputs:
    InstanceIds:
    - "{{instanceIds}}"
    DocumentName: AWS-RunPowerShellScript
    Parameters:
      commands:
      - msiexec /i {{packageName}}
  nextStep: TestInstall
- name: TestInstall
  action: aws:invokeLambdaFunction
  maxAttempts: 1
  timeoutSeconds: 500
  inputs:
    FunctionName: TestLambdaFunction
  isEnd: true
- name: PostFailure
  action: aws:invokeLambdaFunction
  maxAttempts: 1
  timeoutSeconds: 500
  inputs:
    FunctionName: PostFailureRecoveryLambdaFunction
  isEnd: true
...
```

> **Note**
>
> ランブックを処理する前に、システムはランブックが無限ループを作成していないことを確認します。無限ループが検出された場合、自動化はエラー、およびどのステップがループを作成しているかを示すサークルトレースを返します。

重要な手順を定義する動的オートメーションの作成

オートメーション全体の成功にとって非常に重要なステップを指定できます。重要なステップが失敗した場合、1 つ以上のステップが正常に実行されたとしても、オートメーションは実行のステータスを `Failed` としてレポートします。次の例では、InstallMsiPackage ステップが失敗した

(onFailure: step:VerifyDependencies) 場合に、ユーザーは VerifyDependencies ステップを識別します。ユーザーは、InstallMsiPackage ステップが critical ではないことを指定します (isCritical: false)。この例では、アプリケーションのインストールに失敗した場合、自動化は VerifyDependencies ステップを処理して、アプリケーションのインストールが失敗する原因となる、1 つ以上の依存関係が欠落していないかどうかを判断します。

例 3: オートメーションを定義する重要なステップ

```
---
name: InstallMsiPackage
action: aws:runCommand
onFailure: step:VerifyDependencies
isCritical: false
maxAttempts: 2
inputs:
  InstanceIds:
  - "{{instanceIds}}"
  DocumentName: AWS-RunPowerShellScript
  Parameters:
    commands:
    - msiexec /i {{packageName}}
nextStep: TestPackage
...
```

アクション出力の入力としての使用

いくつかのオートメーションアクションは、定義済みの出力を返します。{{*stepName*.*outputName*}} 形式を使用して、これらの出力をランブックの後のステップに入力として渡すことができます。ランブックでは、さまざまなオートメーションアクションについて、その出力を定義することができます。これにより、スクリプトを実行することや、他の AWS のサービス のために API オペレーションを呼び出すことができ、その出力値は、後のアクションで入力として再利用できます。ランブック内のパラメータのデータ型は静的です。つまり、パラメータのデータ型は定義後に変更することはできません。ステップ出力を定義するには、以下のフィールドを指定します。

- 名前: (必須) 後のステップで出力値を参照するために使用する出力名。
- セレクター: (必須) 出力値を決定するために使用される JSONPath 式。
- タイプ: (オプション) セレクターフィールドによって返されます。有効なタイプ値は String、Integer、Boolean、StringList、StringMap、MapList です。デフォルト値は String です。

出力の値が指定したデータ型と一致しない場合、オートメーションはデータ型を変換しようとします。例えば、返される値が Integer で、指定された Type が String の場合、最終的な出力値は String 値です。次のネットワーク接続タイプがサポートされています。

- String 値は StringList、Integer、および Boolean に変換できます。
- Integer 値は String および StringList に変換できます。
- Boolean 値は String および StringList に変換できます。
- 1 つの要素を含む StringList、IntegerList、または BooleanList 値は、String、Integer または Boolean に変換できます。

自動化アクションでパラメータを使用する場合、アクションの入力内でデータ型を動的に変更することはできません。

アクションの出力を定義し、その出力値を後のアクションで入力として参照する方法を示した、ランブックの例を次に示します。このランブックでは、以下を処理します。

- aws:executeAwsApi アクションを使用して Amazon EC2 DescribeImages API オペレーションを呼び出し、特定の Windows Server 2016 AMI の名前を取得します。イメージ ID を ImageId として出力します。
- aws:executeAwsApi アクションを使用して、Amazon EC2 RunInstances API オペレーションを呼び出し、前の手順の ImageId を使用するインスタンスを 1 つ起動します。インスタンス ID を InstanceId として出力します。
- aws:waitForAwsResourceProperty アクションを使用して Amazon EC2 DescribeInstanceStatus API オペレーションをポーリングし、インスタンスが running 状態になるまで待機します。アクションは 60 秒でタイムアウトします。60 秒間のポーリング後にインスタンス状態が running にならなかった場合、このステップはタイムアウトします。
- aws:assertAwsResourceProperty アクションを使用して Amazon EC2 DescribeInstanceStatus API オペレーションを呼び出し、インスタンスが running 状態であることをアサートします。インスタンス状態が running ではない場合、このステップは失敗します。

```
---
description: Sample runbook using AWS API operations
schemaVersion: '0.3'
assumeRole: "{{ AutomationAssumeRole }}"
parameters:
```

```
  AutomationAssumeRole:
    type: String
    description: "(Optional) The ARN of the role that allows Automation to perform the
 actions on your behalf."
    default: ''
  ImageName:
    type: String
    description: "(Optional) Image Name to launch EC2 instance with."
    default: "Windows_Server-2022-English-Full-Base*"
mainSteps:
- name: getImageId
  action: aws:executeAwsApi
  inputs:
    Service: ec2
    Api: DescribeImages
    Filters:
    - Name: "name"
      Values:
      - "{{ ImageName }}"
  outputs:
  - Name: ImageId
    Selector: "$.Images[0].ImageId"
    Type: "String"
- name: launchOneInstance
  action: aws:executeAwsApi
  inputs:
    Service: ec2
    Api: RunInstances
    ImageId: "{{ getImageId.ImageId }}"
    MaxCount: 1
    MinCount: 1
  outputs:
  - Name: InstanceId
    Selector: "$.Instances[0].InstanceId"
    Type: "String"
- name: waitUntilInstanceStateRunning
  action: aws:waitForAwsResourceProperty
  timeoutSeconds: 60
  inputs:
    Service: ec2
    Api: DescribeInstanceStatus
    InstanceIds:
    - "{{ launchOneInstance.InstanceId }}"
    PropertySelector: "$.InstanceStatuses[0].InstanceState.Name"
```

```
    DesiredValues:
    - running
- name: assertInstanceStateRunning
  action: aws:assertAwsResourceProperty
  inputs:
    Service: ec2
    Api: DescribeInstanceStatus
    InstanceIds:
    - "{{ launchOneInstance.InstanceId }}"
    PropertySelector: "$.InstanceStatuses[0].InstanceState.Name"
    DesiredValues:
    - running
outputs:
- "launchOneInstance.InstanceId"
...
```

前述の各オートメーションアクションを使用すると、サービス名前空間、API オペレーション名、入力パラメータ、および出力パラメータを指定して、特定の API オペレーションを呼び出すことができます。入力は、選択した API オペレーションによって定義されます。API オペレーション (メソッド) は、以下の「サービスリファレンス」ページの左側のナビゲーションでサービスを選択することで表示できます。呼び出すサービスの [Client (クライアント)] セクションでメソッドを選択します。例えば、Amazon Relational Database Service (Amazon RDS) のすべての API オペレーション (メソッド) は、Amazon RDS メソッドのページに一覧表示されます。

各オートメーションアクションのスキーマは、次の場所で表示できます。

- aws:assertAwsResourceProperty – AWS リソースの状態またはイベントの状態をアサートする
- aws:executeAwsApi — AWS API オペレーションの呼び出しと実行
- aws:waitForAwsResourceProperty – AWS リソースプロパティを待つ

スキーマには、各アクションを使用するための必須フィールドの説明が含まれています。

Selector/PropertySelector フィールドの使用

各オートメーションアクションでは、出力 Selector (aws:executeAwsApi 用) または PropertySelector (aws:assertAwsResourceProperty および aws:waitForAwsResourceProperty 用) を指定する必要があります。これらのフィールドは、AWS API オペレーションから JSON 応答を処理するために使用されます。これらのフィールドは JSONPath 構文を使用します。

次に、aws:executeAwsAPi アクションのこの概念を説明する例を示します。

```
---
mainSteps:
- name: getImageId
  action: aws:executeAwsApi
  inputs:
    Service: ec2
    Api: DescribeImages
    Filters:
      - Name: "name"
        Values:
          - "{{ ImageName }}"
  outputs:
    - Name: ImageId
      Selector: "$.Images[0].ImageId"
      Type: "String"
...
```

aws:executeAwsApi ステップ getImageId で、オートメーションは DescribeImages API オペレーションを呼び出し、ec2 からレスポンスを受け取ります。次に、オートメーションは Selector - "$.Images[0].ImageId" を API レスポンスに適用し、選択した値を出力 ImageId 変数に割り当てます。同じ自動化の他のステップでは、ImageId を指定して "{{ getImageId.ImageId }}" の値を使用できます。

次に、aws:waitForAwsResourceProperty アクションのこの概念を説明する例を示します。

```
---
- name: waitUntilInstanceStateRunning
  action: aws:waitForAwsResourceProperty
  # timeout is strongly encouraged for action - aws:waitForAwsResourceProperty
  timeoutSeconds: 60
  inputs:
    Service: ec2
    Api: DescribeInstanceStatus
    InstanceIds:
    - "{{ launchOneInstance.InstanceId }}"
    PropertySelector: "$.InstanceStatuses[0].InstanceState.Name"
    DesiredValues:
    - running
...
```

aws:waitForAwsResourceProperty ステップ waitUntilInstanceStateRunning で、オートメーションは DescribeInstanceStatus API オペレーションを呼び出し、ec2 からレスポンスを受け取ります。次に、オートメーションは PropertySelector - "$.InstanceStatuses[0].InstanceState.Name" をレスポンスに適用し、指定された戻り値が DesiredValues リスト (この場合は running) の値と一致するかどうかを確認します。このステップは、レスポンスが running のインスタンスの状態を返すまでプロセスを繰り返します。

ランブックでの JSONPath の使用

JSONPath 式は、「$.」で始まる文字列で、JSON 要素内の 1 つ以上のコンポーネントを選択するために使用されます。次のリストには、Systems Manager Automation でサポートされている JSONPath 演算子に関する情報が含まれています。

- Dot-notated child (.): JSON オブジェクトで使用します。この演算子は、特定のキーの値を選択します。
- Deep-scan (..): JSON 要素で使用します。この演算子は、レベル別に JSON 要素レベルをスキャンし、特定のキーで値のリストを選択します。この演算子の戻り型は、常に JSON 配列です。オートメーションアクションの出力タイプのコンテキストでは、演算子は StringList または MapList のいずれかになります。
- Array-Index([ ]): JSON 配列で使用します。この演算子は、特定のインデックスの値を取得します。
- Filter ([?(***expression***)]): JSON 配列と一緒に使用します。このオペレータは、フィルター式で定義された条件と一致する JSON 配列値をフィルタリングします。フィルター式では、以下の演算子のみを使用できます。==、!=、>、<、>=、<= 複数のフィルター式を AND (&&) または OR (||) と組み合わせることはサポートされていません。この演算子の戻り型は、常に JSON 配列です。

JSONPath 演算子をよりよく理解するために、ec2 DescribeInstances API オペレーションの次の JSON 応答を確認してください。このレスポンスの下には、DescribeInstances API オペレーションからのレスポンスにさまざまな JSONPath 式を適用してさまざまな結果を示すいくつかの例があります。

```
{
    "NextToken": "abcdefg",
    "Reservations": [
        {
            "OwnerId": "123456789012",
            "ReservationId": "r-abcd12345678910",
            "Instances": [
```

```
            {
                "ImageId": "ami-12345678",
                "BlockDeviceMappings": [
                    {
                        "Ebs": {
                            "DeleteOnTermination": true,
                            "Status": "attached",
                            "VolumeId": "vol-000000000000"
                        },
                        "DeviceName": "/dev/xvda"
                    }
                ],
                "State": {
                    "Code": 16,
                    "Name": "running"
                }
            }
        ],
        "Groups": []
    },
    {
        "OwnerId": "123456789012",
        "ReservationId": "r-12345678910abcd",
        "Instances": [
            {
                "ImageId": "ami-12345678",
                "BlockDeviceMappings": [
                    {
                        "Ebs": {
                            "DeleteOnTermination": true,
                            "Status": "attached",
                            "VolumeId": "vol-111111111111"
                        },
                        "DeviceName": "/dev/xvda"
                    }
                ],
                "State": {
                    "Code": 80,
                    "Name": "stopped"
                }
            }
        ],
        "Groups": []
    }
```

```
    ]
}
```

JSONPath 例 1: JSON レスポンスから特定の文字列を取得する

```
JSONPath:
$.Reservations[0].Instances[0].ImageId

Returns:
"ami-12345678"

Type: String
```

JSONPath 例 2: JSON レスポンスから特定のブーリアンを取得する

```
JSONPath:
$.Reservations[0].Instances[0].BlockDeviceMappings[0].Ebs.DeleteOnTermination

Returns:
true

Type: Boolean
```

JSONPath 例 3: JSON レスポンスから特定の整数を取得する

```
JSONPath:
$.Reservations[0].Instances[0].State.Code

Returns:
16

Type: Integer
```

JSONPath 例 4: JSON レスポンスを詳細にスキャンし、VolumeId のすべての値を StringList として取得する

```
JSONPath:
$.Reservations..BlockDeviceMappings..VolumeId

Returns:
[
```

```
   "vol-000000000000",
   "vol-111111111111"
]

Type: StringList
```

JSONPath 例 5: 特定の BlockDeviceMappings オブジェクトを StringMap として取得する

```
JSONPath:
$.Reservations[0].Instances[0].BlockDeviceMappings[0]

Returns:
{
   "Ebs" : {
      "DeleteOnTermination" : true,
      "Status" : "attached",
      "VolumeId" : "vol-000000000000"
   },
   "DeviceName" : "/dev/xvda"
}

Type: StringMap
```

JSONPath 例 6: JSON レスポンスを詳細にスキャンし、すべての State のオブジェクトを MapList として取得します

```
JSONPath:
$.Reservations..Instances..State

Returns:
[
   {
      "Code" : 16,
      "Name" : "running"
   },
   {
      "Code" : 80,
      "Name" : "stopped"
   }
]

Type: MapList
```

JSONPath の例 7: **running** ステート内のインスタンスをフィルター処理する

```
JSONPath:
$.Reservations..Instances[?(@.State.Name == 'running')]

Returns:
[
  {
    "ImageId": "ami-12345678",
    "BlockDeviceMappings": [
      {
        "Ebs": {
          "DeleteOnTermination": true,
          "Status": "attached",
          "VolumeId": "vol-000000000000"
        },
        "DeviceName": "/dev/xvda"
      }
    ],
    "State": {
      "Code": 16,
      "Name": "running"
    }
  }
]

Type: MapList
```

JSONPath の例 8: **running** ステートにないインスタンスのうち、**ImageId** を返す

```
JSONPath:
$.Reservations..Instances[?(@.State.Name != 'running')].ImageId

Returns:
[
  "ami-12345678"
]

Type: StringList | String
```

Automation 向けのウェブフック統合の作成

オートメーション中にウェブフックを使用してメッセージを送信するには、統合を作成します。ランブック内で aws:invokeWebhook アクションを使用すると、統合をオートメーション中に呼び出すことができます。ウェブフックをまだ作成していない場合は、「統合用のウェブフックの作成」を参照してください。aws:invokeWebhook アクションの詳細については、「aws:invokeWebhook – オートメーションのウェブフック統合を呼び出す」を参照してください。

次の手順に示すように、Systems Manager のオートメーションコンソール、または任意のコマンドラインツールを使用して、統合を作成できます。

統合の作成 (コンソール)

オートメーション用に統合を作成するには (コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで [オートメーション] を選択します。
3. [Integrations] (統合) タブを開きます。
4. [Add integration] (統合を追加)、[Webhook] (ウェブフック) の順にクリックします。
5. 統合に適用する、必須の値および任意のオプション値を入力します。
6. [Add] (追加) をクリックして統合を作成します。

統合の作成 (コマンドライン)

コマンドラインツールを使用して統合を作成するためには、その統合に必須の SecureString パラメータを作成します。オートメーションは、統合に関する情報を格納するために、Systems Manager のツールである Parameter Store 内で予約済みの名前空間を使用します。AWS Management Console を使用して統合を作成する場合には、ユーザーに代わりオートメーションがこのプロセスを処理します。名前空間に続いて、作成する統合のタイプ、および統合の名前を指定する必要があります。現在、オートメーションでは webhook タイプの統合がサポートされています。

webhook タイプの統合では、以下のフィールドがサポートされます。

- 説明
- headers
- payload
- [URL]

[開始する前に]

まだ AWS Command Line Interface (AWS CLI) または AWS Tools for PowerShell をインストールして設定していない場合は、インストールして設定します。詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」および「AWS Tools for PowerShell のインストール」を参照してください。

オートメーション用に統合を作成するには (コマンドライン)

- 以下のコマンドを実行して、統合に必須な SecureString パラメータを作成します。各*############*をユーザー自身の情報に置き換えます。/d9d01087-4a3f-49e0-b0b4-d568d7826553/ssm/integrations/webhook/ 名前空間は、Parameter Store 内で統合用として予約されています。パラメータの名前は、この名前空間と同じものを (後に統合の名前を続けて) 使用する必要があります。例: /d9d01087-4a3f-49e0-b0b4-d568d7826553/ssm/integrations/webhook/*myWebhookIntegration*

  Linux & macOS

  ```
  aws ssm put-parameter \
      --name "/d9d01087-4a3f-49e0-b0b4-d568d7826553/ssm/integrations/
  webhook/myWebhookIntegration" \
      --type "SecureString" \
      --data-type "aws:ssm:integration" \
      --value '{"description": "My first webhook integration for Automation.",
   "url": "myWebHookURL"}'
  ```

  Windows

  ```
  aws ssm put-parameter ^
      --name "/d9d01087-4a3f-49e0-b0b4-d568d7826553/ssm/integrations/
  webhook/myWebhookIntegration" ^
      --type "SecureString" ^
      --data-type "aws:ssm:integration" ^
      --value  "{\"description\":\"My first webhook integration for Automation.\",
  \"url\":\"myWebHookURL\"}"
  ```

  PowerShell

  ```
  Write-SSMParameter `
      -Name "/d9d01087-4a3f-49e0-b0b4-d568d7826553/ssm/integrations/
  webhook/myWebhookIntegration" `
  ```

```
    -Type "SecureString"
    -DataType "aws:ssm:integration"
    -Value '{"description": "My first webhook integration for Automation.",
"url": "myWebHookURL"}'
```

統合用のウェブフックの作成

プロバイダでウェブフックを作成する場合は、以下の点に注意してください。

- プロトコルは HTTPS を使用する必要があります。
- カスタムリクエストヘッダーをサポートする必要があります。
- デフォルトのリクエストボディを指定できます。
- デフォルトのリクエストボディは、aws:invokeWebhook アクションを使用して統合が呼び出された時点でオーバーライドされます

ランブックでのタイムアウトの処理

timeoutSeconds プロパティはオートメーションのすべてのアクションで共有されます。このプロパティを使用して、アクションの実行タイムアウト値を指定できます。さらに、アクションのタイムアウトがオートメーションと全体的な実行ステータスに与える影響を変更できます。そのためには、アクションの onFailure および isCritical 共有プロパティも定義します。

たとえば、ユースケースによっては、アクションがタイムアウトした場合に、オートメーションが別のアクションを続行し、オートメーションの全体的なステータスに影響を与えないようにすることもできます。この例では、timeoutSeconds プロパティを使用して、アクションがタイムアウトするまでの待機時間を指定しています。次に、タイムアウトが発生した場合にオートメーションが続行するアクション (ステップ) を指定します。デフォルト値の step:*step name* ではなく、onFailure プロパティの Abort 形式の値を指定します。デフォルトでは、アクションがタイムアウトした場合、オートメーションの実行ステータスは Timed Out になります。タイムアウトが オートメーションの実行ステータスに影響を与えないようにするには、false プロパティに isCritical を指定します。

以下の例では、このシナリオで説明されているアクションの共有プロパティを定義する方法を示しています。

YAML

```
- name: verifyImageAvailability
```

```
  action: 'aws:waitForAwsResourceProperty'
  timeoutSeconds: 600
  isCritical: false
  onFailure: 'step:getCurrentImageState'
  inputs:
    Service: ec2
    Api: DescribeImages
    ImageIds:
      - '{{ createImage.newImageId }}'
    PropertySelector: '$.Images[0].State'
    DesiredValues:
      - available
  nextStep: copyImage
```

JSON

```
{
    "name": "verifyImageAvailability",
    "action": "aws:waitForAwsResourceProperty",
    "timeoutSeconds": 600,
    "isCritical": false,
    "onFailure": "step:getCurrentImageState",
    "inputs": {
        "Service": "ec2",
        "Api": "DescribeImages",
        "ImageIds": [
            "{{ createImage.newImageId }}"
        ],
        "PropertySelector": "$.Images[0].State",
        "DesiredValues": [
            "available"
        ]
    },
    "nextStep": "copyImage"
}
```

オートメーションのすべてのアクションで共有されるプロパティの詳細については、「すべてのアクションで共有されるプロパティ」を参照してください。

Systems Manager Automation ランブックのリファレンス

AWS Systems Manager では、お客様が迅速に使用を開始していただけるように、事前定義済みのランブックが用意されています。これらのランブックは、アマゾンウェブサービス、AWS サポート、および AWS Config によって管理されています。このランブックリファレンスでは、Systems Manager、サポート、および AWS Config から提供される、定義済みのランブックについて説明します。詳細については、Systems Manager Automation ランブックリファレンスを参照してください。

チュートリアル

以下のチュートリアルは、AWS Systems Manager Automation を使用して一般的なユースケースに対応する際の役に立ちます。これらのチュートリアルでは、独自のランブックや、Automation から提供されている事前定義済みのランブックを使用する方法、また、これら以外の Systems Manager のツールを他の AWS のサービスとともに使用する方法について紹介しています。

目次

- AMIs の更新
  - Linux AMI を更新する
  - Linux AMI (AWS CLI) を更新する
  - Windows Server AMI を更新する
  - Automation、AWS Lambda、Parameter Store を使用してゴールデン AMI を更新する
    - タスク 1: Systems Manager Parameter Store でパラメータを作成する
    - タスク 2: 用の IAM ロールを作成するAWS Lambda
    - タスク 3: AWS Lambda 関数を作成する
    - タスク 4: ランブックを作成し、AMI にパッチを適用する
  - オートメーションと Jenkins を使用した AMIs の更新
  - Auto Scaling グループ用の AMIs の更新
    - PatchAMIAndUpdateASG ランブックを作成する
- AWS サポート でのセルフサービスランブックの使用
  - 到達不可能なインスタンスでの EC2Rescue ツールの実行
    - 仕組み
    - 開始する前に
      - インスタンスでアクションを実行するための AWSSupport-EC2Rescue アクセス許可の付与

        - IAM ポリシーを使用したアクセス許可の付与
        - AWS CloudFormation テンプレートを使用したアクセス権限の付与
    - 自動化の実行
- EC2 インスタンスでのパスワードと SSH キーのリセット
    - 仕組み
    - [開始する前に]
        - インスタンスでアクションを実行するための AWSSupport-EC2Rescue アクセス許可の付与
            - IAM ポリシーを使用したアクセス許可の付与
            - AWS CloudFormation テンプレートを使用したアクセス権限の付与
    - 自動化の実行
- 入力トランスフォーマーを使用したオートメーションへのデータの受け渡し

AMIs の更新

以下のチュートリアルでは、最新のパッチを適用するための Amazon Machine Image (AMIs) の更新方法について説明します。

トピック

- Linux AMI を更新する
- Linux AMI (AWS CLI) を更新する
- Windows Server AMI を更新する
- Automation、AWS Lambda、Parameter Store を使用してゴールデン AMI を更新する
- オートメーションと Jenkins を使用した AMIs の更新
- Auto Scaling グループ用の AMIs の更新

Linux AMI を更新する

この Systems Manager Automation チュートリアルでは、コンソールまたは AWS CLI および `AWS-UpdateLinuxAmi` ランブックを使用して、指定したパッケージ用の最新バージョンのパッチを、Linux AMI に適用する方法について説明します。Automation は AWS Systems Manager のツールです。`AWS-UpdateLinuxAmi` ランブックは、その他のサイト固有のパッケージと設定のインストールも自動化します。このチュートリアルを使用して、Ubuntu Server、CentOS、RHEL、SLES、または Amazon Linux AMIs などのさまざまな Linux ディストリ

ビューションを更新できます。サポートされている Linux バージョンの詳細なリストについては、「Patch Manager の前提条件」を参照してください。

AWS-UpdateLinuxAmi ランブックでは、JSON あるいは YAML によりランブックを記述することなく、イメージのメンテナンスタスクを自動化することができます。AWS-UpdateLinuxAmi ランブックを使用して次のタイプのタスクを実行できます。

- Amazon Linux、Red Hat Enterprise Linux、Ubuntu Server、SUSE Linux Enterprise Server、または Cent OS Amazon Machine Image (AMI) 上のすべてのディストリビューションパッケージと Amazon ソフトウェアを更新します。これはデフォルトのランブックの動作です。
- 既存のイメージに AWS Systems Manager SSM Agent をインストールして、AWS Systems Manager Run Command を使用したリモートコマンドの実行や、Inventory を使用したソフトウェアインベントリ収集といった Systems Manager のツールを有効にします。
- 追加のソフトウェアパッケージをインストールします。

開始する前に

ランブックで作業を開始する前に、ロールを設定し、必要に応じてオートメーション用に EventBridge を設定します。詳細については、「オートメーションの設定」を参照してください。このチュートリアルでは、AWS Identity and Access Management (IAM) インスタンスプロファイルの名前を指定する必要もあります。IAM インスタンスプロファイル作成の詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」を参照してください。

AWS-UpdateLinuxAmi ランブックは、次の入力パラメータを受け付けます。

Parameter	Type	説明
SourceAmiId	文字列	(必須) ソース AMI ID。
IamInstanceProfileName	String	(必須)「Systems Manager に必要なインスタンスのアクセス許可を設定する」で作成した IAM インスタンスプロファイルロールの名前。インスタンスプロファイルのロールは、コマンドの実行またはサービスの開始や停止など、インスタンスでアクションを

Parameter	Type	説明
		実行するための自動化のアクセス許可を付与します。ランブックでは、インスタンスプロファイルロールの名前のみが使用されます。Amazon リソースネーム (ARN) を指定すると、オートメーションは失敗します。
AutomationAssumeRole	文字列	(必須) オートメーションの設定 で作成した IAM サービスロールの名前。サービスロール (継承ロールとも呼ばれます) は、オートメーションが IAM ロールを引き受け、代わりにアクションを実行するアクセス許可を与えます。例えば、サービスロールを使用すると、ランブックで `aws:createImage` アクションを実行するとき、Automation で新しい AMI を作成できます。このパラメータには、完全な ARN を指定する必要があります。
TargetAmiName	文字列	(オプション) 作成後の AMI の新しい名前。デフォルト名は、ソース AMI ID および作成日時を含む、システム生成文字列です。

Parameter	Type	説明
InstanceType	文字列	(オプション) WorkSpace ホストとして起動するインスタンスの種類。インスタンスタイプは、リージョンによって異なります。デフォルトのタイプは、t2.micro です。
PreUpdateScript	文字列	(オプション) 更新の適用前に実行するスクリプトの URL。デフォルト (\"none\") は、スクリプトを実行しません。
PostUpdateScript	文字列	(オプション) パッケージの更新の適用後に実行するスクリプトの URL。デフォルト (\"none\") は、スクリプトを実行しません。
IncludePackages	文字列	(オプション) これらの名前付きパッケージのみを更新します。デフォルト (\"all\") では、すべての利用可能な更新が適用されます。
ExcludePackages	文字列	(オプション) すべての条件の下で、更新を保留するパッケージの名前。デフォルト (\"none\") では、パッケージは除外されません。

自動化のステップ

AWS-UpdateLinuxAmi ランブックには、デフォルトで次のオートメーションアクションが含まれています。

ステップ 1: launchInstance (**aws:runInstances** アクション)

このステップでは、Amazon Elastic Compute Cloud (Amazon EC2) ユーザーデータ、および IAM インスタンスプロファイルのロールを使用してインスタンスを起動します。ユーザーデータは、オペレーティングシステムに基づいて、適切な SSM Agent をインストールします。SSM Agent をインストールすると、Run Command、State Manager、Inventory など、Systems Manager のツールを利用できます。

ステップ 2: updateOSSoftware (**aws:runCommand** アクション)

このステップでは、起動したインスタンスで次のコマンドを実行します。

- Amazon S3 からの更新スクリプトをダウンロードします。
- オプションの更新前のスクリプトを実行します。
- ディストリビューションパッケージおよび Amazon ソフトウェアを更新します。
- オプションの更新後のスクリプトを実行します。

実行ログは、ユーザーが後で表示するために /tmp フォルダに保存されます。

特定のパッケージセットをアップグレードする場合は、`IncludePackages` パラメータを使用してリストを指定できます。指定すると、システムはこれらのパッケージおよび依存関係のみを更新するよう試みます。その他の更新は実行されません。デフォルトでは、含まれるパッケージが指定されない場合、プログラムはすべての利用可能なパッケージを更新します。

特定のパッケージセットのアップグレードを除外する場合は、`ExcludePackages` パラメータにリストを指定できます。指定されている場合、これらのパッケージは、指定された他のオプションとは関係なく、現在のバージョンのままです。デフォルトでは、除外するパッケージが指定されていない場合、除外されるパッケージはありません。

ステップ 3: stopInstance (**aws:changeInstanceState** アクション)

このステップでは、更新されたインスタンスを停止します。

ステップ 4: createImage (**aws:createImage** アクション)

このステップでは、ソース ID、および作成時刻にリンクするわかりやすい名前の新しい AMI を作成します。例: 「{{SourceAmiId}} から {{global:DATE_TIME}} に EC2 Automation によって生成された AMI」。ここで DATE_TIME および SourceID は、自動化の変数を表します。

ステップ 5: terminateInstance (**aws:changeInstanceState** アクション)

このステップでは、実行中のインスタンスを終了してオートメーションをクリーンアップします。

出力

オートメーションは、出力として新しい AMI ID を返します。

> **Note**
>
> デフォルトでは、自動化が `AWS-UpdateLinuxAmi` ランブックを実行すると、システムはデフォルト VPC (172.30.0.0/16) に一時インスタンスを作成します。デフォルト VPC を削除した場合、次のエラーが発生します。
> `VPC not defined 400`
> この問題を解決するには、`AWS-UpdateLinuxAmi` ランブックのコピーを作成し、サブネット ID を指定する必要があります。詳細については、「VPC not defined 400」を参照してください。

Automation (AWS Systems Manager) を使用して パッチを適用した AMI を作成するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで [オートメーション] を選択します。
3. [Execute automation] を選択します。
4. [Automation document (オートメーションドキュメント)] リストで、**`AWS-UpdateLinuxAmi`** を選択します。
5. [Document details (ドキュメント詳細)] セクションで、[Document version (ドキュメントバージョン)] が [Default version at runtime (ランタイムのデフォルトバージョン)] に設定されていることを確認します。
6. [Next] を選択します。
7. [実行モード)] セクションで、[シンプルな実行] を選択します。
8. [Input parameters] セクションに、開始する前にセクションで用意した情報を入力します。
9. [Execute] を選択します。自動化の実行のステータスがコンソールに表示されます。

オートメーションが終了したら、更新した AMI からテストインスタンスを起動して、変更を確認します。

> **Note**
>
> オートメーションのいずれかのステップが失敗した場合は、失敗に関する情報が [Automation Executions] ページに表示されます。オートメーションは、すべてのタスクを正常に完了すると、一時インスタンスを終了するように設計されています。失敗したステップがあると、システムはインスタンスを終了できない場合があります。失敗したステップがある場合は、一時インスタンスを手動で終了します。

Linux AMI (AWS CLI) を更新する

この AWS Systems Manager オートメーションチュートリアルでは、AWS Command Line Interface (AWS CLI) と System Manager `AWS-UpdateLinuxAmi` ランブックを使用して、指定した最新バージョンのパッケージを Linux Amazon Machine Image (AMI) に自動的にパッチ適用する方法について説明します。Automation は AWS Systems Manager のツールです。`AWS-UpdateLinuxAmi` ランブックは、その他のサイト固有のパッケージと設定のインストールも自動化します。このチュートリアルを使用して、Ubuntu Server、CentOS、RHEL、SLES、または Amazon Linux AMIs などのさまざまな Linux ディストリビューションを更新できます。サポートされている Linux バージョンの詳細なリストについては、「Patch Manager の前提条件」を参照してください。

`AWS-UpdateLinuxAmi` ランブックでは、JSON あるいは YAML のランブックを作成することなく、イメージメンテナンスタスクを自動化することができます。`AWS-UpdateLinuxAmi` ランブックを使用して次のタイプのタスクを実行できます。

- Amazon Linux、Red Hat Enterprise Linux、Ubuntu Server、SLES、または Cent OS Amazon Machine Image (AMI) 上のすべてのディストリビューションパッケージと Amazon ソフトウェアを更新します。これはデフォルトのランブックの動作です。
- 既存のイメージに AWS Systems Manager SSM Agent をインストールして、AWS Systems Manager Run Command を使用したリモートコマンドの実行や、インベントリを使用したソフトウェアインベントリ収集といった Systems Manager の機能を有効にします。
- 追加のソフトウェアパッケージをインストールします。

開始する前に

ランブックで作業を開始する前に、ロールを設定し、必要に応じてオートメーション用に EventBridge を設定します。詳細については、「オートメーションの設定」を参照してください。このチュートリアルでは、AWS Identity and Access Management (IAM) インスタンスプロファイルの

名前を指定する必要もあります。IAM インスタンスプロファイル作成の詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」を参照してください。

AWS-UpdateLinuxAmi ランブックは、次の入力パラメータを受け付けます。

Parameter	Type	説明
SourceAmiId	文字列	(必須) ソース AMI ID。AWS Systems Manager Parameter Store パブリックパラメータを使用すると、Linux 用の Amazon EC2 AMI の最新の ID を自動的に参照できます。詳細については、「AWS Systems Manager Parameter Store を使用して最新の Amazon Linux AMI ID を取得する」を参照してください。
IamInstanceProfileName	String	(必須)「Systems Manager に必要なインスタンスのアクセス許可を設定する」で作成した IAM インスタンスプロファイルロールの名前。インスタンスプロファイルのロールは、コマンドの実行またはサービスの開始や停止など、インスタンスでアクションを実行するための自動化のアクセス許可を付与します。ランブックでは、インスタンスプロファイルロールの名前のみが使用されます。
AutomationAssumeRole	文字列	(必須) オートメーションの設定 で作成した IAM サービスロールの名前。サービスロール (継承ロールとも呼

Parameter	Type	説明
		ばれます) は、オートメーションが IAM ロールを引き受け、代わりにアクションを実行するアクセス許可を与えます。例えば、サービスロールを使用すると、ランブックで `aws:createImage` アクションを実行するとき、Automation で新しい AMI を作成できます。このパラメータには、完全な ARN を指定する必要があります。
TargetAmiName	文字列	(オプション) 作成後の AMI の新しい名前。デフォルト名は、ソース AMI ID および作成日時を含む、システム生成文字列です。
InstanceType	文字列	(オプション) WorkSpace ホストとして起動するインスタンスの種類。インスタンスタイプは、リージョンによって異なります。デフォルトのタイプは、t2.micro です。
PreUpdateScript	文字列	(オプション) 更新の適用前に実行するスクリプトの URL。デフォルト (\"none\") は、スクリプトを実行しません。
PostUpdateScript	文字列	(オプション) パッケージの更新の適用後に実行するスクリプトの URL。デフォルト (\"none\") は、スクリプトを実行しません。

Parameter	Type	説明
IncludePackages	文字列	(オプション) これらの名前付きパッケージのみを更新します。デフォルト (\"all\") では、すべての利用可能な更新が適用されます。
ExcludePackages	文字列	(オプション) すべての条件の下で、更新を保留するパッケージの名前。デフォルト (\"none\") では、パッケージは除外されません。

自動化のステップ

AWS-UpdateLinuxAmi ランブックには、デフォルトで次の手順が含まれています。

ステップ 1: launchInstance (**aws:runInstances** アクション)

このステップでは、Amazon Elastic Compute Cloud (Amazon EC2) ユーザーデータ、および IAM インスタンスプロファイルのロールを使用してインスタンスを起動します。ユーザーデータは、オペレーティングシステムに基づいて、適切な SSM Agent をインストールします。SSM Agent をインストールすると、Run Command、State Manager、Inventory など、Systems Manager のツールを利用できます。

ステップ 2: updateOSSoftware (**aws:runCommand** アクション)

このステップでは、起動したインスタンスで次のコマンドを実行します。

- Amazon Simple Storage Service (Amazon S3) から更新スクリプトをダウンロードします。
- オプションの更新前のスクリプトを実行します。
- ディストリビューションパッケージおよび Amazon ソフトウェアを更新します。
- オプションの更新後のスクリプトを実行します。

実行ログは、ユーザーが後で表示するために /tmp フォルダに保存されます。

特定のパッケージセットをアップグレードする場合は、IncludePackages パラメータを使用してリストを指定できます。指定すると、システムはこれらのパッケージおよび依存関係のみを更

新するよう試みます。その他の更新は実行されません。デフォルトでは、含まれるパッケージが指定されない場合、プログラムはすべての利用可能なパッケージを更新します。

特定のパッケージセットのアップグレードを除外する場合は、ExcludePackages パラメータにリストを指定できます。指定されている場合、これらのパッケージは、指定された他のオプションとは関係なく、現在のバージョンのままです。デフォルトでは、除外するパッケージが指定されていない場合、除外されるパッケージはありません。

ステップ 3: stopInstance (**aws:changeInstanceState** アクション)

このステップでは、更新されたインスタンスを停止します。

ステップ 4: createImage (**aws:createImage** アクション)

このステップでは、ソース ID、および作成時刻にリンクするわかりやすい名前の新しい AMI を作成します。例: 「{{SourceAmiId}} から {{global:DATE_TIME}} に EC2 Automation によって生成された AMI」。ここで DATE_TIME および SourceID は、自動化の変数を表します。

ステップ 5: terminateInstance (**aws:changeInstanceState** アクション)

このステップでは、実行中のインスタンスを終了してオートメーションをクリーンアップします。

出力

オートメーションは、出力として新しい AMI ID を返します。

> **Note**
>
> デフォルトでは、自動化が AWS-UpdateLinuxAmi ランブックを実行すると、システムはデフォルト VPC (172.30.0.0/16) に一時インスタンスを作成します。デフォルト VPC を削除した場合、次のエラーが発生します。
> `VPC not defined 400`
> この問題を解決するには、AWS-UpdateLinuxAmi ランブックのコピーを作成し、サブネット ID を指定する必要があります。詳細については、「VPC not defined 400」を参照してください。

Automation を使用して パッチを適用した AMI を作成するには

1. まだ AWS Command Line Interface (AWS CLI) をインストールして設定していない場合は、インストールして設定します。

詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」を参照してください。

2. 次のコマンドを実行して、AWS-UpdateLinuxAmi ランブックを実行します。各*##########*をユーザー自身の情報に置き換えます。

```
aws ssm start-automation-execution \
    --document-name "AWS-UpdateLinuxAmi" \
    --parameters \
    SourceAmiId=AMI ID, \
    IamInstanceProfileName=IAM instance profile, \
    AutomationAssumeRole='arn:aws:iam::
{{global:ACCOUNT_ID}}:role/AutomationServiceRole'
```

コマンドによって実行 ID が返されます。この ID をクリップボードにコピーします。この ID を使用して、オートメーションの状態を表示します。

```
{
    "AutomationExecutionId": "automation execution ID"
}
```

3. AWS CLI を使用してオートメーションを表示するには、次のコマンドを実行します。

```
aws ssm describe-automation-executions
```

4. オートメーションの進捗の詳細を表示するには、以下のコマンドを実行します。*[Automation execution ID]* (オートメーション実行 ID) をユーザー自身の情報に置き換えます。

```
aws ssm get-automation-execution --automation-execution-id automation execution ID
```

更新プロセスは完了までに 30 分以上かかる場合があります。

> **Note**
>
> コンソールで、オートメーションのステータスをモニタリングすることもできます。リストで、先ほど開始したオートメーションを選択し、[Steps] タブを選択します。このタブには、オートメーションアクションのステータスが表示されます。

オートメーションが終了したら、更新した AMI からテストインスタンスを起動して、変更を確認します。

> **Note**
>
> オートメーションのいずれかのステップが失敗した場合は、失敗に関する情報が [Automation Executions] ページに表示されます。オートメーションは、すべてのタスクを正常に完了すると、一時インスタンスを終了するように設計されています。失敗したステップがあると、システムはインスタンスを終了できない場合があります。失敗したステップがある場合は、一時インスタンスを手動で終了します。

Windows Server AMI を更新する

`AWS-UpdateWindowsAmi` ランブックでは、JSON あるいは YAML のランブックを作成することなく、Amazon Windows Amazon Machine Image (AMI) のイメージメンテナンスタスクを自動化することができます。このランブックは Windows Server 2008 R2 以降でサポートされています。`AWS-UpdateWindowsAmi` ランブックを使用して次のタイプのタスクを実行できます。

- すべての Windows 更新プログラムをインストールし、Amazon ソフトウェアをアップグレードする (デフォルトの動作)。
- 特定の Windows 更新プログラムをインストールし、Amazon ソフトウェアをアップグレードする。
- スクリプトを使用して AMI をカスタマイズする。

開始する前に

ランブックの使用を開始する前に、ロールを Automation 用に設定して、アクセスを許可するインスタンスプロファイルの ARN を参照する `iam:PassRole` ポリシーを追加します。オプションで、AWS Systems Manager のツールである Automation 向けに Amazon EventBridge を設定することができます。詳細については、「オートメーションの設定」を参照してください。このチュートリアルでは、AWS Identity and Access Management (IAM) インスタンスプロファイルの名前を指定する必要もあります。IAM インスタンスプロファイル作成の詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」を参照してください。

> **Note**
>
> AWS Systems Manager SSM Agent の更新は、通常、リージョン別に異なる時間に展開されます。AMI をカスタマイズまたは更新する際、作業しているリージョンで公開されているソース AMI のみを使用してください。これは、そのリージョンでリリースされている最新の SSM Agent を使用していることを確実にし、互換性の問題を防ぎます。

`AWS-UpdateWindowsAmi` ランブックは、次の入力パラメータを受け付けます。

Parameter	Type	説明
SourceAmiId	文字列	(必須) ソース AMI ID。Systems Manager Parameter Store パブリックパラメータを使用して、最新の Windows Server AMI ID を自動的に参照できます。詳細については、「AWS Systems ManagerParameter Store を使用して、最新の Windows AMI ID をクエリする」を参照してください。
SubnetId	String	(オプション) 一時インスタンスを起動するサブネット。デフォルト VPC を削除した場合は、このパラメータの値を指定する必要があります。
IamInstanceProfileName	String	(必須)「Systems Manager に必要なインスタンスのアクセス許可を設定する」で作成した IAM インスタンスプロファイルロールの名前。インスタンスプロファイルのロールは、コマンドの実行またはサービスの開始や停止など、イン

Parameter	Type	説明
		スタンスでアクションを実行するための自動化のアクセス許可を付与します。ランブックでは、インスタンスプロファイルロールの名前のみが使用されます。
AutomationAssumeRole	文字列	(必須) オートメーションの設定 で作成した IAM サービスロールの名前。サービスロール (継承ロールとも呼ばれます) は、オートメーションが IAM ロールを引き受け、代わりにアクションを実行するアクセス許可を与えます。例えば、サービスロールを使用すると、ランブックで `aws:createImage` アクションを実行するとき、Automation で新しい AMI を作成できます。このパラメータには、完全な ARN を指定する必要があります。
TargetAmiName	文字列	(オプション) 作成後の AMI の新しい名前。デフォルト名は、ソース AMI ID および作成日時を含む、システム生成文字列です。

Parameter	Type	説明
InstanceType	文字列	(オプション) WorkSpace ホストとして起動するインスタンスの種類。インスタンスタイプは、リージョンによって異なります。デフォルトのタイプは、t2.medium です。
PreUpdateScript	文字列	(オプション) AMI を更新する前に実行するスクリプト。スクリプトをランブックに入力するか、実行時にパラメータとして入力します。
PostUpdateScript	文字列	(オプション) AMI を更新した後に実行するスクリプト。スクリプトをランブックに入力するか、実行時にパラメータとして入力します。
IncludeKbs	文字列	(任意) 含める Microsoft Knowledge Base (KB) 記事 ID を 1 つ以上指定します。コンマ区切り値を使って複数の ID をインストールできます。有効な形式: KB9876543 または 9876543。
ExcludeKbs	文字列	(任意) 除外する Microsoft Knowledge Base (KB) 記事 ID を 1 つ以上指定します。コンマ区切り値を使って複数の ID を除外できます。有効な形式: KB9876543 または 9876543。

Parameter	Type	説明
カテゴリ	文字列	(任意) 1 つ以上の更新カテゴリを指定します。カンマ区切り値を使ってカテゴリをフィルターできます。オプション: 重要な更新プログラム、セキュリティ更新プログラム、定義ファイルの更新、更新プログラムのロールアップ、Service Pack、ツール、更新、またはドライバー。有効な形式には、「重要なアップデート」といった単一のエントリが含まれます。または、カンマ区切りのリストを指定できます。たとえば、重要な更新プログラム,セキュリティ更新プログラム,定義ファイルの更新となります。
SeverityLevels	文字列	(任意) 更新と関連付けられた MSRC 重要度レベルを 1 つ以上指定します。カンマ区切り値を使って重要度をフィルターできます。オプション: 非常事態、重要、低、中、または指定しない。有効な形式には、「非常事態」といった単一のエントリが含まれます。または、カンマ区切りリストを指定できます: 非常事態,重要,低。

自動化のステップ

AWS-UpdateWindowsAmi ランブックには、デフォルトで次の手順が含まれています。

ステップ 1: launchInstance (**aws:runInstances** アクション)

このステップは、指定された SourceAmiID の IAM インスタンスプロファイルロールでインスタンスを起動します。

ステップ 2: runPreUpdateScript (**aws:runCommand** アクション)

このステップでは、更新がインストールされる前に実行される文字列としてスクリプトを指定できます。

ステップ 3: updateEC2Config (**aws:runCommand**アクション)

この手順では、AWS-InstallPowerShellModule ランブックを使用して AWS パブリック PowerShell モジュールをダウンロードします。Systems Manager は SHA-256 ハッシュを使用してモジュールの整合性を検証します。Systems Manager はその次にオペレーティングシステムを確認して、EC2Config または EC2Launch のどちらを更新するかを判断します。EC2Config は Windows Server 2008 R2 から Windows Server 2012 R2 で実行されます。EC2Launch は Windows Server 2016 で実行されます。

ステップ 4: updateSSMAgent (**aws:runCommand**アクション)

この手順では、AWS-UpdateSSMAgent ランブックを使用して SSM Agent を更新します。

ステップ 5: updateAWSPVDriver (**aws:runCommand**アクション)

この手順では、AWS-ConfigureAWSPackage ランブックを使用して AWS PV ドライバーを更新します。

ステップ 6: updateAwsEnaNetworkDriver (**aws:runCommand**アクション)

この手順では、AWS-ConfigureAWSPackage ランブックを使用して AWS ENA ネットワークドライバーを更新します。

ステップ 7: installWindowsUpdates (**aws:runCommand** アクション)

この手順では、AWS-InstallWindowsUpdates ランブックを使用して Windows 更新プログラムをインストールします。デフォルトでは、Systems Manager は不足している更新を検索し、インストールします。次のパラメータのいずれかを指定することで、デフォルトの動作を変更できます: IncludeKbs、ExcludeKbs、Categories、またはSeverityLevels。

ステップ 8: runPostUpdateScript (**aws:runCommand**アクション)

このステップでは、更新がインストールされた後に実行される文字列としてスクリプトを指定することができます。

ステップ 9: runSysprepGeneralize (**aws:runCommand**アクション)

この手順では、AWS-InstallPowerShellModule ランブックを使用して AWS パブリック PowerShell モジュールをダウンロードします。Systems Manager は SHA-256 ハッシュを使用してモジュールの整合性を検証します。Systems Manager はその次に、AWS がサポートする方法を使用して EC2Launch (Windows Server 2016) または EC2Config (Windows Server 2008 R2 から 2012 R2) に sysprep を実行します。

ステップ 10: stopInstance (**aws:changeInstanceState** アクション)

このステップでは、更新されたインスタンスを停止します。

ステップ 11: createImage (**aws:createImage** アクション)

このステップでは、ソース ID、および作成時刻にリンクするわかりやすい名前の新しい AMI を作成します。例: 「{{SourceAmiId}} から {{global:DATE_TIME}} に EC2 Automation によって生成された AMI」。ここで DATE_TIME および SourceID は、自動化の変数を表します。

ステップ 12: TerminateInstance (**aws:changeInstanceState** アクション)

このステップでは、実行中のインスタンスを終了してオートメーションをクリーンアップします。

出力

このセクションでは、任意のパラメータの様々なステップや値の出力を、自動化の出力として指定できます。デフォルトでは、出力は、オートメーションによって作成された更新済みの Windows AMI の ID です。

> **Note**
>
> デフォルトでは、オートメーションが AWS-UpdateWindowsAmi ランブックを実行して一時インスタンスを作成すると、システムはデフォルト default VPC (172.30.0.0/16) を使用します。デフォルト VPC を削除した場合、次のエラーが発生します。
> VPC not defined 400
> この問題を解決するには、AWS-UpdateWindowsAmi ランブックのコピーを作成し、サブネット ID を指定する必要があります。詳細については、「VPC not defined 400」を参照してください。

Automation を使用してパッチを適用した Windows AMI を作成するには

1. まだ AWS Command Line Interface (AWS CLI) をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」を参照してください。

2. 次のコマンドを実行して、AWS-UpdateWindowsAmi ランブックを実行します。各*########*をユーザー自身の情報に置き換えます。以下のコマンド例では、最新の Amazon EC2 AMI を使用して、適用する必要があるパッチの数を最小限に抑えています。このコマンドを複数回実行する場合は、targetAMIname に一意の値を指定する必要があります。AMI 名は一意のものでなければなりません。

   ```
   aws ssm start-automation-execution \
       --document-name="AWS-UpdateWindowsAmi" \
       --parameters SourceAmiId='AMI ID',IamInstanceProfileName='IAM
    instance profile',AutomationAssumeRole='arn:aws:iam::
   {{global:ACCOUNT_ID}}:role/AutomationServiceRole'
   ```

   コマンドによって実行 ID が返されます。この ID をクリップボードにコピーします。この ID を使用して、オートメーションの状態を表示します。

   ```
   {
       "AutomationExecutionId": "automation execution ID"
   }
   ```

3. AWS CLI を使用してオートメーションを表示するには、次のコマンドを実行します。

   ```
   aws ssm describe-automation-executions
   ```

4. オートメーションの進捗の詳細を表示するには、以下のコマンドを実行します。

   ```
   aws ssm get-automation-execution
       --automation-execution-id automation execution ID
   ```

> **Note**
>
> 適用されるパッチの数に応じて、このサンプルオートメーションで実行される Windows パッチ適用プロセスは、完了までに 30 分以上かかることがあります。

Automation、AWS Lambda、Parameter Store を使用してゴールデン AMI を更新する

次の例では、Amazon Elastic Compute Cloud (Amazon EC2) AMIs から構築するのではなく、組織が独自の AMIs を維持し、定期的にパッチを適用するモデルを使用しています。

次の手順は、最新または最後の AMI であると既にみなされている AMI にオペレーティングシステム (OS) のパッチを自動的に適用する方法を示しています。この例では、パラメータ `SourceAmiId` のデフォルト値は、`latestAmi` という AWS Systems Manager Parameter Store のパラメータによって定義されます。`latestAmi` の値は、オートメーションの終了時に呼び出される AWS Lambda 関数によって更新されます。このオートメーションプロセスの結果として、パッチ適用が常に最新の AMI に適用されるため、AMIs のパッチ適用に費やされる時間と労力が最小限に抑えられます。Parameter Store と Automation は AWS Systems Manager のツールです。

[開始する前に]

Automation ロール、およびオプションで、Automation 用の Amazon EventBridge を設定します。詳細については、「オートメーションの設定」を参照してください。

内容

- タスク 1: Systems Manager Parameter Store でパラメータを作成する
- タスク 2: 用の IAM ロールを作成するAWS Lambda
- タスク 3: AWS Lambda 関数を作成する
- タスク 4: ランブックを作成し、AMI にパッチを適用する

タスク 1: Systems Manager Parameter Store でパラメータを作成する

Parameter Store で以下の情報を使用する文字列パラメータを作成します。

- Name (名前)`latestAmi`]: 。
- 値: AMI ID。例: `ami-188d6e0e`。

Parameter Store の文字列パラメータの作成方法については、「Systems Manager での Parameter Store パラメータの作成」を参照してください。

タスク 2: 用の IAM ロールを作成するAWS Lambda

の IAM サービスロールを作成するために、次の手順を使用しますAWS Lambda これらのポリシーは、Lambda に Lambda 関数および Systems Manager を使用して、`latestAmi` パラメータの値を更新する権限を与えます。

Lambda の IAM サービスロールを作成するには

1. AWS Management Console にサインインして、IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. ナビゲーションペインで、[Policies] を選択し、次に [Create policy] を選択します。
3. [JSON] タブを選択します。
4. デフォルトのコンテンツを次のポリシーに置き換えます。各*###############*をユーザー自身の情報に置き換えます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "logs:CreateLogGroup",
            "Resource": "arn:aws:logs:region:123456789012:*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:region:123456789012:log-group:/aws/lambda/function
 name:*"
            ]
        }
    ]
}
```

5. [Next: Tags] (次へ: タグ) を選択します。

6. (オプション) 1 つ以上のタグキーと値のペアを追加して、このポリシーのアクセスを整理、追跡、または制御します。
7. [次へ: レビュー] を選択します。
8. [Review policy (ポリシーの確認)] ページで、[Name (名前)] にインラインポリシーの名前を入力します (**amiLambda** など)。
9. [Create policy] を選択します。
10. ステップ 2 と 3 を繰り返します。
11. 次のポリシーを貼り付けます。各*##############*をユーザー自身の情報に置き換えます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ssm:PutParameter",
            "Resource": "arn:aws:ssm:region:123456789012:parameter/latestAmi"
        },
        {
            "Effect": "Allow",
            "Action": "ssm:DescribeParameters",
            "Resource": "*"
        }
    ]
}
```

12. [Next: Tags] (次へ: タグ) を選択します。
13. (オプション) 1 つ以上のタグキーと値のペアを追加して、このポリシーのアクセスを整理、追跡、または制御します。
14. [次へ: レビュー] を選択します。
15. [Review policy (ポリシーの確認)] ページで、[Name (名前)] にインラインポリシーの名前を入力します (**amiParameter** など)。
16. [Create policy] を選択します。
17. ナビゲーションペインで [Roles] を選択し、続いて [Create role] を選択します。
18. [ユースケース] のすぐ下で、[Lambda]、[次へ] の順に選択します。
19. [アクセス許可の追加] ページで [検索] フィールドを使用し、前に作成した 2 つのポリシーを見つけます。
20. ポリシーの横にあるチェックボックスをオンにして、[次へ] を選択します。

21. [ロール名] に、新しいロールの名前を入力 (**lambda-ssm-role** など) するか、希望する別の名前を入力します。

> **Note**
>
> 多くのエンティティによりロールが参照されるため、作成後にロール名を変更することはできません。

22. (オプション) 1 つ以上のタグキーと値のペアを追加して、このロールのアクセスを整理、追跡、制御し、[ロールの作成] を選択します。

タスク 3: AWS Lambda 関数を作成する

`latestAmi` パラメータの値を自動的に更新する Lambda 関数を作成するには、次の手順を使用します。

Lambda 関数を作成するには

1. AWS Management Console にサインインして AWS Lambda コンソール (https://console.aws.amazon.com/lambda/) を開きます。
2. [Create function] を選択します。
3. [Create function] ページで、[Author from scratch] を選択します。
4. [関数名] に「**Automation-UpdateSsmParam**」と入力します。
5. ランタイム] では、Python 3.8] を選択します。
6. [アーキテクチャ] で、関数の実行に使用する Lambda のコンピュータープロセッサーのタイプ、[x86_64] または [arm64] を選択します。
7. [アクセス許可] セクションで、[デフォルトの実行ロールの変更] を展開します。
8. [Use an existing role (既存のロールの使用)] を選択し、タスク 2 で作成した Lambda のサービスロールを選択します。
9. [Create function] を選択します。
10. [コードソース] 領域の [lambda_function] タブで、フィールドにあらかじめ入力されているコードを削除し、次のコードサンプルを貼り付けます。

```
from __future__ import print_function

import json
import boto3
```

```
print('Loading function')


#Updates an SSM parameter
#Expects parameterName, parameterValue
def lambda_handler(event, context):
    print("Received event: " + json.dumps(event, indent=2))

    # get SSM client
    client = boto3.client('ssm')

    #confirm  parameter exists before updating it
    response = client.describe_parameters(
       Filters=[
          {
           'Key': 'Name',
           'Values': [ event['parameterName'] ]
          },
        ]
    )

    if not response['Parameters']:
        print('No such parameter')
        return 'SSM parameter not found.'

    #if parameter has a Description field, update it PLUS the Value
    if 'Description' in response['Parameters'][0]:
        description = response['Parameters'][0]['Description']

        response = client.put_parameter(
          Name=event['parameterName'],
          Value=event['parameterValue'],
          Description=description,
          Type='String',
          Overwrite=True
        )

    #otherwise just update Value
    else:
        response = client.put_parameter(
          Name=event['parameterName'],
          Value=event['parameterValue'],
          Type='String',
```

```
            Overwrite=True
        )

    responseString = 'Updated parameter %s with value %s.' %
 (event['parameterName'], event['parameterValue'])

    return responseString
```

11. [ファイル]、[保存] の順に選択します。
12. Lambda 関数をテストするには、[テスト] メニューで、[テストイベントの設定] を選択します。
13. [Event name] で、**MyTestEvent** など、テストイベントの名前を入力します。
14. 既存のテキストを次の JSON に置き換えます。*[AMI ID]* をユーザー自身の情報に置き換え、latestAmi パラメータ値を設定します。

```
{
   "parameterName":"latestAmi",
   "parameterValue":"AMI ID"
}
```

15. [Save] を選択します。
16. [テスト (Test)] を選択して関数をテストします。[実行結果] タブに、更新に関するその他の詳細とともに、ステータスが [成功] として報告されます。

タスク 4: ランブックを作成し、AMI にパッチを適用する

以下の手順を使用して、[latestAmi] パラメータに指定した AMI にパッチを適用したランブックを作成して実行します。オートメーションが完了すると、latestAmi の値は、新しくパッチ適用された AMI の ID で更新されます。以降のオートメーションは、以前の実行で作成された AMI を使用します。

ランブックを作成して実行するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[ドキュメント] を選択します。
3. [ドキュメントの作成] で [オートメーション] を選択します。
4. [名前] に**UpdateMyLatestWindowsAmi**と入力してください。
5. [Editor (エディタ)] タブを選択し、次に [Edit (編集)] を選択します。

6. プロンプトが表示されたら、[OK] を選択します。
7. [ドキュメントエディタ] フィールドで、デフォルトのコンテンツを、次の YAML サンプルランブックコンテンツに置き換えます。

```
---
description: Systems Manager Automation Demo - Patch AMI and Update ASG
schemaVersion: '0.3'
assumeRole: '{{ AutomationAssumeRole }}'
parameters:
  AutomationAssumeRole:
    type: String
    description: '(Required) The ARN of the role that allows Automation to perform
 the actions on your behalf. If no role is specified, Systems Manager Automation
 uses your IAM permissions to execute this document.'
    default: ''
  SourceAMI:
    type: String
    description: The ID of the AMI you want to patch.
    default: '{{ ssm:latestAmi }}'
  SubnetId:
    type: String
    description: The ID of the subnet where the instance from the SourceAMI
 parameter is launched.
  SecurityGroupIds:
    type: StringList
    description: The IDs of the security groups to associate with the instance
 that's launched from the SourceAMI parameter.
  NewAMI:
    type: String
    description: The name of of newly patched AMI.
    default: 'patchedAMI-{{global:DATE_TIME}}'
  InstanceProfile:
    type: String
    description: The name of the IAM instance profile you want the source instance
 to use.
  SnapshotId:
    type: String
    description: (Optional) The snapshot ID to use to retrieve a patch baseline
 snapshot.
    default: ''
  RebootOption:
    type: String
```

```
    description: '(Optional) Reboot behavior after a patch Install operation. If
 you choose NoReboot and patches are installed, the instance is marked as non-
compliant until a subsequent reboot and scan.'
    allowedValues:
      - NoReboot
      - RebootIfNeeded
    default: RebootIfNeeded
  Operation:
    type: String
    description: (Optional) The update or configuration to perform on the instance.
 The system checks if patches specified in the patch baseline are installed on the
 instance. The install operation installs patches missing from the baseline.
    allowedValues:
      - Install
      - Scan
    default: Install
mainSteps:
  - name: startInstances
    action: 'aws:runInstances'
    timeoutSeconds: 1200
    maxAttempts: 1
    onFailure: Abort
    inputs:
      ImageId: '{{ SourceAMI }}'
      InstanceType: m5.large
      MinInstanceCount: 1
      MaxInstanceCount: 1
      IamInstanceProfileName: '{{ InstanceProfile }}'
      SubnetId: '{{ SubnetId }}'
      SecurityGroupIds: '{{ SecurityGroupIds }}'
  - name: verifyInstanceManaged
    action: 'aws:waitForAwsResourceProperty'
    timeoutSeconds: 600
    inputs:
      Service: ssm
      Api: DescribeInstanceInformation
      InstanceInformationFilterList:
        - key: InstanceIds
          valueSet:
            - '{{ startInstances.InstanceIds }}'
      PropertySelector: '$.InstanceInformationList[0].PingStatus'
      DesiredValues:
        - Online
    onFailure: 'step:terminateInstance'
```

```
  - name: installPatches
    action: 'aws:runCommand'
    timeoutSeconds: 7200
    onFailure: Abort
    inputs:
      DocumentName: AWS-RunPatchBaseline
      Parameters:
        SnapshotId: '{{SnapshotId}}'
        RebootOption: '{{RebootOption}}'
        Operation: '{{Operation}}'
      InstanceIds:
        - '{{ startInstances.InstanceIds }}'
  - name: stopInstance
    action: 'aws:changeInstanceState'
    maxAttempts: 1
    onFailure: Continue
    inputs:
      InstanceIds:
        - '{{ startInstances.InstanceIds }}'
      DesiredState: stopped
  - name: createImage
    action: 'aws:createImage'
    maxAttempts: 1
    onFailure: Continue
    inputs:
      InstanceId: '{{ startInstances.InstanceIds }}'
      ImageName: '{{ NewAMI }}'
      NoReboot: false
      ImageDescription: Patched AMI created by Automation
  - name: terminateInstance
    action: 'aws:changeInstanceState'
    maxAttempts: 1
    onFailure: Continue
    inputs:
      InstanceIds:
        - '{{ startInstances.InstanceIds }}'
      DesiredState: terminated
  - name: updateSsmParam
    action: aws:invokeLambdaFunction
    timeoutSeconds: 1200
    maxAttempts: 1
    onFailure: Abort
    inputs:
        FunctionName: Automation-UpdateSsmParam
```

```
        Payload: '{"parameterName":"latestAmi",
 "parameterValue":"{{createImage.ImageId}}"}'
outputs:
- createImage.ImageId
```

8. [Create automation (オートメーションを作成)] を選択します。
9. ナビゲーションペインで、[オートメーション]、[オートメーションの実行] の順に選択します。
10. [Choose document] (ドキュメントを選択) ページで、[Owned by me] (自分が所有) タブを選択します。
11. UpdateMyLatestWindowsAmi ランブックを検索し、UpdateMyLatestWindowsAmi カードのボタンを選択します。
12. [Next] を選択します。
13. [Simple execution (シンプルな実行)] を選択します。
14. 入力パラメータの値を指定します。
15. [実行] を選択してください。
16. 実行の完了後に、ナビゲーションペインで [Parameter Store] を選択し、`latestAmi` の新しい値がオートメーションから返された値と一致することを確認します。新しい AMI ID が、Amazon EC2 コンソールの [AMIs] セクションに表示される Automation の出力と一致することを確認することもできます。

オートメーションと Jenkins を使用した AMIs の更新

CI/CD のパイプラインで Jenkins ソフトウェアを使用する組織では、オートメーションをビルド後のステップとして追加して、アプリケーションリリースを Amazon Machine Images (AMIs) に事前インストールできます。Automation は AWS Systems Manager のツールです。Jenkins のスケジューリング機能を使用して、オートメーションを呼び出し、独自のオペレーティングシステム (OS) への定期的なパッチ適用を作成することもできます。

以下の例は、オンプレミスまたは Amazon Elastic Compute Cloud (Amazon EC2) のいずれかで実行している Jenkins サーバーからオートメーションを呼び出す方法を示しています。Jenkins サーバーは、認証のために、この例で作成した IAM ポリシーに基づく AWS 認証情報を使用して、インスタンスプロファイルにアタッチします。

> **Note**
>
> インスタンスの設定時は、Jenkins のセキュリティについてのベストプラクティスに従う必要があります。

[開始する前に]

Jenkins を使用してオートメーションを設定する前に、次のタスクを完了します。

- Automation、AWS Lambda、Parameter Store を使用してゴールデン AMI を更新する の例を完了します。次の例では、この例で作成された UpdateMyLatestWindowsAmi ランブックを使用します。
- オートメーションの IAM ロールを設定します。Systems Manager には、オートメーションを処理するためのインスタンスプロファイルのロールおよびサービスロールの ARN が必要です。詳細については、「オートメーションの設定」を参照してください。

Jenkins サーバーで IAM ポリシーを作成するには

1. AWS Management Console にサインインして、IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. ナビゲーションペインで、[Policies] を選択し、次に [Create policy] を選択します。
3. [JSON] タブを選択します。
4. 各##############をユーザー自身の情報に置き換えます。

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Effect": "Allow",
                "Action": "ssm:StartAutomationExecution",
                "Resource": [
                    "arn:aws:ssm:region:account ID:document/
UpdateMyLatestWindowsAmi",
                    "arn:aws:ssm:region:account ID:automation-definition/
UpdateMyLatestWindowsAmi:$DEFAULT"
                ]
            }
        ]
```

```
    }
```

5. [ポリシーの確認] を選択します。
6. [Review policy (ポリシーの確認)] ページで、[Name (名前)] にインラインポリシーの名前を入力します (**`JenkinsPolicy`** など)。
7. [Create policy] を選択します。
8. ナビゲーションペインで [ロール] を選択します。
9. Jenkins サーバーにアタッチされているインスタンスプロファイルを選択します。
10. [アクセス許可] タブで、[許可の追加]、[ポリシーのアタッチ] の順に選択します。
11. [その他のアクセス許可ポリシー] セクションで、前の手順で作成したポリシー名を入力します。例えば、[JenkinsPolicy] などです。
12. ポリシーの横にあるチェックボックスをオンにして、[ポリシーのアタッチ] を選択します。

Jenkins サーバーで AWS CLI を設定するには、次の手順を使用します。

オートメーション用に Jenkins サーバーを設定するには

1. 管理インターフェイスにアクセスするには、ご使用のブラウザを使用してポート 8080 で Jenkins サーバーに接続します。
2. `/var/lib/jenkins/secrets/initialAdminPassword` で見つかったパスワードを入力します。パスワードを表示するには、次のコマンドを実行します。

```
sudo cat /var/lib/jenkins/secrets/initialAdminPassword
```

3. Jenkins インストールスクリプトでは、[Jenkins のカスタマイズ] ページが表示されます。[Install suggested plugins (推奨プラグインをインストール)] を選択します。
4. インストールが完了したら、[管理者認証情報] を選択し、[認証情報を保存] を選択してから、[Jenkins の使用を開始] を選択します。
5. 左側のナビゲーションペインで、[Jenkins の管理]、[プラグインの管理] の順に選択します。
6. [Available (使用可能)] タブを選択し、**`Amazon EC2 plugin`** と入力します。
7. **`Amazon EC2 plugin`** のチェックボックスをオンにし、[Install without restart (再起動せずにインストール)] を選択します。
8. インストールが完了したら、[Go back to the top page (トップページに戻る)]を選択します。
9. [Jenkins の管理]、[ノードとクラドの管理] の順に選択します。
10. [クラウドの設定] セクションで [新しいクラウドの追加]、[Amazon EC2] の順に選択します。

11. 残りのフィールドに情報を入力します。必ず、[EC2 インスタンスプロファイルを使用して認証情報を取得] オプションを選択してください。

オートメーションを呼び出すように Jenkins プロジェクトを設定するには、次の手順を使用します。

オートメーションを呼び出すように Jenkins サーバー を設定するには

1. ウェブブラウザで、Jenkins コンソールを開きます。
2. Automation を使用して設定するプロジェクトを選択し、[Configure] を選択します。
3. [Build] タブで、[Add Build Step] を選択します。
4. [Execute shell] または [Execute Windows batch command] (オペレーティングシステムによって異なります) を選択します。
5. [Command] (コマンド)フィールドで、以下のように AWS CLI コマンドを実行します。各*##########*をユーザー自身の情報に置き換えます。

```
aws ssm start-automation-execution \
        --document-name runbook name \
        --region AWS ##### of your source AMI \
        --parameters runbook parameters
```

以下のサンプルコマンドは、UpdateMyLatestWindowsAmi ランブックや、`latestAmi` で作成された Systems Manager Parameter Automation、AWS Lambda、Parameter Store を使用してゴールデン AMI を更新する を使用しています。

```
aws ssm start-automation-execution \
        --document-name UpdateMyLatestWindowsAmi \
        --parameters \
            "sourceAMIid='{{ssm:latestAmi}}'"
        --region region
```

Jenkins では、コマンドは次のスクリーンショットの例のようになります。

6. Jenkins プロジェクトで、[今すぐビルド] を選択します。Jenkins は次の例のような出力を返します。

Auto Scaling グループ用の AMIs の更新

次の例では、新しくパッチが適用された AMI で Auto Scaling グループを更新します。このアプローチにより、Auto Scaling グループを使用するさまざまなコンピューティング環境で、新しいイメージが自動的に利用可能になります。

この例のオートメーションの最後のステップでは、Python 関数を使用して、新しくパッチが適用された AMI を使用する新しい起動テンプレートを作成します。その後、Auto Scaling グループが更新され、新しい起動テンプレートが使用されます。このタイプの Auto Scaling シナリオでは、ユーザーが Auto Scaling グループ内の既存のインスタンスを終了して、新しいイメージを使用する新しいインスタンスを強制的に起動できます。ユーザーは、スケールインまたはスケールアウトイベントが新しいインスタンスを自然に起動させるのを待つこともできます。

開始する前に

この例を開始する前に、次のタスクを完了してください。

- AWS Systems Manager のツールである Automation の IAM ロールを設定します。Systems Manager には、オートメーションを処理するためのインスタンスプロファイルのロールおよびサービスロールの ARN が必要です。詳しくは、「オートメーションの設定」を参照してください。

PatchAMIAndUpdateASG ランブックを作成する

次の手順を使用して、SourceAMI パラメータ向けに指定した AMI にパッチを適用する PatchAMIAndUpdateASG ランブックを作成します。ランブックは、Auto Scaling グループも更新して、パッチが適用された最新の AMI を使用するようにします。

ランブックを作成して実行するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[ドキュメント] を選択します。
3. [Create document (ドキュメントの作成)] ドロップダウンで [Automation (オートメーション)] を選択します。
4. [名前] フィールドに **PatchAMIAndUpdateASG** を入力してください。
5. [Editor] (エディタ) タブを選択し、次に [Edit] (編集) を選択します。
6. プロンプトが表示されたら [OK] を選択し、[Document editor] (ドキュメントエディタ) フィールドのコンテンツを削除します。
7. [Document editor] (ドキュメントエディタ) フィールドに、以下の YAML サンプルランブックコンテンツを貼り付けます。

```
---
description: Systems Manager Automation Demo - Patch AMI and Update ASG
schemaVersion: '0.3'
assumeRole: '{{ AutomationAssumeRole }}'
parameters:
  AutomationAssumeRole:
    type: String
    description: '(Required) The ARN of the role that allows Automation to perform
 the actions on your behalf. If no role is specified, Systems Manager Automation
 uses your IAM permissions to execute this document.'
    default: ''
  SourceAMI:
    type: String
```

```
    description: '(Required) The ID of the AMI you want to patch.'
  SubnetId:
    type: String
    description: '(Required) The ID of the subnet where the instance from the
 SourceAMI parameter is launched.'
  SecurityGroupIds:
    type: StringList
    description: '(Required) The IDs of the security groups to associate with the
 instance launched from the SourceAMI parameter.'
  NewAMI:
    type: String
    description: '(Optional) The name of of newly patched AMI.'
    default: 'patchedAMI-{{global:DATE_TIME}}'
  TargetASG:
    type: String
    description: '(Required) The name of the Auto Scaling group you want to
 update.'
  InstanceProfile:
    type: String
    description: '(Required) The name of the IAM instance profile you want the
 source instance to use.'
  SnapshotId:
    type: String
    description: (Optional) The snapshot ID to use to retrieve a patch baseline
 snapshot.
    default: ''
  RebootOption:
    type: String
    description: '(Optional) Reboot behavior after a patch Install operation. If
 you choose NoReboot and patches are installed, the instance is marked as non-
compliant until a subsequent reboot and scan.'
    allowedValues:
      - NoReboot
      - RebootIfNeeded
    default: RebootIfNeeded
  Operation:
    type: String
    description: (Optional) The update or configuration to perform on the instance.
 The system checks if patches specified in the patch baseline are installed on the
 instance. The install operation installs patches missing from the baseline.
    allowedValues:
      - Install
      - Scan
    default: Install
```

```
mainSteps:
  - name: startInstances
    action: 'aws:runInstances'
    timeoutSeconds: 1200
    maxAttempts: 1
    onFailure: Abort
    inputs:
      ImageId: '{{ SourceAMI }}'
      InstanceType: m5.large
      MinInstanceCount: 1
      MaxInstanceCount: 1
      IamInstanceProfileName: '{{ InstanceProfile }}'
      SubnetId: '{{ SubnetId }}'
      SecurityGroupIds: '{{ SecurityGroupIds }}'
  - name: verifyInstanceManaged
    action: 'aws:waitForAwsResourceProperty'
    timeoutSeconds: 600
    inputs:
      Service: ssm
      Api: DescribeInstanceInformation
      InstanceInformationFilterList:
        - key: InstanceIds
          valueSet:
            - '{{ startInstances.InstanceIds }}'
      PropertySelector: '$.InstanceInformationList[0].PingStatus'
      DesiredValues:
        - Online
    onFailure: 'step:terminateInstance'
  - name: installPatches
    action: 'aws:runCommand'
    timeoutSeconds: 7200
    onFailure: Abort
    inputs:
      DocumentName: AWS-RunPatchBaseline
      Parameters:
        SnapshotId: '{{SnapshotId}}'
        RebootOption: '{{RebootOption}}'
        Operation: '{{Operation}}'
      InstanceIds:
        - '{{ startInstances.InstanceIds }}'
  - name: stopInstance
    action: 'aws:changeInstanceState'
    maxAttempts: 1
    onFailure: Continue
```

```
    inputs:
      InstanceIds:
        - '{{ startInstances.InstanceIds }}'
      DesiredState: stopped
  - name: createImage
    action: 'aws:createImage'
    maxAttempts: 1
    onFailure: Continue
    inputs:
      InstanceId: '{{ startInstances.InstanceIds }}'
      ImageName: '{{ NewAMI }}'
      NoReboot: false
      ImageDescription: Patched AMI created by Automation
  - name: terminateInstance
    action: 'aws:changeInstanceState'
    maxAttempts: 1
    onFailure: Continue
    inputs:
      InstanceIds:
        - '{{ startInstances.InstanceIds }}'
      DesiredState: terminated
  - name: updateASG
    action: 'aws:executeScript'
    timeoutSeconds: 300
    maxAttempts: 1
    onFailure: Abort
    inputs:
      Runtime: python3.8
      Handler: update_asg
      InputPayload:
        TargetASG: '{{TargetASG}}'
        NewAMI: '{{createImage.ImageId}}'
      Script: |-
        from __future__ import print_function
        import datetime
        import json
        import time
        import boto3

        # create auto scaling and ec2 client
        asg = boto3.client('autoscaling')
        ec2 = boto3.client('ec2')

        def update_asg(event, context):
```

```
            print("Received event: " + json.dumps(event, indent=2))

            target_asg = event['TargetASG']
            new_ami = event['NewAMI']

            # get object for the ASG we're going to update, filter by name of
 target ASG
            asg_query =
 asg.describe_auto_scaling_groups(AutoScalingGroupNames=[target_asg])
            if 'AutoScalingGroups' not in asg_query or not
 asg_query['AutoScalingGroups']:
                return 'No ASG found matching the value you specified.'

            # gets details of an instance from the ASG that we'll use to model the
 new launch template after
            source_instance_id = asg_query.get('AutoScalingGroups')[0]['Instances']
[0]['InstanceId']
            instance_properties = ec2.describe_instances(
                InstanceIds=[source_instance_id]
            )
            source_instance = instance_properties['Reservations'][0]['Instances']
[0]

            # create list of security group IDs
            security_groups = []
            for group in source_instance['SecurityGroups']:
                security_groups.append(group['GroupId'])

            # create a list of dictionary objects for block device mappings
            mappings = []
            for block in source_instance['BlockDeviceMappings']:
                volume_query = ec2.describe_volumes(
                    VolumeIds=[block['Ebs']['VolumeId']]
                )
                volume_details = volume_query['Volumes']
                device_name = block['DeviceName']
                volume_size = volume_details[0]['Size']
                volume_type = volume_details[0]['VolumeType']
                device = {'DeviceName': device_name, 'Ebs': {'VolumeSize':
 volume_size, 'VolumeType': volume_type}}
                mappings.append(device)

            # create new launch template using details returned from instance in
 the ASG and specify the newly patched AMI
```

```
            time_stamp = time.time()
            time_stamp_string =
 datetime.datetime.fromtimestamp(time_stamp).strftime('%m-%d-%Y_%H-%M-%S')
            new_template_name = f'{new_ami}_{time_stamp_string}'
            try:
                ec2.create_launch_template(
                    LaunchTemplateName=new_template_name,
                    LaunchTemplateData={
                        'BlockDeviceMappings': mappings,
                        'ImageId': new_ami,
                        'InstanceType': source_instance['InstanceType'],
                        'IamInstanceProfile': {
                            'Arn': source_instance['IamInstanceProfile']['Arn']
                        },
                        'KeyName': source_instance['KeyName'],
                        'SecurityGroupIds': security_groups
                    }
                )
            except Exception as e:
                return f'Exception caught: {str(e)}'
            else:
                # update ASG to use new launch template
                asg.update_auto_scaling_group(
                    AutoScalingGroupName=target_asg,
                    LaunchTemplate={
                        'LaunchTemplateName': new_template_name
                    }
                )
                return f'Updated ASG {target_asg} with new launch template
 {new_template_name} which uses AMI {new_ami}.'
outputs:
  - createImage.ImageId
```

8. [Create automation (オートメーションを作成)] を選択します。
9. ナビゲーションペインで、[オートメーション]、[オートメーションの実行] の順に選択します。
10. [Choose document] (ドキュメントを選択) ページで、[Owned by me] (自分が所有) タブを選択します。
11. PatchAMIAndUpdateASG ランブックを検索し、PatchAMIAndUpdateASG カードのボタンを選択します。
12. [Next] を選択します。
13. [Simple execution (シンプルな実行)] を選択します。

14. 入力パラメータの値を指定します。指定する SubnetId と SecurityGroupIds が、パブリック Systems Manager エンドポイント、または Systems Manager のインターフェイスエンドポイントへのアクセスを許可していることを確認してください。
15. [実行] を選択してください。
16. オートメーションが完了したら、Amazon EC2 コンソールで [Auto Scaling]、[Launch Templates] (テンプレートを起動) の順に選択します。新しい起動テンプレートが表示され、新しい AMI を使用していることを確認します。
17. [Auto Scaling]、[Auto Scaling グループ] の順に選択します。Auto Scaling グループで新しい起動テンプレートが使用されていることを確認します。
18. Auto Scaling グループ内の 1 つ以上のインスタンスを終了します。代替インスタンスは、新しい AMI を使用して起動されます。

AWS サポート でのセルフサービスランブックの使用

このセクションでは、AWS サポート チームによって作成されたセルフサービスオートメーションの一部を使用する方法について説明します。このオートメーションは、AWS リソースの管理に役立ちます。

サポートオートメーションワークフロー

サポートオートメーションワークフロー (SAW) は、AWS サポート チームによって作成および保守されるオートメーションランブックです。このランブックは、AWS リソースに関する一般的な問題のトラブルシューティング、ネットワーク問題のプロアクティブなモニタリングと特定、ログの収集と分析などを支援します。

SAW ランブックは、**AWSSupport** プレフィックスを使用します。例えば、AWSSupport-ActivateWindowsWithAmazonLicense と指定します。

さらに、AWS エンタープライズおよびビジネスサポートのお客様は、**AWSPremiumSupport** プレフィックスを使用するランブックにもアクセスできます。例えば、AWSPremiumSupport-TroubleshootEC2DiskUsage と指定します。

AWS サポート の詳細については、「AWS サポート の開始方法」を参照してください。

トピック

- 到達不可能なインスタンスでの EC2Rescue ツールの実行
- EC2 インスタンスでのパスワードと SSH キーのリセット

到達不可能なインスタンスでの EC2Rescue ツールの実行

EC2Rescue は、Linux および Windows Server 用の Amazon Elastic Compute Cloud (Amazon EC2) インスタンスの問題の診断とトラブルシューティングに役立ちます。ツールを手動で実行するには、「Linux Server 用 EC2Rescue の使用」と「EC2Rescue for Windows Server の使用」を参照してください。または、ツールを自動的に実行するには、Systems Manager Automation と **AWSSupport-ExecuteEC2Rescue** ランブックを使用します。Automation は AWS Systems Manager のツールです。**AWSSupport-ExecuteEC2Rescue** ランブックは、Systems Manager アクション、AWS CloudFormation アクション、および Lambda 関数を組み合わせて実行するように設計されています。これにより、EC2Rescue の使用に通常必要なステップが自動化されます。

AWSSupport-ExecuteEC2Rescue ランブックでは、オペレーティングシステム (OS) のタイプ別にトラブルシューティングを行い、問題を修正できます。暗号化されたルートボリュームを持つインスタンスはサポートされていません。詳細なリストについては、以下のトピックを参照してください。

Windows: 「コマンドラインでの EC2Rescue for Windows Server の使用」の「レスキューアクション」を参照してください。

Linux および macOS: 一部の Linux 用 EC2Rescue モジュールでは、問題を検出して修正を試みます。詳細については、GitHub で モジュール別の `aws-ec2rescue-linux` ドキュメントを参照してください。

仕組み

Automation と **AWSSupport-ExecuteEC2Rescue** ランブックによるインスタンスのトラブルシューティングは、次のように機能します。

- 到達不能インスタンスの ID を指定し、ランブックを起動します。
- システムは一時 VPC を作成し、一連の Lambda 関数を実行して VPC を設定します。
- システムは元のインスタンスと同じアベイラビリティーゾーン内で一時 VPC のサブネットを識別します。
- システムは一時的な、SSM を有効にした ヘルパーインスタンスを起動します。
- システムは元のインスタンスを停止して、バックアップを作成します。次に、元のルートボリュームをヘルパーインスタンスにアタッチします。
- システムは、Run Command を使用してヘルパーインスタンスで EC2Rescue を実行します。EC2Rescue は、アタッチされた元のルートボリュームの問題の修正を試みます。完了すると、EC2Rescue は元のインスタンスにルートボリュームを再アタッチします。

- システムは元のインスタンスを再起動して、一時インスタンスを削除します。また、一時 VPC と、自動化の開始時に作成された Lambda 関数を削除します。

開始する前に

次の自動化を実行する前に、以下の操作を行います。

- 到達不可能なインスタンスのインスタンス ID をコピーします。この ID は次の手順で指定します。
- オプションとして、到達不可能なインスタンスと同じアベイラビリティーゾーンのサブネットの ID を収集します。このサブネットに EC2Rescue インスタンスが作成されます。サブネットを指定しないと、Automation により、新しい一時 VPC が に作成されますAWS アカウント AWS アカウント に、少なくとも 1 つの利用可能な VPC があることを確認します。デフォルトでは、リージョンで最大 5 つの VPC を作成できます。リージョンですでに 5 つの VPC を作成した場合、自動化は失敗し、インスタンスへの変更は行われません。Amazon VPC クォータの詳細については、「Amazon VPC ユーザーガイド」の「VPC とサブネット」を参照してください。
- 必要に応じて、自動化用の AWS Identity and Access Management (IAM) ロールを作成および指定できます。このロールを指定しない場合、自動化はそれを実行したユーザーのコンテキストで実行されます。

インスタンスでアクションを実行するための **AWSSupport-EC2Rescue** アクセス許可の付与

EC2Rescue では、オートメーション中にインスタンスで一連のアクションを実行するためのアクセス許可が必要です。これらのアクションでは、AWS Lambda、IAM、および Amazon EC2 サービスを呼び出して、インスタンスの問題の安全な修正を試みます。AWS アカウント、VPC、またはその両方で管理者レベルのアクセス許可がある場合は、このセクションで説明しているように、アクセス許可を設定することなく自動化を実行できることがあります。管理者レベルのアクセス許可がない場合は、ユーザーまたは管理者が、次のいずれかのオプションを使用してアクセス許可を設定する必要があります。

- IAM ポリシーを使用したアクセス許可の付与
- AWS CloudFormation テンプレートを使用したアクセス権限の付与

IAM ポリシーを使用したアクセス許可の付与

次の IAM ポリシーをユーザー、グループ、ロールにインラインポリシーとしてアタッチするか、新しい IAM マネージドポリシーを作成し、ユーザー、グループ、ロールにアタッチできます。ユー

ザー、グループ、ロールへのインラインポリシーの追加の詳細については、「インラインポリシーの使用」を参照してください。新しい管理ポリシーの作成の詳細については、「管理ポリシーの使用」を参照してください。

> **Note**
>
> 新しい IAM 管理ポリシーを作成する場合、AmazonSSMAutomationRole 管理ポリシーもアタッチし、インスタンスが Systems Manager API と通信できるようにする必要があります。

AWSSupport-EC2Rescue 用の IAM ポリシー

[Account ID] (アカウント ID) をユーザー自身の情報に置き換えます。

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Action": [
            "lambda:InvokeFunction",
            "lambda:DeleteFunction",
            "lambda:GetFunction"
         ],
         "Resource": "arn:aws:lambda:*:account ID:function:AWSSupport-EC2Rescue-*",
         "Effect": "Allow"
      },
      {
         "Action": [
            "s3:GetObject",
            "s3:GetObjectVersion"
         ],
         "Resource": [
            "arn:aws:s3:::awssupport-ssm.*/*.template",
            "arn:aws:s3:::awssupport-ssm.*/*.zip"
         ],
         "Effect": "Allow"
      },
      {
         "Action": [
            "iam:CreateRole",
            "iam:CreateInstanceProfile",
            "iam:GetRole",
```

```
            "iam:GetInstanceProfile",
            "iam:PutRolePolicy",
            "iam:DetachRolePolicy",
            "iam:AttachRolePolicy",
            "iam:PassRole",
            "iam:AddRoleToInstanceProfile",
            "iam:RemoveRoleFromInstanceProfile",
            "iam:DeleteRole",
            "iam:DeleteRolePolicy",
            "iam:DeleteInstanceProfile"
         ],
         "Resource": [
            "arn:aws:iam::account ID:role/AWSSupport-EC2Rescue-*",
            "arn:aws:iam::account ID:instance-profile/AWSSupport-EC2Rescue-*"
         ],
         "Effect": "Allow"
      },
      {
         "Action": [
            "lambda:CreateFunction",
            "ec2:CreateVpc",
            "ec2:ModifyVpcAttribute",
            "ec2:DeleteVpc",
            "ec2:CreateInternetGateway",
            "ec2:AttachInternetGateway",
            "ec2:DetachInternetGateway",
            "ec2:DeleteInternetGateway",
            "ec2:CreateSubnet",
            "ec2:DeleteSubnet",
            "ec2:CreateRoute",
            "ec2:DeleteRoute",
            "ec2:CreateRouteTable",
            "ec2:AssociateRouteTable",
            "ec2:DisassociateRouteTable",
            "ec2:DeleteRouteTable",
            "ec2:CreateVpcEndpoint",
            "ec2:DeleteVpcEndpoints",
            "ec2:ModifyVpcEndpoint",
            "ec2:Describe*",
            "autoscaling:DescribeAutoScalingInstances"
         ],
         "Resource": "*",
         "Effect": "Allow"
      }
```

```
    ]
}
```

AWS CloudFormation テンプレートを使用したアクセス権限の付与

AWS CloudFormation は事前設定されたテンプレートを使用して、IAM ロールとポリシーを作成するプロセスを自動化します。 を使用して、EC2Rescue の Automation に必要な IAM ロールとポリシーを作成するには、次の手順を使用しますAWS CloudFormation

EC2Rescue に必要な IAM ロールとポリシーを作成するには

1. AWSSupport-EC2RescueRole.zip をダウンロードし、AWSSupport-EC2RescueRole.json ファイルをローカルマシン上のディレクトリに展開します。
2. AWS アカウント が特殊なパーティションにある場合は、テンプレートを編集して、ARN 値をパーティションの ARN 値に変更します。

   例えば、中国リージョンの場合は、arn:aws のすべてのケースを arn:aws-cn に変更します。
3. AWS Management Console にサインインし、AWS CloudFormation コンソール (https://console.aws.amazon.com/cloudformation) を開きます。
4. [スタックの作成] を選択し、[新しいリソースの使用 (標準)] を選択します。
5. [スタックの作成] ページの [前提条件 - テンプレートの準備] で、[テンプレートの準備完了] を選択します。
6. [テンプレートの指定] で、[テンプレートファイルのアップロード] を選択します。
7. [ファイルを選択] を選択し、展開したディレクトリから AWSSupport-EC2RescueRole.json ファイルを参照して選択します。
8. [次へ] を選択します。
9. [スタックの詳細の指定] ページの [スタック名] フィールドに、このスタックを識別する名前を入力し、[次へ] を選択します。
10. (オプション) [タグ] 領域で、1 つ以上のタグキーの名前と値のペアをスタックに適用します。

    タグは、リソースに割り当てるオプションのメタデータです。タグを使用すると、目的、所有者、環境などのさまざまな方法でリソースを分類できます。たとえば、スタックにタグを付けると、スタックが実行するタスクのタイプ、関連するターゲットまたはその他のリソースのタイプ、およびスタックが実行される環境を識別できます。
11. [Next] (次へ) を選択します。

12. [確認] ページでスタックの詳細を確認し、下にスクロールして、[AWS CloudFormation によって IAM リソースが作成される場合があることを了承する] オプションを選択します。
13. [スタックの作成] を選択します。

    AWS CloudFormation は、[CREATE_IN_PROGRESS] ステータスを数分間表示します。スタックを作成すると、ステータスは [CREATE_COMPLETE] に変わります。更新アイコンを選択して、作成プロセスのステータスを確認することもできます。
14. [スタック] リストで、先ほど作成したスタックのオプションボタンを選択し、[出力] タブを選択します。
15. [値] を書き留めます。これは AssumeRole の ARN です。この ARN は、手順 自動化の実行 でオートメーションを実行するときに指定します。

自動化の実行

> **Important**
>
> 次のオートメーションでは、到達不可能なインスタンスを停止します。インスタンスを停止すると、アタッチされたインスタンスストアボリュームのデータが失われます (存在する場合)。また、インスタンスを停止すると、Elastic IP が関連付けられていない場合、そのパブリック IP アドレスも変更されます。

`AWSSupport-ExecuteEC2Rescue` Automation を実行するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで [オートメーション] を選択します。
3. [オートメーションを実行] を選択します。
4. オートメーションドキュメント] セクションで、リストから [Amazon が所有] を選択します。
5. ランブックリストで、**`AWSSupport-ExecuteEC2Rescue`** のカード内のボタンを選択し、[次へ] を選択します。
6. [オートメーションドキュメントの実行] ページで、[シンプルな実行] を選択します。
7. [ドキュメント詳細] セクションで、[ドキュメントバージョン] が最大のデフォルトバージョンに設定されていることを確認します。例えば、[$DEFAULT] または [3 (デフォルト)] のように指定します。

8. [パラメータの入力] セクションで、以下のパラメータを指定します。

   a. [UnreachableInstanceId] で、到達不可能なインスタンスの ID を指定します。

   b. (オプション) [EC2RescueInstanceType] で、EC2Rescue インスタンスのインスタンスタイプを指定します。デフォルトのインスタンスタイプは `t2.medium` です。

   c. [AutomationAssumeRole] の場合、このトピックで前述した AWS CloudFormation 手順を使用してこのオートメーションのロールを作成していた場合は、AWS CloudFormation コンソールで作成した AssumeRole の ARN を選択します。

   d. (オプション) インスタンスのトラブルシューティング時にオペレーティングシステムレベルのログを収集する場合は、[LogDestination] で S3 バケットを指定します。ログは、指定したバケットに自動的にアップロードされます。

   e. [SubnetId] で、到達不可能なインスタンスと同じアベイラビリティーゾーンの既存の VPC のサブネットを指定します。デフォルトでは、Systems Manager によって新しい VPC が作成されますが、必要に応じて既存の VPC のサブネットを指定できます。

   > **Note**
   >
   > バケットまたはサブネット ID を指定するオプションが表示されない場合は、最新の [デフォルト] バージョンのランブックを使用していることを確認します。

9. (オプション) [タグ] 領域で、オートメーションを識別するためにタグキーの名前と値のペアを 1 つ以上適用します (例: `Key=Purpose,Value=EC2Rescue`)。

10. [実行] を選択します。

ランブックにより、オートメーションの一環としてバックアップ AMI が作成されます。オートメーションで作成された他のすべてのリソースは自動的に削除されますが、この AMI はアカウントに残ります。AMI の名前は次の命名規則に従います。

バックアップ AMI: AWSSupport-EC2Rescue:*`UnreachableInstanceId`*

この AMI は、Automation の実行 ID で検索することで、Amazon EC2 コンソールで見つけることができます。

EC2 インスタンスでのパスワードと SSH キーのリセット

`AWSSupport-ResetAccess` ランブックを使用して、Windows Server 用の Amazon Elastic Compute Cloud (Amazon EC2) インスタンスでローカル管理者パスワード生成を自動的に再有効化し、Linux 用の EC2 インスタンスで新しい SSH キーを生成できます。`AWSSupport-ResetAccess`

ランブックは、AWS Systems Manager アクション、AWS CloudFormation アクション、および AWS Lambda 関数の組み合わせを実行することで、ローカル管理者パスワードのリセットに通常必要なステップを自動化するよう設計されています。

AWS Systems Manager のツールである Automation を使用して、`AWSSupport-ResetAccess` ランブックで、以下の問題を解決できます。

Windows

EC2 キーペアを紛失した場合: この問題を解決するには、AWSSupport-ResetAccess ランブックを使用して現在のインスタンスからパスワード対応の AMI を作成し、この AMI から新しいインスタンスを起動して、所有するキーペアを選択します。

ローカル管理者パスワードを紛失した場合: この問題を解決するには、`AWSSupport-ResetAccess` ランブックを使用して、現在の EC2 キーペアで復号できる新しいパスワードを生成できます。

Linux

EC2 キーペアを紛失したか、インスタンスへの SSH アクセスを設定したキーを紛失した場合: この問題を解決するには、`AWSSupport-ResetAccess` ランブックを使用し、現在のインスタンス用に新しい SSH キーを作成することで、インスタンスに再接続できます。

> **Note**
>
> Windows Server の EC2 インスタンスが Systems Manager 用に設定されている場合、EC2Rescue と AWS Systems Manager Run Command を使用してローカル管理者パスワードをリセットすることもできます。詳細については、「Amazon EC2 ユーザーガイド」の「EC2Rescue for Windows Server を Systems Manager の Run Command で使用する」を参照してください。

関連情報

「Amazon EC2 ユーザーガイド」の「PuTTY を使用した Windows から Linux インスタンスへの接続」

仕組み

Automation と `AWSSupport-ResetAccess` ランブックによるインスタンスのトラブルシューティングは、次のように機能します。

- インスタンスの ID を指定して、ランブックを実行します。
- システムは一時 VPC を作成し、一連の Lambda 関数を実行して VPC を設定します。
- システムは元のインスタンスと同じアベイラビリティーゾーン内で一時 VPC のサブネットを識別します。
- システムは一時的な、SSM を有効にした ヘルパーインスタンスを起動します。
- システムは元のインスタンスを停止して、バックアップを作成します。次に、元のルートボリュームをヘルパーインスタンスにアタッチします。
- システムは、Run Command を使用してヘルパーインスタンスで EC2Rescue を実行します。Windows の場合、EC2Rescue は、アタッチされた元のルートボリュームで EC2Config または EC2Launch を使用することで、ローカル管理者のパスワード生成を有効にします。Linux の場合、EC2Rescue は新しい SSH キーを生成して挿入し、プライベートキーで暗号化して Parameter Store に保存します。完了すると、EC2Rescue は元のインスタンスにルートボリュームを再アタッチします。
- パスワード生成が有効になっているため、システムはインスタンスの新しい Amazon Machine Image (AMI) を作成します。この AMI を使用して新しい EC2 インスタンスを作成し、必要に応じて新しいキーペアを関連付けます。
- システムは元のインスタンスを再起動して、一時インスタンスを削除します。また、一時 VPC と、自動化の開始時に作成された Lambda 関数を削除します。
- Windows: インスタンスでは、それに割り当てられている現在のキーペアを使用して Amazon EC2 コンソールから復号できる新しいパスワードを生成します。

  Linux: SSH を通じてインスタンスと通信できます。これには、Systems Manager Parameter Store に保存されている SSH キー (/ec2rl/openssh/***instance ID***/key) を使用します。

[開始する前に]

次の自動化を実行する前に、以下の操作を行います。

- 管理者パスワードをリセットするインスタンスのインスタンス ID をコピーします。この ID は次の手順で指定します。
- オプションとして、到達不可能なインスタンスと同じアベイラビリティーゾーンのサブネットの ID を収集します。このサブネットに EC2Rescue インスタンスが作成されます。サブネットを指定しないと、Automation により、新しい一時 VPC が に作成されますAWS アカウント AWS アカウント に、少なくとも 1 つの利用可能な VPC があることを確認します。デフォルトでは、リージョンで最大 5 つの VPC を作成できます。リージョンですでに 5 つの VPC を作成した場合、

自動化は失敗し、インスタンスへの変更は行われません。Amazon VPC クォータの詳細については、「Amazon VPC ユーザーガイド」の「VPC とサブネット」を参照してください。

- 必要に応じて、自動化用の AWS Identity and Access Management (IAM) ロールを作成および指定できます。このロールを指定しない場合、自動化はそれを実行したユーザーのコンテキストで実行されます。

インスタンスでアクションを実行するための AWSSupport-EC2Rescue アクセス許可の付与

EC2Rescue では、オートメーション中にインスタンスで一連のアクションを実行するためのアクセス許可が必要です。これらのアクションでは、AWS Lambda、IAM、および Amazon EC2 サービスを呼び出して、インスタンスの問題の安全な修正を試みます。AWS アカウント、VPC、またはその両方で管理者レベルのアクセス許可がある場合は、このセクションで説明しているように、アクセス許可を設定することなく自動化を実行できることがあります。管理者レベルのアクセス許可がない場合は、ユーザーまたは管理者が、次のいずれかのオプションを使用してアクセス許可を設定する必要があります。

- IAM ポリシーを使用したアクセス許可の付与
- AWS CloudFormation テンプレートを使用したアクセス権限の付与

IAM ポリシーを使用したアクセス許可の付与

次の IAM ポリシーをユーザー、グループ、ロールにインラインポリシーとしてアタッチするか、新しい IAM マネージドポリシーを作成し、ユーザー、グループ、ロールにアタッチできます。ユーザー、グループ、ロールへのインラインポリシーの追加の詳細については、「インラインポリシーの使用」を参照してください。新しい管理ポリシーの作成の詳細については、「管理ポリシーの使用」を参照してください。

> **Note**
>
> 新しい IAM 管理ポリシーを作成する場合、AmazonSSMAutomationRole 管理ポリシーもアタッチし、インスタンスが Systems Manager API と通信できるようにする必要があります。

AWSSupport-ResetAccess の IAM ポリシー

[Account ID] (アカウント ID) をユーザー自身の情報に置き換えます。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
       {
          "Action": [
             "lambda:InvokeFunction",
             "lambda:DeleteFunction",
             "lambda:GetFunction"
          ],
          "Resource": "arn:aws:lambda:*:account ID:function:AWSSupport-EC2Rescue-*",
          "Effect": "Allow"
       },
       {
          "Action": [
             "s3:GetObject",
             "s3:GetObjectVersion"
          ],
          "Resource": [
             "arn:aws:s3:::awssupport-ssm.*/*.template",
             "arn:aws:s3:::awssupport-ssm.*/*.zip"
          ],
          "Effect": "Allow"
       },
       {
          "Action": [
             "iam:CreateRole",
             "iam:CreateInstanceProfile",
             "iam:GetRole",
             "iam:GetInstanceProfile",
             "iam:PutRolePolicy",
             "iam:DetachRolePolicy",
             "iam:AttachRolePolicy",
             "iam:PassRole",
             "iam:AddRoleToInstanceProfile",
             "iam:RemoveRoleFromInstanceProfile",
             "iam:DeleteRole",
             "iam:DeleteRolePolicy",
             "iam:DeleteInstanceProfile"
          ],
          "Resource": [
             "arn:aws:iam::account ID:role/AWSSupport-EC2Rescue-*",
             "arn:aws:iam::account ID:instance-profile/AWSSupport-EC2Rescue-*"
          ],
          "Effect": "Allow"
       },
```

```
      {
         "Action": [
            "lambda:CreateFunction",
            "ec2:CreateVpc",
            "ec2:ModifyVpcAttribute",
            "ec2:DeleteVpc",
            "ec2:CreateInternetGateway",
            "ec2:AttachInternetGateway",
            "ec2:DetachInternetGateway",
            "ec2:DeleteInternetGateway",
            "ec2:CreateSubnet",
            "ec2:DeleteSubnet",
            "ec2:CreateRoute",
            "ec2:DeleteRoute",
            "ec2:CreateRouteTable",
            "ec2:AssociateRouteTable",
            "ec2:DisassociateRouteTable",
            "ec2:DeleteRouteTable",
            "ec2:CreateVpcEndpoint",
            "ec2:DeleteVpcEndpoints",
            "ec2:ModifyVpcEndpoint",
            "ec2:Describe*"
         ],
         "Resource": "*",
         "Effect": "Allow"
      }
   ]
}
```

AWS CloudFormation テンプレートを使用したアクセス権限の付与

AWS CloudFormation は事前設定されたテンプレートを使用して、IAM ロールとポリシーを作成するプロセスを自動化します。 を使用して、EC2Rescue の Automation に必要な IAM ロールとポリシーを作成するには、次の手順を使用しますAWS CloudFormation

EC2Rescue に必要な IAM ロールとポリシーを作成するには

1. AWSSupport-EC2RescueRole.zip をダウンロードし、AWSSupport-EC2RescueRole.json ファイルをローカルマシン上のディレクトリに展開します。
2. AWS アカウント が特殊なパーティションにある場合は、テンプレートを編集して、ARN 値をパーティションの ARN 値に変更します。

例えば、中国リージョンの場合は、`arn:aws` のすべてのケースを `arn:aws-cn` に変更します。

3. AWS Management Console にサインインし、AWS CloudFormation コンソール (https://console.aws.amazon.com/cloudformation) を開きます。
4. [スタックの作成] を選択し、[新しいリソースの使用 (標準)] を選択します。
5. [スタックの作成] ページの [前提条件 - テンプレートの準備] で、[テンプレートの準備完了] を選択します。
6. [テンプレートの指定] で、[テンプレートファイルのアップロード] を選択します。
7. [ファイルを選択] を選択し、展開したディレクトリから `AWSSupport-EC2RescueRole.json` ファイルを参照して選択します。
8. [次へ] を選択します。
9. [スタックの詳細の指定] ページの [スタック名] フィールドに、このスタックを識別する名前を入力し、[次へ] を選択します。
10. (オプション) [タグ] 領域で、1 つ以上のタグキーの名前と値のペアをスタックに適用します。

    タグは、リソースに割り当てるオプションのメタデータです。タグを使用すると、目的、所有者、環境などのさまざまな方法でリソースを分類できます。たとえば、スタックにタグを付けると、スタックが実行するタスクのタイプ、関連するターゲットまたはその他のリソースのタイプ、およびスタックが実行される環境を識別できます。
11. [Next] (次へ) を選択します。
12. [確認] ページでスタックの詳細を確認し、下にスクロールして、[AWS CloudFormation によって IAM リソースが作成される場合があることを了承する] オプションを選択します。
13. AWS CloudFormation は、[CREATE_IN_PROGRESS] ステータスを数分間表示します。スタックを作成すると、ステータスは [CREATE_COMPLETE] に変わります。更新アイコンを選択して、作成プロセスのステータスを確認することもできます。
14. スタックリストで、先ほど作成したスタックの横にあるオプションを選択し、[Outputs] タブを選択します。
15. [Value] をコピーします。これは AssumeRole の ARN です。自動化を実行するときに、この ARN を指定します。

自動化の実行

次の手順では、AWS Systems Manager コンソールを使用して `AWSSupport-ResetAccess` ランブックを実行する方法について説明します。

> **Important**
>
> 次のオートメーションではインスタンスを停止します。インスタンスを停止すると、アタッチされたインスタンスストアボリュームのデータが失われます (存在する場合)。また、インスタンスを停止すると、Elastic IP が関連付けられていない場合、そのパブリック IP アドレスも変更されます。これらの設定変更を避けるには、Run Command を使用してアクセスをリセットします。詳細については、「Amazon EC2 ユーザーガイド」の「EC2Rescue for Windows Server を Systems Manager の Run Command で使用する」を参照してください。

AWSSupport-ResetAccess の自動化を実行するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで [オートメーション] を選択します。
3. [オートメーションを実行] を選択します。
4. [Automation document (オートメーションドキュメント)] セクションで、リストから [Owned by Amazon (Amazon が所有)] を選択します。
5. ランブックリストで、[AWSSupport-ResetAccess] のカードのボタンを選択し、[Next (次へ)] を選択します。
6. [Execute automation document (オートメーションドキュメントの実行)] ページで、[Simple execution (シンプルな実行)] を選択します。
7. [ドキュメント詳細] セクションで、[ドキュメントバージョン] が最大のデフォルトバージョンに設定されていることを確認します。例えば、[$DEFAULT] または [3 (デフォルト)] のように指定します。
8. [Input parameters] セクションで、以下のパラメータを指定します。
   a. [InstanceID] で、到達不可能なインスタンスの ID を指定します。
   b. [SubnetId] で、指定したインスタンスと同じアベイラビリティーゾーンの既存の VPC のサブネットを指定します。デフォルトでは、Systems Manager によって新しい VPC が作成されますが、必要に応じて既存の VPC のサブネットを指定できます。

> **Note**
>
> サブネット ID を指定するオプションが表示されない場合は、最新のデフォルトバージョンのランブックを使用していることを確認します。

c. [EC2RescueInstanceType] で、EC2Rescue インスタンスのインスタンスタイプを指定します。デフォルトのインスタンスタイプは `t2.medium` です。

d. [AssumeRole] で、AWS CloudFormation コンソールでメモした AssumeRole ARN を指定します (この Automation 用のロールをこのトピックで前述した AWS CloudFormation の手順を使用して作成している場合)。

9. (オプション) [Tags (タグ)] 領域で、オートメーションを識別するためにタグキーの名前と値のペアを 1 つ以上適用します。たとえば、`Key=Purpose,Value=ResetAccess` です。

10. [Execute] を選択します。

11. オートメーションの進捗をモニタリングするには、実行中のオートメーションを選択し、[Steps] タブを選択します。オートメーションが終了したら、[Descriptions] タブを選択し、[View output] を選択して結果を表示します。個別のステップの出力を表示するには、[Steps] タブを選択し、ステップの横にある [View Outputs] を選択します。

ランブックは、オートメーションの一環としてバックアップ AMI とパスワード対応の AMI を作成します。オートメーションで作成された他のすべてのリソースは自動的に削除されますが、これらの AMIs はアカウントに残ります。AMIs の名前は次の命名規則に従います。

- バックアップ AMI: `AWSSupport-EC2Rescue:`*`InstanceID`*
- パスワード対応の AMI: AWSSupport-EC2Rescue: *`###### ID`* のパスワード対応の AMI

これらの AMIs は、Automation の実行 ID で検索することで見つけることができます。

Linux の場合、インスタンスの新しい SSH プライベートキーは暗号化されて Parameter Store に保存されます。パラメータ名は /ec2rl/openssh/***`instance ID`***/key です。

入力トランスフォーマーを使用したオートメーションへのデータの受け渡し

この AWS Systems Manager Automation チュートリアルでは、Amazon EventBridge の入力トランスフォーマー機能を使用して、インスタンスの状態変更イベントから、 Amazon Elastic Compute Cloud (Amazon EC2) インスタンスの `instance-id` を抽出する方法を説明します。Automation は AWS Systems Manager のツールです。入力トランスフォーマーを使用して、そのデータを `AWS-`

`CreateImage` ランブックターゲットに `InstanceId` 入力パラメータとして渡します。ルールは、任意のインスタンスが `stopped` 状態に変わった時点でトリガーされます。

入力トランスフォーマーの使用方法の詳細については、Amazon EventBridge ユーザーガイドの「チュートリアル: イベントターゲットに渡されるものを入力トランスフォーマーを使用してカスタマイズする」を参照してください。

開始する前に

EventBridge に必要なアクセス許可と信頼ポリシーを、Systems Manager Automation サービスロールに追加したことを確認します。詳細については、Amazon EventBridge ユーザーガイドの「EventBridge リソースへのアクセス許可の管理の概要」を参照してください。

オートメーションで Input Transformers を使用するには

1. Amazon EventBridge コンソール (https://console.aws.amazon.com/events/) を開きます。
2. ナビゲーションペインで ルール] を選択します。
3. [ルールの作成] を選択します。
4. ルールの名前と説明を入力します。

   ルールには同じリージョン内および同じイベントバス上の別のルールと同じ名前を付けることはできません。
5. [イベントバス] で、このルールに関連付けるイベントバスを選択します。このルールを使用して、自分の AWS アカウント の一致するイベントに応答する場合は、[default] (デフォルト) を選択します。アカウントの AWS のサービスで発生したイベントは、常にアカウントのデフォルトのイベントバスに移動します。
6. [ルールタイプ] で、[イベントパターンを持つルール] を選択してください。
7. [Next] を選択します。
8. [Event source] (イベントソース) で、[AWS events or EventBridge partner events] (イベントまたは EventBridge パートナーイベント) を選択してください。
9. [Event pattern] (イベントパターン) セクションで [Event pattern form] (イベントパターンフォーム) を選択します。
10. [イベントソース] で、[AWS のサービス] を選択してください。
11. [AWS のサービス] で [EC2] を選択します。
12. [イベントタイプ] に、[EC2 インスタンスの状態変更通知] を選択してください。
13. [Specific state(s)] (特定の状態) で [stopped] (停止) を選択します。

14. [Next] を選択します。
15. [ターゲットタイプ] で、[AWS のサービス] を選択します。
16. [Select a target] (ターゲットを選択) では、[Systems Manager オートメーション] を選択します。
17. [Document (ドキュメント)] で、[AWS-CreateImage] を選択します。
18. [Configure automation parameter(s)] (オートメーションパラメータの構成) で [Input Transformer] (入力トランスフォーマー) を選択します。
19. [Input path] (入力パス) に「**{"instance":"$.detail.instance-id"}**」と入力します。
20. [Template] テンプレートに「**{"InstanceId":[<instance>]}**」と入力します。
21. [Execution role] (実行ロール) で [Use existing role] (既存のロールを使用) を選択し、オートメーションサービスロールを選択します。
22. [Next] を選択します。
23. (オプション) ルールに 1 つ以上のタグを入力します。詳細については、Amazon EventBridge ユーザーガイドの「Amazon EventBridge リソースのタグ付け」を参照してください 。
24. [Next] を選択します。
25. ルールの詳細を確認し、[Create rule] (ルールの作成) を選択します。

Systems Manager Automation が返すステータスについて学ぶ

AWS Systems Manager Automation は、Automation の実行時およびAutomation 全体について、Automation アクションまたはステップが通過するさまざまなステータスに関する詳細なステータス情報をレポートします。Automation は AWS Systems Manager のツールです。次の方法を使用して、コマンドのステータスを監視できます。

- Systems Manager Automation コンソールで、実行ステータスをモニタリングします。
- 任意のコマンドラインツールを使用します。AWS Command Line Interface(AWS CLI) では、describe-automation-step-executions または get-automation-execution を使用できます。AWS Tools for Windows PowerShell では、 Get-SSMAUTOMationStepExecution または Get-SSMAUTOMationExecution を使用できます。
- アクションまたはオートメーションステータスの変更に応答するように Amazon EventBridge を設定します。

オートメーションにおけるタイムアウトの処理の詳細については、「ランブックでのタイムアウトの処理」を参照してください。

オートメーションステータスについて

オートメーションは、全体的なオートメーションに加え、個々のオートメーションアクションのステータスの詳細もレポートします。

全体的なオートメーションステータスは、次の表に示す個々のアクションまたはステップによって報告されるステータスと異なる場合があります。

コマンドの詳細なステータス

ステータス	詳細
Pending	ステップの実行が開始されていません。オートメーションで条件付きアクションが使用されている場合、ステップを実行するための条件が満たされなかった場合、オートメーションが完了した後も、ステップはこの状態のままになります。ステップが実行される前にオートメーションがキャンセルされた場合も、ステップはこの状態のままになります。
InProgress	ステップは実行中です。
待機中です	ステップは入力を待っています。
成功	ステップは正しく完了しています。これは終了状態です。
TimedOut	指定されたタイムアウト期間より前にステップまたは承認が完了しませんでした。これは終了状態です。
キャンセル	ステップは、リクエスタによってキャンセルされた後に停止中です。
キャンセル	ステップは、完了する前にリクエスタによって停止されました。これは終了状態です。
失敗	ステップは正常に完了しませんでした。これは終了状態です。

ステータス	詳細
Exited	aws:loop アクションによってのみ返されます。ループは完全には完了しませんでした。ループ内のステップが nextStep、onCancel、または onFailure プロパティを使用して外部のステップに移動しました。

オートメーションの詳細なステータス

ステータス	詳細
Pending	オートメーションの実行が開始されていません。
InProgress	オートメーションが実行されています。
待機中です	オートメーションは入力を待っています。
成功	オートメーションが正常に完了しました。これは終了状態です。
TimedOut	指定されたタイムアウト期間より前にステップまたは承認が完了しませんでした。これは終了状態です。
キャンセル	オートメーションは、リクエスタによってキャンセルされた後に停止中です。
キャンセル	オートメーションは、完了する前にリクエスタによって停止されました。これは終了状態です。
失敗	オートメーションは正常に完了しませんでした。これは終了状態です。

Systems Manager Automation のトラブルシューティング

AWS Systems Manager のツールである AWS Systems Manager Automation に問題が生じた場合にトラブルシューティングするときは、次の情報が役立ちます。このトピックには、自動化エラーメッセージにおける問題を解決するための特定のタスクが含まれます。

トピック

- 一般的な自動化エラー
- 自動化の実行開始の失敗
- 実行は開始するが、ステータスが失敗になる
- 実行は開始するが、タイムアウトになる

一般的な自動化エラー

このセクションでは、一般的な自動化エラーについて説明します。

VPC not defined 400

デフォルトでは、オートメーションが `AWS-UpdateLinuxAmi` ランブックまたは `AWS-UpdateWindowsAmi` ランブックを実行すると、システムはデフォルト VPC (172.30.0.0/16) に一時インスタンスを作成します。デフォルト VPC を削除した場合、次のエラーが発生します。

```
VPC not defined 400
```

この問題を解決するには、`SubnetId` 入力パラメータに値を指定する必要があります。

自動化の実行開始の失敗

AWS Identity and Access Management (IAM) ロール、オートメーションのポリシーが正しく設定されていない場合、オートメーションはアクセス拒否エラーまたは無効な継承ロールエラーによって失敗する可能性があります。

アクセスが拒否されました

次の例では、オートメーションがアクセス拒否エラーによって失敗した状態を説明します。

Systems Manager API へのアクセスが拒否されました

エラーメッセージ: `User: user arn isn't authorized to perform: ssm:StartAutomationExecution on resource: document arn (Service:`

AWSSimpleSystemsManagement; Status Code: 400; Error Code: AccessDeniedException; Request ID: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx)

- 考えられる原因 1: オートメーションを開始しようとしているユーザーに、StartAutomationExecution API を呼び出すアクセス許可がない。この問題を解決するには、オートメーションを開始するために使用されるユーザーに、必要な IAM ポリシーをアタッチします。
- 考えられる原因 2: オートメーションを開始しようとしているユーザーに StartAutomationExecution API を呼び出すアクセス許可があるが、特定のランブックを使用して API を呼び出すアクセス許可がない。この問題を解決するには、オートメーションを開始するために使用されるユーザーに、必要な IAM ポリシーをアタッチします。

PassRole 許可がないことによるアクセスの拒否

エラーメッセージ: User: user arn isn't authorized to perform: iam:PassRole on resource: automation assume role arn (Service: AWSSimpleSystemsManagement; Status Code: 400; Error Code: AccessDeniedException; Request ID: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx)

オートメーションを開始しようとしているユーザーに、ロールを継承するための PassRole 許可がない。この問題を解決するには、オートメーションを開始しようとしているユーザーのロールに、iam:PassRole ポリシーをアタッチします。詳細については、「タスク 2: iam:PassRole ポリシーをオートメーションロールにアタッチする」を参照してください。

無効な継承ロール

自動化を実行するとき、継承ロールはランブックで提供されるか、あるいはランブックにパラメータ値として渡されます。継承ロールが指定されていない、あるいは正しく設定されていない場合、複数の種類のエラーが発生することがあります。

形式が正しくない継承ロール

エラーメッセージ: The format of the supplied assume role ARN isn't valid. 継承ロールが不適切にフォーマットされている。この問題を解決するには、ランブックで有効な継承ロールが指定されていること、あるいは自動化を開始するときにランタイムパラメータとして指定されていることを確認します。

継承ロールが継承されない

エラーメッセージ: `The defined assume role is unable to be assumed. (Service: AWSSimpleSystemsManagement; Status Code: 400; Error Code: InvalidAutomationExecutionParametersException; Request ID: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx)`

- 考えられる原因 1: 継承ロールが存在しない。この問題を解決するには、ロールを作成します。詳細については、「」を参照してくださいthe section called “オートメーションの設定” このロールを作成するための詳細は、このトピック「タスク 1: 自動化のサービスロールを作成する」で説明されています。
- 考えられる原因 2: 継承ロールに Systems Manager サービスとの信頼関係がない。この問題を解決するには、信頼関係を作成します。詳細については、IAM ユーザーガイドの「ロールを引き受けることができない」を参照してください。

実行は開始するが、ステータスが失敗になる

アクション固有の失敗

ランブックには、ステップとステップの実行が順番に含まれています。各ステップは、1 つまたは複数の AWS のサービス API を起動します。この API は、ステップの入力、動作、出力を決定します。エラーによって 1 つのステップが失敗する可能性のある複数の場所があります。失敗メッセージは、いつどこでエラーが発生したかを示します。

Amazon Elastic Compute Cloud (Amazon EC2) コンソールで失敗メッセージを表示するには、失敗したステップの [出力を表示] リンクを選択します。AWS CLI から失敗メッセージを表示するには、`get-automation-execution` を呼び出して、失敗した `FailureMessage` から `StepExecution` 属性を検索します。

次の例では、`aws:runInstance` アクションに関連付けられたステップが失敗しています。それぞれの例では、異なる種類のエラーを示しています。

イメージの欠落

エラーメッセージ: `Automation Step Execution fails when it's launching the instance(s). Get Exception from RunInstances API of ec2 Service. Exception Message from RunInstances API: [The image id '[ami id]' doesn't exist (Service: AmazonEC2; Status Code: 400; Error Code: InvalidAMIID.NotFound; Request ID: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx)]. Please refer to Automation Service Troubleshooting Guide for more diagnosis details.`

aws:runInstances アクションは、存在しない ImageId への入力を受信しました。この問題を解決するには、適切な AMI ID を使用してランブックまたはパラメータ値を更新します。

継承ロールポリシーに十分なアクセス許可がない

エラーメッセージ: Automation Step Execution fails when it's launching the instance(s). Get Exception from RunInstances API of ec2 Service. Exception Message from RunInstances API: [You aren't authorized to perform this operation. Encoded authorization failure message: xxxxxxx (Service: AmazonEC2; Status Code: 403; Error Code: UnauthorizedOperation; Request ID: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx)]. Please refer to Automation Service Troubleshooting Guide for more diagnosis details.

継承ロールに、EC2 インスタンスで RunInstances API を呼び出す十分なアクセス許可がありません。この問題を解決するには、継承ロールに RunInstances API を呼び出すアクセス許可がある継承ロールに IAM ポリシーをアタッチします。詳細については、「コンソールを使用して Automation 用のサービスロールを作成する」を参照してください。

予期できないステート

エラーメッセージ: Step fails when it's verifying launched instance(s) are ready to be used. Instance i-xxxxxxxxx entered unexpected state: shutting-down. Please refer to Automation Service Troubleshooting Guide for more diagnosis details.

- 考えられる原因 1: インスタンスまたは Amazon EC2 サービスに問題がある。この問題を解決するには、インスタンスにログインするか、インスタンスシステムログを参照して、インスタンスがシャットダウンするようになった原因を検索します。
- 考えられる原因 2: aws:runInstances アクションに指定されるユーザーデータスクリプトに問題があるか、あるいは正しくない構文がある。ユーザーデータスクリプトの構文を確認します。また、ユーザーデータスクリプトがインスタンスをシャットダウンしていない、あるいはインスタンスをシャットダウンするその他のスクリプトを呼び出していないかも確認します。

アクション固有の失敗リファレンス

ステップが失敗すると、失敗発生時にどのサービスが呼び出されたかが失敗のメッセージに示されることもあります。次の表は、各アクションによって呼び出されるサービスを一覧表示します。また、この表にはそれぞれのサービスの情報へのリンクも提供しています。

アクション	このアクションによって呼び出される AWS のサービス	このサービスについての情報	トラブルシューティングのコンテンツ
`aws:runInstances`	Amazon EC2	Amazon EC2 ユーザーガイド	EC2 インスタンスのトラブルシューティング
`aws:changeInstanceState`	Amazon EC2	Amazon EC2 ユーザーガイド	EC2 インスタンスのトラブルシューティング
`aws:runCommand`	Systems Manager	AWS Systems Manager Run Command	Systems Manager Run Command のトラブルシューティング
`aws:createImage`	Amazon EC2	Amazon Machine Images	
`aws:createStack`	AWS CloudFormation	AWS CloudFormation ユーザーガイド	AWS CloudFormation のトラブルシューティング
`aws:deleteStack`	AWS CloudFormation	AWS CloudFormation ユーザーガイド	AWS CloudFormation のトラブルシューティング
`aws:deleteImage`	Amazon EC2	Amazon マシンイメージ	
`aws:copyImage`	Amazon EC2	Amazon Machine Images	
`aws:createTag`	Amazon EC2、Systems Manager	EC2 リソースとタグ	

アクション	このアクションによって呼び出される AWS のサービス	このサービスについての情報	トラブルシューティングのコンテンツ
aws:invokeLambdaFunction	AWS Lambda	AWS Lambda デベロッパーガイド	Lambda のトラブルシューティング

自動化サービス内部エラー

エラーメッセージ: `Internal Server Error. Please refer to Automation Service Troubleshooting Guide for more diagnosis details.`

自動化サービスに関する問題は、特定のランブックが正常に実行されることに影響を及ぼします。この問題を解決するには、 にお問い合わせくださいAWS サポート 可能な範囲で、実行 ID とカスタマー ID をご用意ください。

実行は開始するが、タイムアウトになる

エラーメッセージ: `Step timed out while step is verifying launched instance(s) are ready to be used. Please refer to Automation Service Troubleshooting Guide for more diagnosis details.`

`aws:runInstances` アクションのステップがタイムアウトになります。これは、ステップで `timeoutSeconds` に指定された値よりステップアクションの実行に時間がかかる場合に発生します。この問題を解決するには、`aws:runInstances` アクションで `timeoutSeconds` パラメータにより長い時間を指定してください。問題が解決しない場合は、ステップが予期される時間より長くかかる原因を診断します。

AWS Systems Manager Change Calendar

AWS Systems Manager のツールである Change Calendar では、指定したアクション (Systems Manager Automation ランブックなど) が AWS アカウントで実行できるまたはできない日付と時刻の範囲を設定できます。Change Calendar では、これらの範囲をイベントと呼びます。Change Calendar エントリを作成すると、`ChangeCalendar` タイプの Systems Manager ドキュメントが作成されます。Change Calendar では、ドキュメントに iCalendar 2.0 データがプレーンテキスト形式で保存されます。Change Calendar エントリに追加したイベントは、ドキュメントの一部になります。Change Calendar の使用を開始するには、Systems Manager コンソールを開きます。ナビゲーションペインで、[Change Calendar] を選択します。

Systems Manager コンソールでカレンダーとそのイベントを作成できます。また、サポートされているサードパーティーのカレンダープロバイダからエクスポートした iCalendar (`.ics`) ファイルをインポートして、そのイベントを自分のカレンダーに追加できます。サポートされているプロバイダには、Google カレンダー、Microsoft Outlook、iCloud カレンダーが含まれます。

Change Calendar エントリは、次の 2 つのタイプのいずれかになります。

`DEFAULT_OPEN`、またはデフォルトでオープン

カレンダーイベント中を除き、デフォルトですべてのアクションの実行が可能です。イベント中、`DEFAULT_OPEN` カレンダーの状態は `CLOSED` となり、イベントの実行がブロックされます。

`DEFAULT_CLOSED`、またはデフォルトでクローズ

カレンダーイベント中を除き、すべてのアクションがデフォルトでブロックされます。イベント中、`DEFAULT_CLOSED` カレンダーの状態は `OPEN` となり、アクションの実行が許可されます。

スケジュールされたすべての自動化ワークフロー、メンテナンスウィンドウ、および State Manager の関連付けをカレンダーに自動的に追加するように選択できます。また、これらのそれぞれのタイプをカレンダー表示から削除することもできます。

Change Calendar はどのようなユーザーに適していますか?

- 次のアクションタイプを実行する AWS の顧客:
  - 自動化ランブックを作成または実行します。
  - Change Manager で変更リクエストを作成します。
  - メンテナンスウィンドウを実行します。
  - State Manager で関連付けを作成します。

  Automation、Change Manager、Maintenance Windows、State Manager はすべて AWS Systems Manager のツールです。これらのツールを Change Calendar と統合することにより、それぞれに関連付ける変更カレンダーの現在の状態に応じて、これらのアクションタイプを許可またはブロックできます。
- Systems Manager マネージドノードの設定の一貫性、安定性、機能性を維持する管理者。

Change Calendar の利点

Change Calendar には次のような利点があります。

- 変更を適用する前に確認する

  Change Calendar エントリを使用すると、環境に破壊的な影響を及ぼす可能性のある変更を適用する前に確認できます。

- 適切な時間帯にのみ変更を適用する

  Change Calendar エントリを使用すると、イベント期間中に環境を安定に維持できます。たとえば、カンファレンスや公開マーケティングのプロモーションなど、リソースに対する需要が高くなると予想される期間に変更をブロックする Change Calendar エントリを作成できます。カレンダーエントリは、休暇中や祝日中など、管理者サポートが制限されると予想される期間に変更をブロックすることもできます。カレンダーエントリを使用すると、失敗したアクションやデプロイのトラブルシューティングを行うための管理者サポートが制限されている時間以外の、特定の時間帯以外の変更を許可できます。

- カレンダーの現在または今後の状態を取得する

  Systems Manager `GetCalendarState` API オペレーションを実行して、カレンダーの現在の状態、指定した時刻の状態、次にカレンダーの状態が変更されるようにスケジュールされている時刻を表示できます。

- EventBridge のサポート

  この Systems Manager ツールは、Amazon EventBridge ルールのイベントタイプとしてサポートされています。詳細については、「Amazon EventBridge を使用して Systems Manager イベントをモニタリングする」および「リファレンス: Systems Manager 用の Amazon EventBridge イベントパターンとタイプ」を参照してください。

トピック

- Change Calendar を設定する
- 「Change Calendar」 の使用
- Automation ランブックへの Change Calendar の依存関係の追加
- Change Calendar のトラブルシューティング

Change Calendar を設定する

AWS Systems Manager のツールである Change Calendar を使用する前に、以下を完了してください。

最新のコマンドラインツールをインストールする

最新のコマンドラインツールをインストールして、カレンダーに関する状態情報を取得します。

要件	説明
AWS CLI	(オプション) AWS Command Line Interface (AWS CLI) を使用してカレンダーに関する状態情報を取得するには、AWS CLI の最新リリースをローカルコンピュータにインストールします。 CLI をインストールまたはアップグレードする方法の詳細については、AWS Command Line Interface ユーザーガイドの「AWS CLI のインストール、更新、アンインストール」を参照してください。
AWS Tools for PowerShell	(オプション) Tools for PowerShell を使用してカレンダーに関する状態情報を取得するには、ローカルコンピュータに Tools for PowerShell の最新リリースをインストールします。 Tools for PowerShell をインストールまたはアップグレードする方法の詳細については、AWS Tools for PowerShell ユーザーガイドの「AWS Tools for PowerShell のインストール」を参照してください。

アクセス許可の設定

ユーザー、グループ、ロールに管理者権限が割り当てられている場合は、Change Calendar に完全にアクセスできます。管理者権限がない場合は、管理者に `AmazonSSMFullAccess` マネージドポリシーの割り当てを依頼するか、ユーザー、グループ、ロールに必要なアクセス許可を付与するポリシーの割り当てを依頼してください。

Change Calendar を使用するには、以下のアクセス権限が必要です。

Change Calendar エントリ

エントリにイベントを追加および削除したり、Change Calendar エントリを作成、更新、削除したりするには、ユーザー、グループ、またはロールにアタッチされたポリシーで次のアクションが許可されている必要があります。

- ssm:CreateDocument
- ssm:DeleteDocument
- ssm:DescribeDocument
- ssm:DescribeDocumentPermission
- ssm:GetCalendar
- ssm:ListDocuments
- ssm:ModifyDocumentPermission
- ssm:PutCalendar
- ssm:UpdateDocument
- ssm:UpdateDocumentDefaultVersion

カレンダーの状態

カレンダーの現在または今後の状態に関する情報を取得するには、ユーザー、グループ、またはロールにアタッチされたポリシーで次のアクションが許可されている必要があります。

- ssm:GetCalendarState

運用イベント

メンテナンスウィンドウ、関連付け、計画された自動化などの運用イベントを表示するには、ユーザー、グループ、またはロールにアタッチされたポリシーで次のアクションが許可されている必要があります。

- ssm:DescribeMaintenanceWindows
- ssm:DescribeMaintenanceWindowExecution
- ssm:DescribeAutomationExecutions
- ssm:ListAssociations

> **Note**
>
> 自分以外のアカウントが所有している (つまり、自分以外のアカウントによって作成されている) Change Calendar エントリは、自分のアカウントと共有されている場合でも読み取り

専用になります。メンテナンスウィンドウ、State Manager の関連付け、オートメーションは共有されません。

「Change Calendar」 の使用

AWS Systems Manager のツールである Change Calendar でエントリを追加、管理、削除するときは AWS Systems Manager コンソールを使用します。ソースカレンダーからエクスポートした iCalendar (`.ics`) ファイルをインポートすると、サポートされているサードパーティーのカレンダープロバイダからイベントをインポートすることもできます。また、`GetCalendarState` API オペレーションまたは `get-calendar-state` AWS Command Line Interface (AWS CLI) コマンドを使用すると、特定の時刻の Change Calendar の状態に関する情報を取得できます。

トピック

- Change Calendar の作成
- Change Calendar でのイベントの作成と管理
- サードパーティーのカレンダーからのイベントのインポートと管理
- Change Calendar の更新
- Change Calendar の共有
- Change Calendar の削除
- Change Calendar の状態の取得

Change Calendar の作成

AWS Systems Manager のツールである Change Calendar でエントリを作成すると、`text` 形式を使用する Systems Manager ドキュメント (SSM ドキュメント) が作成されます。

Change Calendar を作成するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Change Calendar] を選択します。
3. [Create calendar (カレンダーの作成)] を選択します。

   -または-

Change Calendar ホームページが開いたら、最初に [Create change calendar] (変更カレンダーの作成) をクリックします。

4. [Create calendar (カレンダーの作成)] ページの [Calendar details (カレンダーの詳細)] に、カレンダーエントリの名前を入力します。カレンダーエントリ名には、文字、数字、ピリオド、ダッシュ、アンダースコアを使用できます。カレンダーのエントリの目的がひとめでわかるような具体的な名前にしてください。例: 「**`support-off-hours`**」。カレンダーエントリを作成した後、この名前を更新することはできません。
5. (オプション) [Description] (説明) に、カレンダーエントリの説明を入力します。
6. (オプション) [Import calendar (カレンダーのインポート)] で [Choose file (ファイルの選択)] を選び、サードパーティーのカレンダープロバイダからエクスポートしたiCalendar (`.ics`) ファイルを選択します。ファイルをインポートすると、そのイベントがカレンダーに追加されます。

   サポートされているプロバイダには、Google カレンダー、Microsoft Outlook、iCloud カレンダーが含まれます。

   詳細については、「サードパーティーのカレンダープロバイダからのイベントのインポート」を参照してください。
7. [Calendar type (カレンダーの種類)] で、次のいずれかを選択します。

   - [Open by default (デフォルトでオープン)] - カレンダーはオープン (Automation アクションはイベントが開始するまで実行可能) で、関連付けられたイベントの期間中はクローズになります。
   - [Closed by default (デフォルトでクローズ)] - カレンダーはクローズ (Automation アクションはイベントが開始されるまで実行不可) で、関連付けられたイベントの期間中はオープンになります。
8. (オプション) [変更管理イベント] で、[変更管理イベントをカレンダーに追加] を選択します。これを選択すると、毎月のカレンダー表示に、予定されているメンテナンスウィンドウ、State Manager の関連付け、自動化ワークフロー、Change Manager 変更リクエストがすべて表示されます。

   > **Tip**
   >
   > 後でこれらのイベントタイプをカレンダー表示から完全に削除する場合は、カレンダーを編集してこのチェックボックスをオフにして、[保存] を選択します。
9. [Create calendar (カレンダーの作成)] を選択します。

カレンダーエントリが作成されると、Systems Manager は、Change Calendar の一覧にカレンダーエントリを表示します。列には、カレンダーのバージョンとカレンダーの所有者の AWS アカウント 番号が表示されます。少なくとも 1 つのイベントを作成するかインポートするまでは、カレンダーエントリでアクションを禁止または許可することはできません。イベント作成の詳細については、「Change Calendar イベントの作成」を参照してください。イベントのインポートについては、「サードパーティーのカレンダープロバイダからのイベントのインポート」を参照してください。

Change Calendar でのイベントの作成と管理

カレンダーを AWS Systems Manager Change Calendar で作成した後、開いているカレンダーまたは閉じているカレンダーに含まれているイベントを作成、更新、削除できます。Change Calendar は AWS Systems Manager のツールです。

> **Tip**
>
> Systems Manager コンソールでイベントを直接作成する代わりに、サポートされているサードパーティーのカレンダーアプリケーションから iCalendar (`.ics`) ファイルをインポートできます。詳細については、サードパーティーのカレンダーからのイベントのインポートと管理 を参照してください。

トピック

- Change Calendar イベントの作成
- Change Calendar イベントの更新
- Change Calendar イベントの削除

Change Calendar イベントの作成

AWS Systems Manager のツールである Change Calendar のエントリにイベントを追加すると、カレンダーエントリのデフォルトのアクションが中断される期間を指定することができます。たとえば、カレンダーエントリの種類がデフォルトでクローズの場合、カレンダーはイベント中に変更に対してオープンになります。(または、カレンダー上のみで情報ロールを提供する、アドバイザリイベントを作成することもできます。)

現在は、コンソールを使用して作成できるのは、Change Calendar イベントのみです。イベントは、Change Calendar エントリの作成時に作成する Change Calendar ドキュメントに追加されます。

Change Calendar イベントを作成するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Change Calendar] を選択します。
3. カレンダーのリストから、イベントを追加するカレンダーエントリの名前を選択します。
4. カレンダーエントリの詳細ページで、[Create event (イベントの作成)] を選択します。
5. [Create scheduled event (スケジュールされたイベントの作成)] ページの [Event details (イベントの詳細)] に、イベントの表示名を入力します。イベント名には、文字、数字、ピリオド、ダッシュ、アンダースコアを使用できます。イベントの目的がひとめでわかるような具体的な名前にしてください。例: 「**nighttime-hours**」。
6. [Description] (説明) にイベントの説明を入力します。例えば、**The support team isn't available during these hours** と指定します。
7. (オプション) このイベントを、視覚的な通知やリマインダーとしてのみ使用する場合は、[Advisory] (アドバイザリ) チェックボックスをオンにします。アドバイザリーイベントには、カレンダー上での機能はありません。これらは、カレンダーを表示しているユーザーに情報を提供するためだけのものです。
8. [Event start date] (イベント開始日) で、イベントを開始する日付を `MM/DD/YYYY` 形式で入力 (または選択) し、指定した日にイベントを開始する時刻を `hh:mm:ss` (時、分、秒) 形式で入力します。
9. [Event end date] (イベント終了日) で、イベントを終了する日付を `MM/DD/YYYY` 形式で入力 (または選択) し、指定した日にイベントを終了する時刻を `hh:mm:ss` (時、分、秒) 形式で入力します。
10. [Schedule time zone] (タイムゾーンをスケジュール) で、イベントの開始時刻と終了時刻が適用されるタイムゾーンを選択します。都市名の一部またはグリニッジ標準時 (GMT) とのタイムゾーンの差を入力すると、タイムゾーンをすばやく検索できます。デフォルトは協定世界時 (UTC) です。
11. (オプション) 日ごと、週ごと、月ごとで繰り返されるイベントを作成するには、[Recurrence] (繰り返し) をオンにした上で、繰り返しの頻度および (オプションとして) 終了日を指定します。

12. [Create scheduled event (スケジュールされたアクションの作成)] を選択します。新しいイベントがカレンダーエントリに追加され、カレンダーエントリの詳細ページの [Events (イベント)] タブに表示されます。

Change Calendar イベントの更新

次の手順に従い、AWS Systems Manager コンソールで Change Calendar イベントを更新します。Change Calendar は AWS Systems Manager のツールです。

Change Calendar イベントを更新するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Change Calendar] を選択します。
3. カレンダーのリストから、イベントを編集するカレンダーエントリの名前を選択します。
4. カレンダーエントリの詳細ページで、[Events (イベント)] を選択します。
5. カレンダーページで、編集するイベントを選択します。

> **Tip**
>
> 左上のボタンを使用すると、1 年前後に移動したり、1 か月前後に移動したりできます。タイムゾーンの変更が必要な場合は、右上リストから適切なタイムゾーンを選択します。

6. [Event details] (イベントの詳細) で [Edit] (編集) をクリックします。

   イベントの名前と説明を変更するには、現在のテキスト値に追加するか、その値を置き換えます。

7. [Event start date] (イベント開始日) の値を変更するには、現在の開始日を選択した上で、カレンダーから新しい日付を選択します。開始時刻を変更するには、現在の開始時刻を選択した上で、リストから新しい時刻を選択します。
8. [Event end date] (イベント終了日) の値を変更するには、現在の日付を選択した上で、カレンダーから新しい終了日を選択します。終了時刻を変更するには、現在の終了時刻を選択した上で、リストから新しい時刻を選択します。
9. [Schedule time zone] (タイムゾーンのスケジュール) の値を変更するには、イベントの開始時刻と終了時刻が適用されるタイムゾーンを選択します。都市名の一部またはグリニッジ標準時

(GMT) とのタイムゾーンの差を入力すると、タイムゾーンをすばやく検索できます。デフォルトは協定世界時 (UTC) です。

10. (オプション) このイベントを、視覚的な通知やリマインダーとしてのみ使用する場合は、[Advisory] (アドバイザリ) チェックボックスをオンにします。アドバイザリーイベントには、カレンダー上での機能はありません。これらは、カレンダーを表示しているユーザーに情報を提供するためだけのものです。
11. [Save] を選択します。変更内容は、カレンダーエントリの詳細ページの [Events (イベント)] タブに表示されます。更新したイベントを選択して、変更を表示します。

Change Calendar イベントの削除

AWS Management Consoleを使用して、AWS Systems Manager のツールである Change Calendar で一度にひとつずつイベントを削除できます。

> **Tip**
>
> カレンダーの作成時に [変更管理イベントをカレンダーに追加] を選択した場合は、次の操作を実行できます。
>
> - 変更管理イベントタイプをカレンダー表示から「一時的に」非表示にするには、月次プレビューの上部でタイプの [X] を選択します。
> - これらのタイプをカレンダー表示から「完全に」削除するには、カレンダーを編集し、[カレンダーに変更管理イベントを追加] チェックボックスをオフにして、[保存] を選択します。カレンダー表示からタイプを削除しても、アカウントからは削除されません。

Change Calendar イベントを削除するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Change Calendar] を選択します。
3. カレンダーのリストから、イベントを削除するカレンダーエントリの名前を選択します。
4. カレンダーエントリの詳細ページで、[Events (イベント)] を選択します。
5. カレンダーページで、削除するイベントを選択します。

> **Tip**
>
> 左上のボタンを使用して、カレンダーを 1 年前後に移動したり、1 か月前後に移動したりできます。タイムゾーンの変更が必要な場合は、右上リストから適切なタイムゾーンを選択します。

6. [Event details (イベント詳細)] ページで、[Delete (削除)] を選択します。イベントの削除を確認するプロンプトが表示されたら、[Confirm] (確認) をクリックします。

サードパーティーのカレンダーからのイベントのインポートと管理

イベントを直接 AWS Systems Manager コンソールで作成する代わりに、サポートされているサードパーティーのカレンダーアプリケーションから iCalendar (`.ics`) ファイルをインポートできます。カレンダーには、インポートしたイベントのほか、AWS Systems Manager のツールである Change Calendar で作成したイベントを含めることができます。

[開始する前に]

カレンダーファイルをインポートする前に、次の要件と制約を確認してください。

カレンダーのファイル形式

有効な iCalendar ファイル (`.ics`) のみがサポートされています。

サポートされているカレンダープロバイダ

以下のサードパーティーのカレンダープロバイダからエクスポートされた `.ics` ファイルのみがサポートされています。

- Google カレンダー (エクスポート手順)
- Microsoft Outlook (エクスポート手順)
- iCloud カレンダー (エクスポート手順)

ファイルサイズ

任意の数の有効な `.ics` ファイルをインポートできます。ただし、各カレンダーでインポートされたファイルすべての合計サイズは 64 KB を超えられません。

> **Tip**
>
> .ics ファイルのサイズを最小化するには、カレンダーのエントリに関する基本的な詳細のみをエクスポートしてください。必要に応じて、エクスポートする期間を短縮します。

[Time zone] (タイムゾーン)

カレンダー名、カレンダープロバイダ、および少なくとも 1 つのイベントのほか、エクスポートされた .ics ファイルには、カレンダーのタイムゾーンも示されます。これが表示されない場合、またはタイムゾーンの識別に問題がある場合は、ファイルをインポートした後、タイムゾーンを指定するように求められます。

反復イベントの制限

エクスポートされた .ics ファイルには、反復するイベントを含めることができます。ただし、ソースカレンダーで 1 つ以上の反復イベントが削除された場合、インポートは失敗します。

トピック

- サードパーティーのカレンダープロバイダからのイベントのインポート
- サードパーティーのカレンダープロバイダからのすべてのイベントの更新
- サードパーティーのカレンダーからインポートされたすべてのイベントの削除

サードパーティーのカレンダープロバイダからのイベントのインポート

以下の手順に従い、サポートされているサードパーティーのカレンダーアプリケーションから iCalendar (.ics) ファイルをインポートします。ファイルに含まれるイベントは、開いているカレンダーまたは閉じているカレンダーのルールに組み込まれます。Change Calendar (AWS Systems Manager のツール) を使用して作成している新しいカレンダー、または既存のカレンダーにファイルをインポートできます。

.ics ファイルをインポートした後、Change Calendar インターフェイスを使用して個々のイベントをそのファイルから削除できます。詳細については、Change Calendar イベントの削除 を参照してください。.ics ファイルを削除して、ソースカレンダーからすべてのイベントを削除することもできます。詳細については、「サードパーティーのカレンダーからインポートされたすべてのイベントの削除」を参照してください。

サードパーティーのカレンダープロバイダからイベントをインポートするには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Change Calendar] を選択します。
3. 新しいカレンダーから開始するには、[Create calendar (カレンダーの作成)] を選択します。[Import calendar (カレンダーのインポート)] で [Choose file (ファイルの選択)] を選びます。新しいカレンダーを作成する他の手順については、「Change Calendar の作成」を参照してください。

   -または-

   サードパーティーのイベントを既存のカレンダーにインポートするには、既存のカレンダーの名前を選択して開きます。
4. [Actions、Edit] (編集アクション) をクリックした後、[Import calendar] (カレンダーのインポート) エリアで、[Choose file] (ファイルの選択) をクリックします。
5. ローカルコンピュータで、エクスポートされた `.ics` ファイルに移動して選択します。
6. プロンプトが表示されたら、Select a time zone (タイムゾーンの選択)] で、カレンダーに適用するタイムゾーンを選択します。
7. [Save] を選択します。

サードパーティーのカレンダープロバイダからのすべてのイベントの更新

iCalendar `.ics` ファイルのインポート後、ソースカレンダーに複数のイベントが追加されるか削除されると、これらの変更を Change Calendar で反映できます。まず、元のカレンダーを再エクスポートし、新しいファイルを Change Calendar (AWS Systems Manager のツール) にインポートします。Change Calendar のイベントは、新しいファイルの内容を反映するように更新されます。

サードパーティーのカレンダープロバイダからすべてのイベントを更新するには

1. サードパーティーのカレンダーで、Change Calendar に反映させたいイベントを追加するか削除し、カレンダーを新しい `.ics` ファイルに再エクスポートします。
2. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
3. ナビゲーションペインで、[Change Calendar] を選択します。
4. カレンダーの一覧からカレンダー名を選択します。

5. [ファイルの選択] を選択して、置き換える .ics ファイルに移動して選択します。
6. 既存のファイルの上書きに関する通知に対して、[Confirm (確認)] を選択します。

サードパーティーのカレンダーからインポートされたすべてのイベントの削除

サードパーティーのプロバイダからインポートしたイベントをカレンダーに含める必要がなくなった場合は、インポートした iCalendar .ics ファイルを削除できます。

サードパーティーのカレンダーからインポートされたすべてのイベントを削除するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Change Calendar] を選択します。
3. カレンダーの一覧からカレンダー名を選択します。
4. [Import calendar (カレンダーのインポート)] の [My imported calendars (インポート済みのカレンダー)] で、インポートされたカレンダーの名前を見つけ、そのカードで X を選択します。
5. [Save] を選択します。

Change Calendar の更新

Change Calendar の説明を更新できますが、名前は変更できません。カレンダーのデフォルトの状態は変更できますが、このカレンダーに関連付けられているイベント中の変更アクションの動作が逆になることに注意してください。たとえば、カレンダーの状態を [Open by default (デフォルトでオープン)] から [Closed by default (デフォルトでクローズ)] に変更すると、関連付けられたイベントを作成したユーザーが変更を予期していないイベント期間中に不要な変更が加えられることがあります。

Change Calendar を更新すると、エントリの作成時に作成した Change Calendar ドキュメントが編集されます。Change Calendar は AWS Systems Manager のツールです。

Change Calendar を更新するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Change Calendar] を選択します。
3. カレンダーのリストから、更新するカレンダーの名前を選択します。

4. カレンダーの詳細ページで、[Actions, Edit] (編集アクション) をクリックします。
5. [Description (説明)] で、説明テキストを変更できます。Change Calendar の名前は編集できません。
6. カレンダーの状態を変更するには、[Calendar type (カレンダータイプ)] で別の値を選択します。これにより、カレンダーに関連付けられているイベント中の変更アクションの動作が逆になることに注意してください。カレンダータイプを変更する前に、カレンダータイプを変更しても、作成済みのイベント中の不要な変更は許可されないことを他の Change Calendar ユーザーと確認する必要があります。

   - [Open by default (デフォルトでオープン)] - カレンダーはオープン (Automation アクションはイベントが開始するまで実行可能) で、関連付けられたイベントの期間中はクローズになります。
   - [Closed by default (デフォルトでクローズ)] - カレンダーはクローズ (Automation アクションはイベントが開始されるまで実行不可) で、関連付けられたイベントの期間中はオープンになります。
7. [Save] を選択します。

   少なくとも 1 つのイベントを追加するまで、カレンダーでアクションを禁止または許可することはできません。イベントを追加する方法については、「Change Calendar イベントの作成」を参照してください。

Change Calendar の共有

AWS Systems Manager コンソールを使用して、AWS Systems Manager のツールである Change Calendar のカレンダーを他の AWS アカウントと共有できます。カレンダーを共有した場合、そのカレンダーは共有アカウントのユーザーに対して読み取り専用になります。メンテナンスウィンドウ、State Manager の関連付け、オートメーションは共有されません。

Change Calendar を共有するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Change Calendar] を選択します。
3. カレンダーのリストから、共有するカレンダーの名前を選択します。
4. カレンダーの詳細ページで、[Sharing] (共有) をクリックします。
5. [Actions, Share] (共有アクション) をクリックします。

6. [Share calendar (カレンダーの共有)] の [Account ID (アカウント ID)] に、有効な AWS アカウント の ID 番号を入力し、[Share (共有)] を選択します。

   共有アカウントのユーザーは Change Calendar を読むことはできますが、変更できません。

Change Calendar の削除

Systems Manager コンソールまたは AWS Command Line Interface (AWS CLI) を使用して、AWS Systems Manager のツールである Change Calendar でカレンダーを削除できます。Change Calendar を削除すると、関連するすべてのイベントが削除されます。

Change Calendar を削除するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Change Calendar] を選択します。
3. カレンダーのリストから、削除するカレンダーの名前を選択します。
4. カレンダーの詳細ページで、[Actions, Delete] (削除アクション) をクリックします。カレンダーの削除を確認するプロンプトが表示されたら、[Delete (削除)] を選択します。

Change Calendar の状態の取得

AWS Systems Manager のツールである Change Calendar では、カレンダーの全体的な状態、または特定の時刻における状態を把握できます。また、カレンダーの状態が次回、`OPEN` から `CLOSED`、またはその逆に変化する時刻を表示することも可能です。

このタスクは、`GetCalendarState` API オペレーションを使用してのみ実行できます。このセクションの手順では、AWS Command Line Interface (AWS CLI) を使用します。

Change Calendar の状態を取得するには

- 次のコマンドを実行して、特定の時刻の 1 つ以上のカレンダーの状態を表示します。`--calendar-names` パラメータは必須ですが、`--at-time` はオプションです。各**##############**をユーザー自身の情報に置き換えます。

  Linux & macOS

```
aws ssm get-calendar-state \
```

```
    --calendar-names "Calendar_name_or_document_ARN_1"
 "Calendar_name_or_document_ARN_2" \
    --at-time "ISO_8601_time_format"
```

以下はその例です。

```
aws ssm get-calendar-state \
    --calendar-names "arn:aws:ssm:us-east-2:123456789012:document/
MyChangeCalendarDocument" "arn:aws:ssm:us-east-2:123456789012:document/
SupportOffHours" \
    --at-time "2020-07-30T11:05:14-0700"
```

Windows

```
aws ssm get-calendar-state ^
    --calendar-names "Calendar_name_or_document_ARN_1"
 "Calendar_name_or_document_ARN_2" ^
    --at-time "ISO_8601_time_format"
```

以下はその例です。

```
aws ssm get-calendar-state ^
    --calendar-names "arn:aws:ssm:us-east-2:123456789012:document/
MyChangeCalendarDocument" "arn:aws:ssm:us-east-2:123456789012:document/
SupportOffHours" ^
    --at-time "2020-07-30T11:05:14-0700"
```

このコマンドによって以下のような情報が返されます。

```
{
    "State": "OPEN",
    "AtTime": "2020-07-30T16:18:18Z",
    "NextTransitionTime": "2020-07-31T00:00:00Z"
}
```

結果には、アカウントによって所有または共有されている指定されたカレンダーエントリのカレンダーの状態 (カレンダーのタイプが DEFAULT_OPEN か DEFAULT_CLOSED か)、--at-time の値として指定された時刻、次の移行の時刻が表示されます。--at-time パラメータを追加しない場合は、現在の時間が使用されます。

> **Note**
>
> 1 つの要求に複数のカレンダーを指定すると、要求内のすべてのカレンダーが開いている場合にのみ、コマンドは OPEN のステータスを返します。要求内の 1 つ以上のカレンダーが閉じている場合、返されるステータスは CLOSED です。

Automation ランブックへの Change Calendar の依存関係の追加

Automation アクションを AWS Systems Manager のツールである Change Calendar に準拠させるには、aws:assertAwsResourceProperty アクションを使用する Automation ランブックにステップを追加します。指定したカレンダーエントリが目的の状態 (GetCalendarState または OPEN) であることを確認するために CLOSED を実行するアクションを設定します。オートメーションランブックは、カレンダーの状態が OPEN である場合にのみ次のステップに進むことができます。以下はオートメーションランブックの YAML ベースのサンプル抜粋です。カレンダーの状態が OPEN (DesiredValues で指定された状態) に一致しない限り、次の手順である LaunchInstance に進むことはできません。

以下に例を示します。

```
mainSteps:
  - name: MyCheckCalendarStateStep
    action: 'aws:assertAwsResourceProperty'
    inputs:
      Service: ssm
      Api: GetCalendarState
      CalendarNames: ["arn:aws:ssm:us-east-2:123456789012:document/SaleDays"]
      PropertySelector: '$.State'
      DesiredValues:
      - OPEN
    description: "Use GetCalendarState to determine whether a calendar is open or
 closed."
    nextStep: LaunchInstance
  - name: LaunchInstance
    action: 'aws:executeScript'
    inputs:
      Runtime: python3.8
...
```

Change Calendar のトラブルシューティング

AWS Systems Manager のツールである Change Calendar を使用したトラブルシューティングでは、以下の情報を使用します。

トピック

- 「カレンダーのインポートに失敗しました」エラー

「カレンダーのインポートに失敗しました」エラー

問題: iCalendar (`.ics`) ファイルをインポートする際、カレンダーのインポートが失敗したことが報告されます。

- 解決策 1 — サポートされているサードパーティーのカレンダープロバイダからエクスポートされたファイルをインポートしていることを確認します。この中には以下が含まれます。
  - Google カレンダー (エクスポート手順)
  - Microsoft Outlook (エクスポート手順)
  - iCloud カレンダー (エクスポート手順)
- 解決策 2 -ソースカレンダーに反復イベントが含まれている場合は、そのイベントの個々の発生がキャンセルまたは削除されていないことを確認します。現在、Change Calendar は、個々のキャンセルを伴う反復イベントのインポートに対応していません。この問題を解決するには、ソースカレンダーから反復イベントを削除し、カレンダーを再エクスポートして Change Calendar に再インポートします。その後、Change Calendar インターフェイスを使用して反復イベントを追加します。詳細については、Change Calendar イベントの作成 を参照してください。
- 解決策 3 - ソースカレンダーに少なくとも 1 つのイベントが含まれていることを確認します。イベントの含まれていない `.ics` ファイルをアップロードしても成功しません。
- 解決策 4 — `.ics` が大きすぎるためにインポートが失敗したと報告された場合は、カレンダーのエントリに関する基本的な詳細のみをエクスポートしていることを確認してください。必要に応じて、エクスポート期間を短縮します。
- 解決策 5 — [Events (イベント)] タブからインポートしようとしている際、エクスポートされたカレンダーのタイムゾーンを Change Calendar が判別できない場合は、「カレンダーのインポートに失敗しました。Change Calendar は有効なタイムゾーンを見つけるられませんでした。カレンダーは [Edit (編集)] メニューからインポートできます」というメッセージが表示される可能性があります。この場合は、[Actions, Edit (アクション、編集)] を選択し、[Edit calendar (カレンダーの編集)] ページからファイルをインポートしてみてください。

- 解決策 6 — インポート前に .ics ファイルを編集しないでください。ファイルの内容を変更しようとすると、カレンダーのデータが破損する可能性があります。インポートを試みる前にファイルを変更した場合は、元のカレンダーからカレンダーを再度エクスポートし、アップロードを再試行してください。

AWS Systems Manager Change Manager

AWS Systems Manager のツールである Change Manager は、アプリケーションの設定とインフラストラクチャに対する運用上の変更をリクエスト、承認、実装、および報告するためのエンタープライズ変更管理フレームワークです。単一の委任管理者アカウントから AWS Organizations を使用すると、複数の AWS アカウント と複数の AWS リージョン 全体で変更を管理することができます。または、ローカルアカウントを使用して、単一の AWS アカウント の変更を管理できます。AWSリソースとオンプレミスリソースの両方に対する変更を管理する場合に Change Manager を使用します。Change Manager の使用を開始するには、Systems Manager コンソールを開きます。ナビゲーションペインで、[Change Manager] を選択します。

Change Manager では、事前に承認された変更テンプレートを使用して、リソースに対する変更プロセスのオートメーションと、運用上の変更を行う際の意図しない結果の回避に役立てることができます。各変更テンプレートでは、次の項目を指定します。

- 変更リクエストの作成時にユーザーが選択できる 1 つ、または複数のオートメーションランブック。リソースに対して行われる変更は、オートメーションランブックに定義されています。作成する変更テンプレートには、カスタムランブックまたはAWS マネージドランブックを含めることができます。ユーザーが変更リクエストを作成するときは、利用可能なランブックからリクエストに含めるランブックを選択できます。さらに、リクエストを作成するユーザーが変更リクエストで任意のランブックを指定できるようにする変更テンプレートを作成できます。
- その変更テンプレートを使用して行われた変更リクエストを確認する必要がある、アカウントのユーザー。
- Amazon Simple Notification Service (Amazon SNS) トピックは、割り当てられた承認者に変更リクエストを確認する準備ができたことを通知するために使用されます。
- ランブックワークフローをモニタリングするために使用される Amazon CloudWatch アラーム。
- 変更テンプレートを使用して作成された変更リクエストのステータスの変更に関する通知を送信するために使用される Amazon SNS トピック。
- 変更テンプレートの分類とフィルタリングに使用する変更テンプレートに適用するタグ。
- 変更テンプレートから作成された変更リクエストを承認ステップなしで実行できるかどうか (自動承認リクエスト)。

Systems Manager のもうひとつのツールである Change Calendar との統合により、Change Manager は重要なビジネスイベントとのスケジュール競合を回避しながら、変更を安全に実装するためにも役立ちます。Change Manager の AWS Organizations および AWS IAM Identity Center との統合により、既存の ID 管理システムを使用して、シングルアカウントから組織全体の変更を管理できるようになります。Change Managerから変更の進捗状況を監視して、組織全体における運用上の変更を監査することができるため、可視性と説明責任が向上します。

Change Manager は、継続的インテグレーション (CI) プラクティスと継続的デリバリー (CD) 手法の安全管理を補完します。例外がある場合、または承認が必要な場合を除き、Change Managerは CI/CD パイプラインなどの自動化されたリリースプロセスの一環として行われる変更を対象としません。

Change Manager の仕組み

標準または緊急の運用変更を行う必要性が特定されると、組織内の人物が、組織、またはアカウントでの使用のために作成された変更テンプレートのいずれかに基づく変更リクエストを作成します。

リクエストされた変更が手動承認を必要とする場合、Change Manager は Amazon SNS 通知を通じて、指定された承認者に変更リクエストの確認の準備ができたことを通知します。変更テンプレートで変更リクエストの承認者を指定したり、変更リクエスト自体で承認者を指定したりできます。レビューワーは、テンプレートごとに異なる担当者を割り当てることができます。例えば、マネージドノードに対する変更のリクエストを承認する必要がある 1 人のユーザー、ユーザーグループ、または AWS Identity and Access Management (IAM) ロールを割り当てて、データベース変更については別のユーザー、グループ、または IAM ロールを割り当てられます。変更テンプレートで自動承認が許可され、リクエスタのユーザーポリシーで禁止されていない場合、ユーザーはレビューステップなしでリクエストのオートメーションランブックを実行することもできます (変更のフリーズイベントを除く)。

変更テンプレートごとに、最大 5 レベルの承認者を追加できます。例えば、まずテクニカルレビューワーに変更テンプレートから作成された変更リクエストを承認してもらってから、1 人以上のマネージャに第 2 レベルの承認を求めます。

Change Manager は AWS Systems Manager Change Calendar と統合されています。リクエストされた変更が承認されると、システムはまず、そのリクエストがスケジュールされた他のビジネスアクティビティと競合していないかどうかを判断します。競合が検出された場合、Change Manager は変更をブロックするか、ランブックワークフローを開始する前に追加の承認を要求することができます。例えば、営業時間内の変更のみを許可して、チームが予想外の問題を管理できるようにすることが可能です。営業時間内外での実行をリクエストする変更については、変更凍結承認者という形でよ

り高いレベルの経営陣の承認を義務付けることができます。緊急変更の場合、Change Manager は変更リクエストの承認後、競合について Change Calendar をチェックするステップ、またはイベントをブロックするステップを省略できます。

承認された変更を実装するときは、Change Manager が関連する変更リクエストで指定されているオートメーションランブックを実行します。ランブックワークフローの実行時には、承認された変更リクエストで定義されている操作のみが許可されます。このアプローチは、変更の実装時における意図しない結果を回避するために役立ちます。

ランブックワークフローの実行時に実施できる変更を制限することに加えて、Change Manager は同時実行性とエラーしきい値の制御にも役立ちます。ユーザーは、ランブックワークフローが一度に実行できるリソースの数、一度に変更を実行できるアカウントの数、およびプロセスを停止し、ロールバックする (ランブックにロールバックスクリプトが含まれている場合) までに許可する失敗の回数を選択できます。また、CloudWatch アラームを使用して、行われている変更の進捗状況をモニタリングすることもできます。

ランブックワークフローが完了したら、行われた変更の詳細を確認できます。これらの詳細には、変更リクエストの理由、使用された変更テンプレート、変更のリクエスト者と承認者、および変更の実装方法が含まれます。

詳細情報

Introducing AWS Systems ManagerChange Manager (AWS ニュースブログ)

Change Managerは、どのような運用上のメリットを提供できますか?

Change Manager には以下のような利点があります。

- サービスの中断とダウンタイムのリスクを軽減する

  Change Manager では、ランブックワークフローの実行時に承認された変更のみが実施されるようにすることで、運用上の変更を安全にします。計画されていない、またはレビューされていない変更は、ブロックすることができます。Change Managerは、何時間にも及ぶ高額な調査やバックトラッキングが必要となるような、人為的なエラーに起因する意図しない結果を避けるために役立ちます。
- 変更履歴に関する詳細な監査とレポートを取得する

  Change Managerは、組織全体で行われた変更、それらの変更の意図、およびそれらの承認者と実装者に関する詳細を報告し、監査するための一貫した方法を用いて説明責任を提供します。

- スケジュールの競合または違反を回避する

  Change Managerは、組織のためのアクティブな変更カレンダーに基づいて、祝祭日イベント、または新製品のローンチなどのスケジュールの競合を検出できます。ランブックワークフローの実行を営業時間内に限定する、または追加の承認がある場合にのみ許可することが可能です。

- 変化するビジネスに合わせて変更要件を導入する

  異なる事業期間には、異なる変更管理要件を実装することができます。例えば、月末のレポート作成、納税申告時期、またはその他の重要な事業期間中には、変更をブロックする、または不必要な運用上のリスクを生じる可能性がある変更に対して取締役レベルの承認を義務付けることができます。

- 複数のアカウント全体における変更を一元的に管理する

  Organizations との統合により、Change Manager は、すべての組織単位 (OU) 全体における変更を単一の委任管理者アカウントから管理することを可能にします。Change Manager は、組織全体での使用、または一部の OU のみでの使用のために有効化できます。

Change Manager はどのようなユーザーに適していますか?

Change Managerは、次のような AWS のお客様と組織に適しています。

- クラウドまたはオンプレミス環境に対して行われる運用上の変更の安全性とガバナンスを向上させたいとお考えの AWS のお客様。
- チーム間のコラボレーションと可視性の向上、ダウンタイムの回避によるアプリケーションの可用性の改善、および手動タスクと反復的なタスクに関連するリスクの軽減を求める組織。
- 変更管理のベストプラクティスに従う必要がある組織
- アプリケーションの設定とインフラストラクチャに対して行われた変更について、完全に監査可能な履歴を必要とするお客様。

Change Manager の主な特徴は何ですか。

Change Managerの主な特徴には以下が含まれます。

- 変更管理のベストプラクティスに対する統合サポート

  Change Managerでは、選択した変更管理のベストプラクティスを運用に適用することができ、以下のオプションを有効にすることが可能です。

  - Change Calendarをチェックしてイベントが現在制限されているかどうかを確認し、変更がカレンダーのオープン期間中にのみ行われるようにする。
  - 変更凍結承認者からの追加の承認によって、制限されたイベント中における変更を許可する。
  - すべての変更テンプレートに対して CloudWatch アラームを指定する必要があります。
  - 変更リクエストの作成に使用する前に、アカウントで作成されたすべての変更テンプレートを確認および承認する必要があります。
- カレンダーのクローズ期間と緊急の変更リクエストに対する異なる承認経路

  制限されたイベントに対して Change Calendar をチェックするオプションを有効にして、そのイベントが完了になるまで承認済みの変更リクエストをブロックすることができます。ただし、カレンダーがクローズ状態になっている場合でも変更を行うことを許可できる 2 番目の承認者 (変更凍結承認者) グループを指定することも可能です。緊急の変更テンプレートを作成することもできます。緊急の変更テンプレートを使用して作成された変更リクエストには引き続き通常の承認が必要ですが、カレンダー制限の対象にはならず、変更凍結承認も必要ありません。
- ランブックワークフローの開始方法とタイミングを制御する

  ランブックワークフローは、スケジュールに従って開始する、または承認が完了され次第開始することができます (カレンダー制限規則の対象となります)。
- 組み込み通知のサポート

  組織内で変更テンプレートと変更リクエストを確認および承認するユーザーを指定します。Amazon SNS トピックを変更テンプレートに割り当てると、その変更テンプレートで作成された変更リクエストのステータスの変更に関する通知をトピックのサブスクライバーに送信します。
- AWS Systems Manager Change Calendarとの統合

  Change Managerでは、管理者が指定された期間内におけるスケジュール変更を制限することができます。例えば、営業時間内の変更のみを許可するポリシーを作成して、チームが問題に対処できるようにすることが可能です。重要なビジネスイベント中における変更を制限することもできます。例えば、小売業者は、大規模な販売イベント中に変更を制限することが可能です。制限期間中に追加の承認を義務付けることもできます。
- AWS IAM Identity Center との統合と Active Directory のサポート

  IAM Identity Center との統合により、組織のメンバーは共通のユーザー のアイデンティティで Systems Manager を使用し、AWS アカウント にアクセスしてリソースを管理することができま

す。IAM Identity Center を使用することで、AWS 全体のアカウントへのアクセス権をユーザーに割り当てることができます

Active Directory との統合は、Active Directory アカウントのユーザーを Change Manager 操作用に作成された変更テンプレートの承認者として割り当てることを可能にします。

- Amazon CloudWatch アラームとの統合

  Change Manager は CloudWatch アラームと統合されています。Change Manager はランブックのワークフロー中に CloudWatch アラームをリッスンし、通知の送信などアラームに対して定義されたあらゆるアクションを実行します。

- AWS CloudTrail Lake との統合

  AWS CloudTrail Lake にイベントデータストアを作成すると、アカウントまたは組織で実行されたリクエストにより加えられた変更に関して、監査可能な情報を表示できます。保存されるイベント情報には、以下のような詳細が含まれます。

  - 実行された API アクション
  - これのアクションに含まれるリクエストパラメータ
  - アクションを実行したユーザー
  - 処理中に更新されたリソース

- AWS Organizations との統合

  Organizations が提供するクロスアカウント機能を使用することで、組織内の OU での Change Manager 操作の管理に委任管理者アカウントを使用することができます。Organizations の管理アカウントで、委任管理者アカウントにするアカウントを指定できます。どの OU でChange Managerを使用できるかを制御することも可能です。

Change Manager の使用料金はかかりますか?

はい。Change Managerの料金は従量課金制に基づいて設定されています。お支払いいただくのは、使用分の料金だけです。詳細については、AWS Systems Manager 料金を参照してください。

Change Managerの主要コンポーネントは何ですか?

組織、またはアカウント内での変更プロセスの管理に使用されるChange Managerコンポーネントには、以下が含まれます。

委任された管理者アカウント

組織全体でChange Managerを使用する場合は、委任管理者アカウントを使用します。これは、Change Manager を含む Systems Manager 全体の操作アクティビティを管理するためのアカウントとして指定される AWS アカウント です。委任管理者アカウントは、組織全体の変更アクティビティを管理します。Change Managerでの使用のために組織をセットアップするときは、どのアカウントがこの役割を担うかを指定します。委任管理者アカウントは、それが割り当てられている組織単位 (OU) 唯一のメンバーである必要があります。Change Manager を単一の AWS アカウント のみで使用する場合、委任管理者アカウントは必要ありません。

> **Important**
>
> 組織全体で Change Manager を使用する場合は、常に委任管理者アカウントから変更を行うことをお勧めします。組織内の他のアカウントから変更を行うことはできますが、それらの変更は、委任管理者アカウントで報告されず、表示することもできません。

変更テンプレート

変更テンプレートは、必要な承認、利用可能なランブック、変更リクエストの通知オプションなどの項目を定義する、Change Manager の設定のコレクションです。

組織またはアカウント内のユーザーによって作成された変更テンプレートは、承認プロセスを経てから使用することを義務付けることができます。

Change Manager は、2 種類の変更テンプレートをサポートしています。緊急の変更テンプレートに基づく承認済み変更リクエストの場合、Change Calendar にブロッキングイベントがある場合でも、要求された変更を行うことができます。標準的な変更テンプレートに基づく承認済みの変更リクエストについては、指定された 変更凍結イベント承認者から追加の承認を受け取っている場合を除いて、Change Calendar にブロッキングイベントがある場合にリクエストされた変更を行うことはできません。

変更リクエスト

変更リクエストは、AWS またはオンプレミス環境の 1 つ以上のリソースを更新する Automation ランブックを実行するための Change Manager のリクエストです。変更リクエストは、変更テンプレートを使用して作成されます。

変更リクエストを作成するときは、組織またはアカウント内の 1 人、または複数人の承認者がリクエストを確認して承認する必要があります。必要な承認がなければ、リクエストされた変更を適用するランブックワークフローの実行は許可されません。

システムでは、変更リクエストは AWS Systems Manager OpsCenter の OpsItem の一種です。ただし、`/aws/changerequest` タイプの OpsItems は OpsCenter に表示されません。OpsItems である変更リクエストには、他のタイプの OpsItems に課されているものと同じクォータが適用されます。

さらに、変更リクエストをプログラム的に作成するには、`CreateOpsItem` API オペレーションを呼び出しません。代わりに、`StartChangeRequestExecution` API オペレーションを使用します。ただし、変更リクエストは直ちに実行されず、承認を受ける必要があります。また、ワークフローの実行を妨げるブロッキングイベントが Change Calendar に存在していない必要もあります。`StartChangeRequestExecution` アクションは、承認が受け取られており、カレンダーがブロックされていない (またはブロッキングカレンダーイベントを回避する許可が付与されている) 場合に完了することができます。

Runbook ワークフロー

ランブックワークフローは、クラウドまたはオンプレミス環境にあるターゲットリソースに対して行われるリクエストされた変更のプロセスです。各変更リクエストには、リクエストされた変更を行うために使用される単一のオートメーションランブックが指定されています。ランブックワークフローは、必要な承認がすべて付与され、Change Calendar にブロッキングイベントがなくなったときに発生します。変更が特定の日時にスケジュールされている場合、ランブックワークフローは、すべての承認が受け取られ、カレンダーがブロックされていないとしても、スケジュールされた日時まで開始されません。

トピック

- Change Manager を設定する
- 「Change Manager」 の使用
- Change Manager アクティビティの監査と口グ記録
- Change Manager のトラブルシューティング

Change Manager を設定する

AWS Systems Manager のツールである Change Manager を使用して、AWS Organizations で構成されている組織全体、またはシングル AWS アカウントの変更を管理できます。

Change Manager を組織で使用している場合は、「組織の Change Manager の設定 (管理アカウント)」トピックから始めて、「Change Managerオプションとベストプラクティスの設定」に進みます。

単一のアカウントで Change Manager を使用している場合は、直接「Change Managerオプションとベストプラクティスの設定」に進んでください。

> **Note**
>
> 単一のアカウントで Change Manager を使用し始めて、そのアカウントが後ほど Change Manager が有効化されている組織単位に追加された場合は、単一のアカウントでの設定が無視されます。

トピック

- 組織の Change Manager の設定 (管理アカウント)
- Change Managerオプションとベストプラクティスの設定
- Change Manager のロールとアクセス許可の設定
- 自動承認のランブックワークフローへのアクセスを制御する

組織の Change Manager の設定 (管理アカウント)

このトピックのタスクは、AWS Organizations で設定された組織で、AWS Systems Manager のツールである Change Manager を使用している場合に適用されます。単一の AWS アカウント のみで Change Manager を使用する場合は、「Change Managerオプションとベストプラクティスの設定」トピックに進んでください。

Organizations の管理アカウントとして機能する AWS アカウント で、 内のこのセクションのタスクを実行します。管理アカウントおよびその他の Organizations の概念については、「AWS Organizations Organizations の用語と概念」を参照してください。

先に進む前に、Organizations を有効にし、お使いのアカウントを管理アカウントとして指定する必要がある場合は、AWS Organizations ユーザーガイドの「組織の作成と管理」を参照してください。

> **Note**
>
> 以下の AWS リージョン ではこのセットアッププロセスを実行できません。

- 欧州 (ミラノ) (eu-south-1)
- 中東 (バーレーン) (me-south-1)
- アフリカ (ケープタウン) (af-south-1)
- アジアパシフィック (香港) (ap-east-1)

この手順では、確実に管理アカウントの別のリージョンで作業するようにしてください。

セットアップ手順の最中に、AWS Systems Manager のツールである Quick Setup で以下の主要タスクを実行します。

- タスク 1: 組織の委任管理者アカウントを登録する

  Change Managerを使用して実行される変更関連のタスクは、メンバーアカウントの 1 つで管理されます。このアカウントは、委任管理者アカウントとして指定されるアカウントです。Change Manager に登録する委任管理者アカウントは、すべての Systems Manager 操作のための委任管理者アカウントになります。(他の AWS のサービスに対する委任管理者アカウントがある可能性があります)。Change Manager の管理者アカウント (管理アカウントとは異なります) は、変更テンプレート、変更リクエスト、およびそれぞれの承認を含めた、組織全体での変更アクティビティを管理します。委任管理者アカウントでは、Change Manager操作に対するその他の設定オプションも指定します。

  > **Important**
  >
  > 委任管理者アカウントは、Organizations でそれが割り当てられている組織単位 (OU) 唯一のメンバーである必要があります。

- タスク 2: Change Manager操作に使用する変更依頼者ロール、またはカスタム職務機能に対するランブックアクセスポリシーを定義して指定する

  Change Manager で変更リクエストを作成するには、メンバーアカウントのユーザーに AWS Identity and Access Management (IAM) アクセス許可を付与する必要があります。このアクセス許可により、ユーザーは、ユーザーが使用できるように選択したオートメーションランブックと変更テンプレートにのみアクセスできます。

> **Note**
>
> ユーザーが変更リクエストを作成するときは、まず変更テンプレートを選択します。この変更テンプレートでは複数のランブックを使用できますが、ユーザーは変更リクエストごとに 1 つのランブックしか選択できません。変更テンプレートは、ユーザーがリクエストに使用できるランブックを含めることができるように設定することもできます。

Change Manager は、必要な許可を付与するために職務機能という概念を使用します。この概念は IAM でも使用されています。IAM での職務機能の AWS 管理ポリシーとは異なり、ユーザーは Change Manager 職務機能の名前と、それらの職務機能に対する IAM アクセス許可の両方を指定します。

職務機能を設定するときは、カスタムポリシーを作成して、変更管理タスクの実行に必要な許可のみを提供することをお勧めします。例として、定義した職務機能に基づいて、特定のランブック一式にユーザーを制限する許可を指定できます。

例えば、`DBAdmin` という名前の職務機能を作成できます。この職務機能では、`AWS-CreateDynamoDbBackup` や `AWSConfigRemediation-DeleteDynamoDbTable` などの Amazon DynamoDB データベースに関連するランブックに必要なアクセス許可のみを付与できます。

別の例として、`AWS-ConfigureS3BucketLogging` や `AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock` などの Amazon Simple Storage Service (Amazon S3) バケットに関連するランブックの使用に必要な許可のみを一部のユーザーに付与することもできます。

Change Manager のための Quick Setup の設定プロセスは、作成する管理者ロールへの適用に利用できる完全な Systems Manager 管理者権限のセットも作成します。

デプロイする各Change ManagerのQuick Setup設定は、選択した組織単位でChange Managerテンプレートとオートメーションランブックを実行する許可を持つ委任管理者アカウントに職務機能を作成します。Change Manager の Quick Setup 設定は最大で 15 個作成できます。

- タスク 3: Change Managerで使用する組織内のメンバーアカウントを選択する

  Change Manager は、Organizations でセットアップされているすべての組織単位、およびそれらが運用されているすべての AWS リージョン 内のすべてのメンバーアカウントで使用できます。必要に応じて、Change Managerを一部の組織単位のみで使用することもできます。

> **Important**
>
> この手順を開始する前に、手順にあるステップに目を通して、選択する設定と、付与する許可を理解しておくことを強くお勧めします。特に、作成するカスタム職務機能と、各職務機能に割り当てる許可を計画しておくようにしてください。そうすることによって、この後で作成する職務機能ポリシーを個々のユーザー、ユーザーグループ、または IAM ロールにアタッチするときに、それらのユーザーとグループを対象とする許可のみが付与されることを確実にすることができます。
>
> ベストプラクティスとして、まず、AWS アカウント 管理者のログイン情報を使用して、委任された管理者アカウントを設定します。その後、変更テンプレートを作成し、それぞれが使用するランブックを特定した後、職務機能とそのアクセス権限を設定します。

組織で使用する Change Manager を設定するには、Systems Manager コンソールの Quick Setup エリアで次のタスクを実行します。

このタスクは、組織用に作成する職務機能ごとに繰り返し実行します。作成する各職務機能には、異なる一連の組織単位に対する許可を設定することができます。

Organizations の管理アカウントで Change Manager の組織を設定するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Quick Setup] を選択します。
3. Change Manager カードで [Create] (作成) を選択します。
4. [Delegated administrator account (委任管理者アカウント)] に、Change Manager の変更テンプレート、変更リクエスト、およびランブックワークフローの管理に使用する の AWS アカウント の ID を入力します。

   以前に Systems Manager 用の委任管理者アカウントを指定した場合は、このフィールドにその ID が既に入力されています。

   > **Important**
   >
   > 委任管理者アカウントは、Organizations でそれが割り当てられている組織単位 (OU) 唯一のメンバーである必要があります。
   >
   > 登録した委任管理者アカウントが後ほどそのロールから登録解除された場合は、システムが、解除と当時に Systems Manager 操作を管理するための許可を削除します。Quick

Setupに戻って別の委任管理者アカウントを指定し、すべての職務機能と許可を再度指定する必要があることに留意してください。
組織全体で Change Manager を使用する場合は、常に委任管理者アカウントから変更を行うことをお勧めします。組織内の他のアカウントから変更を行うことはできますが、それらの変更は、委任管理者アカウントで報告されず、表示することもできません。

5. [Permissions to request and make changes] (変更をリクエストして実行する許可) セクションで、以下を実行します。

> **Note**
>
> 作成するデプロイメント設定は、それぞれ 1 つの職務機能のみに対する許可ポリシーを提供します。操作で使用する変更テンプレートを作成したら、後で Quick Setup に戻って、さらにジョブ機能を作成できます。

管理者ロールを作成する – すべての AWS アクションに対する IAM アクセス許可を持つ管理者職務機能については、以下を実行します。

> **Important**
>
> ユーザーに完全な管理者許可の付与は頻繁に行わず、ユーザーのロールに完全な Systems Manager アクセスが必要な場合のみにする必要があります。Systems Manager アクセスに関するセキュリティ面での考慮事項についての重要な情報は、「AWS Systems Manager のためのアイデンティティおよびアクセス管理」および「Systems Manager のセキュリティに関するベストプラクティス」を参照してください。

1. [Job function] (職務機能) には、このロールとそのアクセス許可を識別するための名前 (例: **`MyAWSAdmin`**) を入力します。
2. [Role and permissions] (ロールとアクセス許可) オプションには、[Administrator permissions] (管理者許可) を選択します。

その他の職務機能を作成する – 管理者ロール以外のロールを作成するには、以下を実行します。

1. [Job function] (職務機能) に、このロールを識別し、その許可を示す名前を入力します。選択する名前は、DBAdmin または S3Admin など、許可を提供するランブックの範囲を表している必要があります。
2. [Role and permissions] (ロールとアクセス許可) オプションには、[Custom permissions] (カスタム許可) を選択します。
3. [Permissions policy editor] (許可ポリシーエディタ) に、この職務機能に付与する IAM アクセス許可を JSON 形式で入力します。

> **Tip**
>
> IAM ポリシーエディタを使用してポリシーを作成してから、ポリシー JSON を [Permissions policy] (アクセス許可ポリシー) フィールドに貼り付けることが推奨されます。

サンプルポリシー: DynamoDB データベース管理

例えば、職務機能がアクセスする必要がある Systems Manager ドキュメント (SSM ドキュメント) を使用するためのアクセス許可を提供するポリシーコンテンツから始めることができます。以下は、DynamoDB データベースに関連する AWS 管理の Automation ランブックのすべてと、米国東部 (オハイオ) リージョン (us-east-2) のサンプル AWS アカウント 123456789012 で作成された 2 つの変更テンプレートに対するアクセス権を付与するサンプルポリシーコンテンツです。

このポリシーには、Change Calendar での変更リクエストの作成に必要な StartChangeRequestExecution オペレーションのアクセス許可も含まれます。

> **Note**
>
> この例は包括的ではありません。データベース、およびノードどのその他の AWS リソースを使用するには、追加のアクセス権限が必要になる場合があります。

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

```
        {
            "Effect": "Allow",
            "Action": [
                "ssm:CreateDocument",
                "ssm:DescribeDocument",
                "ssm:DescribeDocumentParameters",
                "ssm:DescribeDocumentPermission",
                "ssm:GetDocument",
                "ssm:ListDocumentVersions",
                "ssm:ModifyDocumentPermission",
                "ssm:UpdateDocument",
                "ssm:UpdateDocumentDefaultVersion"
            ],
            "Resource": [
                "arn:aws:ssm:region:*:document/AWS-CreateDynamoDbBackup",
                "arn:aws:ssm:region:*:document/AWS-AWS-DeleteDynamoDbBackup",
                "arn:aws:ssm:region:*:document/AWS-DeleteDynamoDbTableBackups",
                "arn:aws:ssm:region:*:document/AWSConfigRemediation-
DeleteDynamoDbTable",
                "arn:aws:ssm:region:*:document/AWSConfigRemediation-
EnableEncryptionOnDynamoDbTable",
                "arn:aws:ssm:region:*:document/AWSConfigRemediation-
EnablePITRForDynamoDbTable",
                "arn:aws:ssm:region:123456789012:document/MyFirstDBChangeTemplate",
                "arn:aws:ssm:region:123456789012:document/MySecondDBChangeTemplate"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "ssm:ListDocuments",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ssm:StartChangeRequestExecution",
            "Resource": "arn:aws:ssm:region:123456789012:automation-definition/*:*"
        }
    ]
}
```

IAM ポリシーの詳細については、IAM ユーザーガイドの「AWS リソースのアクセス管理」および「IAM ポリシーの作成」を参照してください。

6. [Targets] (ターゲット) セクションで、作成している職務機能の許可を組織全体に付与するか、一部の組織単位のみに付与するかを選択します。

   [Entire organization] (組織全体) を選択した場合は、ステップ 9 に進みます。

   [Custom] (カスタム) を選択した場合は、ステップ 8 に進みます。
7. [Target OUs] (ターゲット OU) セクションで、Change Managerで使用する組織単位のチェックボックスをオンにします。
8. [Create] (作成) を選択します。

システムが組織のためのChange Managerのセットアップを完了したら、デプロイメントの概要が表示されます。この概要情報には、設定した職務機能用に作成されたロールの名前が含まれています。例えば、`AWS-QuickSetup-SSMChangeMgr-DBAdminInvocationRole` と指定します。

> **Note**
>
> Quick Setupは、AWS CloudFormation StackSets を使用して設定をデプロイします。AWS CloudFormation コンソールでは、完了したデプロイメント設定に関する情報を表示することもできます。StackSets の詳細については、AWS CloudFormation ユーザーガイドの「AWS CloudFormation StackSets の操作」を参照してください。

次のステップは、追加のChange Managerオプションの設定です。このタスクは、委任管理者アカウント、または Change Manager での使用のために有効化した組織単位内の任意のアカウントで実行することができます。このタスクでは、ユーザーアイデンティティ管理オプションの選択、変更テンプレートと変更リクエストをレビューして承認または拒否できるユーザーの指定、および組織に対して有効化するベストプラクティスオプションの選択などのオプションを設定します。詳細については、Change Managerオプションとベストプラクティスの設定 を参照してください。

Change Managerオプションとベストプラクティスの設定

このセクションのタスクは、組織全体で使用するか、シングル AWS アカウントで使用するかにかかわらず、AWS Systems Manager のツールである Change Manager を実行する必要があります。

組織で Change Manager を使用する場合は、委任管理者アカウント、または Change Manager での使用のために有効化した組織単位内の任意のアカウントで以下のタスクを実行することができます。

トピック

- タスク 1: Change Managerユーザー ID 管理とテンプレートレビューワーの設定

- タスク 2: Change Manager 変更凍結イベント承認者とベストプラクティスの設定
- Change Manager 通知用の Amazon SNS トピックの設定

タスク 1: Change Managerユーザー ID 管理とテンプレートレビューワーの設定

この手順のタスクは、Change Managerに初めてにアクセスするときに実行します。これらの設定は、Change Manager に戻り [Settings] (設定) タブの [Edit] (編集) を選択することで、後ほど更新できます。

Change Managerユーザー ID 管理とテンプレートレビューワーを設定する

1. AWS Management Consoleにサインインします。

   組織のために Change Manager を使用している場合は、委任管理者アカウントの認証情報を使用してサインインします。ユーザーには、Change Manager 設定を更新するための AWS Identity and Access Management (IAM) アクセス許可が必要です。
2. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
3. ナビゲーションペインで、[Change Manager] を選択します。
4. サービスのホームページで、使用可能なオプションに応じて、次のいずれかを実行します。

   - AWS Organizations で Change Manager を使用する場合は、[Set up delegated account] (委任アカウントをセットアップする) をクリックします。
   - Change Manager を単一の AWS アカウント で使用する場合は、[Change Manager のセットアップ] をクリックします。

     -または-

     サンプル変更リクエストの作成、[Skip] を選択し、[設定] タブに進みます。
5. [User identity management] (ユーザー ID 管理) には、次のいずれかを選択します。

   - AWS Identity and Access Management (IAM) – 既存のユーザー、グループ、ロールを使用して、Change Manager でリクエストの作成と承認、その他のアクションを実行するユーザーを識別します。
   - AWS IAM Identity Center (IAM Identity Center) – IAM Identity Center でアイデンティティの作成と管理を行うか、既存のアイデンティティソースに接続して、Change Manager でアクションを実行するユーザーを識別することができます。

6. [Template reviewer notification] (テンプレートレビューワーの通知) セクションで、新しい 変更テンプレートまたは変更テンプレートバージョンをレビューする準備が整ったことをテンプレートレビューワーに通知するために使用する Amazon Simple Notification Service (Amazon SNS) トピックを指定します。選択する Amazon SNS トピックが、テンプレートレビューワーに通知を送信するように設定されていることを確認します。

   変更テンプレートのレビューワーに通知するための Amazon SNS トピックの作成と設定については、「Change Manager 通知用の Amazon SNS トピックの設定」を参照してください。

   1. テンプレートレビューワー通知の Amazon SNS トピックを指定するには、以下のいずれかを選択します。

      - Enter an SNS Amazon Resource Name (ARN)(SNS Amazon リソースネーム (ARN) を入力) – [Topic ARN (トピック ARN) には、既存の Amazon SNS トピックの ARN を入力します。このトピックは、組織のどのアカウントのものでも使用できます。
      - Select an existing SNS topic (既存の SNS トピックを選択) – [Target notification topic] (ターゲット通知トピック) には、現在 AWS アカウント にある既存の Amazon SNS トピックの ARN を選択します。(このオプションは、現在の AWS アカウント と AWS リージョン で Amazon SNS トピックをまだ作成していない場合は使用できません)。

      > **Note**
      >
      > 選択する Amazon SNS トピックは、送信する通知とその送信先のサブスクライバーを指定するように設定されている必要があります。Amazon SNアクセスポリシーは、Change Manager が通知を送信できるように、Systems Manager にアクセス許可も付与する必要があります。詳細については、Change Manager 通知用の Amazon SNS トピックの設定 を参照してください。

   2. [Add notification] (通知を追加) をクリックします。

7. [Change template reviewers] (変更テンプレートレビューワー) セクションで、運用での使用に先立って新しい変更テンプレートまたは変更テンプレートバージョンをレビューする、組織またはアカウント内のユーザーを選択します。

   変更テンプレートレビューワーは、他のユーザーが Change Manager ランブックワークフローでの使用のために提出したテンプレートの適合性とセキュリティを検証する責任を担います。

   次の手順を実行して、変更テンプレートのレビューワーを選択します。

   1. [Add] (追加) をクリックします。

2. 変更テンプレートレビューワーとして割り当てる各ユーザー、グループ、または IAM ロールの名前の横にあるチェックボックスをオンにします。
3. [Add approvers] (承認者を追加) をクリックします。

8. [Submit] (送信) をクリックします。

この初期セットアッププロセスを完了したら、タスク 2: Change Manager 変更凍結イベント承認者とベストプラクティスの設定 にあるステップに従って、追加のChange Manager設定とベストプラクティスの設定を行います。

タスク 2: Change Manager 変更凍結イベント承認者とベストプラクティスの設定

タスク 1: Change Managerユーザー ID 管理とテンプレートレビューワーの設定 のステップを完了したら、変更凍結イベント 時の変更リクエストを処理する追加のレビューワーを指定し、Change Manager 操作に対して有効化する利用可能なベストプラクティスを指定できます。

変更凍結イベントとは、現在の変更カレンダーに制限が設定されていることを意味します (AWS Systems Manager Change Calendarのカレンダー状態は CLOSED です)。このような場合、変更リクエストを処理する通常の承認者に加えて、または、自動承認が可能なテンプレートを使用して変更リクエストを作成する場合、変更凍結承認者もこの変更リクエストを実行するためのアクセス許可を付与する必要があります。許可が付与されなければ、カレンダーの状態が再度 OPEN になるまで変更は処理されません。

Change Managerの変更凍結イベント承認者とベストプラクティスを設定する

1. ナビゲーションペインで、Change Manager を選択します。
2. [Settings] (設定) タブを選択し、[Edit] (編集) をクリックします。
3. [Approvers for change freeze events] (変更凍結イベントの承認者) セクションで、Change Calendarで使用されているカレンダーが CLOSED 状態の場合でも変更の実行を承認できる、組織またはアカウント内のユーザーを選択します。

> **Note**
>
> 変更凍結レビューを有効にするには、[Best practices] (ベストプラクティス) にある [Check Change Calendar for restricted change events] (制限された変更イベントについて変更カレンダーをチェックする) オプションを有効にする必要があります。

以下を実行して変更凍結イベントの承認者を選択します。

1. [Add] (追加) をクリックします。
2. 変更凍結イベントの承認者として割り当てる各ユーザー、グループ、または IAM ロールの名前の横にあるチェックボックスをオンにします。
3. [Add approvers] (承認者を追加) をクリックします。

4. ページの下部にある [Best practices] (ベストプラクティス) セクションで、以下の各オプションに実施するベストプラクティスを有効にします。

- オプション: [Check Change Calendar for restricted change events] (制限された変更イベントについて変更カレンダーをチェックする)

  Change Manager が、スケジュールされたイベントによって変更がブロックされていないことを確認するためにChange Calendarのカレンダーをチェックすることを指定するには、まず [Enabled] (有効) チェックボックスをオンにしてから、[Change Calendar] (変更カレンダー) リストから制限されたイベントをチェックするカレンダーを選択します。

  Change Calendar の詳細については、「AWS Systems Manager Change Calendar」を参照してください。

- オプション: [SNS topic for approvers for closed events] (クローズドイベントの承認者のための SNS トピック)

  1. 以下のいずれかを選択して、アカウント内の Amazon Simple Notification Service (Amazon SNS) トピックを指定します。これは、変更凍結イベント中に、承認者に通知を送信するために使用されます。([Best practices] (ベストプラクティス) の上にある [Approvers for change freeze events] (変更凍結イベントの承認者) セクションでも承認者を指定する必要があることに注意してください。)

     - Enter an SNS Amazon Resource Name (ARN)(SNS Amazon リソースネーム (ARN) を入力) – [Topic ARN (トピック ARN) には、既存の Amazon SNS トピックの ARN を入力します。このトピックは、組織のどのアカウントのものでも使用できます。
     - Select an existing SNS topic (既存の SNS トピックを選択) – [Target notification topic] (ターゲット通知トピック) には、現在 AWS アカウント にある既存の Amazon SNS トピックの ARN を選択します。(このオプションは、現在の AWS アカウント と AWS リージョン で Amazon SNS トピックをまだ作成していない場合は使用できません)。

     > **Note**
     >
     > 選択する Amazon SNS トピックは、送信する通知とその送信先のサブスクライバーを指定するように設定されている必要があります。Amazon SNアクセスポリ

シーは、Change Manager が通知を送信できるように、Systems Manager にアクセス許可も付与する必要があります。詳細については、Change Manager 通知用の Amazon SNS トピックの設定 を参照してください。

2. [Add notification] (通知を追加) をクリックします。

- オプション: [Require monitors for all templates] (すべてのテンプレートにモニタリングを義務付ける)

  組織またはアカウントのすべてのテンプレートに変更操作を監視するための Amazon CloudWatch アラームが指定されていることを確実にしたい場合は、[Enabled] (有効) チェックボックスをオンにします。

- オプション: [Require template review and approval before use] (使用前のテンプレートのレビューと承認を義務付ける)

  レビューと承認が完了したテンプレートに基づかずに変更リクエストが作成されたり、ランブックワークフローが実行されたりするこがないようにするには、[Enabled] (有効) チェックボックスをオンにします。

5. [Save] を選択します。

Change Manager 通知用の Amazon SNS トピックの設定

AWS Systems Manager のツールである Change Manager を設定して、変更リクエストおよび変更テンプレートに関連するイベントについて、Amazon Simple Notification Service (Amazon SNS) トピックに通知を送信できます。トピックを追加するChange Managerイベントの通知を受け取るには、以下のタスクを完了します。

トピック

- タスク 1: Amazon SNS トピックを作成してサブスクライブする
- タスク 2: Amazon SNS アクセスポリシーを更新する
- タスク 3: (オプション) AWS Key Management Service アクセスポリシーを更新する

タスク 1: Amazon SNS トピックを作成してサブスクライブする

まず、Amazon SNS トピックを作成し、サブスクライブする必要があります。詳細については、Amazon Simple Notification Service デベロッパーガイドの「Amazon SNS トピックの作成」および「Amazon SNS トピックへのサブスクライブ」を参照してください。

> **Note**
>
> 通知を受け取るには、委任管理アカウントと同じ AWS リージョン と AWS アカウント にある Amazon SNS トピックの Amazon リソースネーム (ARN) を指定する必要があります。

タスク 2: Amazon SNS アクセスポリシーを更新する

以下の手順を使用して Amazon SNS アクセスポリシーを更新し、Systems Manager がタスク 1 で作成した Amazon SNS トピックに Change Manager 通知を発行できるようにします。このタスクを完了しなければ、トピックを追加するイベントの通知を送信するアクセス許可が Change Manager に付与されません。

1. AWS Management Console にサインインして Amazon SNS コンソール (https://console.aws.amazon.com/sns/v3/home) を開きます。
2. ナビゲーションペインで、[トピック] を選択します。
3. タスク 1 で作成したトピックを選択してから、[Edit] (編集) をクリックします。
4. [アクセスポリシー] を展開します。
5. 以下の `Sid` ブロックを既存のポリシーに追加して更新し、それぞれの`##############`をあなた自身の情報で置き換えます

```
{
    "Sid": "Allow Change Manager to publish to this topic",
    "Effect": "Allow",
    "Principal": {
        "Service": "ssm.amazonaws.com"
    },
    "Action": "sns:Publish",
    "Resource": "arn:aws:sns:region:account-id:topic-name",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": [
                "account-id"
            ]
        }
    }
}
```

既存の Sid ブロックの後にこのブロックを入力し、作成したトピックの該当する値で *region*、*account-id*、および *topic-name* を置き換えます。

6. [Save changes] を選択します。

これで、トピックに追加するイベントタイプが発生すると、システムが Amazon SNS トピックに通知を送信するようになりました。

> **Important**
>
> AWS Key Management Service (AWS KMS) のサーバー側の暗号化キーを使用して Amazon SNS トピックを設定した場合は、タスク 3 を完了する必要があります。

タスク 3: (オプション) AWS Key Management Service アクセスポリシーを更新する

Amazon SNS トピックに対して AWS Key Management Service (AWS KMS) サーバー側の暗号化を有効にした場合、トピックを設定したときに選択した AWS KMS key のアクセスポリシーも更新する必要があります。以下の手順を実行してアクセスポリシーを更新し、Systems Manager がタスク 1 で作成した Amazon SNS トピックに Change Manager の承認通知を発行できるようにします。

1. AWS KMS コンソール (https://console.aws.amazon.com/kms) を開きます。
2. ナビゲーションペインで、[Customer managed keys (カスタマー管理型のキー)] を選択します。
3. トピックの作成時に選択したカスタマーマネージドキーの ID を選択します。
4. [Key Policy] (キーポリシー) セクションで、[Switch to policy view] (ポリシービューへの切り替え) を選択します。
5. [Edit] を選択します。
6. 既存のポリシーの既存の Sid ブロックのいずれかの後に、次の Sid ブロックを入力します。各###############を独自の情報に置き換えます。

```
{
    "Sid": "Allow Change Manager to decrypt the key",
    "Effect": "Allow",
    "Principal": {
        "Service": "ssm.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
```

```
            "kms:GenerateDataKey*"
        ],
        "Resource": "arn:aws:kms:region:account-id:key/key-id",
        "Condition": {
            "StringEquals": {
                "aws:SourceAccount": [
                    "account-id"
                ]
            }
        }
}
```

7. 次に、リソースポリシーの既存の Sid ブロックのいずれかの後に次の Sid ブロックを入力して、サービス間の混乱した使節の問題を防止します。

   このブロックは、aws:SourceArn および aws:SourceAccount グローバル条件コンテキストキーを使用して、Systems Manager がリソースに別のサービスを提供する許可を制限します。

   各###############を独自の情報に置き換えます。

```
{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Sid": "Configure confused deputy protection for AWS KMS keys used in Amazon
 SNS topic when called from Systems Manager",
      "Effect": "Allow",
      "Principal": {
        "Service": "ssm.amazonaws.com"
      },
      "Action": [
        "sns:Publish"
      ],
      "Resource": "arn:aws:sns:region:account-id:topic-name",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:ssm:region:account-id:*"
        },
        "StringEquals": {
          "aws:SourceAccount": "account-id"
        }
      }
    }
```

```
    ]
}
```

8. [Save changes] (変更の保存) をクリックします。

Change Manager のロールとアクセス許可の設定

デフォルトでは、Change Manager にはリソースでアクションを実行するアクセス許可がありません。AWS Identity and Access Management (IAM) サービスロールまたはロールの継承を使用してアクセスを許可する必要があります。このロールでは、ユーザーに代わって Change Manager が承認済み変更リクエストで指定された Runbook ワークフローを安全に実行できます。このロールは、Change Manager に対して AWS Security Token Service (AWS STS) AssumeRole 信頼を付与します。

これらのアクセス許可を組織内の複数のユーザーの代理として行動するために 1 つのロールに提供すれば、該当するユーザーは、そのアクセス許可の配列を自分で取得する必要がなくなります アクセス許可で許可されるアクションは、承認済みの操作のみに制限されます。

アカウントまたは組織のユーザーは、変更リクエストを作成するときに、このロールの継承を選択して変更オペレーションを実行できます。

Change Manager の新しいロールの継承を作成するか、必要なアクセス許可で既存のロールを更新できます。

Change Manager のサービスロールを作成する必要がある場合、次のタスクを完了します。

タスク

- タスク 1: Change Manager のロールの継承ポリシーを作成する
- タスク 2: Change Manager のロールの継承を作成する
- タスク 3: iam:PassRole ポリシーを他のロールにアタッチする
- タスク 4: 他の AWS のサービスを呼び出すためにロールの継承をインラインポリシーに追加する
- タスク 5: Change Manager へのユーザーアクセスを設定する

タスク 1: Change Manager のロールの継承ポリシーを作成する

以下の手順を使用して、Change Manager ロールの継承にアタッチするポリシーを作成します。

Change Manager のロールの継承ポリシーを作成するには

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. ナビゲーションペインで、Policies を選択し、Create Policy を選択します。
3. [ポリシーの作成] ページで [JSON] タブをクリックし、デフォルトのコンテンツを次のように置き換えます。これは次のステップで実際の Change Manager オペレーションで変更します。

> **Note**
>
> 複数のアカウントとAWS リージョンを持つ組織ではなく、1 つの AWS アカウントで使用するポリシーを作成する場合、最初のステートメントブロックを省略できます。Change Manager を使用する単一のアカウントの場合、`iam:PassRole` アクセス許可は必要ありません。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::delegated-admin-account-id:role/AWS-
SystemsManager-job-functionAdministrationRole",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "ssm.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeDocument",
                "ssm:GetDocument",
                "ssm:StartChangeRequestExecution"
            ],
            "Resource": [
                "arn:aws:ssm:region:account-id:automation-definition/template-name:
$DEFAULT",
                "arn:aws:ssm:region::document/template-name"
            ]
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:ListOpsItemEvents",
                "ssm:GetOpsItem",
                "ssm:ListDocuments",
                "ssm:DescribeOpsItems"
            ],
            "Resource": "*"
        }
    ]
}
```

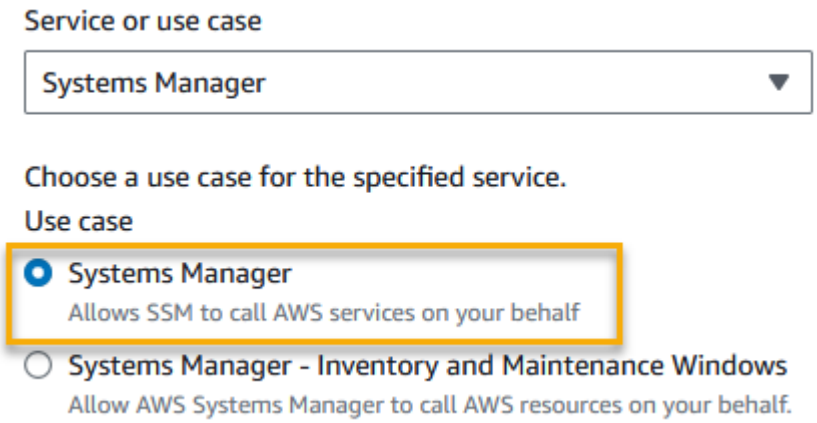
4. iam:PassRole アクションに対して、Resource 値を更新して Runbook ワークフローを開始するアクセス許可を付与する組織に対して定義されているすべてのジョブ関数の ARN を含めます。
5. *region*、*account-id*、*template-name*、*delegated-admin-account-id*、および *job-function* プレスホルダーを実際の Change Manager オペレーションの値で置き換えてください。
6. 2 番目の Resource ステートメントでリストを更新して、アクセス許可を付与するすべての変更テンプレートを含めます。"Resource": "*" を指定して組織のすべての変更テンプレートにアクセス許可を付与することもできます。
7. [Next: Tags] (次へ: タグ) を選択します。
8. (オプション) 1 つ以上のタグキーと値のペアを追加して、このポリシーのアクセスを整理、追跡、または制御します。
9. [次へ: レビュー] を選択します。
10. [Review policy] (ポリシーの確認) ページの [Name] (名前) ボックスに **MyChangeManagerAssumeRole** などの名前を入力し、説明を入力します。
11. [ポリシーの作成] を選択し、「タスク 2: Change Manager のロールの継承を作成する」に進みます。

タスク 2: Change Manager のロールの継承を作成する

以下の手順を使用して、Change Manager の Change Manager のロールの継承 (サービスロールの一種) を作成します

Change Manager のロールの継承ポリシーを作成するには

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. ナビゲーションペインで ロール を選択してから、ロールを作成する を選択します。
3. [Select trusted entity] (信頼できるエンティティを選択) で、次のように選択します。
   1. [Trusted entity type] (信頼できるエンティティタイプ) で、[AWS service] (のサービス) を選択します。
   2. [その他の AWS のサービス のユースケース] で、[Systems Manager] を選択します
   3. 以下のイメージに示されている、[Systems Manager] を選択します。



4. [Next] を選択します。
5. [アタッチされたアクセス許可ポリシー] ページで、タスク 1: Change Manager のロールの継承ポリシーを作成する で作成したロールの継承 (**MyChangeManagerAssumeRole** など) を検索します。
6. ロールの継承ポリシー名の横にあるチェックボックスを選択し、[次へ: タグ] を選択します。
7. [Role name] (ロール名) に、新しいインスタンスプロファイルの名前 (**MyChangeManagerAssumeRole** など) を入力します。
8. (オプション) [Description] (説明) で、このインスタンスロールの説明を更新します。
9. (オプション) 1 つ以上のタグキーと値のペアを追加して、このロールのアクセスを整理、追跡、または制御します。
10. [次へ: レビュー] を選択します。
11. (オプション) [Tags] (タグ) で、1 つ以上のタグキーと値のペアを追加し、このロールのアクセスを整理、追跡、制御して、[Create role] (ロールの作成) を選択します。ロールページが再度表示されます。
12. [ロールの作成] を選択します。ロールページが再度表示されます。

13. ロール ページで作成したロールを選択して、概要 ページを開きます。

タスク 3: **iam:PassRole** ポリシーを他のロールにアタッチする

`iam:PassRole` ポリシーを IAM インスタンスプロファイルまたは IAM サービスロールにアタッチするには、次の手順を使用します。(Systems Manager サービスは IAM インスタンスプロファイルを使用して EC2 インスタンスと通信します。ハイブリッドおよびマルチクラウド環境の非 EC2 マネージドノードでは、代わりに IAM サービスロールが使用されます。)

`iam:PassRole` ポリシーをアタッチすることにより、Change Manager サービスは、ランブックワークフローを実行するときに他のサービスまたは Systems Manager ツールにロールの継承アクセス許可を渡すことができます。

iam:PassRole ポリシーを IAM インスタンスプロファイルまたはサービスロールにアタッチするには

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. ナビゲーションペインで [Roles] (ロール) を選択します。
3. 前のステップで作成した Change Manager のロールの継承 (**MyChangeManagerAssumeRole** など) を検索し、その名前を選択します。
4. ロールの継承の [Summary] (サマリー) ページで [Permissions] (アクセス許可) タブを選択します。
5. [Add permissions, Create inline policy] (アクセス許可の追加、インラインポリシーの作成) を選択します。
6. [ポリシーの作成] ページの [Visual editor] (ビジュアルエディタ) タブを選択します。
7. [サービス]、[IAM] の順に選択します。
8. [Filter actions (フィルタアクション)] テキストボックスに「**PassRole**」と入力し、[PassRole] オプションを選択します。
9. [リソース] を展開します。[Specific] (固有) が選択されていることを確認し、[Add ARN] (ARN の追加) を選択します。
10. [ロールの ARN を指定する] フィールドに、ロールの継承アクセス許可を渡す IAM インスタンスプロファイルロールまたは IAM サービスロールの ARN を入力します。システムによって、[アカウント] と [Role name with path (ロール名とパス)] フィールドが入力されます。
11. [Add] (追加) をクリックします。
12. [ポリシーの確認] を選択します。

13. [Name] (名前) に、このポリシーを識別する名前を入力し、[Create policy] (ポリシーの作成) を選択します。

詳細情報

- Systems Manager に必要なインスタンスのアクセス許可を設定する
- ハイブリッドおよびマルチクラウド環境で Systems Manager に必要な IAM サービスロールを作成する

タスク 4: 他の AWS のサービスを呼び出すためにロールの継承をインラインポリシーに追加する

Change Manager のロールの継承を使用して変更リクエストが他の AWS のサービスを呼び出すとき、ロールの継承は、該当するサービスを呼び出すアクセス許可で設定されている必要があります。この要件は、変更リクエストで使用される `AWS-ConfigureS3BucketLogging`、`AWS-CreateDynamoDBBackup`、`AWS-RestartEC2Instance` ランブックなど、すべての AWS オートメーションランブック (AWS-* runbooks) に適用されます。この要件は、他のサービスを呼び出すアクションを使用して他の AWS のサービスを呼び出すように作成したカスタムランブックにも適用されます。たとえば、`aws:executeAwsApi`、`aws:CreateStack`、または `aws:copyImage` などのアクションを使用する場合は、それらのサービスを呼び出すためのアクセス許可を持つサービスロールを設定する必要があります。ロールに IAM インラインポリシーを追加することで、他の AWS のサービスへのアクセス許可を有効にできます。

インラインポリシーをロールの継承に追加して、他の AWS のサービス (IAM コンソール) を呼び出すには

1. AWS Management Console にサインインして、IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. ナビゲーションペインで Roles (ロール) を選択します。
3. リストで、更新するロールの継承の名前 (`MyChangeManagerAssumeRole` など) を選択します。
4. [アクセス許可] タブを選択します。
5. [Add permissions, Create inline policy] (アクセス許可の追加、インラインポリシーの作成) を選択します。
6. [JSON] タブを選択します。
7. 呼び出す AWS のサービスの JSON ポリシードキュメントを入力します。JSON ポリシードキュメントの 2 つの例を以下に示します。

Amazon S3 **PutObject** および **GetObject** の例

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
        }
    ]
}
```

Amazon EC2 **CreateSnapshot** および **DescribeSnapShots** の例

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshot",
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action":"ec2:DescribeSnapshots",
         "Resource":"*"
      }
   ]
}
```

IAM ポリシー言語の詳細については、IAM ユーザーガイドの「IAM JSON ポリシーリファレンス」を参照してください。

8. 完了したら、[ポリシーの確認] を選択します。構文エラーがある場合は、Policy Validator (ポリシー検証) によってレポートされます。

9. [Name] (名前) に、作成するポリシーを識別する名前を入力します。ポリシーの [Summary] (概要) を参照して、ポリシーによって付与された許可を確認します。次に [ポリシーの作成] を選択して作業を保存します。
10. インラインポリシーを作成した後は、自動的にロールに埋め込まれます。

タスク 5: Change Manager へのユーザーアクセスを設定する

ユーザー、グループ、ロールに管理者権限が割り当てられている場合は、Change Manager にアクセスできます。管理者権限がない場合は、管理者が `AmazonSSMFullAccess` マネージドポリシー (または同等のアクセス許可を付与するポリシー) を ユーザー、グループ、ロールに割り当てる必要があります。

Change Manager を使用するようにユーザーを設定するには、次の手順を使用します。選択したユーザーには、Change Manager を設定して実行するアクセス許可が付与されます。

組織で使用している アイデンティティアプリケーションに応じて、ユーザーアクセスを設定するために使用できる 3 つのオプションのいずれかを選択できます。ユーザーアクセスを設定するときに、以下を割り当て、または追加します。

1. Systems Manager へのアクセスを許可する `AmazonSSMFullAccess` ポリシーまたは同等のポリシーを割り当てます。
2. `iam:PassRole` ポリシーを割り当てます。
3. タスク 2: Change Manager のロールの継承を作成する の最後にコピーしたロールを継承する Change Manager の ARN を追加します。

アクセス権限を付与するにはユーザー、グループ、またはロールにアクセス許可を追加します。

- AWS IAM Identity Center のユーザーとグループ:

  アクセス許可セットを作成します。「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」の手順に従ってください。
- IAM 内で、ID プロバイダーによって管理されているユーザー:

  ID フェデレーションのロールを作成します。詳細については「IAM ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) 用のロールを作成する」を参照してください。
- IAM ユーザー:

- ユーザーが担当できるロールを作成します。手順については「IAM ユーザーガイド」の「IAM ユーザーのロールの作成」を参照してください。
- (お奨めできない方法) ポリシーをユーザーに直接アタッチするか、ユーザーをユーザーグループに追加します。詳細については「IAM ユーザーガイド」の「ユーザー (コンソール) へのアクセス権限の追加」を参照してください。

これで Change Manager に必要なロールの設定が完了しました。これで Change Manager オペレーションで Change Manager のロールの継承 ARN を使用できるようになりました。

自動承認のランブックワークフローへのアクセスを制御する

組織またはアカウント用に作成された各変更テンプレートでは、そのテンプレートから作成された変更リクエストを自動承認済変更リクエストとして実行できるかどうかを指定できます。つまり、レビューステップなしで自動的に実行できます (変更凍結イベントを除く)。

ただし、特定のユーザー、グループ、または AWS Identity and Access Management (IAM) ロールは、変更テンプレートで許可されている場合でも、自動承認の変更リクエストを実行しないようにした方がいいかもしれません。これを行うには、ユーザー、グループ、または IAM ロールに割り当てられる IAM ポリシーで、`StartChangeRequestExecution` オペレーションの `ssm:AutoApprove` 条件キーを使用します。

次のポリシーをインラインポリシーとして追加できます。このポリシーでは、条件を `false` に指定し、ユーザーが自動承認可能な変更リクエストを実行できないようにします。

```
{
    "Version": "2012-10-17",
    "Statement": [
            {
            "Effect": "Allow",
            "Action": "ssm:StartChangeRequestExecution",
            "Resource": "*",
            "Condition": {
                "BoolIfExists": {
                    "ssm:AutoApprove": "false"
                }
            }
        }
    ]
}
```

インラインポリシーの指定の詳細については、IAM ユーザーガイドで「インラインポリシー」と「IAM ID のアクセス許可の追加および削除」を参照してください。

Systems Manager ポリシーの条件キーの詳細については、「Condition keys for Systems Manager」(Systems Manager の条件キー) を参照してください。

「Change Manager」 の使用

AWS Systems Manager のツールである Change Manager では、組織全体のユーザー、またはシングル AWS アカウント内のユーザーが、必要な許可が付与されている変更関連タスクを実行できます。Change Manager タスクには、以下が含まれます。

- 変更テンプレートを作成、確認、承認または拒否します。

  変更テンプレートは、必要な承認、利用可能なランブック、変更リクエストの通知オプションなどの項目を定義する、Change Manager の設定のコレクションです。
- 変更リクエストを作成、確認、承認または拒否します。

  変更リクエストは、AWS またはオンプレミス環境の 1 つ以上のリソースを更新する Automation ランブックを実行するための Change Manager のリクエストです。変更リクエストは、変更テンプレートを使用して作成されます。
- 組織またはアカウントのどのユーザーを変更テンプレートおよび変更リクエストに対するレビューワーにできるかを指定します。
- Change Managerでのユーザー ID の管理方法、およびChange Manager操作で実施される利用可能なベストプラクティスオプションなどの構成設定を編集する。これらの設定の実行に関する詳細については、「Change Managerオプションとベストプラクティスの設定」を参照してください。

トピック

- 変更テンプレートの使用
- 変更リクエストの使用
- 変更リクエストの詳細、タスク、およびタイムラインの確認 (コンソール)
- 変更リクエストの集計数の表示 (コマンドライン)

変更テンプレートの使用

変更テンプレートは、必要な承認、利用可能なランブック、変更リクエストの通知オプションなどの項目を定義する、Change Manager の設定のコレクションです。

> **Note**
>
> AWS には、AWS Systems Manager のツールである Change Manager を試すために使用できるサンプルの Hello World 変更テンプレートが用意されています。組織またはアカウント内のリソースに許可する変更を定義するには、独自の変更テンプレートを作成してください。

ランブックワークフローの実行時に行われる変更は、オートメーションランブックの内容に基づきます。作成する変更テンプレートには、変更リクエストを作成するユーザーが、更新時の実行用に選択できる 1 つ、または複数のオートメーションランブックを含めることができます。また、変更テンプレートを作成して、リクエスタが変更リクエストに対して利用できるオートメーションランブックを選択できるようにすることもできます。

変更テンプレートは、[Create template] (テンプレートの作成) コンソールページの [Builder] (ビルダー) オプションを使用して簡単に作成することができます。または、[Editor] (エディタ) オプションを使用して、ランブックワークフローに望ましい設定を使った JSON または YAML コンテンツを手動で作成することも可能です。コマンドラインツールを使用して、変更テンプレートの JSON コンテンツを外部ファイルに保存して、変更テンプレートを作成することもできます。

トピック

- AWS 管理の Hello World 変更テンプレートを試す
- 変更テンプレートの作成
- 変更テンプレートの確認と、承認または拒否
- 変更テンプレートの削除

AWS 管理の **Hello World** 変更テンプレートを試す

AWS Systems Manager のツールである Change Manager の設定が完了したら、サンプルの変更テンプレート `AWS-HelloWorldChangeTemplate` を使用してレビューと承認のプロセスをテストすることができます。このテンプレートでは、サンプル Automation ランブック `AWS-HelloWorld` を使用します。このテンプレートは、設定された許可、承認者の割り当て、および承認プロセスをテスト、または検証するために設計されています。AWS から、組織またはアカウントでこの変更テンプレートを使用するための承認が既に提供されています。この変更テンプレートに基づく変更リクエストは、いずれも組織またはアカウントのレビューワーによる承認を受ける必要があります。

このテンプレートに関連付けられたランブックワークフローの結果は、リソースに変更を行うのではなく、オートメーションステップの出力にメッセージを書き出します。

開始する前に

作業を開始する前に、次のタスクが完了していることを確認してください。

- 組織全体の変更の管理に AWS Organizations を使用して場合は、「組織の Change Manager の設定 (管理アカウント)」で説明されている組織のセットアップタスクを完了します。
- 「Change Managerオプションとベストプラクティスの設定」の説明に従って、委任管理者アカウントまたは単一のアカウントにChange Managerを設定します。

> **Note**
>
> Change Manager 設定で [Require monitors for all templates (すべてのテンプレートに監視プログラムを義務付ける)] のベストプラクティスのオプションを有効にした場合は、Hello World 変更テンプレートをテストしている間、それを一時的に無効にしてください。

AWS 管理の Hello World 変更テンプレートを試すには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Change Manager] を選択します。
3. [Create request] (リクエストを作成) をクリックします。
4. 「`AWS-HelloWorldChangeTemplate`」という名前の変更テンプレートを選択し、[Next] (次へ) を選択します。
5. [Name] (名前) には、**`MyChangeRequestTest`** など、その目的を識別しやすくする変更リクエストの名前を入力します。
6. 変更リクエストを作成する残りの手順については、「変更リクエストの作成」を参照してください。

次のステップ

変更リクエストの承認については、「変更リクエストの確認と、承認または拒否」を参照してください。

変更リクエストのステータスと結果を表示するには、Change Manager の [Requests (リクエスト)] タブで変更リクエストの名前を選択します。

変更テンプレートの作成

変更テンプレートは、必要な承認、利用可能なランブック、変更リクエストの通知オプションなどの項目を定義する、Change Manager の設定のコレクションです。

AWS Systems Manager のツールである Change Manager で、ビルダーオプションとエディタオプション、コマンドラインツールが含まれているコンソールを使用して、オペレーションの変更テンプレートを作成できます。

トピック

- 変更テンプレートの承認について
- ビルダーを使用した変更テンプレートの作成
- エディタを使用した変更テンプレートの作成
- コマンドラインツールを使用した変更テンプレートの作成

変更テンプレートの承認について

作成する各変更テンプレートでは、そのテンプレートから作成された変更リクエストの承認レベルを最大 5 つ指定できます。これらのレベルごとに、最大 5 人の潜在的な承認者を指定できます。承認者は 1 人のユーザーに限定されません。IAM グループまたは IAM ロールを個別の承認者として指定することもできます。IAM グループと IAM ロールでは、そのグループまたはロールに属する 1 人以上のユーザーが、変更リクエストに必要な承認の総数の受け取りに対して、承認を提供することができます。変更テンプレートに必要な数よりも多くの承認者を指定することもできます。

Change Manager では、レベルごとの承認とラインごとの承認という、2 つの主要な承認アプローチをサポートしています。状況によっては、この 2 つのタイプを組み合わせることもできます。Change Manager オペレーションでは、レベルごとの承認のみを使用することをお勧めします。

Per-level approvals

> 推奨 2023 年 1 月 23 日現在、Change Manager はレベルごとの承認をサポートしています。このモデルでは、変更テンプレートの各承認レベルにおいて、最初にそのレベルに必要な承認数を指定します。次に、そのレベルに必要な数以上の承認者を指定し、さらに多くの承認者を指定できます。ただし、変更リクエストの承認に必要なのは、指定したレベルごとの承認者数だけです。例えば、5 人の承認者を指定できますが、必要なのは 3 人です。

この承認タイプのコンソールビューと JSON サンプルについては、「the section called “レベルごとの承認設定の例”」を参照してください。

Per-line approvals

下位互換性のサポート Change Manager のオリジナルリリースでは、行ごとの承認のみがサポートされていました。このモデルでは、承認レベルに指定されたすべての承認者が、承認ラインとして表示されます。変更リクエストをそのレベルで承認するには、各承認者が承認する必要がありました。2023 年 1 月 23 日より前は、これが承認をサポートする唯一のモデルでした。この日付より前に作成された変更テンプレートは、引き続き行単位の承認をサポートしますが、代わりにレベルごとの承認を使用することをお勧めします。

この承認タイプのコンソールビューと JSON サンプルについては、「the section called “行ごとの承認設定の例”」を参照してください。

Combined per-line and per-level approvals

非推奨 コンソールの [ビルダー] タブでは、行ごとの承認の追加がサポートされなくなりました。ただし、場合によっては、変更テンプレートで行ごとの承認とレベルごとの承認の両方が行われることがあります。これは、2023 年 1 月 23 日より前に作成された変更テンプレートを更新した場合や、YAML コンテンツを手動で編集して変更テンプレートを作成または更新した場合に発生する可能性があります。

この承認タイプのコンソールビューと JSON サンプルについては、「the section called “レベルごとと行ごとの承認設定を組み合わせた例”」を参照してください。

> **Important**
>
> ラインごとの承認とレベルごとの承認を組み合わせた変更テンプレートを作成することは可能ですが、この設定は推奨されておらず、必要もありません。より多くの承認が必要な承認タイプ (ラインごとまたはレベルごとの承認) が優先されます。例:
>
> - 変更テンプレートでレベルごとに 3 つの承認が指定されているが、1 行につき 5 つの承認が指定されている場合は、5 つの承認が必要です。
> - 変更テンプレートでレベルごとに 4 つの承認が指定されているが、1 行につき 2 つの承認が指定されている場合は、4 つの承認が必要です。

YAML または JSON コンテンツを手動で編集することで、行ごとおよびレベルごとの両方の承認を含むレベルを作成できます。作成すると、[ビルダー] タブに、レベルと個々のラインの両方に必要な

承認数を指定するためのコントロールが表示されます。ただし、コンソールを使用して追加した新しいレベルでは、引き続きレベルごとの承認設定のみがサポートされます。

変更リクエストの通知と拒否

Amazon SNSの通知

変更テンプレートを使用して変更リクエストが作成されると、そのレベルの承認通知対象として指定されている Amazon Simple Notification Service (Amazon SNS) トピックのサブスクライバーに通知が送信されます。変更テンプレートで通知トピックを指定することも、変更リクエストを作成するユーザーに通知トピックを指定させることもできます。

あるレベルで必要最小限の承認が受理されると、次のレベルの Amazon SNS トピックのサブスクライバーに通知が送信され、以降も同様に通知が送信されます。

> **Important**
>
> 指定した IAM ロール、グループ、ユーザーに、指定した必要な承認数を満たすのに十分な承認者を指定してください。例えば、3 人のユーザーを含む 1 つの IAM グループのみを 1 人の承認者として指定した場合、そのレベルで必須と指定できるのは 5 つの承認ではなく、3 つ以下となります。

変更リクエストの却下

承認レベルと承認者をいくつ指定していても、そのリクエストのランブックワークフローの発生を防ぐには、変更リクエストを 1 回却下するだけで済みます。

Change Manager 承認タイプの例

次のサンプルは、Change Manager の 3 種類の承認タイプのコンソールビューと JSON コンテンツを示しています。

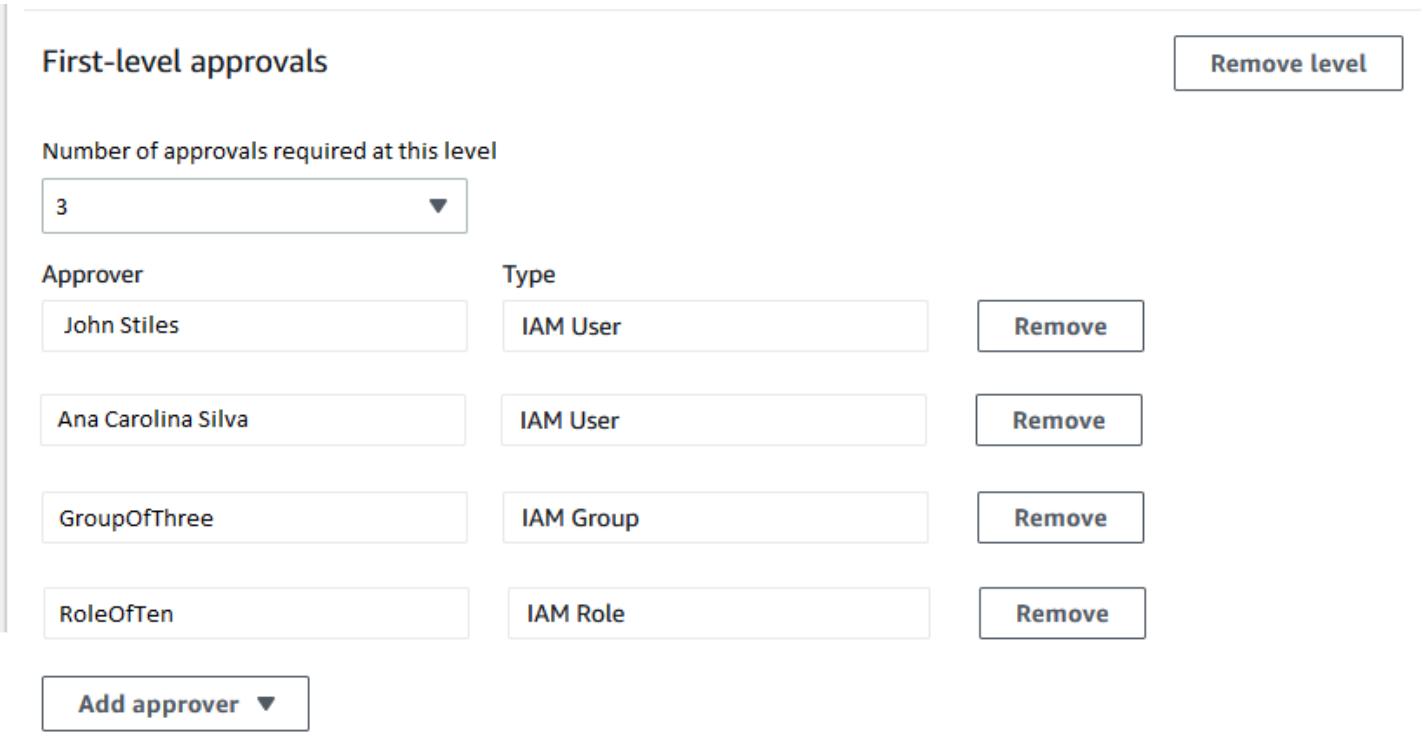
トピック

- レベルごとの承認設定の例
- 行ごとの承認設定の例
- レベルごとと行ごとの承認設定を組み合わせた例

レベルごとの承認設定の例

次のイメージに示されたレベルごとの承認レベル設定では、3 つの承認が必要です。これらの承認は、承認者として指定された IAM ユーザー、グループ、ロールを自由に組み合わせて行うことができます。指定された承認者には、2 人の IAM ユーザー (John Stiles と Ana Carolina Silva)、3 人のメンバーを含むユーザーグループ (`GroupOfThree`)、10 人のユーザーを代表するユーザーロール (`RoleOfTen`) が含まれます。

`GroupOfThree` グループ内の 3 人のユーザー全員が変更リクエストを承認すると、そのレベルで変更リクエストが承認されます。各ユーザー、グループ、ロールの承認を受け取る必要はありません。承認の最小数は、指定した承認者を任意に組み合わせて得ることができます。Change Manager オペレーションでは、レベルごとの承認を使用することをお勧めします。



次のサンプルは、この構成の YAML コードの一部を示しています。

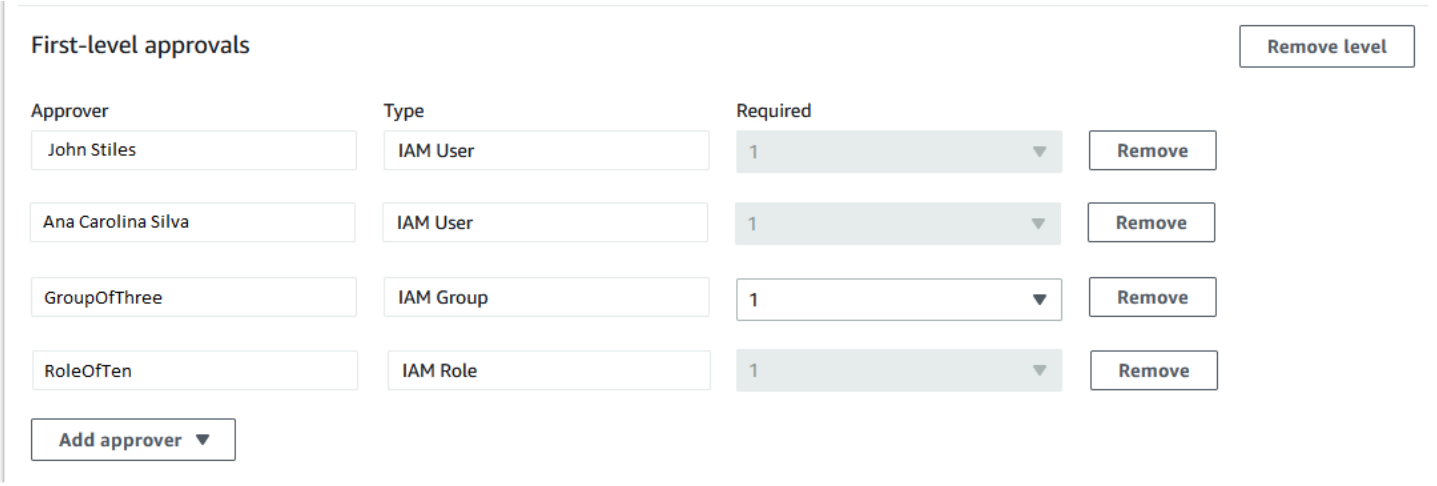
> **Note**
>
> このバージョンの YAML コードには、追加の入力である `MinRequiredApprovals` (先頭が大文字の `M`) が含まれています。この入力の値は、利用可能なすべてのレビューワーから必要とされる承認数を示します。`Approvers` リスト内の各承認者の `minRequiredApprovals`

(先頭が小文字の m) 値が 0 (ゼロ) であることにも注意してください。これは、承認者が承認全体に貢献できるが、必要ではないことを示しています。

```
schemaVersion: "0.3"
emergencyChange: false
autoApprovable: false
mainSteps:
  - name: ApproveAction1
    action: aws:approve
    timeoutSeconds: 604800
    inputs:
      Message: Please approve this change request
      MinRequiredApprovals: 3
      EnhancedApprovals:
        Approvers:
          - approver: John Stiles
            type: IamUser
            minRequiredApprovals: 0
          - approver: Ana Carolina Silva
            type: IamUser
            minRequiredApprovals: 0
          - approver: GroupOfThree
            type: IamGroup
            minRequiredApprovals: 0
          - approver: RoleOfTen
            type: IamRole
            minRequiredApprovals: 0
templateInformation: >
  #### What is the purpose of this change?
    //truncated
```

行ごとの承認設定の例

次のイメージに示された承認レベルの設定では、4 人の承認者が指定されています。指定された承認者には、2 人の IAM ユーザー (John Stiles と Ana Carolina Silva)、3 人のメンバーを含むユーザーグループ (GroupOfThree)、10 人のユーザーを代表するユーザーロール (RoleOfTen) が含まれます。下位互換性のために行ごとの承認がサポートされていますが、推奨されていません。



この行ごとの承認設定で変更リクエストが承認されるには、John Stiles、Ana Carolina Silva、GroupOfThree グループの 1 人のメンバー、RoleOfTen ロールの 1 人のメンバー全員による承認が必要です。

次のサンプルは、この構成の YAML コードの一部を示しています。

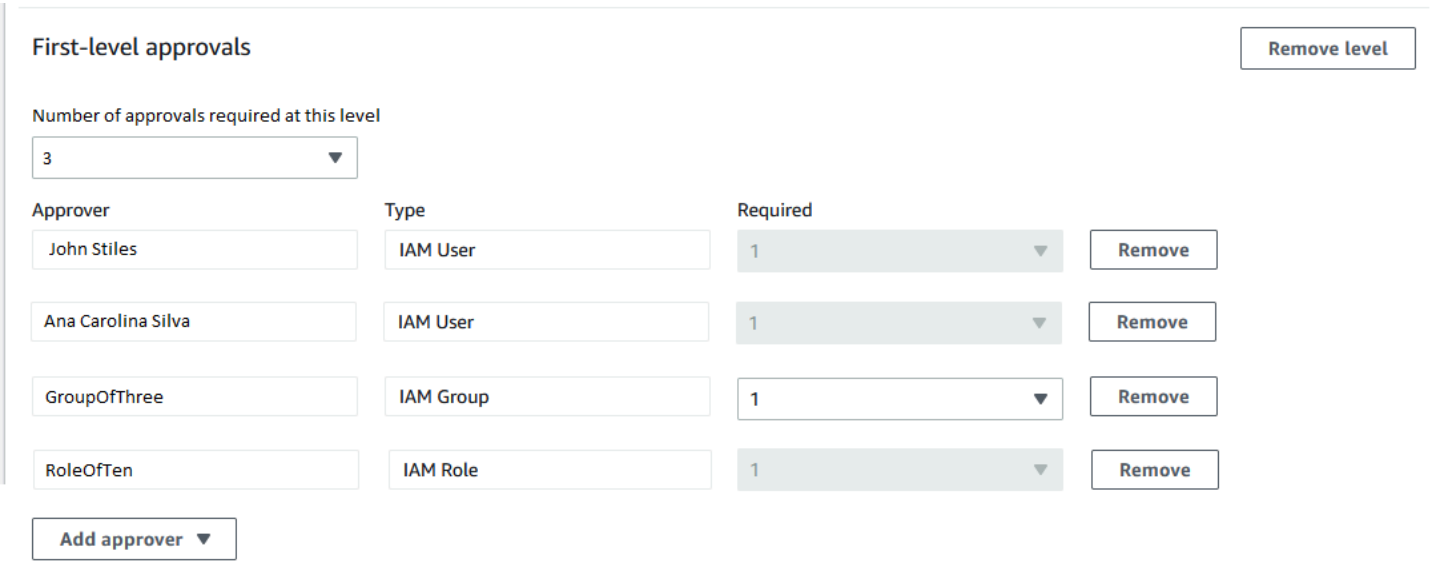
> **Note**
>
> 各 minRequiredApprovals 承認者の値が 1 であることに注意してください。これは、各承認者から 1 つの承認が必要であることを示しています。

```
schemaVersion: "0.3"
emergencyChange: false
autoApprovable: false
mainSteps:
  - name: ApproveAction1
    action: aws:approve
    timeoutSeconds: 10000
    inputs:
      Message: Please approve this change request
      EnhancedApprovals:
        Approvers:
          - approver: John Stiles
            type: IamUser
            minRequiredApprovals: 1
          - approver: Ana Carolina Silva
            type: IamUser
            minRequiredApprovals: 1
```

```
          - approver: GroupOfThree
            type: IamGroup
            minRequiredApprovals: 1
          - approver: RoleOfTen
            type: IamRole
            minRequiredApprovals: 1
executableRunBooks:
  - name: AWS-HelloWorld
    version: $DEFAULT
templateInformation: >
  #### What is the purpose of this change?
    //truncated
```

レベルごとと行ごとの承認設定を組み合わせた例

次のイメージに示されているように、レベルごとと行ごとの承認を組み合わせた設定では、レベルに 3 つの承認が指定され、明細項目の承認に 4 つの承認が指定されています。より多くの承認が必要な承認タイプが他の承認タイプよりも優先されるため、この設定では 4 つの承認が必要です。レベルごとの承認と行ごとの承認の組み合わせは推奨されていません。




```
schemaVersion: "0.3"
emergencyChange: false
autoApprovable: false
mainSteps:
  - name: ApproveAction1
    action: aws:approve
    timeoutSeconds: 604800
```

```
    inputs:
      Message: Please approve this change request
      MinRequiredApprovals: 3
      EnhancedApprovals:
        Approvers:
          - approver: John Stiles
            type: IamUser
            minRequiredApprovals: 1
          - approver: Ana Carolina Silva
            type: IamUser
            minRequiredApprovals: 1
          - approver: GroupOfThree
            type: IamGroup
            minRequiredApprovals: 1
          - approver: RoleOfTen
            type: IamRole
            minRequiredApprovals: 1
templateInformation: >
  #### What is the purpose of this change?
    //truncated
```

トピック

- ビルダーを使用した変更テンプレートの作成
- エディタを使用した変更テンプレートの作成
- コマンドラインツールを使用した変更テンプレートの作成

ビルダーを使用した変更テンプレートの作成

AWS Systems Manager のツールである Change Manager の変更テンプレートにビルダーを使用して、JSON または YAML 構文を使用しなくても、変更テンプレートで定義されたランブックワークフローを設定できます。オプションを指定すると、入力が、Systems Manager がランブックワークフローを実行するために使用できる YAML 形式に変換されます。

ビルダーを使用して変更テンプレートを作成するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Change Manager] を選択します。
3. [Create template] (テンプレートの作成) をクリックします。

4. [Name] (名前) には、**UpdateEC2LinuxAMI** など、その目的を識別しやすくするテンプレート名を入力します。
5. [Change template details] (変更テンプレートの詳細) セクションで、以下を実行します。

   - [Description] (説明) には、作成している変更テンプレートが、いつ、どのように使用されるのかに関する簡単な説明を入力します。

     この説明は、変更リクエストを作成するユーザーが、正しい変更テンプレートを使用しているかどうかを判断するのに役立ちます。変更リクエストのレビューワーが、リクエストを承認すべきかどうかを理解するためにも役立ちます。
   - [Change template type] (変更テンプレートタイプ) で、標準変更テンプレートと緊急変更テンプレートのどちらを作成するかを指定します。

     緊急変更テンプレートは、AWS Systems Manager Change Calendar で使用されているカレンダー内のイベントによって変更がブロックされている場合でも、変更を行う必要がある場合に使用されます。緊急変更テンプレートから作成された変更リクエストは、指定された承認者によって承認される必要がありますが、要求された変更は、カレンダーがブロックされている場合でも実行できます。
   - [Runbook options] (ランブックオプション) では、変更リクエストの作成時にユーザーが選択できるランブックを指定します。ランブックは、1 つ、または複数追加することができます。その代わりに、リクエスタが使用するランブックを指定できるようにすることも可能です。いずれの場合も、変更リクエストに含めることができるランブックは 1 つだけです。
   - [Runbook] (ランブック) には、ユーザーがその変更リクエスト用に選択できるランブックの名前と、それらのバージョンを選択します。変更テンプレートに追加するランブックの数に関係なく、変更リクエストごとに選択できるランブックは 1 つだけです。

     上記の [Any runbook can be used] (任意のランブックを使用できる) を先に選択した場合は、ランブックを指定しません。

     > **Tip**
     > ランブックとそのバージョンを選択したら、[View] (表示) をクリックし、Systems Manager ドキュメントインターフェイスでランブックの内容を調べます。
6. [Template information] (テンプレート情報) セクションで、Markdown を使用して、この変更テンプレートから変更リクエストを作成するユーザーの情報を入力します。当社では、変更リクエ

ストを作成するユーザーに対して含めることができる質問セットを用意していますが、代わりに他の情報や質問を追加することもできます。

> **Note**
>
> Markdown は、ドキュメント、およびドキュメント内の個々のステップに wiki 形式の説明を追加できるようにするマークアップ言語です。Markdown の使用に関する詳細については、「AWS での Markdown の使用」を参照してください。

これには、変更、およびロールバック計画の一環として実行する必要がある手動ステップをリストアップするなど、承認者が各変更リクエストを許可するかどうかを判断できるように、ユーザーがその変更リクエストについて回答する質問を提供することをお勧めします。

> **Tip**
>
> [Hide preview] (プレビューを非表示)と [Show preview] (プレビューを表示) を切り替えて、作成しながら内容を確認します。

7. [Change request approvals] (変更リクエスト承認) セクションで、以下を実行します。

   - (オプション) この変更テンプレートから作成された変更リクエストを、承認者が確認せずに自動的に実行できるようにする場合は (変更凍結イベントを除く)、[Enable auto-approval (自動承認の有効化)] を選択します。

     > **Note**
     >
     > 変更テンプレートで自動承認を有効にすると、レビュー担当者をバイパスするオプションをユーザーに提供できます。レビュー担当者は、変更リクエストの作成時に指定できます。このため、変更テンプレートでレビュー担当者のオプションを指定する必要があります。

     > **Important**
     >
     > 変更テンプレートの自動承認を有効にすると、ユーザーは変更リクエストを実行する前にレビュー担当者によるレビューが不要なテンプレートを使用して変更リクエストを送信できます (変更凍結イベントの承認者を除く)。特定のユーザー、グループ、ま

たは IAM ロールによる自動承認リクエストの送信を制限する場合は、この目的で IAM ポリシーの条件を使用できます。詳細については、「自動承認のランブックワークフローへのアクセスを制御する」を参照してください。

- [このレベルで必要な承認数] で、この変更テンプレートから作成された変更リクエストがこのレベルで受け取る必要がある承認数を選択します。
- 必須の第 1 レベルの承認者を追加するには、[Add approver (承認者を追加)] を選択した後、以下のいずれかを選択します。
  - Template specified approvers (テンプレートで指定された承認者) – この変更テンプレートから作成された変更リクエストを承認するために、アカウントからユーザー、グループ、または AWS Identity and Access Management (IAM) ロールを 1 つ以上選択します。このテンプレートを使用して作成された変更リクエストはいずれも、指定された各承認者によって確認および承認される必要があります。
  - Request specified approvers (リクエストで指定された承認者) – 変更リクエストを作成するユーザーがリクエストの作成時にレビューワーを指定します。レビューワーは、アカウント内のユーザーのリストから選択できます。

    [Required] (必須) 列に入力する数字は、この変更テンプレートを使用する変更リクエストによって指定される必要があるレビューワーの人数を決定します。

> **Important**
>
> 2023 年 1 月 23 日より前は、[ビルダー] タブでは、行ごとの承認のみの指定がサポートされていました。[ビルダー] タブを使用して既存の変更テンプレートに追加する新しい変更テンプレートと新しいレベルは、レベルごとの承認のみをサポートしています。Change Manager オペレーションでは、レベルごとの承認のみを使用することをお勧めします。
> 詳細については、「変更テンプレートの承認について」を参照してください。

- [SNS topic to notify approvers] (承認者に通知する SNS トピック) には、以下を実行します。
  1. 次のいずれかを選択して、アカウント内の Amazon Simple Notification Service (Amazon SNS) トピックを指定します。これは、変更リクエストがレビューできることを承認者に通知を送信するときに使用されます。
     - Enter an SNS Amazon Resource Name (ARN)(SNS Amazon リソースネーム (ARN) を入力) – [Topic ARN (トピック ARN) には、既存の Amazon SNS トピックの ARN を入力します。このトピックは、組織のどのアカウントのものでも使用できます。

- Select an existing SNS topic (既存の SNS トピックを選択) – [Target notification topic] (ターゲット通知トピック) には、現在 AWS アカウント にある既存の Amazon SNS トピックの ARN を選択します。(このオプションは、現在の AWS アカウント と AWS リージョン で Amazon SNS トピックをまだ作成していない場合は使用できません)。
- Specify SNS topic when the change request is created(変更リクエストの作成時に SNS トピックを指定) – 変更リクエストを作成するユーザーが、通知に使用する Amazon SNS トピックを指定できます。

> **Note**
>
> 選択する Amazon SNS トピックは、送信する通知とその送信先のサブスクライバーを指定するように設定されている必要があります。Amazon SNアクセスポリシーは、Change Manager が通知を送信できるように、Systems Manager にアクセス許可も付与する必要があります。詳細については、Change Manager 通知用の Amazon SNS トピックの設定 を参照してください。

2. [Add notification] (通知を追加) をクリックします。

8. (オプション) 承認者のレベルを追加するには、[Add approval level] (承認レベルを追加) をクリックし、このレベルのテンプレートで指定された承認者とリクエストで指定された承認者の中から選択します。次に、このレベルの承認者に通知する SNS トピックを選択します。

   第 1 レベルの承認者がすべての承認を受信すると、第 2 レベルの承認者に通知され、という流れをたどります。

   各テンプレートには、最大 5 レベルの承認者を追加できます。例えば、第 1 レベルでは技術ロールのユーザーの承認を求め、次に 2 番目のレベルでは管理職の承認を求めることができます。

9. [Monitoring] (モニタリング) セクションの [CloudWatch alarm to monitor] (監視する CloudWatch アラーム) に、このテンプレートに基づくランブックワークフローの進行状況を監視するための、現在のアカウントにある Amazon CloudWatch アラームの名前を入力します。

> **Tip**
>
> 新しいアラームを作成する、または指定するアラームの設定を確認するには、[Open the Amazon CloudWatch console] (Amazon CloudWatch コンソールを開く) をクリックしま

す。CloudWatch アラームの使用の詳細については、Amazon CloudWatch ユーザーガイドの「CloudWatch アラームの使用」を参照してください。

10. [Notifications] (通知) セクションで、以下を実行します。

    1. 次のいずれかを選択して、アカウント内の Amazon SNS トピックを指定します。これは、この変更テンプレートを使用して作成された変更リクエストに関する通知を送信するために使用されます。

       - Enter an SNS Amazon Resource Name (ARN)(SNS Amazon リソースネーム (ARN) を入力) – [Topic ARN (トピック ARN) には、既存の Amazon SNS トピックの ARN を入力します。このトピックは、組織のどのアカウントのものでも使用できます。
       - Select an existing SNS topic (既存の SNS トピックを選択) – [Target notification topic] (ターゲット通知トピック) には、現在 AWS アカウント にある既存の Amazon SNS トピックの ARN を選択します。(このオプションは、現在の AWS アカウント と AWS リージョン で Amazon SNS トピックをまだ作成していない場合は使用できません)。

       > **Note**
       >
       > 選択する Amazon SNS トピックは、送信する通知とその送信先のサブスクライバーを指定するように設定されている必要があります。Amazon SNアクセスポリシーは、Change Manager が通知を送信できるように、Systems Manager にアクセス許可も付与する必要があります。詳細については、Change Manager 通知用の Amazon SNS トピックの設定 を参照してください。

    2. [Add notification] (通知を追加) をクリックします。

11. (オプション) [Tags] (タグ) セクションで、変更テンプレートにタグキーの名前/値ペアを 1 つ、または複数適用します。

    タグは、リソースに割り当てるオプションのメタデータです。タグを使用することで、目的、所有者、または環境などの異なる方法でリソースを分類できます。例えば、変更テンプレートが実行する変更のタイプと、実行される環境を特定するために、タグを付けることができます。この場合、以下のキーの名前と値のペアを指定します。

    - `Key=TaskType,Value=InstanceRepair`
    - `Key=Environment,Value=Production`

12. [Save and preview] (保存してプレビュー) をクリックします。
13. 作成する変更テンプレートの詳細を確認します。

レビューのために送信する前に変更テンプレートを変更したい場合は、[Actions、Edit] (アクション、編集) と選択します。

変更テンプレートの内容に問題がなければ、[Submit for Review] (レビューのために送信) をクリックします。Change Manager の [Settings] (設定) タブでテンプレートレビューワーとして指定された組織またはアカウント内のユーザーに、新しい変更テンプレートのレビューが保留中であることが通知されます。

Amazon SNS トピックが変更テンプレートで指定されている場合、変更テンプレートが拒否または承認されたときに通知が送信されます。この変更テンプレートに関連する通知が届かない場合は、後ほど Change Manager に戻って、そのステータスを確認できます。

エディタを使用した変更テンプレートの作成

コンソールコントロールを使用する代わりに JSON または YAML を入力して、AWS Systems Manager のツールである Change Manager に変更テンプレートを設定するには、このトピックの手順を実行します。

エディタを使用して変更テンプレートを作成するには

1. ナビゲーションペインで、Change Manager を選択します。
2. [Create template] (テンプレートの作成) をクリックします。
3. [Name] (名前) には、**`RestartEC2LinuxInstance`** など、その目的を識別しやすくするテンプレート名を入力します。
4. 上記の [Change template details] (変更テンプレートの詳細) で [Editor] (エディタ) を選択します。
5. [Document editor] (ドキュメントエディタ) セクションで [Edit] (編集) をクリックしてから、変更テンプレートの JSON コンテンツ、または YAML コンテンツを入力します。

   以下に例を示します。

> **Note**
>
> パラメータ `minRequiredApprovals` は、このテンプレートを使用して作成された変更リクエストを承認する必要がある、指定されたレベルのレビュー担当者の数を指定するために使用されます。

この例では、2 つのレベルの承認を示しています。承認レベルは最大 5 つまで指定できますが、必要なレベルは 1 つだけです。
最初のレベルでは、特定のユーザー「John-Doe」が各変更リクエストを承認する必要があります。その後、IAM ロール Admin のいずれか 3 名のメンバーが変更リクエストを承認する必要があります。
変更テンプレートの承認の詳細については、「変更テンプレートの承認について」を参照してください。

YAML

```
description: >-
  This change template demonstrates the feature set available for creating
  change templates for Change Manager. This template starts a Runbook workflow
  for the Automation runbook called AWS-HelloWorld.
templateInformation: >
  ### Document Name: HelloWorldChangeTemplate

  ## What does this document do?

  This change template demonstrates the feature set available for creating
  change templates for Change Manager. This template starts a Runbook workflow
  for the Automation runbook called AWS-HelloWorld.

  ## Input Parameters

  * ApproverSnsTopicArn: (Required) Amazon Simple Notification Service ARN for
  approvers.

  * Approver: (Required) The name of the approver to send this request to.

  * ApproverType: (Required) The type of reviewer.
    * Allowed Values: IamUser, IamGroup, IamRole, SSOGroup, SSOUser

  ## Output Parameters

  This document has no outputs
schemaVersion: '0.3'
parameters:
  ApproverSnsTopicArn:
    type: String
    description: Amazon Simple Notification Service ARN for approvers.
```

```
  Approver:
    type: String
    description: IAM approver
  ApproverType:
    type: String
    description: >-
      Approver types for the request. Allowed values include IamUser, IamGroup,
      IamRole, SSOGroup, and SSOUser.
executableRunBooks:
  - name: AWS-HelloWorld
    version: '1'
emergencyChange: false
autoApprovable: false
mainSteps:
  - name: ApproveAction1
    action: 'aws:approve'
    timeoutSeconds: 3600
    inputs:
      Message: >-
        A sample change request has been submitted for your review in Change
        Manager. You can approve or reject this request.
      EnhancedApprovals:
        NotificationArn: '{{ ApproverSnsTopicArn }}'
        Approvers:
          - approver: John-Doe
            type: IamUser
            minRequiredApprovals: 1
  - name: ApproveAction2
    action: 'aws:approve'
    timeoutSeconds: 3600
    inputs:
      Message: >-
        A sample change request has been submitted for your review in Change
        Manager. You can approve or reject this request.
      EnhancedApprovals:
        NotificationArn: '{{ ApproverSnsTopicArn }}'
        Approvers:
          - approver: Admin
            type: IamRole
            minRequiredApprovals: 3
```

JSON

```
{
   "description": "This change template demonstrates the feature set available
 for creating
  change templates for Change Manager. This template starts a Runbook workflow
  for the Automation runbook called AWS-HelloWorld",
   "templateInformation": "### Document Name: HelloWorldChangeTemplate\n\n
    ## What does this document do?\n
    This change template demonstrates the feature set available for creating
 change templates for Change Manager.
    This template starts a Runbook workflow for the Automation runbook called
 AWS-HelloWorld.\n\n
    ## Input Parameters\n* ApproverSnsTopicArn: (Required) Amazon Simple
 Notification Service ARN for approvers.\n
    * Approver: (Required) The name of the approver to send this request to.\n
    * ApproverType: (Required) The type of reviewer.  * Allowed Values: IamUser,
 IamGroup, IamRole, SSOGroup, SSOUser\n\n
    ## Output Parameters\nThis document has no outputs\n",
   "schemaVersion": "0.3",
   "parameters": {
      "ApproverSnsTopicArn": {
         "type": "String",
         "description": "Amazon Simple Notification Service ARN for approvers."
      },
      "Approver": {
         "type": "String",
         "description": "IAM approver"
      },
      "ApproverType": {
         "type": "String",
         "description": "Approver types for the request. Allowed values include
 IamUser, IamGroup, IamRole, SSOGroup, and SSOUser."
      }
   },
   "executableRunBooks": [
      {
         "name": "AWS-HelloWorld",
         "version": "1"
      }
   ],
   "emergencyChange": false,
   "autoApprovable": false,
```

```
  "mainSteps": [
     {
        "name": "ApproveAction1",
        "action": "aws:approve",
        "timeoutSeconds": 3600,
        "inputs": {
           "Message": "A sample change request has been submitted for your
review in Change Manager. You can approve or reject this request.",
           "EnhancedApprovals": {
              "NotificationArn": "{{ ApproverSnsTopicArn }}",
              "Approvers": [
                 {
                    "approver": "John-Doe",
                    "type": "IamUser",
                    "minRequiredApprovals": 1
                 }
              ]
           }
        }
     },
       {
        "name": "ApproveAction2",
        "action": "aws:approve",
        "timeoutSeconds": 3600,
        "inputs": {
           "Message": "A sample change request has been submitted for your
review in Change Manager. You can approve or reject this request.",
           "EnhancedApprovals": {
              "NotificationArn": "{{ ApproverSnsTopicArn }}",
              "Approvers": [
                 {
                    "approver": "Admin",
                    "type": "IamRole",
                    "minRequiredApprovals": 3
                 }
              ]
           }
        }
     }
  ]
}
```

6. [Save and preview] (保存してプレビュー) をクリックします。

7. 作成する変更テンプレートの詳細を確認します。

   レビューのために送信する前に変更テンプレートを変更したい場合は、[Actions、Edit] (アクション、編集) と選択します。

   変更テンプレートの内容に問題がなければ、[Submit for Review] (レビューのために送信) をクリックします。Change Manager の [Settings] (設定) タブでテンプレートレビューワーとして指定された組織またはアカウント内のユーザーに、新しい変更テンプレートのレビューが保留中であることが通知されます。

   Amazon Simple Notification Service (Amazon SNS) トピックが変更テンプレートで指定されている場合、変更テンプレートが拒否または承認されたときに通知が送信されます。この変更テンプレートに関連する通知が届かない場合は、後ほど Change Manager に戻って、そのステータスを確認できます。

コマンドラインツールを使用した変更テンプレートの作成

以下の手順では、AWS Command Line Interface (AWS CLI) (Linux、macOS、または Windows の場合) または AWS Tools for Windows PowerShell を使用して、AWS Systems Manager のツールである Change Manager で変更リクエストを作成する方法について説明します。

変更テンプレートを作成するには

1. まだ AWS CLI または AWS Tools for PowerShell をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」および「AWS Tools for PowerShell のインストール」を参照してください。

2. ローカルマシンに `MyChangeTemplate.json` などの名前の JSON ファイルを作成してから、変更テンプレートのコンテンツを貼り付けます。

   > **Note**
   >
   > 変更テンプレートは、オートメーションランブックと同じサポートのすべてが含まれていないスキーマ 0.3 のバージョンを使用します。

   以下に例を示します。

> **Note**
>
> パラメータ minRequiredApprovals は、このテンプレートを使用して作成された変更リクエストを承認する必要がある、指定されたレベルのレビュー担当者の数を指定するために使用されます。
> この例では、2 つのレベルの承認を示しています。承認レベルは最大 5 つまで指定できますが、必要なレベルは 1 つだけです。
> 最初のレベルでは、特定のユーザー「John-Doe」が各変更リクエストを承認する必要があります。その後、IAM ロール Admin のいずれか 3 名のメンバーが変更リクエストを承認する必要があります。
> 変更テンプレートの承認の詳細については、「変更テンプレートの承認について」を参照してください。

```
{
   "description": "This change template demonstrates the feature set available for
 creating
  change templates for Change Manager. This template starts a Runbook workflow
  for the Automation runbook called AWS-HelloWorld",
   "templateInformation": "### Document Name: HelloWorldChangeTemplate\n\n
    ## What does this document do?\n
    This change template demonstrates the feature set available for creating change
 templates for Change Manager.
    This template starts a Runbook workflow for the Automation runbook called AWS-
HelloWorld.\n\n
    ## Input Parameters\n* ApproverSnsTopicArn: (Required) Amazon Simple
 Notification Service ARN for approvers.\n
    * Approver: (Required) The name of the approver to send this request to.\n
    * ApproverType: (Required) The type of reviewer.  * Allowed Values: IamUser,
 IamGroup, IamRole, SSOGroup, SSOUser\n\n
    ## Output Parameters\nThis document has no outputs\n",
  "schemaVersion": "0.3",
  "parameters": {
     "ApproverSnsTopicArn": {
        "type": "String",
        "description": "Amazon Simple Notification Service ARN for approvers."
     },
     "Approver": {
        "type": "String",
        "description": "IAM approver"
```

```
      },
      "ApproverType": {
         "type": "String",
         "description": "Approver types for the request. Allowed values include
IamUser, IamGroup, IamRole, SSOGroup, and SSOUser."
      }
   },
   "executableRunBooks": [
      {
         "name": "AWS-HelloWorld",
         "version": "1"
      }
   ],
   "emergencyChange": false,
   "autoApprovable": false,
   "mainSteps": [
      {
         "name": "ApproveAction1",
         "action": "aws:approve",
         "timeoutSeconds": 3600,
         "inputs": {
            "Message": "A sample change request has been submitted for your review
in Change Manager. You can approve or reject this request.",
            "EnhancedApprovals": {
               "NotificationArn": "{{ ApproverSnsTopicArn }}",
               "Approvers": [
                  {
                     "approver": "John-Doe",
                     "type": "IamUser",
                     "minRequiredApprovals": 1
                  }
               ]
            }
         }
      },
        {
         "name": "ApproveAction2",
         "action": "aws:approve",
         "timeoutSeconds": 3600,
         "inputs": {
            "Message": "A sample change request has been submitted for your review
in Change Manager. You can approve or reject this request.",
            "EnhancedApprovals": {
               "NotificationArn": "{{ ApproverSnsTopicArn }}",
```

```
                "Approvers": [
                   {
                      "approver": "Admin",
                      "type": "IamRole",
                      "minRequiredApprovals": 3
                   }
                ]
             }
          }
       }
    ]
}
```

3. 次のコマンドを実行して、変更テンプレートを作成します。

Linux & macOS

```
aws ssm create-document \
    --name MyChangeTemplate \
    --document-format JSON \
    --document-type Automation.ChangeTemplate \
    --content file://MyChangeTemplate.json \
    --tags Key=tag-key,Value=tag-value
```

Windows

```
aws ssm create-document ^
    --name MyChangeTemplate ^
    --document-format JSON ^
    --document-type Automation.ChangeTemplate ^
    --content file://MyChangeTemplate.json ^
    --tags Key=tag-key,Value=tag-value
```

PowerShell

```
$json = Get-Content -Path "C:\path\to\file\MyChangeTemplate.json" | Out-String
New-SSMDocument `
    -Content $json `
    -Name "MyChangeTemplate" `
    -DocumentType "Automation.ChangeTemplate" `
    -Tags "Key=tag-key,Value=tag-value"
```

指定できるオプションの詳細については、「create-document」を参照してください。

システムが以下のような情報をレスポンスします。

```
{
   "DocumentDescription":{
      "CreatedDate":1.585061751738E9,
      "DefaultVersion":"1",
      "Description":"Use this template to update an EC2 Linux AMI. Requires one
      approver specified in the template and an approver specified in the
 request.",
      "DocumentFormat":"JSON",
      "DocumentType":"Automation",
      "DocumentVersion":"1",
      "Hash":"0d3d879b3ca072e03c12638d0255ebd004d2c65bd318f8354fcde820dEXAMPLE",
      "HashType":"Sha256",
      "LatestVersion":"1",
      "Name":"MyChangeTemplate",
      "Owner":"123456789012",
      "Parameters":[
         {
            "DefaultValue":"",
            "Description":"Level one approvers",
            "Name":"LevelOneApprovers",
            "Type":"String"
         },
         {
            "DefaultValue":"",
            "Description":"Level one approver type",
            "Name":"LevelOneApproverType",
            "Type":"String"
         },
   "cloudWatchMonitors": {
      "monitors": [
         "my-cloudwatch-alarm"
      ]
   }
      ],
      "PlatformTypes":[
         "Windows",
         "Linux"
      ],
```

```
        "SchemaVersion":"0.3",
        "Status":"Creating",
        "Tags":[

        ]
    }
}
```

Change Manager の [Settings] (設定) タブでテンプレートレビューワーとして指定された組織またはアカウント内のユーザーに、新しい変更テンプレートのレビューが保留中であることが通知されます。

Amazon Simple Notification Service (Amazon SNS) トピックが変更テンプレートで指定されている場合、変更テンプレートが拒否または承認されたときに通知が送信されます。この変更テンプレートに関連する通知が届かない場合は、後ほど Change Manager に戻って、そのステータスを確認できます。

変更テンプレートの確認と、承認または拒否

AWS Systems Manager のツールである Change Manager で変更テンプレートのレビューワーとして指定されている場合、新しい変更テンプレートまたは変更テンプレートの新しいバージョンが確認待ちであるときに通知を受け取ります。Amazon Simple Notification Service (Amazon SNS) トピックから通知が送信されます。

> **Note**
>
> この機能は、変更テンプレート確認通知の送信に Amazon SNS トピックを使用するようにアカウントが設定されているかどうかにより異なります。テンプレートレビューワーの通知トピックの指定に関する情報については、「タスク 1: Change Managerユーザー ID 管理とテンプレートレビューワーの設定」を参照してください。

変更テンプレートをレビューするには、通知に記載されているリンクを開き、AWS Management Console にサインインして、この手順のステップに従います。

変更テンプレートを確認して承認または却下するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。

2. ナビゲーションペインで、[Change Manager] を選択します。
3. [Overview] (概要) タブの [Change templates] (変更テンプレート) セクションで、[Pending review] (レビュー待ち) の番号を選択します。
4. [Change templates] (変更テンプレート) のリストで、確認する変更テンプレートの名前を見つけて選択します。
5. [Summary] (概要) ページで、提案された変更テンプレートのコンテンツを確認して、以下のいずれかを実行します。
   - 変更テンプレートを承認し、変更リクエストで使用できるようにするには、[Approve] (承認) を選択します。
   - 変更テンプレートを拒否し、変更リクエストで使用できないようにするには、[Reject] (拒否) を選択します。

変更テンプレートの削除

このトピックでは、Systems Manager のツールである Change Manager で作成したテンプレートを削除する方法について説明します。組織で Change Manager を使用している場合、この手順は委任された管理者アカウントで実行します。

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Change Manager] を選択します。
3. [Templates (テンプレート)] タブを選択します。
4. 削除するテンプレートの名前を選択します。
5. [アクション、テンプレートの削除] を選択します。
6. 確認ダイアログに「**DELETE**」という語を入力してから、[削除] を選択します。

変更リクエストの使用

変更リクエストは、AWS またはオンプレミス環境の 1 つ以上のリソースを更新する Automation ランブックを実行するための Change Manager のリクエストです。変更リクエストは、変更テンプレートを使用して作成されます。

AWS Systems Manager のツールである Change Manager で変更リクエストを作成する場合、組織またはアカウント内の 1 人以上の承認者がリクエストを確認して承認する必要があります。必要な

承認がなければ、リクエストされた変更を実施するランブックワークフローの実行は許可されません。

トピック

- 変更リクエストの作成
- 変更リクエストの確認と、承認または拒否

変更リクエストの作成

AWS Systems Manager のツールである Change Manager で変更リクエストを作成すると、選択する変更テンプレートでは通常次の処理が行われます。

- 変更リクエストの承認者を指定する、または必要な承認の数を指定する
- 変更リクエストについて承認者に通知するために使用する Amazon Simple Notification Service (Amazon SNS) トピックを指定します。
- Amazon CloudWatch アラームを指定して、変更リクエストのランブックワークフローをモニタリングします
- リクエストされた変更を行うために選択できるオートメーションランブックを特定する

変更テンプレートは、使用する独自のオートメーションランブックを指定して、誰がリクエストのレビューと承認を行うかを指定できるように設定されている場合もあります。

> **Important**
>
> 組織全体で Change Manager を使用する場合は、常に委任管理者アカウントから変更を行うことをお勧めします。組織内の他のアカウントから変更を行うことはできますが、それらの変更は、委任管理者アカウントで報告されず、表示することもできません。

トピック

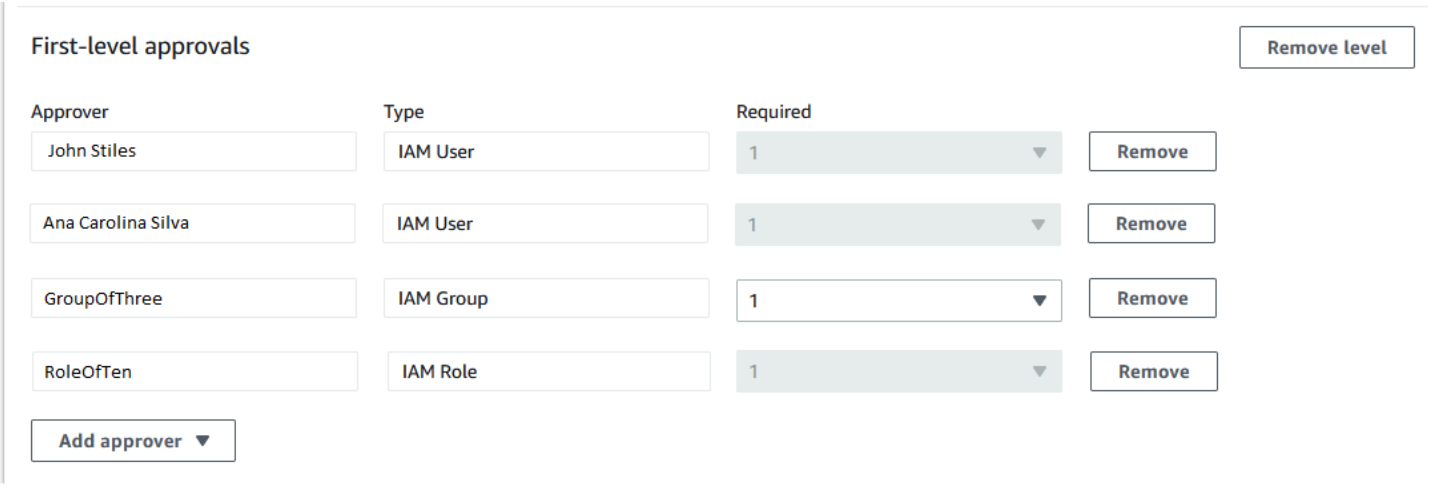
- 変更リクエストの承認について
- 変更リクエストの作成 (コンソール)
- 変更リクエストの作成 (AWS CLI)

変更リクエストの承認について

変更テンプレートに指定された要件によっては、そのテンプレートから作成する変更リクエストは、リクエストのランブックワークフローを実行する前に、最大 5 つのレベルの承認を必要とする場合があります。これらの各レベルに関して、テンプレート作成者は最大 5 人の潜在的な承認者を指定できます。承認者は 1 人のユーザーに限定されません。この意味での承認者は、IAM グループまたは IAM ロールとすることもできます。IAM グループと IAM ロールでは、そのグループまたはロールに属する 1 人以上のユーザーが、変更リクエストに必要な承認の総数の受け取りに対して、承認を提供することができます。テンプレート作成者は、変更テンプレートに必要な数よりも多くの承認者を指定することもできます。

オリジナルの承認ワークフローと更新および/または承認

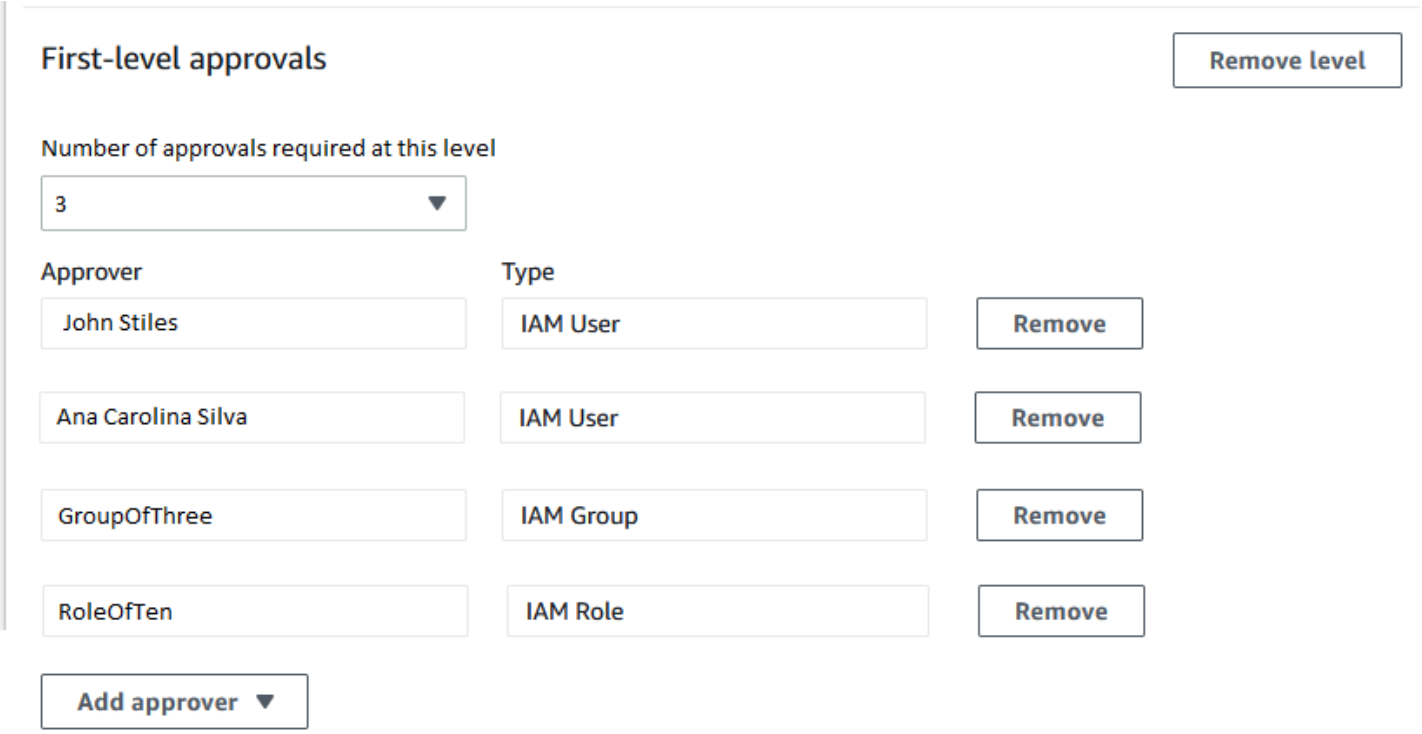
2023 年 1 月 23 日より前に作成された変更テンプレートを使用する場合、変更リクエストをそのレベルで承認するには、指定された各承認者から承認を受ける必要があります。例えば、次のイメージに示された承認レベルの設定では、4 人の承認者が指定されています。指定承認者には、2 人のユーザー (John Stiles と Ana Carolina Silva)、3 人のメンバーで構成されたユーザーグループ (GroupOfThree)、10 人のユーザーを代表するユーザーロール (RoleOfTen) が含まれます。



このレベルで変更リクエストが承認されるには、John Stiles、Ana Carolina Silva、`GroupOfThree` グループの 1 人のメンバー、`RoleOfTen` ロールの 1 人のメンバーによる承認が必要です。

テンプレート作成者は、2023 年 1 月 23 日以降に作成された変更テンプレートを使用して、承認レベルごとに必要な承認の総数を指定できます。これらの承認は、承認者として指定されたユーザー、グループ、ロールを自由に組み合わせて行うことができます。変更テンプレートでは、1 つのレベルに対して 1 つの承認しか必要としませんが、例えば、2 人の個人ユーザー、2 つのグループ、1 人のロールを潜在的な承認者として指定できます。

例えば、次のイメージに示された承認レベルエリアでは、3 つの承認が必要です。テンプレートで指定された承認者には、2 人のユーザー (John Stiles と Ana Carolina Silva)、3 人のメンバーを含むユーザーグループ (`GroupOfThree`)、10 人のユーザーを代表するユーザーロール (`RoleOfTen`) が含まれます。



`GroupOfThree` グループ内の 3 人のユーザー全員が変更リクエストを承認すると、そのレベルで変更リクエストが承認されます。各ユーザー、グループ、ロールの承認を受け取る必要はありません。承認の最小数は、潜在的な承認者を任意に組み合わせて得ることができます。

変更リクエストが作成されると、そのレベルの承認通知対象として指定されている Amazon SNS トピックのサブスクライバーに通知が送信されます。変更テンプレートの作成者が、使用する必要のある通知トピックを指定したか、指定を許可した可能性があります。

任意のレベルで必要最小限の承認が受理されると、次のレベルの Amazon SNS トピックのサブスクライバーに通知が送信され、以降も同様に通知が送信されます。

承認レベルと承認者がいくつ指定されていても、そのリクエストのランブックワークフローの発生を防ぐには、変更リクエストを 1 回却下するだけで済みます。

変更リクエストの作成 (コンソール)

次の手順では、Systems Manager コンソールを使用して変更リクエストを作成する方法について説明します。

変更リクエストを作成するには (コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Change Manager] を選択します。
3. [Create request] (リクエストを作成) をクリックします。
4. この変更リクエストに使用する変更テンプレートを検索して選択します。
5. [Next] を選択します。
6. [Name] (名前) には、**UpdateEC2LinuxAMI-us-east-2** など、その目的を識別しやすくする変更リクエストの名前を入力します。
7. [Runbook] (ランブック) には、リクエストした変更を行うために使用するランブックを選択します。

   > **Note**
   >
   > ランブックを選択するオプションが利用できなくなっている場合は、使用する必要があるランブックが変更テンプレートの作成者によって指定されています。

8. [Change request information] (変更リクエストの情報) には、Markdown を使用して、変更リクエストに関する追加情報を提供します。これは、レビューワーが変更リクエストを承認するか拒否するかを決定するために役立ちます。使用しているテンプレートの作成者が、指示、または回答する質問を提供している場合もあります。

   > **Note**
   >
   > Markdown は、ドキュメント、およびドキュメント内の個々のステップに wiki 形式の説明を追加できるようにするマークアップ言語です。Markdown の使用に関する詳細については、「AWS での Markdown の使用」を参照してください。

9. [Workflow start time] (ワークフロー開始時刻) セクションで、以下のいずれかを選択します。

   - スケジュールされた時刻にオペレーションを実行する – [Requested start time] (リクエストされた開始時刻) には、このリクエストのランブックワークフローの実行について提案する日付と時刻を入力します。[Estimated end time] (予想終了時間) で、ランブックワークフローが完了する予想日時を入力します。(この時間は、レビュー担当者に伝える予想に過ぎません。)

> **Tip**
>
> [View Change Calendar] (変更カレンダーを表示) をクリックして、指定した時刻にブロッキングイベントがないかどうかをチェックします。

- Run the operation as soon as possible after approval (承認後、できるだけ早くオペレーションを実行する) – 変更リクエストが承認されると、変更を行うことができる無制限期間になり次第、ランブックワークフローが実行されます。

10. [Change request approvals] (変更リクエスト承認) セクションで、以下を実行します。

    1. 承認タイプオプションを表示するには、以下のいずれかを選択します。

       - 自動承認 - 選択した変更テンプレートは、変更リクエストを自動的に実行できるように設定され、承認者の確認は不要です。ステップ 11 に進みます。

         > **Note**
         >
         > Systems Manager の使用を管理する IAM ポリシーで指定されているアクセス許可は、自動承認の変更リクエストを自動的に実行するために送信することを制限してはなりません。

       - 承認者の指定 — この変更リクエストを確認および承認するには、単一または複数のユーザー、グループ、または IAM ロールを追加する必要があります。

         > **Note**
         >
         > Systems Manager の使用を管理する IAM ポリシーで指定されているアクセス許可によって、自動承認変更リクエストを実行できる場合でも、レビュー担当者を指定できます。

    2. [Add approver (承認者を追加)] をクリックして、利用可能なレビュー担当者のリストから単一または複数のユーザー、グループ、またはまたは AWS Identity and Access Management (IAM) ロールを選択します。

       > **Note**
       >
       > 1 人、または複数人の承認者が既に指定されている場合があります。これは、選択した変更テンプレートに、必須の承認者が既に指定されていることを意味します。これ

らの承認者をリクエストから削除することはできません。[承認者を追加] ボタンが有効になっていない場合は、選択したテンプレートでリクエストへのレビューワーの追加が許可されていません。

変更リクエストの承認の詳細については、「変更リクエストの承認について」を参照してください。

3. [SNS topic to notify approvers] (承認者に通知する SNS トピック) で以下のいずれかを選択して、この変更リクエストに追加している承認者への通知の送信に使用される、アカウント内の Amazon SNS トピックを指定します。

> **Note**
>
> Amazon SNS トピックを指定するオプションが利用できなくなっている場合、選択した変更テンプレートで、使用する Amazon SNS トピックが既に指定されています。

- Enter an SNS Amazon Resource Name (ARN)(SNS Amazon リソースネーム (ARN) を入力) – [Topic ARN (トピック ARN) には、既存の Amazon SNS トピックの ARN を入力します。このトピックは、組織のどのアカウントのものでも使用できます。
- Select an existing SNS topic (既存の SNS トピックを選択) – [Target notification topic] (ターゲット通知トピック) には、現在のアカウントにある既存の Amazon SNS トピックの ARN を選択します。(このオプションは、現在の AWS アカウント と AWS リージョン で Amazon SNS トピックをまだ作成していない場合は使用できません)。

> **Note**
>
> 選択する Amazon SNS トピックは、送信する通知とその送信先のサブスクライバーを指定するように設定されている必要があります。Amazon SNアクセスポリシーは、Change Manager が通知を送信できるように、Systems Manager にアクセス許可も付与する必要があります。詳細については、Change Manager 通知用の Amazon SNS トピックの設定 を参照してください。

4. [Add notification] (通知を追加) をクリックします。

11. [Next] を選択します。

12. [IAM role (IAM ロール)] では、この変更リクエストに指定されたランブックの実行に必要な許可を持つ、現在のアカウントの IAM ロールを選択します。

    このロールは、オートメーションのサービスロール (または assume ロール) と呼ばれることもあります。このロールの詳細については、「オートメーションの設定」を参照してください。

13. [Deployment location] (デプロイの場所) セクションで、以下のいずれかを選択します。

> **Note**
>
> AWS Organizations でセットアップされた組織ではなく、単一の AWS アカウント アカウントのみで Change Manager を使用している場合、デプロイ先を指定する必要はありません。

- Apply change to this account (このアカウントに変更を適用) – ランブックワークフローは現在のアカウントのみで実行されます。組織の場合、これは委任管理者アカウントを意味します。
- Apply change to multiple organizational units (OUs) (複数の組織単位 (OU) に変更を適用) – 以下を実行します。

  1. [Accounts and organizational units (OUs)] (アカウントと組織単位 (OU)) には、組織内のメンバーアカウントの ID を **123456789012** 形式で入力、または組織単位の ID を **o-o96EXAMPLE** 形式で入力します。
  2. (オプション) [Execution role name] (実行ロール名) に、ターゲットアカウント、またはこの変更リクエストに指定されているランブックを実行するために必要な許可を持つ OU の IAM ロールの名前を入力します。このロールの名前は、指定した OU 内のすべてのアカウントが同じ名前を使用する必要があります。
  3. (オプション) 指定する追加のアカウント、または OU ごとに [Add another target location] (別のターゲットロケーションを追加する) を選択して、ステップ a と b を繰り返します。
  4. [ターゲット AWS リージョン] には、米国東部 (オハイオ) の `Ohio (us-east-2)` など、変更を行うリージョンを選択します。
  5. [Rate control] (レート制御) を展開します。

     [Concurrency] (同時実行値) に数値を入力して、それがランブックワークフローを同時に実行できるアカウントの数と割合のどちらを表しているかをリストから選択します。

[Error threshold] (エラーしきい値) に数値を入力して、それが操作の停止までにランブックワークフローが失敗できるアカウントの数と割合のどちらを表しているかをリストから選択します。

14. [Deployment targets] (デプロイターゲット) セクションで、以下を実行します。

    1. 次のいずれかを選択します。

       - Single resource (単一のリソース) – 変更は 1 つのリソースにしか行われません。例えば、この変更リクエストのランブックで定義されている操作に応じて、これは 1 つのノード、または 1 つの Amazon Machine Image (AMI) になります。
       - Multiple resources (複数のリソース) – [Parameter] (パラメータ) には、この変更リクエストのランブックからの利用可能なパラメータから選択します。この選択は、更新されるリソースのタイプを反映します。

         例えば、この変更リクエストのランブックが `AWS-RetartEC2Instance` である場合は、`InstanceId` を選択してから、以下を選択することで、どのインスタンスが更新されるのかを定義します。

         - Specify tags (タグを指定する) – 更新されるすべてのリソースに付けられるタグのキーバリューペアを入力します。
         - [Choose a resource group] (リソースグループを選択する) – 更新されるすべてのリソースが属するリソースグループの名前を選択します。
         - Specify parameter values (パラメータ値を指定する) – [Runbook parameters] (ランブックのパラメータ) セクションで更新するリソースを特定します。
         - Target all instances (すべてのインスタンスをターゲットにする) – ターゲットロケーションにあるすべてのマネージドノードで変更を行います。

    2. [Multiple resources] (複数のリソース) を選択した場合は、[Rate control] (レート制御) を展開します。

       [Concurrency] (同時実行値) に数値を入力して、ランブックワークフローが同時に更新できるターゲットの数と割合のどちらを表しているかをリストから選択します。

       [Error threshold] (エラーしきい値) に数値を入力して、操作の停止までに更新が失敗できるターゲットの数と割合のどちらを表しているかをリストから選択します。

15. 前のステップで、複数のリソースを更新するために [Specify parameter values] (パラメータ値を指定する) を選択した場合: [Runbook parameters] (ランブックのパラメータ) セクションで、必

要な入力パラメータの値を指定します。指定する必要があるパラメータ値は、選択した変更テンプレートに関連付けられたオートメーションランブックの内容に基づきます。

例えば、変更テンプレートが `AWS-RetartEC2Instance` ランブックを使用する場合、[instanceId] パラメータには 1 つ、または複数のインスタンス ID を入力する必要があります。または、[Show interactive instance picker] (インタラクティブなインスタンスピッカーを表示) を選択して、利用可能なインスタンスを 1 つずつ選択します。

16. [Next] を選択します。
17. [Review and submit] (レビューして送信) ページで、この変更リクエストに指定したリソースとオプションを再確認します。

    変更を行うすべてのセクションの [Edit] (編集) ボタンをクリックします。

    変更リクエストの内容に問題がなければ、[Submit for approval] (承認のために送信) をクリックします。

リクエスト用に選択した変更テンプレートで Amazon SNS トピックが指定されている場合は、リクエストが拒否または承認されたときに通知が送信されます。リクエストの通知が届かない場合は、Change Manager に戻って、リクエストのステータスを確認できます。

変更リクエストの作成 (AWS CLI)

変更リクエストを作成するには、AWS Command Line Interface(AWS CLI) を使用して、変更リクエストのオプションとパラメータを JSON ファイルで指定し、`--cli-input-json` オプションを使用してコマンドに含めることができます。

変更リクエストを作成するには (AWS CLI)

1. まだ AWS CLI または AWS Tools for PowerShell をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」および「AWS Tools for PowerShell のインストール」を参照してください。
2. `MyChangeRequest.json` などの名前でローカルマシンに JSON ファイルを作成し、次の内容を貼り付けます。

   変更リクエストの値で`########`を置き換えます。

> **Note**
>
> このサンプル JSON では、AWS-HelloWorldChangeTemplate 変更テンプレートおよび AWS-HelloWorld ランブックを使用して変更リクエストを作成します。このサンプルを独自の変更リクエストに適用するには、「AWS Systems Manager API リファレンス」で「StartChangeRequestExecution」を参照してください。使用可能なすべてのパラメータに関する情報が掲載されています。
> 変更リクエストの承認の詳細については、「変更リクエストの承認について」を参照してください。

```
{
    "ChangeRequestName": "MyChangeRequest",
    "DocumentName": "AWS-HelloWorldChangeTemplate",
    "DocumentVersion": "$DEFAULT",
    "ScheduledTime": "2021-12-30T03:00:00",
    "ScheduledEndTime": "2021-12-30T03:05:00",
    "Tags": [
        {
            "Key": "Purpose",
            "Value": "Testing"
        }
    ],
    "Parameters": {
        "Approver": [
            "JohnDoe"
        ],
        "ApproverType": [
            "IamUser"
        ],
        "ApproverSnsTopicArn": [
            "arn:aws:sns:us-east-2:123456789012:MyNotificationTopic"
        ]
    },
    "Runbooks": [
        {
            "DocumentName": "AWS-HelloWorld",
            "DocumentVersion": "1",
            "MaxConcurrency": "1",
            "MaxErrors": "1",
```

```
            "Parameters": {
                "AutomationAssumeRole": [
                    "arn:aws:iam::123456789012:role/MyChangeManagerAssumeRole"
                ]
            }
        }
    ],
    "ChangeDetails": "### Document Name: HelloWorldChangeTemplate\n\n## What does
 this document do?\nThis change template demonstrates the feature set available
 for creating change templates for Change Manager. This template starts a Runbook
 workflow for the Automation document called AWS-HelloWorld.\n\n## Input Parameters
\n* ApproverSnsTopicArn: (Required) Amazon Simple Notification Service ARN for
 approvers.\n* Approver: (Required) The name of the approver to send this request
 to.\n* ApproverType: (Required) The type of reviewer.\n  * Allowed Values:
 IamUser, IamGroup, IamRole, SSOGroup, SSOUser\n\n## Output Parameters\nThis
 document has no outputs \n"
}
```

3. JSON ファイルを作成したディレクトリで、次のコマンドを実行します。

```
aws ssm start-change-request-execution --cli-input-json file://MyChangeRequest.json
```

システムが以下のような情報をレスポンスします。

```
{
    "AutomationExecutionId": "b3c1357a-5756-4839-8617-2d2a4EXAMPLE"
}
```

変更リクエストの確認と、承認または拒否

AWS Systems Manager のツールである Change Manager で変更リクエストのレビューワーとして指定されている場合、新しい変更リクエストが確認待ちであるときに、Amazon Simple Notification Service (Amazon SNS) トピックを通じて通知を受け取ります。

> **Note**
>
> この機能は、変更テンプレートで、確認通知を送信するために Amazon SNS が指定されているかどうかによって異なります。詳細については、Change Manager 通知用の Amazon SNS トピックの設定 を参照してください。

変更リクエストをレビューするには、通知に記載されているリンクを開く、または AWS Management Console に直接サインインして、この手順のステップに従うことができます。

> **Note**
>
> Amazon SNS トピックが変更テンプレートのレビューワーに割り当てられている場合、変更リクエストのステータスが変更されたときに、トピックのサブスクライバーに通知が送信されます。
> 変更リクエストの承認の詳細については、「変更リクエストの承認について」を参照してください。

変更リクエストの確認と、承認または拒否 (コンソール)

次の手順では、Systems Manager コンソールを使用して変更リクエストを確認して承認または拒否する方法について説明します。

1 つの変更リクエストを確認して承認または却下するには

1. 受け取った E メール通知のリンクを開き、AWS Management Console にサインインすると、レビューする変更リクエストに移動します。
2. [Summary] (概要) ページで、提案された変更リクエストの内容を確認します。

   変更リクエストを承認するには、[承認] を選択します。この承認に追加するコメントをダイアログボックスに入力してから、[Approve] (承認) をクリックします。このリクエストによって提示されるランブックワークフローの実行は、スケジュールされている日時に開始、または変更を妨げる制限がなくなり次第開始されます。

   -または-

   変更リクエストを拒否するには、[Reject] (却下) を選択します。この拒否に追加するコメントをダイアログボックスに入力してから、[Reject] (拒否) をクリックします。

複数の変更リクエストを一括で確認して承認または却下するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Change Manager] を選択します。
3. [Approvals] (承認) タブを選択します。

4. (オプション) 各リクエストの名前を選択してユーザーの承認待ちのリクエストの詳細を確認し、[Approvals] (承認) タブに戻ります。
5. 承認する各変更リクエストのチェックボックスを選択します。

   -または-

   拒否する各変更リクエストのチェックボックスを選択します。
6. この承認または居にに関するコメントをダイアログボックスに入力します。
7. 選択した変更リクエストを承認するか拒否するかに応じて、[承認] または [拒否] を選択します。

変更リクエストの確認と、承認または拒否 (コマンドライン)

次の手順には、レビューして承認または変更の要求を拒否するために AWS Command Line Interface (AWS CLI) (Linux、macOS または Windows) を使用する方法が説明されています。

変更リクエストを確認して承認または却下するには

1. まだ AWS Command Line Interface (AWS CLI) をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」を参照してください。
2. ローカルマシンで、AWS CLI コールのパラメータを指定する JSON ファイルを作成します。

```
{
  "OpsItemFilters":
  [
    {
      "Key": "OpsItemType",
      "Values": ["/aws/changerequest"],
      "Operator": "Equal"
    }
  ],
  "MaxResults": number
}
```

   JSON ファイルに承認者の Amazon リソースネーム (ARN) を指定することで、特定の承認者の結果をフィルタリングできます。以下はその例です。

```
{
  "OpsItemFilters":
  [
    {
      "Key": "OpsItemType",
      "Values": ["/aws/changerequest"],
      "Operator": "Equal"
    },
    {
      "Key": "ChangeRequestByApproverArn",
      "Values": ["arn:aws:iam::account-id:user/user-name"],
      "Operator": "Equal"
    }
  ],
  "MaxResults": number
}
```

3. JSON ファイルに指定した変更リクエストの最大数を表示するには、次のコマンドを実行します。

   Linux & macOS

   ```
   aws ssm describe-ops-items \
   --cli-input-json file://filename.json
   ```

   Windows

   ```
   aws ssm describe-ops-items ^
   --cli-input-json file://filename.json
   ```

4. 次のコマンドを実行して、変更リクエストを承認または拒否します。

   Linux & macOS

   ```
   aws ssm send-automation-signal \
       --automation-execution-id ID \
       --signal-type Approve_or_Reject \
       --payload Comment="message"
   ```

Windows

```
aws ssm send-automation-signal ^
--automation-execution-id ID ^
    --signal-type Approve_or_Reject ^
    --payload Comment="message"
```

リクエスト用に選択した変更テンプレートで Amazon SNS トピックが指定されている場合は、リクエストが拒否または承認されたときに通知が送信されます。リクエストの通知が届かない場合は、Change Manager に戻って、リクエストのステータスを確認できます。このコマンドを使用するときのその他のオプションの詳細については、AWS CLI コマンドリファレンスの「AWS Systems Manager」セクションの「send-automation-signal」を参照してください。

変更リクエストの詳細、タスク、およびタイムラインの確認 (コンソール)

AWS Systems Manager のツールである Change Manager のダッシュボードで、変更リクエストに関する情報 (変更処理済みのリクエストを含む) を表示できます。これらの詳細情報には、変更を行うランブックを実行するオートメーションオペレーションへのリンクが含まれます。オートメーション実行 ID はリクエストの作成時に生成されますが、プロセスは、すべての承認が付与され、変更を妨げる制限がなくなるまで実行されません。

変更リクエストの詳細、タスク、タイムラインを確認するには

1. ナビゲーションペインで、Change Manager を選択します。
2. [Requests] (リクエスト) タブを選択します。
3. [Change requests] (変更リクエスト) セクションで、確認する変更リクエストを検索します。

   検索結果は、[Create date range] (作成日付の範囲) オプションを使用して特定の期間に制限することができます。

   以下のプロパティを使ってリクエストをフィルタリングできます。

   - `Status`
   - `Request ID`
   - `Approver`
   - `Requester`

例えば、過去 24 時間に正常に完了したすべての変更リクエストの詳細を表示するには、以下を実行します。

1. [Create date range] (作成日付の範囲) で [1d] を選択します。
2. 検索ボックスで、[Status, CompletedWithSuccess] (ステータス、CompletedWithSuccess) の順に選択します。
3. 検索結果から正常に完了した変更リクエストの名前を選択して、結果を確認します。

4. 次のタブに変更リクエストに関する情報を表示します。

- [Request details] (リクエストの詳細) – リクエスタ、変更テンプレート、および変更用に選択したオートメーションランブックなどの変更リクエストに関する基本的な詳細情報を表示します。また、オートメーションオペレーションの詳細へのリンクを開いて、リクエストで指定されているランブックパラメータ、変更リクエストに割り当てられた Amazon CloudWatch アラーム、およびそのリクエストに提供された承認とコメントに関する情報を表示することもできます。
- Task (タスク) – 完了した変更リクエストのタスクステータス、ターゲットリソース、関連するオートメーションランブック内のステップ、および同時実行値とエラーしきい値の詳細など、変更におけるタスクに関する情報を表示します。
- Timeline (タイムライン) – 日時順にリストされた変更リクエストに関連するすべてのイベントの概要を表示します。概要には、変更リクエストが作成された日時、割り当てられた承認者によるアクション、承認された変更リクエストの実行がスケジュールされている日時に関するメモ、ランブックワークフローの詳細、および変更プロセスの全体とランブックの各ステップに関するステータス変更が表示されます。
- 関連付けられたイベント – AWS CloudTrail Lake に記録された変更リクエストに関する監査可能な詳細を表示します。詳細には、実行された API アクション、それらアクションに含まれるリクエストパラメータ、アクションを実行したユーザーアカウント、プロセス中に更新されたリソースなどが含まれています。

  CloudTrail Lake イベントトラッキングを有効にすると、CloudTrail Lake に変更リクエストに関連するイベントのイベントデータストアが作成されます。変更リクエストを実行したアカウントまたは組織はイベントの詳細を確認できます。CloudTrail Lake イベントトラッキングは、アカウントまたは組織のどの変更リクエストからでも有効にできます。CloudTrail Lake 統合の有効化とイベントデータストアの作成については、「変更リクエストイベントのモニタリング」を参照してください。

> **Note**
>
> CloudTrail Lake の使用には料金がかかります。詳細については、「AWS CloudTrail 料金表」を参照してください。

変更リクエストの集計数の表示 (コマンドライン)

GetOpsSummary API オペレーションを使用すると、AWS Systems Manager のツールである Change Manager で変更リクエストの集計数を表示できます。この API オペレーションは、単一 AWS リージョン 内の単一の AWS アカウント、または複数のアカウントと複数のリージョンに関する集計数を返します。

> **Note**
>
> 複数の AWS アカウント と複数の AWS リージョン に関する変更リクエストの集計数を表示するには、リソースデータ同期をセットアップして設定する必要があります。詳細については、「インベントリのリソースデータ同期を作成する」を参照してください。

次の手順には、変更要求の集計数を表示するために AWS Command Line Interface (AWS CLI) (Linux、macOS または Windows) を使用する方法が説明されています。

変更リクエストの集計数を表示するには

1. まだ AWS Command Line Interface (AWS CLI) をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」を参照してください。
2. 以下のコマンドのいずれかを実行します。

   単一のアカウントとリージョン

   このコマンドは、AWS CLI セッションが設定されている AWS アカウント と AWS リージョン に対するすべての変更リクエストの数を返します。

Linux & macOS

```
aws ssm get-ops-summary \
--filters Key=AWS:OpsItem.OpsItemType,Values="/aws/changerequests",Type=Equal \
--aggregators AggregatorType=count,AttributeName=Status,TypeName=AWS:OpsItem
```

Windows

```
aws ssm get-ops-summary ^
--filters Key=AWS:OpsItem.OpsItemType,Values="/aws/changerequests",Type=Equal ^
--aggregators AggregatorType=count,AttributeName=Status,TypeName=AWS:OpsItem
```

このコールは、以下のような情報を返します。

```
{
    "Entities": [
        {
            "Data": {
                "AWS:OpsItem": {
                    "Content": [
                        {
                            "Count": "38",
                            "Status": "Open"
                        }
                    ]
                }
            }
        }
    ]
}
```

複数のアカウントおよび/またはリージョン

このコマンドは、リソースデータ同期に指定されている AWS アカウント と AWS リージョン のすべての変更リクエストの数を返します。

Linux & macOS

```
aws ssm get-ops-summary \
```

```
    --sync-name resource_data_sync_name \
    --filters Key=AWS:OpsItem.OpsItemType,Values="/aws/
changerequests",Type=Equal \
    --aggregators AggregatorType=count,AttributeName=Status,TypeName=AWS:OpsItem
```

Windows

```
aws ssm get-ops-summary ^
    --sync-name resource_data_sync_name ^
    --filters Key=AWS:OpsItem.OpsItemType,Values="/aws/
changerequests",Type=Equal ^
    --aggregators AggregatorType=count,AttributeName=Status,TypeName=AWS:OpsItem
```

このコールは、以下のような情報を返します。

```
{
    "Entities": [
        {
            "Data": {
                "AWS:OpsItem": {
                    "Content": [
                        {
                            "Count": "43",
                            "Status": "Open"
                        },
                        {
                            "Count": "2",
                            "Status": "Resolved"
                        }
                    ]
                }
            }
        }
    ]
}
```

複数のアカウントと特定のリージョン

このコマンドは、リソースデータ同期に指定されている AWS アカウント のすべての変更リクエストの数を返します。返されるのはコマンドで指定されたリージョンからのデータのみです。

Linux & macOS

```
aws ssm get-ops-summary \
    --sync-name resource_data_sync_name \
    --filters Key=AWS:OpsItem.SourceRegion,Values='Region',Type=Equal
 Key=AWS:OpsItem.OpsItemType,Values="/aws/changerequests",Type=Equal \
    --aggregators AggregatorType=count,AttributeName=Status,TypeName=AWS:OpsItem
```

Windows

```
aws ssm get-ops-summary ^
    --sync-name resource_data_sync_name ^
    --filters Key=AWS:OpsItem.SourceRegion,Values='Region',Type=Equal
 Key=AWS:OpsItem.OpsItemType,Values="/aws/changerequests",Type=Equal ^
    --aggregators AggregatorType=count,AttributeName=Status,TypeName=AWS:OpsItem
```

複数のアカウントとリージョン (出力をリージョンごとに分類)

このコマンドは、リソースデータ同期に指定されている AWS アカウント と AWS リージョン のすべての変更リクエストの数を返します。出力には、リージョンごとの集計数情報が表示されます。

Linux & macOS

```
aws ssm get-ops-summary \
    --sync-name resource_data_sync_name \
    --filters Key=AWS:OpsItem.OpsItemType,Values="/aws/
changerequests",Type=Equal \
    --aggregators
 '[{"AggregatorType":"count","TypeName":"AWS:OpsItem","AttributeName":"Status","Aggregat
[{"AggregatorType":"count","TypeName":"AWS:OpsItem","AttributeName":"SourceRegion"}]}]'
```

Windows

```
aws ssm get-ops-summary ^
    --sync-name resource_data_sync_name ^
    --filters Key=AWS:OpsItem.OpsItemType,Values="/aws/
changerequests",Type=Equal ^
```

```
    --aggregators
 '[{"AggregatorType":"count","TypeName":"AWS:OpsItem","AttributeName":"Status","Aggregat
[{"AggregatorType":"count","TypeName":"AWS:OpsItem","AttributeName":"SourceRegion"}]}]'
```

このコールは、以下のような情報を返します。

```
{
        "Entities": [
            {
                "Data": {
                    "AWS:OpsItem": {
                        "Content": [
                            {
                                "Count": "38",
                                "SourceRegion": "us-east-1",
                                "Status": "Open"
                            },
                            {
                                "Count": "4",
                                "SourceRegion": "us-east-2",
                                "Status": "Open"
                            },
                            {
                                "Count": "1",
                                "SourceRegion": "us-west-1",
                                "Status": "Open"
                            },
                            {
                                "Count": "2",
                                "SourceRegion": "us-east-2",
                                "Status": "Resolved"
                            }
                        ]
                    }
                }
            }
        ]
    }
```

複数のアカウントとリージョン (出力をアカウントおよびリージョンごとに分類)

このコマンドは、リソースデータ同期に指定されている AWS アカウント と AWS リージョン のすべての変更リクエストの数を返します。出力は、集計数情報をアカウントおよびリージョン別に分類します。

Linux & macOS

```
aws ssm get-ops-summary \
    --sync-name resource_data_sync_name \
    --filters Key=AWS:OpsItem.OpsItemType,Values="/aws/
changerequests",Type=Equal \
    --aggregators
 '[{"AggregatorType":"count","TypeName":"AWS:OpsItem","AttributeName":"Status","Aggregat
[{"AggregatorType":"count","TypeName":"AWS:OpsItem","AttributeName":"SourceAccountId","A
[{"AggregatorType":"count","TypeName":"AWS:OpsItem","AttributeName":"SourceRegion"}]}]}]
```

Windows

```
aws ssm get-ops-summary ^
    --sync-name resource_data_sync_name ^
    --filters Key=AWS:OpsItem.OpsItemType,Values="/aws/
changerequests",Type=Equal ^
    --aggregators
 '[{"AggregatorType":"count","TypeName":"AWS:OpsItem","AttributeName":"Status","Aggregat
[{"AggregatorType":"count","TypeName":"AWS:OpsItem","AttributeName":"SourceAccountId","A
[{"AggregatorType":"count","TypeName":"AWS:OpsItem","AttributeName":"SourceRegion"}]}]}]
```

このコールは、以下のような情報を返します。

```
{
    "Entities": [
        {
            "Data": {
                "AWS:OpsItem": {
                    "Content": [
                        {
                            "Count": "38",
                            "SourceAccountId": "123456789012",
                            "SourceRegion": "us-east-1",
                            "Status": "Open"
                        },
```

```
                        {
                            "Count": "4",
                            "SourceAccountId": "111122223333",
                            "SourceRegion": "us-east-2",
                            "Status": "Open"
                        },
                        {
                            "Count": "1",
                            "SourceAccountId": "111122223333",
                            "SourceRegion": "us-west-1",
                            "Status": "Open"
                        },
                        {
                            "Count": "2",
                            "SourceAccountId": "444455556666",
                            "SourceRegion": "us-east-2",
                            "Status": "Resolved"
                        },
                        {
                            "Count": "1",
                            "SourceAccountId": "222222222222",
                            "SourceRegion": "us-east-1",
                            "Status": "Open"
                        }
                    ]
                }
            }
        }
    ]
}
```

Change Manager アクティビティの監査とログ記録

Amazon CloudWatch と AWS CloudTrail アラームを使用して、AWS Systems Manager のツールである Change Manager でアクティビティを監査できます。

Systems Manager の監査とログ記録のオプションに関する詳細については、「AWS Systems Manager でのログ記録とモニタリング」を参照してください。

CloudWatch アラームを使用した Change Manager アクティビティの監査

CloudWatch アラームを設定して、変更テンプレートに割り当てることができます。アラームで定義された条件のいずれかが満たされると、そのアラームに指定されたアクションが実行されます。アラームの設定では、アラーム条件が満たされたときに通知する Amazon Simple Notification Service (Amazon SNS) トピックを指定できます。

Change Managerテンプレートの作成に関する詳細については、「変更テンプレートの使用」を参照してください。

CloudWatch アラームの作成の詳細については、Amazon CloudWatch ユーザーガイドの「CloudWatch アラームの使用」を参照してください。

CloudTrail を使用した Change Manager アクティビティの監査

CloudTrail は、Systems Manager コンソール、AWS Command Line Interface (AWS CLI)、および Systems Manager SDK で実行された API 呼び出しをキャプチャします。情報は、この情報が保存されている CloudTrail コンソールまたは Amazon Simple Storage Service (Amazon S3) バケットで確認できます。アカウントのすべての CloudTrail ログに対して 1 つのバケットが使用されています。

Change Manager アクションのログには、変更テンプレートドキュメントの作成、変更テンプレートおよび変更リクエストの承認と拒否、オートメーションランブックによって生成されたアクティビティなどが表示されます。Systems Manager アクティビティの CloudTrail ログの表示と使用の詳細については、「AWS Systems Manager による AWS CloudTrail API コールのログ記録」を参照してください。

Change Manager のトラブルシューティング

AWS Systems Manager のツールである Change Manager を使用したトラブルシューティングでは、以下の情報を使用します。

トピック

- Active Directory (グループの使用時における変更リクエストの承認中に発生する「グループ {GUID} が見つかりません」エラー

Active Directory (グループの使用時における変更リクエストの承認中に発生する「グループ *{GUID}* が見つかりません」エラー

問題: ユーザー ID 管理に AWS IAM Identity Center (IAM Identity Center) を使用するとき、承認許可が付与された Active Directory グループのメンバーに「承認されていません」または「グループが見つかりません」というエラーが Change Manager に表示されます。

- 解決策: AWS Management Console へのアクセスのために IAM Identity Center で Active Directory グループを選択すると、これらの Active Directory グループからの情報を IAM Identity Center にコピーする定期的な同期がスケジュールされます。このプロセスは、Active Directory グループメンバーシップを通じて承認されたユーザーがリクエストを正常に承認する前に完了しておく必要があります。詳細については、AWS IAM Identity Center ユーザーガイドの「Microsoft AD directory に接続する」を参照してください。

AWS Systems Manager ドキュメント

AWS Systems Manager ドキュメント (SSM ドキュメント) は、Systems Manager がマネージドインスタンスで実行するアクションを定義します。Systems Manager には、ランタイムでパラメータを指定して使用できる事前設定済みのドキュメントが 100 件以上含まれています。Systems Manager のドキュメントコンソールの、[Owned by Amazon] (Amazon 所有) タブを選択するか、`ListDocuments` API オペレーションを呼び出す際に `Owner` フィルターで Amazon を指定することで、事前設定済みのドキュメントを確認できます。ドキュメントは JavaScript Object Notation (JSON) や YAML を使用し、これにはユーザーが指定するパラメータおよびステップが含まれます。SSM ドキュメントの使用を開始するには、Systems Manager コンソールを開きます。ナビゲーションペインで、[ドキュメント] を選択します。

> **Important**
>
> Systems Manager において、Amazon 所有の SSM ドキュメントとは、Amazon Web Services 自体によって作成および管理されているドキュメントです。Amazon 所有のドキュメントでは、ドキュメント名に `AWS-*` のようなプレフィックスが含まれます。ドキュメントの所有者は、AWS 内の特定のユーザーアカウントではなく Amazon と見なされます。これらのドキュメントは公開されており、誰でも使用できます。

ドキュメントツールには自社の組織にどのようなメリットがありますか?

AWS Systems Manager のツールであるドキュメントには以下のメリットがあります。

- ドキュメントのカテゴリ

  必要なドキュメントを検索しやすくするには、検索するドキュメントの種類に応じてカテゴリを選択します。検索範囲を広げる場合は、同じドキュメントタイプに対して複数のカテゴリを選択できます。異なるドキュメントタイプに関するカテゴリの選択はサポートされていません。カテゴリーは、Amazon が所有するドキュメントでのみ使用できます。

- ドキュメントのバージョン

  ドキュメントの異なるバージョンを作成して保存できます。その後、各ドキュメントのデフォルトのバージョンを指定できます。ドキュメントのデフォルトバージョンは、新しいバージョンに更新したり、古いバージョンのドキュメントに戻すことができます。ドキュメントのコンテンツを変更すると、Systems Manager は自動的にドキュメントのバージョンを増やします。コンソール、AWS Command Line Interface (AWS CLI) コマンド、または API コールでドキュメントバージョンを指定することで、ドキュメントの任意のバージョンを取得または使用できます。

- 必要に応じてドキュメントをカスタマイズする

  ドキュメントのステップやアクションをカスタマイズする場合は、独自のドキュメントを作成できます。システムが、それが作成された AWS リージョン 内の AWS アカウント により、ドキュメントを保存します。SSM ドキュメントの作成方法の詳細については、「SSM ドキュメントコンテンツを作成する」を参照してください。

- タグのドキュメント

  ドキュメントにタグを付けると、そのタグに基づいてドキュメントをすばやく識別できます。たとえば、特定の環境、部門、ユーザー、グループ、または期間でドキュメントをタグ付けできます。ユーザーやグループがアクセスできるタグを指定する AWS Identity and Access Management (IAM) ポリシーを作成することで、ドキュメントへのアクセスを制限することもできます。

- ドキュメントの共有

  ドキュメントを公開するか、または同じ AWS リージョン の特定の AWS アカウント と共有できます。例えば、顧客または従業員に提供するすべての Amazon Elastic Compute Cloud (Amazon EC2) インスタンスに同じ設定を適用したい場合などは、アカウント間でドキュメントを共有すると便利です。これは、インスタンス上のアプリケーションまたはパッチを最新の状態に保つことに加えて、顧客のインスタンスで特定のアクティビティを拒否したい場合にも利用できます。または、組織全体の従業員アカウントで使用されているインスタンスに、特定の内部リソースへのアクセス許可が確実に付与されるようにする場合があります。詳細については、「SSM ドキュメントの共有」を参照してください。

ドキュメントを使用すべきユーザー

- 大規模な運用での効率改善、手動による介入が原因で起きうるエラー数の削減、一般的な問題の解決までの時間の短縮などに、AWS Systems Manager ツールの使用をお考えのすべてのお客様。
- デプロイおよび設定タスクを自動化しようとするインフラストラクチャの専門家。
- 一般的な問題の確実な解決、トラブルシューティングの効率向上、および反復処理の削減を希望する管理者。
- 通常手動で実行しているタスクの自動化を目指すユーザー。

SSM ドキュメントの種類について教えてください。

次の表に、各タイプの SSM ドキュメントと、それらの用途についての説明を示します。

タイプ	以下で使用	詳細
ApplicationConfiguration ApplicationConfigurationSchema	AWS AppConfig	AWS Systems Manager のツールである AWS AppConfig を使用すると、アプリケーション設定を作成、管理し、迅速にデプロイできます。`ApplicationConfiguration` ドキュメントタイプを使用するドキュメントを作成することにより、設定データを SSM ドキュメントに保存できます。詳細については、「AWS AppConfig ユーザーガイド」の「Freeform configurations」(自由形式の設定) を参照してください。 SSM ドキュメントで設定を作成する場合は、対応する JSON スキーマを指定する必要があります。スキーマは `ApplicationConfigu`

タイプ	以下で使用	詳細
		rationSchema ドキュメントタイプを使用し、一連のルールと同様に、各アプリケーション構成設定で許可されるプロパティを定義します。詳細については、「AWS AppConfig ユーザーガイド」の「About validators」(バリデーターについて) を参照してください。

タイプ	以下で使用	詳細
Automation ランブック	オートメーション State Manager Maintenance Windows	Amazon Machine Image (AMI) の作成や更新など、一般的なメンテナンスやデプロイメントタスクを実行する際に、Automation ランブックを使用します。State Manager は、Automation ランブックを使用して設定を適用します。これらのアクションは、インスタンスのライフサイクル中いつでも 1 つ、または複数のターゲットで実行できます。Maintenance Windows は、指定されたスケジュールに基づいた一般的なメンテナンスタスクとデプロイメントタスクの実行に Automation ランブックを使用します。 Linux ベースのオペレーティングシステム用にサポートされているAutomation ランブックはすべて、macOS 向けの EC2 インスタンスでもサポートされています。

タイプ	以下で使用	詳細
Change Calendar ドキュメント	Change Calendar	AWS Systems Manager のツールである Change Calendar は、`ChangeCalendar` ドキュメントタイプを使用します。Change Calendar ドキュメントには、Automation アクションによる環境の変更を許可または禁止できるカレンダーエントリと関連するイベントが保存されます。Change Calendar では、ドキュメントに iCalendar 2.0 データがプレーンテキスト形式で保存されます。 Change Calendar は、macOS の EC2 インスタンスではサポートされていません。

タイプ	以下で使用	詳細
AWS CloudFormation テンプレート	AWS CloudFormation	AWS CloudFormation テンプレートは、CloudFormation スタックでプロビジョニングするリソースについて記述します。CloudFormation テンプレートを Systems Manager のドキュメントとして保存すると、Systems Manager のドキュメント機能のメリットを活用できます。これには、複数のバージョンのテンプレートの作成と比較、同じ AWS リージョン の他のアカウントとのテンプレートの共有が含まれます。 Systems Manager のツールである Application Manager を使用して、CloudFormation テンプレートとスタックを作成して編集できます。詳細については、「Application Manager での AWS CloudFormation テンプレートとスタックの使用」を参照してください。

タイプ	以下で使用	詳細
コマンドのドキュメント	Run Command State Manager Maintenance Windows	AWS Systems Manager のツールである Run Command は、コマンドドキュメントを使用してコマンドを実行します。AWS Systems Manager のツールである State Manager は、コマンドドキュメントを使用して設定を適用します。これらのアクションは、インスタンスのライフサイクル中にいつでも、1 つまたは複数のターゲットで実行できます。AWS Systems Manager のツールである Maintenance Windows は、指定されたスケジュールに基づいて設定を適用するためにコマンドドキュメントを使用します。 ほとんどのコマンドドキュメントは、Systems Manager でサポートされているすべての Linux および Windows Server オペレーティングシステムでサポートされています。mac OS 向けの EC2 インスタンスでは、以下のコマンドドキュメントがサポートされています。 • `AWS-ConfigureAWSPackage` • `AWS-RunPatchBaseline`

タイプ	以下で使用	詳細
		• AWS-RunPatchBaselineAssociation • AWS-RunShellScript
AWS Config コンフォーマンスパックテンプレート	AWS Config	AWS Config コンフォーマンスパックテンプレートは YAML 形式のドキュメントで、AWS Config マネージドルールまたはカスタムルールおよび修復アクションのリストを含むコンフォーマンスパックを作成するために使用されます。 詳細については、「コンフォーマンスパック」を参照してください。

タイプ	以下で使用	詳細
パッケージドキュメント	Distributor	AWS Systems Manager のツールである Distributor では、パッケージは、SSM ドキュメントで表されます。パッケージドキュメントには、マネージドインスタンスにインストールするソフトウェアまたはアセットを含む添付 ZIP アーカイブファイルが含まれています。Distributor でパッケージを作成するパッケージドキュメントを作成します。 Distributor は、Oracle Linux および macOS マネージドインスタンスではサポートされていません。

タイプ	以下で使用	詳細
ポリシードキュメント	State Manager	AWS Systems Manager のツールである Inventory では、`AWS-GatherSoftwareInventory` ポリシードキュメントと State Manager の関連付けを使って、マネージドインスタンスからインベントリデータを収集します。独自の SSM ドキュメントを作成するときは、Automation ランブックとコマンドドキュメントがマネージドインスタンスへのポリシーの適用に推奨される方法です。 Systems Manager Inventory と `AWS-GatherSoftwareInventory` ポリシードキュメントは、Systems Manager のサポート対象のすべてのオペレーティングシステムでサポートされています。

タイプ	以下で使用	詳細
インシデント後分析テンプレート	Incident Manager インシデント後分析	Incident Manager は、インシデント後分析テンプレートを使用して、AWS オペレーション管理のベストプラクティスに基づいて分析を作成します。 御社のチームは、テンプレートを使用して作成した分析を、インシデント対応での改善点を特定するために使用できます。

タイプ	以下で使用	詳細
セッションドキュメント	Session Manager	AWS Systems Manager のツールである Session Manager は、セッションドキュメントを使用して、ポート転送セッション、インタラクティブコマンドを実行するセッション、SSH トンネルを作成するセッションなど、開始するセッションのタイプを決定します。 セッションドキュメントは、Systems Manager でサポートされているすべての Linux および Windows Server オペレーティングシステムでサポートされています。mac OS 向けの EC2 インスタンスでは、以下のコマンドドキュメントがサポートされています。 • `AWS-PasswordReset` • `AWS-StartInteractiveCommand` • `AWS-StartPortForwardingSession` • `AWS-StartPortForwardingSessionToSocket` • `AWS-StartSSHSession`

SSM ドキュメントクォータ

SSM ドキュメントのクォータの詳細については、「Amazon Web Services 全般のリファレンス」の「Systems Manager Service Quotas」を参照してください。

トピック

- ドキュメントコンポーネント
- SSM ドキュメントコンテンツを作成する
- ドキュメントでの作業

ドキュメントコンポーネント

このセクションには、SSM ドキュメントを構成するコンポーネントに関する情報が含まれます。

内容

- スキーマ、機能、および例
- データ要素とパラメータ
- コマンドドキュメントプラグインリファレンス

スキーマ、機能、および例

AWS Systems Manager (SSM) ドキュメントでは以下のスキーマバージョンを使用しています。

- Command タイプのドキュメントは、スキーマバージョン 1.2、2.0 および 2.2 を使用できます。使用しているドキュメントがスキーマ 1.2 である場合は、スキーマバージョン 2.2 を使用するドキュメントを作成することをお勧めします。
- Policy タイプのドキュメントは、スキーマバージョン 2.0 以降を使用する必要があります。
- Automation タイプのドキュメントは、スキーマバージョン 0.3 を使用する必要があります。
- Session タイプのドキュメントは、スキーマバージョン 1.0 を使用する必要があります。
- JSON あるいは YAML でドキュメントを作成できます。

Session ドキュメントスキーマの詳細については、「セッションドキュメントスキーマ」を参照してください。

Command および Policy ドキュメントで最新バージョンのスキーマを使用することで、次の機能を利用できます。

スキーマバージョン 2.2 ドキュメントの機能

機能	詳細
ドキュメントの編集	ドキュメントは更新可能になりました。バージョン 1.2 では、ドキュメントを更新した場合に別の名前で保存する必要がありました。
バージョンの自動管理	ドキュメントを更新すると新しいバージョンが作成されます。これはスキーマのバージョンではなく、ドキュメントのバージョンです。
デフォルトバージョン	ドキュメントに複数のバージョンがある場合、どのバージョンがデフォルトのドキュメントかを指定できます。
順序付け	ドキュメントのプラグインまたはステップを指定した順序で実行します。
クロスプラットフォームのサポート	クロスプラットフォームをサポートすることで、同じ SSM ドキュメント内で異なるプラグインに異なるオペレーティングシステムを指定できます。クロスプラットフォームのサポートはステップ内の `precondition` パラメータを使用します。

> **Note**
>
> 新しい Systems Manager 機能および SSM ドキュメント機能を使用するには、インスタンスの AWS Systems Manager SSM Agent を常に最新バージョンに更新しておく必要があります。詳細については、「Run Command を使用して SSM Agent を更新する」を参照してください。

次の表はスキーマのメジャーバージョン間の相違点の一覧です。

バージョン 1.2	バージョン 2.2 (最新バージョン)	詳細
runtimeConfig	mainSteps	バージョン 2.2 では、`mainSteps` の代わりに `runtimeConfig` セクションを使用します。`mainSteps` セクションでは、Systems Manager でステップを順番に実行できます。
プロパティ	inputs	バージョン 2.2 では、`inputs` セクションの代わりに `properties` セクションを使用します。`inputs` セクションは、ステップのパラメータを受け入れます。
commands	runCommand	バージョン 2.2 では、`inputs` セクションは `runCommand` パラメータを使用します。`commands` パラメータは使用しません。
id	action	バージョン 2.2 では、`Action` の代わりに `ID` を使用します。これは名前のみの変更です。
該当なし	name	バージョン 2.2 では、`name` はステップの任意のユーザー定義名です。

前提条件パラメータを使用する

スキーマバージョン 2.2 以降では、`precondition` パラメータを使用して、各プラグインのターゲットオペレーティングシステムを指定したり、SSM ドキュメントで定義した入力パラメータを検

証したりすることができます。precondition パラメータは、SSM ドキュメントの入力パラメータと、platformType、Linux、および MacOS の値を使用する Windows の参照をサポートします。StringEquals 演算子のみがサポートされています。

スキーマバージョン 2.2 以降を使用するドキュメントの場合、precondition が指定されていないと、各プラグインはそのプラグインとオペレーティングシステムとの互換性に基づいて実行またはスキップされます。オペレーティングシステムとのプラグインの互換性は、precondition の前に評価されます。スキーマ 2.0 以前を使用するドキュメントの場合は、互換性のないプラグインはエラーをスローします。

例えば、スキーマバージョンが 2.2 のドキュメントで、precondition が指定されておらず aws:runShellScript プラグインが一覧表示されている場合、そのステップは Linux インスタンスで実行されますが、Windows Server インスタンスではシステムによってこれがスキップされます。これは、aws:runShellScript が Windows Server インスタンスと互換性がないためです。しかし、スキーマバージョンが 2.0 のドキュメントでは、aws:runShellScript プラグインを指定して、ドキュメントを Windows Server インスタンスで実行した場合、実行は失敗します。SSM ドキュメントでの前提条件パラメータの例は後でこのセクションで確認できます。

スキーマバージョン 2.2

最上位の要素

以下の例では、スキーマバージョン 2.2 を使用した SSM ドキュメントの最上位要素を示しています。

YAML

```
---
schemaVersion: "2.2"
description: A description of the document.
parameters:
  parameter 1:
    property 1: "value"
    property 2: "value"
  parameter 2:
    property 1: "value"
    property 2: "value"
mainSteps:
  - action: Plugin name
    name: A name for the step.
    inputs:
      input 1: "value"
```

```
      input 2: "value"
      input 3: "{{ parameter 1 }}"
```

JSON

```
{
   "schemaVersion": "2.2",
   "description": "A description of the document.",
   "parameters": {
       "parameter 1": {
          "property 1": "value",
          "property 2": "value"
       },
       "parameter 2":{
          "property 1": "value",
          "property 2": "value"
       }
    },
   "mainSteps": [
      {
         "action": "Plugin name",
         "name": "A name for the step.",
         "inputs": {
            "input 1": "value",
            "input 2": "value",
            "input 3": "{{ parameter 1 }}"
         }
      }
   ]
}
```

スキーマバージョン 2.2 の例

以下の例では、aws:runPowerShellScript プラグインを使用してターゲットインスタンスで PowerShell コマンドを実行しています。

YAML

```
---
schemaVersion: "2.2"
description: "Example document"
parameters:
```

```
  Message:
    type: "String"
    description: "Example parameter"
    default: "Hello World"
    allowedValues:
    - "Hello World"
mainSteps:
  - action: "aws:runPowerShellScript"
    name: "example"
    inputs:
      timeoutSeconds: '60'
      runCommand:
      - "Write-Output {{Message}}"
```

JSON

```
{
   "schemaVersion": "2.2",
   "description": "Example document",
   "parameters": {
      "Message": {
         "type": "String",
         "description": "Example parameter",
         "default": "Hello World",
         "allowedValues": ["Hello World"]
      }
   },
   "mainSteps": [
      {
         "action": "aws:runPowerShellScript",
         "name": "example",
         "inputs": {
            "timeoutSeconds": "60",
            "runCommand": [
               "Write-Output {{Message}}"
            ]
         }
      }
   ]
}
```

スキーマバージョン 2.2 の precondition パラメータ例

スキーマバージョン 2.2 ではクロスプラットフォームのサポートを提供します。つまり、単一の SSM ドキュメント内で異なるプラグインに異なるオペレーティングシステムを指定できます。クロスプラットフォームのサポートは、次の例のようにステップ内で `precondition`パラメータを使用します。`precondition` パラメータは、SSM ドキュメントで定義した入力パラメータの検証にも使用できます。これは、次の例の 2 番目にあります。

YAML

```
---
schemaVersion: '2.2'
description: cross-platform sample
mainSteps:
- action: aws:runPowerShellScript
  name: PatchWindows
  precondition:
    StringEquals:
    - platformType
    - Windows
  inputs:
    runCommand:
    - cmds
- action: aws:runShellScript
  name: PatchLinux
  precondition:
    StringEquals:
    - platformType
    - Linux
  inputs:
    runCommand:
    - cmds
```

JSON

```
{
   "schemaVersion": "2.2",
   "description": "cross-platform sample",
   "mainSteps": [
      {
         "action": "aws:runPowerShellScript",
         "name": "PatchWindows",
         "precondition": {
            "StringEquals": [
```

```
                "platformType",
                "Windows"
            ]
         },
         "inputs": {
            "runCommand": [
               "cmds"
            ]
         }
      },
      {
         "action": "aws:runShellScript",
         "name": "PatchLinux",
         "precondition": {
            "StringEquals": [
               "platformType",
               "Linux"
            ]
         },
         "inputs": {
            "runCommand": [
               "cmds"
            ]
         }
      }
   ]
}
```

YAML

```
---
schemaVersion: '2.2'
parameters:
  action:
    type: String
    allowedValues:
    - Install
    - Uninstall
  confirmed:
    type: String
    allowedValues:
    - True
```

```
    - False
mainSteps:
- action: aws:runShellScript
  name: InstallAwsCLI
  precondition:
    StringEquals:
    - "{{ action }}"
    - "Install"
  inputs:
    runCommand:
    - sudo apt install aws-cli
- action: aws:runShellScript
  name: UninstallAwsCLI
  precondition:
    StringEquals:
    - "{{ action }} {{ confirmed }}"
    - "Uninstall True"
  inputs:
    runCommand:
    - sudo apt remove aws-cli
```

JSON

```
{
   "schemaVersion": "2.2",
   "parameters": {
      "action": {
         "type": "String",
         "allowedValues": [
            "Install",
            "Uninstall"
         ]
      },
      "confirmed": {
         "type": "String",
         "allowedValues": [
            true,
            false
         ]
      }
   },
   "mainSteps": [
      {
```

```
         "action": "aws:runShellScript",
         "name": "InstallAwsCLI",
         "precondition": {
            "StringEquals": [
               "{{ action }}",
               "Install"
            ]
         },
         "inputs": {
            "runCommand": [
               "sudo apt install aws-cli"
            ]
         }
      },
      {
         "action": "aws:runShellScript",
         "name": "UninstallAwsCLI",
         "precondition": {
            "StringEquals": [
               "{{ action }} {{ confirmed }}",
               "Uninstall True"
            ]
         },
         "inputs": {
            "runCommand": [
               "sudo apt remove aws-cli"
            ]
         }
      }
   ]
}
```

スキーマバージョン 2.2 State Manager の例

Systems Manager のツールである State Manager で以下の SSM ドキュメントを使用すると、ClamAV のウイルス対策ソフトウェアをダウンロードしてインストールできます。State Manager によって特定の設定が適用されます。つまり、State Manager 関連付けが実行されるごとに、ClamAV ソフトウェアがインストールされているかが、システムによってチェックされます。インストールされていない場合には、State Manager はこのドキュメントを返します。

YAML

```
---
schemaVersion: '2.2'
description: State Manager Bootstrap Example
parameters: {}
mainSteps:
- action: aws:runShellScript
  name: configureServer
  inputs:
    runCommand:
    - sudo yum install -y httpd24
    - sudo yum --enablerepo=epel install -y clamav
```

JSON

```
{
   "schemaVersion": "2.2",
   "description": "State Manager Bootstrap Example",
   "parameters": {},
   "mainSteps": [
      {
         "action": "aws:runShellScript",
         "name": "configureServer",
         "inputs": {
            "runCommand": [
               "sudo yum install -y httpd24",
               "sudo yum --enablerepo=epel install -y clamav"
            ]
         }
      }
   ]
}
```

スキーマバージョン 2.2 インベントリの例

State Manager で以下の SSM ドキュメントを使用すると、インスタンスに関するインベントリのメタデータを収集できます。

YAML

```
---
```

```
schemaVersion: '2.2'
description: Software Inventory Policy Document.
parameters:
  applications:
    type: String
    default: Enabled
    description: "(Optional) Collect data for installed applications."
    allowedValues:
    - Enabled
    - Disabled
  awsComponents:
    type: String
    default: Enabled
    description: "(Optional) Collect data for AWS Components like amazon-ssm-agent."
    allowedValues:
    - Enabled
    - Disabled
  networkConfig:
    type: String
    default: Enabled
    description: "(Optional) Collect data for Network configurations."
    allowedValues:
    - Enabled
    - Disabled
  windowsUpdates:
    type: String
    default: Enabled
    description: "(Optional) Collect data for all Windows Updates."
    allowedValues:
    - Enabled
    - Disabled
  instanceDetailedInformation:
    type: String
    default: Enabled
    description: "(Optional) Collect additional information about the instance,
 including
      the CPU model, speed, and the number of cores, to name a few."
    allowedValues:
    - Enabled
    - Disabled
  customInventory:
    type: String
    default: Enabled
    description: "(Optional) Collect data for custom inventory."
```

```
    allowedValues:
    - Enabled
    - Disabled
mainSteps:
- action: aws:softwareInventory
  name: collectSoftwareInventoryItems
  inputs:
    applications: "{{ applications }}"
    awsComponents: "{{ awsComponents }}"
    networkConfig: "{{ networkConfig }}"
    windowsUpdates: "{{ windowsUpdates }}"
    instanceDetailedInformation: "{{ instanceDetailedInformation }}"
    customInventory: "{{ customInventory }}"
```

JSON

```
{
   "schemaVersion": "2.2",
   "description": "Software Inventory Policy Document.",
   "parameters": {
      "applications": {
         "type": "String",
         "default": "Enabled",
         "description": "(Optional) Collect data for installed applications.",
         "allowedValues": [
            "Enabled",
            "Disabled"
         ]
      },
      "awsComponents": {
         "type": "String",
         "default": "Enabled",
         "description": "(Optional) Collect data for AWS Components like amazon-ssm-
agent.",
         "allowedValues": [
            "Enabled",
            "Disabled"
         ]
      },
      "networkConfig": {
         "type": "String",
         "default": "Enabled",
         "description": "(Optional) Collect data for Network configurations.",
```

```
         "allowedValues": [
            "Enabled",
            "Disabled"
         ]
      },
      "windowsUpdates": {
         "type": "String",
         "default": "Enabled",
         "description": "(Optional) Collect data for all Windows Updates.",
         "allowedValues": [
            "Enabled",
            "Disabled"
         ]
      },
      "instanceDetailedInformation": {
         "type": "String",
         "default": "Enabled",
         "description": "(Optional) Collect additional information about the
instance, including\nthe CPU model, speed, and the number of cores, to name a
few.",
         "allowedValues": [
            "Enabled",
            "Disabled"
         ]
      },
      "customInventory": {
         "type": "String",
         "default": "Enabled",
         "description": "(Optional) Collect data for custom inventory.",
         "allowedValues": [
            "Enabled",
            "Disabled"
         ]
      }
   },
   "mainSteps": [
      {
         "action": "aws:softwareInventory",
         "name": "collectSoftwareInventoryItems",
         "inputs": {
            "applications": "{{ applications }}",
            "awsComponents": "{{ awsComponents }}",
            "networkConfig": "{{ networkConfig }}",
            "windowsUpdates": "{{ windowsUpdates }}",
```

```
            "instanceDetailedInformation": "{{ instanceDetailedInformation }}",
            "customInventory": "{{ customInventory }}"
         }
      }
   ]
}
```

スキーマバージョン 2.2 **AWS-ConfigureAWSPackage** の例

以下の例は AWS-ConfigureAWSPackage ドキュメントを示しています。mainSteps セクションの aws:configurePackage ステップには action プラグインが含まれています。

> **Note**
>
> Linux オペレーティングシステムでは、AmazonCloudWatchAgent パッケージ、および AWSSupport-EC2Rescue パッケージのみがサポートされています。

YAML

```
---
schemaVersion: '2.2'
description: 'Install or uninstall the latest version or specified version of an AWS
  package. Available packages include the following: AWSPVDriver,
 AwsEnaNetworkDriver,
  AwsVssComponents, and AmazonCloudWatchAgent, and AWSSupport-EC2Rescue.'
parameters:
  action:
    description: "(Required) Specify whether or not to install or uninstall the
 package."
    type: String
    allowedValues:
    - Install
    - Uninstall
  name:
    description: "(Required) The package to install/uninstall."
    type: String
    allowedPattern: "^arn:[a-z0-9][-.a-z0-9]{0,62}:[a-z0-9][-.a-z0-9]{0,62}:([a-
z0-9][-.a-z0-9]{0,62})?:([a-z0-9][-.a-z0-9]{0,62})?:package\\/[a-zA-Z][a-zA-Z0-9\\-
_]{0,39}$|^[a-zA-Z][a-zA-Z0-9\\-_]{0,39}$"
  version:
```

```
    type: String
    description: "(Optional) A specific version of the package to install or
 uninstall."
mainSteps:
- action: aws:configurePackage
  name: configurePackage
  inputs:
    name: "{{ name }}"
    action: "{{ action }}"
    version: "{{ version }}"
```

JSON

```
{
   "schemaVersion": "2.2",
   "description": "Install or uninstall the latest version or specified version
 of an AWS package. Available packages include the following: AWSPVDriver,
 AwsEnaNetworkDriver, AwsVssComponents, and AmazonCloudWatchAgent, and AWSSupport-
EC2Rescue.",
   "parameters": {
      "action": {
         "description":"(Required) Specify whether or not to install or uninstall
 the package.",
         "type":"String",
         "allowedValues":[
            "Install",
            "Uninstall"
         ]
      },
      "name": {
         "description": "(Required) The package to install/uninstall.",
         "type": "String",
         "allowedPattern": "^arn:[a-z0-9][-.a-z0-9]{0,62}:[a-z0-9][-.a-z0-9]{0,62}:
([a-z0-9][-.a-z0-9]{0,62})?:([a-z0-9][-.a-z0-9]{0,62})?:package\\/[a-zA-Z][a-zA-
Z0-9\\-_]{0,39}$|^[a-zA-Z][a-zA-Z0-9\\-_]{0,39}$"
      },
      "version": {
         "type": "String",
         "description": "(Optional) A specific version of the package to install or
 uninstall."
      }
   },
   "mainSteps":[
```

```
      {
         "action": "aws:configurePackage",
         "name": "configurePackage",
         "inputs": {
            "name": "{{ name }}",
            "action": "{{ action }}",
            "version": "{{ version }}"
         }
      }
   ]
}
```

スキーマバージョン 1.2

次の例では、スキーマバージョン 1.2 のドキュメントの最上位要素を示します。

```
{
   "schemaVersion":"1.2",
   "description":"A description of the SSM document.",
   "parameters":{
      "parameter 1":{
         "one or more parameter properties"
      },
      "parameter 2":{
         "one or more parameter properties"
      },
      "parameter 3":{
         "one or more parameter properties"
      }
   },
   "runtimeConfig":{
      "plugin 1":{
         "properties":[
            {
               "one or more plugin properties"
            }
         ]
      }
   }
}
```

スキーマバージョン 1.2 **aws:runShellScript** の例

以下の例は AWS-RunShellScript SSM ドキュメントを示しています。runtimeConfig セクションには aws:runShellScript プラグインが含まれます。

```
{
    "schemaVersion":"1.2",
    "description":"Run a shell script or specify the commands to run.",
    "parameters":{
        "commands":{
            "type":"StringList",
            "description":"(Required) Specify a shell script or a command to run.",
            "minItems":1,
            "displayType":"textarea"
        },
        "workingDirectory":{
            "type":"String",
            "default":"",
            "description":"(Optional) The path to the working directory on your
 instance.",
            "maxChars":4096
        },
        "executionTimeout":{
            "type":"String",
            "default":"3600",
            "description":"(Optional) The time in seconds for a command to complete
 before it is considered to have failed. Default is 3600 (1 hour). Maximum is 172800
 (48 hours).",
            "allowedPattern":"([1-9][0-9]{0,3})|(1[0-9]{1,4})|(2[0-7][0-9]{1,3})|
(28[0-7][0-9]{1,2})|(28800)"
        }
    },
    "runtimeConfig":{
        "aws:runShellScript":{
            "properties":[
                {
                    "id":"0.aws:runShellScript",
                    "runCommand":"{{ commands }}",
                    "workingDirectory":"{{ workingDirectory }}",
                    "timeoutSeconds":"{{ executionTimeout }}"
                }
            ]
        }
    }
}
```

スキーマバージョン 0.3

最上位の要素

次の例では、スキーマバージョン 0.3 の Automation ランブックの最上位要素を JSON 形式で示します。

```
{
    "description": "document-description",
    "schemaVersion": "0.3",
    "assumeRole": "{{assumeRole}}",
    "parameters": {
        "parameter1": {
            "type": "String",
            "description": "parameter-1-description",
            "default": ""
        },
        "parameter2": {
            "type": "String",
            "description": "parameter-2-description",
            "default": ""
        }
    },
    "variables": {
        "variable1": {
            "type": "StringMap",
            "description": "variable-1-description",
            "default": {}
        },
        "variable2": {
            "type": "String",
            "description": "variable-2-description",
            "default": "default-value"
        }
    },
    "mainSteps": [
        {
            "name": "myStepName",
            "action": "action-name",
            "maxAttempts": 1,
            "inputs": {
                "Handler": "python-only-handler-name",
                "Runtime": "runtime-name",
                "Attachment": "script-or-zip-name"
```

```
            },
            "outputs": {
                "Name": "output-name",
                "Selector": "selector.value",
                "Type": "data-type"
            }
        }
    ],
    "files": {
        "script-or-zip-name": {
            "checksums": {
                "sha256": "checksum"
            },
            "size": 1234
        }
    }
}
```

YAML Automation ランブックの例

次の例では、Automation ランブックの内容を YAML 形式で示します。このバージョン 0.3 のドキュメントスキーマの実例では、Markdown を使用してドキュメントの説明をフォーマットする方法も示しています。

```
description: >-
  ##Title: LaunchInstanceAndCheckState

  -----

  **Purpose**: This Automation runbook first launches an EC2 instance
  using the AMI ID provided in the parameter ```imageId```. The second step of
  this document continuously checks the instance status check value for the
  launched instance until the status ```ok``` is returned.


  ##Parameters:

  -----

  Name | Type | Description | Default Value

  ------------- | ------------- | ------------- | -------------
```

```
  assumeRole | String | (Optional) The ARN of the role that allows Automation to
  perform the actions on your behalf. | -

  imageId  | String | (Optional) The AMI ID to use for launching the instance.
  The default value uses the latest Amazon Linux AMI ID available. | {{
  ssm:/aws/service/ami-amazon-linux-latest/amzn-ami-hvm-x86_64-gp2 }}
schemaVersion: '0.3'
assumeRole: 'arn:aws:iam::111122223333::role/AutomationServiceRole'
parameters:
  imageId:
    type: String
    default: '{{ ssm:/aws/service/ami-amazon-linux-latest/amzn-ami-hvm-x86_64-gp2 }}'
    description: >-
      (Optional) The AMI ID to use for launching the instance. The default value
      uses the latest released Amazon Linux AMI ID.
  tagValue:
    type: String
    default: ' LaunchedBySsmAutomation'
    description: >-
      (Optional) The tag value to add to the instance. The default value is
      LaunchedBySsmAutomation.
  instanceType:
    type: String
    default: t2.micro
    description: >-
      (Optional) The instance type to use for the instance. The default value is
      t2.micro.
mainSteps:
  - name: LaunchEc2Instance
    action: 'aws:executeScript'
    outputs:
      - Name: payload
        Selector: $.Payload
        Type: StringMap
    inputs:
      Runtime: python3.8
      Handler: launch_instance
      Script: ''
      InputPayload:
        image_id: '{{ imageId }}'
        tag_value: '{{ tagValue }}'
        instance_type: '{{ instanceType }}'
      Attachment: launch.py
    description: >-
```

```
    **About This Step**


    This step first launches an EC2 instance using the ```aws:executeScript```
    action and the provided python script.
- name: WaitForInstanceStatusOk
  action: 'aws:executeScript'
  inputs:
    Runtime: python3.8
    Handler: poll_instance
    Script: |-
      def poll_instance(events, context):
        import boto3
        import time

        ec2 = boto3.client('ec2')

        instance_id = events['InstanceId']

        print('[INFO] Waiting for instance status check to report ok', instance_id)

        instance_status = "null"

        while True:
          res = ec2.describe_instance_status(InstanceIds=[instance_id])

          if len(res['InstanceStatuses']) == 0:
            print("Instance status information is not available yet")
            time.sleep(5)
            continue

          instance_status = res['InstanceStatuses'][0]['InstanceStatus']['Status']

          print('[INFO] Polling to get status of the instance', instance_status)

          if instance_status == 'ok':
            break

          time.sleep(10)

        return {'Status': instance_status, 'InstanceId': instance_id}
    InputPayload: '{{ LaunchEc2Instance.payload }}'
  description: >-
    **About This Step**
```

```
      The python script continuously polls the instance status check value for
      the instance launched in Step 1 until the ```ok``` status is returned.
files:
  launch.py:
    checksums:
      sha256: 18871b1311b295c43d0f...[truncated]...772da97b67e99d84d342ef4aEXAMPLE
```

データ要素とパラメータ

このトピックでは、SSM ドキュメントで使用されるデータ要素について説明します。ドキュメントの作成に使用されるスキーマのバージョンは、ドキュメントで使用できる構文とデータ要素を定義します。コマンドドキュメントには、スキーマバージョン 2.2 以降を使用することをお勧めします。Automation ランブックはスキーマバージョン 0.3 を使用します。さらに、Automation ランブックでは、マークアップ言語である Markdown の使用がサポートされています。これにより、wiki スタイルの説明をドキュメントやドキュメント内の個々のステップに追加できます。Markdown の使用に関する詳細については、「AWS Management Console 入門ガイド」の「コンソールでの Markdown の使用」を参照してください。

次のセクションでは、SSM ドキュメントに含めることができるデータ要素について説明します。

最上位のデータ要素

schemaVersion

使用するスキーマバージョン。

型: バージョン

必須: はい

description

ドキュメントの目的を説明するために提供する情報。またこのフィールドを使用して、ドキュメントの実行にパラメータの値が必要か否か、またはパラメータの値の指定が任意か否かを指定することもできます。必須と任意のパラメータはこのトピックのサンプルをご参照ください。

タイプ: 文字列

必須: いいえ

パラメータ

ドキュメントが許可するパラメータを定義する構造。

頻繁に使用するパラメータの場合は、そのパラメータを AWS Systems Manager のツールである Parameter Store に保存することをお勧めします。次に、デフォルト値として Parameter Store パラメータを参照するパラメータをドキュメントで定義できます。Parameter Store パラメータを参照するには、次の構文を使用します。

```
{{ssm:parameter-name}}
```

他のドキュメントパラメータと同じ方法で、Parameter Store パラメータを参照するパラメータを使用できます。次の例では、commands パラメータのデフォルト値は Parameter Store パラメータ myShellCommands です。commands パラメータを runCommand 文字列として指定すると、ドキュメントは myShellCommands パラメータに格納されているコマンドを実行します。

YAML

```
---
schemaVersion: '2.2'
description: runShellScript with command strings stored as Parameter Store
 parameter
parameters:
  commands:
    type: StringList
    description: "(Required) The commands to run on the instance."
    default: ["{{ ssm:myShellCommands }}"]
mainSteps:
- action: aws:runShellScript
  name: runShellScriptDefaultParams
  inputs:
    runCommand:"{{ commands }}"
```

JSON

```
{
    "schemaVersion": "2.2",
    "description": "runShellScript with command strings stored as Parameter Store
 parameter",
    "parameters": {
      "commands": {
```

```
        "type": "StringList",
        "description": "(Required) The commands to run on the instance.",
        "default": ["{{ ssm:myShellCommands }}"]
      }
    },
    "mainSteps": [
      {
        "action": "aws:runShellScript",
        "name": "runShellScriptDefaultParams",
        "inputs": {
            "runCommand": [
              "{{ commands }}"
          ]
        }
      }
    ]
  }
```

> **Note**
>
> String および StringList Parameter Store パラメータは、ドキュメントの parameters セクションで参照できます。SecureString Parameter Store パラメータは参照できません。

Parameter Store の詳細については、「AWS Systems Manager Parameter Store」を参照してください。

型: 構造

parameters構造は次のフィールドと値を受け入れます。

- type: (必須) その値として String、StringList、Integer、Boolean、MapList、StringMap を使用できます。各タイプの例を表示するには、次のセクションの「SSM ドキュメントパラメータ type の例」を参照してください。

  > **Note**
  >
  > コマンドタイプのドキュメントでは、String および StringList パラメータタイプのみがサポートされます。

- `description`: (オプション) パラメータグループの説明。
- `default`: (オプション) Parameter Store でのパラメータのデフォルト値またはパラメータへの参照。
- `allowedValues`: (オプション) パラメータに使用できる値の配列。パラメータに使用できる値を定義すると、ユーザー入力が検証されます。使用できない値をユーザーが入力すると、実行の開始に失敗します。

  YAML

  ```
  DirectoryType:
    type: String
    description: "(Required) The directory type to launch."
    default: AwsMad
    allowedValues:
    - AdConnector
    - AwsMad
    - SimpleAd
  ```

  JSON

  ```
  "DirectoryType": {
    "type": "String",
    "description": "(Required) The directory type to launch.",
    "default": "AwsMad",
    "allowedValues": [
      "AdConnector",
      "AwsMad",
      "SimpleAd"
    ]
  }
  ```

- `allowedPattern`: (オプション) ユーザー入力がパラメータに対して定義されたパターンと一致するかどうかを検証する正規表現。ユーザー入力が使用できるパターンと一致しない場合、実行は開始されません。

  > **Note**
  >
  > Systems Manager は、`allowedPattern` について 2 つの検証を実行します。1 つ目の検証は、ドキュメントを使用するときに API レベルで Java 正規表現ライブラリを使用

して実行されます。2 つ目の検証は、ドキュメントを処理する前に GO regexp ライブラリを使用して SSM Agent に対して実行されます。

YAML

```
InstanceId:
  type: String
  description: "(Required) The instance ID to target."
  allowedPattern: "^i-[a-z0-9]{8,17}$"
  default: ''
```

JSON

```
"InstanceId": {
  "type": "String",
  "description": "(Required) The instance ID to target.",
  "allowedPattern": "^i-[a-z0-9]{8,17}$",
  "default": ""
}
```

- displayType: (オプション) textfield の textarea または AWS Management Console のいずれかを表示するために使用されます。textfield は、1 行のテキストボックスで、textarea は、複数行のテキストエリアです。
- minItems: (オプション) 許可される項目の最小数。
- maxItems: (オプション) 許可される項目の最大数。
- minChars: (オプション) 許可される項目の最小数。
- maxChars: (オプション) を許可されているパラメータ文字の最大数。

必須: いいえ

variables

(スキーマバージョン 0.3 のみ) 自動化ランブックのステップ全体で参照または更新できる値。変数はパラメーターと似ていますが、非常に重要な点において異なります。パラメーター値はランブックのコンテキストでは静的ですが、変数の値はランブックのコンテキストでは変更できます。変数の値を更新する場合、データ型は定義されたデータ型と一致する必要があります。オートメーションの変数値の更新に関する詳細は、「aws:updateVariable — ランブック変数の値を更新します。」を参照してください。

型: ブール値 | 整数 | マップリスト | 文字列 | 文字列リスト | 文字列マップ

必須: いいえ

YAML

```
variables:
    payload:
        type: StringMap
        default: "{}"
```

JSON

```
{
    "variables": [
        "payload": {
            "type": "StringMap",
            "default": "{}"
        }
    ]
}
```

runtimeConfig

(スキーマバージョン 1.2 のみ) 1 つ以上の Systems Manager プラグインによって適用されるインスタンスの構成。プラグインは必ずしも順番に実行されるとは限りません。

型: Dictionary<string,PluginConfiguration>

必須: いいえ

mainSteps

(スキーマバージョン 0.3、2.0、および 2.2 のみ) 複数のステップ (プラグイン) を含むことができるオブジェクト。プラグインはステップ内で定義されます。ステップは、ドキュメントに記載されている順番に実行されます。

型: Dictionary<string,PluginConfiguration>

必須: はい

出力

(スキーマバージョン 0.3 のみ) このドキュメントの実行によって生成され、他のプロセスで使用できるデータ。例えば、ドキュメントで新しい AMI を作成する場合、出力値として

「CreateImage.ImageId」を指定すると、この出力を使用して後続のオートメーションの実行から新しいインスタンスを作成できます。出力の詳細については、「アクション出力の入力としての使用」を参照してください。

型: Dictionary<string,OutputConfiguration>

必須: いいえ

files

(スキーマバージョン 0.3 のみ) ドキュメントに添付され、自動実行時に実行されるスクリプトファイル (およびそのチェックサム)。aws:executeScript アクションを含むドキュメントのうち、添付ファイルが 1 つ以上のステップに指定されているもののみに適用されます。

オートメーションランブックでサポートされているランタイムについては、「aws:executeScript – スクリプトを実行する」を参照してください。Automation ランブックにスクリプトを含める方法の詳細については、「ランブックでのスクリプトの使用」および「オートメーションランブックのビジュアルデザインエクスペリエンス」を参照してください。

アタッチメントの付いたオートメーションランブックを作成するときは、--attachments オプション (AWS CLI の場合) または Attachments (API および SDK の場合) を使用して添付ファイルを指定する必要があります。SSM ドキュメントと、Amazon Simple Storage Service (Amazon S3) バケット内に保存されているファイルの両方で、ファイルの場所を指定できます。詳細については、「AWS Systems Manager API リファレンス」の「Attachments」(アタッチメント) を参照してください。

YAML

```
---
files:
  launch.py:
    checksums:
      sha256: 18871b1311b295c43d0f...
[truncated]...772da97b67e99d84d342ef4aEXAMPLE
```

JSON

```
"files": {
    "launch.py": {
        "checksums": {
            "sha256": "18871b1311b295c43d0f...
[truncated]...772da97b67e99d84d342ef4aEXAMPLE"
```

```
        }
    }
}
```

型: Dictionary<string,FilesConfiguration>

必須: いいえ

SSM ドキュメントパラメータ **type** の例

SSM ドキュメント内のパラメータのデータ型は静的です。つまり、パラメータのデータ型は定義後に変更することはできません。SSM ドキュメントプラグインでパラメータを使用する場合、パラメータのデータ型をプラグインの入力内で動的に変更することはできません。例えば、Integer プラグインの runCommand 入力内の aws:runShellScript パラメータを参照することはできません。この入力は文字列または文字列のリストを受け入れるためです。プラグインの入力にパラメータを使用するには、パラメータのデータ型が、入力の受け入れ可能なデータ型と一致している必要があります。例えば、Boolean プラグインの allowDowngrade 入力には aws:updateSsmAgent 型のパラメータを指定する必要があります。パラメータのデータ型がプラグインの入力のデータ型と一致しない場合、SSM ドキュメントの検証は失敗となり、システムによってドキュメントは作成されません。これは、他のプラグイン、もしくは AWS Systems Manager のオートメーションアクション用に、入力内にある下流のパラメータを使用する場合にも当てはまります。例えば、aws:runDocument プラグインの documentParameters 入力にある StringList パラメータを参照することはできません。ダウンストリーム SSM ドキュメントパラメータのタイプが StringList パラメータで、かつ参照しようとしているパラメータと一致する場合でも、documentParameters 入力は、文字列へのマッピングを受け入れます。

オートメーションアクションでパラメータを使用するときは、ほとんどの場合、SSM ドキュメントを作成するときにパラメータのデータ型は検証されません。aws:runCommand アクションを使用する場合にのみ、SSM ドキュメントを作成するときにパラメータのデータ型が検証されます。それ以外の場合、オートメーションの実行中、アクションが実行される前にその入力が検証されるときに、パラメータが検証されます。例えば、入力パラメータが String であり、それを MaxInstanceCount アクションの aws:runInstances 入力の値として参照する場合は、SSM ドキュメントが作成されます。ただし、ドキュメントを実行すると、aws:runInstances アクションの検証中にオートメーションは失敗します。MaxInstanceCount 入力に Integer が必要なためです。

以下に示しているのは、各パラメータ type の例です。

文字列

引用符で囲んだ 0 個以上の Unicode 文字のシーケンス。例えば、"i-1234567890abcdef0" など。バックスラッシュを使用して エスケープします。

YAML

```
---
InstanceId:
  type: String
  description: "(Optional) The target EC2 instance ID."
```

JSON

```
"InstanceId":{
  "type":"String",
  "description":"(Optional) The target EC2 instance ID."
}
```

StringList

カンマ区切りの文字列項目のリスト。例えば、["cd ~", "pwd"] など。

YAML

```
---
commands:
  type: StringList
  description: "(Required) Specify a shell script or a command to run."
  default: ""
  minItems: 1
  displayType: textarea
```

JSON

```
"commands":{
  "type":"StringList",
  "description":"(Required) Specify a shell script or a command to run.",
  "minItems":1,
  "displayType":"textarea"
}
```

Boolean

true または false のみを使用できます。"true" または 0 は使用できません。

YAML

```
---
canRun:
  type: Boolean
  description: ''
  default: true
```

JSON

```
"canRun": {
  "type": "Boolean",
  "description": "",
  "default": true
}
```

整数

整数。小数 (3.14159 など) や引用符で囲んだ数字 ("3" など) は使用できません。

YAML

```
---
timeout:
  type: Integer
  description: The type of action to perform.
  default: 100
```

JSON

```
"timeout": {
  "type": "Integer",
  "description": "The type of action to perform.",
  "default": 100
}
```

StringMap

キーと値のマッピング。キーと値は文字列でなければなりません。例えば、{"Env": "Prod"} など。

YAML

```
---
notificationConfig:
  type: StringMap
  description: The configuration for events to be notified about
  default:
    NotificationType: 'Command'
    NotificationEvents:
    - 'Failed'
    NotificationArn: "$dependency.topicArn"
  maxChars: 150
```

JSON

```
"notificationConfig" : {
  "type" : "StringMap",
  "description" : "The configuration for events to be notified about",
  "default" : {
    "NotificationType" : "Command",
    "NotificationEvents" : ["Failed"],
    "NotificationArn" : "$dependency.topicArn"
  },
  "maxChars" : 150
}
```

MapList

StringMap オブジェクトのリスト。

YAML

```
blockDeviceMappings:
  type: MapList
  description: The mappings for the create image inputs
  default:
  - DeviceName: "/dev/sda1"
    Ebs:
      VolumeSize: "50"
  - DeviceName: "/dev/sdm"
    Ebs:
      VolumeSize: "100"
  maxItems: 2
```

JSON

```
"blockDeviceMappings":{
  "type":"MapList",
  "description":"The mappings for the create image inputs",
  "default":[
    {
      "DeviceName":"/dev/sda1",
      "Ebs":{
        "VolumeSize":"50"
      }
    },
    {
      "DeviceName":"/dev/sdm",
      "Ebs":{
        "VolumeSize":"100"
      }
    }
  ],
  "maxItems":2
}
```

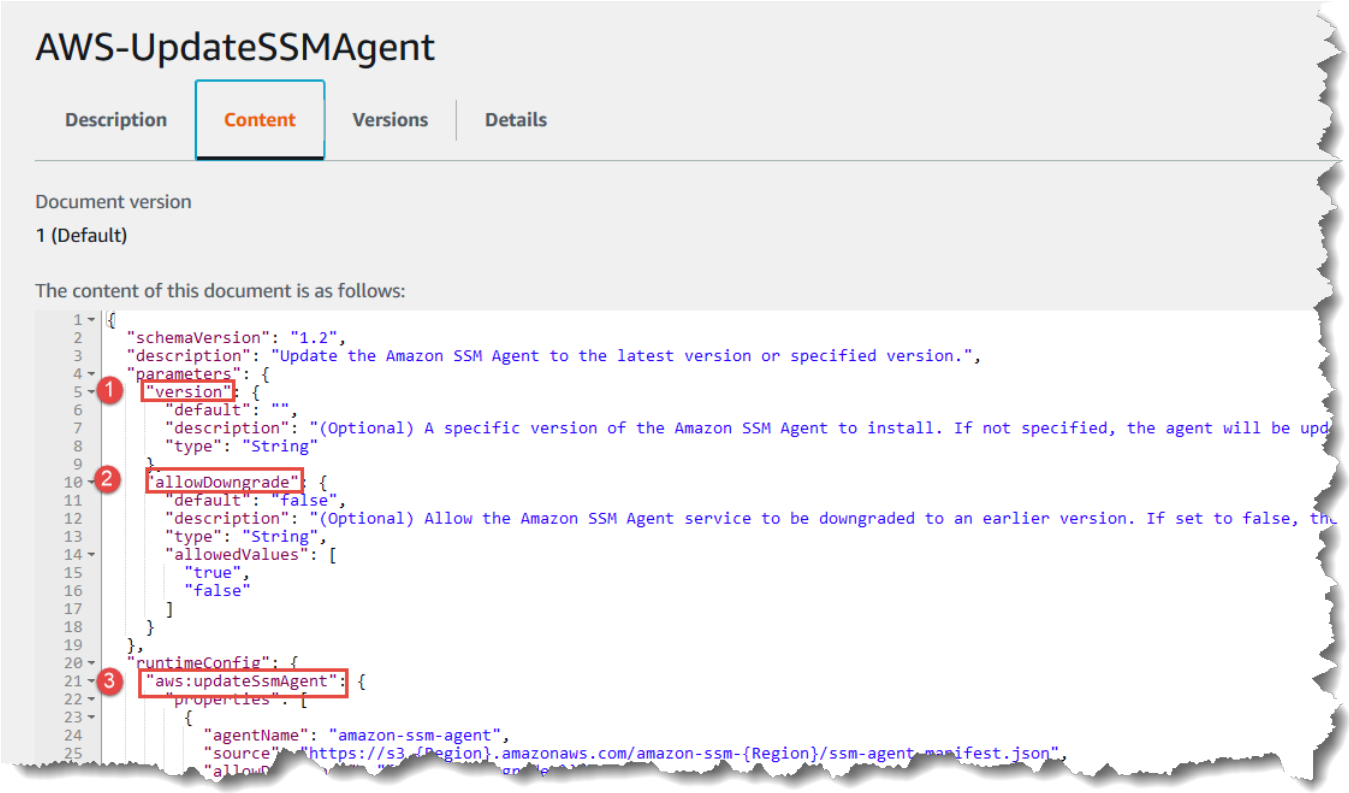
SSM コマンドドキュメントの内容の表示

AWS Systems Manager (SSM) コマンドドキュメントの必須パラメータとオプションのパラメータ、およびドキュメントが実行するアクションをプレビューするには、Systems Manager コンソールでドキュメントのコンテンツを表示できます。

SSM コマンドドキュメントの内容を表示するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[ドキュメント] を選択します。
3. 検索ボックスで、[ドキュメントのタイプ] を選択し、[コマンド] を選択します。
4. ドキュメントの名前を選択し、[コンテンツ] タブをクリックします。
5. [コンテンツ] フィールドで、ドキュメントで使用できるパラメータとアクションステップを確認します。

例えば、次の図は、(1) `version` と (2) `allowDowngrade` が `AWS-UpdateSSMAgent` ドキュメントのオプションのパラメータで、ドキュメントによって実行される最初のアクションが (3) `aws:updateSsmAgent` であることを示しています。



コマンドドキュメントプラグインリファレンス

このリファレンスでは、AWS Systems Manager (SSM) コマンドドキュメントで指定できるプラグインが説明されています。これらのプラグインは、オートメーションアクションを使用する SSM オートメーションランブックでは使用できません。AWS Systems Manager Automation アクションについては、「Systems Manager Automation アクションのリファレンス」を参照してください。

Systems Manager は、SSM ドキュメントの内容を読み取ることによって、マネージドインスタンスで実行するアクションを判別します。各ドキュメントにはコード実行セクションが含まれています。ドキュメントのスキーマバージョンに応じて、このコード実行セクションには 1 つ以上のプラグインまたはステップが含まれます。このヘルプトピックの目的上、プラグインとステップはプラグインと呼んでいます。このセクションには、各 Systems Manager プラグインに関して説明します。ドキュメントの作成に関する情報やスキーマのバージョンの違いなど、ドキュメントの詳細については、「AWS Systems Manager ドキュメント」を参照してください。

> **Note**
>
> ここで説明するプラグインの中には、Windows Server インスタンスまたは Linux インスタンスのいずれかでのみ実行されるものがあります。各プラグインにはプラットフォームの依存関係が記載されています。
> macOS 向けの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスでは、以下のドキュメントプラグインがサポートされています。
>
> - `aws:refreshAssociation`
> - `aws:runShellScript`
> - `aws:runPowerShellScript`
> - `aws:softwareInventory`
> - `aws:updateSsmAgent`

目次

- 共有入力
- aws:applications
- aws:cloudWatch
- aws:configureDocker
- aws:configurePackage
- aws:domainJoin
- aws:downloadContent
- aws:psModule
- aws:refreshAssociation
- aws:runDockerAction
- aws:runDocument
- aws:runPowerShellScript
- aws:runShellScript
- aws:softwareInventory
- aws:updateAgent
- aws:updateSsmAgent

共有入力

あらゆるプラグインが以下の入力を使用できるのは、SSM Agent バージョン 3.0.502 以降のみです。

finallyStep

ドキュメントに実行させる最後のステップです。この入力がステップに定義されている場合、exit または onFailure 入力で指定されている onSuccess 値よりもこれが優先されます。この入力が定義されたステップを期待どおりに実行するには、このステップをドキュメントの mainSteps で定義されている最後のステップにする必要があります。

タイプ: ブール値

有効な値: true | false

必須: いいえ

onFailure

exit 値を使用するプラグインにこの入力を指定して、ステップが失敗した場合は、ステップのステータスにこの障害が反映され、finallyStep が定義されない限り、ドキュメントは残りのステップを実行しません。successAndExit 値を使用するプラグインにこの入力を値で指定して、ステップが失敗した場合は、ステップのステータスが成功になり、finallyStep が定義されない限り、ドキュメントは残りのステップを実行しません。

型: 文字列

有効な値: exit | successAndExit

必須: いいえ

onSuccess

プラグインにこの入力を指定し、ステップが正常に実行した場合、finallyStep が定義されている場合を除き、ドキュメントは残りのステップを実行しません。

型: 文字列

有効な値: exit

必須: いいえ

YAML

```
---
schemaVersion: '2.2'
description: Shared inputs example
parameters:
  customDocumentParameter:
    type: String
    description: Example parameter for a custom Command-type document.
mainSteps:
- action: aws:runDocument
  name: runCustomConfiguration
  inputs:
    documentType: SSMDocument
    documentPath: "yourCustomDocument"
    documentParameters: '"documentParameter":{{customDocumentParameter}}'
    onSuccess: exit
- action: aws:runDocument
  name: ifConfigurationFailure
  inputs:
    documentType: SSMDocument
    documentPath: "yourCustomRepairDocument"
    onFailure: exit
- action: aws:runDocument
  name: finalConfiguration
  inputs:
    documentType: SSMDocument
    documentPath: "yourCustomFinalDocument"
    finallyStep: true
```

JSON

```
{
   "schemaVersion": "2.2",
   "description": "Shared inputs example",
   "parameters": {
      "customDocumentParameter": {
         "type": "String",
         "description": "Example parameter for a custom Command-type document."
      }
   },
   "mainSteps":[
      {
```

```
         "action": "aws:runDocument",
         "name": "runCustomConfiguration",
         "inputs": {
            "documentType": "SSMDocument",
            "documentPath": "yourCustomDocument",
            "documentParameters": "\"documentParameter\":
{{customDocumentParameter}}",
            "onSuccess": "exit"
         }
      },
      {
         "action": "aws:runDocument",
         "name": "ifConfigurationFailure",
         "inputs": {
            "documentType": "SSMDocument",
            "documentPath": "yourCustomRepairDocument",
            "onFailure": "exit"
         }
      },
      {
         "action": "aws:runDocument",
         "name":"finalConfiguration",
         "inputs": {
            "documentType": "SSMDocument",
            "documentPath": "yourCustomFinalDocument",
            "finallyStep": true
         }
      }
   ]
}
```

aws:applications

EC2 インスタンスでアプリケーションをインストール、修復、またはアンインストールします。このプラグインは、Windows Server オペレーティングシステムでのみ実行されます。

構文

スキーマ 2.2

YAML

```
---
```

```
schemaVersion: '2.2'
description: aws:applications plugin
parameters:
  source:
    description: "(Required) Source of msi."
    type: String
mainSteps:
- action: aws:applications
  name: example
  inputs:
    action: Install
    source: "{{ source }}"
```

JSON

```
{
  "schemaVersion":"2.2",
  "description":"aws:applications",
  "parameters":{
    "source":{
    "description":"(Required) Source of msi.",
    "type":"String"
    }
  },
  "mainSteps":[
    {
      "action":"aws:applications",
      "name":"example",
      "inputs":{
        "action":"Install",
        "source":"{{ source }}"
      }
    }
  ]
}
```

スキーマ 1.2

YAML

```
---
runtimeConfig:
```

```
  aws:applications:
    properties:
    - id: 0.aws:applications
      action: "{{ action }}"
      parameters: "{{ parameters }}"
      source: "{{ source }}"
      sourceHash: "{{ sourceHash }}"
```

JSON

```
{
   "runtimeConfig":{
      "aws:applications":{
         "properties":[
            {
               "id":"0.aws:applications",
               "action":"{{ action }}",
               "parameters":"{{ parameters }}",
               "source":"{{ source }}",
               "sourceHash":"{{ sourceHash }}"
            }
         ]
      }
   }
}
```

プロパティ

アクション

取るべきアクション。

タイプ: Enum

有効な値: `Install` | `Repair` | `Uninstall`

必須: はい

パラメータ

インストーラのパラメータ。

型: 文字列

必須: いいえ

source

アプリケーションの .msi ファイルの URL。

型: 文字列

必須: はい

sourceHash

.msi ファイルの SHA256 ハッシュ。

型: 文字列

必須: いいえ

aws:cloudWatch

Windows Server から Amazon CloudWatch または Amazon CloudWatch Logs にデータをエクスポートし、CloudWatch メトリクスを使用してデータをモニタリングします。このプラグインは、Windows Server オペレーティングシステムでのみ実行されます。Amazon Elastic Compute Cloud (Amazon EC2) との CloudWatch 統合の設定の詳細については、「Amazon CloudWatch ユーザーガイド」の「CloudWatch エージェントを使用したメトリクス、ログ、トレースの収集」を参照してください。

> **Important**
>
> CloudWatch の統合エージェントによって、ログデータを Amazon CloudWatch Logs に送信するためのツールとして SSM Agent が置き換えられました。SSM Agent aws:cloudWatch プラグインはサポートされていません。ログ収集プロセスには、統合された CloudWatch エージェントのみを使用することをお勧めします。詳細については、以下の各トピックを参照してください。
>
> - 統合された CloudWatch Logs へのノードログの送信 (CloudWatch エージェント)
> - Windows Server ノードのログ収集を CloudWatch エージェントに移行する
> - 「Amazon CloudWatch ユーザーガイド」の「CloudWatch エージェントを使用してメトリクス、ログ、トレースを収集する」。

次のデータ型をエクスポートおよび監視できます。

ApplicationEventLog

アプリケーションイベントログデータを CloudWatch Logs に送信します。

CustomLogs

テキストベースのログファイルを Amazon CloudWatch Logs に送信します。CloudWatch プラグインは、ログファイルのフィンガープリントを作成します。次に、システムは各フィンガープリントにデータオフセットを関連付けます。プラグインは、変更があったときにファイルをアップロードし、オフセットを記録し、オフセットをフィンガープリントに関連付けます。この方法は、ユーザーがプラグインを有効にし、多数のファイルを含むディレクトリにサービスを関連付け、システムがすべてのファイルをアップロードすることを避けるために使用されます。

> **Warning**
>
> アプリケーションがポーリング中にログをトランケートまたは消去しようとすると、`LogDirectoryPath` で指定されたログではエントリが失われることに注意してください。たとえば、ログファイルのサイズを制限する場合は、その制限に達すると新しいログファイルを作成し、新しいファイルにデータを書き続ける必要があります。

ETW

Windows のイベントトレース (ETW) データを CloudWatch Logs に送信します。

IIS

IIS ログデータを CloudWatch Logs に送信します。

PerformanceCounter

Windows パフォーマンスカウンターを CloudWatch に送信します。メトリクスとして CloudWatch にアップロードするさまざまなカテゴリを選択できます。アップロードするパフォーマンスカウンタごとに、一意の ID (たとえば、「PerformanceCounter2」、「PerformanceCounter3」など) を持つ[PerformanceCounter] セクションを作成し、そのプロパティを設定します。

> **Note**
>
> AWS Systems Manager SSM Agent または CloudWatch プラグインが停止した場合、パフォーマンスカウンターのデータは、CloudWatch に ログ記録されません。この動作

は、カスタムログまたは Windows イベントログとは異なります。SSM Agent または CloudWatch プラグインを使用できる場合、カスタムログと Windows イベントログはパフォーマンスカウンタデータを保持し、CloudWatch にアップロードします。

SecurityEventLog

セキュリティイベントログデータを CloudWatch Logs に送信します。

SystemEventLog

システムイベントログデータを CloudWatch Logs に送信します。

データの送信先として以下を定義できます。

CloudWatch

パフォーマンスカウンターのメトリクスデータの送信先。同じデータを別の場所に送信するには、一意の ID (例: 「CloudWatch2」、「CloudWatch3」) を使用してセクションを追加し、新しい ID ごとに異なるリージョンを指定します。

CloudWatchLogs

ログデータの送信先。一意の ID (例: 「CloudWatchLogs2」、「CloudWatchLogs3」) を含むセクションを追加し、新しい ID ごとに異なるリージョンを指定して、同じデータを別の場所に送信できます。

構文

```
"runtimeConfig":{
        "aws:cloudWatch":{
            "settings":{
                "startType":"{{ status }}"
            },
            "properties":"{{ properties }}"
        }
    }
```

設定とプロパティ

AccessKey

お客様のアクセスキー ID。IAM ロールを使用してインスタンスを起動しない限り、このプロパティは必須です。このプロパティは SSM では使用できません。

型: 文字列

必須: いいえ

CategoryName

パフォーマンスモニターのパフォーマンスカウンタカテゴリ。

型: 文字列

必須: はい

CounterName

パフォーマンスモニターのパフォーマンスカウンターの名前。

型: 文字列

必須: はい

CultureName

タイムスタンプが記録されるロケール。CultureName を空白にした場合は、Windows Server インスタンスで使用されているものと同じロケールになります。

型: 文字列

有効な値: サポートされている値のリストについては、Microsoft ウェブサイトの「National Language Support (NLS)」を参照してください。div、div-MV、hu、および hu-HU の値はサポートされません。

必須: いいえ

DimensionName

Amazon CloudWatch メトリクスのディメンション。`DimensionName` を指定する場合は、`DimensionValue` を指定する必要があります。これらのパラメータにより、メトリクスが一覧表示される別のビューが表示されます。複数のメトリクスに同じディメンションを使用して、特定のディメンションに属するすべてのメトリクスを表示することができます。

型: 文字列

必須: いいえ

DimensionValue

Amazon CloudWatch メトリクスのディメンション値。

型: 文字列

必須: いいえ

エンコード

使用するファイルエンコード (たとえば、UTF-8)。表示名ではなく、エンコード名を使用します。

タイプ: 文字列

有効な値: サポートされる値の一覧については、Microsoft Learn Library の「Encoding クラス」を参照してください。

必須: はい

フィルタ

ログ名のプレフィックス。すべてのファイルをモニタリングするには、このパラメータを空白のままにします。

型: 文字列

有効な値: サポートされる値の一覧については、MSDN ライブラリの「FileSystemWatcherFilter プロパティ」を参照してください。

必須: いいえ

フロー

アップロードする各データタイプ、およびデータの送信先 (CloudWatch または CloudWatch Logs)。例えば、["Id": "PerformanceCounter"] で定義されたパフォーマンスカウンタを CloudWatch に送信するには、"Id": "CloudWatch" で定義された送信先、["PerformanceCounter,CloudWatch"] を入力します。同様に、カスタムログ、ETW ログ、システムログを "Id": "ETW" で定義された CloudWatch Logs の送信先に送信するには、「"(ETW),CloudWatchLogs"」と入力します。加えて、同じパフォーマンスカウンターまたはログファイルを複数の宛先に送信することもできます。たとえば、アプリケーションログを "Id":

"CloudWatchLogs" と "Id": "CloudWatchLogs2" で定義した 2 つの異なる宛先に送信するには、「"ApplicationEventLog,(CloudWatchLogs, CloudWatchLogs2)"」と入力します。

型: 文字列

有効な値 (ソース): ApplicationEventLog | CustomLogs | ETW | PerformanceCounter | SystemEventLog | SecurityEventLog

有効な値 (送信先): CloudWatch | CloudWatchLogs | CloudWatch*n* | CloudWatchLogs*n*

必須: はい

FullName

コンポーネントのフルネーム。

型: 文字列

必須: はい

ID

データソースまたは送信先を識別します。この識別子は、設定ファイル内で一意である必要があります。

型: 文字列

必須: はい

InstanceName

パフォーマンスカウンターインスタンスの名前。各パフォーマンスカウンターコンポーネントではメトリクスが 1 つしかサポートされないため、アスタリスク (*) を使用してすべてのインスタンスを指定しないでください。ただし、_Total は使用できます。

型: 文字列

必須: はい

レベル

Amazon CloudWatch に送信するメッセージのタイプ。

型: 文字列

有効な値:

- 1 - エラーメッセージだけがアップロードされます。
- 2 - 警告メッセージだけがアップロードされます。
- 4 - 情報メッセージだけがアップロードされます。

値を加算すると、複数の種類のメッセージを含めることができます。たとえば、3 はエラーメッセージ (1) と警告メッセージ (2) が含まれることを意味します。7 の値は、エラーメッセージ (1)、警告メッセージ (2)、情報メッセージ (4) が含まれることを意味します。

必須: はい

> **Note**
>
> Windows セキュリティログではレベルを 7 に設定する必要があります。

LineCount

ログファイルを識別するヘッダーの行数。たとえば、IIS のログファイルのヘッダーはほぼ同じです。「3」と入力すると、ログファイルのヘッダーの最初の 3 行が読み取られ、ログファイルを識別できます。IIS のログファイルでは、3 行目は日付と時刻のタイムスタンプで、ログファイル間で異なります。

タイプ: 整数

必須: いいえ

LogDirectoryPath

CustomLogs の場合、EC2 インスタンスにログが保存されるパス。IIS ログの場合、IIS ログが個々のサイト (たとえば、C:\\inetpub\\logs\\LogFiles\\W3SVC***n***) に保存されるフォルダ。IIS ログの場合、W3C ログ形式のみがサポートされます。IIS、NCSA、カスタム形式はサポートされません。

型: 文字列

必須: はい

LogGroup

ロググループの名前です。この名前は、CloudWatch コンソールの [ロググループ] 画面に表示されます。

型: 文字列

必須: はい

LogName

ログファイルの名前。

1. ログの名前を検索するには、イベントビューアーのナビゲーションペインで、[Applications and Services Logs] を選択します。
2. ログの一覧で、アップロードするログを右クリックし (例えば、[Microsoft] > [Windows] > [Backup] > [Operational] など)、[Create Custom View] を選択します。
3. [Create Custom View] ダイアログボックスの [XML] タブを選択します。[LogName] は、<Select Path=> タグにあります (たとえば、`Microsoft-Windows-Backup` など)。このテキストを [LogName] パラメータにコピーします。

型: 文字列

有効な値: `Application` | `Security` | `System` | `Microsoft-Windows-WinINet/Analytic`

必須: はい

LogStream

送信先ログストリーム。[{instance_id}] (デフォルト) を使用した場合、このインスタンスのインスタンス ID がログストリーム名として使用されます。

型: 文字列

有効な値: `{instance_id}` | `{hostname}` | `{ip_address}` *`<log_stream_name>`*

存在しないログストリーム名を入力すると、CloudWatch Logs によってログストリームが自動的に作成されます。リテラル文字列、定義済み変数 ({instance_id}、{hostname}、{ip_address}) 、またはこれらの組み合わせを使用して、ログストリーム名を定義できます。

このパラメータで指定されたログのストリーム名は、CloudWatch コンソールの [Log Groups > Streams for ***`<YourLogStream>`***] 画面に表示されます。

必須: はい

MetricName

パフォーマンスデータが含まれる CloudWatch メトリクス。

> **Note**
>
> 名前に特殊文字を使用しないでください。使用した場合、メトリクスおよびその関連付けられたアラームが機能しないことがあります。

型: 文字列

必須: はい

NameSpace

パフォーマンスカウンターデータを書き込むメトリック名前空間。

型: 文字列

必須: はい

PollInterval

新しいパフォーマンスカウンタとログデータがアップロードされるまでに必要な経過秒数。

タイプ: 整数

有効な値: これを 5 秒以上に設定します。15 秒 (00:00: 15) をお勧めします。

必須: はい

リージョン

ログデータを送信する AWS リージョン。パフォーマンスカウンターは、ログデータの送信元とは異なるリージョンに送信できますが、インスタンスが実行されているのと同じリージョンにこのパラメータを設定することをお勧めします。

型: 文字列

有効な値: Systems Manager と CloudWatch Logs の両方でサポートされる AWS リージョン のリージョン ID (`us-east-2`、`eu-west-1`、`ap-southeast-1` など)。各サービスでサポートされる AWS リージョン のリストについては、「Amazon Web Services 全般のリファレンス」の「Amazon CloudWatch Logs サービスエンドポイント」と「Systems Manager サービスエンドポイント」を参照してください。

必須: はい

SecretKey

お客様のシークレットアクセスキー。IAM ロールを使用してインスタンスを起動しない限り、このプロパティは必須です。

型: 文字列

必須: いいえ

startType

インスタンスで CloudWatch をオンまたはオフにします。

型: 文字列

有効な値: `Enabled` | `Disabled`

必須: はい

TimestampFormat

使用するタイムスタンプ形式。サポートされる値の一覧については、MSDN ライブラリの「カスタムの日付と時刻の書式指定文字列」を参照してください。

型: 文字列

必須: はい

TimeZoneKind

ログのタイムスタンプにタイムゾーン情報が含まれていない場合にタイムゾーン情報を提供できます。このパラメータが空になっていて、タイムスタンプにタイムゾーン情報が含まれていない場合、CloudWatch Logs ではデフォルトでローカルタイムゾーンが使用されます。タイムスタンプに既にタイムゾーン情報が含まれている場合、このパラメータは無視されます。

型: 文字列

有効な値: `Local` | `UTC`

必須: いいえ

単位

メトリクスの適切な測定単位。

型: 文字列

有効な値: Seconds | Microseconds | Milliseconds | Bytes | Kilobytes | Megabytes | Gigabytes | Terabytes | Bits | Kilobits | Megabits | Gigabits | Terabits | Percent | Count | Bytes/Second | Kilobytes/Second | Megabytes/Second | Gigabytes/Second | Terabytes/Second | Bits/Second | Kilobits/Second | Megabits/Second | Gigabits/Second | Terabits/Second | Count/Second | None

必須: はい

aws:configureDocker

(スキーマバージョン 2.0 以降) コンテナと Docker と連携するインスタンスを設定します。このプラグインは、Linux のほとんどのバージョンと Windows Server オペレーティングシステムでのみサポートされています。

構文

スキーマ 2.2

YAML

```
---
schemaVersion: '2.2'
description: aws:configureDocker
parameters:
  action:
    description: "(Required) The type of action to perform."
    type: String
    default: Install
    allowedValues:
    - Install
    - Uninstall
mainSteps:
- action: aws:configureDocker
  name: configureDocker
  inputs:
    action: "{{ action }}"
```

JSON

```
{
```

```
  "schemaVersion": "2.2",
  "description": "aws:configureDocker plugin",
  "parameters": {
    "action": {
      "description": "(Required) The type of action to perform.",
      "type": "String",
      "default": "Install",
      "allowedValues": [
        "Install",
        "Uninstall"
      ]
    }
  },
  "mainSteps": [
    {
      "action": "aws:configureDocker",
      "name": "configureDocker",
      "inputs": {
        "action": "{{ action }}"
      }
    }
  ]
}
```

入力

アクション

実行するアクションのタイプ。

タイプ: Enum

有効な値: `Install` | `Uninstall`

必須: はい

aws:configurePackage

(スキーマバージョン 2.0 以降) AWS Systems Manager Distributor パッケージをインストールまたはアンインストールします。最新バージョン、デフォルトバージョン、または指定したパッケージのバージョンをインストールできます。AWS が提供するパッケージもサポートされています。こ

のプラグインは、Windows Server および Linux オペレーティングシステムで実行されます。ただし、Linux オペレーティングシステムでは、すべての利用可能なパッケージがサポートされているわけではありません。

Windows Server 用の利用できる AWS パッケージには、AWSPVDriver、AWSNVMe、AwsEnaNetworkDriver、AwsVssComponents、AmazonCloudWatchAgent、EC2Rescue. などがあります。

Linux オペレーティングシステムで使用できる AWSパッケージには、AmazonCloudWatchAgent、CodeDeployAgent、AWSSupport-EC2Rescue などがあります。

構文

スキーマ 2.2

YAML

```
---
schemaVersion: '2.2'
description: aws:configurePackage
parameters:
  name:
    description: "(Required) The name of the AWS package to install or uninstall."
    type: String
  action:
    description: "(Required) The type of action to perform."
    type: String
    default: Install
    allowedValues:
    - Install
    - Uninstall
  ssmParameter:
    description: "(Required) Argument stored in Parameter Store."
    type: String
    default: "{{ ssm:parameter_store_arg }}"
mainSteps:
- action: aws:configurePackage
  name: configurePackage
  inputs:
    name: "{{ name }}"
    action: "{{ action }}"
```

```
    additionalArguments:
      "{\"SSM_parameter_store_arg\": \"{{ ssmParameter }}\", \"SSM_custom_arg\":
 \"myValue\"}"
```

JSON

```
{
   "schemaVersion": "2.2",
   "description": "aws:configurePackage",
   "parameters": {
      "name": {
         "description": "(Required) The name of the AWS package to install or
 uninstall.",
         "type": "String"
      },
      "action": {
         "description": "(Required) The type of action to perform.",
         "type": "String",
         "default": "Install",
         "allowedValues": [
            "Install",
            "Uninstall"
         ]
      },
      "ssmParameter": {
         "description": "(Required) Argument stored in Parameter Store.",
         "type": "String",
         "default": "{{ ssm:parameter_store_arg }}"
      }
   },
   "mainSteps": [
      {
         "action": "aws:configurePackage",
         "name": "configurePackage",
         "inputs": {
            "name": "{{ name }}",
            "action": "{{ action }}",
            "additionalArguments": "{\"SSM_parameter_store_arg\":
 \"{{ ssmParameter }}\", \"SSM_custom_arg\": \"myValue\"}"
         }
      }
   ]
}
```

入力

名前

インストールまたはアンインストールする AWS パッケージの名前。使用可能なパッケージには AWSPVDriver、AwsEnaNetworkDriver、AwsVssComponents、AmazonCloudWatchAgent などがあります。

型: 文字列

必須: はい

action

パッケージをインストールまたはアンインストールします。

タイプ: Enum

有効な値: `Install` | `Uninstall`

必須: はい

installationType

実行するインストールのタイプ。`Uninstall and reinstall` を指定した場合、パッケージは完全にアンインストールされてから再インストールされます。再インストールが完了するまで、アプリケーションは利用できません。`In-place update` を指定した場合、更新スクリプトに指定した手順に従って、新しいファイルまたは変更されたファイルのみが既存のインストールに追加されます。アプリケーションは、更新プロセス中も引き続き使用できます。`In-place update` オプションは、AWS 公開パッケージではサポートされていません。`Uninstall and reinstall` がデフォルト値です。

タイプ: Enum

有効な値: `Uninstall and reinstall` | `In-place update`

必須: いいえ

additionalArguments

インストール、アンインストール、または更新スクリプトに指定する追加パラメータの JSON 文字列。各パラメータには、接頭辞 SSM_ を付ける必要があります。規則 {{ssm:*parameter-name*}} を使用して、追加の引数で Parameter Store パラメータを参照できます。インストー

ル、アンインストール、または更新スクリプトで追加のパラメータを使用するには、オペレーティングシステムに適した構文を使用して、パラメータを環境変数として参照する必要があります。たとえば、PowerShell では、SSM_arg 引数を $Env:SSM_arg として参照します。定義する引数の数に制限はありませんが、追加の引数の入力には 4,096 文字の制限があります。この制限には、定義するすべてのキーと値が含まれます。

型: StringMap

必須: いいえ

バージョン

インストールまたはアンインストールするパッケージの特定のバージョン。インストールする場合、デフォルトで最新の公開バージョンがインストールされます。アンインストールすると、デフォルトで現在インストールされているバージョンがアンインストールされます。インストールされているバージョンが見つからない場合は、最新の公開バージョンがダウンロードされ、アンインストール処理が実行されます。

型: 文字列

必須: いいえ

aws:domainJoin

ドメインに EC2 インスタンスを結合します。このプラグインは、Linux および Windows Server オペレーティングシステムでのみ実行されます。このプラグインは、Linux インスタンスのホスト名を EC2AMAZ-*XXXXXXX* の形式に変更します。EC2 インスタンスの結合の詳細については、AWS Directory Service 管理ガイドの EC2 インスタンスの AWS Managed Microsoft AD ディレクトリへの結合を参照してください。

構文

スキーマ 2.2

YAML

```
---
schemaVersion: '2.2'
description: aws:domainJoin
parameters:
  directoryId:
```

```
    description: "(Required) The ID of the directory."
    type: String
  directoryName:
    description: "(Required) The name of the domain."
    type: String
  directoryOU:
    description: "(Optional) The organizational unit to assign the computer object
 to."
    type: String
  dnsIpAddresses:
    description: "(Required) The IP addresses of the DNS servers for your
 directory."
    type: StringList
  hostname:
    description: "(Optional) The hostname you want to assign to the node."
    type: String
mainSteps:
- action: aws:domainJoin
  name: domainJoin
  inputs:
    directoryId: "{{ directoryId }}"
    directoryName: "{{ directoryName }}"
    directoryOU: "{{ directoryOU }}"
    dnsIpAddresses: "{{ dnsIpAddresses }}"
    hostname: "{{ hostname }}"
```

JSON

```
{
  "schemaVersion": "2.2",
  "description": "aws:domainJoin",
  "parameters": {
    "directoryId": {
      "description": "(Required) The ID of the directory.",
      "type": "String"
    },
    "directoryName": {
      "description": "(Required) The name of the domain.",
      "type": "String"
    },
    "directoryOU": {
        "description": "(Optional) The organizational unit to assign the computer
 object to.",
```

```
        "type": "String"
      },
    "dnsIpAddresses": {
      "description": "(Required) The IP addresses of the DNS servers for your
 directory.",
      "type": "StringList"
    },
    "hostname": {
        "description": "(Optional) The hostname you want to assign to the node.",
        "type": "String"
      }
  },
  "mainSteps": [
    {
      "action": "aws:domainJoin",
      "name": "domainJoin",
      "inputs": {
        "directoryId": "{{ directoryId }}",
        "directoryName": "{{ directoryName }}",
        "directoryOU":"{{ directoryOU }}",
        "dnsIpAddresses":"{{ dnsIpAddresses }}",
        "hostname":"{{ hostname }}"
      }
    }
  ]
}
```

スキーマ 1.2

YAML

```
---
runtimeConfig:
  aws:domainJoin:
    properties:
      directoryId: "{{ directoryId }}"
      directoryName: "{{ directoryName }}"
      directoryOU: "{{ directoryOU }}"
      dnsIpAddresses: "{{ dnsIpAddresses }}"
```

JSON

```
{
   "runtimeConfig":{
      "aws:domainJoin":{
         "properties":{
            "directoryId":"{{ directoryId }}",
            "directoryName":"{{ directoryName }}",
            "directoryOU":"{{ directoryOU }}",
            "dnsIpAddresses":"{{ dnsIpAddresses }}"
         }
      }
   }
}
```

プロパティ

directoryId

ディレクトリの ID。

型: 文字列

必須: はい

例: "directoryId": "d-1234567890"

directoryName

ドメインの名前。

型: 文字列

必須: はい

例: "directoryName": "example.com"

directoryOU

部門単位 (OU)。

型: 文字列

必須: いいえ

例: "directoryOU": "OU=test,DC=example,DC=com"

dnsIpAddresses

DNS サーバーの IP アドレス。

タイプ: StringList

必須: はい

例: "dnsIpAddresses": ["198.51.100.1","198.51.100.2"]

hostname

ノードに割り当てるホスト名。指定しない場合、Windows インスタンスの名前は変更されませんが、Linux インスタンスはデフォルトの命名パターンを使用します。指定した場合、Windows インスタンスは正確に指定された値を使用しますが、Linux インスタンスの場合はプレフィックスとして機能します (keepHostName が「true」に設定されている場合を除く)。

タイプ: 文字列

必須: いいえ

keepHostName

ドメインに参加したときに Linux インスタンスのホスト名を変更するかどうかを決定します。これは Linux のみのパラメータです。デフォルトでは (hostname、hostnameNumAppendDigits への入力なしで、keepHostName が「false」の場合)、Linux ホストの名前はパターン EC2AMAZ-XXXXXX に変更されます。「true」に設定すると、元のホスト名が保持され、hostname と hostnameNumAppendDigits への入力は無視されます。

型: ブール値

必須: いいえ

hostnameNumAppendDigits

ホスト名値の後に追加するランダムな数値の数を定義します。これは Linux 専用パラメータであり、hostname パラメータと一緒に使用されます。これは、hostname が指定されなかった場合に無視されます。

タイプ: 文字列

許可される値: 1 ~ 5

必須: いいえ

例

例については、AWS Directory Service 管理ガイドの「Amazon EC2 インスタンスを AWS Managed Microsoft AD に結合する」を参照してください。

aws:downloadContent

(スキーマバージョン 2.0 以降) リモートの場所から SSM ドキュメントとスクリプトをダウンロードします。GitHub Enterprise リポジトリはサポートされていません。このプラグインは、Linux および Windows Server オペレーティングシステムでのみサポートされています。

構文

スキーマ 2.2

YAML

```
---
schemaVersion: '2.2'
description: aws:downloadContent
parameters:
  sourceType:
    description: "(Required) The download source."
    type: String
  sourceInfo:
    description: "(Required) The information required to retrieve the content from
      the required source."
    type: StringMap
mainSteps:
- action: aws:downloadContent
  name: downloadContent
  inputs:
    sourceType: "{{ sourceType }}"
    sourceInfo: "{{ sourceInfo }}"
```

JSON

```
{
  "schemaVersion": "2.2",
  "description": "aws:downloadContent",
```

```
  "parameters": {
    "sourceType": {
    "description": "(Required) The download source.",
    "type": "String"
  },
  "sourceInfo": {
    "description": "(Required) The information required to retrieve the content from
 the required source.",
    "type": "StringMap"
    }
  },
  "mainSteps": [
    {
      "action": "aws:downloadContent",
      "name": "downloadContent",
      "inputs": {
        "sourceType":"{{ sourceType }}",
        "sourceInfo":"{{ sourceInfo }}"
      }
    }
  ]
}
```

入力

sourceType

ソースをダウンロードします。Systems Manager は、スクリプトおよび SSM ドキュメントのダウンロード用に GitHub、Git、HTTP、S3、および SSMDocument のソースタイプをサポートしています。

型: 文字列

必須: はい

sourceInfo

必須ソースからコンテンツを取得するために必要な情報。

型: StringMap

必須: はい

sourceType が **GitHub,** の場合は以下を指定します。

- 所有者: リポジトリ所有者。
- リポジトリ: リポジトリの名前。
- パス: ダウンロードするファイルまたはディレクトリのパス。
- getOptions: マスター以外のブランチまたはリポジトリ内の特定のコミットからコンテンツを取得するための追加オプション。マスターブランチで最新のコミットを使用している場合は、getOptions を省略できます。2020 年 10 月 1 日以降にリポジトリが作成された場合、デフォルトのブランチの名前は master ではなく main になる場合があります。この場合、getOptions パラメータの値を指定する必要があります。

  このパラメータは次の形式を使用します。

  - ブランチ: refs/heads/*branch_name*

    デフォルトは `master` です。

    デフォルト以外のブランチを指定するには、次の形式を使用します。

    ブランチ: refs/heads/*branch_name*
  - commitID:*commitID*

    デフォルト: `head`。

    最新ではないコミットにあるバージョンの SSM ドキュメントを使用するには、完全なコミット ID を指定します。例:

    ```
    "getOptions": "commitID:bbc1ddb94...b76d3bEXAMPLE",
    ```
- tokenInfo: GitHub アクセストークン情報を {{ssm-secure:*secure-string-token-name*}} 形式で保存する先の Systems Manager パラメータ (SecureString パラメータ)。

  > **Note**
  >
  > この `tokenInfo` フィールドは、SecureString パラメータをサポートする唯一の SSM ドキュメントプラグインフィールドです。SecureString パラメータは、他のフィールドや他の SSM ドキュメントプラグインではサポートされません。

```
{
    "owner":"TestUser",
    "repository":"GitHubTest",
```

```
    "path":"scripts/python/test-script",
    "getOptions":"branch:master",
    "tokenInfo":"{{ssm-secure:secure-string-token}}"
}
```

sourceType **Git** には、以下を指定する必要があります。

- repository

  ダウンロードするファイルまたはディレクトリへの Git リポジトリの URL です。

  型: 文字列

さらに、以下のオプションのパラメータを指定できます。

- getOptions

  マスター以外のブランチ、またはリポジトリ内の特定のコミットからコンテンツを取得するための追加オプションです。マスターブランチで最新のコミットを使用している場合は、getOptions を省略できます。

  型: 文字列

  このパラメータは次の形式を使用します。

  - ブランチ: refs/heads/*branch_name*

    デフォルト: `master`。

    "branch" は、SSM ドキュメントが 以外のブランチに保存されている場合にのみ必要です。`master`例:

    ```
    "getOptions": "branch:refs/heads/main"
    ```

  - commitID:*commitID*

    デフォルト: head。

    最新ではないコミットにあるバージョンの SSM ドキュメントを使用するには、完全なコミット ID を指定します。以下に例を示します。

    ```
    "getOptions": "commitID:bbc1ddb94...b76d3bEXAMPLE",
    ```

- privateSSHKey

指定した repository への接続時に使用する SSH キーです。SSH キーの値に対する SecureString パラメータを参照するには、{{ssm-secure:*your-secure-string-parameter*}} の形式を使用できます。

型: 文字列

- skipHostKeyChecking

  指定した repository に接続するときの stricthOstKeyChecking オプションの値を決定します。デフォルト値は false です。

  タイプ: ブール値

- username

  HTTP を使用して指定した repository への接続時に使用するユーザー名です。ユーザー名の値に対する SecureStringパラメータを参照するには、{{ssm-secure:*your-secure-string-parameter*}} の形式を使用できます。

  型: 文字列

- password

  HTTP を使用して指定した repository への接続時に使用するパスワードです。パスワードの値に対する SecureStringパラメータを参照するには、{{ssm-secure:*your-secure-string-parameter*}} の形式を使用できます。

  型: 文字列

sourceType **HTTP** には、以下を指定する必要があります。

- url

  ダウンロードするファイルまたはディレクトリの URL です。

  型: 文字列

さらに、以下のオプションのパラメータを指定できます。

- allowInsecureDownload

  Secure Socket Layer (SSL) または Transport Layer Security (TLS) で暗号化されていない接続経由でダウンロードを実行できるかどうかを決定します。デフォルト値は false です。暗号化を使用せずにダウンロードを実行することは推奨されません。このようなダウンロードの実

行を選択する場合は、ユーザーが関連するすべてのリスクに対する責任を負います。セキュリティは、AWS とお客様の間の共有責任です。これは、責任共有モデルと説明されます。詳細については、責任共有モデルを参照してください。

タイプ: ブール値

- authMethod

  指定した url への接続時の認証にユーザー名とパスワードを使用するかどうかを決定します。Basic または Digest を指定する場合は、username および password パラメータの値を入力する必要があります。Digest メソッドを使用するには、SSM Agent バージョン 3.0.1181.0 以降がインスタンスにインストールされている必要があります。Digest メソッドは、MD5 および SHA256 暗号化をサポートします。

  型: 文字列

  有効な値: None | Basic | Digest

- username

  指定した url に Basic 認証を使用して接続するときに使用するユーザー名です。ユーザー名の値に対する SecureStringパラメータを参照するには、{{ssm-secure:*your-secure-string-parameter*}} の形式を使用できます。

  型: 文字列

- password

  指定した url に Basic 認証を使用して接続するときに使用するパスワードです。パスワードの値に対する SecureStringパラメータを参照するには、{{ssm-secure:*your-secure-string-parameter*}} の形式を使用できます。

  型: 文字列

sourceType **S3** では以下を指定します。

- パス: Amazon S3 からダウンロードするファイルまたはディレクトリの URL。

```
{
    "path": "https://s3.amazonaws.com/amzn-s3-demo-bucket/powershell/
helloPowershell.ps1"
}
```

sourceType **SSMDocument** では、以下のいずれかを指定します。

- 名前: name:version の形式のドキュメントの名前とバージョン。バージョンは省略できます。

```
{
    "name": "Example-RunPowerShellScript:3"
}
```

- name: arn:aws:ssm:*region*:*account_id*:document/*document_name* の形式のドキュメントの ARN。

```
{
   "name":"arn:aws:ssm:us-east-2:3344556677:document/MySharedDoc"
}
```

destinationPath

ファイルのダウンロード先としてオプションで指定する、インスタンス上のローカルパス。パスを指定しない場合、コンテンツは、コマンド ID に相対的なパスにダウンロードされます。

型: 文字列

必須: いいえ

aws:psModule

Amazon EC2 インスタンスに PowerShell モジュールをインストールします。このプラグインは、Windows Server オペレーティングシステムでのみ実行されます。

構文

スキーマ 2.2

YAML

```
---
schemaVersion: '2.2'
description: aws:psModule
parameters:
  source:
    description: "(Required) The URL or local path on the instance to the
 application
```

```
      .zip file."
    type: String
mainSteps:
- action: aws:psModule
  name: psModule
  inputs:
    source: "{{ source }}"
```

JSON

```
{
  "schemaVersion": "2.2",
  "description": "aws:psModule",
  "parameters": {
    "source": {
      "description": "(Required) The URL or local path on the instance to the
 application .zip file.",
      "type": "String"
    }
  },
  "mainSteps": [
    {
      "action": "aws:psModule",
      "name": "psModule",
      "inputs": {
        "source": "{{ source }}"
      }
    }
  ]
}
```

スキーマ 1.2

YAML

```
---
runtimeConfig:
  aws:psModule:
    properties:
    - runCommand: "{{ commands }}"
      source: "{{ source }}"
      sourceHash: "{{ sourceHash }}"
```

```
      workingDirectory: "{{ workingDirectory }}"
      timeoutSeconds: "{{ executionTimeout }}"
```

JSON

```
{
   "runtimeConfig":{
      "aws:psModule":{
         "properties":[
            {
               "runCommand":"{{ commands }}",
               "source":"{{ source }}",
               "sourceHash":"{{ sourceHash }}",
               "workingDirectory":"{{ workingDirectory }}",
               "timeoutSeconds":"{{ executionTimeout }}"
            }
         ]
      }
   }
}
```

プロパティ

runCommand

モジュールのインストール後に実行する PowerShell コマンド。

タイプ: StringList

必須: いいえ

source

アプリケーション.zip ファイルへのインスタンスの URL またはローカルパス。

型: 文字列

必須: はい

sourceHash

.zip ファイルの SHA256 ハッシュ。

型: 文字列

必須: いいえ

timeoutSeconds

コマンドが失敗したとみなされるまでの経過時間 (秒)。

型: 文字列

必須: いいえ

workingDirectory

インスタンスの作業ディレクトリへのパス。

型: 文字列

必須: いいえ

aws:refreshAssociation

(スキーマ バージョン 2.0 以降) 必要に応じて関連付けを更新 (強制適用) します。このアクションは、選択された関連付けで定義されている内容またはターゲットにバインドされているすべての関連付けに基づいてシステム状態を変更します。このプラグインは、Linux および Microsoft Windows Server オペレーティングシステムでのみ実行されます。

構文

スキーマ 2.2

YAML

```
---
schemaVersion: '2.2'
description: aws:refreshAssociation
parameters:
  associationIds:
    description: "(Optional) List of association IDs. If empty, all associations
 bound
      to the specified target are applied."
    type: StringList
```

```
mainSteps:
- action: aws:refreshAssociation
  name: refreshAssociation
  inputs:
    associationIds:
    - "{{ associationIds }}"
```

JSON

```
{
  "schemaVersion": "2.2",
  "description": "aws:refreshAssociation",
  "parameters": {
    "associationIds": {
      "description": "(Optional) List of association IDs. If empty, all associations
 bound to the specified target are applied.",
      "type": "StringList"
    }
  },
  "mainSteps": [
    {
      "action": "aws:refreshAssociation",
      "name": "refreshAssociation",
      "inputs": {
        "associationIds": [
          "{{ associationIds }}"
        ]
      }
    }
  ]
}
```

入力

associationIds

関連付け ID の一覧。空の場合、指定されたターゲットにバインドされたすべての関連付けが適用されます。

タイプ: StringList

必須: いいえ

aws:runDockerAction

(スキーマバージョン 2.0 以降) コンテナで Docker アクションを実行します。このプラグインは、Linux および Microsoft Windows Server オペレーティングシステムでのみ実行されます。

構文

スキーマ 2.2

YAML

```
---
mainSteps:
- action: aws:runDockerAction
  name: RunDockerAction
  inputs:
    action: "{{ action }}"
    container: "{{ container }}"
    image: "{{ image }}"
    memory: "{{ memory }}"
    cpuShares: "{{ cpuShares }}"
    volume: "{{ volume }}"
    cmd: "{{ cmd }}"
    env: "{{ env }}"
    user: "{{ user }}"
    publish: "{{ publish }}"
    workingDirectory: "{{ workingDirectory }}"
    timeoutSeconds: "{{ timeoutSeconds }}"
```

JSON

```
{
   "mainSteps":[
      {
         "action":"aws:runDockerAction",
         "name":"RunDockerAction",
         "inputs":{
            "action":"{{ action }}",
            "container":"{{ container }}",
            "image":"{{ image }}",
            "memory":"{{ memory }}",
            "cpuShares":"{{ cpuShares }}",
            "volume":"{{ volume }}",
```

```
            "cmd":"{{ cmd }}",
            "env":"{{ env }}",
            "user":"{{ user }}",
            "publish":"{{ publish }}",
            "workingDirectory": "{{ workingDirectory }}",
            "timeoutSeconds": "{{ timeoutSeconds }}"
         }
      }
   ]
}
```

入力

アクション

実行するアクションのタイプ。

型: 文字列

必須: はい

コンテナ

Docker コンテナ ID。

型: 文字列

必須: いいえ

イメージ

Docker イメージ名。

型: 文字列

必須: いいえ

cmd

コンテナコマンド。

型: 文字列

必須: いいえ

メモリ

コンテナメモリの制限。

型: 文字列

必須: いいえ

cpuShares

コンテナの CPU シェア (相対重み)。

型: 文字列

必須: いいえ

ボリューム

コンテナボリュームのマウント。

タイプ: StringList

必須: いいえ

env

コンテナ環境変数。

型: 文字列

必須: いいえ

ユーザー

コンテナユーザー名。

型: 文字列

必須: いいえ

publish

コンテナ公開されたポート。

型: 文字列

必須: いいえ

workingDirectory

マネージドノードの作業ディレクトリへのパス。

タイプ: 文字列

必須: いいえ

timeoutSeconds

コマンドが失敗したとみなされるまでの経過時間 (秒)。

型: 文字列

必須: いいえ

aws:runDocument

(スキーマバージョン 2.0 以降) Systems Manager またはローカル共有に格納された SSM ドキュメントを実行します。このプラグインと aws:downloadContent プラグインを使用して、リモートの場所から SSM ドキュメントをローカル共有にダウンロードして実行できます。このプラグインは、Linux および Windows Server オペレーティングシステムでのみサポートされています。このプラグインは、AWS-UpdateSSMAgent ドキュメントの実行または aws:updateSsmAgent を使用するドキュメントをサポートしていません。

構文

スキーマ 2.2

YAML

```
---
schemaVersion: '2.2'
description: aws:runDocument
parameters:
  documentType:
    description: "(Required) The document type to run."
    type: String
    allowedValues:
    - LocalPath
    - SSMDocument
```

```
mainSteps:
- action: aws:runDocument
  name: runDocument
  inputs:
    documentType: "{{ documentType }}"
```

JSON

```
{
  "schemaVersion": "2.2",
  "description": "aws:runDocument",
  "parameters": {
    "documentType": {
      "description": "(Required) The document type to run.",
      "type": "String",
      "allowedValues": [
        "LocalPath",
        "SSMDocument"
      ]
    }
  },
  "mainSteps": [
    {
      "action": "aws:runDocument",
      "name": "runDocument",
      "inputs": {
        "documentType": "{{ documentType }}"
      }
    }
  ]
}
```

入力

documentType

実行するドキュメントタイプ。ローカルドキュメント (LocalPath) または Systems Manager (SSMDocument) に保存されているドキュメントを実行できます。

型: 文字列

必須: はい

documentPath

ドキュメントへのパス。documentType が LocalPath の場合は、ローカル共有上のドキュメントへのパスを指定します。documentType が SSMDocument の場合は、ドキュメントの名前を指定します。

型: 文字列

必須: いいえ

documentParameters

ドキュメントのパラメータ。

型: StringMap

必須: いいえ

aws:runPowerShellScript

PowerShell スクリプトを実行するか、またはスクリプトを実行するパスを指定します。このプラグインは、Microsoft Windows Server および Linux オペレーティングシステムでのみ実行されます。

構文

スキーマ 2.2

YAML

```
---
schemaVersion: '2.2'
description: aws:runPowerShellScript
parameters:
  commands:
    type: String
    description: "(Required) The commands to run or the path to an existing script
      on the instance."
    default: Write-Host "Hello World"
mainSteps:
- action: aws:runPowerShellScript
  name: runPowerShellScript
  inputs:
```

```
    timeoutSeconds: '60'
    runCommand:
    - "{{ commands }}"
```

JSON

```
{
  "schemaVersion": "2.2",
  "description": "aws:runPowerShellScript",
  "parameters": {
    "commands": {
      "type": "String",
      "description": "(Required) The commands to run or the path to an existing
 script on the instance.",
      "default": "Write-Host \"Hello World\""
    }
  },
  "mainSteps": [
    {
      "action": "aws:runPowerShellScript",
      "name": "runPowerShellScript",
      "inputs": {
        "timeoutSeconds": "60",
        "runCommand": [
          "{{ commands }}"
        ]
      }
    }
  ]
}
```

スキーマ 1.2

YAML

```
---
runtimeConfig:
  aws:runPowerShellScript:
    properties:
    - id: 0.aws:runPowerShellScript
      runCommand: "{{ commands }}"
      workingDirectory: "{{ workingDirectory }}"
```

```
      timeoutSeconds: "{{ executionTimeout }}"
```

JSON

```
{
   "runtimeConfig":{
      "aws:runPowerShellScript":{
         "properties":[
            {
               "id":"0.aws:runPowerShellScript",
               "runCommand":"{{ commands }}",
               "workingDirectory":"{{ workingDirectory }}",
               "timeoutSeconds":"{{ executionTimeout }}"
            }
         ]
      }
   }
}
```

プロパティ

runCommand

実行するコマンド、またはインスタンス上の既存のスクリプトへのパスを指定します。

タイプ: StringList

必須: はい

timeoutSeconds

コマンドが失敗したとみなされるまでの経過時間 (秒)。タイムアウトに達すると、Systems Manager はコマンドの実行を停止します。

型: 文字列

必須: いいえ

workingDirectory

インスタンスの作業ディレクトリへのパス。

型: 文字列

必須: いいえ

aws:runShellScript

Linux シェルスクリプトを実行するか、またはスクリプトを実行するパスを指定します。このプラグインは、Linux オペレーティングシステム上のみで実行されます。

構文

スキーマ 2.2

YAML

```
---
schemaVersion: '2.2'
description: aws:runShellScript
parameters:
  commands:
    type: String
    description: "(Required) The commands to run or the path to an existing script
      on the instance."
    default: echo Hello World
mainSteps:
- action: aws:runShellScript
  name: runShellScript
  inputs:
    timeoutSeconds: '60'
    runCommand:
    - "{{ commands }}"
```

JSON

```
{
  "schemaVersion": "2.2",
  "description": "aws:runShellScript",
  "parameters": {
    "commands": {
      "type": "String",
      "description": "(Required) The commands to run or the path to an existing
 script on the instance.",
      "default": "echo Hello World"
    }
```

```
  },
  "mainSteps": [
    {
      "action": "aws:runShellScript",
      "name": "runShellScript",
      "inputs": {
        "timeoutSeconds": "60",
        "runCommand": [
          "{{ commands }}"
        ]
      }
    }
  ]
}
```

スキーマ 1.2

YAML

```
---
runtimeConfig:
  aws:runShellScript:
    properties:
    - runCommand: "{{ commands }}"
      workingDirectory: "{{ workingDirectory }}"
      timeoutSeconds: "{{ executionTimeout }}"
```

JSON

```
{
   "runtimeConfig":{
      "aws:runShellScript":{
         "properties":[
            {
               "runCommand":"{{ commands }}",
               "workingDirectory":"{{ workingDirectory }}",
               "timeoutSeconds":"{{ executionTimeout }}"
            }
         ]
      }
   }
}
```

プロパティ

runCommand

実行するコマンド、またはインスタンス上の既存のスクリプトへのパスを指定します。

タイプ: StringList

必須: はい

timeoutSeconds

コマンドが失敗したとみなされるまでの経過時間 (秒)。タイムアウトに達すると、Systems Manager はコマンドの実行を停止します。

型: 文字列

必須: いいえ

workingDirectory

インスタンスの作業ディレクトリへのパス。

型: 文字列

必須: いいえ

`aws:softwareInventory`

(スキーマバージョン 2.0 以降) マネージドインスタンスのアプリケーション、ファイル、および設定に関するメタデータを収集します。このプラグインは、Linux および Microsoft Windows Server オペレーティングシステムでのみ実行されます。インベントリ収集を設定する際は、まず AWS Systems Manager State Manager の関連付けを作成します。関連付けが実行されると、Systems Manager はインベントリデータを収集します。最初に関連付けを作成せずに、`aws:softwareInventory` プラグインを呼び出そうとすると、システムは次のエラーを返します。

```
The aws:softwareInventory plugin can only be invoked via ssm-associate.
```

インスタンスには、一度に 1 つのインベントリのみ関連付けることができます。インスタンスに 2 つ以上関連付けを設定した場合、そのインベントリの関連付けは実行されず、インベントリデータは収集されません。インベントリの収集の詳細については、「AWS Systems Manager インベントリ」を参照してください。

構文

スキーマ 2.2

YAML

```
---
mainSteps:
- action: aws:softwareInventory
  name: collectSoftwareInventoryItems
  inputs:
    applications: "{{ applications }}"
    awsComponents: "{{ awsComponents }}"
    networkConfig: "{{ networkConfig }}"
    files: "{{ files }}"
    services: "{{ services }}"
    windowsRoles: "{{ windowsRoles }}"
    windowsRegistry: "{{ windowsRegistry}}"
    windowsUpdates: "{{ windowsUpdates }}"
    instanceDetailedInformation: "{{ instanceDetailedInformation }}"
    customInventory: "{{ customInventory }}"
```

JSON

```
{
   "mainSteps":[
      {
         "action":"aws:softwareInventory",
         "name":"collectSoftwareInventoryItems",
         "inputs":{
            "applications":"{{ applications }}",
            "awsComponents":"{{ awsComponents }}",
            "networkConfig":"{{ networkConfig }}",
            "files":"{{ files }}",
            "services":"{{ services }}",
            "windowsRoles":"{{ windowsRoles }}",
            "windowsRegistry":"{{ windowsRegistry}}",
            "windowsUpdates":"{{ windowsUpdates }}",
            "instanceDetailedInformation":"{{ instanceDetailedInformation }}",
            "customInventory":"{{ customInventory }}"
         }
      }
   ]
```

```
}
```

入力

applications

(オプション) インストールされているアプリケーションのメタデータを収集します。

型: 文字列

必須: いいえ

awsComponents

(オプション) amazon-ssm-agent などの AWS コンポーネントのメタデータを収集します。

型: 文字列

必須: いいえ

ファイル

(オプション: SSM Agent バージョン 2.2.64.0 以降が必要) ファイル名、ファイル作成時間、ファイルの最終変更時間および最新アクセス時間、およびファイルサイズを含むファイルのメタデータを収集します (これらはほんの数例です)。ファイルインベントリの収集の詳細については、「ファイルと Windows レジストリインベントリで作業する」を参照してください。

型: 文字列

必須: いいえ

networkConfig

(オプション) ネットワーク設定のメタデータを収集します。

型: 文字列

必須: いいえ

billingInfo

(オプション) AMI の請求コードに関連付けられたプラットフォーム情報のメタデータを収集します。

タイプ: 文字列

必須: いいえ

windowsUpdates

(オプション) すべての Windows アップデートのメタデータを収集します。

型: 文字列

必須: いいえ

InstanceDetailedInformation

(オプション) CPU モデル、速度、コア数を含む、デフォルトのインベントリプラグイン (`aws:instanceInformation`) によって提供されるよりも多くのインスタンス情報を収集します (これらはほんの数例です)。

型: 文字列

必須: いいえ

サービス

(オプション: Windows OS のみ、SSM Agent バージョン 2.2.64.0 以降が必要) サービス設定のメタデータを収集します。

タイプ: 文字列

必須: いいえ

windowsRegistry

(オプション: Windows OS のみ、SSM Agent バージョン 2.2.64.0 以降が必要) Windows レジストリキーと値を収集します。キーパスを選択して、すべてのキーと値を再帰的に収集できます。指定するパスで指定するレジストリキーおよびその値を収集することもできます。インベントリは、キーパス、名前、タイプ、値を収集します。Windows レジストリインベントリの収集についての詳細は、「ファイルと Windows レジストリインベントリで作業する」を参照してください。

型: 文字列

必須: いいえ

windowsRoles

(オプション: Windows OS のみ、SSM Agent バージョン 2.2.64.0 以降が必要) Microsoft Windows ロール設定のメタデータを収集します。

タイプ: 文字列

必須: いいえ

customInventory

(オプション) カスタムインベントリのデータを収集します。カスタムインベントリの詳細については、「カスタムインベントリの操作」を参照してください。

型: 文字列

必須: いいえ

customInventoryDirectory

(オプション) 指定したディレクトリからカスタムインベントリデータを収集します。カスタムインベントリの詳細については、「カスタムインベントリの操作」を参照してください。

型: 文字列

必須: いいえ

aws:updateAgent

EC2Config サービスを最新バージョンに更新するか、または古いバージョンを指定します。このプラグインは、Microsoft Windows Server オペレーティングシステムでのみ実行されます。EC2Config サービスの詳細については、「Amazon EC2 ユーザーガイド」の「EC2Config サービスを使用した Windows インスタンスの設定 (レガシー)」を参照してください。

構文

スキーマ 2.2

YAML

```
---
schemaVersion: '2.2'
description: aws:updateAgent
mainSteps:
```

```
- action: aws:updateAgent
  name: updateAgent
  inputs:
    agentName: Ec2Config
    source: https://s3.{Region}.amazonaws.com/aws-ssm-{Region}/manifest.json
```

JSON

```
{
  "schemaVersion": "2.2",
  "description": "aws:updateAgent",
  "mainSteps": [
    {
      "action": "aws:updateAgent",
      "name": "updateAgent",
      "inputs": {
        "agentName": "Ec2Config",
        "source": "https://s3.{Region}.amazonaws.com/aws-ssm-{Region}/manifest.json"
      }
    }
  ]
}
```

スキーマ 1.2

YAML

```
---
runtimeConfig:
  aws:updateAgent:
    properties:
      agentName: Ec2Config
      source: https://s3.{Region}.amazonaws.com/aws-ssm-{Region}/manifest.json
      allowDowngrade: "{{ allowDowngrade }}"
      targetVersion: "{{ version }}"
```

JSON

```
{
   "runtimeConfig":{
      "aws:updateAgent":{
         "properties":{
```

```
            "agentName":"Ec2Config",
            "source":"https://s3.{Region}.amazonaws.com/aws-ssm-{Region}/
manifest.json",
            "allowDowngrade":"{{ allowDowngrade }}",
            "targetVersion":"{{ version }}"
         }
      }
   }
}
```

プロパティ

agentName

EC2Config。これは、EC2Config サービスを実行するエージェントの名前です。

型: 文字列

必須: はい

allowDowngrade

EC2Config サービスを以前のバージョンにダウングレードできるようにします。false に設定すると、サービスは新しいバージョンにのみアップグレードできます (デフォルト)。true に設定すると、以前のバージョンを指定します。

タイプ: ブール値

必須: いいえ

source

Systems Manager がインストールする EC2Config のバージョンをコピーする場所。この場所は変更できません。

型: 文字列

必須: はい

targetVersion

インストールする EC2Config サービスの特定のバージョン。指定しない場合、サービスは最新バージョンに更新されます。

型: 文字列

必須: いいえ

aws:updateSsmAgent

SSM Agent を最新バージョンに更新するか、古いバージョンを指定します。このプラグインは、Linux および Windows Server オペレーティングシステムでのみ実行されます。詳細については、「「SSM Agent」 の使用」を参照してください。

構文

スキーマ 2.2

YAML

```
---
schemaVersion: '2.2'
description: aws:updateSsmAgent
parameters:
  allowDowngrade:
    default: 'false'
    description: "(Optional) Allow the Amazon SSM Agent service to be downgraded to
      an earlier version. If set to false, the service can be upgraded to newer
 versions
      only (default). If set to true, specify the earlier version."
    type: String
    allowedValues:
    - 'true'
    - 'false'
mainSteps:
- action: aws:updateSsmAgent
  name: updateSSMAgent
  inputs:
    agentName: amazon-ssm-agent
    source: https://s3.{Region}.amazonaws.com/amazon-ssm-{Region}/ssm-agent-
manifest.json
    allowDowngrade: "{{ allowDowngrade }}"
```

JSON

```
{
  "schemaVersion": "2.2",
  "description": "aws:updateSsmAgent",
```

```
  "parameters": {
    "allowDowngrade": {
      "default": "false",
      "description": "(Required) Allow the Amazon SSM Agent service to be downgraded
 to an earlier version. If set to false, the service can be upgraded to newer
 versions only (default). If set to true, specify the earlier version.",
      "type": "String",
      "allowedValues": [
        "true",
        "false"
      ]
    }
  },
  "mainSteps": [
    {
      "action": "aws:updateSsmAgent",
      "name": "awsupdateSsmAgent",
      "inputs": {
        "agentName": "amazon-ssm-agent",
        "source": "https://s3.{Region}.amazonaws.com/amazon-ssm-{Region}/ssm-agent-
manifest.json",
        "allowDowngrade": "{{ allowDowngrade }}"
      }
    }
  ]
}
```

スキーマ 1.2

YAML

```
---
runtimeConfig:
  aws:updateSsmAgent:
    properties:
    - agentName: amazon-ssm-agent
      source: https://s3.{Region}.amazonaws.com/aws-ssm-{Region}/manifest.json
      allowDowngrade: "{{ allowDowngrade }}"
```

JSON

```
{
```

```
   "runtimeConfig":{
      "aws:updateSsmAgent":{
         "properties":[
            {
               "agentName":"amazon-ssm-agent",
               "source":"https://s3.{Region}.amazonaws.com/aws-ssm-{Region}/
manifest.json",
               "allowDowngrade":"{{ allowDowngrade }}"
            }
         ]
      }
   }
}
```

プロパティ

agentName

amazon-ssm-agent。これは、リクエストを処理してインスタンス上でコマンドを実行する Systems Manager Agent の名前です。

型: 文字列

必須: はい

allowDowngrade

SSM Agent を以前のバージョンにダウングレードできるようにします。false に設定すると、エージェントは新しいバージョンにのみアップグレードできます (デフォルト)。true に設定すると、以前のバージョンを指定します。

タイプ: ブール値

必須: はい

ソース

Systems Manager がインストールする SSM Agent のバージョンをコピーする場所。この場所は変更できません。

型: 文字列

必須: はい

targetVersion

インストールする SSM Agent の特定のバージョン。指定しない場合、エージェントは最新バージョンに更新されます。

型: 文字列

必須: いいえ

SSM ドキュメントコンテンツを作成する

AWS Systems Manager のパブリックドキュメントが AWS リソースで実行したいすべてのアクションを実行しない場合は、独自の SSM ドキュメントを作成できます。コンソールを使用して SSM ドキュメントのクローンを作成することもできます。ドキュメントのクローンにより、既存のドキュメントから変更可能な新しいドキュメントにコンテンツをコピーします。作成またはクローンするドキュメントは、その内容が 64KB を超えることはできません。このクォータには、ランタイム時に入力パラメータで指定される内容も含みます。新しい `Command` または `Policy` ドキュメントを作成する場合は、ドキュメントの編集、バージョンの自動管理、順序付けなどの最新の機能を利用できるように、スキーマバージョン 2.2 以降を使用することをお勧めします。

SSM ドキュメントコンテンツを書き込む

独自の SSM ドキュメントコンテンツを作成するには、SSM ドキュメントで使用できるさまざまなスキーマ、機能、プラグイン、および構文を理解することが重要です。次のリソースに精通することをお勧めします。

- 独自の AWS Systems Manager ドキュメントを作成する
- データ要素とパラメータ
- スキーマ、機能、および例
- コマンドドキュメントプラグインリファレンス
- Systems Manager Automation アクションのリファレンス
- オートメーションシステム変数
- その他のランブックの例
- AWS Toolkit for Visual Studio Code を使用して、Systems Manager オートメーションランブックを操作する
- オートメーションランブックのビジュアルデザインエクスペリエンス
- ランブックでのスクリプトの使用

AWS の事前に定義された SSM ドキュメントでは、必要なアクションの一部を実行することがあります。これらのドキュメントは、ドキュメントタイプに応じて、カスタム SSM ドキュメント内で、aws:runDocument、aws:runCommand、または aws:executeAutomation プラグインを使用して呼び出すことができます。また、これらのドキュメントの一部をカスタム SSM ドキュメントにコピーし、要件に合わせてコンテンツを編集することもできます。

Tip

SSM ドキュメントコンテンツを作成する場合、テスト中にコンテンツを変更し、SSM ドキュメントを数回更新することがあります。次のコマンドでは、最新のコンテンツで SSM ドキュメントを更新し、ドキュメントのデフォルトバージョンをドキュメントの最新バージョンに更新します。

Note

Linux および Windows のコマンドでは、jq コマンドラインツールを使用して JSON レスポンスデータをフィルタリングします。

Linux & macOS

```
latestDocVersion=$(aws ssm update-document \
    --content file://path/to/file/documentContent.json \
    --name "ExampleDocument" \
    --document-format JSON \
    --document-version '$LATEST' \
    | jq -r '.DocumentDescription.LatestVersion')

aws ssm update-document-default-version \
    --name "ExampleDocument" \
    --document-version $latestDocVersion
```

Windows

```
latestDocVersion=$(aws ssm update-document ^
    --content file://C:\path\to\file\documentContent.json ^
    --name "ExampleDocument" ^
    --document-format JSON ^
    --document-version "$LATEST" ^
    | jq -r '.DocumentDescription.LatestVersion')
```

```
aws ssm update-document-default-version ^
    --name "ExampleDocument" ^
    --document-version $latestDocVersion
```

PowerShell

```
$content = Get-Content -Path "C:\path\to\file\documentContent.json" | Out-
String
$latestDocVersion = Update-SSMDocument `
    -Content $content `
    -Name "ExampleDocument" `
    -DocumentFormat "JSON" `
    -DocumentVersion '$LATEST' `
    | Select-Object -ExpandProperty LatestVersion

Update-SSMDocumentDefaultVersion `
    -Name "ExampleDocument" `
    -DocumentVersion $latestDocVersion
```

SSM ドキュメントの複製

Systems Manager のドキュメントコンソールを使用して、AWS Systems Manager のドキュメントのクローンを作成し、SSM ドキュメントを作成できます。SSM ドキュメントの複製により、既存のドキュメントから変更可能な新しいドキュメントにコンテンツをコピーします。64KB を超えるドキュメントをクローンすることはできません。

SSM ドキュメントを複製するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[ドキュメント] を選択します。
3. 検索ボックスに、複製するドキュメントの名前を入力します。
4. 複製するドキュメントの名前を選択し、「アクション」ドロップダウンで「ドキュメントの複製」を選択します。
5. 必要に応じてドキュメントを変更し、[ドキュメントの作成] を選択してドキュメントを保存します。

SSM ドキュメントコンテンツを作成したら、次のいずれかの方法を使用して、コンテンツを使って SSM ドキュメントを作成できます。

SSM ドキュメントを作成する

- 複合ドキュメントの作成

複合ドキュメントの作成

複合 AWS Systems Manager (SSM) ドキュメントは、1 つまたは複数のセカンダリ SSM ドキュメントを実行して一連のアクションを実行するカスタムドキュメントです。複合ドキュメントは、ブートストラップソフトウェアやドメイン結合インスタンスなどの一般的なタスク用の標準 SSM ドキュメントセットを作成できるようにすることで、Infrastructure as Code (コードとしてのインフラストラクチャ)を推進します。これらのドキュメントを同じ AWS リージョン の AWS アカウント 間で共有して、SSM ドキュメントのメンテナンスを減らし、整合性を確保することができます。

たとえば、次のアクションを実行する複合ドキュメントを作成できます。

1. 許可リストのすべてのパッチをインストールする。
2. ウイルス対策ソフトウェアをインストールする。
3. GitHub からスクリプトをダウンロードして実行する。

この例では、カスタム SSM ドキュメントに以下のアクションを実行するためのプラグインが含まれています。

1. `AWS-RunPatchBaseline` ドキュメントを実行する `aws:runDocument` プラグインは、すべての許可されたリストのパッチをインストールします。
2. `aws:runDocument` ドキュメントを実行する `AWS-InstallApplication` プラグインは、ウイルス対策ソフトウェアをインストールします。
3. `aws:downloadContent` プラグインは、GitHub からスクリプトをダウンロードして実行します。

複合ドキュメントとセカンダリドキュメントは、Systems Manager、GitHub (パブリックおよびプライベートリポジトリ)、または Amazon S3 に保存できます。複合ドキュメントおよびセカンダリドキュメントは JSON あるいは YAML で作成できます。

> **Note**
>
> 複合ドキュメントは最大 3 階層のドキュメントまでしか実行できません。つまり、複合ドキュメントは子ドキュメントを呼び出すことができます。その子ドキュメントは最後の 1 つのドキュメントを呼び出すことができます。

複合ドキュメントを作成するには、カスタム SSM ドキュメントで aws:runDocument プラグインを開き、必要な入力を指定します。以下に、次のアクションを実行する複合ドキュメントの例を示します。

1. aws:downloadContent プラグインを実行して、GitHub パブリックリポジトリからブートストラップというローカルディレクトリに SSM ドキュメントをダウンロードします。SSM ドキュメントは StateManagerBootstrap.yml (YAML ドキュメント) と呼ばれます。
2. aws:runDocument プラグインを実行して StateManagerBootstrap.yml ドキュメントを実行します。パラメータは指定されません。
3. aws:runDocument プラグインを実行して AWS-ConfigureDocker pre-defined SSM ドキュメントを実行します。指定されたパラメータが、インスタンスに Docker をインストールします。

```
{
  "schemaVersion": "2.2",
  "description": "My composite document for bootstrapping software and installing
 Docker.",
  "parameters": {
  },
  "mainSteps": [
    {
      "action": "aws:downloadContent",
      "name": "downloadContent",
      "inputs": {
        "sourceType": "GitHub",
        "sourceInfo": "{\"owner\":\"TestUser1\",\"repository\":\"TestPublic\", \"path
\":\"documents/bootstrap/StateManagerBootstrap.yml\"}",
        "destinationPath": "bootstrap"
      }
    },
    {
      "action": "aws:runDocument",
```

```
      "name": "runDocument",
      "inputs": {
        "documentType": "LocalPath",
        "documentPath": "bootstrap",
        "documentParameters": "{}"
      }
    },
    {
      "action": "aws:runDocument",
      "name": "configureDocker",
      "inputs": {
        "documentType": "SSMDocument",
        "documentPath": "AWS-ConfigureDocker",
        "documentParameters": "{\"action\":\"Install\"}"
      }
    }
  ]
}
```

詳細情報

- Run Command を使用してスクリプトを呼び出すときに使用するサーバーとインスタンスの再起動については、「コマンド実行時の再起動の処理」を参照してください。
- カスタム SSM ドキュメントに追加できるプラグインの詳細については、「コマンドドキュメントプラグインリファレンス」を参照してください。
- 複合ドキュメントを作成せずにリモートロケーションからドキュメントを実行するだけの場合は、「遠隔で ドキュメントを実行する」を参照してください。

ドキュメントでの作業

このセクションには、SSM ドキュメントの使用方法と操作方法に関する情報が含まれています。

トピック

- SSM ドキュメントのバージョンを比較する
- SSM ドキュメントを作成する
- カスタム SSM ドキュメントの削除
- 遠隔で ドキュメントを実行する
- SSM ドキュメントの共有
- SSM ドキュメントを検索する

SSM ドキュメントのバージョンを比較する

Systems Manager ドキュメントコンソールで、AWS Systems Manager (SSM) ドキュメントのバージョン間のコンテンツの違いを比較できます。SSM ドキュメントのバージョンを比較するときは、バージョンのコンテンツの違いが強調表示されます。

SSM ドキュメントのコンテンツを比較する (コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[ドキュメント] を選択します。
3. ドキュメントのリストから、コンテンツを比較するドキュメントを選択します。
4. [Content] (コンテンツ) タブで [Compare versions] (バージョンを比較) をクリックして、コンテンツを比較するドキュメントのバージョンを選択します。

SSM ドキュメントを作成する

カスタム SSM ドキュメントのコンテンツを作成した後、SSM ドキュメントコンテンツを書き込むの説明に従って Systems Manager コンソールを使用し、コンテンツを使って SSM ドキュメントを作成できます。

SSM ドキュメントを作成するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[ドキュメント] を選択します。
3. [Create command or session (コマンドまたはセッションの作成)] を選択します。
4. ドキュメントの説明的な名前を入力します。
5. (オプション) [Target type (ターゲットタイプ)] で、ドキュメントを実行できるリソースの種類を指定します。
6. [ドキュメントタイプ] リストで、作成するドキュメントのタイプを選択します。
7. [Content (コンテンツ)] フィールドの括弧を削除した後に、先に作成したドキュメントコンテンツを貼り付けます。
8. (オプション) [Document tags (ドキュメントタグ)] セクションで、1 つ以上のタグキーの名前と値のペアをドキュメントに適用します。

タグは、リソースに割り当てるオプションのメタデータです。タグを使用すると、目的、所有者、環境などのさまざまな方法でリソースを分類できます。たとえば、ドキュメントにタグを付けて、ドキュメントが実行するタスクの種類、ターゲットとするオペレーティングシステムの種類、およびドキュメントが動作する環境を指定できます。この場合、以下のキーの名前と値のペアを指定します。

- `Key=TaskType,Value=MyConfigurationUpdate`
- `Key=OS,Value=AMAZON_LINUX_2`
- `Key=Environment,Value=Production`

9. [ドキュメントの作成] を選択してドキュメントを保存します。

カスタム SSM ドキュメントの削除

カスタム SSM ドキュメントを使用する必要がなくなった場合は、AWS Systems Manager コンソールを使用して削除できます。

SSM ドキュメントを削除するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[ドキュメント] を選択します。
3. 削除したいドキュメントを選択します。
4. [削除] を選択します。ドキュメントを削除するように求められたら、[削除] を選択します。

コマンドラインツールまたは SDK を使用して SSM ドキュメントを削除する例については、「AWS SDK または CLI で `DeleteDocument` を使用する」を参照してください。

遠隔で ドキュメントを実行する

`AWS-RunDocument` 事前定義 SSM ドキュメントを使用すると、リモートの場所から AWS Systems Manager (SSM) ドキュメントを実行できます。このドキュメントでは、次の場所に保存されている SSM ドキュメントの実行がサポートされています。

- パブリックおよびプライベート GitHub リポジトリ (GitHub Enterprise はサポートされていません)
- Amazon S3 バケット
- Systems Manager

AWS Systems Manager のツールである State Manager または Automation を使用してリモートドキュメントを実行することもできますが、次の手順では、Systems Manager コンソールで AWS Systems Manager Run Command を使用してリモート SSM ドキュメントを実行する方法のみを説明します。

> **Note**
>
> AWS-RunDocument は、コマンドタイプの SSM ドキュメントのみを実行するために使用でき、Automation ランブックなど他のタイプは実行できません。AWS-RunDocument は、aws:downloadContent プラグインを使用します。aws:downloadContent の詳細については、「aws:downloadContent」を参照してください。

開始する前に

リモートドキュメントを実行する前に、次のタスクを完了する必要があります。

- SSM コマンドドキュメントを作成し、リモートの場所に保存します。詳細については、「SSM ドキュメントコンテンツを作成する」を参照してください。
- プライベート GitHub リポジトリに保存されているリモートドキュメントを実行する場合は、GitHub セキュリティアクセストークンの Systems Manager SecureString パラメータを作成する必要があります。SSH 経由でトークンを手動で渡すことで、プライベート GitHub リポジトリのリモートドキュメントにアクセスすることはできません。アクセストークンは、Systems Manager SecureString パラメータとして渡す必要があります。SecureString パラメータの作成の詳細については、「Systems Manager での Parameter Store パラメータの作成」を参照してください。

リモートドキュメントを実行する (コンソール)

リモートドキュメントを実行するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Run Command] を選択します。
3. [Run command (コマンドの実行)] を選択します。
4. [Document (ドキュメント)] リストで、[**AWS-RunDocument**] を選択します。

5. [Command parameters (コマンドパラメータ)] で、[Source Type (ソースタイプ)] としてオプションを選択します。

   - [GitHub] を選択した場合は、[ソース情報] の情報を次の形式で指定します。

     ```
     {
         "owner": "owner_name",
         "repository": "repository_name",
         "path": "path_to_document",
         "getOptions":"branch:branch_name",
         "tokenInfo": "{{ssm-secure:secure-string-token}}"
     }
     ```

     例：

     ```
     {
         "owner":"TestUser",
         "repository":"GitHubTestExamples",
         "path":"scripts/python/test-script",
         "getOptions":"branch:exampleBranch",
         "tokenInfo":"{{ssm-secure:my-secure-string-token}}"
     }
     ```

     > **Note**
     >
     > getOptions は、マスター以外のブランチまたはリポジトリ内の特定のコミットからコンテンツを取得するための追加オプションです。マスターブランチで最新のコミットを使用している場合は、getOptions を省略できます。branch は、SSM ドキュメントが master 以外のブランチに保存されている場合にのみ必要です。
     > リポジトリ内の特定のコミットにあるバージョンの SSM ドキュメントを使用するには、commitID ではなく、getOptions を指定して branch を使用します。以下に例を示します。
     >
     > ```
     > "getOptions": "commitID:bbc1ddb94...b76d3bEXAMPLE",
     > ```

   - [S3] を選択した場合は、[Source Info] 情報を次の形式で指定します。

     ```
     {"path":"URL_to_document_in_S3"}
     ```

以下に例を示します。

```
{"path":"https://s3.amazonaws.com/amzn-s3-demo-bucket/scripts/ruby/
mySSMdoc.json"}
```

- [SSMDocument] を選択した場合は、[Source Info] 情報を次の形式で指定します。

```
{"name": "document_name"}
```

以下に例を示します。

```
{"name": "mySSMdoc"}
```

6. [Document Parameters] フィールドに、リモート SSM ドキュメントのパラメータを入力します。例えば、AWS-RunPowerShell ドキュメントを実行する場合、以下を指定できます。

```
{"commands": ["date", "echo \"Hello World\""]}
```

AWS-ConfigureAWSPack ドキュメントを実行する場合は、以下を指定できます。

```
{
   "action":"Install",
   "name":"AWSPVDriver"
}
```

7. [Targets] (ターゲット) セクションで、タグの指定、インスタンスやエッジデバイスの手動選択、リソースグループの指定により、このオペレーションを実行するマネージドノードを選択します。

> **Tip**
>
> 表示されるはずのマネージドノードが表示されない場合は、トラブルシューティングのヒントについて「マネージドノードの可用性のトラブルシューティング」を参照してください。

8. [その他のパラメータ] で、以下の操作を行います。

- [コメント] に、このコマンドに関する情報を入力します。

- [タイムアウト (秒)] に、コマンドの実行全体が失敗するまでにシステムが待機する秒数を指定します。

9. [レート制御] の場合:

   - [同時実行数] の場合、コマンドを同時に実行するマネージドノードの数または割合を指定します。

     > **Note**
     >
     > マネージドノードに適用されるタグを指定するか、AWS リソースグループを指定してターゲットを選択し、ターゲットとなるマネージドノードの数が不明な場合は、割合を指定してドキュメントを同時に実行できるターゲットの数を制限します。

   - [エラーのしきい値] で、ノードの数または割合のいずれかで失敗した後、他のマネージドノードでのコマンドの実行をいつ停止するか指定します。例えば、3 つのエラーを指定した場合、4 番目のエラーが受信されると、システムマネージャー はコマンドの送信を停止します。コマンドを処理しているマネージドノードもエラーを送信する可能性があります。

10. (オプション) コマンド出力をファイルに保存する場合は、[出力オプション] の [S3 バケットにコマンド出力を書き込む] ボックスを選択します。ボックスにバケット名とプレフィックス (フォルダ) 名を入力します。

    > **Note**
    >
    > S3 バケットにデータを書き込む機能を許可する S3 許可は、このタスクを実行する IAM ユーザーのものではなく、インスタンスに割り当てられたインスタンスプロファイル (EC2 インスタンスの場合) または IAM サービスロール (ハイブリッドアクティベーションマシン) のものです。詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」または「ハイブリッド環境に IAM サービスロールを作成する」を参照してください。さらに、指定された S3 バケットが別の AWS アカウント にある場合は、マネージドノードに関連付けられたインスタンスプロファイルまたは IAM サービスロールが、そのバケットへの書き込みに必要なアクセス許可があることを確認してください。

11. [SNS Notifications (SNS 通知)] セクションで、コマンドの実行状態に関する通知を受け取る場合は、[Enable SNS notifications (SNS 通知を有効にする)] チェックボックスをオンにします。

Run Command 用の Amazon SNS 通知の設定の詳細については、「Amazon SNS 通知を使用した Systems Manager のステータス変更のモニタリング」を参照してください。

12. [Run (実行)] を選択します。

> **Note**
>
> Run Command を使用してスクリプトを呼び出すときに使用するサーバーとインスタンスの再起動については、「コマンド実行時の再起動の処理」を参照してください。

SSM ドキュメントの共有

AWS Systems Manager (SSM) ドキュメントは、同じ AWS リージョン のアカウントとプライベートに共有することも、パブリックに共有することもできます。ドキュメントをプライベートに共有するには、ドキュメントのアクセス許可を変更して、特定の人物が AWS アカウント ID に基づいてドキュメントにアクセスできるようにします。SSM ドキュメントをパブリックに共有するには、ドキュメントのアクセス許可を変更し、[All] を指定します。ドキュメントをパブリックとプライベートで同時に共有することはできません。

> **Warning**
>
> 信頼できるソースの共有 SSM ドキュメントのみ使用してください。共有ドキュメントを使用するときは、使用する前にドキュメントのコンテンツを慎重に確認し、インデックスの設定がどのように変わるかを理解してください。共有ドキュメントのベストプラクティスの詳細については、「共有 SSM ドキュメントのベストプラクティス」を参照してください。

制限

SSM ドキュメントの作業を始めるときは、次の制限事項に注意してください。

- 所有者のみがドキュメントを共有できます。
- ドキュメントを削除するには、その前にドキュメントの共有を停止する必要があります。詳細については、「共有 SSM ドキュメントのアクセス許可を変更する」を参照してください。
- 最大 1000 個の でドキュメントを共有できますAWS アカウント この制限の引き上げをリクエストするには、サポート センターまでお問い合わせください。[制限のタイプ] で、[EC2 Systems Manager] を選択し、リクエストの理由を入力します。

- パブリックに最大 5 件の SSM ドキュメントを共有できます。この制限の引き上げをリクエストするには、サポート センターまでお問い合わせください。[制限のタイプ] で、[EC2 Systems Manager] を選択し、リクエストの理由を入力します。
- ドキュメントは、同じ AWS リージョン の他のアカウントとのみ共有できます。クロスリージョン共有はサポートされていません。

> **Important**
>
> Systems Manager において、Amazon 所有の SSM ドキュメントとは、Amazon Web Services 自体によって作成および管理されているドキュメントです。Amazon 所有のドキュメントでは、ドキュメント名に `AWS-*` のようなプレフィックスが含まれます。ドキュメントの所有者は、AWS 内の特定のユーザーアカウントではなく Amazon と見なされます。これらのドキュメントは公開されており、誰でも使用できます。

Systems Manager のService Quotas の詳細については、「AWS Systems Manager の Service Quotas」を参照してください。

目次

- 共有 SSM ドキュメントのベストプラクティス
- SSM ドキュメントのパブリック共有をブロックする
- SSM ドキュメントを共有する
- 共有 SSM ドキュメントのアクセス許可を変更する
- 共有 SSM ドキュメントを使用する

共有 SSM ドキュメントのベストプラクティス

共有ドキュメントを共有したり使用したりする前に、次のガイドラインを確認してください。

機密情報を削除する

AWS Systems Manager (SSM) ドキュメントを慎重に確認して、機密情報があればそれを削除します。例えば、ドキュメントに AWS 認証情報が含まれていないことを確認します。特定のユーザーとドキュメントを共有する場合、そのユーザーはドキュメント内の情報を表示することができます。パブリックにドキュメントを共有する場合、誰でもドキュメント内の情報を表示することができます。

ドキュメントのパブリック共有をブロックする

アカウント内のすべてのパブリック共有されている SSM ドキュメントを確認し、共有を継続するかどうかを確認します。特定のドキュメントのパブリック共有を停止するには、このトピックの 共有 SSM ドキュメントのアクセス許可を変更する セクションで説明しているように、そのドキュメントのアクセス許可設定を変更する必要があります。パブリック共有ブロック設定を有効にしても、現在パブリック共有しているドキュメントには影響しません。ユースケースでパブリック共有を有効にする必要がある場合を除き、Systems Manager ドキュメントコンソールの [詳細設定] セクションで、SSM ドキュメントのパブリック共有ブロック設定をオンにすることをお勧めします。この設定をオンにすると、SSM ドキュメントへの不要なアクセスを防止できます。パブリック共有のブロック設定は、アカウントレベルの設定で、各 AWS リージョン で異なる可能性があります。

IAM 信頼ポリシーを使用して Run Command アクションを制限する

ドキュメントにアクセスできるユーザーに対する制限付き AWS Identity and Access Management (IAM) ポリシーを作成します。IAM ポリシーにより、ユーザーが Amazon Elastic Compute Cloud (Amazon EC2) コンソールで表示できるか、AWS Command Line Interface (AWS CLI) または AWS Tools for Windows PowerShell で `ListDocuments` を呼び出して表示できる SSM ドキュメントが決まります。このポリシーでは、SSM ドキュメントに対してユーザーが実行できるアクションも制限されます。制限付きポリシーを作成し、ユーザーが特定のドキュメントのみを表示するようにできます。詳細については、「カスタマーマネージドポリシーの例」を参照してください。

共有 SSM ドキュメントを使用する際の注意事項

インスタンスで実行されるコマンドを理解するために、共有されている各ドキュメント (特にパブリックドキュメント) のコンテンツを確認します。ドキュメントは、実行後に意図的または非意図的に悪影響を及ぼすことがあります。ドキュメントが外部ネットワークを参照している場合、ドキュメントを使用する前に外部ソースを確認してください。

ドキュメントハッシュを使用してコマンドを送信する

ドキュメントを共有する場合、システムは Sha-256 ハッシュを作成し、それをドキュメントに割り当てます。また、システムはドキュメントコンテンツのスナップショットを保存します。共有ドキュメントを使用してコマンドを送信するときは、コマンドでハッシュを指定して、次の条件が確実に該当するようにできます。

- 正しい Systems Manager ドキュメントからコマンドを実行している
- ドキュメントが自分と共有されてからコンテンツが変更されていない

ハッシュが、指定されたドキュメントと一致しない場合、または共有ドキュメントのコンテンツが変更されている場合、コマンドは `InvalidDocument` 例外を返します。ハッシュは、外部の場所からドキュメントのコンテンツを確認することはできません。

SSM ドキュメントのパブリック共有をブロックする

開始する前に、AWS アカウント でパブリック共有されている SSM ドキュメントをすべて確認し、共有を継続するかどうかを確認します。特定の SSM ドキュメントのパブリック共有を停止するには、このトピックの 共有 SSM ドキュメントのアクセス許可を変更する セクションで説明しているように、そのドキュメントのアクセス許可設定を変更する必要があります。パブリック共有ブロック設定を有効にしても、現在パブリック共有している SSM ドキュメントには影響しません。パブリック共有ブロック設定を有効にすると、追加の SSM ドキュメントをパブリック共有できなくなります。

ユースケースでパブリック共有を有効にする必要がある場合を除き、SSM ドキュメントのパブリック共有ブロック設定をオンにすることをお勧めします。この設定をオンにすると、SSM ドキュメントへの不要なアクセスを防止できます。パブリック共有のブロック設定は、アカウントレベルの設定で、各 AWS リージョン で異なる可能性があります。現在共有していない SSM ドキュメントについてパブリック共有をブロックするには、次のタスクを完了します。

パブリック共有のブロック (コンソール)

SSM ドキュメントのパブリック共有をブロックするには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[ドキュメント] を選択します。
3. [Preferences (設定)] を選択してから、パブリック共有のブロックセクションにある [編集] を選択します。
4. [パブリック共有のブロック] のチェックボックスを選択してから、[保存]を選択します。

パブリック共有のブロック (コマンドライン)

AWS Command Line Interface(AWS CLI) を開く、またはローカルコンピュータの AWS Tools for Windows PowerShellを開き、以下のコマンドを実行してSSM ドキュメントのパブリック共有をブロックします。

Linux & macOS

```
aws ssm update-service-setting  \
    --setting-id /ssm/documents/console/public-sharing-permission \
    --setting-value Disable \
    --region 'The AWS ##### you want to block public sharing in'
```

Windows

```
aws ssm update-service-setting ^
    --setting-id /ssm/documents/console/public-sharing-permission ^
    --setting-value Disable ^
    --region "The AWS ##### you want to block public sharing in"
```

PowerShell

```
Update-SSMServiceSetting `
    -SettingId /ssm/documents/console/public-sharing-permission `
    -SettingValue Disable `
    -Region The AWS ##### you want to block public sharing in
```

以下のコマンドで、設定値が更新されたことを確認します。

Linux & macOS

```
aws ssm get-service-setting   \
    --setting-id /ssm/documents/console/public-sharing-permission \
    --region The AWS ##### you blocked public sharing in
```

Windows

```
aws ssm get-service-setting  ^
    --setting-id /ssm/documents/console/public-sharing-permission ^
    --region "The AWS ##### you blocked public sharing in"
```

PowerShell

```
Get-SSMServiceSetting `
    -SettingId /ssm/documents/console/public-sharing-permission `
    -Region The AWS ##### you blocked public sharing in
```

IAM によるパブリック共有をブロックするためのアクセスの制限

AWS Identity and Access Management (IAM) ポリシーを作成して、ユーザーによるパブリック共有のブロック設定の変更を制限します。これにより、SSM ドキュメントへの不要なアクセスをユーザーが許可できなくなります。

以下は、ユーザーがパブリック共有をブロックする設定を更新できないようにする IAM ポリシーの例です。この例を使用するには、Amazon Web Services のアカウント ID の例を自分のアカウント ID に置き換える必要があります。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "ssm:UpdateServiceSetting",
            "Resource": "arn:aws:ssm:*:987654321098:servicesetting/ssm/documents/
console/public-sharing-permission"
        }
    ]
}
```

SSM ドキュメントを共有する

Systems Manager コンソールを使用して AWS Systems Manager (SSM) ドキュメントを共有できます。コンソールからドキュメントを共有する場合、共有できるのはドキュメントのデフォルトバージョンのみです。また、AWS Command Line Interface (AWS CLI)、AWS Tools for Windows PowerShell、または AWS SDK を使用して、`ModifyDocumentPermission` API オペレーションを呼び出すことで、プログラムで SSM ドキュメントを共有することもできます。ドキュメントを共有する前に、共有するユーザーの AWS アカウント ID を取得します。ドキュメントを共有する場合に、これらのアカウント ID を指定します。

ドキュメントを共有する (コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[ドキュメント] を選択します。
3. ドキュメントリストで共有するドキュメントを選択し、[詳細を表示] を選択します。[Permissions] タブで自分がドキュメントの所有者であることを確認します。ドキュメントの所有者のみがドキュメントを共有できます。

4. [Edit] を選択します。
5. コマンドをパブリックに共有するには、[Public] を選択し、[Save] を選択します。コマンドをプライベートに共有するには、[Private (プライベート)] を選択し、AWS アカウント ID を入力します。次に、[Add permission (アクセス権限の追加)] を選択し、[Save (保存)] を選択します。

ドキュメントの共有 (コマンドライン)

次の手順では、コマンドラインセッションの AWS リージョン を指定する必要があります。

1. ローカルコンピュータで AWS CLI または AWS Tools for Windows PowerShell を開き、以下のコマンドを実行して認証情報を指定します。

   次のコマンドで、*[Region]* (リージョン) をユーザー自身の情報に置き換えます。サポートされている *region* 値の一覧については、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」にある Region 列を参照してください。

   Linux & macOS

   ```
   aws config

   AWS Access Key ID: [your key]
   AWS Secret Access Key: [your key]
   Default region name: region
   Default output format [None]:
   ```

   Windows

   ```
   aws config

   AWS Access Key ID: [your key]
   AWS Secret Access Key: [your key]
   Default region name: region
   Default output format [None]:
   ```

   PowerShell

   ```
   Set-AWSCredentials -AccessKey your key -SecretKey your key
   Set-DefaultAWSRegion -Region region
   ```

2. 次のコマンドを使用して、使用可能なすべての SSM ドキュメントの一覧を表示します。一覧には、作成したドキュメント、および自分と共有されたドキュメントが含まれます。

   Linux & macOS

   ```
   aws ssm list-documents
   ```

   Windows

   ```
   aws ssm list-documents
   ```

   PowerShell

   ```
   Get-SSMDocumentList
   ```

3. 特定のドキュメントを取得するには、次のコマンドを使用します。

   Linux & macOS

   ```
   aws ssm get-document \
       --name document name
   ```

   Windows

   ```
   aws ssm get-document ^
       --name document name
   ```

   PowerShell

   ```
   Get-SSMDocument `
       -Name document name
   ```

4. ドキュメントの説明を表示するには、次のコマンドを使用します。

   Linux & macOS

   ```
   aws ssm describe-document \
       --name document name
   ```

Windows

```
aws ssm describe-document ^
    --name document name
```

PowerShell

```
Get-SSMDocumentDescription `
    -Name document name
```

5. ドキュメントのアクセス権限を表示するには、次のコマンドを使用します。

Linux & macOS

```
aws ssm describe-document-permission \
    --name document name \
    --permission-type Share
```

Windows

```
aws ssm describe-document-permission ^
    --name document name ^
    --permission-type Share
```

PowerShell

```
Get-SSMDocumentPermission `
    -Name document name `
    -PermissionType Share
```

6. ドキュメントのアクセス権限を変更して共有するには、次のコマンドを使用します。アクセス権限を編集するには、ドキュメントの所有者である必要があります。オプションで、特定の AWS アカウント ID と共有するドキュメントの場合は、`--shared-document-version` パラメータを使用して共有するドキュメントのバージョンを指定できます。バージョンを指定しない場合、ドキュメント の `Default` バージョンが共有されます。ドキュメントをパブリックに (`all` と) 共有する場合は、指定したドキュメントのすべてのバージョンがデフォルトで共有されます。次のコマンド例は、特定の個人の AWS アカウント ID に基づいて、その個人とドキュメントをプライベートに共有します。

Linux & macOS

```
aws ssm modify-document-permission \
    --name document name \
    --permission-type Share \
    --account-ids-to-add AWS ##### ID
```

Windows

```
aws ssm modify-document-permission ^
    --name document name ^
    --permission-type Share ^
    --account-ids-to-add AWS ##### ID
```

PowerShell

```
Edit-SSMDocumentPermission `
    -Name document name `
    -PermissionType Share `
    -AccountIdsToAdd AWS ##### ID
```

7. 次のコマンドを使用してドキュメントをパブリックに共有します。

> **Note**
>
> ドキュメントをパブリックに (all と) 共有する場合は、指定したドキュメントのすべてのバージョンがデフォルトで共有されます。

Linux & macOS

```
aws ssm modify-document-permission \
    --name document name \
    --permission-type Share \
    --account-ids-to-add 'all'
```

Windows

```
aws ssm modify-document-permission ^
```

```
    --name document name ^
    --permission-type Share ^
    --account-ids-to-add "all"
```

PowerShell

```
Edit-SSMDocumentPermission `
    -Name document name `
    -PermissionType Share `
    -AccountIdsToAdd ('all')
```

共有 SSM ドキュメントのアクセス許可を変更する

コマンドを共有する場合、AWS Systems Manager (SSM) ドキュメントへのアクセス権を削除するか、SSM ドキュメントを削除するまで、そのコマンドを表示および使用できます。ただし、共有されている限り、ドキュメントを削除することはできません。ドキュメントを削除する前に、共有を停止する必要があります。

ドキュメント共有の停止 (コンソール)

ドキュメント共有の停止

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[ドキュメント] を選択します。
3. ドキュメントリストで共有を停止するドキュメントを選択し、[詳細] を選択します。[アクセス許可] セクションで自分がドキュメントの所有者であることを確認します。ドキュメントの所有者のみが、ドキュメントの共有を停止できます。
4. [Edit] を選択します。
5. [X] を選択してコマンドへのアクセス権を取り消す AWS アカウント ID を削除し、[Save] を選択します。

ドキュメントの共有の停止 (コマンドライン)

ローカルコンピュータで AWS CLI または AWS Tools for Windows PowerShell を開き、次のコマンドを実行してコマンドの共有を停止します。

Linux & macOS

```
aws ssm modify-document-permission \
    --name document name \
    --permission-type Share \
    --account-ids-to-remove 'AWS ##### ID'
```

Windows

```
aws ssm modify-document-permission ^
    --name document name ^
    --permission-type Share ^
    --account-ids-to-remove "AWS ##### ID"
```

PowerShell

```
Edit-SSMDocumentPermission `
    -Name document name `
    -PermissionType Share `
    -AccountIdsToRemove AWS ##### ID
```

共有 SSM ドキュメントを使用する

AWS Systems Manager (SSM) ドキュメントを共有すると、システムは Amazon リソースネーム (ARN) を生成して、コマンドに割り当てます。Systems Manager コンソールから共有ドキュメントを選択して実行する場合、ARN は表示されません。ただし、Systems Manager コンソール以外の方法を使用して共有 SSM ドキュメントを実行する場合は、DocumentName リクエストパラメータにドキュメントの完全な ARN を指定する必要があります。コマンドを実行してドキュメントをリストすると、SSM ドキュメントの完全な ARN が表示されます。

> **Note**
>
> AWS のパブリックドキュメント (先頭に AWS-* が付くドキュメント)、または自己所有のドキュメントに ARN を指定する必要はありません。

共有 SSM ドキュメントを使用する (コマンドライン)

すべてのパブリック SSM ドキュメントをリスト表示するには

Linux & macOS

```
aws ssm list-documents \
    --filters Key=Owner,Values=Public
```

Windows

```
aws ssm list-documents ^
    --filters Key=Owner,Values=Public
```

PowerShell

```
$filter = New-Object Amazon.SimpleSystemsManagement.Model.DocumentKeyValuesFilter
$filter.Key = "Owner"
$filter.Values = "Public"

Get-SSMDocumentList `
    -Filters @($filter)
```

自分と共有されているプライベート SSM ドキュメントをリスト表示するには

Linux & macOS

```
aws ssm list-documents \
    --filters Key=Owner,Values=Private
```

Windows

```
aws ssm list-documents ^
    --filters Key=Owner,Values=Private
```

PowerShell

```
$filter = New-Object Amazon.SimpleSystemsManagement.Model.DocumentKeyValuesFilter
$filter.Key = "Owner"
$filter.Values = "Private"

Get-SSMDocumentList `
    -Filters @($filter)
```

使用できるすべての SSM ドキュメントをリスト表示するには

Linux & macOS

```
aws ssm list-documents
```

Windows

```
aws ssm list-documents
```

PowerShell

```
Get-SSMDocumentList
```

自分と共有されている SSM ドキュメントについての情報を入手するには

Linux & macOS

```
aws ssm describe-document \
    --name arn:aws:ssm:us-east-2:12345678912:document/documentName
```

Windows

```
aws ssm describe-document ^
    --name arn:aws:ssm:us-east-2:12345678912:document/documentName
```

PowerShell

```
Get-SSMDocumentDescription `
    -Name arn:aws:ssm:us-east-2:12345678912:document/documentName
```

共有 SSM ドキュメントを実行するには

Linux & macOS

```
aws ssm send-command \
    --document-name arn:aws:ssm:us-east-2:12345678912:document/documentName \
```

```
    --instance-ids ID
```

Windows

```
aws ssm send-command ^
    --document-name arn:aws:ssm:us-east-2:12345678912:document/documentName ^
    --instance-ids ID
```

PowerShell

```
Send-SSMCommand `
    -DocumentName arn:aws:ssm:us-east-2:12345678912:document/documentName `
    -InstanceIds ID
```

SSM ドキュメントを検索する

AWS Systems Manager (SSM) ドキュメントストアでは、フリーテキスト検索やフィルターによる検索を使用して、SSM ドキュメントを検索することができます。また、頻繁に使用する SSM ドキュメントを見つけるのに役立つように、ドキュメントをお気に入りに追加することもできます。ここでは、これらを使用する方法について説明します。

フリーテキスト検索の使用

Systems Manager の [ドキュメント] ページの検索ボックスでは、フリーテキスト検索がサポートされています。フリーテキスト検索では、入力した検索語を各 SSM ドキュメントのドキュメント名と比較します。例えば、「**ansible**」という 1 つの検索語を入力すると、Systems Manager はこの語を含むすべての SSM ドキュメントを返します。複数の検索語を入力すると、Systems Manager は OR ステートメントを使用して検索します。例えば、**ansible** と **linux** を指定すると、名前にどちらかの検索語を含むすべてのドキュメントが返されます。

フリーテキスト検索用語を入力して [Platform type] (プラットフォームタイプ) などの検索オプションを選択する場合は、検索が AND 文を使用して、名前に指定したキーワードが含まれ、かつ指定したプラットフォームタイプのすべてのドキュメントを返します。

> **Note**
>
> フリーテキスト検索では、次の点に注意してください。
>
> - フリーテキスト検索では、大文字と小文字は区別されません。
> - 検索語は 3～20 文字にする必要があります。

- フリーテキスト検索では、検索語を 5 つまで使用できます。
- 検索語の間にスペースを入れると、検索時にスペースが含まれます。
- フリーテキスト検索は、[Document type (ドキュメントタイプ)] や [Platform type (プラットフォームタイプ)] などの他の検索オプションと組み合わせることができます。
- [Document name prefix (ドキュメント名のプレフィックス)] フィルターとフリーテキスト検索は一緒に使用できません。

SSM ドキュメントを検索するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[ドキュメント] を選択します。
3. 検索ボックスに検索語を入力し、Enter キーを押します。

AWS CLI を使用したドキュメントのフリーテキスト検索の実行

CLI を使用してドキュメントのフリーテキスト検索を実行するには

1. まだ AWS Command Line Interface (AWS CLI) をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」を参照してください。
2. 1 つの検索語でドキュメントのフリーテキスト検索を実行するには、次のコマンドを実行します。このコマンドの *search_term* を使用する検索語に置き換えてください。

   ```
   aws ssm list-documents --filters Key="SearchKeyword",Values="search_term"
   ```

   以下に例を示します。

   ```
   aws ssm list-documents --filters Key="SearchKeyword",Values="aws-asg" --region us-east-2
   ```

   複数の検索語を使用して AND 演算で検索するには、次のコマンドを実行します。このコマンドの *search_term_1* と *search_term_2* を使用する検索語に置き換えてください。

```
aws ssm list-documents --filters
 Key="SearchKeyword",Values="search_term_1","search_term_2","search_term_3" --
region us-east-2
```

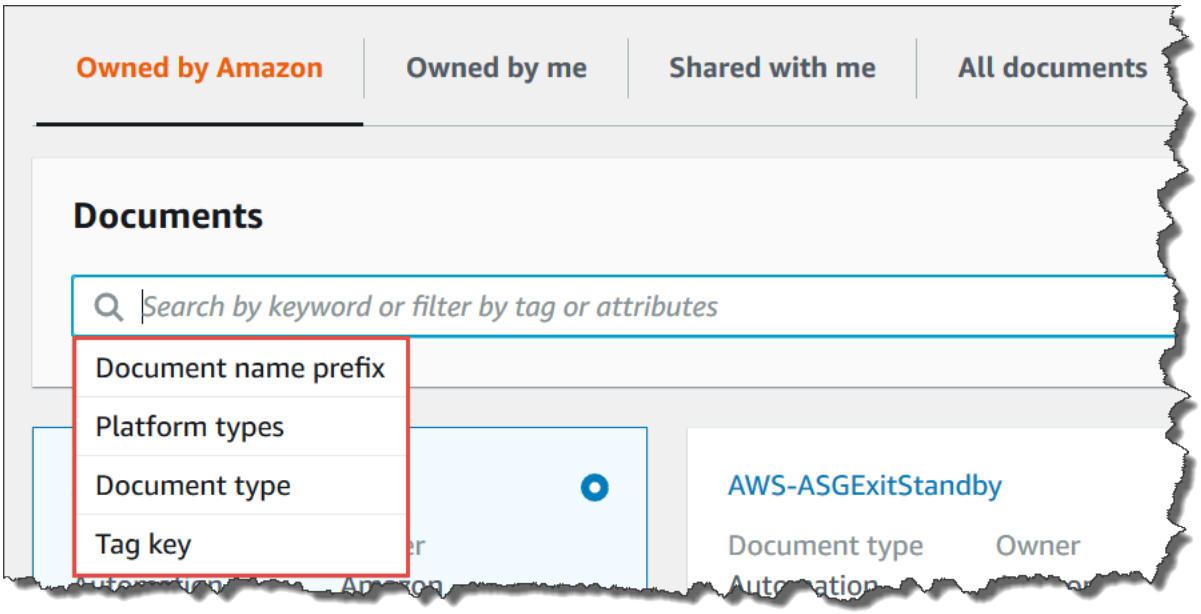
以下に例を示します。

```
aws ssm list-documents --filters Key="SearchKeyword",Values="aws-asg","aws-
ec2","restart" --region us-east-2
```

フィルターの使用

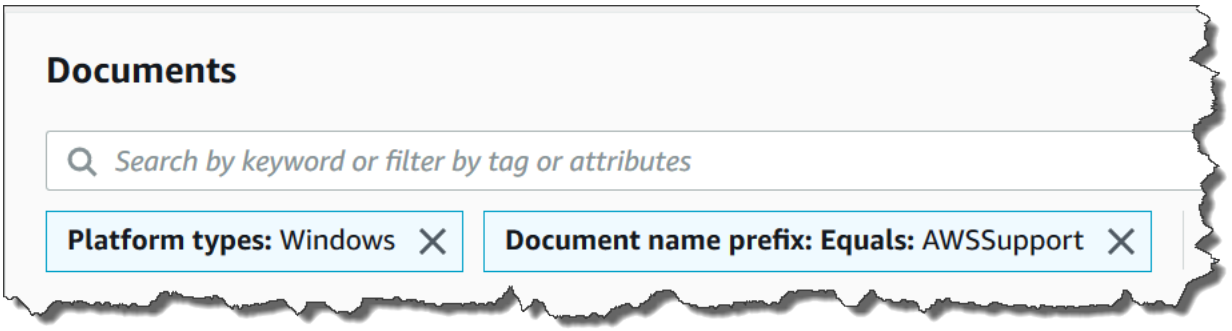
Systems Manager の [Documents (ドキュメント)] ページの検索ボックスを選択すると、以下のフィルターが自動的に表示されます。

- [Document name prefix (ドキュメント名のプレフィックス)]
- [Platform types (プラットフォームタイプ)]
- [Document type (ドキュメントタイプ)]
- タグキー



1 つのフィルターを使用して、SSM ドキュメントを検索できます。より具体的な SSM ドキュメントのセットを返す場合は、複数のフィルターを適用できます。次の図は、[Platform types (プラット

フォームタイプ)] フィルターと [Document name prefix (ドキュメント名のプレフィックス)] フィルターを使用した検索の例を示しています。



複数のフィルターを適用すると、Systems Manager は選択したフィルターに基づいて異なる検索ステートメントで検索します。

- 同じフィルター ([Document name prefix (ドキュメント名のプレフィックス)] など) を複数回適用すると、Systems Manager は OR ステートメントを使用して検索します。例えば、1 つ目の [Document name prefix (ドキュメント名のプレフィックス)] フィルターに「**AWS**」を指定し、2 つ目の [Document name prefix (ドキュメント名のプレフィックス)] フィルターに「**Lambda**」を指定した場合、検索ではプレフィックスが「AWS」のすべてのドキュメントとプレフィックスが「Lambda」のすべてのドキュメントが返されます。
- 異なるフィルターを適用する場合 ([Document name prefix] (ドキュメント名プレフィックス) と [Platform types] (プラットフォームタイプ) など)、Systems Manager は検索に AND ステートメントを使用します。例えば、[Document name prefix] (ドキュメント名プレフィックス) のフィルターに **AWS** を使用し、[Platform types] (プラットフォームタイプ) のフィルターに **Linux** を指定した場合、検索結果は「AWS」のプレフィックスが付いたドキュメントのうち、Linux プラットフォーム固有のものをすべて表示します。

> **Note**
>
> フィルターを使用する検索では、大文字と小文字は区別されます。

ドキュメントのお気に入りへの追加

頻繁に使用する SSM ドキュメントを見つけやすいように、ドキュメントをお気に入りに追加してください。1 つのドキュメントタイプ、AWS アカウント および AWS リージョン 1 つにつき、最大 20 のドキュメントをお気に入りに追加できます。ドキュメント AWS Management Console からお気に

入りを選択、変更、表示できます。次の手順は、お気に入りを選択、変更、表示する方法について説明します。

SSM ドキュメントをお気に入りにするには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[ドキュメント] を選択します。
3. お気に入りにしたいドキュメント名の横にある星のアイコンを選択します。

SSM ドキュメントをお気に入りから削除するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[ドキュメント] を選択します。
3. お気に入りから削除するドキュメント名の横にある星アイコンを選択解除します。

ドキュメント AWS Management Console からお気に入りを表示するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[ドキュメント] を選択します。
3. [お気に入り] タブを選択します。

AWS Systems Manager Maintenance Windows

AWS Systems Manager のツールである Maintenance Windows では、オペレーティングシステムのパッチ適用、ドライバーの更新、ソフトウェアやパッチのインストールなど、ノードに対して破壊的になり得るアクションを実行するスケジュールを定義できます。

> **Note**
>
> State Manager および Maintenance Windows は、マネージドノードで同様の種類の更新を実行できます。どちらを選択するかは、システムコンプライアンスを自動化する必要があるか、指定した期間中に優先度の高い、時間的制約のあるタスクを実行するかによって異なります。

詳細については、「State Manager または Maintenance Windows の選択」を参照してください。

Maintenance Windows により、Amazon Simple Storage Service (Amazon S3) バケット、Amazon Simple Queue Service (Amazon SQS) キュー、AWS Key Management Service (AWS KMS) キーなど、他の AWS リソースタイプでアクションをスケジュールできます。

メンテナンスウィンドウのターゲットに含めることができるサポートされているリソースタイプの詳細なリストについては、「AWS Resource Groups ユーザーガイド」の「AWS Resource Groups およびタグエディタで使用できるリソース」を参照してください。Maintenance Windows の使用を開始するには、Systems Manager コンソールを開きます。ナビゲーションペインで、[Maintenance Windows] を選択します。

各メンテナンスウィンドウには、スケジュール、最長期間、登録されたターゲットのセット (実行されるマネージドノード、または他の AWS リソース)、登録されたタスクのセットがあります。タグを作成または更新するときに、タグをメンテナンスウィンドウに追加できます。(タグは、企業内のリソースを識別およびソートするのに役立ちます)。また、メンテナンスウィンドウを前後に実行しない日付を指定することもでき、さらにメンテナンスウィンドウのスケジュールの基準となる国際タイムゾーンを指定することもできます。

メンテナンスウィンドウのスケジュールに関するオプションの相互関係については、「メンテナンスウィンドウのスケジューリングおよび有効期間のオプション」を参照してください。

`--schedule` オプションの使用方法の詳細については、「リファレンス: Systems Manager の Cron 式および rate 式」を参照してください。

サポートされているタスクタイプ

メンテナンスウィンドウでは、次の 4 種類のタスクを実行できます:

- Systems Manager のツール Run Command のコマンド

  Run Command の詳細については、「AWS Systems Manager Run Command」を参照してください。
- Systems Manager のツールである Automation のワークフロー

  オートメーションワークフローの詳細については、「AWS Systems Manager Automation」を参照してください。

- の関数AWS Lambda

  Lambda 関数の詳細については、AWS Lambda デベロッパーガイドの「Lambda の開始方法」を参照してください。

- のタスクAWS Step Functions

  > **Note**
  >
  > メンテナンスウィンドウタスクは、Step Functions 標準ステートマシンワークフローのみをサポートします。Express ステートマシンワークフローはサポートされていません。ステートマシンワークフロータイプの詳細については、「AWS Step Functions デベロッパーガイド」の「標準ワークフローと Express ワークフロー」を参照してください。

  Step Functions の詳細については、AWS Step Functions デベロッパーガイドを参照してください。

これにより、メンテナンスウィンドウを使用して、選択されたターゲットで以下のようなタスクを実行できます。

- アプリケーションをインストールまたは更新します。
- パッチを適用します。
- SSM Agent をインストールまたは更新します。
- Systems Manager Run Command タスクを使用して PowerShell コマンドと Linux シェルスクリプトを実行します。
- Amazon Machine Images (AMIs) の構築、ソフトウェアのブートストラップ、Systems Manager Automation タスクを使用したノードの設定を行います。
- ノードをスキャンしてパッチ更新を探すなどの追加アクションを起動する AWS Lambda 関数を実行します。
- AWS Step Functions ステートマシンを実行して、ノードを Elastic Load Balancing 環境から削除し、ノードにパッチを適用してから Elastic Load Balancing 環境に戻すなどのタスクを行います。
- オフラインのノードをターゲットにするには、AWS リソースグループをターゲットとして指定します。

> **Note**
>
> メンテナンスウィンドウ Run Command タイプのタスクには、1 つ以上のターゲットを指定する必要があります。タスクに応じて、他のメンテナンスウィンドウタスクタイプ (Automation、AWS Lambda、AWS Step Functions) に対するターゲットはオプションです。ターゲットを指定しないタスクの実行の詳細については、「ターゲットのないメンテナンスウィンドウタスクを登録」を参照してください。

EventBridge のサポート

この Systems Manager ツールは、Amazon EventBridge ルールのイベントタイプとしてサポートされています。詳細については、「Amazon EventBridge を使用して Systems Manager イベントをモニタリングする」および「リファレンス: Systems Manager 用の Amazon EventBridge イベントパターンとタイプ」を参照してください。

内容

- Maintenance Windows を設定する
- コンソールを使用してメンテナンスウィンドウを作成および管理する
- チュートリアル
- メンテナンスウィンドウのタスクを登録する際の疑似パラメータの使用
- メンテナンスウィンドウのスケジューリングおよび有効期間のオプション
- ターゲットのないメンテナンスウィンドウタスクを登録
- メンテナンスウィンドウのトラブルシューティング

Maintenance Windows を設定する

AWS アカウント内のユーザーが AWS Systems Manager のツールである Maintenance Windows を使用してメンテナンスウィンドウタスクを作成およびスケジュールできるようにするには、必要なアクセス許可を付与する必要があります。さらに、メンテナンスウィンドウ用の IAM サービスロールと、それにアタッチする IAM ポリシーを作成する必要があります。

[開始する前に]

このセクションで設定するアクセス許可に加えて、メンテナンスウィンドウを操作する IAM エンティティ (ユーザー、ロール、またはグループ) が既に一般的なメンテナンスウィンドウのアクセス

許可をもっている必要があります。そのようなアクセス許可は、対象エンティティに IAM ポリシーの AmazonSSMFullAccess を割り当てるか、またはメンテナンスウィンドウのタスクを対象とするより小規模な Systems Manager アクセス許可セットを提供するカスタム IAM ポリシーを割り当てることによって付与できます。

トピック

- コンソールを使用したメンテナンスウィンドウへのアクセスの制御
- AWS CLI を使用したメンテナンスウィンドウへのアクセスの制御

コンソールを使用したメンテナンスウィンドウへのアクセスの制御

以下の手順では、AWS Systems Manager コンソールを使用して、メンテナンスウィンドウに必要なロールとアクセス許可を作成する方法を説明します。

トピック

- タスク 1: コンソールを使用して、メンテナンスウィンドウサービスロール用にカスタムポリシーを作成する
- タスク 2: コンソールを使用して、メンテナンスウィンドウのカスタムサービスロールを作成する
- タスク 3: コンソールを使用して、特定のユーザーにメンテナンスウィンドウタスクを登録するアクセス許可を付与する
- タスク 4: 指定されたユーザーがコンソールを使用してメンテナンスウィンドウタスクを登録できないようにする

タスク 1: コンソールを使用して、メンテナンスウィンドウサービスロール用にカスタムポリシーを作成する

メンテナンスウィンドウのタスクには、ターゲットリソースで実行するために必要なアクセス許可を提供するための IAM ロールが必要です。アクセス許可は、ロールにアタッチされた IAM ポリシーを通じて提供されます。実行するタスクのタイプおよびその他の運用要件によって、このポリシーの内容が決定されます。ユーザーのニーズに対応する基本ポリシーを提供しています。メンテナンスウィンドウで実行するタスクおよびタスクのタイプによっては、このポリシーのすべてのアクセス許可が必要ではなく、追加のアクセス許可を含める必要がある場合があります。後ほど タスク 2: コンソールを使用して、メンテナンスウィンドウのカスタムサービスロールを作成する に作成するロールに、このポリシーをアタッチします。

コンソールを使用してカスタムポリシーを作成するには

1. https://console.aws.amazon.com/iam/ で IAM コンソール を開きます。
2. ナビゲーションペインで ポリシーを選択してから ポリシーの作成を選択します。
3. [ポリシーエディタ] 欄で、[JSON] を選択します。
4. デフォルトのコンテンツを以下と置き換えます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand",
                "ssm:CancelCommand",
                "ssm:ListCommands",
                "ssm:ListCommandInvocations",
                "ssm:GetCommandInvocation",
                "ssm:GetAutomationExecution",
                "ssm:StartAutomationExecution",
                "ssm:ListTagsForResource",
                "ssm:DescribeInstanceInformation",
                "ssm:GetParameters"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "states:DescribeExecution",
                "states:StartExecution"
            ],
            "Resource": [
                "arn:aws:states:*:*:execution:*:*",
                "arn:aws:states:*:*:stateMachine:*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "lambda:InvokeFunction"
            ],
```

```
            "Resource": [
                "arn:aws:lambda:*:*:function:*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "resource-groups:ListGroups",
                "resource-groups:ListGroupResources"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "ssm.amazonaws.com"
                    ]
                }
            }
        }
    ]
}
```

5. 必要に応じて、アカウントで実行するメンテナンスタスクの JSON コンテンツを変更します。変更した内容は、ユーザーが計画したオペレーションに固有のものです。

   例:

- ワイルドカード (*) 修飾子を使用する代わりに、特定の関数およびステートマシンに Amazon リソースネーム (ARN) を指定できます。
- AWS Step Functions タスクを実行する予定がない場合は、`states` のアクセス許可と (ARN) を削除できます。
- AWS Lambda タスクを実行する予定がない場合は、`lambda` のアクセス許可と ARN を削除できます。
- オートメーションタスクを実行する予定がない場合は、`ssm:GetAutomationExecution` および `ssm:StartAutomationExecution` のアクセス許可を削除できます。
- タスクの実行に必要な追加のアクセス許可を追加します。たとえば、一部のオートメーションアクションは AWS CloudFormation スタックと連携します。そのため、`cloudformation:CreateStack`、`cloudformation:DescribeStacks`、および `cloudformation:DeleteStack` のアクセス許可が必要です。

  別の例: オートメーションランブックの `AWS-CopySnapshot` では、Amazon Elastic Block Store (Amazon EBS) スナップショットを作成するためのアクセス許可が必要です。このため、サービスロールに許可 `ec2:CreateSnapshot` が必要です。

  オートメーションランブックで必要なロールの許可については、「AWS Systems Manager オートメーションランブックレファレンス」にあるランブックの説明を参照してください。

6. ポリシーのリビジョンを完了したら、[次へ] をクリックします。
7. [ポリシー名] に、作成したサービスロールにアタッチするポリシーを識別するためのポリシー名を入力します。例: **`my-maintenance-window-role-policy`**。
8. (オプション) [タグを追加] 欄では、1 つ以上のタグキーと値のペアを追加して、このポリシーのアクセスを整理、追跡、または制御できます。
9. [Create policy] (ポリシーの作成) を選択します。

   ポリシーに指定した名前をメモしておきます。次の手順、「タスク 2: コンソールを使用して、メンテナンスウィンドウのカスタムサービスロールを作成する」で参照します。

タスク 2: コンソールを使用して、メンテナンスウィンドウのカスタムサービスロールを作成する

前のタスクで作成したポリシーを、このタスクで作成するメンテナンスウィンドウサービスロールにアタッチします。ユーザーがメンテナンスウィンドウタスクを登録すると、タスク設定の一部としてこの IAM ロールが指定されます。このロールでアクセス許可が付与され、Systems Manager がユーザーに代わって、メンテナンスウィンドウでタスクを実行できます。

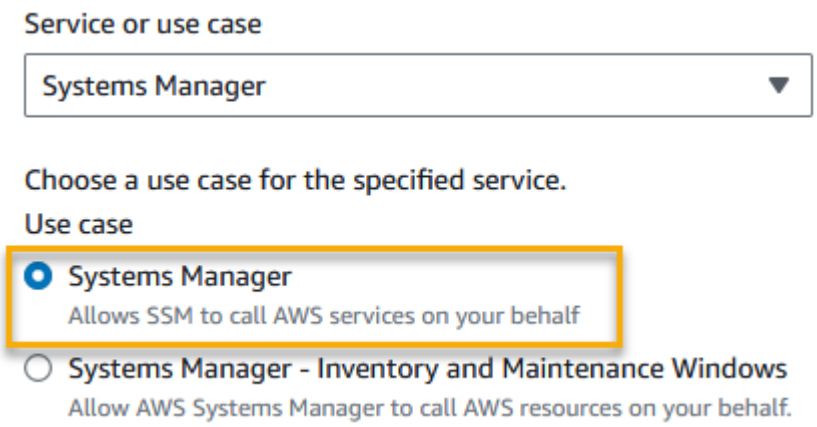
> **Important**
>
> 以前は、Systems Manager コンソールが、AWS マネージド IAM サービスリンクロール AWSServiceRoleForAmazonSSM を選択して、タスクのメンテナンスロールとして使用する機能を提供していました。メンテナンスウィンドウのタスクにおける、このロールとそれに関連するポリシーである AmazonSSMServiceRolePolicy の使用は推奨されなくなりました。このロールをメンテナンスウィンドウのタスクに使用している場合は、使用を中止することをお勧めします。代わりに、メンテナンスウィンドウのタスクが実行されたときに、Systems Manager と他の AWS のサービス間の通信を可能にする独自の IAM ロールを作成します。

以下の手順を使用して、Systems Manager がユーザーに代わって Maintenance Windows タスクを実行するための Maintenance Windows のカスタムサービスロールを作成します。前のタスクで作成したポリシーを、新しく作成したカスタムサービスロールにアタッチします。

コンソールを使用して、メンテナンスウィンドウのカスタムサービスロールを作成する

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. ナビゲーションペインで ロール を選択してから、ロールを作成する を選択します。
3. [Select trusted entity] (信頼できるエンティティを選択) で、次のように選択します。
   1. [信頼できるエンティティタイプ] で、[AWS サービス] を選択してください。
   2. [ユースケース] で、[Systems Manager] を選択します
   3. [Systems Manager] を選択します。

      次の画像は、Systems Manager オプションの場所を示しています。



4. [次へ] を選択します。
5. [アクセス許可ポリシー] 欄で、タスク 1: コンソールを使用して、メンテナンスウィンドウサービスロール用にカスタムポリシーを作成する で作成したポリシー名を検索ボックスに入力します。名前の横にあるチェックボックスをオンにして、[次へ] を選択します。
6. [Role name] (ロール名) に、このロールが Maintenance Windows ロールであることを識別できる名前を入力します。例: **my-maintenance-window-role**。
7. (オプション) デフォルトのロールの説明を変更して、このロールの目的を反映させます。例: **Performs maintenance window tasks on your behalf**。
8. [ステップ 1: 信頼できるエンティティを選択する] で、[信頼ポリシー] に次のポリシーが表示されていることを確認します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "ssm.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

9. [ステップ 2: アクセス許可を追加する] で、タスク 1: コンソールを使用して、メンテナンスウィンドウサービスロール用にカスタムポリシーを作成する で作成したポリシーが存在するのを確認します。
10. (オプション) [ステップ3: タグを追加する] で、タグとキーの値のペアを 1 つまたは複数追加して、このロールのアクセスを整理、追跡、または制御できます。
11. [Create role] (ロールの作成) を選択します。ロールページが再度表示されます。
12. さきほど作成した IAM ロールの名前を選択します。
13. [Summary] (概要) エリアのロール名と [ARN] をコピーするか、書き留めます。アカウントのユーザーは、メンテナンスウィンドウを作成するときにこの情報を指定します。

タスク 3: コンソールを使用して、特定のユーザーにメンテナンスウィンドウタスクを登録するアクセス許可を付与する

メンテナンスウィンドウのカスタムサービスロールにアクセスする許可をユーザーに付与すると、ユーサーはそのロールを自分のメンテナンスウィンドウタスクで使用できます。これは、Maintenance Windows ツール用に Systems Manager API コマンドを操作するために既に付与されているアクセス許可に追加されます。この IAM ロールは、メンテナンスウィンドウタスクを実行するために必要なアクセス許可を伝えます。このため、これらの IAM アクセス許可を渡す権限がないと、ユーザーは、カスタムサービスロールを使用してメンテナンスウィンドウにタスクを登録することができません。

メンテナンスウィンドウにタスクを登録する場合、実際のタスクオペレーションを実行するためのサービスロールを指定します。これは、サービスがユーザーに代わってタスクを実行するときに引き受けるロールです。その前に、タスク自体を登録するには、IAM PassRole ポリシーを IAM エンティティ (ユーザーまたはグループ) に割り当てます。これにより、これらのタスクをメンテナンスウィンドウに登録する一環として、タスク実行時に使用するロールを指定することを IAM エンティティに許可します。詳細については、「IAM ユーザーガイド」の「AWS のサービスにロールを渡すアクセス権限をユーザーに付与する」を参照してください。

メンテナンスウィンドウタスクの登録を許可するアクセス許可をユーザーに設定するには

IAM エンティティ (ユーザー、ロール、またはグループ) に管理者権限が設定されている場合、その IAM ユーザーまたはロールはメンテナンスウィンドウにアクセスできます。管理者権限のない IAM エンティティの場合、管理者は IAM エンティティに次の権限を付与する必要があります。タスクをメンテナンスウィンドウに登録するために必要な最低限の権限です。

- AmazonSSMFullAccess マネージドポリシー、または同等のアクセス許可を付与するポリシー。
- 次の iam:PassRole および iam:ListRoles のアクセス許可。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::account-id:role/my-maintenance-window-role"
        },
        {
            "Effect": "Allow",
            "Action": "iam:ListRoles",
```

```
            "Resource": "arn:aws:iam::account-id:role/"
        },
        {
            "Effect": "Allow",
            "Action": "iam:ListRoles",
            "Resource": "arn:aws:iam::account-id:role/aws-service-role/
ssm.amazonaws.com/"
        }
    ]
}
```

my-maintenance-window-role は、前に作成したカスタムメンテナンスウィンドウ向けサービスロールの名前を表します。

account-id は、AWS アカウント の ID を表します。リソース arn:aws:iam::*account-id*:role/ に対してこのアクセス許可を追加すると、ユーザーはメンテナンスウィンドウタスクを作成するときに、コンソールでカスタマーロールを表示および選択できます。arn:aws:iam::*account-id*:role/aws-service-role/ssm.amazonaws.com/ に対してこのアクセス許可を追加すると、ユーザーはメンテナンスウィンドウタスクを作成するときに、コンソールで Systems Manager サービスにリンクされたロールを選択できます。

アクセス権限を付与するにはユーザー、グループ、またはロールにアクセス許可を追加します。

- AWS IAM Identity Center のユーザーとグループ:

  アクセス許可セットを作成します。「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」の手順に従ってください。

- IAM 内で、ID プロバイダーによって管理されているユーザー:

  ID フェデレーションのロールを作成します。詳細については「IAM ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) 用のロールを作成する」を参照してください。

- IAM ユーザー:
  - ユーザーが担当できるロールを作成します。手順については「IAM ユーザーガイド」の「IAM ユーザーのロールの作成」を参照してください。
  - (お奨めできない方法) ポリシーをユーザーに直接アタッチするか、ユーザーをユーザーグループに追加します。詳細については「IAM ユーザーガイド」の「ユーザー (コンソール) へのアクセス権限の追加」を参照してください。

コンソールを使用して、メンテナンスウィンドウタスクの登録を許可するグループのアクセス許可を設定するには

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. ナビゲーションペインで、[ユーザーグループ] を選択します。
3. グループリストで iam:PassRole のアクセス許可を割り当てるグループの名前を選択するか、必要に応じて新しいグループを作成します。
4. [Permissions] (アクセス許可) タブで、[Add permissions, Create inline policy] (アクセス許可の追加、インラインポリシーの作成) をクリックします。
5. [ポリシーエディタ] 欄で [JSON] を選択し、ボックスのデフォルトの内容を以下に置き換えます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::account-id:role/my-maintenance-window-role"
        },
        {
            "Effect": "Allow",
            "Action": "iam:ListRoles",
            "Resource": "arn:aws:iam::account-id:role/"
        },
        {
            "Effect": "Allow",
            "Action": "iam:ListRoles",
            "Resource": "arn:aws:iam::account-id:role/aws-service-role/
ssm.amazonaws.com/"
        }
    ]
}
```

my-maintenance-window-role は、前に作成したカスタムメンテナンスウィンドウロールの名前を表します。

account-id は、AWS アカウント の ID を表します。リソース arn:aws:iam::*account-id*:role/ に対してこのアクセス許可を追加すると、ユーザーはメンテナンスウィンドウタスクを作成するときに、コンソールでカスタマーロールを表示および選択できま

す。arn:aws:iam::*account-id*:role/aws-service-role/ssm.amazonaws.com/ に対してこのアクセス許可を追加すると、ユーザーはメンテナンスウィンドウタスクを作成するときに、コンソールで Systems Manager サービスにリンクされたロールを選択できます。

6. [次へ] を選択します。
7. [レビューと確認] ページで、この PassRole ポリシーを識別するための名前を [ポリシー名] ボックスに入力し (**my-group-iam-passrole-policy** など)、[ポリシーの作成] を選択します。

タスク 4: 指定されたユーザーがコンソールを使用してメンテナンスウィンドウタスクを登録できないようにする

メンテナンスウィンドウでタスクを登録したくない AWS アカウント 内のユーザーに対する ssm:RegisterTaskWithMaintenanceWindow アクセス許可を拒否できます。これにより、メンテナンスウィンドウのタスクを登録してはいけないユーザーに対して、追加の予防レイヤーが提供されます。

コンソールを使用して、メンテナンスウィンドウタスクの登録を許可しないグループ向けのアクセス許可を設定するには

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. ナビゲーションペインで、[ユーザーグループ] を選択します。
3. グループのリストで、ssm:RegisterTaskWithMaintenanceWindow のアクセス許可を拒否するグループの名前を選択するか、もしくは必要に応じて新しいグループを作成します。
4. [Permissions] (アクセス許可) タブで、[Add permissions, Create inline policy] (アクセス許可の追加、インラインポリシーの作成) をクリックします。
5. [ポリシーエディタ] 欄で [JSON] を選択し、ボックスのデフォルトの内容を以下に置き換えます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "ssm:RegisterTaskWithMaintenanceWindow",
            "Resource": "*"
        }
    ]
```

```
}
```

6. [次へ] を選択します。
7. [レビューと確認] ページで、このポリシーを識別するための名前 (**my-groups-deny-mw-tasks-policy** など) を [ポリシー名] ボックスに入力し、[ポリシーの作成] を選択します。

AWS CLI を使用したメンテナンスウィンドウへのアクセスの制御

以下の手順では、AWS Command Line Interface (AWS CLI) を使用して、AWS Systems Manager のツールである Maintenance Windows に必要なロールとアクセス許可を作成する方法について説明します。

トピック

- タスク 1: 信頼ポリシーとカスタマー管理ポリシーファイルを JSON 形式で作成する
- タスク 2: AWS CLI を使用して、メンテナンスウィンドウ用にカスタムサービスロールを作成し確認する
- タスク 3: AWS CLI を使用して、特定のユーザーにメンテナンスウィンドウタスクを登録するアクセス許可を付与する
- タスク 4: 指定したユーザーが AWS CLI を使用してメンテナンスウィンドウタスクを登録できないようにする

タスク 1: 信頼ポリシーとカスタマー管理ポリシーファイルを JSON 形式で作成する

メンテナンスウィンドウのタスクには、ターゲットリソースで実行するために必要なアクセス許可を提供するための IAM ロールが必要です。アクセス許可は、ロールにアタッチされた IAM ポリシーを通じて提供されます。実行するタスクのタイプおよびその他の運用要件によって、このポリシーの内容が決定されます。ユーザーのニーズに対応する基本ポリシーを提供しています。メンテナンスウィンドウで実行するタスクおよびタスクのタイプによっては、このポリシーのすべてのアクセス許可が必要ではなく、追加のアクセス許可を含める必要がある場合があります。

このタスクでは、カスタムメンテナンスウィンドウロールに必要なアクセス許可を JSON ファイルのペアで指定します。後ほど タスク 2: AWS CLI を使用して、メンテナンスウィンドウ用にカスタムサービスロールを作成し確認する に作成するロールに、このポリシーをアタッチします。

信頼ポリシーとカスタマー管理ポリシーファイルを作成するには

1. 次のトラストポリシーをテキストファイルに貼り付けます。次の名前と拡張子でファイルを保存します: **mw-role-trust-policy.json**。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ssm.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

2. 次の JSON ポリシーを別のテキストファイルに貼り付けます。最初のファイルを作成したのと同じディレクトリに、このファイルを次の名前と拡張子で保存します: **mw-role-custom-policy.json**。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand",
                "ssm:CancelCommand",
                "ssm:ListCommands",
                "ssm:ListCommandInvocations",
                "ssm:GetCommandInvocation",
                "ssm:GetAutomationExecution",
                "ssm:StartAutomationExecution",
                "ssm:ListTagsForResource",
                "ssm:GetParameters"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "states:DescribeExecution",
                "states:StartExecution"
            ],
            "Resource": [
```

```
                "arn:aws:states:*:*:execution:*:*",
                "arn:aws:states:*:*:stateMachine:*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "lambda:InvokeFunction"
            ],
            "Resource": [
                "arn:aws:lambda:*:*:function:*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "resource-groups:ListGroups",
                "resource-groups:ListGroupResources"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "tag:GetResources"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "ssm.amazonaws.com"
                    ]
                }
            }
        }
```

```
    ]
}
```

3. 必要に応じて、アカウントで実行するメンテナンスタスク用に mw-role-custom-policy.json のコンテンツを変更します。変更した内容は、ユーザーが計画したオペレーションに固有のものです。

   例:

   - ワイルドカード (*) 修飾子を使用する代わりに、特定の関数およびステートマシンに Amazon リソースネーム (ARN) を指定できます。
   - AWS Step Functions タスクを実行する予定がない場合は、states のアクセス許可と (ARN) を削除できます。
   - AWS Lambda タスクを実行する予定がない場合は、lambda のアクセス許可と ARN を削除できます。
   - オートメーションタスクを実行する予定がない場合は、ssm:GetAutomationExecution および ssm:StartAutomationExecution のアクセス許可を削除できます。
   - タスクの実行に必要な追加のアクセス許可を追加します。たとえば、一部のオートメーションアクションは AWS CloudFormation スタックと連携します。そのため、cloudformation:CreateStack、cloudformation:DescribeStacks、および cloudformation:DeleteStack のアクセス許可が必要です。

     別の例: オートメーションランブックの AWS-CopySnapshot では、Amazon Elastic Block Store (Amazon EBS) スナップショットを作成するためのアクセス許可が必要です。このため、サービスロールに許可 ec2:CreateSnapshot が必要です。

     オートメーションランブックで必要なロールの許可については、「AWS Systems Manager オートメーションランブックレファレンス」にあるランブックの説明を参照してください。

   必要な変更を行った後、ファイルを再保存します。

タスク 2: AWS CLI を使用して、メンテナンスウィンドウ用にカスタムサービスロールを作成し確認する

前のタスクで作成したポリシーを、このタスクで作成するメンテナンスウィンドウサービスロールにアタッチします。ユーザーがメンテナンスウィンドウタスクを登録すると、タスク設定の一部として

この IAM ロールが指定されます。このロールでアクセス許可が付与され、Systems Manager がユーザーに代わって、メンテナンスウィンドウでタスクを実行できます。

> **Important**
>
> 以前は、Systems Manager コンソールが、AWS マネージド IAM サービスリンクロール AWSServiceRoleForAmazonSSM を選択して、タスクのメンテナンスロールとして使用する機能を提供していました。メンテナンスウィンドウのタスクにおける、このロールとそれに関連するポリシーである AmazonSSMServiceRolePolicy の使用は推奨されなくなりました。このロールをメンテナンスウィンドウのタスクに使用している場合は、使用を中止することをお勧めします。代わりに、メンテナンスウィンドウのタスクが実行されたときに、Systems Manager と他の AWS のサービス間の通信を可能にする独自の IAM ロールを作成します。

このタスクでは、CLI コマンドを実行してメンテナンスウィンドウサービスロールを作成し、作成した JSON ファイルからポリシーコンテンツを追加します。

AWS CLI を使用して、メンテナンスウィンドウ用にカスタムサービスロールを作成する

1. mw-role-custom-policy.json と mw-role-trust-policy.json を保存したディレクトリで、AWS CLI を開いて次のコマンドを実行します。このコマンドにより、my-maintenance-window-role というメンテナンスウィンドウサービスロールが作成され、信頼ポリシーがアタッチされます。

   Linux & macOS

   ```
   aws iam create-role \
       --role-name "my-maintenance-window-role" \
       --assume-role-policy-document file://mw-role-trust-policy.json
   ```

   Windows

   ```
   aws iam create-role ^
       --role-name "my-maintenance-window-role" ^
       --assume-role-policy-document file://mw-role-trust-policy.json
   ```

   システムは以下のような情報を返します。

```
{
    "Role": {
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Action": "sts:AssumeRole",
                    "Effect": "Allow",
                    "Principal": {
                        "Service": "ssm.amazonaws.com"
                    }
                }
            ]
        },
        "RoleId": "AROAIIZKPBKS2LEXAMPLE",
        "CreateDate": "2024-08-19T03:40:17.373Z",
        "RoleName": "my-maintenance-window-role",
        "Path": "/",
        "Arn": "arn:aws:iam::123456789012:role/my-maintenance-window-role"
    }
}
```

> **Note**
>
> RoleName と Arn を書き留めておきます。それらを次のコマンドに含めます。

2. 次のコマンドを実行して、カスタマー管理ポリシーをロールにアタッチします。*account-id* のプレースホルダーをお使いのアカウント AWS アカウント ID に置き換えます。

   Linux & macOS

   ```
   aws iam attach-role-policy \
       --role-name "my-maintenance-window-role" \
       --policy-arn "arn:aws:iam::account-id:policy/mw-role-custom-policy.json"
   ```

   Windows

   ```
   aws iam attach-role-policy ^
       --role-name "my-maintenance-window-role" ^
       --policy-arn "arn:aws:iam::account-id:policy/mw-role-custom-policy.json"
   ```

3. 次のコマンドを実行して、ロールが作成され、信頼ポリシーがアタッチされていることを確認します。

```
aws iam get-role --role-name my-maintenance-window-role
```

コマンドは以下のような情報を返します。

```
{
    "Role": {
        "Path": "/",
        "RoleName": "my-maintenance-window-role",
        "RoleId": "AROA123456789EXAMPLE",
        "Arn": "arn:aws:iam::123456789012:role/my-maintenance-window-role",
        "CreateDate": "2024-08-19T14:13:32+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Principal": {
                        "Service": "ssm.amazonaws.com"
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        },
        "MaxSessionDuration": 3600,
        "RoleLastUsed": {
            "LastUsedDate": "2024-08-19T14:30:44+00:00",
            "Region": "us-east-2"
        }
    }
}
```

4. 次のコマンドを実行して、カスタマー管理ポリシーがロールにアタッチされていることを確認します。

```
aws iam list-attached-role-policies --role-name my-maintenance-window-role
```

コマンドは以下のような情報を返します。

```
{
    "AttachedPolicies": [
        {
            "PolicyName": "mw-role-custom-policy",
            "PolicyArn": "arn:aws:iam::123456789012:policy/mw-role-custom-policy"
        }
    ]
}
```

タスク 3: AWS CLI を使用して、特定のユーザーにメンテナンスウィンドウタスクを登録するアクセス許可を付与する

メンテナンスウィンドウのカスタムサービスロールにアクセスする許可をユーザーに付与すると、ユーザーはそのロールを自分のメンテナンスウィンドウタスクで使用できます。これは、Maintenance Windows ツール用に Systems Manager API コマンドを操作するために既に付与されているアクセス許可に追加されます。この IAM ロールは、メンテナンスウィンドウタスクを実行するために必要なアクセス許可を伝えます。このため、これらの IAM アクセス許可を渡す権限がないと、ユーザーは、カスタムサービスロールを使用してメンテナンスウィンドウにタスクを登録することができません。

メンテナンスウィンドウにタスクを登録する場合、実際のタスクオペレーションを実行するためのサービスロールを指定します。これは、サービスがユーザーに代わってタスクを実行するときに引き受けるロールです。その前に、タスク自体を登録するには、IAM `PassRole` ポリシーを IAM エンティティ (ユーザーまたはグループ) に割り当てます。これにより、これらのタスクをメンテナンスウィンドウに登録する一環として、タスク実行時に使用するロールを指定することを IAM エンティティに許可します。詳細については、「IAM ユーザーガイド」の「AWS のサービスにロールを渡すアクセス権限をユーザーに付与する」を参照してください。

AWS CLI を使用して、メンテナンスウィンドウタスクの登録を許可されているユーザー向けにアクセス許可を設定するには

1. 次の AWS Identity and Access Management (IAM) ポリシーをコピーしてテキストエディタに貼り付け、`mw-passrole-policy.json` というファイル名および拡張子で保存します。

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

```
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::account-id:role/my-maintenance-window-role"
        },
        {
            "Effect": "Allow",
            "Action": "iam:ListRoles",
            "Resource": "arn:aws:iam::account-id:role/"
        },
        {
            "Effect": "Allow",
            "Action": "iam:ListRoles",
            "Resource": "arn:aws:iam::account-id:role/aws-service-role/
ssm.amazonaws.com/"
        }
    ]
}
```

my-maintenance-window-role を、前に作成したカスタムメンテナンスウィンドウロールの名前に置き換えます。

accountId を AWS アカウント の ID に置き換えます。リソース arn:aws:iam::*account-id*:role/ に対してこのアクセス許可を追加すると、グループ内のユーザーは、メンテナンスウィンドウタスクを作成するときに、コンソールでカスタマーロールを表示および選択できます。arn:aws:iam::*account-id*:role/aws-service-role/ssm.amazonaws.com/ に対してこのアクセス許可を追加すると、グループ内のユーザーは、メンテナンスウィンドウタスクを作成するときに、コンソールで Systems Manager サービスにリンクされたロールを選択できます。

2. AWS CLI を開きます。
3. IAM エンティティ (ユーザーまたはグループ) にアクセス許可を割り当てるかどうかに応じて、以下のいずれかのコマンドを実行します。

   - IAM エンティティの場合:

     Linux & macOS

     ```
     aws iam put-user-policy \
         --user-name "user-name" \
         --policy-name "policy-name" \
         --policy-document file://path-to-document
     ```

Windows

```
aws iam put-user-policy ^
    --user-name "user-name" ^
    --policy-name "policy-name" ^
    --policy-document file://path-to-document
```

user-name では、メンテナンスウィンドウにタスクを割り当てるユーザーを指定します。*policy-name* では、ポリシーを識別するための名前を入力します (例: **my-iam-passrole-policy**)。*path-to-document* では、ステップ 1 で保存したファイルへのパスを指定します。例: `file://C:\Temp\mw-passrole-policy.json`

> **Note**
>
> Systems Manager コンソールを使用してメンテナンスウィンドウにタスクを登録するためのアクセス許可をユーザーに付与するには、AmazonSSMFullAccess ポリシー (または、メンテナンスウィンドウのタスクを対象として限られた範囲のアクセス許可を Systems Manager に提供する IAM ポリシー) もユーザーに割り当てる必要があります。AmazonSSMFullAccess ポリシーをユーザーに割り当てるには、次のコマンドを実行します。
>
> Linux & macOS
>
> ```
> aws iam attach-user-policy \
>     --policy-arn "arn:aws:iam::aws:policy/AmazonSSMFullAccess" \
>     --user-name "user-name"
> ```
>
> Windows
>
> ```
> aws iam attach-user-policy ^
>     --policy-arn "arn:aws:iam::aws:policy/AmazonSSMFullAccess" ^
>     --user-name "user-name"
> ```

- IAM グループの場合:

  Linux & macOS

  ```
  aws iam put-group-policy \
      --group-name "group-name" \
  ```

```
    --policy-name "policy-name" \
    --policy-document file://path-to-document
```

Windows

```
aws iam put-group-policy ^
    --group-name "group-name" ^
    --policy-name "policy-name" ^
    --policy-document file://path-to-document
```

group-name では、メンテナンスウィンドウにタスクを割り当てるメンバーが属するグループを指定します。*policy-name* では、ポリシーを識別するための名前を入力します (例: **my-iam-passrole-policy**)。*path-to-document* では、ステップ 1 で保存したファイルへのパスを指定します。例: `file://C:\Temp\mw-passrole-policy.json`

> **Note**
>
> Systems Manager コンソールを使用してメンテナンスウィンドウのタスクを登録するためのアクセス許可をグループのメンバーに付与するには、`AmazonSSMFullAccess` ポリシーもグループに割り当てる必要があります。このポリシーをグループに割り当てるには、次のコマンドを実行します。
>
> Linux & macOS
>
> ```
> aws iam attach-group-policy \
>     --policy-arn "arn:aws:iam::aws:policy/AmazonSSMFullAccess" \
>     --group-name "group-name"
> ```
>
> Windows
>
> ```
> aws iam attach-group-policy ^
>     --policy-arn "arn:aws:iam::aws:policy/AmazonSSMFullAccess" ^
>     --group-name "group-name"
> ```

4. ポリシーがグループに割り当てられたことを確認するには、次のコマンドを実行します。

Linux & macOS

```
aws iam list-group-policies \
```

```
    --group-name "group-name"
```

Windows

```
aws iam list-group-policies ^
    --group-name "group-name"
```

タスク 4: 指定したユーザーが AWS CLI を使用してメンテナンスウィンドウタスクを登録できないようにする

メンテナンスウィンドウでタスクを登録したくない AWS アカウント 内のユーザーに対する `ssm:RegisterTaskWithMaintenanceWindow` アクセス許可を拒否できます。これにより、メンテナンスウィンドウのタスクを登録してはいけないユーザーに対して、追加の予防レイヤーが提供されます。

個別のユーザーまたはグループに `ssm:RegisterTaskWithMaintenanceWindow` アクセス許可を拒否するかどうかに応じ、以下の手順のいずれかを使用して、ユーザーがメンテナンスウィンドウにタスクを登録できないようにします。

AWS CLI を使用して、メンテナンスウィンドウタスクの登録を許可されていないユーザー向けのアクセス許可を設定するには

1. 次の IAM ポリシーをコピーしてテキストエディタに貼り付け、**deny-mw-tasks-policy.json** というファイル名および拡張子で保存します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "ssm:RegisterTaskWithMaintenanceWindow",
            "Resource": "*"
        }
    ]
}
```

2. AWS CLI を開きます。
3. IAM エンティティ (ユーザーまたはグループ) にアクセス許可を割り当てるかどうかに応じて、以下のいずれかのコマンドを実行します。

- ユーザーの場合:

  Linux & macOS

  ```
  aws iam put-user-policy \
      --user-name "user-name" \
      --policy-name "policy-name" \
      --policy-document file://path-to-document
  ```

  Windows

  ```
  aws iam put-user-policy ^
      --user-name "user-name" ^
      --policy-name "policy-name" ^
      --policy-document file://path-to-document
  ```

  user-name では、メンテナンスウィンドウにタスクを割り当てられないようにするユーザーを指定します。*policy-name* では、ポリシーを識別するための名前を入力します (例: **my-deny-mw-tasks-policy**)。*path-to-document* では、ステップ 1 で保存したファイルへのパスを指定します。例: `file://C:\Temp\deny-mw-tasks-policy.json`

- グループの場合:

  Linux & macOS

  ```
  aws iam put-group-policy \
      --group-name "group-name" \
      --policy-name "policy-name" \
      --policy-document file://path-to-document
  ```

  Windows

  ```
  aws iam put-group-policy ^
      --group-name "group-name" ^
      --policy-name "policy-name" ^
      --policy-document file://path-to-document
  ```

  group-name では、メンテナンスウィンドウにタスクを割り当てられないようにするグループを指定します。*policy-name* では、ポリシーを識別するための名前を入力します (例: **my-**

deny-mw-tasks-policy)。*path-to-document* では、ステップ 1 で保存したファイルへのパスを指定します。例: `file://C:\Temp\deny-mw-tasks-policy.json`

4. ポリシーがグループに割り当てられたことを確認するには、次のコマンドを実行します。

Linux & macOS

```
aws iam list-group-policies \
    --group-name "group-name"
```

Windows

```
aws iam list-group-policies ^
    --group-name "group-name"
```

コンソールを使用してメンテナンスウィンドウを作成および管理する

このセクションでは、AWS Systems Manager コンソールを使用してメンテナンスウィンドウを作成、設定、更新、削除する方法について説明します。このセクションでは、メンテナンスウィンドウのターゲットとタスクの管理についても説明しています。

> **Important**
>
> 最初はメンテナンスウィンドウをテスト環境に作成して設定することをお勧めします。

[開始する前に]

メンテナンスウィンドウを作成する前に、AWS Systems Manager のツールである Maintenance Windows へのアクセスを設定する必要があります。詳細については、「Maintenance Windows を設定する」を参照してください。

トピック

- コンソールを使用してメンテナンスウィンドウを作成する
- コンソールを使用してメンテナンスウィンドウにターゲットを割り当てる
- コンソールを使用してメンテナンスウィンドウにタスクを割り当てる
- コンソールを使用してメンテナンスウィンドウを有効、または無効にする
- コンソールを使用してメンテナンスウィンドウリソースを更新または削除する

コンソールを使用してメンテナンスウィンドウを作成する

この手順では、AWS Systems Manager のツールである Maintenance Windows でメンテナンスウィンドウを作成します。名前、スケジュール、期間などの基本オプションを指定できます。後続のステップでは、それによって更新されるターゲット、またはリソース、およびメンテナンスウィンドウの実行中に実行されるタスクを選択します。

> **Note**
>
> メンテナンスウィンドウのスケジュールに関するオプションの相互関係については、「メンテナンスウィンドウのスケジューリングおよび有効期間のオプション」を参照してください。
> `--schedule` オプションの使用方法の詳細については、「リファレンス: Systems Manager の Cron 式および rate 式」を参照してください。

コンソールを使用してメンテナンスウィンドウを作成するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Maintenance Windows] を選択します。
3. [Create maintenance window] を選択します。
4. [名前] に、このメンテナンスウィンドウを識別するためのわかりやすい名前を入力します。
5. (オプション) [Description] (説明) に、このメンテナンスウィンドウの使用に関する説明を入力します。
6. (オプション) ターゲットとして登録されていないマネージドノードに対しても、メンテナンスウィンドウタスクの実行を許可する場合は、[Allow unregistered targets] (未登録ターゲットを許可する) を選択します。

   このオプションを選択すると、タスクをメンテナンスウィンドウに登録する際に、未登録ノードを (ノード ID で) 選択できます。

   このオプションを選択しない場合、タスクをメンテナンスウィンドウに登録する際、以前に登録していたターゲットを選択する必要があります。
7. 次の 3 つのうちいずれかのスケジュールオプションを使用して、メンテナンスウィンドウのスケジュールを指定します。

cron/rate 式の作成の詳細については、「リファレンス: Systems Manager の Cron 式および rate 式」を参照してください。

8. [期間] に、メンテナンスウィンドウを実行する時間数を入力します。指定する値は、開始時刻に基づいてメンテナンスウィンドウの具体的な終了時刻を決定します。メンテナンスウィンドウタスクは、決定された終了時刻から、次のステップで [タスクの開始を停止] に指定する時間数を引いて求められる時刻の後に開始することは許可されません。

   たとえば、メンテナンスウィンドウが午後 3 時に開始され、期間が 3 時間で、[タスクの開始を停止] の値が 1 時間の場合、午後 5 時以降はメンテナンスウィンドウのタスクを開始できません。

9. [Stop initiating tasks] に、メンテナンスウィンドウが終了してから新しいタスクの実行のスケジュールが停止されるまでの時間数を入力します。

10. (オプション) [Window start date] (ウィンドウ開始日) で、メンテナンスウィンドウをアクティブにする日時を ISO-8601 拡張形式で指定します。これにより、指定した将来の日付までメンテナンスウィンドウのアクティベーションを遅らせることができます。

    > **Note**
    >
    > 過去の開始日時を指定することはできません。

11. (オプション) [Window end date] (ウィンドウ終了日) で、メンテナンスウィンドウを非アクティブにする日時を ISO-8601 拡張形式で指定します。これにより、メンテナンスウィンドウの実行を停止する将来の日時を設定できるようになります。

12. (オプション) [Schedule time zone] (タイムゾーンのスケジュール) で、スケジュールされたメンテナンスウィンドウの実行の基準とするタイムゾーンを、IANA (Internet Assigned Numbers Authority) 形式で指定します。例: 「America/Los_Angeles」、「etc/UTC」、または「Asia/Seoul」。

    有効な形式の詳細については、IANA ウェブサイトの「Time Zone Database」を参照してください。

13. (オプション) [Schedule offset] (スケジュールオフセット) に、cron もしくは rate 式で指定された日時から、メンテナンスウィンドウを実行するまでに待機する日数を入力します。1 ~ 6 日の間で指定できます。

> **Note**
>
> このオプションは、cron または rate 式を手動で入力してスケジュールを指定した場合にのみ有効です。

14. (オプション) [タグの管理] 領域で、1 つ以上のタグキーの名前と値のペアをメンテナンスウィンドウに適用します。

    タグは、リソースに割り当てるオプションのメタデータです。タグを使用すると、目的、所有者、環境などのさまざまな方法でリソースを分類できます。たとえば、メンテナンスウィンドウにタグを付けて、実行するタスクの種類、ターゲットの種類、実行される環境を指定できます。この場合、以下のキーの名前と値のペアを指定します。

    - `Key=TaskType,Value=AgentUpdate`
    - `Key=OS,Value=Windows`
    - `Key=Environment,Value=Production`

15. [Create maintenance window] を選択します。メンテナンスウィンドウのページに戻ります。先ほど作成したメンテナンスウィンドウの状態が [Enabled] になっています。

コンソールを使用してメンテナンスウィンドウにターゲットを割り当てる

この手順では、ターゲットをメンテナンスウィンドウに登録します。つまり、メンテナンスウィンドウがアクションを実行するリソースを指定します。

> **Note**
>
> 1 つのメンテナンスウィンドウタスクが複数のターゲットに登録されている場合、そのタスクの呼び出しは並列ではなく、順番に実行されます。複数のターゲットで同時にタスクを実行する必要がある場合は、各ターゲットでタスクを個別に登録し、各タスクに同じ優先度レベルを割り当てます。

コンソールを使用してメンテナンスウィンドウにターゲットを割り当てるには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Maintenance Windows] を選択します。

3. メンテナンスウィンドウのリストで、ターゲットを追加するメンテナンスウィンドウを選択します。
4. [Actions]、[Register targets] の順に選択します。
5. (オプション) [ターゲット名] にターゲットの名前を入力します。
6. (オプション) [説明] に説明を入力します。
7. (オプション) [所有者情報] で、このメンテナンスウィンドウでこれらのターゲットのタスクを実行中に発生した Amazon EventBridge イベントに含める情報を指定します。

   EventBridge を使用して Systems Manager イベントをモニタリングする方法については、「Amazon EventBridge を使用して Systems Manager イベントをモニタリングする」を参照してください。
8. [Targets] エリアで、次の表で説明されているオプションのいずれかを選択します。

オプション	説明
インスタンスタグを指定する	[Specify instance tags] (インスタンスタグを指定) ボックスで、アカウントのマネージドノードに追加されている、または追加する 1 つ以上のタグキーと (オプション) 値を指定します。メンテナンスウィンドウが実行されると、これらのタグが追加されたすべてのマネージドノードでタスクが実行されます。 複数のタグキーを指定する場合、ターゲットグループに含めるように指定したすべてのタグキーと値で、ノードにタグ付けする必要があります。
インスタンスを手動で選択する	リストから、メンテナンスウィンドウターゲットに含めるノードごとにチェックボックスをオンにします。 リストには、Systems Manager で使用するために設定されたアカウントのノードをすべて含めます。

オプション	説明
	表示されるはずのマネージドノードが表示されない場合は、トラブルシューティングのヒントについて「マネージドノードの可用性のトラブルシューティング」を参照してください。 エッジデバイス、オンプレミスサーバー、仮想マシン (VM) については、「Systems Manager を利用したハイブリッド環境およびマルチクラウド環境でのノードの管理」を参照してください。

オプション	説明
リソースグループの選択	[リソースグループ] で、リストからアカウントの既存のリソースグループの名前を選択します。 リソースグループの作成と操作については、次のトピックを参照してください。 • AWS Resource Groupsユーザーガイドのリソースグループとは何ですか • AWS ニュースブログの AWS の Resource Groups とタグ付け [Resource types] (リソースタイプ) で、使用可能なリソースタイプから最大 5 つを選択するか、[All resource types] (すべてのリソースタイプ) を選択します。 メンテナンスウィンドウに割り当てたタスクが、ターゲットに追加したいずれかのリソースタイプで動作しない場合、システムよりエラーがレポートされる場合があります。これらのエラーにもかかわらず、サポートされているリソースタイプが検出されたタスクは引き続き実行されます。 たとえば、このターゲットに次のリソースタイプを追加するとします。 • `AWS::S3::Bucket` • `AWS::DynamoDB::Table` • `AWS::EC2::Instance` ただし、後でメンテナンスウィンドウにタスクを追加する場合は、パッチベースラインの適用やノードの再起動など、ノードでアク

オプション	説明
	ションを実行するタスクのみを含めます。メンテナンスウィンドウログで、Amazon Simple Storage Service (Amazon S3) バケットまたは Amazon DynamoDB テーブルが見つからない場合、エラーがレポートされることがあります。ただし、メンテナンスウィンドウはリソースグループ内のノードでタスクを引き続き実行します。

9. [Register target] を選択します。

このメンテナンスウィンドウにさらにターゲットを割り当てるには、[ターゲット] タブを選択し、次に [ターゲットの登録] を選択します。このオプションを使用すると、ターゲットにするためのさまざまな方法を選択できます。たとえば、以前にノード ID でノードをターゲットにした場合は、マネージドノードに適用されるタグを指定するか、リソースグループからリソースタイプを選択することで、新しいターゲットとターゲットノードを登録できます。

コンソールを使用してメンテナンスウィンドウにタスクを割り当てる

この手順では、タスクをメンテナンスウィンドウに追加します。タスクは、メンテナンスウィンドウ実行時に実行されるアクションです。

以下の 4 種類のタスクをメンテナンスウィンドウに追加することができます。

- AWS Systems Manager Run Command コマンド
- Systems Manager Automation ワークフロー
- AWS Step Functions タスク
- AWS Lambda 関数

> **Important**
>
> Maintenance Windows の IAM ポリシーでは、Lambda 関数名 (またはエイリアス) の前にプレフィックス `SSM` を付ける必要があります。このタイプのタスクを登録する前に、AWS Lambda で `SSM` を含めるようにその名前を更新します。例えば、Lambda 関数名が `MyLambdaFunction` の場合は、`SSMMyLambdaFunction` に変更します。

メンテナンスウィンドウにタスクを割り当てるには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Maintenance Windows] を選択します。
3. メンテナンスウィンドウのリストで、メンテナンスウィンドウを選択します。
4. [アクション] を選択してから、メンテナンスウィンドウに登録するタスクの種類に応じたオプションを選択します。

   - Run コマンドタスクの登録
   - オートメーションタスクの登録
   - Lambda タスクの登録
   - Step Functions タスクの登録

   > **Note**
   >
   > メンテナンスウィンドウタスクは、Step Functions 標準ステートマシンワークフローのみをサポートします。Express ステートマシンワークフローはサポートされていません。ステートマシンワークフロータイプの詳細については、「AWS Step Functions デベロッパーガイド」の「標準ワークフローと Express ワークフロー」を参照してください。

5. (オプション) [名前] にタスクの名前を入力します。
6. (オプション) [説明] に説明を入力します。
7. 新しいタスク呼び出しのカットオフで、メンテナンスウィンドウのカットオフ時間に達した後に新しいタスク呼び出しを開始したくない場合は、[有効] を選択します。

   このオプションが有効でない場合、カットオフ時間に達してもタスクの実行が継続され、完了するまで新しいタスク呼び出しが開始されます。

   > **Note**
   >
   > このオプションを有効にすると、完了しないタスクのステータスは `TIMED_OUT` です。

8. このステップでは、選択したタスクタイプのサブステップに従います。

Run Command

1. [コマンドドキュメント] リストで、実行するタスクを定義する Systems Manager コマンドドキュメント (SSM ドキュメント) を選択します。
2. [Document version (ドキュメントのバージョン)] で、使用するドキュメントのバージョンを選択します。
3. [タスクの優先順位] で、このタスクの優先度を指定します。ゼロ (0) が最高の優先度になります。メンテナンスウィンドウのタスクは、優先度順にスケジュールされ、優先度が同じタスクは並行してスケジュールされます。

Automation

1. [オートメーションドキュメント] リストで、実行するタスクを定義するオートメーションランブックを選択します。
2. [Document version (ドキュメントのバージョン)] で、使用するランブックのバージョンを選択します。
3. [タスクの優先順位] で、このタスクの優先度を指定します。ゼロ (0) が最高の優先度になります。メンテナンスウィンドウのタスクは、優先度順にスケジュールされ、優先度が同じタスクは並行してスケジュールされます。

Lambda

1. [Lambda パラメータ] エリアにあるリストから、Lambda 関数を選択します。
2. (オプション) [Payload] (ペイロード)、[Client Context] (クライアントコンテキスト)、または [Qualifier] (修飾子) で、指定したい任意の内容を入力します。

   > **Note**
   >
   > 場合によっては、疑似パラメータを `Payload` 値の一部として使用できます。その後、メンテナンスウィンドウタスクが実行されると、擬似パラメータプレースホルダーの代わりに正しい値を渡します。詳細については、メンテナンスウィンドウのタスクを登録する際の疑似パラメータの使用 を参照してください。

3. [タスクの優先順位] で、このタスクの優先度を指定します。ゼロ (0) が最高の優先度になります。メンテナンスウィンドウのタスクは、優先度順にスケジュールされ、優先度が同じタスクは並行してスケジュールされます。

Step Functions

1. [Step Functions パラメータ] のエリアにあるリストから、ステートマシンを選択します。
2. (オプション) ステートマシンの実行の名前と、その他の指定したい情報を、[Input] (入力) に入力します。

   > **Note**
   >
   > 場合によっては、疑似パラメータを `Input` 値の一部として使用できます。その後、メンテナンスウィンドウタスクが実行されると、擬似パラメータプレースホルダーの代わりに正しい値を渡します。詳細については、メンテナンスウィンドウのタスクを登録する際の疑似パラメータの使用 を参照してください。

3. [タスクの優先順位] で、このタスクの優先度を指定します。ゼロ (0) が最高の優先度になります。メンテナンスウィンドウのタスクは、優先度順にスケジュールされ、優先度が同じタスクは並行してスケジュールされます。

9. [ターゲット] 領域で、次のいずれかを選択します。

   - 登録済みターゲットグループの選択: 現在のメンテナンスウィンドウに登録したメンテナンスウィンドウターゲットを 1 つ以上選択します。
   - 未登録のターゲットの選択: タスクのターゲットとして、使用可能なリソースを 1 つずつ選択します。

     表示されるはずのマネージドノードが表示されない場合は、トラブルシューティングのヒントについて「マネージドノードの可用性のトラブルシューティング」を参照してください。
   - タスクターゲットは不要: タスクのターゲットは、Run Command タイプのタスク以外のすべての機能で既に指定されている可能性があります。

     メンテナンスウィンドウの Run Command タイプのタスクには、1 つ以上のターゲットを指定します。タスクに応じて、他のメンテナンスウィンドウタスクタイプ (Automation、AWS Lambda、AWS Step Functions) に対するターゲットはオプションです。ターゲットを指定しないタスクの実行の詳細については、「ターゲットのないメンテナンスウィンドウタスクを登録」を参照してください。

> **Note**
>
> 多くの場合、オートメーションタスクのターゲットを明示的に指定する必要はありません。例えば、`AWS-UpdateLinuxAmi` ランブックを使用して Linux 用の Amazon Machine Image (AMI) を更新するためのオートメーションタイプのタスクを作成するとします。このタスクが実行されると、AMI は最新の利用可能な Linux ディストリビューションパッケージと Amazon ソフトウェアを反映して更新されます。AMI から作成した新しいインスタンスには、これらの更新がインストール済みです。更新する AMI の ID はランブックの入力パラメータで指定されるため、メンテナンスウィンドウタスクでターゲットを再度指定する必要はありません。

10. オートメーションタスクのみ:

    [Input parameters] (入力パラメータ) のエリアで、タスクの実行に必須のパラメータ値、またはオプションのパラメータ値を指定します。

    > **Note**
    >
    > 場合によっては、特定の入力パラメータ値に疑似パラメータを使用できます。その後、メンテナンスウィンドウタスクが実行されると、擬似パラメータプレースホルダーの代わりに正しい値を渡します。詳細については、メンテナンスウィンドウのタスクを登録する際の疑似パラメータの使用 を参照してください。

11. [レート制御] の場合:

    - [同時実行数] の場合、コマンドを同時に実行するマネージドノードの数または割合を指定します。

      > **Note**
      >
      > マネージドノードに適用されるタグを指定するか、AWS リソースグループを指定してターゲットを選択し、ターゲットとなるマネージドノードの数が不明な場合は、割合を指定してドキュメントを同時に実行できるターゲットの数を制限します。

    - [エラーのしきい値] で、ノードの数または割合のいずれかで失敗した後、他のマネージドノードでのコマンドの実行をいつ停止するか指定します。例えば、3 つのエラーを指定した場合、4 番目のエラーが受信されると、システムマネージャー はコマンドの送信を停止します。コマンドを処理しているマネージドノードもエラーを送信する可能性があります。

12. (オプション) [IAM サービスロール] で、Systems Manager がメンテナンスウィンドウタスクの実行時期を推測するための許可を付与するロールを選択します。

    サービスロール ARN を指定しない場合、Systems Manager はアカウントのサービスにリンクされたロールを使用します。このロールはドロップダウンメニューに表示されません。アカウントに Systems Manager 用の適切なサービスにリンクされたロールが存在しない場合は、タスクが正常に登録されるとロールが作成されます。

    > **Note**
    >
    > セキュリティ体制を強化するために、メンテナンスウィンドウタスクを実行するためのカスタムポリシーとカスタムサービスロールを作成することを強くお勧めします。ポリシーは、特定のメンテナンスウィンドウタスクに必要なアクセス許可のみを提供するように作成できます。詳細については、「Maintenance Windows を設定する」を参照してください。

13. Run Command タスクのみ:

    (オプション) [Output options] (出力オプション) で以下のいずれかを行います。

    - [S3 への書き込みを有効にする] チェックボックスをオンにして、コマンド出力をファイルに保存します。ボックスにバケット名とプレフィックス (フォルダ) 名を入力してください。
    - [CloudWatch 出力] チェックボックスを選択して、Amazon CloudWatch Logs に詳細な出力を書き込みます。CloudWatch Logs のロググループ名を入力します。

    > **Note**
    >
    > S3 バケットまたは CloudWatch Logs にデータを書き込む機能を許可するアクセス許可は、このタスクを実行する IAM ユーザーのものではなく、ノードに割り当てられたインスタンスプロファイルのものです。詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」を参照してください。さらに、指定した S3 バケットまたはロググループが別の AWS アカウント にある場合は、ノードに関連付けられたインスタンスプロファイルに、そのバケットへの書き込みに必要なアクセス許可があることを確認してください。

14. Run Command タスクのみ:

    [SNS Notifications (SNS 通知)] セクションで、コマンドの実行状態に関する通知を受け取る場合は、[Enable SNS notifications (SNS 通知を有効にする)] チェックボックスをオンにします。

Run Command 用の Amazon SNS 通知の設定の詳細については、「Amazon SNS 通知を使用した Systems Manager のステータス変更のモニタリング」を参照してください。

15. Run Command タスクのみ:

    [パラメータ] 領域で、ドキュメントのパラメータを指定します。

    > **Note**
    >
    > 場合によっては、特定の入力パラメータ値に疑似パラメータを使用できます。その後、メンテナンスウィンドウタスクが実行されると、擬似パラメータプレースホルダーの代わりに正しい値を渡します。詳細については、メンテナンスウィンドウのタスクを登録する際の疑似パラメータの使用 を参照してください。

16. Run Command とオートメーションタスクのみ:

    (オプション) [CloudWatch アラーム] エリアの [アラーム名] で、モニタリング用のタスクに適用する既存の CloudWatch アラームを選択します。

    アラームが作動すると、タスクは停止されます。

    > **Note**
    >
    > CloudWatch アラームをタスクにアタッチするには、タスクを実行する IAM プリンシパルに `iam:createServiceLinkedRole` アクションの権限が必要です。CloudWatch アラームの詳細については、「Amazon CloudWatch でのアラームの使用」を参照してください。

17. タスプタイプに応じて、次のいずれかを選択します。

    - Run コマンドタスクの登録
    - オートメーションタスクの登録
    - Lambda タスクの登録
    - Step Functions タスクの登録

コンソールを使用してメンテナンスウィンドウを有効、または無効にする

メンテナンスウィンドウは、AWS Systems Manager のツールである Maintenance Windows で無効化または有効化できます。メンテナンスウィンドウを一度に 1 つ選択して、メンテナンスウィンドウの実行を無効または有効にすることができます。また、複数またはすべてのメンテナンスウィンドウを選択して有効または無効にすることもできます。

このセクションでは、Systems Manager コンソールを使用してメンテナンスウィンドウを無効または有効にする方法を説明します。AWS Command Line Interface (AWS CLI) を使用してこれを行う方法の例については、「チュートリアル : AWS CLI を使用してメンテナンスウィンドウを更新する」を参照してください。

トピック

- コンソールを使用してメンテナンスウィンドウを無効にする
- コンソールを使用してメンテナンスウィンドウを有効にする

コンソールを使用してメンテナンスウィンドウを無効にする

メンテナンスウィンドウを無効にして、指定した期間タスクを一時停止でき、後で再び有効にできます。

メンテナンスウィンドウを無効にするには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Maintenance Windows] を選択します。
3. 無効にするメンテナンスウィンドウの隣にあるチェックボックスを使用して、1 つ以上のメンテナンスウィンドウを選択します。
4. [アクション] メニューで、[メンテナンスウィンドウの無効化] を選択します。システムからアクションを確認するよう求められます。

コンソールを使用してメンテナンスウィンドウを有効にする

メンテナンスウィンドウを有効にしてタスクを再開できます。

> **Note**
>
> メンテナンスウィンドウが rate スケジュールを使用し、現時点で開始日が過去の日付と時刻に設定されている場合、現在の日付と時刻がメンテナンスウィンドウの開始日として使用されます。メンテナンスウィンドウの開始日は、有効化の前後の日付に変更できます。詳細については、コンソールを使用してメンテナンスウィンドウリソースを更新または削除する を参照してください。

メンテナンスウィンドウを有効にするには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Maintenance Windows] を選択します。
3. 有効にするメンテナンスウィンドウの横にあるチェックボックスをオンにします。
4. [アクション] で、[メンテナンスウィンドウの有効化] を選択します。システムからアクションを確認するよう求められます。

コンソールを使用してメンテナンスウィンドウリソースを更新または削除する

メンテナンスウィンドウは、AWS Systems Manager のツールである Maintenance Windows で更新または削除できます。また、メンテナンスウィンドウのターゲットやタスクも更新または削除できます。メンテナンスウィンドウの詳細を編集する場合は、スケジュール、ターゲット、タスクを変更できます。また、ウィンドウ、ターゲット、タスクの名前や説明を指定して、それらの目的を明確にし、ウィンドウのキューを管理しやすくすることもできます。

このセクションでは、Systems Manager コンソールを使用してメンテナンスウィンドウ、ターゲット、タスクを更新または削除する方法を説明します。AWS Command Line Interface (AWS CLI) を使用してこれを行う方法の例については、「チュートリアル : AWS CLI を使用してメンテナンスウィンドウを更新する」を参照してください。

トピック

- コンソールを使用してメンテナンスウィンドウを更新または削除する
- コンソールを使用してメンテナンスウィンドウターゲットを更新または登録解除する
- コンソールを使用してメンテナンスウィンドウタスクを更新または登録解除する

コンソールを使用してメンテナンスウィンドウを更新または削除する

名前、説明、スケジュールのほか、メンテナンスウィンドウで未登録ターゲットを許可するかどうかを変更するにはメンテナンスウィンドウを更新します。

メンテナンスウィンドウを更新または削除するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Maintenance Windows] を選択します。
3. 更新または削除するメンテナンスウィンドウの隣にあるボタンを選択してから、次のいずれかを実行します。

   - [削除] を選択します。システムからアクションを確認するよう求められます。
   - [Edit] を選択します。[Edit maintenance window] (メンテナンス時間の編集) ページで値とオプションを変更した後、[Save changes] (変更を保存) をクリックします。

     設定の選択肢については、「コンソールを使用してメンテナンスウィンドウを作成する」を参照してください。

コンソールを使用してメンテナンスウィンドウターゲットを更新または登録解除する

メンテナンスウィンドウのターゲットは、更新または登録解除することができます。メンテナンスウィンドウのターゲットを更新する場合、新しいターゲット名、説明、所有者を指定できます。また、別のターゲットを選択することもできます。

メンテナンスウィンドウのターゲットを更新または削除するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Maintenance Windows] を選択します。
3. 更新するメンテナンスウィンドウの名前を選択してから、[Targets] (ターゲット) タブを選択した上で、以下のいずれかを行います。

   - ターゲットを更新するには、対象のターゲットの横にあるボタンをクリックした後に、[Edit] (編集) をクリックします。

- ターゲットの登録解除を行うには、対象のターゲットの横にあるボタンをクリックした後に、[Deregister target] (ターゲットの登録解除) をクリックします。[メンテナンスウィンドウのターゲットを登録解除する] ダイアログボックスで、[登録解除] を選びます。

コンソールを使用してメンテナンスウィンドウタスクを更新または登録解除する

メンテナンスウィンドウのタスクは、更新または登録解除することができます。更新する場合、新しいタスク名、説明、所有者を指定できます。Run Command とオートメーションタスクの場合は、タスクに別の SSM ドキュメントを選択できます。ただし、タスクのタイプを変更する編集はできません。たとえば、オートメーションタスクを作成した場合、そのタスクを編集して Run Command タスクに変更することはできません。

コンソールを使用してメンテナンスウィンドウのタスクを更新または削除するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Maintenance Windows] を選択します。
3. 更新するメンテナンスウィンドウの名前を選択します。
4. [Tasks] (タスク) タブを選択し、更新するタスクの横にあるボタンをクリックします。
5. 次のいずれかを行います：

   - タスクを登録解除するには、[Deregister task] (タスクの登録解除) をクリックします。
   - タスクを編集するには、[編集] を選択します。目的の値やオプションを変更し、[Edit task] (タスクの編集) をクリックします。

チュートリアル

このセクションのチュートリアルでは、メンテナンスウィンドウを操作する際の一般的なタスクを実行する方法について説明する。

前提条件を完了します。

これらのチュートリアルを試す前に、以下の前提条件を満たしてください。

- ローカルマシンで AWS CLI を設定する – AWS CLI コマンドを実行する前に、ローカルマシンに CLI をインストールして設定する必要があります。詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」および「AWS Tools for PowerShell のインストール」を参照してください。

- メンテナンスウィンドウのロールとアクセス許可を確認する – アカウントの AWS 管理者は、CLI を使用してメンテナンスウィンドウを管理するのに必要な AWS Identity and Access Management (IAM) アクセス許可をユーザーに付与する必要があります。詳細については、Maintenance Windows を設定する を参照してください。
- Systems Manager と互換性のあるインスタンスを作成または設定する – チュートリアルを完了するには、Systems Manager で使用するように設定された Amazon Elastic Compute Cloud (Amazon EC2) インスタンスが少なくとも 1 つ必要です。つまり、SSM Agent がインスタンスにインストールされ、Systems Manager の IAM インスタンスプロファイルがインスタンスにアタッチされていることになります。

  プリインストールされたエージェントにより、マネージド Amazon Machine Image (AMI) の 1 つの AWS からインスタンスを起動することをお勧めします。詳細については、「SSM Agent がプリインストールされている AMIs を見つける」を参照してください。

  インスタンスへの SSM Agent のインストールについては、以下のトピックを参照してください。

  - Windows Server 用の EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする
  - Linux 用 EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする

  Systems Manager に IAM アクセス許可を設定する方法については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」を参照してください。
- 必要に応じて追加のリソースを作成する – Systems Manager のツールである Run Command には、この前提条件トピックに記載されているもの以外のリソースを作成する必要のないタスクが多く含まれています。そのため、チュートリアルを通して初めて使用するためのシンプルな Run Command タスクが用意されています。このトピックで前述のように、Systems Manager で使用するように設定されている EC2 インスタンスも必要です。そのインスタンスを設定した後、シンプルな Run Command タスクを登録できます。

  Systems Manager の Maintenance Windows ツールは、4 種類のタスクの実行をサポートします。

  - Run Command コマンド
  - Systems Manager Automation ワークフロー
  - AWS Lambda 関数
  - AWS Step Functions タスク

  一般的に、メンテナンスウィンドウ、タスク、実行する追加のリソースが必要です。これらを作成する必要があります。たとえば、AWS Lambda 関数を実行するメンテナンスウィンドウが必要な

場合は、始める前に Lambda 関数を作成します。Run Command タスクの場合は、コマンド出力を保存できる S3 バケットを作成するなどの作業を行います (必要に応じて)。

チュートリアル

- チュートリアル: AWS CLI を使用したメンテナンスウィンドウの作成と管理
- チュートリアル: コンソールを使用してパッチ用メンテナンスウィンドウを作成する

チュートリアル: AWS CLI を使用したメンテナンスウィンドウの作成と管理

このセクションには、AWS Command Line Interface (AWS CLI) を使用して以下を行う方法を理解するのに役立つチュートリアルが含まれています。

- メンテナンスウィンドウを作成および設定する
- メンテナンスウィンドウに関する情報を表示する
- メンテナンスウィンドウのタスクとタスク実行に関する情報を表示する
- メンテナンスウィンドウを更新する
- メンテナンスウィンドウを削除する

リソース ID を記録する

この AWS CLI チュートリアルのタスクを完了したら、実行するコマンドによって生成されたリソース ID を記録します。これらの ID の多くを後続のコマンドの入力として使用します。例えば、メンテナンスウィンドウを作成すると、このシステムによって以下の形式でメンテナンスウィンドウ ID が表示されます。

```
{
   "WindowId":"mw-0c50858d01EXAMPLE"
}
```

システムによって生成された以下の ID をメモします。それらの ID はこのセクションのチュートリアルで必要になります。

- `WindowId`
- `WindowTargetId`
- `WindowTaskId`

- `WindowExecutionId`
- `TaskExecutionId`
- `InvocationId`
- `ExecutionId`

チュートリアルで使用する EC2 インスタンスの ID も必要です。例: `i-02573cafcfEXAMPLE`

チュートリアル

- チュートリアル: AWS CLI を使用してメンテナンスウィンドウを作成および設定する
- チュートリアル: AWS CLI を使用してメンテナンスウィンドウに関する情報を確認する
- チュートリアル: AWS CLI を使用してタスクおよびタスク実行に関する情報を確認する
- チュートリアル : AWS CLI を使用してメンテナンスウィンドウを更新する
- チュートリアル: AWS CLI を使用してメンテナンスウィンドウを削除する

チュートリアル: AWS CLI を使用してメンテナンスウィンドウを作成および設定する

このチュートリアルでは、AWS Command Line Interface (AWS CLI) を使用して、メンテナンスウィンドウおよびそのターゲットとタスクを作成し設定する方法について説明します。チュートリアルの主な手順はシンプルなステップで構成されています。1 つのメンテナンスウィンドウを作成し、1 つのターゲットを識別して、メンテナンスウィンドウで実行するシンプルなタスクを設定します。また、より複雑なシナリオを試すのに役立つ情報も提供しています。

このチュートリアルの手順に従う際に、斜体の*##*テキストの値を、独自のオプションおよび ID に置き換えてください。例えば、メンテナンスウィンドウ ID *mw-0c50858d01EXAMPLE* とインスタンス ID *i-02573cafcfEXAMPLE* を、作成したリソースの ID に置き換えます。

内容

- ステップ 1: AWS CLI を使用してメンテナンスウィンドウを作成する
- ステップ 2: AWS CLI を使用してメンテナンスウィンドウにターゲットノードを登録する
- ステップ 3: AWS CLI を使用してメンテナンスウィンドウにタスクを登録する

ステップ 1: AWS CLI を使用してメンテナンスウィンドウを作成する

このステップではメンテナンスウィンドウを作成して、名前、スケジュール、所要時間などの基本的なオプションを指定します。以降の手順で、更新するインスタンスと実行するタスクを選択します。

この例では、5 分ごとに実行されるメンテナンスウィンドウを作成します。通常は、メンテナンスウィンドウを頻繁に実行することはありません。ただし、この頻度では、チュートリアルの結果をすぐに確認できます。タスクが正常に実行された後、頻度を減らす方法を示します。

> **Note**
>
> メンテナンスウィンドウのスケジュールに関するオプションの相互関係については、「メンテナンスウィンドウのスケジューリングおよび有効期間のオプション」を参照してください。
> `--schedule` オプションの使用方法の詳細については、「リファレンス: Systems Manager の Cron 式および rate 式」を参照してください。

AWS CLIを使用してメンテナンスウィンドウを作成するには

1. AWS Command Line Interface (AWS CLI) を開き、ローカルマシンで次のコマンドを実行して、以下を実行するメンテナンスウィンドウを作成します。

   - 5 分ごとに最大 2 時間実行します (必要に応じて)。
   - メンテナンスウィンドウのオペレーションが終了してから 1 時間以内に新しいタスクが開始されないようにします。
   - 関連付けられていないターゲット (メンテナンスウィンドウに登録されていないインスタンス) を許可します。
   - カスタムタグによって、メンテナンスウィンドウをその作成者がチュートリアルで使用することを示します。

   Linux & macOS

   ```
   aws ssm create-maintenance-window \
       --name "My-First-Maintenance-Window" \
       --schedule "rate(5 minutes)" \
       --duration 2 \
       --cutoff 1 \
       --allow-unassociated-targets \
       --tags "Key=Purpose,Value=Tutorial"
   ```

Windows

```
aws ssm create-maintenance-window ^
    --name "My-First-Maintenance-Window" ^
    --schedule "rate(5 minutes)" ^
    --duration 2 ^
    --cutoff 1 ^
    --allow-unassociated-targets ^
    --tags "Key"="Purpose","Value"="Tutorial"
```

システムは以下のような情報を返します。

```
{
   "WindowId":"mw-0c50858d01EXAMPLE"
}
```

2. 次に、以下のコマンドを実行して、既にアカウントにあるこのメンテナンスウィンドウおよび他のウィンドウの詳細を表示します。

```
aws ssm describe-maintenance-windows
```

システムは以下のような情報を返します。

```
{
   "WindowIdentities":[
      {
            "WindowId": "mw-0c50858d01EXAMPLE",
            "Name": "My-First-Maintenance-Window",
            "Enabled": true,
            "Duration": 2,
            "Cutoff": 1,
            "NextExecutionTime": "2019-05-11T16:46:16.991Z"
      }
   ]
}
```

「ステップ 2: AWS CLI を使用してメンテナンスウィンドウにターゲットノードを登録する」に進みます。

ステップ 2: AWS CLI を使用してメンテナンスウィンドウにターゲットノードを登録する

このステップでは、新しいメンテナンスウィンドウでターゲットを登録します。この場合、メンテナンスウィンドウ実行時に更新するノードを指定します。

ノード ID を使用して一度に複数のノードを登録する例、タグを使用して複数のノードを識別する例、およびリソースグループをターゲットとして指定する例については、「例: ターゲットをメンテナンスウィンドウに登録する」を参照してください。

> **Note**
>
> Maintenance Windows のチュートリアルの前提条件で説明されているように、このステップで使用する Amazon Elastic Compute Cloud (Amazon EC2) インスタンスは既に作成されているはずです。

AWS CLI を使用してメンテナンスウィンドウにターゲットノードを登録するには

1. ローカルマシンで次のコマンドを実行します。各##############をユーザー自身の情報に置き換えます。

   Linux & macOS

   ```
   aws ssm register-target-with-maintenance-window \
       --window-id "mw-0c50858d01EXAMPLE" \
       --resource-type "INSTANCE" \
       --target "Key=InstanceIds,Values=i-02573cafcfEXAMPLE"
   ```

   Windows

   ```
   aws ssm register-target-with-maintenance-window ^
       --window-id "mw-0c50858d01EXAMPLE" ^
       --resource-type "INSTANCE" ^
       --target "Key=InstanceIds,Values=i-02573cafcfEXAMPLE"
   ```

   システムは以下のような情報を返します。

   ```
   {
       "WindowTargetId":"e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE"
   ```

```
}
```

2. ここで、ローカルマシンで次のコマンドを実行して、メンテナンスウィンドウのターゲットに関する詳細を表示します。

   Linux & macOS

   ```
   aws ssm describe-maintenance-window-targets \
       --window-id "mw-0c50858d01EXAMPLE"
   ```

   Windows

   ```
   aws ssm describe-maintenance-window-targets ^
       --window-id "mw-0c50858d01EXAMPLE"
   ```

   システムは以下のような情報を返します。

   ```
   {
       "Targets": [
           {
               "WindowId": "mw-0c50858d01EXAMPLE",
               "WindowTargetId": "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE",
               "ResourceType": "INSTANCE",
               "Targets": [
                   {
                       "Key": "InstanceIds",
                       "Values": [
                           "i-02573cafcfEXAMPLE"
                       ]
                   }
               ]
           }
       ]
   }
   ```

「ステップ 3: AWS CLI を使用してメンテナンスウィンドウにタスクを登録する」に進みます。

例: ターゲットをメンテナンスウィンドウに登録する

ステップ 2: AWS CLI を使用してメンテナンスウィンドウにターゲットノードを登録する で示すように、ノード ID を使用して、単一のノードをターゲットとして登録できます。このページのコマンド形式を使用すると、複数のノードをターゲットとして登録することもできます。

一般的に、メンテナンスウィンドウのターゲットとして使用するノードを特定する方法は 2 つあります。個々のノードを指定する方法と、リソースタグを使用する方法です。例 2～3 に示すように、リソースタグメソッドには、さらに多くのオプションがあります。

メンテナンスウィンドウのターゲットとして、1 つ以上のリソースグループを指定することもできます。リソースグループには、ノードおよびサポートされている他の多くの種類の AWS リソースを含めることができます。次に、例 4 と 5 で、リソースグループをメンテナンスウィンドウのターゲットに追加する方法を示しています。

> **Note**
>
> 1 つのメンテナンスウィンドウタスクが複数のターゲットに登録されている場合、そのタスクの呼び出しは並列ではなく、順番に実行されます。複数のターゲットで同時にタスクを実行する必要がある場合は、各ターゲットでタスクを個別に登録し、各タスクに同じ優先度レベルを割り当てます。

リソースグループの作成と管理の詳細については、AWS Resource Groups ユーザーガイドの「リソースグループとは」およびAWS ニュースブログの「AWS のリソースグループとタグ付け」を参照してください。

AWS Systems Manager のツールである Maintenance Windows のクォータについては、次の例で指定されているものに加えて、「Amazon Web Services 全般のリファレンス」の「Systems Manager のサービスクォータ」を参照してください。

例 1: ノード ID を使用して複数のターゲットを登録する

次のコマンドをローカルマシン形式で実行し、ノード ID を使用して複数のノードをターゲットとして登録します。各##########を##########ユーザー自身の情報に置き換えます。

Linux & macOS

```
aws ssm register-target-with-maintenance-window \
```

```
    --window-id "mw-0c50858d01EXAMPLE" \
    --resource-type "INSTANCE" \
    --target
 "Key=InstanceIds,Values=i-02573cafcfEXAMPLE,i-0471e04240EXAMPLE,i-07782c72faEXAMPLE"
```

Windows

```
aws ssm register-target-with-maintenance-window ^
    --window-id "mw-0c50858d01EXAMPLE ^
    --resource-type "INSTANCE" ^
    --target
 "Key=InstanceIds,Values=i-02573cafcfEXAMPLE,i-0471e04240EXAMPLE,i-07782c72faEXAMPLE
```

推奨用途: 最初はメンテナンスウィンドウに一意のノードグループを登録し、共通のノードタグを共有しないのが最も有益です。

クォータ: 各メンテナンスウィンドウターゲットに対して、ノードを合計 50 個まで指定できます。

例 2: ノードに適用されたリソースタグを使用してターゲットを登録する

ローカルマシンで次のコマンドを実行して、割り当てたキーと値のペアで既にすべてがタグ付けされているノードを登録します。各##############をユーザー自身の情報に置き換えます。

Linux & macOS

```
aws ssm register-target-with-maintenance-window \
    --window-id "mw-0c50858d01EXAMPLE" \
    --resource-type "INSTANCE" \
    --target "Key=tag:Region,Values=East"
```

Windows

```
aws ssm register-target-with-maintenance-window ^
    --window-id "mw-0c50858d01EXAMPLE" ^
    --resource-type "INSTANCE" ^
    --target "Key=tag:Region,Values=East"
```

推奨用途: 最初はメンテナンスウィンドウに一意のノードグループを登録し、共通のノードタグを共有するのが最も有益です。

クォータ: ターゲットごとにキーと値のペアを合計 5 つまで指定できます。複数のキーと値のペアを指定する場合、ターゲットグループに含めると指定したすべてのタグキーと値でノードをタグ付けする必要があります。

> **Note**
>
> タグキー Patch Group または PatchGroup を使用してノードのグループにタグを付け、ノードに共通のキー値 (my-patch-group) を割り当てることができます。(EC2 インスタンスメタデータでタグを許可している場合は、スペースなしで PatchGroup を使用する必要があります。) Systems Manager のツールである Patch Manager は、ノードで Patch Group または PatchGroup キーを評価し、適用されるパッチベースラインを決定するのに役立ちます。タスクで AWS-RunPatchBaseline SSM ドキュメント (またはレガシー AWS-ApplyPatchBaseline の SSM ドキュメント) が実行される場合は、メンテナンスウィンドウにターゲットを登録する際に、同じ Patch Group または PatchGroup のキーの値を指定することができます。例: `--target "Key=tag:PatchGroup,Values=my-patch-group`。そうすることで、メンテナンスウィンドウを使用して、同じパッチベースラインにすでに関連付けられているノードグループのパッチを更新できます。詳細については、「パッチグループ」を参照してください。

例 3: タグキーのグループを使用してターゲットを登録する (タグ値なし)

ローカルマシンで次のコマンドを実行して、キー値に関係なく、複数のタグキーが割り当てられているノードをすべて登録します。各##############をユーザー自身の情報に置き換えます。

Linux & macOS

```
aws ssm register-target-with-maintenance-window \
    --window-id "mw-0c50858d01EXAMPLE" \
    --resource-type "INSTANCE" \
    --target "Key=tag-key,Values=Name,Instance-Type,CostCenter"
```

Windows

```
aws ssm register-target-with-maintenance-window ^
    --window-id "mw-0c50858d01EXAMPLE" ^
    --resource-type "INSTANCE" ^
    --target "Key=tag-key,Values=Name,Instance-Type,CostCenter"
```

推奨用途: 1 つのタグキーやタグキーと値のペアではなく、複数のタグキー (値はなし) を指定して、ノードをターゲットにする場合に役立ちます。

クォータ: ターゲットごとにタグキーを合計 5 つまで指定できます。複数のタグキーを指定する場合、ターゲットグループに含めるように指定したすべてのタグキーで、ノードにタグ付けする必要があります。

例 4: リソースグループ名を使用してターゲットを登録する

ローカルマシンで次のコマンドを実行して、指定されたリソースグループを登録します。含まれるリソースのタイプは関係ありません。*mw-0c50858d01EXAMPLE* を自分の情報に置き換えます。メンテナンスウィンドウに割り当てたタスクが、このリソースグループに含まれるリソースのタイプで動作しない場合は、エラーがレポートされる場合があります。これらのエラーにもかかわらず、サポートされているリソースタイプが検出されたタスクは引き続き実行されます。

Linux & macOS

```
aws ssm register-target-with-maintenance-window \
    --window-id "mw-0c50858d01EXAMPLE" \
    --resource-type "RESOURCE_GROUP" \
    --target "Key=resource-groups:Name,Values=MyResourceGroup"
```

Windows

```
aws ssm register-target-with-maintenance-window ^
    --window-id "mw-0c50858d01EXAMPLE" ^
    --resource-type "RESOURCE_GROUP" ^
    --target "Key=resource-groups:Name,Values=MyResourceGroup"
```

推奨用途: すべてのリソースタイプがメンテナンスウィンドウのターゲットになるかどうかを評価せずに、リソースグループをターゲットとしてすばやく指定する場合、またはタスクでアクションを実行するリソースタイプのみ、リソースグループに含まれていることがわかっている場合に役立ちます。

制限: 1 つのリソースグループのみをターゲットとして指定できます。

例 5: リソースグループのリソースタイプをフィルタリングしてターゲットを登録する

ローカルマシンで次のコマンドを実行して、指定したリソースグループに属する特定のリソースタイプのみを登録します。*mw-0c50858d01EXAMPLE* を自分の情報に置き換えます。このオプションを

使用すると、リソースグループに属するリソースタイプのタスクを追加した場合でも、リソースタイプをフィルタに明示的に追加していない場合、タスクは実行されません。

Linux & macOS

```
aws ssm register-target-with-maintenance-window \
    --window-id "mw-0c50858d01EXAMPLE" \
    --resource-type "RESOURCE_GROUP" \
    --target "Key=resource-groups:Name,Values=MyResourceGroup" \
    "Key=resource-
groups:ResourceTypeFilters,Values=AWS::EC2::Instance,AWS::ECS::Cluster"
```

Windows

```
aws ssm register-target-with-maintenance-window ^
    --window-id "mw-0c50858d01EXAMPLE" ^
    --resource-type "RESOURCE_GROUP" ^
    --target "Key=resource-groups:Name,Values=MyResourceGroup" ^
    "Key=resource-
groups:ResourceTypeFilters,Values=AWS::EC2::Instance,AWS::ECS::Cluster"
```

推奨用途: メンテナンスウィンドウでアクションを実行できる AWS リソースのタイプを厳密に制御する場合、またはリソースグループに多数のリソースタイプが含まれていて、メンテナンスウィンドウログに不要なエラーレポートを含めない場合に役立ちます。

制限: 1 つのリソースグループのみをターゲットとして指定できます。

ステップ 3: AWS CLI を使用してメンテナンスウィンドウにタスクを登録する

チュートリアルのこのステップでは、Linux 用の Amazon Elastic Compute Cloud (Amazon EC2) インスタンスで df コマンドを実行する AWS Systems Manager Run Command タスクを登録します。この標準の Linux コマンドの結果は、空き領域の割合をディスクで使用されているが、インスタンスのファイルシステムです。

-または-

Linux ではなく Windows Server の Amazon EC2 インスタンスをターゲットにしている場合は、以下のコマンドの df を ipconfig に置き換えます。このコマンドからの出力には、ターゲットインスタンスのアダプターの IP アドレス、サブネットマスク、デフォルトゲートウェイに関する詳細が一覧表示されます。

他のタスクタイプを登録したり、使用可能な Systems Manager Run Command オプションを使用する準備ができたら、「例: タスクをメンテナンスウィンドウに登録する」を参照してください。そのトピックでは、より現実的なシナリオを計画するのに役立つように、4 つのすべてのタスクタイプについて、また、それらの最も重要なオプションのいくつかについて、詳細な情報を提供しています。

タスクをメンテナンスウィンドウに登録するには

1. ローカルマシンで次のコマンドを実行します。各##############をユーザー自身の情報に置き換えます。ローカルの Windows マシンから実行するバージョンには、コマンドラインツールからコマンドを実行するのに必要なエスケープ文字 (/) が含まれています。

   Linux & macOS

   ```
   aws ssm register-task-with-maintenance-window \
       --window-id mw-0c50858d01EXAMPLE \
       --task-arn "AWS-RunShellScript" \
       --max-concurrency 1 --max-errors 1 \
       --priority 10 \
       --targets "Key=InstanceIds,Values=i-0471e04240EXAMPLE" \
       --task-type "RUN_COMMAND" \
       --task-invocation-parameters '{"RunCommand":{"Parameters":{"commands":
   ["df"]}}}'
   ```

   Windows

   ```
   aws ssm register-task-with-maintenance-window ^
       --window-id mw-0c50858d01EXAMPLE ^
       --task-arn "AWS-RunShellScript" ^
       --max-concurrency 1 --max-errors 1 ^
       --priority 10 ^
       --targets "Key=InstanceIds,Values=i-02573cafcfEXAMPLE" ^
       --task-type "RUN_COMMAND" ^
       --task-invocation-parameters={\"RunCommand\":{\"Parameters\":{\"commands\":
   [\"df\"]}}}
   ```

   システムは以下のような情報を返します。

   ```
   {
       "WindowTaskId": "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE"
   }
   ```

2. 作成したメンテナンスウィンドウタスクの詳細を表示するには、以下のコマンドを実行します。

   Linux & macOS

   ```
   aws ssm describe-maintenance-window-tasks \
       --window-id mw-0c50858d01EXAMPLE
   ```

   Windows

   ```
   aws ssm describe-maintenance-window-tasks ^
       --window-id mw-0c50858d01EXAMPLE
   ```

3. システムは以下のような情報を返します。

   ```
   {
       "Tasks": [
           {
               "WindowId": "mw-0c50858d01EXAMPLE",
               "WindowTaskId": "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE",
               "TaskArn": "AWS-RunShellScript",
               "Type": "RUN_COMMAND",
               "Targets": [
                   {
                       "Key": "InstanceIds",
                       "Values": [
                           "i-02573cafcfEXAMPLE"
                       ]
                   }
               ],
               "TaskParameters": {},
               "Priority": 10,
               "ServiceRoleArn": "arn:aws:iam::123456789012:role/
   MyMaintenanceWindowServiceRole",
               "MaxConcurrency": "1",
               "MaxErrors": "1"
           }
       ]
   }
   ```

4. 「ステップ 1: AWS CLI を使用してメンテナンスウィンドウを作成する」で指定したスケジュールに基づいて、タスクを実行する時間になるまで待ちます。たとえば、**--schedule "rate(5**

minutes)" を指定した場合は、5 分待ちます。その後、以下のコマンドを実行して、このタスクで発生した実行に関する情報を表示します。

Linux & macOS

```
aws ssm describe-maintenance-window-executions \
    --window-id mw-0c50858d01EXAMPLE
```

Windows

```
aws ssm describe-maintenance-window-executions ^
    --window-id mw-0c50858d01EXAMPLE
```

システムは以下のような情報を返します。

```
{
    "WindowExecutions": [
        {
            "WindowId": "mw-0c50858d01EXAMPLE",
            "WindowExecutionId": "14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE",
            "Status": "SUCCESS",
            "StartTime": 1557593493.096,
            "EndTime": 1557593498.611
        }
    ]
}
```

Tip

タスクが正常に実行した後、メンテナンスウィンドウが実行される頻度を減らすことができます。例えば、以下のコマンドを実行して頻度を週に 1 回に減らします。*mw-0c50858d01EXAMPLE* を自分の情報に置き換えます。

Linux & macOS

```
aws ssm update-maintenance-window \
    --window-id mw-0c50858d01EXAMPLE \
    --schedule "rate(7 days)"
```

Windows

```
aws ssm update-maintenance-window ^
    --window-id mw-0c50858d01EXAMPLE ^
    --schedule "rate(7 days)"
```

メンテナンスウィンドウのスケジュール管理の詳細については、「リファレンス: Systems Manager の Cron 式および rate 式」と「メンテナンスウィンドウのスケジューリングおよび有効期間のオプション」を参照してください。
AWS Command Line Interface (AWS CLI) を使用してメンテナンスウィンドウを変更する方法については、「チュートリアル : AWS CLI を使用してメンテナンスウィンドウを更新する」を参照してください。

AWS CLI コマンドによりメンテナンスウィンドウのタスクとその実行に関する詳細を表示する演習については、「チュートリアル: AWS CLI を使用してタスクおよびタスク実行に関する情報を確認する」に進みます。

チュートリアルコマンド出力へのアクセス

AWS CLI を使用して、メンテナンスウィンドウのタスク実行に関連付けられた Run Command コマンドの出力を表示することは、このチュートリアルの範囲外です。

ただし、AWS CLI を使用してこのデータを表示できます。(コマンド出力をコンソールやログファイルに保存するように、メンテナンスウィンドウを設定している場合、Systems Manager コンソールでも、Amazon Simple Storage Service (Amazon S3) バケットに保存されているログファイルでも、出力を表示できます)。Linux の EC2 インスタンスでの df コマンドの出力は以下のようになります。

```
Filesystem 1K-blocks Used Available Use% Mounted on

devtmpfs 485716 0 485716 0% /dev

tmpfs 503624 0 503624 0% /dev/shm

tmpfs 503624 328 503296 1% /run

tmpfs 503624 0 503624 0% /sys/fs/cgroup

/dev/xvda1 8376300 1464160 6912140 18% /
```

ipconfig の EC2 インスタンスでの Windows Server コマンドの出力は以下のようになります。

```
Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : example.com
   IPv4 Address. . . . . . . . . . . : 10.24.34.0/23
   Subnet Mask . . . . . . . . . . . : 255.255.255.255
   Default Gateway . . . . . . . . . : 0.0.0.0

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : abc1.wa.example.net

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::100b:c234:66d6:d24f%4
   IPv4 Address. . . . . . . . . . . : 192.0.2.0
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.0.2.0

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

例: タスクをメンテナンスウィンドウに登録する

「メンテナンスウィンドウを使用してタスクを登録する」に示されているように、AWS Command Line Interface (AWS CLI) を使用してメンテナンスウィンドウに Run Command (AWS Systems Manager のツール) でタスクを登録できます。このトピックで後ほど示すように、Systems Manager Automation ワークフローのタスク、AWS Lambda 関数、AWS Step Functions タスクを登録することもできます。

> **Note**
>
> メンテナンスウィンドウの Run Command タイプのタスクには、1つ以上のターゲットを指定します。タスクに応じて、他のメンテナンスウィンドウタスクタイプ (Automation、AWS Lambda、AWS Step Functions) に対するターゲットはオプションです。ターゲットを指定しないタスクの実行の詳細については、「ターゲットのないメンテナンスウィンドウタスクを登録」を参照してください。

このトピックでは、AWS Command Line Interface (AWS CLI) コマンド `register-task-with-maintenance-window` を使用して、サポートされている 4 つのタスクタイプをそれぞれメンテナンスウィンドウに登録する例を示しています。それらの例はデモ専用ですが、作業タスクの登録コマンドを作成するように変更できます。

--cli-input-json オプションの使用

タスクオプションをより適切に管理するために、`--cli-input-json` コマンドオプションに、JSON ファイルで参照されるオプション値を指定できます。

以下の例で提供しているサンプル JSON ファイルコンテンツを使用するには、ローカルマシンで以下の手順を実行します。

1. `MyRunCommandTask.json`、`MyAutomationTask.json` などの名前、または他の任意の名前でファイルを作成します。
2. そのファイルに JSON サンプルの内容をコピーします。
3. タスク登録用にその内容を変更し、そのファイルを保存します。
4. ファイルを保存したのと同じディレクトリで、以下のコマンドを実行します。ファイル名を *`MyFile.json`* に置き換えます。

   Linux & macOS

   ```
   aws ssm register-task-with-maintenance-window \
       --cli-input-json file://MyFile.json
   ```

   Windows

   ```
   aws ssm register-task-with-maintenance-window ^
       --cli-input-json file://MyFile.json
   ```

メンテナンスウィンドウタスクの登録における疑似パラメータ

いくつかの例では、ID 情報をタスクに渡すための方法として疑似パラメータを使用します。例えば、{{TARGET_ID}} と {{RESOURCE_ID}} は、AWS リソースの ID を Automation 、Lambda、Step Functions のタスクに渡すために使用されます。--task-invocation-parameters コンテンツ内の疑似パラメータの詳細については、「メンテナンスウィンドウのタスクを登録する際の疑似パラメータの使用」を参照してください。

詳細情報

- "register-task-with-maintenance-window" コマンドのパラメーターオプション.
- register-task-with-maintenance-window「 コマンドリファレンス」の「AWS CLI」を参照してください。
- 「RegisterTaskWithMaintenanceWindow API リファレンス」の「AWS Systems Manager」

タスクの登録例

以下のセクションでは、サポートされているタスクタイプを登録するサンプルの AWS CLI コマンドと、--cli-input-json オプションで用できる JSON サンプルを示しています。

Systems Manager Run Command タスクを登録する

以下の例は、AWS CLI を使用して、メンテナンスウィンドウで Systems Manager Run Command タスクを登録する方法を示しています。

Linux & macOS

```
aws ssm register-task-with-maintenance-window \
    --window-id mw-0c50858d01EXAMPLE \
    --task-arn "AWS-RunShellScript" \
    --max-concurrency 1 --max-errors 1 --priority 10 \
    --targets "Key=InstanceIds,Values=i-02573cafcfEXAMPLE" \
    --task-type "RUN_COMMAND" \
    --task-invocation-parameters '{"RunCommand":{"Parameters":{"commands":["df"]}}}'
```

Windows

```
aws ssm register-task-with-maintenance-window ^
    --window-id mw-0c50858d01EXAMPLE ^
    --task-arn "AWS-RunShellScript" ^
```

```
    --max-concurrency 1 --max-errors 1 --priority 10 ^
    --targets "Key=InstanceIds,Values=i-02573cafcfEXAMPLE" ^
    --task-type "RUN_COMMAND" ^
    --task-invocation-parameters "{\"RunCommand\":{\"Parameters\":{\"commands\":
[\"df\"]}}}"
```

`--cli-input-json` ファイルオプションで使用する JSON コンテンツ:

```
{
    "TaskType": "RUN_COMMAND",
    "WindowId": "mw-0c50858d01EXAMPLE",
    "Description": "My Run Command task to update SSM Agent on an instance",
    "MaxConcurrency": "1",
    "MaxErrors": "1",
    "Name": "My-Run-Command-Task",
    "Priority": 10,
    "Targets": [
        {
            "Key": "WindowTargetIds",
            "Values": [
                "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE"
            ]
        }
    ],
    "TaskArn": "AWS-UpdateSSMAgent",
    "TaskInvocationParameters": {
        "RunCommand": {
            "Comment": "A TaskInvocationParameters test comment",
            "NotificationConfig": {
                "NotificationArn": "arn:aws:sns:region:123456789012:my-sns-topic-name",
                "NotificationEvents": [
                    "All"
                ],
                "NotificationType": "Invocation"
            },
            "OutputS3BucketName": "amzn-s3-demo-bucket",
            "OutputS3KeyPrefix": "S3-PREFIX",
            "TimeoutSeconds": 3600
        }
    }
}
```

Systems Manager Automation タスクを登録する

以下の例では、AWS CLI を使用して Systems Manager Automation タスクをメンテナンスウィンドウに登録する方法を示しています。

AWS CLI コマンド:

Linux & macOS

```
aws ssm register-task-with-maintenance-window \
    --window-id "mw-0c50858d01EXAMPLE" \
    --task-arn "AWS-RestartEC2Instance" \
    --service-role-arn arn:aws:iam::123456789012:role/MyMaintenanceWindowServiceRole
 \
    --task-type AUTOMATION \
    --task-invocation-parameters
 "Automation={DocumentVersion=5,Parameters={InstanceId='{{RESOURCE_ID}}'}}" \
    --priority 0 --name "My-Restart-EC2-Instances-Automation-Task" \
    --description "Automation task to restart EC2 instances"
```

Windows

```
aws ssm register-task-with-maintenance-window ^
    --window-id "mw-0c50858d01EXAMPLE" ^
    --task-arn "AWS-RestartEC2Instance" ^
    --service-role-arn arn:aws:iam::123456789012:role/MyMaintenanceWindowServiceRole
 ^
    --task-type AUTOMATION ^
    --task-invocation-parameters
 "Automation={DocumentVersion=5,Parameters={InstanceId='{{TARGET_ID}}'}}" ^
    --priority 0 --name "My-Restart-EC2-Instances-Automation-Task" ^
    --description "Automation task to restart EC2 instances"
```

`--cli-input-json` ファイルオプションで使用する JSON コンテンツ:

```
{
    "WindowId": "mw-0c50858d01EXAMPLE",
        "TaskArn": "AWS-PatchInstanceWithRollback",
    "TaskType": "AUTOMATION","TaskInvocationParameters": {
        "Automation": {
            "DocumentVersion": "1",
            "Parameters": {
```

```
                "instanceId": [
                    "{{RESOURCE_ID}}"
                ]
            }
        }
    }
}
```

AWS Lambda タスクを登録する

以下の例では、AWS CLI を使用して Lambda 関数タスクをメンテナンスウィンドウに登録する方法を示しています。

これらの例では、Lambda 関数を作成したユーザーがその関数に SSMrestart-my-instances という名前を付け、instanceId と targetType という名前の 2 つのパラメータを作成したとします。

> **Important**
>
> Maintenance Windows の IAM ポリシーでは、Lambda 関数名 (またはエイリアス) の前にプレフィックス SSM を付ける必要があります。このタイプのタスクを登録する前に、AWS Lambda で SSM を含めるようにその名前を更新します。例えば、Lambda 関数名が MyLambdaFunction の場合は、SSMMyLambdaFunction に変更します。

AWS CLI コマンド:

Linux & macOS

> **Important**
>
> AWS CLI のバージョン 2 を使用している場合、Lambda ペイロードが base64 エンコードでなければ、以下のコマンドにオプション --cli-binary-format raw-in-base64-out を含める必要があります。cli_binary_format オプションは、バージョン 2 でしか使用できません。これと他の AWS CLI configファイル設定については、AWS Command Line Interface ユーザーガイドで「サポート対象 config ファイル設定」を参照してください。

```
aws ssm register-task-with-maintenance-window \
```

```
    --window-id "mw-0c50858d01EXAMPLE" \
    --targets "Key=WindowTargetIds,Values=e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE" \
    --priority 2 --max-concurrency 10 --max-errors 5 --name "My-Lambda-Example" \
    --description "A description for my LAMBDA example task" --task-type "LAMBDA" \
    --task-arn "arn:aws:lambda:region:123456789012:function:serverlessrepo-
SSMrestart-my-instances-C4JF9EXAMPLE" \
    --task-invocation-parameters '{"Lambda":{"Payload":"{\"InstanceId\":
\"{{RESOURCE_ID}}\",\"targetType\":\"{{TARGET_TYPE}}\"}","Qualifier": "$LATEST"}}'
```

PowerShell

> **Important**
>
> AWS CLI のバージョン 2 を使用している場合、Lambda ペイロードが base64 エンコードでなければ、以下のコマンドにオプション `--cli-binary-format raw-in-base64-out` を含める必要があります。`cli_binary_format` オプションは、バージョン 2 でしか使用できません。これと他の AWS CLI `config`ファイル設定については、AWS Command Line Interface ユーザーガイドで「サポート対象 config ファイル設定」を参照してください。

```
aws ssm register-task-with-maintenance-window `
    --window-id "mw-0c50858d01EXAMPLE" `
    --targets "Key=WindowTargetIds,Values=e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE" `
    --priority 2 --max-concurrency 10 --max-errors 5 --name "My-Lambda-Example" `
    --description "A description for my LAMBDA example task" --task-type "LAMBDA" `
    --task-arn "arn:aws:lambda:region:123456789012:function:serverlessrepo-
SSMrestart-my-instances-C4JF9EXAMPLE" `
    --task-invocation-parameters '{\"Lambda\":{\"Payload\":\"{\\\"InstanceId\\\":\\
\"{{RESOURCE_ID}}\\\",\\\"targetType\\\":\\\"{{TARGET_TYPE}}\\\"}\",\"Qualifier\":
 \"$LATEST\"}}'
```

`--cli-input-json` ファイルオプションで使用する JSON コンテンツ:

```
{
    "WindowId": "mw-0c50858d01EXAMPLE",
    "Targets": [
        {
            "Key": "WindowTargetIds",
            "Values": [
```

```
                "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE"
            ]
        }
    ],
    "TaskArn": "SSM_RestartMyInstances",
    "TaskType": "LAMBDA",
    "MaxConcurrency": "10",
    "MaxErrors": "10",
    "TaskInvocationParameters": {
        "Lambda": {
            "ClientContext": "ew0KICAi--truncated--0KIEXAMPLE",
            "Payload": "{ \"instanceId\": \"{{RESOURCE_ID}}\", \"targetType\":
 \"{{TARGET_TYPE}}\" }",
            "Qualifier": "$LATEST"
        }
    },
    "Name": "My-Lambda-Task",
    "Description": "A description for my LAMBDA task",
    "Priority": 5
}
```

Step Functions タスクを登録する

以下の例では、AWS CLI を使用して Step Functions ステートマシンタスクをメンテナンスウィンドウに登録する方法を示しています。

> **Note**
>
> メンテナンスウィンドウタスクは、Step Functions 標準ステートマシンワークフローのみをサポートします。Express ステートマシンワークフローはサポートされていません。ステートマシンワークフロータイプの詳細については、「AWS Step Functions デベロッパーガイド」の「標準ワークフローと Express ワークフロー」を参照してください。

これらの例では、ステップ関数ステートマシンを作成したユーザーが、`SSMMyStateMachine` というパラメータを指定して、`instanceId` という名前のステートマシンを作成しました。

> **Important**
>
> Maintenance Windows の AWS Identity and Access Management (IAM) ポリシーでは、Step Functions ステートマシン名の前に `SSM` でプレフィックスを付ける必要があります。こ

のタイプのタスクを登録する前に、AWS Step Functions で SSM を含めるようにその名前を更新する必要があります。たとえば、ステートマシン名が MyStateMachine の場合は、SSMMyStateMachine に変更します。

AWS CLI コマンド:

Linux & macOS

```
aws ssm register-task-with-maintenance-window \
    --window-id "mw-0c50858d01EXAMPLE" \
    --targets "Key=WindowTargetIds,Values=e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE" \
    --task-arn arn:aws:states:region:123456789012:stateMachine:SSMMyStateMachine-
MggiqEXAMPLE \
    --task-type STEP_FUNCTIONS \
    --task-invocation-parameters '{"StepFunctions":{"Input":"{\"InstanceId\":
\"{{RESOURCE_ID}}\"}", "Name":"{{INVOCATION_ID}}"}}' \
    --priority 0 --max-concurrency 10 --max-errors 5 \
    --name "My-Step-Functions-Task" --description "A description for my Step
 Functions task"
```

PowerShell

```
aws ssm register-task-with-maintenance-window `
    --window-id "mw-0c50858d01EXAMPLE" `
    --targets "Key=WindowTargetIds,Values=e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE" `
    --task-arn arn:aws:states:region:123456789012:stateMachine:SSMMyStateMachine-
MggiqEXAMPLE `
    --task-type STEP_FUNCTIONS `
    --task-invocation-parameters '{\"StepFunctions\":{\"Input\":\"{\\\"InstanceId\\
\":\\\"{{RESOURCE_ID}}\\\"}\", \"Name\":\"{{INVOCATION_ID}}\"}}' `
    --priority 0 --max-concurrency 10 --max-errors 5 `
    --name "My-Step-Functions-Task" --description "A description for my Step
 Functions task"
```

--cli-input-json ファイルオプションで使用する JSON コンテンツ:

```
{
    "WindowId": "mw-0c50858d01EXAMPLE",
    "Targets": [
        {
```

```
            "Key": "WindowTargetIds",
            "Values": [
                "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE"
            ]
        }
    ],
    "TaskArn": "SSM_MyStateMachine",
    "TaskType": "STEP_FUNCTIONS",
    "MaxConcurrency": "10",
    "MaxErrors": "10",
    "TaskInvocationParameters": {
        "StepFunctions": {
            "Input": "{ \"instanceId\": \"{{TARGET_ID}}\" }",
            "Name": "{{INVOCATION_ID}}"
        }
    },
    "Name": "My-Step-Functions-Task",
    "Description": "A description for my Step Functions task",
    "Priority": 5
}
```

"register-task-with-maintenance-window" コマンドのパラメーターオプション

register-task-with-maintenance-window コマンドには、必要に応じてタスクを設定するためのいくつかのオプションがあります。それらは、必須のオプション、任意のオプション、1 つのメンテナンスウィンドウタスクタイプにのみ適用されるオプションです。

このトピックでは、このチュートリアルのセクションでサンプルを使用するのに役立つ、これらのオプションのいくつかについて情報を提供します。すべてのコマンドオプションについては、AWS CLI コマンドリファレンスの「register-task-with-maintenance-window」を参照してください。

コマンドオプション: **`--task-arn`**

`--task-arn` オプションでは、タスクが実行するリソースを指定するために使用します。以下の表に示しているように、指定する値は登録するタスクのタイプによって異なります。

メンテナンスウィンドウタスクの TaskArn 形式

メンテナンスウィンドウタスクのタイプ	TaskArn 値
`RUN_COMMAND` および **`AUTOMATION`**	`TaskArn` は SSM ドキュメント名または Amazon リソースネーム (ARN) です。以下に例を示します。

メンテナンスウィンドウタスクのタイプ	TaskArn 値
	AWS-RunBatchShellScript -または- arn:aws:ssm: *region*:11112222 3333:document/My-Document .
LAMBDA	TaskArn は関数名または ARN です。以下に例を示します。 SSMMy-Lambda-Function -または- arn:aws:lambda: *region*:11112222 3333:function:SSMMyLambdaFu nction . **Important** Maintenance Windows の IAM ポリシーでは、Lambda 関数名 (またはエイリアス) の前にプレフィックス SSM を付ける必要があります。このタイプのタスクを登録する前に、AWS Lambda で SSM を含めるようにその名前を更新します。例えば、Lambda 関数名が MyLambdaFunction の場合は、SSMMyLambdaFunction に変更します。

メンテナンスウィンドウタスクのタイプ	TaskArn 値
STEP_FUNCTIONS	TaskArn はステートマシン ARN です。以下に例を示します。 arn:aws:states:us-east-2:111122223333:stateMachine:SSMMyStateMachine . **Important** メンテナンスウィンドウの IAM ポリシーでは、Step Functions ステートマシン名の前に SSM を付ける必要があります。このタイプのタスクを登録する前に、AWS Step Functions を含むように SSM の名前を更新する必要があります。たとえば、ステートマシン名が MyStateMachine の場合は、SSMMyStateMachine に変更します。

コマンドオプション: **--service-role-arn**

メンテナンスウィンドウタスクを実行するときに AWS Systems Manager が引き受けるロール。

詳細については、「Maintenance Windows を設定する」を参照してください。

コマンドオプション: **--task-invocation-parameters**

--task-invocation-parameters オプションを使用して、4 つのタスクタイプのそれぞれに固有のパラメータを指定します。以下の表では、4 つのタスクタイプそれぞれでサポートされているパラメータを示しています。

> **Note**
>
> `--task-invocation-parameters` コンテンツでの {{TARGET_ID}} などの疑似パラメータの使用については、「メンテナンスウィンドウのタスクを登録する際の疑似パラメータの使用」を参照してください。

メンテナンスウィンドウタスク用のタスク呼び出しパラメータのオプション

メンテナンスウィンドウタスクのタイプ	使用できるパラメータ	例

RUN_COMMAND	Comment
	DocumentHash
	DocumentHashType
	NotificationConfig
	OutputS3BucketName
	OutPutS3KeyPrefix
	Parameters
	ServiceRoleArn
	TimeoutSeconds
		<pre>"TaskInvocationParameters": {
		"RunCommand": {
		"Comment": "My Run Command task comment",
		"DocumentHash": "6554ed3d--truncated--5EXAMPLE",
		"DocumentHashType": "Sha256",
		"NotificationConfig": {
		"NotificationArn": "arn:aws:sns: region:123456789012:my-sns-topic-name",
		"NotificationEvents": [
		"FAILURE"
		],
		"NotificationType": "Invocation"
		},</pre>

メンテナンスウィンドウタスクのタイプ	使用できるパラメータ	例

		"OutputS3BucketName": "amzn-s3-demo-bucket",
		"OutputS3KeyPrefix": " *S3-PREFIX* ",
		"Parameters": {
		"commands": [
		"Get-ChildItem$env:temp-Recurse|Remove-Item-Recurse-force"
		]
		},
		"ServiceRoleArn": "arn:aws:iam::123456789012:role/MyMaintenanceWindowServiceRole",
		"TimeoutSeconds": 3600
		}
		}

メンテナンスウィンドウタスクのタイプ	使用できるパラメータ	例

AUTOMATION	DocumentVersion
	
	Parameters
		"TaskInvocationParameters": {
		"Automation": {
		"DocumentVersion": "3",
		"Parameters": {
		"instanceid": [
		"{{TARGET_ID}}"
		]
		}
		}
		}

LAMBDA	ClientContext
	
	Payload
	
	Qualifier
		"TaskInvocationParameters": {
		"Lambda": {
		"ClientContext": "ew0KICAi--truncated--0KIEXAMPLE",
		"Payload": "{ \"targetId\": \"{{TARGET_ID}}\",
		\"targetType\": \"{{TARGET_TYPE}}\" }",
		"Qualifier": "$LATEST"
		}
		}

メンテナンスウィンドウタスクのタイプ	使用できるパラメータ	例
STEP_FUNCTIONS	Input Name	"TaskInvocationParameters": { "StepFunctions": { "Input": "{ \"targetId\": \"{{TARGET_ID}}\" }", "Name": "{{INVOCATION_ID}}" } }

チュートリアル: AWS CLI を使用してメンテナンスウィンドウに関する情報を確認する

このチュートリアルでは、メンテナンスウィンドウ、タスク、実行、呼び出しに関する情報の更新や取得に役立つコマンドについて説明します。この例はコマンド別にまとめられており、表示したい詳細の種類をフィルタリングするためにコマンドオプションを使用する方法を示しています。

このチュートリアルの手順に従う際に、斜体の*##*テキストの値を、独自のオプションおよび ID に置き換えてください。例えば、メンテナンスウィンドウ ID *mw-0c50858d01EXAMPLE* とインスタンス ID *i-02573cafcfEXAMPLE* を、作成したリソースの ID に置き換えます。

AWS Command Line Interface (AWS CLI) のセットアップと構成については、「AWS CLI のインストール、更新、アンインストール」および「AWS CLI の設定」を参照してください。

コマンド例

- 'describe-maintenance-windows' の例
- 'describe-maintenance-window-targets' の例
- 'describe-maintenance-window-tasks' の例
- 「describe-maintenance-windows-for-target」の例
- 'describe-maintenance-window-executions'
- 'describe-maintenance-window-schedule'

'describe-maintenance-windows' の例

のすべてのメンテナンスウィンドウを一覧表示するAWS アカウント

以下のコマンドを実行します。

```
aws ssm describe-maintenance-windows
```

システムは以下のような情報を返します。

```
{
   "WindowIdentities":[
      {
         "WindowId":"mw-0c50858d01EXAMPLE",
         "Name":"My-First-Maintenance-Window",
         "Enabled":true,
         "Duration":2,
         "Cutoff":0,
         "NextExecutionTime": "2019-05-18T17:01:01.137Z"
      },
      {
         "WindowId":"mw-9a8b7c6d5eEXAMPLE",
         "Name":"My-Second-Maintenance-Window",
         "Enabled":true,
         "Duration":4,
         "Cutoff":1,
         "NextExecutionTime": "2019-05-30T03:30:00.137Z"
      },
   ]
}
```

有効なすべてのメンテナンスウィンドウを一覧表示する

以下のコマンドを実行します。

```
aws ssm describe-maintenance-windows --filters "Key=Enabled,Values=true"
```

システムは以下のような情報を返します。

```
{
   "WindowIdentities":[
```

```
      {
         "WindowId":"mw-0c50858d01EXAMPLE",
         "Name":"My-First-Maintenance-Window",
         "Enabled":true,
         "Duration":2,
         "Cutoff":0,
         "NextExecutionTime": "2019-05-18T17:01:01.137Z"
      },
      {
         "WindowId":"mw-9a8b7c6d5eEXAMPLE",
         "Name":"My-Second-Maintenance-Window",
         "Enabled":true,
         "Duration":4,
         "Cutoff":1,
         "NextExecutionTime": "2019-05-30T03:30:00.137Z"
      },
   ]
}
```

無効なすべてのメンテナンスウィンドウを一覧表示する

以下のコマンドを実行します。

```
aws ssm describe-maintenance-windows --filters "Key=Enabled,Values=false"
```

システムは以下のような情報を返します。

```
{
    "WindowIdentities": [
        {
            "WindowId": "mw-6e5c9d4b7cEXAMPLE",
            "Name": "My-Disabled-Maintenance-Window",
            "Enabled": false,
            "Duration": 2,
            "Cutoff": 1
        }
    ]
}
```

特定のプレフィックスから始まる名前を持つすべてのメンテナンスウィンドウを一覧表示する

以下のコマンドを実行します。

```
aws ssm describe-maintenance-windows --filters "Key=Name,Values=My"
```

システムは以下のような情報を返します。

```
{
    "WindowIdentities": [
        {
            "WindowId": "mw-0c50858d01EXAMPLE",
            "Name": "My-First-Maintenance-Window",
            "Enabled": true,
            "Duration": 2,
            "Cutoff": 0,
            "NextExecutionTime": "2019-05-18T17:01:01.137Z"
        },
        {
            "WindowId": "mw-9a8b7c6d5eEXAMPLE",
            "Name": "My-Second-Maintenance-Window",
            "Enabled": true,
            "Duration": 4,
            "Cutoff": 1,
            "NextExecutionTime": "2019-05-30T03:30:00.137Z"
        },
        {
            "WindowId": "mw-6e5c9d4b7cEXAMPLE",
            "Name": "My-Disabled-Maintenance-Window",
            "Enabled": false,
            "Duration": 2,
            "Cutoff": 1
        }
    ]
}
```

'describe-maintenance-window-targets' の例

特定の所有者情報の値に一致するメンテナンスウィンドウのターゲットを表示する

次のコマンドを実行します。

Linux & macOS

```
aws ssm describe-maintenance-window-targets \
    --window-id "mw-6e5c9d4b7cEXAMPLE" \
```

```
    --filters "Key=OwnerInformation,Values=CostCenter1"
```

Windows

```
aws ssm describe-maintenance-window-targets ^
    --window-id "mw-6e5c9d4b7cEXAMPLE" ^
    --filters "Key=OwnerInformation,Values=CostCenter1"
```

> **Note**
>
> サポートされているフィルタキーは Type、WindowTargetId、OwnerInformation です。

システムは以下のような情報を返します。

```
{
    "Targets": [
        {
            "WindowId": "mw-0c50858d01EXAMPLE",
            "WindowTargetId": "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE",
            "ResourceType": "INSTANCE",
            "Targets": [
                {
                    "Key": "tag:Name",
                    "Values": [
                        "Production"
                    ]
                }
            ],
            "OwnerInformation": "CostCenter1",
            "Name": "Target1"
        }
    ]
}
```

'describe-maintenance-window-tasks' の例

SSM コマンドドキュメント **AWS-RunPowerShellScript** を呼び出す登録されたタスクをすべて表示する

次のコマンドを実行します。

Linux & macOS

```
aws ssm describe-maintenance-window-tasks \
    --window-id "mw-0c50858d01EXAMPLE" \
    --filters "Key=TaskArn,Values=AWS-RunPowerShellScript"
```

Windows

```
aws ssm describe-maintenance-window-tasks ^
    --window-id "mw-0c50858d01EXAMPLE" ^
    --filters "Key=TaskArn,Values=AWS-RunPowerShellScript"
```

システムは以下のような情報を返します。

```
{
   "Tasks":[
      {
         "ServiceRoleArn": "arn:aws:iam::111122223333:role/
MyMaintenanceWindowServiceRole",
         "MaxErrors":"1",
         "TaskArn":"AWS-RunPowerShellScript",
         "MaxConcurrency":"1",
         "WindowTaskId":"4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE",
         "TaskParameters":{
            "commands":{
               "Values":[
                  "driverquery.exe"
               ]
            }
         },
         "Priority":3,
         "Type":"RUN_COMMAND",
         "Targets":[
            {
               "TaskTargetId":"i-02573cafcfEXAMPLE",
               "TaskTargetType":"INSTANCE"
            }
         ]
      },
      {
```

```
         "ServiceRoleArn":"arn:aws:iam::111122223333:role/
MyMaintenanceWindowServiceRole",
         "MaxErrors":"1",
         "TaskArn":"AWS-RunPowerShellScript",
         "MaxConcurrency":"1",
         "WindowTaskId":"4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE",
         "TaskParameters":{
            "commands":{
               "Values":[
                  "ipconfig"
               ]
            }
         },
         "Priority":1,
         "Type":"RUN_COMMAND",
         "Targets":[
            {
               "TaskTargetId":"i-02573cafcfEXAMPLE",
               "TaskTargetType":"WINDOW_TARGET"
            }
         ]
      }
   ]
}
```

優先度 "3" の登録されたタスクをすべて表示する

次のコマンドを実行します。

Linux & macOS

```
aws ssm describe-maintenance-window-tasks \
    --window-id "mw-9a8b7c6d5eEXAMPLE" \
    --filters "Key=Priority,Values=3"
```

Windows

```
aws ssm describe-maintenance-window-tasks ^
    --window-id "mw-9a8b7c6d5eEXAMPLE" ^
    --filters "Key=Priority,Values=3"
```

システムは以下のような情報を返します。

```
{
   "Tasks":[
      {
         "ServiceRoleArn":"arn:aws:iam::111122223333:role/
MyMaintenanceWindowServiceRole",
         "MaxErrors":"1",
         "TaskArn":"AWS-RunPowerShellScript",
         "MaxConcurrency":"1",
         "WindowTaskId":"4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE",
         "TaskParameters":{
            "commands":{
               "Values":[
                  "driverquery.exe"
               ]
            }
         },
         "Priority":3,
         "Type":"RUN_COMMAND",
         "Targets":[
            {
               "TaskTargetId":"i-02573cafcfEXAMPLE",
               "TaskTargetType":"INSTANCE"
            }
         ]
      }
   ]
}
```

優先度 "1" および Run Command を使用するすべての登録されたタスクを表示する

以下のコマンドを実行します。

Linux & macOS

```
aws ssm describe-maintenance-window-tasks \
    --window-id "mw-0c50858d01EXAMPLE" \
    --filters "Key=Priority,Values=1" "Key=TaskType,Values=RUN_COMMAND"
```

Windows

```
aws ssm describe-maintenance-window-tasks ^
    --window-id "mw-0c50858d01EXAMPLE" ^
```

```
    --filters "Key=Priority,Values=1" "Key=TaskType,Values=RUN_COMMAND"
```

システムは以下のような情報を返します。

```
{
    "Tasks": [
        {
            "WindowId": "mw-0c50858d01EXAMPLE",
            "WindowTaskId": "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE",
            "TaskArn": "AWS-RunShellScript",
            "Type": "RUN_COMMAND",
            "Targets": [
                {
                    "Key": "InstanceIds",
                    "Values": [
                        "i-02573cafcfEXAMPLE"
                    ]
                }
            ],
            "TaskParameters": {},
            "Priority": 1,
            "ServiceRoleArn": "arn:aws:iam::111122223333:role/
MyMaintenanceWindowServiceRole",
            "MaxConcurrency": "1",
            "MaxErrors": "1"
        },
        {
            "WindowId": "mw-0c50858d01EXAMPLE",
            "WindowTaskId": "8a5c4629-31b0-4edd-8aea-33698EXAMPLE",
            "TaskArn": "AWS-UpdateSSMAgent",
            "Type": "RUN_COMMAND",
            "Targets": [
                {
                    "Key": "InstanceIds",
                    "Values": [
                        "i-0471e04240EXAMPLE"
                    ]
                }
            ],
            "TaskParameters": {},
            "Priority": 1,
```

```
            "ServiceRoleArn": "arn:aws:iam::111122223333:role/
MyMaintenanceWindowServiceRole",
            "MaxConcurrency": "1",
            "MaxErrors": "1",
            "Name": "My-Run-Command-Task",
            "Description": "My Run Command task to update SSM Agent on an instance"
        }
    ]
}
```

「describe-maintenance-windows-for-target」の例

特定のノードに関連付けられたメンテナンスウィンドウターゲットまたはタスクに関する情報を一覧表示する

以下のコマンドを実行します。

Linux & macOS

```
aws ssm describe-maintenance-windows-for-target \
    --resource-type INSTANCE \
    --targets "Key=InstanceIds,Values=i-02573cafcfEXAMPLE" \
    --max-results 10
```

Windows

```
aws ssm describe-maintenance-windows-for-target ^
    --resource-type INSTANCE ^
    --targets "Key=InstanceIds,Values=i-02573cafcfEXAMPLE" ^
    --max-results 10
```

システムは以下のような情報を返します。

```
{
    "WindowIdentities": [
        {
            "WindowId": "mw-0c50858d01EXAMPLE",
            "Name": "My-First-Maintenance-Window"
        },
        {
            "WindowId": "mw-9a8b7c6d5eEXAMPLE",
            "Name": "My-Second-Maintenance-Window"
```

```
        }
    ]
}
```

'describe-maintenance-window-executions'

特定の日付の前に実行されたタスクを一覧表示する

次のコマンドを実行します。

Linux & macOS

```
aws ssm describe-maintenance-window-executions \
    --window-id "mw-9a8b7c6d5eEXAMPLE" \
    --filters "Key=ExecutedBefore,Values=2019-05-12T05:00:00Z"
```

Windows

```
aws ssm describe-maintenance-window-executions ^
    --window-id "mw-9a8b7c6d5eEXAMPLE" ^
    --filters "Key=ExecutedBefore,Values=2019-05-12T05:00:00Z"
```

システムは以下のような情報を返します。

```
{
    "WindowExecutions": [
        {
            "WindowId": "mw-0c50858d01EXAMPLE",
            "WindowExecutionId": "14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE",
            "Status": "FAILED",
            "StatusDetails": "The following SSM parameters are invalid: LevelUp",
            "StartTime": 1557617747.993,
            "EndTime": 1557617748.101
        },
        {
            "WindowId": "mw-9a8b7c6d5eEXAMPLE",
            "WindowExecutionId": "791b72e0-f0da-4021-8b35-f95dfEXAMPLE",
            "Status": "SUCCESS",
            "StartTime": 1557594085.428,
            "EndTime": 1557594090.978
        },
        {
```

```
            "WindowId": "mw-0c50858d01EXAMPLE",
            "WindowExecutionId": "ecec60fa-6bb0-4d26-98c7-140308EXAMPLE",
            "Status": "SUCCESS",
            "StartTime": 1557593793.483,
            "EndTime": 1557593798.978
        }
    ]
}
```

特定の日付の後で実行されるすべてのタスクを一覧表示する

次のコマンドを実行します。

Linux & macOS

```
aws ssm describe-maintenance-window-executions \
    --window-id "mw-9a8b7c6d5eEXAMPLE" \
    --filters "Key=ExecutedAfter,Values=2018-12-31T17:00:00Z"
```

Windows

```
aws ssm describe-maintenance-window-executions ^
    --window-id "mw-9a8b7c6d5eEXAMPLE" ^
    --filters "Key=ExecutedAfter,Values=2018-12-31T17:00:00Z"
```

システムは以下のような情報を返します。

```
{
    "WindowExecutions": [
        {
            "WindowId": "mw-0c50858d01EXAMPLE",
            "WindowExecutionId": "14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE",
            "Status": "FAILED",
            "StatusDetails": "The following SSM parameters are invalid: LevelUp",
            "StartTime": 1557617747.993,
            "EndTime": 1557617748.101
        },
        {
            "WindowId": "mw-9a8b7c6d5eEXAMPLE",
            "WindowExecutionId": "791b72e0-f0da-4021-8b35-f95dfEXAMPLE",
            "Status": "SUCCESS",
            "StartTime": 1557594085.428,
```

```
            "EndTime": 1557594090.978
        },
        {
            "WindowId": "mw-0c50858d01EXAMPLE",
            "WindowExecutionId": "ecec60fa-6bb0-4d26-98c7-140308EXAMPLE",
            "Status": "SUCCESS",
            "StartTime": 1557593793.483,
            "EndTime": 1557593798.978
        }
    ]
}
```

'describe-maintenance-window-schedule'

特定のノードで実行する次の 10 個のスケジュールされたメンテナンスウィンドウを表示する

以下のコマンドを実行します。

Linux & macOS

```
aws ssm describe-maintenance-window-schedule \
    --resource-type INSTANCE \
    --targets "Key=InstanceIds,Values=i-07782c72faEXAMPLE" \
    --max-results 10
```

Windows

```
aws ssm describe-maintenance-window-schedule ^
    --resource-type INSTANCE ^
    --targets "Key=InstanceIds,Values=i-07782c72faEXAMPLE" ^
    --max-results 10
```

システムは以下のような情報を返します。

```
{
    "ScheduledWindowExecutions": [
        {
            "WindowId": "mw-0c50858d01EXAMPLE",
            "Name": "My-First-Maintenance-Window",
            "ExecutionTime": "2019-05-18T23:35:24.902Z"
        },
        {
```

```
            "WindowId": "mw-0c50858d01EXAMPLE",
            "Name": "My-First-Maintenance-Window",
            "ExecutionTime": "2019-05-25T23:35:24.902Z"
        },
        {
            "WindowId": "mw-0c50858d01EXAMPLE",
            "Name": "My-First-Maintenance-Window",
            "ExecutionTime": "2019-06-01T23:35:24.902Z"
        },
        {
            "WindowId": "mw-0c50858d01EXAMPLE",
            "Name": "My-First-Maintenance-Window",
            "ExecutionTime": "2019-06-08T23:35:24.902Z"
        },
        {
            "WindowId": "mw-9a8b7c6d5eEXAMPLE",
            "Name": "My-Second-Maintenance-Window",
            "ExecutionTime": "2019-06-15T23:35:24.902Z"
        },
        {
            "WindowId": "mw-0c50858d01EXAMPLE",
            "Name": "My-First-Maintenance-Window",
            "ExecutionTime": "2019-06-22T23:35:24.902Z"
        },
        {
            "WindowId": "mw-9a8b7c6d5eEXAMPLE",
            "Name": "My-Second-Maintenance-Window",
            "ExecutionTime": "2019-06-29T23:35:24.902Z"
        },
        {
            "WindowId": "mw-0c50858d01EXAMPLE",
            "Name": "My-First-Maintenance-Window",
            "ExecutionTime": "2019-07-06T23:35:24.902Z"
        },
        {
            "WindowId": "mw-9a8b7c6d5eEXAMPLE",
            "Name": "My-Second-Maintenance-Window",
            "ExecutionTime": "2019-07-13T23:35:24.902Z"
        },
        {
            "WindowId": "mw-0c50858d01EXAMPLE",
            "Name": "My-First-Maintenance-Window",
            "ExecutionTime": "2019-07-20T23:35:24.902Z"
        }
```

```
    ],
    "NextToken": "AAEABUXdceT92FvtKld/dGHELj5Mi+GKW/EXAMPLE"
}
```

特定のキーと値のペアでタグ付けされたノードのメンテナンスウィンドウのスケジュールを表示する

以下のコマンドを実行します。

Linux & macOS

```
aws ssm describe-maintenance-window-schedule \
    --resource-type INSTANCE \
    --targets "Key=tag:prod,Values=rhel7"
```

Windows

```
aws ssm describe-maintenance-window-schedule ^
    --resource-type INSTANCE ^
    --targets "Key=tag:prod,Values=rhel7"
```

システムは以下のような情報を返します。

```
{
    "ScheduledWindowExecutions": [
        {
            "WindowId": "mw-0c50858d01EXAMPLE",
            "Name": "DemoRateStartDate",
            "ExecutionTime": "2019-10-20T05:34:56-07:00"
        },
        {
            "WindowId": "mw-0c50858d01EXAMPLE",
            "Name": "DemoRateStartDate",
            "ExecutionTime": "2019-10-21T05:34:56-07:00"
        },
        {
            "WindowId": "mw-0c50858d01EXAMPLE",
            "Name": "DemoRateStartDate",
            "ExecutionTime": "2019-10-22T05:34:56-07:00"
        },
        {
            "WindowId": "mw-0c50858d01EXAMPLE",
```

```
            "Name": "DemoRateStartDate",
            "ExecutionTime": "2019-10-23T05:34:56-07:00"
        },
        {
            "WindowId": "mw-0c50858d01EXAMPLE",
            "Name": "DemoRateStartDate",
            "ExecutionTime": "2019-10-24T05:34:56-07:00"
        }
    ],
    "NextToken": "AAEABccwSXqQRGKiTZ1yzGELR6cxW4W/EXAMPLE"
}
```

次の 4 つの開始時間を表示し、メンテナンスウィンドウの実行

次のコマンドを実行します。

Linux & macOS

```
aws ssm describe-maintenance-window-schedule \
    --window-id "mw-0c50858d01EXAMPLE" \
    --max-results "4"
```

Windows

```
aws ssm describe-maintenance-window-schedule ^
    --window-id "mw-0c50858d01EXAMPLE" ^
    --max-results "4"
```

システムは以下のような情報を返します。

```
{
    "WindowSchedule": [
        {
            "ScheduledWindowExecutions": [
                {
                    "ExecutionTime": "2019-10-04T10:10:10Z",
                    "Name": "My-First-Maintenance-Window",
                    "WindowId": "mw-0c50858d01EXAMPLE"
                },
                {
                    "ExecutionTime": "2019-10-11T10:10:10Z",
                    "Name": "My-First-Maintenance-Window",
```

```
                "WindowId": "mw-0c50858d01EXAMPLE"
            },
            {
                "ExecutionTime": "2019-10-18T10:10:10Z",
                "Name": "My-First-Maintenance-Window",
                "WindowId": "mw-0c50858d01EXAMPLE"
            },
            {
                "ExecutionTime": "2019-10-25T10:10:10Z",
                "Name": "My-First-Maintenance-Window",
                "WindowId": "mw-0c50858d01EXAMPLE"
            }
        ]
    }
]
}
```

チュートリアル: AWS CLI を使用してタスクおよびタスク実行に関する情報を確認する

このチュートリアルでは、AWS Command Line Interface (AWS CLI) を使用して、完了したメンテナンスウィンドウの実行に関する詳細を表示する方法を説明します。

チュートリアル: AWS CLI を使用してメンテナンスウィンドウを作成および設定する から直接進む場合は、実行結果を確認するために、メンテナンスウィンドウが少なくとも 1 回実行できる十分な時間があることを確認してください。

このチュートリアルの手順に従う際に、斜体の*##*テキストの値を、独自のオプションおよび ID に置き換えてください。例えば、メンテナンスウィンドウ ID *mw-0c50858d01EXAMPLE* とインスタンス ID *i-02573cafcfEXAMPLE* を、作成したリソースの ID に置き換えます。

AWS CLI を使用してタスクおよびタスク実行に関する情報を確認するには

1. 以下のコマンドを実行して、特定のメンテナンスウィンドウのタスクの実行を一覧表示します。

   Linux & macOS

   ```
   aws ssm describe-maintenance-window-executions \
       --window-id "mw-0c50858d01EXAMPLE"
   ```

   Windows

   ```
   aws ssm describe-maintenance-window-executions ^
   ```

```
    --window-id "mw-0c50858d01EXAMPLE"
```

システムは以下のような情報を返します。

```
{
    "WindowExecutions": [
        {
            "WindowId": "mw-0c50858d01EXAMPLE",
            "WindowExecutionId": "14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE",
            "Status": "SUCCESS",
            "StartTime": 1557593793.483,
            "EndTime": 1557593798.978
        },
        {
            "WindowId": "mw-0c50858d01EXAMPLE",
            "WindowExecutionId": "791b72e0-f0da-4021-8b35-f95dfEXAMPLE",
            "Status": "SUCCESS",
            "StartTime": 1557593493.096,
            "EndTime": 1557593498.611
        },
        {
            "WindowId": "mw-0c50858d01EXAMPLE",
            "WindowExecutionId": "ecec60fa-6bb0-4d26-98c7-140308EXAMPLE",
            "Status": "SUCCESS",
            "StatusDetails": "No tasks to execute.",
            "StartTime": 1557593193.309,
            "EndTime": 1557593193.334
        }
    ]
}
```

2. 次のコマンドを実行して、メンテナンスウィンドウのタスクの実行に関する情報を取得します。

Linux & macOS

```
aws ssm get-maintenance-window-execution \
    --window-execution-id "14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE"
```

Windows

```
aws ssm get-maintenance-window-execution ^
```

```
    --window-execution-id "14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE"
```

システムは以下のような情報を返します。

```
{
    "WindowExecutionId": "14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE",
    "TaskIds": [
        "c9b05aba-197f-4d8d-be34-e73fbEXAMPLE"
    ],
    "Status": "SUCCESS",
    "StartTime": 1557593493.096,
    "EndTime": 1557593498.611
}
```

3. 次のコマンドを実行して、メンテナンスウィンドウの一部として実行されるタスクリストを実行します。

Linux & macOS

```
aws ssm describe-maintenance-window-execution-tasks \
    --window-execution-id "14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE"
```

Windows

```
aws ssm describe-maintenance-window-execution-tasks ^
    --window-execution-id "14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE"
```

システムは以下のような情報を返します。

```
{
    "WindowExecutionTaskIdentities": [
        {
            "WindowExecutionId": "14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE",
            "TaskExecutionId": "c9b05aba-197f-4d8d-be34-e73fbEXAMPLE",
            "Status": "SUCCESS",
            "StartTime": 1557593493.162,
            "EndTime": 1557593498.57,
            "TaskArn": "AWS-RunShellScript",
            "TaskType": "RUN_COMMAND"
        }
```

```
    ]
}
```

4. 次のコマンドを実行して、タスク実行の詳細を取得します。

Linux & macOS

```
aws ssm get-maintenance-window-execution-task \
    --window-execution-id "14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE" \
    --task-id "c9b05aba-197f-4d8d-be34-e73fbEXAMPLE"
```

Windows

```
aws ssm get-maintenance-window-execution-task ^
    --window-execution-id "14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE" ^
    --task-id "c9b05aba-197f-4d8d-be34-e73fbEXAMPLE"
```

システムは以下のような情報を返します。

```
{
    "WindowExecutionId": "14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE",
    "TaskExecutionId": "c9b05aba-197f-4d8d-be34-e73fbEXAMPLE",
    "TaskArn": "AWS-RunShellScript",
    "ServiceRole": "arn:aws:iam::111122223333:role/MyMaintenanceWindowServiceRole",
    "Type": "RUN_COMMAND",
    "TaskParameters": [
        {
            "aws:InstanceId": {
                "Values": [
                    "i-02573cafcfEXAMPLE"
                ]
            },
            "commands": {
                "Values": [
                    "df"
                ]
            }
        }
    ],
    "Priority": 10,
    "MaxConcurrency": "1",
```

```
    "MaxErrors": "1",
    "Status": "SUCCESS",
    "StartTime": 1557593493.162,
    "EndTime": 1557593498.57
}
```

5. 次のコマンドを実行して、タスク実行のために行われた特定のタスク呼び出しを取得します。

   Linux & macOS

   ```
   aws ssm describe-maintenance-window-execution-task-invocations \
       --window-execution-id "14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE" \
       --task-id "c9b05aba-197f-4d8d-be34-e73fbEXAMPLE"
   ```

   Windows

   ```
   aws ssm describe-maintenance-window-execution-task-invocations ^
       --window-execution-id "14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE" ^
       --task-id "c9b05aba-197f-4d8d-be34-e73fbEXAMPLE"
   ```

   システムは以下のような情報を返します。

   ```
   {
       "WindowExecutionTaskInvocationIdentities": [
           {
               "WindowExecutionId": "14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE",
               "TaskExecutionId": "c9b05aba-197f-4d8d-be34-e73fbEXAMPLE",
               "InvocationId": "c336d2ab-09de-44ba-8f6a-6136cEXAMPLE",
               "ExecutionId": "76a5a04f-caf6-490c-b448-92c02EXAMPLE",
               "TaskType": "RUN_COMMAND",
               "Parameters": "{\"documentName\":\"AWS-RunShellScript\",\"instanceIds
   \":[\"i-02573cafcfEXAMPLE\"],\"maxConcurrency\":\"1\",\"maxErrors\":\"1\",
   \"parameters\":{\"commands\":[\"df\"]}}",
               "Status": "SUCCESS",
               "StatusDetails": "Success",
               "StartTime": 1557593493.222,
               "EndTime": 1557593498.466
           }
       ]
   }
   ```

チュートリアル : AWS CLI を使用してメンテナンスウィンドウを更新する

このチュートリアルでは、メンテナンスウィンドウの更新に AWS Command Line Interface (AWS CLI) を使用する方法を示します。異なるタスクタイプを更新する方法についても説明します。これらには、AWS Systems Manager Run Command と Automation、AWS Lambda、AWS Step Functions が含まれます。

このセクションの例では、メンテナンスウィンドウの更新に次の Systems Manager アクションを使用します。

- UpdateMaintenanceWindow
- UpdateMaintenanceWindowTarget
- UpdateMaintenanceWindowTask
- DeregisterTargetFromMaintenanceWindow

Systems Manager コンソールを使用してメンテナンスウィンドウを更新する方法については、「コンソールを使用してメンテナンスウィンドウリソースを更新または削除する」を参照してください。

このチュートリアルの手順に従う際に、斜体の*##*テキストの値を、独自のオプションおよび ID に置き換えてください。例えば、メンテナンスウィンドウ ID *mw-0c50858d01EXAMPLE* とインスタンス ID *i-02573cafcfEXAMPLE* を、作成したリソースの ID に置き換えます。

AWS CLI を使用してメンテナンスウィンドウを更新するには

1. AWS CLI を開き、次のコマンドを実行して、ターゲットを更新し、名前と説明を含めます。

   Linux & macOS

   ```
   aws ssm update-maintenance-window-target \
       --window-id "mw-0c50858d01EXAMPLE" \
       --window-target-id "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE" \
       --name "My-Maintenance-Window-Target" \
       --description "Description for my maintenance window target"
   ```

   Windows

   ```
   aws ssm update-maintenance-window-target ^
       --window-id "mw-0c50858d01EXAMPLE" ^
       --window-target-id "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE" ^
   ```

```
    --name "My-Maintenance-Window-Target" ^
    --description "Description for my maintenance window target"
```

システムは以下のような情報を返します。

```
{
    "WindowId": "mw-0c50858d01EXAMPLE",
    "WindowTargetId": "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE",
    "Targets": [
        {
            "Key": "InstanceIds",
            "Values": [
                "i-02573cafcfEXAMPLE"
            ]
        }
    ],
    "Name": "My-Maintenance-Window-Target",
    "Description": "Description for my maintenance window target"
}
```

2. 次のコマンドを実行し、replace オプションを使用して説明フィールドを削除して別のターゲットを追加します。後進に説明フィールドが含まれていない (Null 値) ため、このフィールドは削除されます。Systems Manager で使用するように設定されている追加のノードを必ず指定してください。

   Linux & macOS

   ```
   aws ssm update-maintenance-window-target \
       --window-id "mw-0c50858d01EXAMPLE" \
       --window-target-id "d208dedf-3f6b-41ff-ace8-8e751EXAMPLE" \
       --targets "Key=InstanceIds,Values=i-02573cafcfEXAMPLE,i-0471e04240EXAMPLE" \
       --name "My-Maintenance-Window-Target" \
       --replace
   ```

   Windows

   ```
   aws ssm update-maintenance-window-target ^
       --window-id "mw-0c50858d01EXAMPLE" ^
       --window-target-id "d208dedf-3f6b-41ff-ace8-8e751EXAMPLE" ^
       --targets "Key=InstanceIds,Values=i-02573cafcfEXAMPLE,i-0471e04240EXAMPLE" ^
       --name "My-Maintenance-Window-Target" ^
   ```

```
    --replace
```

システムは以下のような情報を返します。

```
{
    "WindowId": "mw-0c50858d01EXAMPLE",
    "WindowTargetId": "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE",
    "Targets": [
        {
            "Key": "InstanceIds",
            "Values": [
                "i-02573cafcfEXAMPLE",
                "i-0471e04240EXAMPLE"
            ]
        }
    ],
    "Name": "My-Maintenance-Window-Target"
}
```

3. start-date オプションにより、指定した将来の日付までメンテナンスウィンドウのアクティベーションを遅らせることができます。この end-date オプションを設定できます。その後、将来の日付と時刻をメンテナンスウィンドウが実行されなくなりました。拡張された形式の ISO-8601 のオプションを指定します。

   次のコマンドを実行し、日時の範囲を指定する場合は定期的にスケジュールされたメンテナンスを実行します。

   Linux & macOS

   ```
   aws ssm update-maintenance-window \
       --window-id "mw-0c50858d01EXAMPLE" \
       --start-date "2020-10-01T10:10:10Z" \
       --end-date "2020-11-01T10:10:10Z"
   ```

   Windows

   ```
   aws ssm update-maintenance-window ^
       --window-id "mw-0c50858d01EXAMPLE" ^
       --start-date "2020-10-01T10:10:10Z" ^
       --end-date "2020-11-01T10:10:10Z"
   ```

4. 次のコマンドを実行して Run Command タスクを更新します。

> **Tip**
>
> ターゲットが Windows Server の Amazon Elastic Compute Cloud (Amazon EC2) インスタンスの場合は、以下のコマンドで df を ipconfig に、AWS-RunShellScript を AWS-RunPowerShellScript に変更します。

Linux & macOS

```
aws ssm update-maintenance-window-task \
    --window-id "mw-0c50858d01EXAMPLE" \
    --window-task-id "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE" \
    --targets "Key=WindowTargetIds,Values=e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE"
 \
    --task-arn "AWS-RunShellScript" \
    --service-role-arn "arn:aws:iam::account-id:role/MaintenanceWindowsRole" \
    --task-invocation-parameters "RunCommand={Comment=Revising my Run Command
 task,Parameters={commands=df}}" \
    --priority 1 --max-concurrency 10 --max-errors 4 \
    --name "My-Task-Name" --description "A description for my Run Command task"
```

Windows

```
aws ssm update-maintenance-window-task ^
    --window-id "mw-0c50858d01EXAMPLE" ^
    --window-task-id "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE" ^
    --targets "Key=WindowTargetIds,Values=e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE"
 ^
    --task-arn "AWS-RunShellScript" ^
    --service-role-arn "arn:aws:iam::account-id:role/MaintenanceWindowsRole" ^
    --task-invocation-parameters "RunCommand={Comment=Revising my Run Command
 task,Parameters={commands=df}}" ^
    --priority 1 --max-concurrency 10 --max-errors 4 ^
    --name "My-Task-Name" --description "A description for my Run Command task"
```

システムは以下のような情報を返します。

```
{
```

```
    "WindowId": "mw-0c50858d01EXAMPLE",
    "WindowTaskId": "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE",
    "Targets": [
        {
            "Key": "WindowTargetIds",
            "Values": [
                "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE"
            ]
        }
    ],
    "TaskArn": "AWS-RunShellScript",
    "ServiceRoleArn": "arn:aws:iam::111122223333:role/MaintenanceWindowsRole",
    "TaskParameters": {},
    "TaskInvocationParameters": {
        "RunCommand": {
            "Comment": "Revising my Run Command task",
            "Parameters": {
                "commands": [
                    "df"
                ]
            }
        }
    },
    "Priority": 1,
    "MaxConcurrency": "10",
    "MaxErrors": "4",
    "Name": "My-Task-Name",
    "Description": "A description for my Run Command task"
}
```

5. 次のコマンドを調整および実行して Lambda タスクを更新します。

   Linux & macOS

```
aws ssm update-maintenance-window-task \
    --window-id mw-0c50858d01EXAMPLE \
    --window-task-id 4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE \
    --targets "Key=WindowTargetIds,Values=e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE"
 \
    --task-arn "arn:aws:lambda:region:111122223333:function:SSMTestLambda" \
    --service-role-arn "arn:aws:iam:account-id:role/MaintenanceWindowsRole" \
    --task-invocation-parameters '{"Lambda":{"Payload":"{\"InstanceId\":
\"{{RESOURCE_ID}}\",\"targetType\":\"{{TARGET_TYPE}}\"}"}}' \
    --priority 1 --max-concurrency 10 --max-errors 5 \
```

```
    --name "New-Lambda-Task-Name" \
    --description "A description for my Lambda task"
```

Windows

```
aws ssm update-maintenance-window-task ^
    --window-id mw-0c50858d01EXAMPLE ^
    --window-task-id 4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE ^
    --targets "Key=WindowTargetIds,Values=e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE"
 ^
    --task-arn --task-arn
 "arn:aws:lambda:region:111122223333:function:SSMTestLambda" ^
    --service-role-arn "arn:aws:iam:account-id:role/MaintenanceWindowsRole" ^
    --task-invocation-parameters '{"Lambda":{"Payload":"{\"InstanceId\":
\"{{RESOURCE_ID}}\",\"targetType\":\"{{TARGET_TYPE}}\"}"}}' ^
    --priority 1 --max-concurrency 10 --max-errors 5 ^
    --name "New-Lambda-Task-Name" ^
    --description "A description for my Lambda task"
```

システムは以下のような情報を返します。

```
{
    "WindowId": "mw-0c50858d01EXAMPLE",
    "WindowTaskId": "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE",
    "Targets": [
        {
            "Key": "WindowTargetIds",
            "Values": "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE"
        }
    ],
    "TaskArn": "arn:aws:lambda:us-east-2:111122223333:function:SSMTestLambda",
    "ServiceRoleArn": "arn:aws:iam::111122223333:role/MaintenanceWindowsRole",
    "TaskParameters": {},
    "TaskInvocationParameters": {
        "Lambda": {
            "Payload": "e30="
        }
    },
    "Priority": 1,
    "MaxConcurrency": "10",
    "MaxErrors": "5",
    "Name": "New-Lambda-Task-Name",
```

```
    "Description": "A description for my Lambda task"
}
```

6. Step Functions タスクを更新する場合は、task-invocation-parameters を更新するように以下のコマンドを調整して実行します。

   Linux & macOS

```
aws ssm update-maintenance-window-task \
    --window-id "mw-0c50858d01EXAMPLE" \
    --window-task-id "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE" \
    --targets "Key=WindowTargetIds,Values=e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE"
 \
    --task-arn "arn:aws:states:region:execution:SSMStepFunctionTest" \
    --service-role-arn "arn:aws:iam:account-id:role/MaintenanceWindowsRole" \
    --task-invocation-parameters '{"StepFunctions":{"Input":"{\"InstanceId\":
\"{{RESOURCE_ID}}\"}"}}' \
    --priority 0 --max-concurrency 10 --max-errors 5 \
    --name "My-Step-Functions-Task" \
    --description "A description for my Step Functions task"
```

   Windows

```
aws ssm update-maintenance-window-task ^
    --window-id "mw-0c50858d01EXAMPLE" ^
    --window-task-id "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE" ^
    --targets "Key=WindowTargetIds,Values=e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE"
 ^
    --task-arn "arn:aws:states:region:execution:SSMStepFunctionTest" ^
    --service-role-arn "arn:aws:iam:account-id:role/MaintenanceWindowsRole" ^
    --task-invocation-parameters '{"StepFunctions":{"Input":"{\"InstanceId\":
\"{{RESOURCE_ID}}\"}"}}' ^
    --priority 0 --max-concurrency 10 --max-errors 5 ^
    --name "My-Step-Functions-Task" ^
    --description "A description for my Step Functions task"
```

   システムは以下のような情報を返します。

```
{
    "WindowId": "mw-0c50858d01EXAMPLE",
    "WindowTaskId": "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE",
```

```
    "Targets": [
        {
            "Key": "WindowTargetIds",
            "Values": [
                "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE"
            ]
        }
    ],
    "TaskArn": "arn:aws:states:us-
east-2:111122223333:execution:SSMStepFunctionTest",
    "ServiceRoleArn": "arn:aws:iam::111122223333:role/MaintenanceWindowsRole",
    "TaskParameters": {},
    "TaskInvocationParameters": {
        "StepFunctions": {
            "Input": "{\"instanceId\":\"{{RESOURCE_ID}}\"}"
        }
    },
    "Priority": 0,
    "MaxConcurrency": "10",
    "MaxErrors": "5",
    "Name": "My-Step-Functions-Task",
    "Description": "A description for my Step Functions task"
}
```

7. 以下のコマンドを実行して、メンテナンスウィンドウからターゲットを登録解除します。この例では、safe パラメータを使用してターゲットがタスクから参照されているかどうかを判別しているため、安全に登録解除できます。

   Linux & macOS

   ```
   aws ssm deregister-target-from-maintenance-window \
       --window-id "mw-0c50858d01EXAMPLE" \
       --window-target-id "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE" \
       --safe
   ```

   Windows

   ```
   aws ssm deregister-target-from-maintenance-window ^
       --window-id "mw-0c50858d01EXAMPLE" ^
       --window-target-id "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE" ^
       --safe
   ```

システムは以下のような情報を返します。

```
An error occurred (TargetInUseException) when calling the
 DeregisterTargetFromMaintenanceWindow operation:
This Target cannot be deregistered because it is still referenced in Task:
 4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE
```

8. 次のコマンドを実行して、ターゲットがタスクから参照されている場合でもメンテナンスウィンドウからターゲットを登録解除します。no-safe パラメータを使用して、登録解除オペレーションを強制できます。

   Linux & macOS

   ```
   aws ssm deregister-target-from-maintenance-window \
       --window-id "mw-0c50858d01EXAMPLE" \
       --window-target-id "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE" \
       --no-safe
   ```

   Windows

   ```
   aws ssm deregister-target-from-maintenance-window ^
       --window-id "mw-0c50858d01EXAMPLE" ^
       --window-target-id "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE" ^
       --no-safe
   ```

   システムは以下のような情報を返します。

   ```
   {
       "WindowId": "mw-0c50858d01EXAMPLE",
       "WindowTargetId": "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE"
   }
   ```

9. 次のコマンドを実行して Run Command タスクを更新します。この例では、UpdateLevel という名前の Systems Manager Parameter Store パラメータを「{{ssm:UpdateLevel}}」という形式で使用しています。

Linux & macOS

```
aws ssm update-maintenance-window-task \
    --window-id "mw-0c50858d01EXAMPLE" \
    --window-task-id "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE" \
    --targets "Key=InstanceIds,Values=i-02573cafcfEXAMPLE"  \
    --task-invocation-parameters "RunCommand={Comment=A comment for my task
 update,Parameters={UpdateLevel='{{ssm:UpdateLevel}}'}}"
```

Windows

```
aws ssm update-maintenance-window-task ^
    --window-id "mw-0c50858d01EXAMPLE" ^
    --window-task-id "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE" ^
    --targets "Key=InstanceIds,Values=i-02573cafcfEXAMPLE"  ^
    --task-invocation-parameters "RunCommand={Comment=A comment for my task
 update,Parameters={UpdateLevel='{{ssm:UpdateLevel}}'}}"
```

システムは以下のような情報を返します。

```
{
    "WindowId": "mw-0c50858d01EXAMPLE",
    "WindowTaskId": "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE",
    "Targets": [
        {
            "Key": "InstanceIds",
            "Values": [
                "i-02573cafcfEXAMPLE"
            ]
        }
    ],
    "TaskArn": "AWS-RunShellScript",
    "ServiceRoleArn": "arn:aws:iam::111122223333:role/
MyMaintenanceWindowServiceRole",
    "TaskParameters": {},
    "TaskInvocationParameters": {
        "RunCommand": {
            "Comment": "A comment for my task update",
            "Parameters": {
                "UpdateLevel": [
```

```
                    "{{ssm:UpdateLevel}}"
                ]
            }
        }
    },
    "Priority": 10,
    "MaxConcurrency": "1",
    "MaxErrors": "1"
}
```

10. 次のコマンドを実行してオートメーションタスクを更新し、WINDOW_ID パラメータに WINDOW_TASK_ID パラメータと task-invocation-parameters パラメータを指定します。

    Linux & macOS

    ```
    aws ssm update-maintenance-window-task \
        --window-id "mw-0c50858d01EXAMPLE" \
        --window-task-id "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE" \
        --targets "Key=WindowTargetIds,Values=e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE \
        --task-arn "AutoTestDoc" \
        --service-role-arn "arn:aws:iam:account-id:role/
    MyMaintenanceWindowServiceRole \
        --task-invocation-parameters
     "Automation={Parameters={InstanceId='{{RESOURCE_ID}}',initiator='{{WINDOW_ID}}.Task-
    {{WINDOW_TASK_ID}}'}}" \
        --priority 3 --max-concurrency 10 --max-errors 5
    ```

    Windows

    ```
    aws ssm update-maintenance-window-task ^
        --window-id "mw-0c50858d01EXAMPLE" ^
        --window-task-id "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE" ^
        --targets "Key=WindowTargetIds,Values=e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE ^
        --task-arn "AutoTestDoc" ^
        --service-role-arn "arn:aws:iam:account-id:role/
    MyMaintenanceWindowServiceRole ^
        --task-invocation-parameters
     "Automation={Parameters={InstanceId='{{RESOURCE_ID}}',initiator='{{WINDOW_ID}}.Task-
    {{WINDOW_TASK_ID}}'}}" ^
        --priority 3 --max-concurrency 10 --max-errors 5
    ```

システムは以下のような情報を返します。

```
{
    "WindowId": "mw-0c50858d01EXAMPLE",
    "WindowTaskId": "4f7ca192-7e9a-40fe-9192-5cb15EXAMPLE",
    "Targets": [
        {
            "Key": "WindowTargetIds",
            "Values": [
                "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE"
            ]
        }
    ],
    "TaskArn": "AutoTestDoc",
    "ServiceRoleArn": "arn:aws:iam::111122223333:role/
MyMaintenanceWindowServiceRole",
    "TaskParameters": {},
    "TaskInvocationParameters": {
        "Automation": {
            "Parameters": {
                "multi": [
                    "{{WINDOW_TASK_ID}}"
                ],
                "single": [
                    "{{WINDOW_ID}}"
                ]
            }
        }
    },
    "Priority": 0,
    "MaxConcurrency": "10",
    "MaxErrors": "5",
    "Name": "My-Automation-Task",
    "Description": "A description for my Automation task"
}
```

チュートリアル: AWS CLI を使用してメンテナンスウィンドウを削除する

これらのチュートリアルで作成したメンテナンスウィンドウを削除するには、次のコマンドを実行します。

```
aws ssm delete-maintenance-window --window-id "mw-0c50858d01EXAMPLE"
```

システムは以下のような情報を返します。

```
{
   "WindowId":"mw-0c50858d01EXAMPLE"
}
```

チュートリアル: コンソールを使用してパッチ用メンテナンスウィンドウを作成する

> **Important**
>
> このレガシートピックを引き続き使用してパッチ適用のためのメンテナンスウィンドウを作成することができます。ただし、代わりにパッチポリシーを使用することをお勧めします。詳細については、Quick Setup でのパッチポリシー設定 およびQuick Setup パッチポリシーを使用して組織内のインスタンスのためにパッチ適用を設定する を参照してください。

サーバーの可用性に対する影響を最小限に抑えるため、メンテナンスウィンドウを設定して事業運営を中断させない時間帯にパッチ適用を実行することをお勧めします。

この手順を開始する前に、AWS Systems Manager のツールである Maintenance Windows のロールおよびアクセス許可を設定する必要があります。詳細については、「Maintenance Windows を設定する」を参照してください。

パッチ適用のメンテナンスウィンドウを作成するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Maintenance Windows] を選択します。
3. [Create maintenance window] を選択します。
4. [Name] に、緊急および重要な更新プログラムのパッチを適用するメンテナンスウィンドウとして、これを指定する名前を入力します。
5. (オプション) [説明] に説明を入力します。
6. ノードをがターゲットとして登録されていない場合でも、そのマネージドノードでメンテナンスウィンドウタスクの実行を許可する場合は、[Allow unregistered targets] (未登録ターゲットを許可) を選択します。

このオプションを選択すると、タスクをメンテナンスウィンドウに登録する際に、未登録ノードを (ノード ID で) 選択できます。

このオプションを選択しない場合、タスクをメンテナンスウィンドウに登録する際に、事前に登録済みのターゲットを選択する必要があります。

7. [スケジュール] セクションの上部で、3 つのスケジュールオプションのいずれかを使用して、メンテナンスウィンドウのスケジュールを指定します。

   cron/rate 式の作成の詳細については、「リファレンス: Systems Manager の Cron 式および rate 式」を参照してください。

8. [期間] に、メンテナンスウィンドウを実行する時間数を入力します。指定する値は、開始時刻に基づいてメンテナンスウィンドウの具体的な終了時刻を決定します。メンテナンスウィンドウタスクは、決定された終了時刻から、次のステップで [タスクの開始を停止] に指定する時間数を引いて求められる時刻の後に開始することは許可されません。

   たとえば、メンテナンスウィンドウが午後 3 時に開始され、期間が 3 時間で、[タスクの開始を停止] の値が 1 時間の場合、午後 5 時以降はメンテナンスウィンドウのタスクを開始できません。

9. [Stop initiating tasks] に、メンテナンスウィンドウが終了してから新しいタスクの実行のスケジュールが停止されるまでの時間数を入力します。

10. (オプション) [Window start date] (ウィンドウ開始日) で、メンテナンスウィンドウをアクティブにする日時を ISO-8601 拡張形式で指定します。これにより、指定した将来の日付までメンテナンスウィンドウのアクティベーションを遅らせることができます。

11. (オプション) [Window end date] (ウィンドウ終了日) で、メンテナンスウィンドウを非アクティブにする日時を ISO-8601 拡張形式で指定します。これにより、メンテナンスウィンドウの実行を停止する将来の日時を設定できるようになります。

12. (オプション) [タイムゾーンのスケジュール] で、スケジュールされたメンテナンスウィンドウの実行の基準となるタイムゾーンを、IANA (Internet Assigned Numbers Authority) 形式で指定できます。例: 「America/Los_Angeles」、「etc/UTC」、または「Asia/Seoul」。

    有効な形式の詳細については、IANA ウェブサイトの「Time Zone Database」を参照してください。

13. (オプション) [タグの管理] 領域で、1 つ以上のタグキーの名前と値のペアをメンテナンスウィンドウに適用します。

タグは、リソースに割り当てるオプションのメタデータです。タグを使用すると、目的、所有者、環境などのさまざまな方法でリソースを分類できます。例えば、このメンテナンスウィンドウにタグを付けて、実行するタスクのタイプを指定できます。この場合、以下のキーの名前と値のペアを指定します。

- `Key=TaskType,Value=Patching`

14. [Create maintenance window] を選択します。
15. メンテナンスウィンドウのリストで、作成したメンテナンスウィンドウを選択し、[Actions]、[Register targets] の順に選択します。
16. (オプション) [Maintenance window target details] セクションで、このターゲットの名前、説明、所有者情報 (自分の名前またはエイリアス) を指定します。
17. [ターゲットの選択] で、[インスタンスタグの指定] を選択します。
18. [インスタンスタグの指定] で、メンテナンスウィンドウに登録するノードを識別するためのタグキーとタグ値を入力し、[追加] を選択します。
19. [Register target] を選択します。メンテナンスウィンドウのターゲットが作成されます。
20. 作成したメンテナンスウィンドウの詳細ページで、[アクション]、[run command タスクの登録] の順に選択します。
21. (オプション) [Maintenance window task details (メンテナンスウィンドウのタスクの詳細)] に、このタスクの名前と説明を入力します。
22. [Command document] (コマンドのドキュメント) で、`AWS-RunPatchBaseline` を選択します。
23. [Task priority (タスクの優先度)] で、優先度を選択します。ゼロ (`0`) が最高の優先度になります。
24. [Targets (ターゲット)] の [Target by (ターゲットの条件)] で、この手順の前半で作成したメンテナンスウィンドウターゲットを選択します。
25. [レート制御] の場合:

    - [同時実行数] の場合、コマンドを同時に実行するマネージドノードの数または割合を指定します。

> **Note**
>
> マネージドノードに適用されるタグを指定するか、AWS リソースグループを指定してターゲットを選択し、ターゲットとなるマネージドノードの数が不明な場合は、割合を指定してドキュメントを同時に実行できるターゲットの数を制限します。

- [エラーのしきい値] で、ノードの数または割合のいずれかで失敗した後、他のマネージドノードでのコマンドの実行をいつ停止するか指定します。例えば、3 つのエラーを指定した場合、4 番目のエラーが受信されると、システムマネージャー はコマンドの送信を停止します。コマンドを処理しているマネージドノードもエラーを送信する可能性があります。

26. (オプション) [IAM サービスロール] で、Systems Manager がメンテナンスウィンドウタスクの実行時期を推測するための許可を付与するロールを選択します。

    サービスロール ARN を指定しない場合、Systems Manager はアカウントのサービスにリンクされたロールを使用します。アカウントに Systems Manager 用の適切なサービスにリンクされたロールが存在しない場合は、タスクが正常に登録されるとロールが作成されます。

    > **Note**
    >
    > セキュリティ体制を強化するために、メンテナンスウィンドウタスクを実行するためのカスタムポリシーとカスタムサービスロールを作成することを強くお勧めします。ポリシーは、特定のメンテナンスウィンドウタスクに必要なアクセス許可のみを提供するように作成できます。詳細については、「Maintenance Windows を設定する」を参照してください。

27. (オプション) [出力オプション] で、コマンド出力をファイルに保存するには、[S3 への出力の書き込みを有効にします] ボックスをオンにします。ボックスにバケット名とプレフィックス (フォルダ) 名を入力してください。

    > **Note**
    >
    > S3 バケットにデータを書き込む機能を許可する S3 アクセス許可は、このタスクを実行する IAM ユーザーのものではなく、マネージドノードに割り当てられたインスタンスプロファイルのものです。詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」または「ハイブリッド環境に IAM サービスロールを作成する」を参照してください。さらに、指定された S3 バケットが別の AWS アカウント にある場合は、マネージドノードに関連付けられたインスタンスプロファイルまたは IAM

サービスロールに、そのバケットへの書き込みに必要なアクセス許可があることを確認してください。

Amazon CloudWatch Logs ロググループに出力をストリーミングするには、[CloudWatch 出力] ボックスを選択します。ボックスにロググループ名を入力します。

28. [SNS Notifications (SNS 通知)] セクションで、コマンドの実行状態に関する通知を受け取る場合は、[Enable SNS notifications (SNS 通知を有効にする)] チェックボックスをオンにします。

    Run Command 用の Amazon SNS 通知の設定の詳細については、「Amazon SNS 通知を使用した Systems Manager のステータス変更のモニタリング」を参照してください。

29. [Parameters (パラメータ)]。

    - [Operation (オペレーション)] リストで、[Scan (スキャン)] を選択して見つからないパッチをスキャンするか、[Install (インストール)] を選択して見つからないパッチをスキャンしてインストールします。
    - [Snapshot Id (スナップショット ID)] フィールドには何も指定する必要がありません。このシステムでは、このパラメータが自動的に生成されて提供されます。
    - パッチベースラインに指定されているものとは異なるパッチのセットをPatch Managerで使用する場合を除き、[Install Override List (インストール上書きリスト)] フィールドには何も入力する必要はありません。詳細については、パラメータ名: `InstallOverrideList` を参照してください。
    - [再起動オプション] で、`Install` オペレーション中にパッチがインストールされた場合にノードを再起動するか、Patch Manager が前回のノードの再起動後にインストールされた他のパッチを検出した場合にノードを再起動するかを指定します。詳細については、パラメータ名: `RebootOption` を参照してください。
    - (オプション) [Comment (コメント)] に、このコマンドに関する追跡メモまたはリマインダーを入力します。
    - [Timeout (seconds) (タイムアウト (秒))] に、オペレーションが完了せずに失敗したとみなされるまでにシステムが待機する秒数を入力します。

30. [Register Run command task (Run command タスクの登録)] を選択します。

メンテナンスウィンドウタスクが完了したら、Fleet Manager ツールの Systems Manager コンソールで、パッチコンプライアンスの詳細を確認できます。

あるいは Patch Manager ツールの [コンプライアンスレポート] タブでコンプライアンス情報を確認することもできます。

DescribePatchGroupState と DescribeInstancePatchStatesForPatchGroup の API を使用してコンプライアンスの詳細を確認することもできます。パッチコンプライアンスデータの詳細については、「パッチコンプライアンスについて」を参照してください。

メンテナンスウィンドウを使用してスケジュールにパッチを適用する

パッチベースライン (およびオプションのパッチグループ) を設定したら、メンテナンスウィンドウを使用してパッチをノードに適用できます。メンテナンスウィンドウは、パッチ適用プロセスを実行する時間を、事業運営を中断させない時間に指定することで、サーバーの可用性に対する影響を軽減させることができます。メンテナンスウィンドウの動作は次のようになります。

1. メンテナンスウィンドウを作成してパッチ適用オペレーションをスケジュールします。
2. `Patch Group` または `PatchGroup` タグ、Amazon Elastic Compute Cloud (Amazon EC2) タグを定義した値 (「Web サーバー」、「US-EAST-PROD」など) を指定して、メンテナンスウィンドウのターゲットを選択します。(EC2 インスタンスのメタデータでタグを許可している場合は、スペースなしで `PatchGroup` を使用する必要があります。)
3. 新しいメンテナンスウィンドウタスクを作成し、`AWS-RunPatchBaseline`ドキュメントを指定します。

タスクを設定するときに、ノードをスキャンするか、ノードをスキャンしてパッチをインストールするかを選択できます。ノードのスキャンを選択すると、AWS Systems Manager のツールである Patch Manager は各ノードをスキャンし、見つからないパッチのリストを生成して確認できるようにします。

パッチのスキャンとインストールを選択すると、Patch Manager は各ノードをスキャンし、インストールされているパッチのリストとベースラインの承認済みパッチのリストを照合します。Patch Manager は不足しているパッチを特定し、不足しているすべての承認済みパッチをダウンロードしてインストールします。

問題を解決するためにスキャンやインストールを 1 回のみ実行する場合は、Run Command を使用して `AWS-RunPatchBaseline` ドキュメントを直接呼び出すことができます。

> **Important**
>
> パッチをインストールすると、Systems Manager によって各ノードが再起動されます。再起動は、パッチが正しくインストールされていることを確認し、ノードを適切な状態に更

新するために必要です。(例外: RebootOption パラメータが AWS-RunPatchBaseline ドキュメントの NoReboot で設定されている場合、パッチマネージャーの Patch Manager 実行後にマネージドノードは再起動されません。詳細については、「パラメータ名: RebootOption」を参照してください。)

メンテナンスウィンドウのタスクを登録する際の疑似パラメータの使用

AWS Systems Manager のツールである Maintenance Windows でタスクを登録する際、4 つのタスクタイプのそれぞれに固有のパラメータを指定します。(CLI コマンドでは、これらは --task-invocation-parameters オプションを使用して指定されます)。

{{RESOURCE_ID}}、{{TARGET_TYPE}}、{{WINDOW_TARGET_ID}} などの擬似パラメータ構文を使用して、特定の値を参照することもできます。メンテナンスウィンドウタスクが実行されると、擬似パラメータプレースホルダーの代わりに正しい値を渡します。使用できる擬似パラメータすべてのリストについては、このトピックの後半の「サポートされる擬似パラメータ」を参照してください。

Important

RESOURCE_GROUP ターゲットタイプでは、タスクに必要な ID 形式に応じて、タスクの実行時にリソースを参照するために {{TARGET_ID}} と {{RESOURCE_ID}} を使用するかを選択できます。{{TARGET_ID}} は、リソースの完全な ARN を返します。{{RESOURCE_ID}} は、これらの例に示すように、リソースの短い名前または ID のみを返します。

- {{TARGET_ID}} 形式: arn:aws:ec2:us-east-1:123456789012:instance/i-02573cafcfEXAMPLE
- {{RESOURCE_ID}} 形式: i-02573cafcfEXAMPLE

INSTANCE ターゲットタイプの場合、{{TARGET_ID}} パラメータと {{RESOURCE_ID}} パラメータの両方がインスタンス ID のみを生成します。詳細については、「」を参照してくださいサポートされる擬似パラメータ
{{TARGET_ID}} および {{RESOURCE_ID}} を使用して、AWS リソースの ID を Automation、Lambda、Step Functions のタスクにのみ渡すことができます。これら 2 つの擬似パラメータは、Run Command タスクでは使用できません。

擬似パラメータの例

AWS Lambda タスクのペイロードが、ID でインスタンスを参照する必要があるとします。

INSTANCE または RESOURCE_GROUP メンテナンスウィンドウターゲットを使用しているかどうかに関係なく、これは {{RESOURCE_ID}} 擬似パラメータを使用することで実現できます。例:

```
"TaskArn": "arn:aws:lambda:us-east-2:111122223333:function:SSMTestFunction",
    "TaskType": "LAMBDA",
    "TaskInvocationParameters": {
        "Lambda": {
            "ClientContext": "ew0KICAi--truncated--0KIEXAMPLE",
            "Payload": "{ \"instanceId\": \"{{RESOURCE_ID}}\" }",
            "Qualifier": "$LATEST"
        }
    }
```

Lambda タスクが、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスに加えて、サポートされている別のターゲットタイプ (Amazon DynamoDB テーブルなど) に対して実行することを意図している場合は、同じ構文を使用でき、{{RESOURCE_ID}} はテーブルの名前のみを生成します。ただし、テーブルの完全な ARN が必要な場合は、次の例に示すように {{TARGET_ID}} を使用します。

```
"TaskArn": "arn:aws:lambda:us-east-2:111122223333:function:SSMTestFunction",
    "TaskType": "LAMBDA",
    "TaskInvocationParameters": {
        "Lambda": {
            "ClientContext": "ew0KICAi--truncated--0KIEXAMPLE",
            "Payload": "{ \"tableArn\": \"{{TARGET_ID}}\" }",
            "Qualifier": "$LATEST"
        }
    }
```

ターゲットインスタンスやその他のリソースタイプに対しても、同じ構文を使用できます。複数のリソースタイプがリソースグループに追加されている場合、タスクは適切な各リソースに対して実行されます。

> **Important**
>
> リソースグループに含まれるすべてのリソースタイプが {{RESOURCE_ID}} パラメータの値を生成するわけではありません。サポートされているリソースタイプの一覧については、「サポートされる擬似パラメータ」を参照してください。

別の例として、EC2 インスタンスを停止する Automation タスクを実行するには、AWS-StopEC2Instance Systems Manager ドキュメント (SSM ドキュメント) を TaskArn 値として指定し、{{RESOURCE_ID}} 擬似パラメータを使用します。

```
"TaskArn": "AWS-StopEC2Instance",
    "TaskType": "AUTOMATION"
    "TaskInvocationParameters": {
        "Automation": {
            "DocumentVersion": "1",
            "Parameters": {
                "instanceId": [
                    "{{RESOURCE_ID}}"
                ]
            }
        }
    }
```

Amazon Elastic Block Store (Amazon EBS) ボリュームのスナップショットをコピーする Automation タスクを実行するには、AWS-CopySnapshot SSM ドキュメントを TaskArn 値として指定し、{{RESOURCE_ID}} 擬似パラメータを使用します。

```
"TaskArn": "AWS-CopySnapshot",
    "TaskType": "AUTOMATION"
    "TaskInvocationParameters": {
        "Automation": {
            "DocumentVersion": "1",
            "Parameters": {
                "SourceRegion": "us-east-2",
                "targetType":"RESOURCE_GROUP",
                "SnapshotId": [
                    "{{RESOURCE_ID}}"
                ]
            }
        }
```

```
    }
```

サポートされる擬似パラメータ

以下のリストでは、{{*PSEUDO_PARAMETER*}} オプションの `--task-invocation-parameters` 構文を使用して指定できる疑似パラメータについて説明しています。

- **WINDOW_ID**: ターゲットメンテナンスウィンドウの ID。
- **WINDOW_TASK_ID**: 実行されているウィンドウタスクの ID。
- **WINDOW_TARGET_ID**: ターゲット (ターゲット ID) を含むウィンドウターゲットの ID。
- **WINDOW_EXECUTION_ID**: 現在のウィンドウ実行の ID。
- **TASK_EXECUTION_ID**: 現在のタスク実行の ID。
- **INVOCATION_ID**: 現在の呼び出しの ID。
- **TARGET_TYPE**: ターゲットのタイプ。サポートされるタイプには `RESOURCE_GROUP`、`INSTANCE` などがあります。
- **TARGET_ID**:

  指定したターゲットタイプが `INSTANCE` の場合、TARGET_ID擬似パラメータはインスタンスの ID に置き換えられます。例えば、`i-078a280217EXAMPLE` と指定します。

  指定したターゲットタイプが `RESOURCE_GROUP` の場合、タスク実行で参照される値は、リソースの完全な ARN になります。例: `arn:aws:ec2:us-east-1:123456789012:instance/i-078a280217EXAMPLE`。次の表に、リソースグループ内の特定のリソースタイプの `TARGET_ID` 値の例を示します。

> **Note**
>
> `TARGET_ID` は Run Command タスクではサポートされていません。

リソースタイプ	TARGET_ID の例
`AWS::CloudWatch::Alarm`	`arn:aws:cloudwatch:us-east-1:123456789012:alarm:MyClou`

リソースタイプ	TARGET_ID の例	
	dWatchAlarm i-078a280217EXAMPLE	
AWS::DynamoDB::Table	arn:aws:dynamodb:us-east-1:123456789012:table/MyTable	
AWS::EC2::Instance	arn:aws:ec2:us-east-1:123456789012:instance/ i-078a280217EXAMPLE	
AWS::EC2::Image	arn:aws:ec2:us-east-1:123456789012:image/ami-02250b3732EXAMPLE	
AWS::EC2::SecurityGroup	arn:aws:ec2:us-east-1:123456789012:security-group/sg-cEXAMPLE	
AWS::EC2::Snapshot	arn:aws:ec2:us-east-1:123456789012:snapshot/snap-03866bf003EXAMPLE	
AWS::EC2::Volume	arn:aws:ec2:us-east-1:123456789012:volume/vol-0912e04d78EXAMPLE	
AWS::ECS::Service	arn:aws:ecs:us-east-1:123456789012:service/my-ecs-service	

リソースタイプ	TARGET_ID の例
AWS::RDS::DBCluster	arn:aws:rds:us-east-2:123456789012:cluster:My-Cluster
AWS::RDS::DBInstance	arn:aws:rds:us-east-1:123456789012:db:My-SQL-Instance
AWS::S3::Bucket	arn:aws:s3:::amzn-s3-demo-bucket
AWS::SSM::ManagedInstance	arn:aws:ssm:us-east-1:123456789012:managed-instance/mi-0feadcf2d9EXAMPLE

- **RESOURCE_ID**: リソースグループに含まれるリソースタイプの短い ID。次の表に、リソースグループ内の特定のリソースタイプの RESOURCE_ID 値の例を示します。

> **Note**
>
> RESOURCE_ID は Run Command タスクではサポートされていません。

リソースタイプ	RESOURCE_ID の例
AWS::CloudWatch::Alarm	MyCloudWatchAlarm
AWS::DynamoDB::Table	MyTable
AWS::EC2::Instance	i-078a280217EXAMPLE
AWS::EC2::Image	ami-02250b3732EXAMPLE

リソースタイプ	RESOURCE_ID の例	
AWS::EC2::Security Group	sg-cEXAMPLE	
AWS::EC2::Snapshot	snap-03866bf003EXAMPLE	
AWS::EC2::Volume	vol-0912e04d78EXAMPLE	
AWS::ECS::Service	my-ecs-service	
AWS::RDS::DBCluster	My-Cluster	
AWS::RDS::DBInstance	My-SQL-Instance	
AWS::S3::Bucket	amzn-s3-demo-bucket	
AWS::SSM::ManagedInstance	mi-0feadcf2d9EXAMPLE	

> **Note**
>
> 指定した AWS リソースグループに、RESOURCE_ID 値を生成しないリソースタイプが含まれており、前述の表にリストされていない場合、RESOURCE_ID パラメータは入力されません。そのリソースに対して実行の呼び出しは引き続き発生します。このような場合は、代わりに TARGET_ID 擬似パラメータを使用します。このパラメータは、リソースの完全な ARN に置き換えられます。

メンテナンスウィンドウのスケジューリングおよび有効期間のオプション

メンテナンスウィンドウを作成するときは、メンテナンスウィンドウの実行頻度を Cron または Rate 式で指定する必要があります。必要に応じて、メンテナンスウィンドウを定期的なスケジュールで実行できる期間の日付範囲と、その定期的なスケジュールのベースとなるタイムゾーンを指定することができます。

ただし、タイムゾーンオプションおよび開始日と終了日のオプションは互いに影響しない点に注意してください。指定した開始日と終了日時 (タイムゾーンのオフセットの有無にかかわらず) は、メンテナンスウィンドウがそのスケジュールで実行できる有効期間のみを決定します。タイムゾーンオプションは、有効な期間中にメンテナンスウィンドウのスケジュールがベースとする国際タイムゾーンを決定します。

> **Note**
>
> ISO-8601 タイムスタンプ形式で開始日と終了日を指定します。例: `2021-04-07T14:29:00-08:00`
> タイムゾーンを IANA (Internet Assigned Numbers Authority) 形式で指定します。例: `America/Chicago`、`Europe/Berlin`、または `Asia/Tokyo`

例

- 例 1: メンテナンスウィンドウの開始日を指定する
- 例 2: メンテナンスウィンドウの開始日と終了日を指定する
- 例 3: 一度のみ実行するメンテナンスウィンドウを作成する
- 例 4: メンテナンスウィンドウのスケジュールオフセット日数を指定する

例 1: メンテナンスウィンドウの開始日を指定する

AWS Command Line Interface (AWS CLI) を使用し、次のオプションを指定してメンテナンスウィンドウを作成するとします。

- `--start-date 2021-01-01T00:00:00-08:00`
- `--schedule-timezone "America/Los_Angeles"`
- `--schedule "cron(0 09 ? * WED *)"`

以下に例を示します。

Linux & macOS

```
aws ssm create-maintenance-window \
    --name "My-LAX-Maintenance-Window" \
    --allow-unassociated-targets \
    --duration 3 \
```

```
    --cutoff 1 \
    --start-date 2021-01-01T00:00:00-08:00 \
    --schedule-timezone "America/Los_Angeles" \
    --schedule "cron(0 09 ? * WED *)"
```

Windows

```
aws ssm create-maintenance-window ^
    --name "My-LAX-Maintenance-Window" ^
    --allow-unassociated-targets ^
    --duration 3 ^
    --cutoff 1 ^
    --start-date 2021-01-01T00:00:00-08:00 ^
    --schedule-timezone "America/Los_Angeles" ^
    --schedule "cron(0 09 ? * WED *)"
```

これは、2021 年 1 月 1 日金曜日、米国東部標準時の午前 0 時に指定された開始日時以降は、メンテナンスウィンドウの初回実行ができなくなることを意味しています。(このタイムゾーンは UTC 時間より 8 時間遅れています。) この場合、ウィンドウ期間の開始日時が、メンテナンスウィンドウが最初に実行される時期を表すものではありません。総合すると、`--schedule-timezone` と `--schedule` の値は、メンテナンスウィンドウが米国太平洋標準時 (IANA 形式では「America/Los Angeles」で表される) で毎週水曜日の午前 9 時に実行されることを意味しています。有効な期間中の最初の実行は、2021 年 1 月 4 日水曜日、太平洋標準時の午前 9 時となります。

例 2: メンテナンスウィンドウの開始日と終了日を指定する

次に、これらのオプションを使用してメンテナンスウィンドウを作成するとします。

- `--start-date 2019-01-01T00:03:15+09:00`
- `--end-date 2019-06-30T00:06:15+09:00`
- `--schedule-timezone "Asia/Tokyo"`
- `--schedule "rate(7 days)"`

以下に例を示します。

Linux & macOS

```
aws ssm create-maintenance-window \
    --name "My-NRT-Maintenance-Window" \
```

```
    --allow-unassociated-targets \
    --duration 3 \
    --cutoff 1 \
    --start-date 2019-01-01T00:03:15+09:00 \
    --end-date 2019-06-30T00:06:15+09:00 \
    --schedule-timezone "Asia/Tokyo" \
    --schedule "rate(7 days)"
```

Windows

```
aws ssm create-maintenance-window ^
    --name "My-NRT-Maintenance-Window" ^
    --allow-unassociated-targets ^
    --duration 3 ^
    --cutoff 1 ^
    --start-date 2019-01-01T00:03:15+09:00 ^
    --end-date 2019-06-30T00:06:15+09:00 ^
    --schedule-timezone "Asia/Tokyo" ^
    --schedule "rate(7 days)"
```

このメンテナンスウィンドウの有効期間は、2019 年 1 月 1 日の日本標準時午前 3 時 15 分に始まります。このメンテナンスウィンドウの有効期間は、2019 年 6 月 30 日日曜日の日本標準時午前 6 時 15 分に終了します。(このタイムゾーンは UTC 時間より 9 時間進んでいます。) 総合すると、`--schedule-timezone` と `--schedule` の値は、メンテナンスウィンドウが日本標準時 (IANA 形式では「Asia/Tokyo」で表される) で毎週火曜日の午前 3 時 15 分に実行されることを意味しています。これは、メンテナンスウィンドウが 7 日ごとに実行され、1 月 1 日火曜日の午前 3 時 15 分にアクティブになるためです。最後の実行は、2019 年 6 月 25 日火曜日の日本標準時午前 3 時 15 分です。これは、有効なメンテナンスウィンドウ期間が終了する 5 日前の、最後の火曜日です。

例 3: 一度のみ実行するメンテナンスウィンドウを作成する

このオプションでメンテナンスウィンドウを作成できるようになりました。

- `--schedule "at(2020-07-07T15:55:00)"`

以下に例を示します。

Linux & macOS

```
aws ssm create-maintenance-window \
```

```
    --name "My-One-Time-Maintenance-Window" \
    --schedule "at(2020-07-07T15:55:00)" \
    --duration 5 \
    --cutoff 2 \
    --allow-unassociated-targets
```

Windows

```
aws ssm create-maintenance-window ^
    --name "My-One-Time-Maintenance-Window" ^
    --schedule "at(2020-07-07T15:55:00)" ^
    --duration 5 ^
    --cutoff 2 ^
    --allow-unassociated-targets
```

このメンテナンスウィンドウは、2020 年 7 月 7 日午後 3 時 55 分 (UTC 時間) に実行されます。メンテナンスウィンドウは、必要に応じて最大 5 時間実行できますが、メンテナンスウィンドウ期間の終了 2 時間前に新しいタスクを開始することはできません。

例 4: メンテナンスウィンドウのスケジュールオフセット日数を指定する

このオプションでメンテナンスウィンドウを作成できるようになりました。

```
--schedule-offset 2
```

以下に例を示します。

Linux & macOS

```
aws ssm create-maintenance-window \
    --name "My-Cron-Offset-Maintenance-Window" \
    --schedule "cron(0 30 23 ? * TUE#3 *)" \
    --duration 4 \
    --cutoff 1 \
    --schedule-offset 2 \
    --allow-unassociated-targets
```

Windows

```
aws ssm create-maintenance-window ^
```

```
    --name "My-Cron-Offset-Maintenance-Window" ^
    --schedule "cron(0 30 23 ? * TUE#3 *)" ^
    --duration 4 ^
    --cutoff 1 ^
    --schedule-offset 2 ^
    --allow-unassociated-targets
```

スケジュールオフセットは、CRON 式で指定された日時からメンテナンスウィンドウを実行するまでに待機する日数です。

前述の例では、CRON 式により、毎月第 3 火曜日の午後 11:30 にメンテナンスウィンドウがスケジュールされます。

```
--schedule "cron(0 30 23 ? * TUE#3 *)
```

ただし、`--schedule-offset 2` を含めると、メンテナンスウィンドウは、毎月第 3 火曜日の 2 日後の午後 11:30 PM まで実行されません。

スケジュールオフセットは、CRON 式でのみサポートされます。

詳細情報

- リファレンス: Systems Manager の Cron 式および rate 式
- コンソールを使用してメンテナンスウィンドウを作成する
- チュートリアル: AWS CLI を使用してメンテナンスウィンドウを作成および設定する
- AWS Systems Manager API リファレンスの「CreateMaintenanceWindow」
- 「AWS CLI コマンドリファレンスの AWS Systems Manager セクション」内、「create-maintenance-window」
- IANA ウェブサイトの Time Zone Database

ターゲットのないメンテナンスウィンドウタスクを登録

作成するメンテナンスウィンドウごとに、メンテナンスウィンドウの実行時に実行するタスクを 1 つ以上指定できます。ほとんどの場合、タスクを実行するリソース、またはターゲットを指定する必要があります。ただし、タスクでターゲットを明示的に指定する必要がない場合もあります。

メンテナンスウィンドウの Systems Manager Run Command タイプのタスクには、1 つ以上のターゲットを指定する必要があります。タスクの特質に応じて、他のメンテナンスウィンドウタスクタイ

プ (Systems Manager Automation、AWS Lambda、AWS Step Functions) ではターゲットはオプションです。

Lambda および Step Functions タスクタイプの場合、ターゲットが必要かどうかは、作成した関数またはステートマシンの内容によって異なります。

> **Note**
>
> タスクがターゲットを登録すると、オートメーション、AWS Lambda、および AWS Step Functions タスクはリソースグループとタグからターゲットを解決し、解決されたリソースごとに 1 つの呼び出しを送信し、その結果、複数のタスク呼び出しが発生します。例えば、複数のインスタンスを含むリソースグループに登録されている Lambda タスクの呼び出しを 1 つだけ行う必要があるとしましょう。この場合、AWS Management Consoleで作業している場合は、[Register Lambda タスク] ページまたは [Lambda タスクの編集] ページで、[タスクターゲットが不要] なオプションを選択します。AWS CLI コマンドを使用している場合は、register-task-with-maintenance-window コマンドまたは update-maintenance-window-task コマンドの実行時に `--targets` パラメータを使用してターゲットを指定しないでください。

多くの場合、オートメーションタスクのターゲットを明示的に指定する必要はありません。例えば、`AWS-UpdateLinuxAmi` ランブックを使用して Linux 用の Amazon Machine Image (AMI) を更新するためのオートメーションタイプのタスクを作成するとします。このタスクが実行されると、AMI は最新の利用可能な Linux ディストリビューションパッケージと Amazon ソフトウェアを反映して更新されます。AMI から作成した新しいインスタンスには、これらの更新がインストール済みです。更新する AMI の ID はランブックの入力パラメータで指定されるため、メンテナンスウィンドウタスクでターゲットを再度指定する必要はありません。

同様に、AWS Command Line Interface (AWS CLI) を使用して、`AWS-RestartEC2Instance` ランブックを使用するメンテナンスウィンドウのオートメーションタスクを登録するとします。再起動するノードは `--task-invocation-parameters` 引数で指定されるため、`--targets` オプションも指定する必要はありません。

> **Note**
>
> ターゲットが指定されていないメンテナンスウィンドウタスクの場合、`--max-errors` と `--max-concurrency` の値は指定できません。代わりに、システムはプレースホルダ値として 1 を挿入します。これは describe-maintenance-window-tasks や get-maintenance-

window-task などのコマンドへのレスポンスで報告されることがあります。これらの値は、タスクの実行には影響しないため、無視できます。

次の例は、ターゲットなしのメンテナンスウィンドウタスクの `--targets`、`--max-errors`、`--max-concurrency` オプションを省略する方法を示しています。

Linux & macOS

```
aws ssm register-task-with-maintenance-window \
    --window-id "mw-ab12cd34eEXAMPLE" \
    --service-role-arn "arn:aws:iam::123456789012:role/
MaintenanceWindowAndAutomationRole" \
    --task-type "AUTOMATION" \
    --name "RestartInstanceWithoutTarget" \
    --task-arn "AWS-RestartEC2Instance" \
    --task-invocation-parameters "{\"Automation\":{\"Parameters\":{\"InstanceId\":
[\"i-02573cafcfEXAMPLE\"]}}}" \
    --priority 10
```

Windows

```
aws ssm register-task-with-maintenance-window ^
    --window-id "mw-ab12cd34eEXAMPLE" ^
    --service-role-arn "arn:aws:iam::123456789012:role/
MaintenanceWindowAndAutomationRole" ^
    --task-type "AUTOMATION" ^
    --name "RestartInstanceWithoutTarget" ^
    --task-arn "AWS-RestartEC2Instance" ^
    --task-invocation-parameters "{\"Automation\":{\"Parameters\":{\"InstanceId\":
[\"i-02573cafcfEXAMPLE\"]}}}" ^
    --priority 10
```

Note

2020 年 12 月 23 日より前に登録されたメンテナンスウィンドウタスクの場合: タスクのターゲットを指定し、そのターゲットが不要になった場合、Systems Manager コンソールまたは update-maintenance-window-task AWS CLI コマンドを使用して、そのタスクを更新してターゲットを削除できます。

詳細情報

- エラーメッセージ:「Maintenance window tasks without targets don't support MaxConcurrency values」および「Maintenance window tasks without targets don't support MaxErrors values」

メンテナンスウィンドウのトラブルシューティング

以下の情報を参考にして、メンテナンスウィンドウに関する問題のトラブルシューティングを行います。

トピック

- タスクの編集エラー: メンテナンスウィンドウのタスクを編集するためのページで、IAM ロールリストから次のエラーメッセージが返されます。「このタスクに指定されている IAM メンテナンスウィンドウのロールが見つかりませんでした。このロールは削除された可能性があるか、まだ作成されていない可能性があることを示すエラーメッセージを返す
- すべてのメンテナンスウィンドウのターゲットが更新されるわけではありません。
- タスクがタスク呼び出しステータスで失敗する:「The provided role does not contain the correct SSM permissions.」(指定されたロールには正しい SSM 許可が含まれていません。)
- タスクはエラーメッセージで失敗します:「Step fails when it is validating and resolving the step inputs」
- エラーメッセージ:「Maintenance window tasks without targets don't support MaxConcurrency values」および「Maintenance window tasks without targets don't support MaxErrors values」

タスクの編集エラー: メンテナンスウィンドウのタスクを編集するためのページで、IAM ロールリストから次のエラーメッセージが返されます。「このタスクに指定されている IAM メンテナンスウィンドウのロールが見つかりませんでした。このロールは削除された可能性があるか、まだ作成されていない可能性があることを示すエラーメッセージを返す

問題 1: タスクを作成したら、元々指定していたAWS Identity and Access Management（ IAM) メンテナンスウィンドウロールが削除された。

解決方法: 1) 別の IAM メンテナンスウィンドウロールを選択する。(アカウントに存在する場合)、新しいロールを作成してそのタスク用に選択します。

問題 2: AWS Command Line Interface (AWS CLI)、AWS Tools for Windows PowerShell、または AWS SDK を使用してタスクが作成された場合は、存在しない IAM メンテナンスウィンドウロールの名前が指定された可能性があります。例えば、タスクを作成する前に IAM メンテナンスウィ

ンドウロールが削除された、またはロール名が正しく入力されなかった可能性があります (例えば、**myrole** ではなく **my-role** と入力した)。

解決方法: 使用する IAM メンテナンスウィンドウロールの正しい名前を選択するか、新しいロールを作成してそのタスク用に指定します。

すべてのメンテナンスウィンドウのターゲットが更新されるわけではありません。

問題: メンテナンスウィンドウのタスクが、メンテナンスウィンドウの対象となるすべてのリソースで実行されなかったことに気付きました。たとえば、メンテナンスウィンドウの実行結果で、そのリソースのタスクが失敗またはタイムアウトとしてマークされます。

解決方法: メンテナンスウィンドウタスクがターゲットリソースで実行されない最も一般的な理由は、接続性と可用性です。以下に例を示します。

- Systems Manager メンテナンスウィンドウの操作前または操作中にリソースへの接続が失われました。
- リソースがオフラインだったか、メンテナンスウィンドウの操作中に停止しました。

リソースでタスクを実行するために、次のスケジュールされたメンテナンスウィンドウ時間を待つことができます。使用できないリソースまたはオフラインだったリソースに対して、メンテナンスウィンドウタスクを手動で実行できます。

タスクがタスク呼び出しステータスで失敗する:「The provided role does not contain the correct SSM permissions.」(指定されたロールには正しい SSM 許可が含まれていません。)

問題: タスクにメンテナンスウィンドウサービスロールを指定しましたが、タスクが正常に実行されず、タスク呼び出しステータスが「"The provided role does not contain the correct SSM permissions.」(指定されたロールには正しい SSM 許可が含まれていません) とレポートします。

- 解決策: タスク 1: コンソールを使用して、メンテナンスウィンドウサービスロール用にカスタムポリシーを作成する では、カスタムメンテナンスウィンドウのサービスロールにアタッチできる基本ポリシーを提供しています。ポリシーには、多くのタスクシナリオに必要な許可が含まれています。ただし、実行できるタスクは多種多様であるため、メンテナンスウィンドウロールのポリシーで追加の許可を提供する必要がある場合があります。

  たとえば、一部のオートメーションアクションは AWS CloudFormation スタックと連携します。したがって、メンテナンスウィンドウサービスロールのポリシーに、追加の許可 `cloudformation:CreateStack`、`cloudformation:DescribeStacks`、`cloudformation:Delet` を追加する必要がある場合があります。

別の例: オートメーションランブックの AWS-CopySnapshot では、Amazon Elastic Block Store (Amazon EBS) スナップショットを作成するためのアクセス許可が必要です。したがって、許可 ec2:CreateSnapshot を追加する必要がある場合があります。

AWS マネージド Automation ランブックに必要なロール許可については、「AWS Systems Manager Automation ランブックリファレンス」のランブックの説明を参照してください。

AWS マネージド SSM ドキュメントが必要とするロールの許可については、Systems Manager コンソールの「ドキュメント」セクションでドキュメントの内容を確認してください。

Step Functions タスク、Lambda タスク、カスタム Automation ランブックおよび SSM ドキュメントに必要なロール許可については、それらのリソースの作成者に許可要件を確認してください。

タスクはエラーメッセージで失敗します:「Step fails when it is validating and resolving the step inputs」

問題: タスクで使用しているオートメーションランブックまたは Systems Manager Command ドキュメントでは InstanceId や SnapshotId などの入力を指定する必要がありますが、値が指定されていないか、正しく指定されていません。

- 解決策 1 : タスクが 1 つのリソース (単一ノードやスナップショットなど) を対象とする場合は、タスクの入力パラメーターにその ID を入力します。
- 解決策 2: タスクが複数のリソースをターゲットにしている場合 (ランブック AWS-CreateImage を使用するときに複数のノードからイメージを作成する場合など)、メンテナンスウィンドウタスクでサポートされている擬似パラメータの 1 つを入力パラメータで使用して、コマンドでノード ID を表すことができます。

  以下のコマンドは、AWS CLI を使用して、Systems Manager Automation タスクをメンテナンスウィンドウに登録します。--targets の値は、メンテナンスウィンドウのターゲット ID を示します。また、--targets パラメータでウィンドウターゲット ID が指定されていても、Automation ランブックのパラメータにはノード ID を指定する必要があります。この場合、コマンドは擬似パラメーター{{RESOURCE_ID}} を InstanceId の値として使用します。

  AWS CLI コマンド:

Linux & macOS

次のサンプルコマンドは、メンテナンスウィンドウのターゲットグループに属する Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを ID e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE で再起動します。

```
aws ssm register-task-with-maintenance-window \
    --window-id "mw-0c50858d01EXAMPLE" \
    --targets Key=WindowTargetIds,Values=e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE \
    --task-arn "AWS-RestartEC2Instance" \
    --service-role-arn arn:aws:iam::123456789012:role/
MyMaintenanceWindowServiceRole \
    --task-type AUTOMATION \
    --task-invocation-parameters
 "Automation={DocumentVersion=5,Parameters={InstanceId='{{RESOURCE_ID}}'}}" \
    --priority 0 --max-concurrency 10 --max-errors 5 --name "My-Restart-EC2-
Instances-Automation-Task" \
    --description "Automation task to restart EC2 instances"
```

Windows

```
aws ssm register-task-with-maintenance-window ^
    --window-id "mw-0c50858d01EXAMPLE" ^
    --targets Key=WindowTargetIds,Values=e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE ^
    --task-arn "AWS-RestartEC2Instance" ^
    --service-role-arn arn:aws:iam::123456789012:role/
MyMaintenanceWindowServiceRole ^
    --task-type AUTOMATION ^
    --task-invocation-parameters
 "Automation={DocumentVersion=5,Parameters={InstanceId='{{RESOURCE_ID}}'}}" ^
    --priority 0 --max-concurrency 10 --max-errors 5 --name "My-Restart-EC2-
Instances-Automation-Task" ^
    --description "Automation task to restart EC2 instances"
```

メンテナンスウィンドウタスクの擬似パラメータの使用の詳細については、メンテナンスウィンドウのタスクを登録する際の疑似パラメータの使用 および タスクの登録例 を参照してください。

エラーメッセージ:「Maintenance window tasks without targets don't support MaxConcurrency values」および「Maintenance window tasks without targets don't support MaxErrors values」

問題: Run Command タイプタスクを登録するときは、タスクを実行するターゲットを少なくとも 1 つ指定する必要があります。他のタスクタイプ (自動化、AWS Lambda、および AWS Step Functions) では、タスクの特質に応じて、ターゲットはオプションです。ターゲットを指定しないメンテナンスウィンドウタスクでは、オプション `MaxConcurrency` (同時にタスクを実行するリソースの数) と `MaxErrors` (タスクが失敗するまでにターゲットリソースでタスクの実行が失敗できる数) は必須ではなく、サポートされていません。タスクターゲットが指定されていない場合、これらのオプションのいずれかに値が指定されると、システムはこのようなエラーメッセージを生成します。

解決方法: これらのエラーのいずれかを受け取った場合は、メンテナンスウィンドウタスクの登録または更新を続行する前に、同時実行性とエラーしきい値の値を削除します。

ターゲットを指定しないタスクの実行の詳細については、AWS Systems Manager ユーザーガイドの「ターゲットのないメンテナンスウィンドウタスクを登録」を参照してください 。

AWS Systems Manager Quick Setup

AWS Systems Manager のツールである Quick Setup を使用し、推奨されるベストプラクティスを取り入れて頻繁に使用する Amazon Web Services のサービスと機能をすばやく設定します。Quick Setup は一般的なタスクまたは推奨されるタスクを自動化することで、Systems Manager を含むサービスのセットアップを簡素化します。これらのタスクには、例えば、必須の AWS Identity and Access Management (IAM) インスタンスプロファイルロールの作成、定期的なパッチスキャンやインベントリ収集などの運用上のベストプラクティスの設定が含まれます。Quick Setup の使用にコストはかかりません。ただし、設定したサービスの種類と使用制限に基づいて費用が発生する可能性があり、サービスのセットアップに使用したサービスには料金はかかりません。Quick Setup の使用を開始するには、Systems Manager コンソールを開きます。ナビゲーションペインで、[Quick Setup] を選択します。

> **Note**
>
> Quick Setup に移動し、Systems Manager によって管理されるインスタンスを設定できる場合、Quick Setup を使用して Amazon EC2 ホスト管理を設定する の手順を実行します。

Quick Setup の利点は何ですか。

Quick Setup には以下のような利点があります。

- サービスと機能の設定を簡素化

  Quick Setup では、運用上のベストプラクティスの構成手順を説明し、それらの構成を自動的にデプロイします。Quick Setup のダッシュボードには、構成デプロイのステータスがリアルタイムで表示されます。
- 複数のアカウント間で自動的に構成をデプロイ

  AWS Organizations と統合することで、個々の Quick Setup や、複数の AWS アカウント と AWS アカウント にまたがって AWS リージョン を使用できます。複数のアカウントで Quick Setup を使用すると、組織は一貫した構成を維持できます。
- 構成のドリフトを排除

  設定のずれは、Quick Setup によって行われた選択と競合するサービスまたは機能にユーザーが変更を加えるたびに発生します。Quick Setup は定期的に設定のずれをチェックし、修正を試みます。

Quick Setup はどのようなユーザーに適していますか?

Quick Setup は、設定中のサービスや機能を使ったことがあり、セットアッププロセスを簡素化したいお客様に最適です。Quick Setup を使用して構成している AWS のサービスに慣れていない場合は、サービスの詳細を確認するようお勧めします。Quick Setup を使用して設定を作成する前に、適切なユーザガイドの内容を確認してください。

AWS リージョン に Quick Setup の可用性

以下の AWS リージョンでは、AWS Organizations で設定されている組織全体のすべての Quick Setup 設定タイプを使用することも、選択した組織アカウントとリージョンのみに使用することもできます。これらのリージョンでは、1 つのアカウントだけで Quick Setup を使用することもできます。

- 米国東部(オハイオ)
- 米国東部 (バージニア北部)
- 米国西部 (北カリフォルニア)
- 米国西部 (オレゴン)

- アジアパシフィック (ムンバイ)
- アジアパシフィック (ソウル)
- アジアパシフィック (シンガポール)
- アジアパシフィック (シドニー)
- アジアパシフィック (東京)
- カナダ (中部)
- 欧州 (フランクフルト)
- 欧州 (ストックホルム)
- 欧州 (アイルランド)
- 欧州 (ロンドン)
- 欧州 (パリ)
- 南米 (サンパウロ)

以下のリージョンでは、個々のアカウントで使用できるのはホスト管理設定タイプのみです。

- 欧州 (ミラノ)
- アジアパシフィック (香港)
- 中東 (バーレーン)
- 中国 (北京)
- 中国 (寧夏)
- AWS GovCloud (米国東部)
- AWS GovCloud (米国西部)

サポートされているリージョンのリストについては、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」にあるリージョン列を参照してください。

Quick Setup の開始方法

このトピックの情報を利用して、Quick Setup を使用する際の準備に役立ててください。

トピック

- Quick Setup オンボーディングのための IAM ロールと権限
- プログラム的に Quick Setup API を使用するための手動オンボーディング

Quick Setup オンボーディングのための IAM ロールと権限

Quick Setup が新しいコンソールエクスペリエンスと新しい API をリリースしました。今後は、コンソール、AWS CLI、AWS CloudFormation、および SDK を使用してこの API を操作できます。新しいエクスペリエンスをオプトインすると、新しい API を使用して既存の設定が再作成されます。アカウント内の既存の設定の数によっては、このプロセスに数分かかる場合があります。

新しい Quick Setup コンソールを使用するには、次のアクションについての許可が必要です:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm-quicksetup:*",
                "cloudformation:DescribeStackSetOperation",
                "cloudformation:ListStacks",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackResources",
                "cloudformation:ListStackSetOperations",
                "cloudformation:ListStackInstances",
                "cloudformation:DescribeStackSet",
                "cloudformation:ListStackSets",
                "cloudformation:DescribeStackInstance",
                "cloudformation:DescribeOrganizationsAccess",
                "cloudformation:ActivateOrganizationsAccess",
                "cloudformation:GetTemplate",
                "cloudformation:ListStackSetOperationResults",
                "cloudformation:DescribeStackEvents",
                "cloudformation:UntagResource",
                "ec2:DescribeInstances",
                "ssm:DescribeAutomationExecutions",
                "ssm:GetAutomationExecution",
                "ssm:ListAssociations",
                "ssm:DescribeAssociation",
                "ssm:GetDocument",
                "ssm:ListDocuments",
                "ssm:DescribeDocument",
                "ssm:ListResourceDataSync",
                "ssm:DescribePatchBaselines",
                "ssm:GetPatchBaseline",
                "ssm:DescribeMaintenanceWindows",
```

```
                "ssm:DescribeMaintenanceWindowTasks",
                "ssm:GetOpsSummary",
                "organizations:DeregisterDelegatedAdministrator",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListRoots",
                "organizations:ListParents",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:DescribeOrganizationalUnit",
                "organizations:ListAWSServiceAccessForOrganization",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "resource-groups:ListGroups",
                "iam:ListRoles",
                "iam:ListRolePolicies",
                "iam:GetRole",
                "iam:CreatePolicy",
                "organizations:RegisterDelegatedAdministrator",
                "organizations:EnableAWSServiceAccess",
                "cloudformation:TagResource"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:RollbackStack",
                "cloudformation:CreateStack",
                "cloudformation:UpdateStack",
                "cloudformation:DeleteStack"
            ],
            "Resource": [
                "arn:aws:cloudformation:*:*:stack/StackSet-AWS-QuickSetup-*",
                "arn:aws:cloudformation:*:*:stack/AWS-QuickSetup-*",
                "arn:aws:cloudformation:*:*:type/resource/*",
                "arn:aws:cloudformation:*:*:stack/StackSet-SSMQuickSetup"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStackSet",
```

```
                "cloudformation:UpdateStackSet",
                "cloudformation:DeleteStackSet",
                "cloudformation:DeleteStackInstances",
                "cloudformation:CreateStackInstances",
                "cloudformation:StopStackSetOperation"
            ],
            "Resource": [
                "arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-*",
                "arn:aws:cloudformation:*:*:stackset/SSMQuickSetup",
                "arn:aws:cloudformation:*:*:type/resource/*",
                "arn:aws:cloudformation:*:*:stackset-target/AWS-QuickSetup-*:*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:AttachRolePolicy",
                "iam:DetachRolePolicy",
                "iam:GetRolePolicy",
                "iam:PassRole",
                "iam:PutRolePolicy"
            ],
            "Resource": [
                "arn:aws:iam::*:role/AWS-QuickSetup-*",
                "arn:aws:iam::*:role/service-role/AWS-QuickSetup-*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:DeleteAssociation",
                "ssm:CreateAssociation",
                "ssm:StartAssociationsOnce"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ssm:StartAutomationExecution",
            "Resource": "arn:aws:ssm:*:*:automation-definition/AWS-EnableExplorer:*"
        },
        {
```

```
            "Effect": "Allow",
            "Action": [
                "ssm:GetOpsSummary",
                "ssm:CreateResourceDataSync",
                "ssm:UpdateResourceDataSync"
            ],
            "Resource": "arn:aws:ssm:*:*:resource-data-sync/AWS-QuickSetup-*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": [
                        "accountdiscovery.ssm.amazonaws.com",
                        "ssm.amazonaws.com",
                        "ssm-quicksetup.amazonaws.com",
                        "stacksets.cloudformation.amazonaws.com"
                    ]
                }
            },
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/
stacksets.cloudformation.amazonaws.com/
AWSServiceRoleForCloudFormationStackSetsOrgAdmin"
        }
    ]
}
```

ユーザーを読み取り専用許可に制限するには、Quick Setup API のために `ssm-quicksetup:List*` および `ssm-quicksetup:Get*` オペレーションのみを許可します。

オンボーディング中、お客様の代わりに Quick Setup が AWS Identity and Access Management (IAM) ロールを作成します。

- `AWS-QuickSetup-LocalExecutionRole` – パッチポリシーテンプレートを除く任意のテンプレートを使用し、必要なリソースを作成するための AWS CloudFormation 許可を付与します。
- `AWS-QuickSetup-LocalAdministrationRole` – AWS CloudFormation に `AWS-QuickSetup-LocalExecutionRole` を継承する許可を付与します。
- `AWS-QuickSetup-PatchPolicy-LocalExecutionRole` – パッチポリシーテンプレートを使用し、必要なリソースを作成するための許可を AWS CloudFormation に付与します。
- `AWS-QuickSetup-PatchPolicy-LocalAdministrationRole` – AWS CloudFormation に `AWS-QuickSetup-PatchPolicy-LocalExecutionRole` を継承する許可を付与します。

管理アカウント (AWS Organizations で組織の作成に使用するアカウント) をオンボーディングする場合、Quick Setup はまた、ユーザーに代わって次のロールを作成します。

- `AWS-QuickSetup-SSM-RoleForEnablingExplorer` – `AWS-EnableExplorer` オートメーションランブックに許可を付与します。`AWS-EnableExplorer` ランブックは、複数の Explorer と AWS アカウントの情報を表示するように Systems Manager のツールである AWS リージョンを設定します。
- `AWSServiceRoleForAmazonSSM` –サービスにリンクされたロールで、Systems Manager が管理、使用する AWS リソースへのアクセスを付与します。
- `AWSServiceRoleForAmazonSSM_AccountDiscovery` – サービスにリンクされたロールで、データの同期時に AWS のサービスを呼び出して AWS アカウント 情報を検出できるようSystems Manager に許可を付与します。詳細については、「ロールを使用した OpsCenter および Explorer の AWS アカウント 情報の収集」を参照してください。

管理アカウントのオンボーディング中、Quick Setup は、組織全体で Quick Setup をデプロイするために AWS Organizations と CloudFormation の間で安全なアクセスを有効にします。安全なアクセスを有効にするには、管理アカウントに管理者許可が必要です。オンボーディング後、管理者権限は不要になります。詳細については、「組織で安全なアクセスを有効にする」を参照してください。

AWS Organizations アカウントタイプの詳細については、「AWS Organizations ユーザーガイド」の「AWS Organizations Terminology and Concepts」(用語とコンセプト) を参照してください。

> **Note**
>
> Quick Setup は AWS CloudFormation StackSet を使用して、AWS アカウント およびリージョン全体で設定をデプロイします。ターゲットアカウントの数にリージョンの数を乗じて算出した数値が 10,000 を超える場合、設定のデプロイは失敗します。ユースケースを確認

し、組織の成長に合わせて、より少ないターゲットを使用する設定を作成することをお勧めします。スタックインスタンスは、組織の管理アカウントにはデプロイされません。詳細については、「サービスマネージド型のアクセス許可を持つスタックセットを作成する際の考慮事項」を参照してください。

プログラム的に Quick Setup API を使用するための手動オンボーディング

Quick Setup での作業にコンソールを使用する場合は、サービスがユーザーに代わってオンボーディング手順を処理します。Quick Setup API を使用するために SDK または AWS CLI を使用する予定の場合でも、オンボーディング手順はコンソールを使用して完了できるため、この手順を手動で実行する必要はありません。しかし、コンソールを操作せずに Quick Setup のオンボーディング手順をプログラム的に完了する必要があるお客様もいます。この方法がユースケースに適している場合は、次のステップを完了する必要があります。これらのステップはすべて、AWS Organizations 管理アカウントから完了する必要があります。

Quick Setup の手動オンボーディングを完了する

1. Organizations を使用して、AWS CloudFormation の信頼されたアクセスをアクティブ化します。そうすることで、組織の StackSets を作成し管理するためのアクセス許可が管理アカウントに付与されます。このステップは、AWS CloudFormation の `ActivateOrganizationsAccess` API アクションを使用して完了できます。詳細については、「AWS CloudFormation API Reference」の「ActivateOrganizationsAccess」を参照してください。
2. Organizations との Systems Manager の統合を有効にします。そうすることで、Systems Manager が組織内のすべてのアカウントでサービスにリンクされたロールを作成できるようになります。これは、Systems Manager が組織とそのアカウント内で、ユーザーに代わってオペレーションを実行することも可能にします。このステップは、AWS Organizations の `EnableAWSServiceAccess` API アクションを使用して完了できます。Systems Manager のサービスプリンシパルは `ssm.amazonaws.com` です。詳細については、「AWS Organizations API Reference」の「EnableAWSServiceAccess」を参照してください。
3. Explorer に必要な IAM ロールを作成します。そうすることで、Quick Setup が設定のダッシュボードを作成できるようになるため、デプロイと関連付けのステータスを表示することが可能になります。IAM ロールを作成して、`AWSSystemsManagerEnableExplorerExecutionPolicy` マネージドポリシーをアタッチします。以下と一致するようにロールの信頼ポリシーを変更します。各 *`account ID`* は、ユーザー自身の情報に置き換えます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ssm.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "account ID"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:*:ssm:*:account ID:automation-execution/
*"
                }
            }
        }
    ]
}
```

4. Explorer の Quick Setup サービス設定を更新します。このステップは、Quick Setup の UpdateServiceSettings API アクションを使用して完了できます。ExplorerEnablingRoleArn リクエストパラメータに、前のステップで作成した IAM ロールの ARN を指定します。詳細については、「Quick Setup API Reference」の「UpdateServiceSettings」を参照してください。
5. AWS CloudFormation StackSets が使用するための、必要な IAM ロールを作成します。これには、実行ロールと管理ロールを作成する必要があります。

   a. 実行ロールを作成する 実行ロールには、少なくとも AWSQuickSetupDeploymentRolePolicy または AWSQuickSetupPatchPolicyDeploymentRolePolicy 管理ポリシーのいずれかがアタッチされている必要があります。パッチポリシー設定のみを作成している場合は、AWSQuickSetupPatchPolicyDeploymentRolePolicy マネージドポリシーを使用できます。その他すべての設定には、AWSQuickSetupDeploymentRolePolicy ポリシーを使用します。以下と一致するようにロールの信頼ポリシーを変更します。*account ID* と *administration role name* を、ユーザー自身の情報に置き換えます。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::account ID:role/administration role name"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

b. 管理ロールを作成します。許可ポリシーは、以下に一致している必要があります。*account ID* と *execution role name* を、ユーザー自身の情報に置き換えます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": "arn:*:iam::account ID:role/execution role name",
            "Effect": "Allow"
        }
    ]
}
```

以下と一致するようにロールの信頼ポリシーを変更します。各 *account ID* は、ユーザー自身の情報に置き換えます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudformation.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
```

```
                    "aws:SourceAccount": "account ID"
                },
                "StringLike": {
                    "aws:SourceArn": "arn:aws:cloudformation:*:account
 ID:stackset/AWS-QuickSetup-*"
                }
            }
        }
    ]
}
```

Quick Setup での委任管理者の使用

Quick Setup の委任管理者アカウントを登録すると、そのアカウントで適切なアクセス許可を持つユーザーは、AWS Organizations 構造内の組織単位をターゲットとする設定マネージャーを作成、更新、表示、削除できます。委任管理者アカウントはまた、以前、組織の管理アカウントによって作成された設定マネージャーを管理することもできます。

組織の管理アカウントは、組織内の 1 つのアカウントを委任管理者として登録できます。アカウントを Quick Setup の委任管理者として登録すると、このアカウントも AWS CloudFormation StackSets と Systems Manager Explorer の委任管理者になります。これらのサービスは Quick Setup 設定のデプロイとモニタリングに必要になるためです。

> **Note**
>
> 現時点では、パッチポリシー設定タイプは Quick Setup の委任管理者によってサポートされていません。組織のパッチポリシー設定は、組織の管理アカウントで作成および維持する必要があります。詳細については、「the section called “パッチポリシーの作成”」を参照してください。

以下のトピックでは、Quick Setup の委任管理者を登録および登録解除する方法について説明します。

トピック

- Quick Setup の委任管理者の登録
- Quick Setup の委任管理者の登録解除

Quick Setup の委任管理者の登録

Quick Setup の委任管理者を登録するには、次の手順を使用します。

Quick Setup の委任管理者を登録する手順

1. AWS Organizations 管理アカウントにログインします。
2. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
3. ナビゲーションペインで、[Quick Setup] を選択します。
4. [設定] を選択します。
5. [Quick Setup の委任管理者] セクションで、サービスにリンクされた必要なロールとサービスアクセスオプションを設定したことを確認します。必要に応じて、[Create role (ロールの作成)] ボタンと [Enable access (アクセスの有効化)] ボタンを選択して、これらのオプションを設定します。
6. [アカウント ID] に AWS アカウント ID を入力します。このアカウントは、AWS Organizations のメンバーアカウントである必要があります。
7. [Register delegated administrator (委任管理者の登録)] を選択します。

Quick Setup の委任管理者の登録解除

Quick Setup の委任管理者を登録解除するには、次の手順を使用します。

Quick Setup の委任管理者を登録解除する手順

1. AWS Organizations 管理アカウントにログインします。
2. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
3. ナビゲーションペインで、[Quick Setup] を選択します。
4. [設定] を選択します。
5. [Quick Setup の委任された管理者] セクションで、[アクション] ドロップダウンから [登録解除] を選択します。
6. [Confirm] (確認) を選択します。

Quick Setup の用語と詳細を知る

AWS Systems Manager のツールである Quick Setup は、Quick Setup ホームページの [設定マネージャー] テーブルに、すべての AWS リージョンでこれまでに作成したすべての設定マネージャーの結果を表示します。このページから、各設定の [View details] (詳細を表示) したり、[Actions] (アクション) ドロップダウンから設定を削除したり、あるいは設定を [Create] (作成) したりできます。[設定マネージャー] テーブルには次の情報が含まれます。

- [名前] – 作成時に指定された設定マネージャーの名前。
- [Configuration type] (設定タイプ) – 設定の作成時に選択した設定タイプ。
- [バージョン]– 現在デプロイされている設定タイプのバージョン。
- [Organizational units] (組織単位) – ターゲットの [Custom] (カスタム) セットを選択している場合に、対象の設定がデプロイされた組織単位 (OU) を表示します。組織単位とカスタムターゲットは、組織の管理アカウントでのみ使用できます。管理アカウントは、AWS Organizations で組織を作成するために使用するアカウントです。
- [デプロイタイプ] — デプロイが組織全体に適用されるか (`Organizational`)、アカウントのみに適用されるか (`Local`) を示します。
- [Regions] (リージョン) – ターゲットの [Custom] (カスタム) セットを選択した場合、あるいは [Current account] (現在のアカウント) 内のターゲットを選択した場合に、設定がデプロイされているリージョンを示します。
- [Deployment status] (デプロイのステータス) – デプロイのステータスは、ターゲットまたはスタックのインスタンスが、AWS CloudFormation により正常にデプロイされたかどうかを示します。ターゲットとスタックのインスタンスには、設定の作成時に選択した設定オプションが含まれます。
- [Association status] (関連付けのステータス) — 関連付けのステータスは、ユーザーが作成した設定によって作成されたすべての関連付けの状態を示します。すべてターゲットにおいて、関連付けが正常に実行される必要があります。実行されない場合、ステータスは [Failed] (失敗) になります。

  Quick Setup は、各設定ターゲットのための State Manager の関連付けを作成および実行します。State Manager は AWS Systems Manager のツールです。

現在参照しているリージョンにデプロイされている設定を表示するには、[設定] タブを選択します。

設定の詳細

[Configuration details] (設定の詳細) ページに、設定のデプロイとその関連付けに関する情報が表示されます。このページから、設定オプションの編集、ターゲットの更新、または設定の削除を行うことができます。各設定のデプロイに関する詳細を表示し、関連付けに関して、より詳細な情報を取得することもできます。

設定のタイプに応じて、次のステータスグラフが 1 つ以上表示されます。

設定デプロイのステータス

成功、失敗、実行中または保留中のデプロイの数を表示します。デプロイは、設定の影響を受けるノードを含む、指定されたターゲットアカウントとリージョンで実行されます。

設定の関連付けのステータス

成功、失敗、または保留中の State Manager の関連付け数を表示します。Quick Setup は、選択した設定オプション用の関連付けを各デプロイに作成します。

セットアップステータス

設定タイプごとに実行されたアクションの数とそれらの現在のステータスが表示されます。

リソースコンプライアンス

設定で指定されたポリシーに準拠しているリソースの数が表示されます。

[Configuration details] (設定の詳細) テーブルに、設定のデプロイに関する情報が表示されます。デプロイを選択し、[View details] (詳細を表示) をクリックすると、各デプロイをさらに詳細に表示できます。各デプロイの詳細ページには、そのデプロイ内のノードにデプロイされた関連付けが表示されます。

設定の編集と削除

設定のオプションは、[Configuration details] (設定の詳細) ページで、[Actions] (アクション)、[Edit configuration options] (設定オプションの編集) の順にクリックすることで編集できます。設定に新しいオプションを追加すると、Quick Setup がデプロイを実行し、新しい関連付けを作成します。設定からオプションを削除すると、Quick Setup がデプロイを実行し、関連する関連付けを削除します。

> **Note**
>
> アカウントの Quick Setup 設定はいつでも編集することが可能です。[Organization] (組織) 設定を編集するには、[Configuration status] (設定ステータス) が、[Success] (成功) または [Failed] (失敗) のどちらかである必要があります。

[Actions] (アクション) をクリックし、さらに [Add OUs] (OU の追加)、[Add Regions] (リージョンの追加)、[Remove OUs] (OU の削除)、あるいは [Remove Regions] (リージョンの削除) のいずれかをクリックすると、設定に含まれるターゲットを更新することもできます。お使いのアカウントが管理アカウントとして設定されていない場合、または現在のアカウントのみの設定を作成した場合は、ターゲットの組織単位 (OU) は更新できません。リージョンまたは OU を削除すると、それらのリージョンまたは OU から関連付けが削除されます。

定期的に、Quick Setup は設定の新しいバージョンをリリースします。設定を最新バージョンにアップグレードするために、[設定をアップグレード] オプションを選択できます。

設定を選択した上で、[Actions] (アクション)、[Delete configuration] (設定の削除) の順にクリックすると、Quick Setup からその設定を削除できます。または、[Configuration details] (設定の詳細) ページにある [Actions] (アクション) ドロップダウンで、[Delete configuration] (設定の削除) を選択して設定を削除することも可能です。その後 Quick Setup により、[Remove all OUs and Regions] (すべての OU とリージョンを削除する) よう求められます。この処理は完了するまで時間がかかる場合があります。設定を削除すると、関連する関連付けもすべて削除されます。この 2 段階削除プロセスでは、すべてのアカウントとリージョンからデプロイされたすべてのリソースを削除した上で、設定を削除します。

設定コンプライアンス

インスタンスが、設定によって作成された関連付けに準拠しているかどうかは、Explorer または Compliance のいずれか (どちらも AWS Systems Manager に含まれるツール) により確認できます。コンプライアンスの詳細については、「コンプライアンスの詳細について」を参照してください。Explorer でのコンプライアンスの表示については、「AWS Systems Manager Explorer」を参照してください。

Quick Setup API を使用した設定とデプロイの管理

AWS CLI または任意の SDK を用いて設定とデプロイを作成および管理するには、Quick Setup 提供の API を使用できます。AWS CloudFormation を使用して、設定をデプロイする設定マネージャーリソースを作成することも可能です。API を使用して、設定定義をデプロイする設定マネージャーを

作成します。設定定義には、特定の設定タイプをデプロイするために必要な情報のすべてが含まれています。Quick Setup API の詳細については、「Quick Setup API Reference」を参照してください。

以下の例は、AWS CLI と AWS CloudFormation を使用して設定マネージャーを作成する方法を示しています。

AWS CLI

```
aws ssm-quicksetup create-configuration-manager \
--name configuration manager name \
--description Description of your configuration manager
--configuration-definitions JSON string containing configuration defintion
```

以下は、パッチポリシーの設定定義が含まれる JSON 文字列の例です。

```
'{"Type":"AWSQuickSetupType-
PatchPolicy","LocalDeploymentAdministrationRoleArn":"arn:aws:iam::123456789012:role/
AWS-QuickSetup-StackSet-Local-
AdministrationRole","LocalDeploymentExecutionRoleName":"AWS-
QuickSetup-StackSet-Local-ExecutionRole","Parameters":
{"ConfigurationOptionsInstallNextInterval":"true","ConfigurationOptionsInstallValue":"cron(0
 2 ? * SAT#1
 *)","ConfigurationOptionsPatchOperation":"ScanAndInstall","ConfigurationOptionsScanNextInte
 1 * * ?
 *)","HasDeletedBaseline":"false","IsPolicyAttachAllowed":"true","OutputBucketRegion":"","Ou
east-1","PatchBaselineUseDefault":"custom","PatchPolicyName":"dev-patch-
policy","RateControlConcurrency":"5","RateControlErrorThreshold":"0%","RebootOption":"Reboot
\":{\"value\":\"arn:aws:ssm:us-east-1:123456789012:patchbaseline/
pb-0cb0c4966f86b059b\",\"label\":\"AWS-AlmaLinuxDefaultPatchBaseline\",\"description
\":\"Default Patch Baseline for Alma Linux Provided by AWS.\",\"disabled\":false},
\"AMAZON_LINUX\":{\"value\":\"arn:aws:ssm:us-east-1:123456789012:patchbaseline/
pb-0c10e657807c7a700\",\"label\":\"AWS-AmazonLinuxDefaultPatchBaseline\",
\"description\":\"Default Patch Baseline for Amazon Linux Provided by AWS.
\",\"disabled\":false},\"AMAZON_LINUX_2\":{\"value\":\"arn:aws:ssm:us-
east-1:123456789012:patchbaseline/pb-0be8c61cde3be63f3\",\"label\":\"AWS-
AmazonLinux2DefaultPatchBaseline\",\"description\":\"Baseline containing
 all Security and Bugfix updates approved for Amazon Linux 2 instances
\",\"disabled\":false},\"AMAZON_LINUX_2022\":{\"value\":\"arn:aws:ssm:us-
east-1:123456789012:patchbaseline/pb-0028ca011460d5eaf\",\"label\":\"AWS-
AmazonLinux2022DefaultPatchBaseline\",\"description\":\"Default Patch
 Baseline for Amazon Linux 2022 Provided by AWS.\",\"disabled\":false},
\"AMAZON_LINUX_2023\":{\"value\":\"arn:aws:ssm:us-east-1:123456789012:patchbaseline/
pb-05c9c9bf778d4c4d0\",\"label\":\"AWS-AmazonLinux2023DefaultPatchBaseline
```

```
\",\"description\":\"Default Patch Baseline for Amazon Linux 2023 Provided
 by AWS.\",\"disabled\":false},\"CENTOS\":{\"value\":\"arn:aws:ssm:us-
east-1:123456789012:patchbaseline/pb-03e3f588eec25344c\",\"label\":\"AWS-
CentOSDefaultPatchBaseline\",\"description\":\"Default Patch Baseline for CentOS
 Provided by AWS.\",\"disabled\":false},\"DEBIAN\":{\"value\":\"arn:aws:ssm:us-
east-1:123456789012:patchbaseline/pb-09a5f8eb62bde80b1\",\"label\":\"AWS-
DebianDefaultPatchBaseline\",\"description\":\"Default Patch Baseline for Debian
 Provided by AWS.\",\"disabled\":false},\"MACOS\":{\"value\":\"arn:aws:ssm:us-
east-1:123456789012:patchbaseline/pb-0ee4f94581368c0d4\",\"label\":\"AWS-
MacOSDefaultPatchBaseline\",\"description\":\"Default Patch Baseline for
 MacOS Provided by AWS.\",\"disabled\":false},\"ORACLE_LINUX\":{\"value\":
\"arn:aws:ssm:us-east-1:123456789012:patchbaseline/pb-06bff38e95fe85c02\",
\"label\":\"AWS-OracleLinuxDefaultPatchBaseline\",\"description\":\"Default
 Patch Baseline for Oracle Linux Server Provided by AWS.\",\"disabled\":false},
\"RASPBIAN\":{\"value\":\"arn:aws:ssm:us-east-1:123456789012:patchbaseline/
pb-0ec16280999c5c75e\",\"label\":\"AWS-RaspbianDefaultPatchBaseline\",
\"description\":\"Default Patch Baseline for Raspbian Provided by AWS.\",
\"disabled\":false},\"REDHAT_ENTERPRISE_LINUX\":{\"value\":\"arn:aws:ssm:us-
east-1:123456789012:patchbaseline/pb-0cbb3a633de00f07c\",\"label\":\"AWS-
RedHatDefaultPatchBaseline\",\"description\":\"Default Patch Baseline for Redhat
 Enterprise Linux Provided by AWS.\",\"disabled\":false},\"ROCKY_LINUX\":{\"value
\":\"arn:aws:ssm:us-east-1:123456789012:patchbaseline/pb-03ec98bc512aa3ac0\",\"label
\":\"AWS-RockyLinuxDefaultPatchBaseline\",\"description\":\"Default Patch Baseline
 for Rocky Linux Provided by AWS.\",\"disabled\":false},\"SUSE\":{\"value\":
\"arn:aws:ssm:us-east-1:123456789012:patchbaseline/pb-07d8884178197b66b\",\"label\":
\"AWS-SuseDefaultPatchBaseline\",\"description\":\"Default Patch Baseline for Suse
 Provided by AWS.\",\"disabled\":false},\"UBUNTU\":{\"value\":\"pb-06e3563bd35503f2b
\",\"label\":\"custom-UbuntuServer-Blog-Baseline\",\"description\":\"Default Patch
 Baseline for Ubuntu Provided by AWS.\",\"disabled\":false},\"WINDOWS\":{\"value
\":\"pb-016889927b2bb8542\",\"label\":\"custom-WindowsServer-Blog-Baseline\",
\"disabled\":false}}","TargetInstances":"","TargetOrganizationalUnits":"ou-9utf-
example","TargetRegions":"us-east-1,us-
east-2","TargetTagKey":"Patch","TargetTagValue":"true","TargetType":"Tags"}}' \
```

AWS CloudFormation

```
AWSTemplateFormatVersion: '2010-09-09'
Resources:
SSMQuickSetupTestConfigurationManager:
Type: "AWS::SSMQuickSetup::ConfigurationManager"
Properties:
    Name: "MyQuickSetup"
    Description: "Test configuration manager"
```

```
    ConfigurationDefinitions:
    - Type: "AWSQuickSetupType-CFGRecording"
      Parameters:
        TargetAccounts:
            Ref: AWS::AccountId
        TargetRegions:
            Ref: AWS::Region
        LocalDeploymentAdministrationRoleArn: !Sub "arn:aws:iam::
${AWS::AccountId}:role/AWS-QuickSetup-StackSet-ContractTest-AdministrationRole"
        LocalDeploymentExecutionRoleName: "AWS-QuickSetup-StackSet-ContractTest-
ExecutionRole"
    Tags:
        foo1: "bar1"
```

サポートされている Quick Setup 設定タイプ

サポートされている設定タイプ

Quick Setup では、多数の Systems Manager とその他の AWS のサービス の運用上のベストプラクティスを設定し、それらの設定を自動的にデプロイすることができます。Quick Setup のダッシュボードには、構成デプロイのステータスがリアルタイムで表示されます。

Quick Setup は、個々の AWS アカウント で使用するか、AWS Organizations と統合することによって複数の AWS アカウント とリージョンにまたがって使用することができます。複数のアカウントで Quick Setup を使用すると、組織は一貫した構成を維持できます。

Quick Setup は以下の設定タイプにサポートを提供します。

- Quick Setup を使用して Amazon EC2 ホスト管理を設定する
- Quick Setup を使用して組織のために Default Host Management Configuration を設定する
- Quick Setup を使用して AWS Config 設定レコーダーを作成する
- Quick Setup を使用して AWS Config 適合パックをデプロイする
- Quick Setup パッチポリシーを使用して組織内のインスタンスのためにパッチ適用を設定する
- Change Manager 組織設定
- Quick Setup を使用して DevOps Guru をセットアップする
- Quick Setup を使用して Distributor パッケージをデプロイする
- Quick Setup を使用してスケジュールに従って EC2 インスタンスを自動的に停止および起動する

- OpsCenter 組織設定
- Quick Setup を使用して AWS Resource Explorer を設定する

Quick Setup を使用して Amazon EC2 ホスト管理を設定する

AWS Systems Manager のツールである Quick Setup を利用することで、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスで必要なセキュリティロールと一般的に使用される Systems Manager ツールをすばやく設定できます。AWS Organizations と統合することで、個々のアカウントで、または複数のアカウントと AWS リージョン にまたがって Quick Setup を使用できます。これらのツールは、使用を開始するために必要な最小限のアクセス許可を提供しながら、インスタンスの正常性を管理およびモニタリングするのに役立ちます。

Systems Manager のサービスと機能に慣れていない場合は、Quick Setup の設定を作成する前に AWS Systems Manager ユーザーガイドを確認するようお勧めします。Systems Manager の詳細については、「AWS Systems Manager とは」を参照してください。

Important

次のいずれかに当てはまる場合、Quick Setup は EC2 管理には適切なツールではない可能性があります。

- 初めて EC2 インスタンスを作成して、AWS 機能を試してみようとしている。
- EC2 インスタンス管理にまだ慣れていない。

次の内容から始めることをお勧めします。

- Amazon EC2 の開始方法
- 「Amazon EC2 ユーザーガイド」の「新しいインスタンス起動ウィザードを使用してインスタンスを起動する」
- 「Amazon EC2 ユーザーガイド」の「チュートリアル: Amazon EC2 Linux インスタンスの開始方法」

すでに EC2 インスタンス管理に慣れていて、複数の EC2 インスタンスの設定と管理を効率化したい場合は、Quick Setup を使用してください。組織の EC2 インスタンスが数十、数千、数百万のいずれであっても、次の Quick Setup 手順を使用して、複数のオプションを一度に設定してください。

> **Note**
>
> この設定タイプでは、AWS Organizations で定義されている組織全体、一部の組織アカウントとリージョンのみ、または単一のアカウントに複数のオプションを設定できます。これらのオプションの 1 つは、2 週間ごとに SSM Agent への更新を確認して適用することです。組織管理者の場合は、デフォルトのホスト管理設定タイプを使用して、2 週間ごとに組織内のすべての EC2 インスタンスをエージェントアップデートで更新するように選択することもできます。詳細については、Quick Setup を使用して組織のために Default Host Management Configuration を設定する を参照してください。

EC2 インスタンスのホスト管理オプションの設定

ホスト管理を設定するには、AWS Systems Manager Quick Setup コンソールで次のタスクを実行します。

ホスト管理設定ページを開くには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Quick Setup] を選択します。
3. [ホスト管理] カードで、[作成] を選択します。

> **Tip**
>
> アカウントにすでに 1 つ以上の設定がある場合は、まず[設定] セクションで [ライブラリ] タブまたは [作成] ボタンを選択し、カードを表示します。

Systems Manager のホスト管理オプションを設定するには

- Systems Manager 機能を設定するには、[設定オプション] セクションで、設定で有効にする Systems Manager グループの次のオプションを選択します。

Systems Manager (SSM) エージェントを 2 週間ごとに更新する

エージェントの新しいバージョンがあるかどうか Systems Manager が 2 週間ごとに確認できるようにします。新しいバージョンがある場合、Systems Manager はマネージドノード上のエージェントを最新のリリースバージョンに自動的に更新します。Quick Setup は、エージェントがまだ存在しないインスタンスにエージェントをインストールすることはありません。どの AMIs に SSM Agent がプリインストールされているかについては、「SSM Agent がプリインストールされている AMIs を見つける」を参照してください。

ノードが常に最新バージョンの SSM Agent を実行できるように、このオプションを選択することをお勧めします。エージェントを手動でインストールする方法など SSM Agent の詳細については、「「SSM Agent」 の使用」を参照してください。

30 分ごとにインスタンスからインベントリを収集する

次のタイプのメタデータの収集を Quick Setup が設定できるようにします。

- AWS コンポーネント – EC2 ドライバー、エージェント、バージョンなど。
- アプリケーション – アプリケーション名、発行元、バージョンなど。
- ノードの詳細 – システム名、オペレーティングシステム (OS) 名、OS バージョン、最終起動、DNS、ドメイン、ワークグループ、OS アーキテクチャなど。
- ネットワーク設定 – IP アドレス、MAC アドレス、DNS、ゲートウェイ、サブネットマスクなど。
- サービス – 名前、表示名、ステータス、依存サービス、サービスタイプ、スタートタイプなど (Windows Server ノードのみ)。
- Windows ロール – 名前、表示名、パス、特徴タイプ、インストールされている状態など (Windows Server ノードのみ)。
- Windows 更新 – Hotfix ID、インストール者、インストール日など (Windows Server ノードのみ)。

AWS Systems Manager のツールである Inventory の詳細については、「AWS Systems Manager インベントリ」を参照してください。

> **Note**
>
> [Inventory collection] (インベントリ収集) オプションは、数個のノードのみを選択した場合でも、完了までに最大 10 分かかることがあります。

欠落しているパッチを毎日スキャンする

Systems Manager のツールである Patch Manager によって、ノードを毎日スキャンし、[コンプライアンス] ページでレポートを生成できるようにします。このレポートには、デフォルトのパッチベースラインに従って、パッチに準拠しているノードの数が表示されます。このレポートには、各ノードとそのコンプライアンス ステータスのリストが含まれます。

パッチ適用オペレーションとパッチベースラインについては、「AWS Systems Manager Patch Manager」を参照してください。

パッチコンプライアンスについては、Systems Manager の [Compliance] (コンプライアンス) ページを参照してください。

1 つの設定で複数のアカウントとリージョンのマネージドノードにパッチを適用する方法については、「Quick Setup でのパッチポリシー設定 」と「Quick Setup パッチポリシーを使用して組織内のインスタンスのためにパッチ適用を設定する」を参照してください。

> **Important**
>
> Systems Manager では、パッチコンプライアンスに関してマネージドノードをスキャンするいくつかの方法がサポートされています。これらの方法を一度に複数実施した場合、表示されるパッチコンプライアンス情報は常に最新のスキャンの結果です。以前のスキャンの結果は上書きされます。スキャン方法によって異なるパッチベースラインと異なる承認ルールが使用されている場合、パッチコンプライアンス情報が予期せず変化する可能性があります。詳細については、「パッチコンプライアンスデータに対する意図しない上書きの回避」を参照してください。

Amazon CloudWatch ホスト管理オプションを設定するには

- CloudWatch 機能を設定するには、[設定オプション] セクションで、設定で有効にする Amazon CloudWatch グループの次のオプションを選択します。

CloudWatch エージェントをインストールして設定する

統合 CloudWatch エージェントの基本的な設定が、Amazon EC2 インスタンスにインストールされます。エージェントは、Amazon CloudWatch のインスタンスからメトリクスとログファイルを収集します。この情報は統合されているため、インスタンスの正常性をすばやく判断できます。CloudWatch エージェントのベーシック 設定の詳細については、[CloudWatch agent predefined metric sets] (CloudWatch エージェントの定義済みメトリクス セット) を参照してください。追加コストが発生する場合があります。詳細については、「Amazon CloudWatch の料金」を参照してください。

CloudWatch エージェントを 30 日に 1 回更新する

CloudWatch エージェントの新しいバージョンがあるかどうか Systems Manager が 30 日ごとに確認できるようにします。新しいバージョンがある場合、Systems Manager はインスタンスのエージェントを更新します。インスタンスで常に最新バージョンの CloudWatch エージェントが実行されるように、このオプションを選択することをお勧めします。

Amazon EC2 起動エージェントのホスト管理オプションを設定するには

- Amazon EC2 起動エージェント機能を設定するには、[設定オプション] セクションで、設定で有効にする Amazon EC2 起動エージェントグループの次のオプションを選択します。

EC2 起動エージェントを 30 日に 1 回更新する

インスタンスにインストールされている起動エージェントの新しいバージョンを Systems Manager が 30 日ごとに確認できるようにします。新しいバージョンが利用可能である場合、Systems Manager はインスタンスのエージェントを更新します。インスタンスで常に最新バージョンの適切な起動エージェントが実行されるように、このオプションを選択することをお勧めします。Amazon EC2 Windows インスタンスの場合、このオプションは EC2Launch、EC2Launch v2、および EC2Config をサポートします。Amazon EC2 Linux インスタンスの場合、このオプションは `cloud-init` をサポートします。Amazon EC2 Mac インスタンスの場合、このオプションは `ec2-macos-init` をサポートします。Quick Setup は、起動エージェントによってサポートされていないオペレーティングシステムまたは AL2023 にインストールされている起動エージェントの更新をサポートしていません。

これらの初期化エージェントの詳細については、次のトピックを参照してください。

- EC2Launch v2 を使用した Windows インスタンスの設定
- EC2Launch を使用した Windows インスタンスの設定
- EC2Config サービスを使用した Windows インスタンスの設定
- cloud-init ドキュメント
- ec2-macos-init

ホスト管理設定によって更新する EC2 インスタンスを選択するには

- [ターゲット] セクションで、設定をデプロイするアカウントとリージョンを決定する方法を選択します。

> **Note**
>
> 同じ AWS リージョン を対象に複数の Quick Setup ホスト管理設定を作成することはできません。

Entire organization

設定は組織内のすべての組織単位 (OU) と AWS リージョン にデプロイされます。

> **Note**
>
> [Entire organization (組織全体)] オプションは、組織の管理アカウントからホスト管理を設定する場合にのみ使用できます。

Custom

1. [ターゲット OU] セクションで、このホスト管理設定をデプロイする OU を選択します。
2. [ターゲットリージョン] セクションで、このホスト管理設定をデプロイするリージョンを選択します。

Current account

リージョンオプションのいずれかを選択し、そのオプションの手順に従います。

現在のリージョン

現在のリージョンのみの中で、インスタンスをターゲットにする方法を以下のいずれかから選択します。

- すべてのインスタンス – ホスト管理設定は、現在のリージョンのすべての EC2 を自動的にターゲットにします。
- タグ – [追加] を選択し、ターゲットにするインスタンスに追加したキーとオプションの値を入力します。
- リソースグループ – [リソースグループ] で、ターゲットにする EC2 インスタンスを含む既存のリソースグループを選択します。
- 手動 – [インスタンス] セクションで、ターゲットにする各 EC2 インスタンスのチェックボックスを選択します。

リージョンを選択する

以下のいずれかを選択して、指定したリージョンのインスタンスをターゲットにする方法を選択します。

- すべてのインスタンス – 指定したリージョンのすべてのインスタンスがターゲットになります。
- タグ – [追加] を選択し、ターゲットにするインスタンスに追加したキーとオプションの値を入力します。

[ターゲットリージョン] セクションで、このホスト管理設定をデプロイするリージョンを選択します。

インスタンスプロファイルオプションを指定するには

- [組織全体] と [カスタム] ターゲットのみ。

  [インスタンスプロファイルのオプション] セクションで、インスタンスにアタッチされた既存のインスタンスプロファイルに必要な IAM ポリシーを追加するか、選択した設定に必要なアクセス許可を持つ IAM ポリシーとインスタンスプロファイルを Quick Setup で作成できるようにするか選択します。

設定の選択肢をすべて指定したら、[作成] を選択します。

Quick Setup を使用して組織のために Default Host Management Configuration を設定する

Quick Setup で AWS Systems Manager のツールを使用すると、AWS Organizations で組織に追加されたすべてのアカウントとリージョンのデフォルトのホスト管理設定を有効化できます。これにより、組織内のすべての Amazon Elastic Compute Cloud (EC2) インスタンスで SSM Agent が最新の状態に保たれ、Systems Manager に接続できます。

[開始する前に]

この設定を有効にする前に、以下の要件が満たされるようにしてください。

- 組織の管理対象となるすべての EC2 インスタンスに、SSM Agent の最新バージョンがすでにインストールされている。
- 管理対象となる EC2 インスタンスが、インスタンスメタデータサービスのバージョン 2 (IMDSv2) を使用している。
- AWS Organizations で指定されているように、管理者権限を持つ AWS Identity and Access Management (IAM) ID (ユーザー、ロール、またはグループ) を使用して、組織の管理アカウントにサインインしている。

デフォルトの EC2 インスタンス管理ロールを使用する

デフォルトのホスト管理設定は、Systems Manager の `default-ec2-instance-management-role` サービス設定を利用します。これは、インスタンスとクラウド内の Systems Manager サービス上の SSM Agent 間の通信を可能にするために、組織内のすべてのアカウントで利用できるようにしたいアクセス許可を持つロールです。

update-service-setting CLI コマンドを使用してこのロールをすでに設定している場合、デフォルトのホスト管理設定ではそのロールが使用されます。このロールをまだ設定していない場合は、Quick Setup は自動的にロールを作成して適用します。

このロールが組織ですでに指定されているかどうかを確認するには、get-service-setting コマンドを使用します。

2 週間ごとに SSM Agent の自動更新を有効にする

以下の手順に従って、AWS Organizations 組織全体でデフォルトのホスト管理設定オプションを有効にします。

2 週間ごとに SSM Agent の自動更新を有効にするには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Quick Setup] を選択します。
3. [デフォルトのホスト管理設定] カードで、[作成] を選択します。

> **Tip**
>
> アカウントにすでに 1 つ以上の設定がある場合は、まず[設定] セクションで [ライブラリ] タブまたは [作成] ボタンを選択し、カードを表示します。

4. [設定オプション] セクションで、[2 週間ごとに SSM Agent の自動更新を有効にする] を選択します。
5. 作成を選択します。

Quick Setup を使用して AWS Config 設定レコーダーを作成する

AWS Systems Manager のツールである Quick Setup を使用すると、AWS Config による設定レコーダーをすばやく作成できます。設定レコーダーを使用してリソースの設定変更を検出し、これらの変更を設定項目として取り込みます。AWS Config に慣れていない場合は、Quick Setup を使用して設定を作成する前に、 AWS Config デベロッパーガイドの内容を確認して、サービスの詳細を確認するようお勧めします。AWS Config の詳細については、AWS Config デベロッパーガイドの「AWS Config とは」を参照してください。

デフォルトでは、設定レコーダーは AWS Config が実行されている AWS リージョン のすべてのサポートされているリソースを記録します。指定したリソースタイプのみが記録されるように、設定をカスタマイズできます。詳細については、AWS Config デベロッパーガイドの「AWS Config が記録するリソースを選択する」を参照してください。

AWS Config で設定の記録が開始されると、サービスの利用料金が発生します。料金については、AWS Config の料金をご参照ください。

> **Note**
>
> 設定レコーダーを既に作成している場合は、Quick Setup は記録を停止したり、既に記録しているリソースタイプを変更したりしません。Quick Setup を使用して追加のリソースタイプを記録することを選択した場合、サービスはそれらを既存のレコーダーグループに追加し

ます。Quick Setup Config 記録設定タイプを削除しても、設定レコーダーは停止しません。変更は引き続き記録され、設定レコーダーを停止するまでサービス利用料がかかります。設定レコーダーの管理の詳細については、AWS Configデベロッパーガイドの「設定レコーダーの管理」を参照してください。

AWS Config の記録を設定するには、AWS Systems Manager コンソールで次のタスクを実行します。

Quick Setup を使用して AWS Config の記録をセットアップするには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Quick Setup] を選択します。
3. [Config Recording]カードで、[作成] を選択します。

   > **Tip**
   >
   > アカウントにすでに 1 つ以上の設定がある場合は、まず[設定] セクションで [ライブラリ] タブまたは [作成] ボタンを選択し、カードを表示します。

4. [設定オプション] セクションで、次を実行します:

   a. [記録する AWS リソースタイプを選択] で、サポートされているすべてのリソースを記録するか、選択したリソースタイプのみを記録するかを指定します。

   b. [配信設定] では、新しい Amazon Simple Storage Service (Amazon S3) バケットを作成するか、または設定スナップショットを送信する既存のバケットを選択するかを指定します。

   c. [通知オプション] で、希望する通知オプションを選択します。AWS Config は、Amazon Simple Notification Service (Amazon SNS) を使用して、リソースに関連する重要な AWS Config イベントについて通知します。[既存の SNS トピックの使用] オプションを選択した場合は、使用するアカウントの既存の Amazon SNS トピックの AWS アカウント ID と名前を指定する必要があります。複数の AWS リージョン をターゲットにする場合、トピック名は各リージョンで同一である必要があります。

5. [Schedule (スケジュール)] セクションで、設定とは異なるリソースに加えられた変更を Quick Setup で修正する頻度を選択します。[Default (デフォルト)] オプションは 1 回実行されます。設定と異なるリソースに加えられた変更を Quick Setup で修正しない場合は、[Custom (カスタム)] で [Disable remediation (修復を無効にする)] を選択します。

6. [ターゲット] セクションで、次のいずれかを選択して、記録のためにアカウントとリージョンを識別します。

> **Note**
>
> 1 つのアカウントで作業している場合、組織や組織単位 (OU) を使用するオプションは利用できません。この設定をアカウント内のすべての AWS リージョン に適用するか、選択したリージョンのみに適用するかを選択できます。

- [Entire organization] (組織全体) – 組織内のすべてのアカウントとリージョン。
- [Custom] (カスタム) – 指定した OU とリージョンのみ。
  - [ターゲット OU] セクションで、記録を許可する OU を選択します。
  - [ターゲットリージョン] セクションで、記録を許可するリージョンを選択します。
- [Current account] (現在のアカウント) – 現在サインインしているアカウント内の指定したリージョンのみがターゲットになります。次のいずれかを選択します。
  - [Current Region] (現在のリージョン) – コンソールで選択したリージョン内のマネージドノードのみがターゲットになります。
  - [リージョンを選択] – 記録設定を適用する個々のリージョンを選択します。

7. [Create] (作成) を選択します。

Quick Setup を使用して AWS Config 適合パックをデプロイする

コンフォーマンスパックは、AWS Config ルールと是正アクションのコレクションです。Quick Setupでは、アカウントと AWS リージョン で単一のエンティティとして、または AWS Organizations の組織全体でコンフォーマンスパックをデプロイできます。これは、共通のフレームワークとパッケージ化モデルを使用して、ポリシー定義から監査および集約レポートまで大規模に AWS リソースの設定コンプライアンスを管理する際に役立ちます。

コンフォーマンスパックをデプロイするには、AWS Systems Manager Quick Setup コンソールで以下のタスクを実行します。

> **Note**
>
> この設定をデプロイする前に、AWS Config 記録を有効にする必要があります。詳細については、AWS Config デベロッパーガイドの「コンフォーマンスパック」を参照してください。

Quick Setup でコンフォーマンスパックをデプロイするには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Quick Setup] を選択します。
3. [コンフォーマンスパック] カードで、[作成] を選択します。

   > **Tip**
   >
   > アカウントにすでに 1 つ以上の設定がある場合は、まず[設定] セクションで [ライブラリ] タブまたは [作成] ボタンを選択し、カードを表示します。

4. [コンフォーマンスパックを選択] セクションで、デプロイするコンフォーマンスパックを選択します。
5. [Schedule (スケジュール)] セクションで、設定とは異なるリソースに加えられた変更を Quick Setup で修正する頻度を選択します。[Default (デフォルト)] オプションは 1 回実行されます。設定と異なるリソースに加えられた変更を Quick Setup で修正しない場合は、[Custom (カスタム)] で [Disabled (無効にする)] を選択します。
6. [Targets (ターゲット)] セクションで、コンフォーマンスパックを組織全体、一部の AWS リージョン、または現在ログインしているアカウントにデプロイするのか選択します。

   [組織全体] を選択した場合は、ステップ 8 に進みます。

   [カスタム] を選択した場合は、ステップ 7 に進みます。
7. [Target Regions (ターゲットリージョン)] セクションで、 コンフォーマンスパックのデプロイ先リージョンのチェックボックスを選択します。
8. [Create] (作成) を選択します。

Quick Setup パッチポリシーを使用して組織内のインスタンスのためにパッチ適用を設定する

AWS Systems Manager のツールである Quick Setup を使用すると、Patch Manager を利用したパッチポリシーを作成できます。パッチポリシーは、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスなどのマネージドノードに自動的にパッチを適用するときに使用するスケジュールとベースラインを定義します。単一のパッチポリシー設定を使用して、組織内の複数の AWS リージョンのすべてのアカウントにパッチを定義するか、選択したアカウントとリージョンのみに適用するか、単一のアカウントとリージョンのペアに適用するかを定義できます。パッチポリシーの詳細については、「Quick Setup でのパッチポリシー設定」を参照してください。

前提条件

Quick Setup を使用してノードのパッチポリシーを定義するには、そのノードがマネージドノードである必要があります。ノードの管理方法の詳細については、「組織用の Systems Manager 統合コンソールのセットアップ」を参照してください。

> **Important**
>
> パッチコンプライアンスのスキャン方法 – Systems Manager では、パッチコンプライアンスに関してマネージドノードをスキャンするいくつかの方法がサポートされています。これらの方法を一度に複数実施した場合、表示されるパッチコンプライアンス情報は常に最新のスキャンの結果です。以前のスキャンの結果は上書きされます。スキャン方法によって異なるパッチベースラインと異なる承認ルールが使用されている場合、パッチコンプライアンス情報が予期せず変化する可能性があります。詳細については、「パッチコンプライアンスデータに対する意図しない上書きの回避」を参照してください。
>
> 関連付けコンプライアンスステータスとパッチポリシー – Quick Setup パッチポリシーの下にあるマネージドノードのパッチステータスは、そのノードの State Manager 関連付け実行ステータスと一致します。関連付け実行ステータスが `Compliant` の場合、マネージドノードのパッチステータスも `Compliant` とマークされます。関連付け実行ステータスが `Non-Compliant` の場合、マネージドノードのパッチステータスも `Non-Compliant` とマークされます。

パッチポリシー設定がサポートされているリージョン

Quick Setup でのパッチポリシー設定は、現在、次のリージョンでサポートされています。

- 米国東部 (オハイオ) (us-east-2)
- 米国東部 (バージニア北部) (us-east-1)

- 米国西部 (北カリフォルニア) (us-west-1)
- 米国西部 (オレゴン) (us-west-2)
- アジアパシフィック (ムンバイ) (ap-south-1)
- アジアパシフィック (ソウル) (ap-northeast-2)
- アジアパシフィック (シンガポール) (ap-southeast-1)
- アジアパシフィック (シドニー) (ap-southeast-2)
- アジアパシフィック (東京) (ap-northeast-1)
- カナダ (中部) (ca-central-1)
- ヨーロッパ (フランクフルト) (eu-central-1)
- 欧州 (アイルランド) (eu-west-1)
- ヨーロッパ (ロンドン) (eu-west-2)
- 欧州 (パリ) (eu-west-3)
- 欧州 (ストックホルム) (eu-north-1)
- 南米 (サンパウロ) (sa-east-1)

パッチポリシー S3 バケットの許可

パッチポリシーを作成すると、Quick Setup は `baseline_overrides.json` という名前のファイルを含む Amazon S3 バケットを作成します。このファイルには、パッチポリシー用に指定したパッチベースラインに関する情報が保存されます。

S3 バケットの名前は、`aws-quicksetup-patchpolicy-`*`account-id`*`-`*`quick-setup-configuration-id`* の形式で付けられます。

例: `aws-quicksetup-patchpolicy-123456789012-abcde`

組織のパッチポリシーを作成している場合、バケットは組織の管理アカウントに作成されます。

AWS Identity and Access Management (IAM) ポリシーを使用して、この S3 バケットにアクセスするための許可を他の AWS リソースに提供する必要がある場合は、次の 2 つのユースケースが参考になります。

- ケース 1: マネージドノードで、Quick Setup によって提供されるインスタンスプロファイルまたはサービスロールではなく、独自のインスタンスプロファイルまたはサービスロールを使用する

- ケース 2: VPC エンドポイントを使用して Systems Manager に接続する

いずれの場合でも必要な許可ポリシーは、以下のセクション「Quick Setup S3 バケットのポリシー許可」にあります。

ケース 1: マネージドノードで、Quick Setup によって提供されるインスタンスプロファイルまたはサービスロールではなく、独自のインスタンスプロファイルまたはサービスロールを使用する

パッチポリシー設定には、[インスタンスにアタッチされている既存のインスタンスプロファイルに必要な IAM ポリシーを追加] オプションが含まれています。

このオプションを選択せずに、このパッチポリシーを使用してマネージドノードにパッチを Quick Setup に適用する場合は、次が実装されていることを確認する必要があります。

- IAM 管理ポリシー `AmazonSSMManagedInstanceCore` は、マネージドノードに Systems Manager 許可を付与するために使用される IAM インスタンスプロファイルまたは IAM サービスロールにアタッチする必要があります。
- パッチポリシーバケットにアクセスするための許可を、インラインポリシーとして IAM インスタンスプロファイルまたは IAM サービスロールに追加する必要があります。前掲のコードサンプルで示されているとおり、すべての `aws-quicksetup-patchpolicy` バケット、または組織もしくはアカウント用に作成された特定のバケットのみに対するワイルドカードアクセスを提供できます。
- IAM インスタンスプロファイルまたは IAM サービスロールは次に示すキーと値のペアを使用してタグ付けする必要があります。

  `Key: QSConfigId-`*`quick-setup-configuration-id`*`, Value:` *`quick-setup-configuration-id`*

  `quick-setup-configuration-id` は、パッチポリシー設定の作成に使用される AWS CloudFormation スタックに適用されるパラメータの値を表します。この ID を取得するには、次の手順を実行します。

  1. https://console.aws.amazon.com/cloudformation で AWS CloudFormation コンソール を開きます。
  2. パッチポリシーの作成に使用されるスタックの名前を選択します。名前は `StackSet-AWS-QuickSetup-PatchPolicy-LA-q4bkg-52cd2f06-d0f9-499e-9818-d887cEXAMPLE` などの形式です。
  3. [パラメータ] タブを選択します。

4. [パラメータ] リストの [キー] 列で、[QSConfigurationId] を探します。その行の [値] の列で、abcde のような設定 ID を探します。

   この例では、タグをインスタンスプロファイルまたはサービスロールに適用する場合、キーは QSConfigId-abcde、値は abcde です。

IAM ロールにタグを追加する方法については、「IAM ユーザーガイド」の「IAM ロールのタグ付け」と「インスタンスプロファイルのタグの管理」(AWS CLI または AWS API) を参照してください。

ケース 2: VPC エンドポイントを使用して Systems Manager に接続する

VPC エンドポイントを使用して Systems Manager に接続する場合は、S3 の VPC エンドポイントポリシーで Quick Setup パッチポリシー S3 バケットに対するアクセスを許可する必要があります。

S3 の VPC エンドポイントポリシーに対する許可の追加については、「Amazon S3 ユーザーガイド」の「バケットポリシーを使用した VPC エンドポイントからのアクセスコントロール」を参照してください。

Quick Setup S3 バケットのポリシー許可

すべての aws-quicksetup-patchpolicy バケット、または組織もしくはアカウント用に作成された特定のバケットのみに対するワイルドカードアクセスを提供できます。以下で説明する 2 つのケースのために必要な許可を付与するには、いずれかの形式を使用します。

All patch policy buckets

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AccessToAllPatchPolicyRelatedBuckets",
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::aws-quicksetup-patchpolicy-*"
    }
  ]
}
```

Specific patch policy bucket

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AccessToMyPatchPolicyRelatedBucket",
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::aws-quicksetup-patchpolicy-account-id-quick-setup-configuration-
id"[1]
    }
  ]
}
```

[1]パッチポリシー設定が作成されたら、S3 コンソールでバケットの完全な名前を確認できます。例: aws-quicksetup-patchpolicy-123456789012-abcde

パッチポリシー操作におけるランダムパッチベースライン ID

パッチポリシーのパッチ適用操作では AWS-RunPatchBaseline SSM Command ドキュメントの BaselineOverride パラメータを使用します。

パッチポリシー以外のパッチ適用に AWS-RunPatchBaseline を使用する場合、BaselineOverride を使用して、操作中に使用するパッチベースラインのうち、指定したデフォルトとは異なるリストを指定できます。このリストは baseline_overrides.json という名前のファイルに作成し、所有している Amazon S3 バケットに手動で追加します (「BaselineOverride パラメータの使用」を参照)。

ただし、パッチポリシーに基づくパッチ操作の場合、Systems Manager は自動的に S3 バケットを作成し、そこに baseline_overrides.json ファイルを追加します。その後、(Run Command ツールを使用して) Quick Setup がパッチ適用操作機能を実行するたびに、システムはパッチベースラインごとにランダム ID を生成します。この ID はパッチポリシーのパッチ適用操作ごとに異なり、この ID の示すパッチベースラインが、アカウントに保存されたりアクセスされたりすることはありません。

そのため、設定で選択したパッチベースラインの ID はパッチ適用ログに表示されません。これは、AWS のマネージドパッチベースラインと選択したカスタムパッチベースラインの両方に当ては

まります。代わりに、ログに記録されるベースライン ID は、その特定のパッチ適用操作で生成されたベースライン ID です。

さらに、ランダム ID で生成されたパッチベースラインについて、Patch Manager に詳細を表示しようとすると、システムはそのパッチベースラインが存在しないと通知します。この動作は正常であり、無視してもかまいません。

パッチポリシーの作成

パッチポリシーを作成するには、Systems Manager コンソールで次のタスクを実行します。

Quick Setup でパッチポリシーを作成するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。

   組織に対してパッチ適用をセットアップする場合は、その組織の管理アカウントにサインインしていることを確認してください。委任管理者アカウントまたはメンバーアカウントを使用してポリシーをセットアップすることはできません。
2. ナビゲーションペインで、Quick Setup を選択します。
3. [Patch Manager] (パッチマネージャー) で、[Create] (作成) を選択します。

   > **Tip**
   >
   > アカウントにすでに 1 つ以上の設定がある場合は、まず[設定] セクションで [ライブラリ] タブまたは [作成] ボタンを選択し、カードを表示します。
4. [Configuration name] (設定名) に、パッチポリシーを識別するための名前を入力します。
5. [Scanning and installation] (スキャンとインストール) セクションの [Patch operation] (パッチオペレーション) で、パッチポリシーでは、指定したターゲットを [Scan] (スキャン) するか、指定したターゲットにパッチを [Scan and install] (スキャンとインストール) するかを選択します。
6. [Scanning schedule] (スキャンのスケジュール) で、[Use recommended defaults] (推奨される既定値を使用) または [Custom scan schedule] (カスタムスキャンスケジュール) を選択します。デフォルトのスキャンスケジュールでは、毎日 UTC 午前 1:00 にターゲットをスキャンします。

   - [Custom scan schedule] (カスタムスキャンスケジュール) を選択した場合は、[Scanning frequency] (スキャンの頻度) を選択します。
   - [Daily] (毎日) を選択した場合は、ターゲットをスキャンする時刻を UTC で入力します。

- [Custom CRON Expression] (カスタム CRON 式) を選択した場合は、スケジュールを [CRON expression] (CRON 式) として入力します。Systems Manager 用の CRON 式の形式については、「リファレンス: Systems Manager の Cron 式および rate 式」を参照してください。

  また、[Wait to scan targets until first CRON interval] (最初の CRON 間隔が経過してからターゲットをスキャンする) を選択します。デフォルトでは、Patch Manager はノードがターゲットになるとすぐにスキャンします。

7. [Scan and install] (スキャンとインストール) を選択した場合は、指定したターゲットにパッチをインストールするときに使用する [Installation schedule] (インストールスケジュール) を選択します。[Use recommended defaults] (推奨される既定値を使用) を選択すると、Patch Manager では毎週日曜日の午前 2 時 (UTC) にパッチがインストールされます。

   - [Custom install schedule] (カスタムインストールスケジュール) を選択した場合は、[Installation Frequency] (インストールの頻度) を選択します。
   - [Daily] (毎日) を選択した場合は、ターゲットに更新をインストールする時刻を UTC で入力します。
   - [Custom CRON expression] (カスタム CRON 式) を選択した場合は、スケジュールを [CRON expression] (CRON 式) として入力します。Systems Manager 用の CRON 式の形式については、「リファレンス: Systems Manager の Cron 式および rate 式」を参照してください。

     また、[Wait to install updates until first CRON interval] (最初の CRON 間隔が経過してから更新をインストールする) をオフにすると、ノードがターゲットになったらすぐに更新がインストールされます。デフォルトでは、Patch Manager は最初の CRON 間隔が経過してから更新をインストールします。
   - [Reboot if needed] (必要に応じて再起動) を選択すると、パッチのインストール後にノードが再起動されます。インストール後に再起動することをお勧めしますが、その間使用できなくなることが問題になる可能性があります。

8. [Patch baseline] (パッチベースライン) セクションで、ターゲットをスキャンして更新するときに使用するパッチベースラインを選択します。

   デフォルトでは、Patch Manager は定義済みのパッチベースラインを使用します。詳細については、「事前定義されたベースライン」を参照してください。

   [Custom patch baseline] (カスタムパッチベースライン) を選択した場合は、事前定義された AWS パッチベースラインを使用したくないオペレーティングシステム用に選択したパッチベースラインを変更します。

> **Note**
>
> VPC エンドポイントを使用して Systems Manager に接続する場合は、S3 の VPC エンドポイントポリシーでこの S3 バケットへのアクセスが許可されていることを確認してください。詳細については、「パッチポリシー S3 バケットの許可」を参照してください。

> **Important**
>
> Quick Setup でパッチポリシー設定を使用している場合、カスタムパッチベースラインに加えた更新は 1 時間に 1 回 Quick Setup と同期されます。
> パッチポリシーで参照されていたカスタムパッチベースラインを削除すると、Quick Setup のそのパッチポリシーについての [Configuration details] (設定の詳細) ページにバナーが表示されます。バナーには、パッチポリシーが既に存在しないパッチベースラインを参照していること、およびそれ以降のパッチ適用オペレーションができないことが示されます。この場合は、Quick Setup の [Configurations] (設定) ページに戻り、Patch Manager 設定を選択し、[Actions] (アクション)、[Edit configuration] (設定を編集) を選択します。削除されたパッチベースライン名が強調表示されます。影響を受けるオペレーティングシステム用の新しいパッチベースラインを選択する必要があります。

9. (オプション) [Patching log storage] (ログストレージにパッチ適用) セクションで、[Write output to S3 bucket] (出力を S3 バケットに書き込む) を選択し、パッチ適用オペレーションログを Amazon S3 バケットに保存します。

> **Note**
>
> 組織のパッチポリシーを設定する場合、組織の管理アカウントには、少なくともこのバケットに対する読み取り専用アクセス許可が必要です。ポリシーに含まれるすべての組織ユニットには、バケットへの書き込みアクセス権が必要です。他のアカウントへのアクセス権をバケットに付与する方法については、「Amazon Simple Storage Service ユーザーガイド」の「例 2: バケット所有者がクロスアカウントのバケットのアクセス許可を付与する」を参照してください。

10. [S3 を参照] をクリックして、パッチログ出力を保存するバケットを選択します。管理アカウントには、このバケットへの読み取りアクセス権が必要です。[Targets] (ターゲット) セクション

で設定された管理アカウント以外のアカウントとターゲットはすべて、ログ記録用に指定された S3 バケットへの書き込みアクセス権を持っている必要があります。

11. [Targets] (ターゲット) セクションで、次のいずれかを選択して、このパッチポリシーオペレーションのアカウントとリージョンを指定します。

> **Note**
>
> 1 つのアカウントで作業している場合、組織や組織単位 (OU) を使用するオプションは利用できません。この設定をアカウント内のすべての AWS リージョン に適用するか、選択したリージョンのみに適用するかを選択できます。
> 以前にアカウントにホームリージョンを指定していて、新しい Quick Setup コンソールエクスペリエンスにまだオンボードしていない場合、そのリージョンをターゲット設定から除外することはできません。

- [Entire organization] (組織全体) – 組織内のすべてのアカウントとリージョン。
- [Custom] (カスタム) – 指定した OU とリージョンのみ。
  - [Target OUs] (ターゲット OU) セクションで、パッチポリシーをセットアップする OU を選択します。
  - [Target Regions] (ターゲットリージョン) セクションで、パッチポリシーを適用するリージョンを選択します。
- [Current account] (現在のアカウント) – 現在サインインしているアカウント内の指定したリージョンのみがターゲットになります。次のいずれかを選択します。
  - [Current Region] (現在のリージョン) – コンソールで選択したリージョン内のマネージドノードのみがターゲットになります。
  - [Choose Regions] (リージョンを選択) – パッチポリシーを適用する個々のリージョンを選択します。

12. [Choose how you want to target instances] (インスタンスをどのようにターゲットにするかを選択) で、次のいずれかを選択して、パッチを適用するノードを指定します。

- [All managed nodes] (すべての管理対象ノード) – 選択した OU とリージョンのすべてのマネージドノード。
- [Specify the resource group] (リソースグループを指定) – 関連するリソースをターゲットにするリソースグループの名前をリストから選択します。

> **Note**
>
> 現在、リソースグループの選択は、単一アカウント構成でのみサポートされています。複数のアカウントのリソースにパッチを適用するには、別のターゲットオプションを選択します。

- [Specify a node tag] (ノードタグを指定) – 指定したキーと値のペアでタグ付けされたノードのみに、ターゲットにしたすべてのアカウントとリージョンでパッチが適用されます。
- [Manual] (手動) – 指定されたすべてのアカウントとリージョンのマネージドノードをリストから手動で選択します。

> **Note**
>
> 現在、このオプションは Amazon EC2 インスタンスのみをサポートしています。パッチポリシー設定では、最大 25 個のインスタンスを手動で追加できます。

13. [Rate control] (レート制御) セクションで、以下を行います。

    - [Concurrency] (同時実行数) に、パッチポリシーを同時に実行するノードの数または割合を入力します。
    - [Error threshold] (エラーのしきい値) を入力します。エラーが発生したノードの数または割合がこの値を超えると、パッチポリシーはエラーになります。

14. (オプション) [インスタンスにアタッチされている既存のインスタンスプロファイルに必要な IAM ポリシーを追加する] チェックボックスを選択します。

    この選択により、この Quick Setup 設定で作成された IAM ポリシーを、既にインスタンスプロファイルがアタッチされているノード (EC2 インスタンス) またはサービスロールがアタッチされているノード (ハイブリッドアクティベーションノード) に適用します。このオプションは、マネージドノードに既にインスタンスプロファイルまたはサービスロールがアタッチされているが、Systems Manager の操作に必要なすべての許可が含まれていない場合にこの選択をお勧めします。

    ここで選択した内容は、このパッチポリシー設定が適用されるアカウントとリージョンに後で作成されるマネージドノードに適用されます。

> **Important**
>
> このチェックボックスをオフにして、このパッチポリシーを使用してマネージドノードにパッチを Quick Setup に適用する場合は、次を実行する必要があります。
> パッチポリシー用に作成された S3 バケットにアクセスするための許可を IAM インスタンスプロファイルまたは IAM サービスロールに追加する
> IAM インスタンスプロファイルまたは IAM サービスロールに特定の key-value ペアをタグ付けします。
> 詳細については、「ケース 1: マネージドノードで、Quick Setup によって提供されるインスタンスプロファイルまたはサービスロールではなく、独自のインスタンスプロファイルまたはサービスロールを使用する」を参照してください。

15. [作成] を選択します。

    パッチポリシーの作成後にパッチ適用ステータスを確認するには、Quick Setup ページから設定にアクセスします。

Quick Setup を使用して DevOps Guru をセットアップする

Quick Setup を使用すると、DevOps Guru オプションをすばやく設定できます。Amazon DevOps Guru は、アプリケーションの運用パフォーマンスと可用性を簡単に向上させる、Machine Learning (ML) 対応のサービスです。DevOps Guru は、通常の運用パターンとは異なる動作を検出し、顧客に影響を及ぼす前に運用上の問題を特定できるようにします。DevOps Guru は、運用データをAWS アプリケーションから取り込み、運用データの問題を視覚化するための単一のダッシュボードを提供します。DevOps Guru の使用を開始すると、手動セットアップや機械学習の専門知識が不要で、アプリケーションの可用性と信頼性を向上させることができます。

Configuring DevOps Guru with Quick Setup は以下の AWS リージョン があります。

- 米国東部 (バージニア北部)
- 米国東部 (オハイオ)
- 米国西部 (オレゴン)
- 欧州 (フランクフルト)
- 欧州 (アイルランド)
- 欧州 (ストックホルム)
- アジアパシフィック (シンガポール)

- アジアパシフィック (シドニー)
- アジアパシフィック (東京)

料金情報については、「Amazon DevOps Guru の料金」を参照してください。

DevOps Guru を設定するには、AWS Systems Manager Quick Setup コンソールで次のタスクを実行します。

Quick Setup で DevOps Guru を設定するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Quick Setup] を選択します。
3. [DevOps Guru] カードで [作成] を選択します。

   > **Tip**
   >
   > アカウントにすでに 1 つ以上の設定がある場合は、まず次の設定を選択してください。[設定] セクションで [ライブラリ] タブまたは [作成] ボタンを選択し、カードを表示します。

4. 設定オプションセクションで、AWS 分析するリソースタイプと通知プリファレンスを選択します。

   [組織内のすべてのアカウントの AWS リソースをすべて分析] オプションを選択しない場合、AWS リソースを選択すれば、後で DevOps Guru コンソールで分析できます。DevOps Guru は、さまざまな AWS リソースタイプ (Amazon Simple Storage Service (Amazon S3) バケット、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスなど) を分析します。これは、2 つの料金グループに分類されます。アクティブな各リソースについては、分析された AWS リソース時間に対して料金を支払います。リソースは、メトリック、イベント、または口グエントリが 1 時間以内に生成される場合にのみアクティブになります。特定の AWS リソースタイプに対して請求される料金は、価格グループによって異なります。

   [Enable SNS notifications (SNS 通知を有効にする)] オプションを選択した場合、Amazon Simple Notification Service (Amazon SNS) トピックは、設定でターゲットとする組織ユニット (OU) の各 AWS アカウント に作成されます。DevOps Guru トピックを使用して、新しいインサイトの作成など、重要な DevOps Guru イベントを通知します。このオプションを有効にしない場合は、後で DevOps Guru コンソールでトピックを追加できます。

AWS Systems Manager OpsItemsオプションを選択すると、関連する Amazon EventBridge イベントと Amazon CloudWatch アラームに対して運用作業項目（OpsItems）が作成されます。

5. [Schedule (スケジュール)] セクションで、設定とは異なるリソースに加えられた変更を Quick Setup で修正する頻度を選択します。[Default (デフォルト)] オプションは 1 回実行されます。設定と異なるリソースに加えられた変更を Quick Setup で修正しない場合は、[Custom (カスタム)] で [Disabled (無効にする)] を選択します。
6. ターゲットセクションで、DevOps Guru に分析を許可する対象を一部の組織単位 (OU) のリソース、または現在ログインしているアカウントから選択します。

   [Custom] (カスタム) を選択した場合は、ステップ 8 に進みます。

   [現在のアカウント] を選択した場合は、ステップ 9 に進みます。
7. [Target OUs (ターゲット OU)] セクションと [Target Regions (ターゲットリージョン)] セクションで、DevOps Guru を使用する OU とリージョンのチェックボックスを選択します。
8. 現在のアカウントで DevOps Guru を使用するリージョンを選択します。
9. [Create] (作成) を選択します。

Quick Setup を使用して Distributor パッケージをデプロイする

Distributor は AWS Systems Manager のツールです。Distributor パッケージは、インストール可能なソフトウェアやアセットのコレクションで、単一のエンティティとしてデプロイできます。Quick Setup では、Distributor パッケージを AWS アカウント と AWS リージョン、または AWS Organizations の組織全体でデプロイできます。現在、Quick Setup では、EC2Launch v2 エージェント、Amazon Elastic File System (Amazon EFS) ユーティリティパッケージと Amazon CloudWatch エージェントのみをデプロイできます。Distributor の詳細については、「AWS Systems Manager Distributor」を参照してください。

Distributor パッケージをデプロイするには、AWS Systems Manager Quick Setup コンソール]で次のタスクを実行します。

Quick Setup で Distributor をデプロイするには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Quick Setup] を選択します。
3. [ディストリビューター] カードで [作成] を選択します。

> **Tip**
>
> アカウントにすでに 1 つ以上の設定がある場合は、まず[設定] セクションで [ライブラリ] タブまたは [作成] ボタンを選択し、カードを表示します。

4. [Configuration options (設定オプション)] セクションで、デプロイするパッケージを選択します。
5. [Targets (ターゲット)] セクションで、デプロイ先のパッケージを組織全体、組織単位 (OU) の一部、または現在ログインしているアカウントから選択します。

   [組織全体] を選択した場合は、ステップ 8 に進みます。

   [カスタム] を選択した場合は、ステップ 7 に進みます。
6. [ターゲット OU] セクションで、 パッケージのデプロイ先 OU とリージョンのチェックボックスを選択します。
7. [Create] を選択します。

Quick Setup を使用してスケジュールに従って EC2 インスタンスを自動的に停止および起動する

AWS Systems Manager のツールである Quick Setup を使用すると、Resource Scheduler を設定して Amazon Elastic Compute Cloud (Amazon EC2) インスタンスの起動と停止を自動化できます。

この Quick Setup 設定は、指定したスケジュールに従ってインスタンスを起動および停止することで、運用コストを削減するのに役立ちます。このツールにより、必要のないときにインスタンスを実行することで不必要なコストが発生するのを防ぐことができます。

例えば、1 日 10 時間、週 5 日しか使用されていない場合でも、現状、インスタンスを常時稼働させているかもしれません。そうではなく、営業時間後に毎日インスタンスを停止するようにスケジュールできます。その結果、実行時間が 168 時間から 50 時間に短縮されるため、これらのインスタンスでは 70% の節約になります。Quick Setup の使用にコストはかかりません。ただし、セットアップしたリソースと使用制限に基づいて費用が発生する可能性があり、設定のセットアップに使用したサービスには料金はかかりません。

Resource Scheduler を使うことで、指定したスケジュールに従って、複数の AWS リージョンと AWS アカウントにまたがってインスタンスを自動的に停止および起動することもできます。Quick Setup 設定は、指定したタグのキーと値を使用して Amazon EC2 インスタンスをターゲットにします。設定で指定した値と一致するタグを持つインスタンスのみが Resource Scheduler によって停止

または起動されます。インスタンスにアタッチされた Amazon EBS ボリュームが暗号化されている場合は、Resource Scheduler がインスタンスを起動するために AWS KMS キーの必要なアクセス許可を IAM ロールに追加する必要があります。

設定あたりの最大インスタンス数

個々の設定でサポートされるのは、リージョン当たり 5,000 インスタンスまでのスケジュールです。特定のリージョンで 5,000 を超えるインスタンスをスケジュールする必要がある場合は、複数の設定を作成する必要があります。インスタンスに適切にタグを付けて、各設定で管理するインスタンスを 5,000 以下にします。Resource Scheduler の Quick Setup 設定を複数作成する場合、異なるタグキー値を指定する必要があります。例えば、ある設定ではタグキー `Environment` を `Production` の値で使用でき、別の設定では `Environment` と `Development` を使用できます。

スケジュール設定の動作

以下のポイントでは、スケジュール設定の特定の動作について説明します。

- Resource Scheduler では、タグ付けされたインスタンスが起動されるのはは `Stopped` 状態にある場合のみです。同様に、インスタンスが停止されるのは、`running` 状態にある場合のみです。Resource Scheduler はイベント駆動型モデルで動作し、指定した時刻にのみインスタンスを起動または停止します。例えば、午前 9 時にインスタンスを起動するスケジュールを作成します。Resource Scheduler は、指定したタグに関連付けられた、午前 9 時に `Stopped` 状態にあるすべてのインスタンスを起動します。後でインスタンスを手動で停止した場合、Resource Scheduler はインスタンスを再起動せず、`Running` 状態を維持します。同様に、スケジュールに従ってインスタンスが停止された後にインスタンスを手動で起動した場合、Resource Scheduler はインスタンスを再度停止しません。
- 起動時刻が停止時刻より 24 時間遅いスケジュールを作成した場合、Resource Scheduler はインスタンスが翌日にまたがって実行されるものとみなします。例えば、インスタンスを午後 9 時に起動し、午前 7 時に停止するスケジュールを作成したとします。Resource Scheduler は、指定したタグに関連付けられた、午後 9 時に `Stopped` 状態にあるすべてのインスタンスを起動し、翌日の午前 7 時に停止します。翌日にまたがったスケジュールの場合、起動時刻はスケジュールで選択した日に適用されます。一方、停止時刻はスケジュールの翌日に適用されます。
- スケジュール設定を作成すると、現在のインスタンスの状態が、スケジュールの要件に合わせて変更される場合があります。

  例えば、今日が水曜日で、マネージドインスタンスが火曜日と木曜日のみ午前 9 時に開始して午後 5 時に停止するよう、スケジュールを指定するとします。現在は、インスタンスを実行する時刻に該当しないため、設定の作成後にインスタンスは停止します。インスタンスは、次の設定時刻である木曜日の午前 9 時になるまで実行されません。

インスタンスが現在 Stopped の状態で、現在の時刻に実行されるスケジュールを指定すると、Resource Scheduler は設定の作成後にインスタンスを起動します。

設定を削除すると、以前に定義されたスケジュールに従ったインスタンスの停止と起動は行われなくなります。まれに、API オペレーションが失敗してインスタンスが正常に停止または起動しないことがあります。

Amazon EC2 インスタンスのスケジュールをセットアップするには、AWS Systems Manager Quick Setup コンソールで次のタスクを実行します。

Quick Setup でインスタンスのスケジュールを設定するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Quick Setup] を選択します。
3. [Resource Scheduler] カードで [作成] をクリックします。

> **Tip**
>
> アカウントにすでに 1 つ以上の設定がある場合は、まず[設定] セクションで [ライブラリ] タブまたは [作成] ボタンを選択し、カードを表示します。

4. [Instance tag] (インスタンスタグ) セクションで、スケジュールに関連付けるインスタンスに適用されるタグのキーと値を指定します。
5. [Schedule options] (スケジュールオプション) セクションで、インスタンスを起動および停止するタイムゾーン、曜日、時刻を指定します。
6. [Targets] (ターゲット) セクションで、スケジュール設定の対象を、組織単位 (OU) の [Custom] (カスタム) グループにするか、ログインしている [Current account] (現在のアカウント) にするかを次のように選択します。

   - [Custom] (カスタム) – [Target OUs] (ターゲット OU) セクションで、スケジュールをセットアップする OU を選択します。[Target Regions] (ターゲットリージョン) セクションで、スケジュールをセットアップするリージョンを選択します。
   - 現在のアカウント – [Current Region (現在のリージョン)] または [Choose Regions (リージョンの選択)] を選択します。[Choose Regions] (リージョンを選択) を選択した場合は、スケジュールをセットアップする [Target Regions] (ターゲットリージョン) を選択します。

7. [Summary] (概要) セクションのスケジュール情報を確認します。
8. [Create] (作成) を選択します。

Quick Setup を使用して AWS Resource Explorer を設定する

AWS Systems Manager のツールである Quick Setup を使用すると、AWS アカウントまたは AWS 組織全体のリソースを検索して検出するように AWS Resource Explorer をすばやく設定できます。名前、タグ、ID などのメタデータを使用してリソースを検索できます。AWS Resource Explorer は、インデックスを使用して、検索クエリに迅速に応答します。Resource Explorer は、さまざまなデータソースを使用してインデックスを作成および維持し、AWS アカウント 内のリソースに関する情報を収集します。

Quick Setup for Resource Explorer はインデックス設定プロセスを自動化します。AWS Resource Explorer の詳細については、「AWS Resource Explorer ユーザーガイド」の「AWS Resource Explorer とは」を参照してください。

Quick Setup の際に、Resource Explorer は次の処理を行います。

- AWS アカウント 内のすべての AWS リージョン にインデックスを作成します。
- 指定したリージョンのインデックスをアカウントのアグリゲーターインデックスとして更新します。
- アグリゲーターインデックスのリージョンにデフォルトビューを作成します。このビューにはフィルターがないため、インデックスで見つかったすべてのリソースを検索結果として返します。

最小限必要なアクセス権限

以下の手順のステップを実行するには、次のアクセス許可が必要です。

- アクション：`resource-explorer-2:*` — リソース：特定のリソースなし (*)
- アクション：`iam:CreateServiceLinkedRole` — リソース：特定のリソースなし (*)

Resource Explorer を設定するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Quick Setup] を選択します。
3. [Resource Explorer] カードで [作成] をクリックします。

4. [アグリゲーターインデックスリージョン] セクションで、アグリゲーターインデックスを含めたいリージョンを選択します。ユーザーの地理的位置に適したリージョンを選択する必要があります。
5. (オプション) [上で選択したリージョン以外のリージョンの既存のアグリゲーターインデックスを置き換える] チェックボックスを選択します。
6. [ターゲット] セクションで、検出したいリソースを含むターゲット組織または特定の組織単位 (OU) を選択します。
7. [リージョン] セクションで、設定に含めるリージョンを選択します。
8. 設定の要約を確認し、[作成] を選択します。

[Resource Explorer] ページでは、設定ステータスをモニタリングできます。

Quick Setup の結果のトラブルシューティング

AWS Systems Manager のツールである Quick Setup を使用したトラブルシューティングでは、以下の情報を使用します。このトピックには、Quick Setup の問題のタイプに基づいて問題を解決するための特定のタスクが含まれています。

問題: デプロイの失敗

CloudFormation スタックセットの作成が失敗した場合、デプロイは失敗します。デプロイの失敗を調査するには、以下のステップを使用します。

1. AWS CloudFormation コンソールに移動します。
2. Quick Setup 設定で作成されたスタックを選択します。[Stack name] (スタックの名前) には、`QuickSetup` と、それに続き選択した設定のタイプ (例えば `SSMHostMgmt`) が含まれます。

   > **Note**
   >
   > CloudFormation は、失敗したスタックのデプロイを削除することがあります。スタックが [Stacks] (スタック) テーブルに表示されない場合は、フィルターリストから [Deleted] (削除済み) を選択します。

3. [Status] (ステータス) と [Status reason] (ステータス理由) を表示します。スタックのステータスの詳細については、「AWS CloudFormationユーザーガイド」の「スタックステータスコード」を参照してください。

4. 失敗したステップを正確に把握するには、[Events] (イベント) タブを開き、各イベントの [Status] (ステータス) を確認します。
5. 「AWS CloudFormationユーザーガイド」の「トラブルシューティング」を確認してください。
6. CloudFormation のトラブルシューティングに関するステップによりデプロイの失敗を解決できない場合は、設定を削除した上で再設定を行います。

問題: 失敗した関連付け

セットアップ中にいずれかの関連付けが失敗した場合、[Configuration details] (設定の詳細) ページの [Configuration details] (設定の詳細) テーブルには、[Configuration status] (設定ステータス) として [Failed] (失敗) が表示されます。失敗した関連付けのトラブルシューティングを行うには、次のステップを実行します。

1. [Configuration details] (設定の詳細) テーブルで、失敗した設定を選択し、[View Details] (詳細を表示) をクリックします。
2. [Association name] (関連付け名) をコピーします。
3. State Manager に移動し、その関連付け名を検索フィールドに貼り付けます。
4. 関連付けを選択した上で、[Execution history] (実行履歴) タブを開きます。
5. [Execution ID (実行 ID)] で、失敗した関連付けの実行を選択します。
6. [Association execution targets] (関連付け実行ターゲット) ページには、関連付けが実行されたすべてのノードが一覧表示されます。実行に失敗した実行の [Output (出力)] ボタンを選択します。
7. [Output (出力)] ページで、[Step - Output (ステップ - 出力)] を選択して、コマンド実行のステップのエラーメッセージを表示します。各ステップで異なるエラーメッセージを表示できます。すべてのステップのエラーメッセージを確認して、問題のトラブルシューティングに役立ててください。

ステップ出力を表示しても問題を解決しない場合は、関連付けを再作成できます。関連付けを再作成するには、まず、State Manager で失敗した関連付けを削除します。関連付けを削除したら、設定を編集して削除したオプションを指定し直し、その後、[Update] (更新) をクリックします。

> **Note**
>
> [Organization] (組織) に対して [Failed] (失敗) した関連付けを調査するには、先述のとおり、失敗した関連付けを持つアカウントにサインインし、以下の手順を行う必要があります。管理アカウントからの結果を表示する場合、[関連付け ID] はターゲットアカウントへのハイパーリンクではありません。

問題: ドリフトステータス

設定の詳細ページを開くと、各デプロイのドリフトステータスを表示できます。設定のドリフトは、Quick Setup で行った選択と競合するサービスまたは機能に対し、ユーザーが変更を加えるたびに発生します。初期設定後に関連付けが変更された場合、ドリフトした項目の数を示す警告アイコンがテーブルに表示されます。アイコンの上にカーソルを置くと、ドリフトの原因を見ることができます。

State Manager で関連付けが削除されると、関連するデプロイにはドリフトに関する警告が表示されます。これを修正するには、設定を編集し、関連付けとともに削除されたオプションを選択します。[Update] (更新) をクリックし、デプロイが完了するのを待ちます。

AWS Systems Manager アプリケーションツール

アプリケーションツールは、AWS で実行されているアプリケーションの管理に役立つ一連の機能です。

トピック

- AWS AppConfig
- AWS Systems Manager Application Manager
- AWS Systems Manager Parameter Store

AWS AppConfig

AWS AppConfig に関する情報は、別のガイドに移動しました。詳細については次を参照してください:

- AWS AppConfig ユーザーガイド

- AWS AppConfig API リファレンス

AWS Systems Manager Application Manager

AWS Systems Manager のツールである Application Manager は、DevOps エンジニアがアプリケーションとクラスターのコンテキストで AWS リソースに関する問題を調査および修復するのに役立ちます。Application Manager は、複数の AWS のサービスと Systems Manager のツールのオペレーション情報を単一の AWS Management Consoleに集約します。

Application Manager では、アプリケーションはユニットとして動作する AWS リソースの論理グループです。この論理グループは、アプリケーションのさまざまなバージョン、オペレーターの所有権の境界、またはデベロッパー環境などを表すことができます。Application Manager コンテナクラスターのサポートには、Amazon Elastic Kubernetes Service (Amazon EKS) クラスターと Amazon Elastic Container Service (Amazon ECS) クラスターの両方が含まれます。

Application Manager を初めて開くと、「What Application Manager can do for you」ページが表示されます。[開始方法] を選択すると、Application Manager は、他の AWS のサービス または Systems Manager ツールで作成されたリソースに関するメタデータを自動的にインポートします。Application Manager は、これらのリソースを事前定義されたカテゴリ別にグループ化されたリストに表示します。

アプリケーションの場合、リストには次のものが含まれます。

- AWS CloudFormation スタック
- カスタムアプリケーション
- AWS Launch Wizard アプリケーション
- AppRegistry アプリケーション
- AWS SAP Enterprise ワークロードアプリケーション
- Amazon ECS クラスター
- Amazon EKS クラスター

AWS のサービスおよび Systems Manager のツールをセットアップして設定すると、Application Manager はリソースに関する次の種類の情報を表示します。

- アプリケーション内の Amazon Elastic Compute Cloud (Amazon EC2) インスタンスの現在の状態、ステータス、Amazon EC2 Auto Scaling の正常性に関する情報

- Amazon CloudWatch によって提供されるアラーム
- AWS Config および State Manager (Systems Manager のコンポーネント) によってもたらされるコンプライアンス情報
- Amazon EKS によってもたらされる Kubernetes クラスター情報
- AWS CloudTrail および Amazon CloudWatch Logs によってもたらされるログデータ
- Systems Manager OpsCenterによってもたらされる OpsItems
- リソースをホストする AWS のサービスによって提供されるリソースの詳細。
- Amazon ECS によってもたらされるコンテナクラスター情報。

コンポーネントまたはリソースに関する問題の修復を支援するために、Application Manager はアプリケーションに関連付けられるランブックも提供します。Application Manager の使用を開始するには、Systems Manager コンソールを開きます。ナビゲーションペインで、[Application Manager] を選択します。

Application Manager を使用することの利点は何ですか。

Application Manager を使用すると、DevOps エンジニアが AWS リソースに関する問題を検出して調査する時間を短縮できます。これを行うため、Application Managerでは 1 つのコンソールにアプリケーションのコンテキストで多くのタイプのオペレーション情報が表示されます。また、Application Manager により AWS リソースで一般的な修復タスクを実行するランブックが提供されることで、問題の修復にかかる時間を短縮できます。

Application Manager の特徴は何ですか?

Application Manager には、以下の特徴があります。

- AWS リソースを自動的にインポート

  初期セットアップ時に、CloudFormation スタック、AWS Resource Groups、Launch Wizard デプロイ、AppRegistry アプリケーション、Amazon ECS および Amazon EKS クラスターに基づくリソースを、Application Manager が AWS アカウント に自動的にインポートして表示するように選択できます。このシステムにより、これらのリソースは、定義済みのアプリケーションまたはクラスターカテゴリに表示されます。その後、これらのタイプの新しいリソースが AWS アカウントに追加されるたびに、Application Manager では、事前定義されたアプリケーションとクラスターカテゴリに新しいリソースが自動的に表示されます。
- CloudFormation スタックとテンプレートの作成および編集

Application Manager は、CloudFormation と統合することで、アプリケーションのリソースのプロビジョニングと管理を支援します。AWS CloudFormation テンプレートとスタックは、Application Manager で作成、編集、削除できます。Application Manager には、テンプレートのクローン、作成、および格納が可能なテンプレートライブラリも含まれています。Application Manager と CloudFormation には、スタックの現在のステータスに関する同じ情報が表示されます。テンプレートとテンプレートの更新は、スタックをプロビジョニングするまで Systems Manager に格納されます。このとき、変更内容は CloudFormation にも表示されます。

- アプリケーションの観点からインスタンスに関する情報を表示する

  Application Manager は Amazon Elastic Compute Cloud (Amazon EC2) と統合しており、アプリケーションの観点からインスタンスに関する情報を表示することができます。 Application Manager は、選択したアプリケーションのインスタンスの状態、ステータス、および Amazon EC2 Auto Scaling の正常性を、グラフィカルな形式で表示します。[Instances] (インスタンス) タブには、アプリケーション内の各インスタンスに関する以下の情報を示すための表も含まれています。

  - インスタンスの状態 (保留中、停止中、実行中、停止済み)
  - SSM Agent の ping ステータス
  - インスタンス上で最後に処理された、Systems Manager Automation ランブックのステータスと名前
  - 状態ごとの Amazon CloudWatch Logs アラームの数。
    - `ALARM` – メトリクスまたは式が、定義されているしきい値を超えています。
    - `OK` – メトリクスや式は、定義されているしきい値の範囲内です。
    - `INSUFFICIENT_DATA` – アラームが開始直後であるか、メトリクスが利用できないか、メトリクス用のデータが不足しているため、アラームの状態を判定できません。
  - 親および個別の Auto Scaling グループに関する正常性
- アプリケーションまたはクラスターのオペレーションメトリクスおよびアラームの表示

  Application Manager は Amazon CloudWatch と統合され、アプリケーションまたはクラスターのリアルタイムオペレーションメトリクスとアラームを提供します。アプリケーションツリーにドリルダウンして、各コンポーネントレベルのアラームを表示したり、個々のクラスターのアラームを表示したりできます。
- アプリケーションのログデータの表示

  Application Manager は Amazon CloudWatch Logs と統合され、Systems Manager を離れることなく、アプリケーションのコンテキストでログデータが提供されます。

- アプリケーションまたはクラスター用の OpsItems の表示と管理

  Application Manager は、AWS Systems Manager OpsCenter と統合して、アプリケーションとクラスターの運用作業項目 (OpsItems) のリストを提供します。リストには、自動的に生成され、手動で作成された OpsItems が反映されます。OpsItem を作成したリソースの詳細のほか、OpsItem のステータス、ソース、重要度を表示できます。
- アプリケーションまたはクラスターのリソースのコンプライアンスデータの表示

  Application Manager は、AWS Config と統合して、指定したルールに従い、AWS リソースに関するコンプライアンスと履歴の詳細を提供します。Application Manager もまた、AWS Systems Manager State Manager と統合して、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスで維持する状態に関するコンプライアンス情報を提供します。
- Amazon ECS および Amazon EKS クラスターインフラストラクチャ情報の表示

  Application Manager は Amazon ECS および Amazon EKS と統合して、クラスターのインフラストラクチャの正常性に関する情報と、クラスター内のコンピューティング、ネットワーキング、およびストレージリソースのコンポーネントランタイムビューを提供します。

  ただし、Application Manager では、Amazon EKS ポッドまたはコンテナに関するオペレーション情報を管理または表示することはできません。管理および表示できるのは、Amazon EKS リソースをホストしているインフラストラクチャに関するオペレーション情報のみです。
- アプリケーションのリソースコストの詳細の表示

  Application Manager は、[Cost] (コスト) ウィジェットによって、AWS Billing and Cost Management の機能である AWS Cost Explorer と統合されています。請求およびコストマネジメントコンソールで Cost Explorer を有効にした後、Application Manager の [Cost] (コスト) ウィジェットに、特定の非コンテナアプリケーションまたはアプリケーションコンポーネントのコストデータが表示されます。ウィジェットでフィルターを使用して、棒グラフまたは折れ線グラフで、異なる期間、粒度、およびコストタイプに基づいてコストデータを表示できます。
- リソースの詳細情報を 1 つのコンソールで表示

  Application Manager に表示されているリソース名を選択すると、Systems Manager を離れることなくそのリソースに関するコンテキスト情報とオペレーション情報を表示できます。
- アプリケーションのリソース更新の自動受信

  サービスコンソールでリソースに変更を加え、そのリソースが Application Manager のアプリケーションの一部である場合、Systems Manager はそれらの変更を自動的に表示します。たとえば、AWS CloudFormation コンソールでスタックを更新し、そのスタックが Application Manager

アプリケーションの一部である場合、スタックの更新は自動的に Application Manager に反映されます。

- Launch Wizard アプリケーションの自動検出

  Application Manager は AWS Launch Wizard と統合されています。Launch Wizard を使用してアプリケーションのリソースを配置した場合、Application Manager では「Launch Wizard」セクションにリソースを自動的にインポートして表示できます。

- CloudWatch Application Insights を使用した Application Manager でのアプリケーションリソースの監視

  Application Manager は、Amazon CloudWatch Application Insights と統合できます。Application Insights は、アプリケーションリソースとテクノロジースタック全体の主要なメトリクス、ログ、アラームを識別して設定します。また、メトリクスとログを継続的にモニタリングし、異常やエラーを検出して相互に関連付けます。エラーや異常が検出されると、Application Insights は CloudWatch Events を生成します。これを使用すると、通知を設定したり、アクションを実行したりできます。Application Insights は、Application Manager の [Overview (概要)] と [Monitoring (モニタリング)] タブで有効にして表示できます。Application Insights の詳細については、Amazon CloudWatch ユーザーガイドで「Amazon CloudWatch Application Insights とは」を参照してください。

- ランブックに関する問題を修復

  Application Manager には、AWS リソースの一般的な問題を修正するための事前定義された Systems Manager ランブックが含まれています。Application Manager を終了しなくても、アプリケーション内で対象となるすべてのリソースに対してランブックを実行できます。

Application Manager の使用料金はかかりますか?

Application Manager は追加料金なしでご利用いただけます。

Application Manager のリソースクォータについて説明します。

すべての Systems Manager ツールのクォータは、「Amazon Web Services 全般のリファレンス」の「Systems Manager Service Quotas」で確認できます。特に明記されていない限り、クォータはリージョンごとに存在します。

トピック

- 関連サービスのセットアップ

- Systems Manager Application Manager のアクセス許可を設定する
- Application Manager へのアプリケーションとコンテナクラスターの追加
- アプリケーションの使用

関連サービスのセットアップ

AWS Systems Manager のツールである Application Manager は、他の AWS のサービスおよび Systems Manager ツールのリソースと情報を表示します。Application Manager に表示されるオペレーション情報の量を最大化するには、Application Manager を使用する前に、これら他のサービスやツールをセットアップおよび設定することが推奨されます。

トピック

- リソースをインポートするためのタスクのセットアップ
- リソースに関するオペレーション情報を表示するタスクのセットアップ

リソースをインポートするためのタスクのセットアップ

次のセットアップタスクは、Application Manager で AWS リソースを表示するのに役立ちます。これらのタスクがそれぞれ完了すると、Systems Manager はリソースを自動的に Application Manager にインポートできます。リソースのインポート後、Application Manager でアプリケーションを作成し、インポートしたリソースをそのアプリケーションに移動できます。これは、アプリケーションのコンテキストでオペレーション情報を表示するのに役立ちます。

(オプション) タグを使用して AWS リソースを整理する

AWS のリソースにメタデータをタグ形式で割り当てることができます。各タグは、ユーザー定義のキーと値で構成されるラベルです。タグは、リソースの管理、識別、整理、検索、フィルタリングに役立ちます。タグを作成することで、リソースを目的、所有者、環境その他の基準別に分類できます。

(オプション) AWS を使用して AWS Resource Groups リソースを整理する

AWS リソースを整理するには、リソースグループを使用します。リソースグループを使用すると、リソース上の多くのタスクを一度に管理、モニタリング、および自動化しやすくなります。

Application Manager は、すべてのリソースグループを自動的にインポートし、カスタムアプリケーションカテゴリに表示します。

(オプション) AWS を使用して AWS CloudFormation リソースをセットアップおよびデプロイする

AWS CloudFormation は、計画に従い、繰り返し AWS インフラストラクチャデプロイを作成し、プロビジョニングします。Amazon EC2、Amazon Elastic Block Store (Amazon EBS)、Amazon Simple Notification Service (Amazon SNS)、Elastic Load Balancing、AWS Auto Scaling などの AWS のサービスの利用に役立ちます。CloudFormation を使用すると、基盤となる AWS インフラストラクチャを作成したり設定することなく、安定性と拡張性に優れ、費用効率の高いアプリケーションを構築できます。

Application Manager は、すべての AWS CloudFormation リソースを自動的にインポートし、AWS CloudFormation スタック カテゴリに表示します。Application Manager で CloudFormation のスタックとテンプレートを作成できます。スタックとテンプレートの変更は、Application Manager と CloudFormation 間で自動的に同期されます。Application Manager でアプリケーションを作成し、スタックをそこに移動することもできます。これは、アプリケーションのコンテキストで、スタック内のリソースのオペレーション情報を表示するのに役立ちます。料金については、「AWS CloudFormation の料金」を参照してください。

(オプション) AWS Launch Wizard を使用してアプリケーションをセットアップおよびデプロイする

Launch Wizard では、個々の AWS リソースを手動で識別およびプロビジョニングすることなく、サードパーティーアプリケーションの AWS リソースのサイジング、設定、デプロイを行うプロセスを実行します。

Application Manager では、Launch Wizard のすべてのリソースが自動的にインポートされ、Launch Wizard カテゴリに一覧表示されます。AWS Launch Wizard の詳細については、「AWS Launch Wizard for SQL Server の開始方法」を参照してください。Launch Wizard は追加料金なしでご利用いただけます。ソリューションを実行するためプロビジョニングした AWS リソースに対してのみ料金が発生します。

(オプション) Amazon ECS および Amazon EKS を使用した、コンテナ化されたアプリケーションの設定とデプロイ

Amazon Elastic Container Service (Amazon ECS) は、クラスターでコンテナの実行、停止、管理を簡単に行うことのできる、高度にスケーラブルで高速なコンテナ管理サービスです。コンテナは、個々のタスクやサービス内のタスクを実行するために使用するタスク定義で定義されます。

Amazon EKS は、独自の Kubernetes コントロールプレーンまたはノードをインストール、操作、維持することなく、AWS で Kubernetes を簡単に実行できるようにするマネージド型サービスです。Kubernetes は、コンテナ化されたアプリケーションのデプロイ、スケーリング、および管理を自動化するためのオープンソースシステムです。

Application Manager では、Amazon ECS および Amazon EKS インフラストラクチャリソースがすべて自動的にインポートされ、[コンテナクラスター] タブに一覧表示されます。ただし、Application Manager では、Amazon EKS ポッドまたはコンテナに関するオペレーション情報を管理または表示することはできません。管理および表示できるのは、Amazon EKS リソースをホストしているインフラストラクチャに関するオペレーション情報のみです。料金情報については、「Amazon ECS の料金」および「Amazon EKS の料金」を参照してください。

リソースに関するオペレーション情報を表示するタスクのセットアップ

次のセットアップタスクは、Application Manager で AWS リソースに関するオペレーション情報を表示するのに役立ちます。

(推奨) ランブックのアクセス許可の確認

Systems Manager Automation ランブックを使用して、Application Manager から AWS リソースに関する問題を修復できます。この修復ツールを使用するには、アクセス許可を設定または確認する必要があります。料金に関する情報については、[AWS Systems Manager の料金]を参照してください。

(オプション) Cost Explorer を有効にする

AWS Cost Explorer は、詳細な分析のためにコストデータを視覚化するために使用できる AWS Cost Management の機能です。Cost Explorer を有効にすると、アプリケーションのリソースのコスト情報、コスト履歴、コスト最適化を Application Manager コンソールに表示できます。

(オプション) Amazon CloudWatch Logs とアラームのセットアップと設定

CloudWatch は、AWS、ハイブリッド、マルチクラウドのアプリケーションリソースとインフラストラクチャのリソースに関するデータ、および、実用的なインサイトを取得できるモニタリングと管理のサービスです。CloudWatch では、単一のプラットフォームを使用して、ログとメトリクスの形式で生成されたすべてのパフォーマンスとオペレーションのデータを収集し、アクセスできます。Application Manager でリソースの CloudWatch Logs とアラームを表示するには、CloudWatch をセットアップして設定する必要があります。料金の詳細については、「CloudWatch の料金」を参照してください。

> **Note**
>
> CloudWatch Logs のサポートはアプリケーションのみを対象としており、クラスターは対象外です。

(オプション) セットアップおよび設定 AWS Config

AWS Config では、設定内容、相互の関連、時間の経過とともに設定と関係がどのように変化するかなど、AWS アカウント アカウントに関連付けられたリソースの詳細が提供されます。AWS Config を使用して AWS リソースの設定を評価できます。これを行うには、AWS Config ルールを作成して最適な設定内容を定義します。AWS Config はリソースで発生する設定変更を継続的に追跡し、これらの変更がルールの条件に違反していないかどうかを確認します。リソースがルール違反していると、AWS Config はリソースとルールに非準拠のフラグを付けます。Application Manager は、AWS Config ルールに関するコンプライアンス情報を表示します。Application Manager でこのデータを表示するには、AWS Config をセットアップおよび設定する必要があります。料金に関する情報については、[AWS Config の料金]を参照してください。

(オプション) State Manager 関連付け

Systems Manager State Manager を使用して、マネージドノードに割り当てる設定を作成できます。関連付けと呼ばれるこの設定では、ノードで維持する状態を定義します。Application Manager で関連付けのコンプライアンスデータを表示するには、State Manager の関連付けを1つ以上設定する必要があります。State Manager は追加料金なしで提供されます。

(オプション) セットアップおよび設定 OpsCenter

OpsCenter を使用して、Application Managerのリソースに関する運用作業項目 (OpsItems) を表示できます。アラームとイベントに基づいて OpsItems と OpsCenter を自動的に送信するように Amazon CloudWatch と Amazon EventBridge を設定できます。OpsItems を手動で入力することもできます。料金に関する情報については、[AWS Systems Manager の料金]を参照してください。

Systems Manager Application Manager のアクセス許可を設定する

AWS Identity and Access Management (IAM) エンティティ (ユーザー、グループ、ロールなど) に、このトピックに一覧表示されている API オペレーションへのアクセス権がある場合は、AWS Systems Manager のツールである Application Manager のあらゆる機能を使用できます。API オペレーションは 2 つのテーブルに分割され、それらが実行するさまざまな機能を理解するのに役立ちます。

次の表に、リソースの詳細を表示するために Application Manager でリソースを選択した場合に Systems Manager によって呼び出される API オペレーションを示します。例えば、Application Manager で Amazon EC2 Auto Scaling グループを一覧表示し、そのグループの詳細を表示するように選択した場合、Systems Manager で `autoscaling:DescribeAutoScalingGroups` API オペ

レーションが呼び出されます。アカウントに Auto Scaling グループがない場合、この API オペレーションは Application Manager から呼び出されません。

リソースの詳細のみ

```
acm:DescribeCertificate
acm:ListTagsForCertificate
autoscaling:DescribeAutoScalingGroups
cloudfront:GetDistribution
cloudfront:ListTagsForResource
cloudtrail:DescribeTrails
cloudtrail:ListTags
cloudtrail:LookupEvents
codebuild:BatchGetProjects
codepipeline:GetPipeline
codepipeline:ListTagsForResource
dynamodb:DescribeTable
dynamodb:ListTagsOfResource
ec2:DescribeAddresses
ec2:DescribeCustomerGateways
ec2:DescribeHosts
ec2:DescribeInternetGateways
ec2:DescribeNetworkAcls
ec2:DescribeNetworkInterfaces
ec2:DescribeRouteTables
ec2:DescribeSecurityGroups
ec2:DescribeSubnets
ec2:DescribeVolumes
ec2:DescribeVpcs
ec2:DescribeVpnConnections
ec2:DescribeVpnGateways
elasticbeanstalk:DescribeApplications
elasticbeanstalk:ListTagsForResource
elasticloadbalancing:DescribeInstanceHealth
elasticloadbalancing:DescribeListeners
elasticloadbalancing:DescribeLoadBalancers
elasticloadbalancing:DescribeTags
iam:GetGroup
iam:GetPolicy
iam:GetRole
iam:GetUser
lambda:GetFunction
rds:DescribeDBClusters
```

リソースの詳細のみ

```
rds:DescribeDBInstances
rds:DescribeDBSecurityGroups
rds:DescribeDBSnapshots
rds:DescribeDBSubnetGroups
rds:DescribeEventSubscriptions
rds:ListTagsForResource
redshift:DescribeClusterParameters
redshift:DescribeClusterSecurityGroups
redshift:DescribeClusterSnapshots
redshift:DescribeClusterSubnetGroups
redshift:DescribeClusters
s3:GetBucketTagging
```

次の表に、Application Manager で表示されるアプリケーションおよびリソースを変更したり、選択したアプリケーションまたはリソースのオペレーション情報を表示するために Systems Manager が使用する API オペレーションを示します。

アプリケーションのアクションおよび詳細

```
applicationinsights:CreateApplication
applicationinsights:DescribeApplication
applicationinsights:ListProblems
ce:GetCostAndUsage
ce:GetTags
ce:ListCostAllocationTags
ce:UpdateCostAllocationTagsStatus
cloudformation:CreateStack
cloudformation:DeleteStack
cloudformation:DescribeStackDriftDetectionStatus
cloudformation:DescribeStackEvents
cloudformation:DescribeStacks
cloudformation:DetectStackDrift
cloudformation:GetTemplate
cloudformation:GetTemplateSummary
cloudformation:ListStacks
cloudformation:UpdateStack
cloudwatch:DescribeAlarms
cloudwatch:DescribeInsightRules
```

アプリケーションのアクションおよび詳細

```
cloudwatch:DisableAlarmActions
cloudwatch:EnableAlarmActions
cloudwatch:GetMetricData
cloudwatch:ListTagsForResource
cloudwatch:PutMetricAlarm
config:DescribeComplianceByConfigRule
config:DescribeComplianceByResource
config:DescribeConfigRules
config:DescribeRemediationConfigurations
config:GetComplianceDetailsByConfigRule
config:GetComplianceDetailsByResource
config:GetResourceConfigHistory
config:ListDiscoveredResources
config:PutRemediationConfigurations
config:SelectResourceConfig
config:StartConfigRulesEvaluation
config:StartRemediationExecution
ec2:DescribeInstances
ecs:DescribeCapacityProviders
ecs:DescribeClusters
ecs:DescribeContainerInstances
ecs:ListClusters
ecs:ListContainerInstances
ecs:TagResource
eks:DescribeCluster
eks:DescribeFargateProfile
eks:DescribeNodegroup
eks:ListClusters
eks:ListFargateProfiles
eks:ListNodegroups
eks:TagResource
iam:CreateServiceLinkedRole
iam:ListRoles
logs:DescribeLogGroups
resource-groups:CreateGroup
resource-groups:DeleteGroup
resource-groups:GetGroup
resource-groups:GetGroupQuery
resource-groups:GetTags
resource-groups:ListGroupResources
resource-groups:ListGroups
resource-groups:Tag
```

アプリケーションのアクションおよび詳細

```
resource-groups:Untag
resource-groups:UpdateGroup
s3:ListAllMyBuckets
s3:ListBucket
s3:ListBucketVersions
servicecatalog:GetApplication
servicecatalog:ListApplications
sns:CreateTopic
sns:ListSubscriptionsByTopic
sns:ListTopics
sns:Subscribe
ssm:AddTagsToResource
ssm:CreateDocument
ssm:CreateOpsMetadata
ssm:DeleteDocument
ssm:DeleteOpsMetadata
ssm:DescribeAssociation
ssm:DescribeAutomationExecutions
ssm:DescribeDocument
ssm:DescribeDocumentPermission
ssm:GetDocument
ssm:GetInventory
ssm:GetOpsMetadata
ssm:GetOpsSummary
ssm:GetServiceSetting
ssm:ListAssociations
ssm:ListComplianceItems
ssm:ListDocuments
ssm:ListDocumentVersions
ssm:ListOpsMetadata
ssm:ListResourceComplianceSummaries
ssm:ListTagsForResource
ssm:ModifyDocumentPermission
ssm:RemoveTagsFromResource
ssm:StartAssociationsOnce
ssm:StartAutomationExecution
ssm:UpdateDocument
ssm:UpdateDocumentDefaultVersion
ssm:UpdateOpsItem
ssm:UpdateOpsMetadata
ssm:UpdateServiceSetting
tag:GetTagKeys
```

アプリケーションのアクションおよび詳細

```
tag:GetTagValues
tag:TagResources
tag:UntagResources
```

すべての Application Manager 許可のポリシー例

IAM エンティティ (ユーザー、グループ、ロールなど) の Application Manager へのアクセス許可を設定するには、次の例を使用して IAM ポリシーを作成します。このポリシーの例には、Application Manager で使用されるすべての API オペレーションが含まれます。

```
                {
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "acm:DescribeCertificate",
                "acm:ListTagsForCertificate",
                "applicationinsights:CreateApplication",
                "applicationinsights:DescribeApplication",
                "applicationinsights:ListProblems",
                "autoscaling:DescribeAutoScalingGroups",
                "ce:GetCostAndUsage",
                "ce:GetTags",
                "ce:ListCostAllocationTags",
                "ce:UpdateCostAllocationTagsStatus",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStackDriftDetectionStatus",
                "cloudformation:DescribeStackEvents",
                "cloudformation:DescribeStacks",
                "cloudformation:DetectStackDrift",
                "cloudformation:GetTemplate",
                "cloudformation:GetTemplateSummary",
                "cloudformation:ListStacks",
                "cloudformation:ListStackResources",
                "cloudformation:UpdateStack",
                "cloudfront:GetDistribution",
                "cloudfront:ListTagsForResource",
```

```
                "cloudtrail:DescribeTrails",
                "cloudtrail:ListTags",
                "cloudtrail:LookupEvents",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:DescribeInsightRules",
                "cloudwatch:DisableAlarmActions",
                "cloudwatch:EnableAlarmActions",
                "cloudwatch:GetMetricData",
                "cloudwatch:ListTagsForResource",
                "cloudwatch:PutMetricAlarm",
                "codebuild:BatchGetProjects",
                "codepipeline:GetPipeline",
                "codepipeline:ListTagsForResource",
                "config:DescribeComplianceByConfigRule",
                "config:DescribeComplianceByResource",
                "config:DescribeConfigRules",
                "config:DescribeRemediationConfigurations",
                "config:GetComplianceDetailsByConfigRule",
                "config:GetComplianceDetailsByResource",
                "config:GetResourceConfigHistory",
                "config:ListDiscoveredResources",
                "config:PutRemediationConfigurations",
                "config:SelectResourceConfig",
                "config:StartConfigRulesEvaluation",
                "config:StartRemediationExecution",
                "dynamodb:DescribeTable",
                "dynamodb:ListTagsOfResource",
                "ec2:DescribeAddresses",
                "ec2:DescribeCustomerGateways",
                "ec2:DescribeHosts",
                "ec2:DescribeInstances",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeNetworkAcls",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcs",
                "ec2:DescribeVpnConnections",
                "ec2:DescribeVpnGateways",
                "ecs:DescribeCapacityProviders",
                "ecs:DescribeClusters",
                "ecs:DescribeContainerInstances",
```

```
                "ecs:ListClusters",
                "ecs:ListContainerInstances",
                "ecs:TagResource",
                "eks:DescribeCluster",
                "eks:DescribeFargateProfile",
                "eks:DescribeNodegroup",
                "eks:ListClusters",
                "eks:ListFargateProfiles",
                "eks:ListNodegroups",
                "eks:TagResource",
                "elasticbeanstalk:DescribeApplications",
                "elasticbeanstalk:ListTagsForResource",
                "elasticloadbalancing:DescribeInstanceHealth",
                "elasticloadbalancing:DescribeListeners",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTags",
                "iam:CreateServiceLinkedRole",
                "iam:GetGroup",
                "iam:GetPolicy",
                "iam:GetRole",
                "iam:GetUser",
                "iam:ListRoles",
                "lambda:GetFunction",
                "logs:DescribeLogGroups",
                "rds:DescribeDBClusters",
                "rds:DescribeDBInstances",
                "rds:DescribeDBSecurityGroups",
                "rds:DescribeDBSnapshots",
                "rds:DescribeDBSubnetGroups",
                "rds:DescribeEventSubscriptions",
                "rds:ListTagsForResource",
                "redshift:DescribeClusterParameters",
                "redshift:DescribeClusters",
                "redshift:DescribeClusterSecurityGroups",
                "redshift:DescribeClusterSnapshots",
                "redshift:DescribeClusterSubnetGroups",
                "resource-groups:CreateGroup",
                "resource-groups:DeleteGroup",
                "resource-groups:GetGroup",
                "resource-groups:GetGroupQuery",
                "resource-groups:GetTags",
                "resource-groups:ListGroupResources",
                "resource-groups:ListGroups",
                "resource-groups:Tag",
```

```
                "resource-groups:Untag",
                "resource-groups:UpdateGroup",
                "s3:GetBucketTagging",
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:ListBucketVersions",
                "servicecatalog:GetApplication",
                "servicecatalog:ListApplications",
                "sns:CreateTopic",
                "sns:ListSubscriptionsByTopic",
                "sns:ListTopics",
                "sns:Subscribe",
                "ssm:AddTagsToResource",
                "ssm:CreateDocument",
                "ssm:CreateOpsMetadata",
                "ssm:DeleteDocument",
                "ssm:DeleteOpsMetadata",
                "ssm:DescribeAssociation",
                "ssm:DescribeAutomationExecutions",
                "ssm:DescribeDocument",
                "ssm:DescribeDocumentPermission",
                "ssm:GetDocument",
                "ssm:GetInventory",
                "ssm:GetOpsMetadata",
                "ssm:GetOpsSummary",
                "ssm:GetServiceSetting",
                "ssm:ListAssociations",
                "ssm:ListComplianceItems",
                "ssm:ListDocuments",
                "ssm:ListDocumentVersions",
                "ssm:ListOpsMetadata",
                "ssm:ListResourceComplianceSummaries",
                "ssm:ListTagsForResource",
                "ssm:ModifyDocumentPermission",
                "ssm:RemoveTagsFromResource",
                "ssm:StartAssociationsOnce",
                "ssm:StartAutomationExecution",
                "ssm:UpdateDocument",
                "ssm:UpdateDocumentDefaultVersion",
                "ssm:UpdateOpsMetadata",
                "ssm:UpdateOpsItem",
                "ssm:UpdateServiceSetting",
                "tag:GetResources",
                "tag:GetTagKeys",
```

```
                "tag:GetTagValues",
                "tag:TagResources",
                "tag:UntagResources"
            ],
            "Resource": "*"
        }
    ]
}
```

Note

ユーザー、グループ、またはロールにアタッチされた IAM アクセス許可ポリシーから次の API オペレーションを削除することにより、Application Manager でアプリケーションとリソースを変更するユーザーの機能を制限できます。これらのアクションを削除すると、Application Manager で読み取り専用のエクスペリエンスが作成されます。以下に、ユーザーがアプリケーションその他の関連リソースを変更するために使用できる、すべての API を示します。

```
applicationinsights:CreateApplication
ce:UpdateCostAllocationTagsStatus
cloudformation:CreateStack
cloudformation:DeleteStack
cloudformation:UpdateStack
cloudwatch:DisableAlarmActions
cloudwatch:EnableAlarmActions
cloudwatch:PutMetricAlarm
config:PutRemediationConfigurations
config:StartConfigRulesEvaluation
config:StartRemediationExecution
ecs:TagResource
eks:TagResource
iam:CreateServiceLinkedRole
resource-groups:CreateGroup
resource-groups:DeleteGroup
resource-groups:Tag
resource-groups:Untag
resource-groups:UpdateGroup
sns:CreateTopic
sns:Subscribe
ssm:AddTagsToResource
ssm:CreateDocument
```

```
ssm:CreateOpsMetadata
ssm:DeleteDocument
ssm:DeleteOpsMetadata
ssm:ModifyDocumentPermission
ssm:RemoveTagsFromResource
ssm:StartAssociationsOnce
ssm:StartAutomationExecution
ssm:UpdateDocument
ssm:UpdateDocumentDefaultVersion
ssm:UpdateOpsMetadata
ssm:UpdateOpsItem
ssm:UpdateServiceSetting
tag:TagResources
tag:UntagResources
```

IAM ポリシーの作成と編集の詳細については、IAM ユーザーガイドの「IAM ポリシーの作成」を参照してください。このポリシーを IAM エンティティ (ユーザー、グループ、ロールなど) に割り当てる方法については、「IAM ID のアクセス許可の追加および削除」を参照してください。

Application Manager へのアプリケーションとコンテナクラスターの追加

Application Manager は AWS Systems Manager の構成要素です。Application Manager では、アプリケーションはユニットとして動作する AWS リソースの論理グループです。この論理グループは、アプリケーションの異なるバージョン、オペレーターの所有権の境界、またはデベロッパー環境などを表すことができます。

Application Manager を初めて開くと、「What Application Manager can do for you」ページが表示されます。[開始方法] を選択すると、Application Manager は、他の AWS のサービス または Systems Manager ツールで作成されたリソースに関するメタデータを自動的にインポートします。Application Manager は、これらのリソースを事前定義されたカテゴリ別にグループ化されたリストに表示します。

アプリケーションの場合、リストには次のものが含まれます。

- AWS CloudFormation スタック
- カスタムアプリケーション
- AWS Launch Wizard アプリケーション
- AppRegistry アプリケーション

- AWS SAP Enterprise ワークロードアプリケーション
- Amazon ECS クラスター
- Amazon EKS クラスター

インポートが完了すると、これらの定義済みのカテゴリで、アプリケーションまたは特定のリソースに関するオペレーション情報が表示されます。また、リソースのコレクションに関するコンテキストをさらに提供する場合は、Application Manager でアプリケーションを手動で作成できます。その後、そのアプリケーションにリソースまたはリソースのグループを追加できます。Application Manager でアプリケーションを作成すると、アプリケーションのコンテキストで、リソースに関するオペレーション情報を表示できます。

Application Manager でアプリケーションを作成する

Application Manager でアプリケーションを作成し、そのアプリケーションにリソースを追加するには、次の手順に従います。

Application Manager でアプリケーションを作成するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Application Manager] を選択します。
3. [アプリケーションの作成] を選択します。
4. ドロップダウンリストからオプションを選択し、表示されるページのフィールドに入力します。

アプリケーションの使用

Application Manager は AWS Systems Manager の構成要素です。このセクションには、Application Manager アプリケーションの使用および AWS リソースに関するオペレーション情報の表示に役立つトピックが含まれています。

内容

- Application Manager 内のアプリケーション概要
- アプリケーション EC2 インスタンスの管理
- アプリケーションに関連付けられたリソースの表示
- アプリケーションコンプライアンスの管理

- CloudWatch Application Insights を使用したアプリケーションの監視
- アプリケーションでの OpsItems の表示
- アプリケーションログの管理
- Automation ランブックを使用してアプリケーション問題を修正する
- Application Manager 内のリソースのタグ付け
- Application Manager での AWS CloudFormation テンプレートとスタックの使用
- Application Manager でのクラスターの操作

Application Manager 内のアプリケーション概要

AWS Systems Manager の構成要素である Application Manager の [概要] タブには、Amazon CloudWatch アラーム、運用作業項目 (OpsItems)、CloudWatch Application Insights、ランブック履歴の概要が表示されます。カードの [すべて表示] を選択して、対応するタブを開くと、すべての application insights、アラーム、OpsItems、またはランブック履歴を表示できます。

Application Insights について

CloudWatch Application Insights は、アプリケーションリソースとテクノロジースタック全体の主要なメトリクス、ログ、アラームを識別して設定します。また、メトリクスとログを継続的にモニタリングし、異常やエラーを検出して相互に関連付けます。エラーや異常が検出されると、Application Insights は CloudWatch Events を生成します。これを使用すると、通知を設定したり、アクションを実行したりできます。[モニタリング] タブで [設定の編集] ボタンを選択すると、CloudWatch Application Insights コンソールが開きます。Application Insights の詳細については、Amazon CloudWatch ユーザーガイドで「Amazon CloudWatch Application Insights とは」を参照してください。

Cost Explorer について

Application Manager は、[コスト] ウィジェットと [コスト] タブによって、AWS Cost Management の機能である AWS Cost Explorer と統合されています。コストマネジメントコンソールで Cost Explorer を有効にした後、Application Manager の [コスト] ウィジェットと [コスト] タブに、特定の非コンテナアプリケーションまたはアプリケーションコンポーネントのコストデータが表示されます。ウィジェットまたはタブでフィルターを使用して、棒グラフまたは折れ線グラフで、異なる期間、粒度のレベル、コストタイプに基づいてコストデータを表示できます。

この機能は、[Go to AWS Cost Management console] ボタンを選択すると有効化されます。デフォルトでは、データは過去 3 か月間でフィルタリングされています。非コンテナアプリケーションの

場合は、[View all] (すべてを表示) ボタンを選択すると、Application Manager に [Resources] (リソース) タブが開きます。コンテナアプリケーションでは、[View all] (すべてを表示) ボタンで AWS Cost Explorerコンソールが開きます。

このページで実行できるアクション

このページの [Overview] (概要) タブでは、次のウィジェットをオンにしてその情報にアクセスすることができます。ウィジェットが有効になっている場合は、そのウィジェットの [View all] (すべて表示) をクリックすると、そのエリアに関連するアプリケーションの詳細が表示されます。

- [Insights and Alarms] (インサイトとアラーム) セクションで重要度の数値を選択し、[Monitoring] (モニタリング) タブを開きます。このタブで、選択した重要度のアラームについて、その詳細を確認できます。
- [Cost] (コスト) セクションで [View all] (すべて表示) を選択し、[Resources] (リソース) タブを開きます。このタブで、特定のアプリケーションまたはアプリケーションコンポーネントについて、そのコストデータを確認できます。
- [Compliance] (コンプライアンス) セクションで [View all] (すべて表示) を選択し、[Compliance] (コンプライアンス) タブを開きます。このタブで、AWS Config と State Manager の関連付けに関するコンプライアンス情報を確認できます。

  > **Note**
  >
  > パッチに関するコンプライアンスの詳細を表示するには、[Compliance] (コンプライアンス) タブを直接選択します。これで、選択したアプリケーションで使用されているマネージドノードの、パッチに関するコンプライアンスの詳細が表示されます。

- [ランブック] セクションで、ランブックを選択して Systems Manager の [ドキュメント] ページで開きます。このページでは、ドキュメントの詳細を表示できます。
- [OpsItems] セクションで、重要度を選択して [OpsItems] タブを開き、選択した重要度のすべての OpsItems を表示できます。
- [すべて表示] ボタンを選択して、対応するタブを開きます。アプリケーションのすべてのアラーム、OpsItems、またはランブック履歴エントリを表示できます。

[Overview (概要)] タブを開くには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。

2. ナビゲーションペインで、[Application Manager] を選択します。
3. [Applications (アプリケーション)] セクションで、カテゴリを選択します。Application Manager で手動で作成したアプリケーションを開くには、[カスタムアプリケーション] を選択します。
4. リストからアプリケーションを選択します。Application Manager で、[Overview (概要)] タブが開きます。

アプリケーション EC2 インスタンスの管理

Application Manager は Amazon Elastic Compute Cloud (Amazon EC2) と統合しており、アプリケーションの観点からインスタンスに関する情報を表示することができます。 Application Manager は、選択したアプリケーションのインスタンスの状態、ステータス、および Amazon EC2 Auto Scaling の正常性を、グラフィカルな形式で表示します。[Instances] (インスタンス) タブには、アプリケーション内の各インスタンスに関する、以下の情報を含む表も表示されます。

- インスタンスの状態 (保留中、停止中、実行中、停止済み)
- SSM Agent の ping ステータス
- インスタンスで最近処理された、Systems Manager Automation ランブックのステータスと名前
- 状態ごとの Amazon CloudWatch Logs アラームの数。
  - `ALARM` – メトリクスまたは式が、定義されているしきい値を超えています。
  - `OK` – メトリクスや式は、定義されているしきい値の範囲内です。
  - `INSUFFICIENT_DATA` – アラームが開始直後であるか、メトリクスが利用できないか、メトリクス用のデータが不足しているため、アラームの状態を判定できません。
- 親および個別の Auto Scaling グループに関する正常性

[All instances] (すべてのインスタンス) テーブルでインスタンスを選択すると、Application Manager は 4 つのタブで、そのインスタンスに関する情報を表示します。

- [Details] (詳細) – Amazon EC2 のすべてのインスタンスの詳細 (Amazon マシンイメージ (AMI)、DNS 情報、IP アドレス情報、その他)。
- [Health] (正常性) – EC2 システムとインスタンスのステータスチェックが示す現在のステータス。
- [Execution history] (実行履歴) – インスタンスによって処理された、Systems Manager Automation ランブックおよび API コールの実行ログ。
- [CloudWatch alarms] (CloudWatch アラーム) – インスタンスによって生成された CloudWatch アラームの名前、状態、その他の情報。

このページで実行できるアクション

このページでは、次のアクションを実行できます。

- インスタンスを開始、停止、終了します。
- Chef レシピを適用します。
- Auto Scaling グループに対し、インスタンスのアタッチあるいはデタッチを行います。
- SSM Agent の自動更新を有効にします。

[Instances] (インスタンス) タブを開くには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Application Manager] を選択します。
3. [Applications (アプリケーション)] セクションで、カテゴリを選択します。手動により Application Manager で作成したアプリケーションを開くには、[Custom applications] (カスタムアプリケーション) を選択します。
4. リストからアプリケーションを選択します。Application Manager で、[Overview (概要)] タブが開きます。
5. [Instances] タブを選択します。

アプリケーションインスタンスの詳細を表示するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Application Manager] を選択します。
3. [Applications (アプリケーション)] セクションで、カテゴリを選択します。手動により Application Manager で作成したアプリケーションを開くには、[Custom applications] (カスタムアプリケーション) を選択します。
4. リストからアプリケーションを選択します。Application Manager で、[Overview (概要)] タブが開きます。
5. [Instances] タブを選択します。
6. 詳細を表示しようとしているインスタンスの横にあるボタンを選択します。
7. ページの一番下にあるインスタンスの詳細を確認します。

自動的に SSM Agent を更新するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Application Manager] を選択します。
3. [Applications (アプリケーション)] セクションで、カテゴリを選択します。手動により Application Manager で作成したアプリケーションを開くには、[Custom applications] (カスタムアプリケーション) を選択します。
4. リストからアプリケーションを選択します。Application Manager で、[Overview (概要)] タブが開きます。
5. [Instances] タブを選択します。
6. [エージェントアクション] のドロップダウンで [SSM Agent アップデートを設定] を選択します。
7. [すべてのインスタンス] を選択し、すべてのマネージドインスタンスの自動 SSM Agent 更新を設定します。または、[インスタンス] を選択し、アプリケーションの 1 つのインスタンスで自動 SSM Agent 更新を設定します。
8. [自動アップデートを有効化] を選択します。
9. [スケジュールを指定] ドロップダウンで、SSM Agent 更新に使用するスケジュールを選択します。
10. [設定] を選択します。

アプリケーションに関連付けられたリソースの表示

AWS Systems Manager のコンポーネントである Application Manager では、[リソース] タブにアプリケーションの AWS リソースが表示されます。最上位のコンポーネントを選択すると、このページには、そのコンポーネントとサブコンポーネントのすべてのリソースが表示されます。サブコンポーネントを選択すると、このページには、そのサブコンポーネントに割り当てられたリソースのみが表示されます。

このページで実行できるアクション

このページでは、次のアクションを実行できます。

- リソース名を選択して、リソースが作成されたコンソールから提供される詳細、タグ、Amazon CloudWatch アラーム、AWS Config の詳細、AWS CloudTrail のログ情報など、リソースに関する情報を表示できます。

- リソース名の横にあるオプションボタンを選択します。次に、[Resource timeline] ボタンを選択して AWS Config コンソールを開き、選択したリソースに関するコンプライアンス情報を表示できます。
- AWS Cost Explorer を有効にした場合、Cost Explorer セクションには、特定の非コンテナアプリケーションまたはアプリケーションコンポーネントのコストデータが表示されます。この機能は、[Go to AWS Cost Management console] ボタンを選択すると有効化されます。このセクションのフィルターを使用して、アプリケーションに関するコスト情報を表示します。

Resourcesタブを開くには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Application Manager] を選択します。
3. [Applications (アプリケーション)] セクションで、カテゴリを選択します。Application Manager で手動で作成したアプリケーションを開くには、[カスタムアプリケーション] を選択します。
4. リストからアプリケーションを選択します。Application Manager で、[Overview (概要)] タブが開きます。
5. [リソース] タブを選択します。

アプリケーションコンプライアンスの管理

AWS Systems Manager のコンポーネントである Application Manager では、[Configurations] (設定) ページに AWS Config リソースと設定ルールのコンプライアンス情報が表示されます。このページには、AWS Systems Manager State Manager による関連付けのコンプライアンス情報も表示されます。リソース、ルール、または関連付けを選択して、対応するコンソールを開いて詳細を表示できます。このページには、過去 90 日間のコンプライアンス情報が表示されます。

このページで実行できるアクション

このページでは、次のアクションを実行できます。

- リソース名を選択して AWS Config コンソールを開き、選択したリソースに関するコンプライアンス情報を表示できます。
- リソース名の横にあるオプションボタンを選択します。次に、[Resource timeline] ボタンを選択して AWS Config コンソールを開き、選択したリソースに関するコンプライアンス情報を表示できます。

- [Config rules compliance (Config ルールのコンプライアンス)] セクションでは、次の操作を行うことができます。
  - ルール名を選択して AWS Config コンソールを開き、そのルールに関する情報を表示できます。
  - [Add rules] を選択して AWS Config コンソールを開き、ルールを作成できます。
  - ルール名の横にあるオプションボタンを選択して [Actions (アクション)]、[Manage remediation (修復の管理)] の順に選択し、ルールの修正アクションを変更します。
  - ルール名の横にあるオプションボタンを選択して、[Actions (アクション)]、[Re-evaluate (再評価)] の順に選択し、AWS Config で選択したルールに対するコンプライアンスチェックを実行できます。
- [Association compliance (関連付けのコンプライアンス)] セクションでは、以下の操作を行うことができます。
  - 関連付け名を選択して [Associations (関連付け)] ページを開き、その関連付けに関する情報を表示できます。
  - [Create association (関連付けの作成)] を選択して、関連付けを作成できる Systems Manager State Manager を開きます。
  - 関連付けの名前の横にあるオプションボタンを選択し、[Apply Association (関連付けを適用)] を選択し、関連付けで指定されたすべてのアクションを直ちに開始できます。

[Compliance] (コンプライアンス) タブを開くには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Application Manager] を選択します。
3. [Applications (アプリケーション)] セクションで、カテゴリを選択します。Application Manager で手動で作成したアプリケーションを開くには、[カスタムアプリケーション] を選択します。
4. リストからアプリケーションを選択します。Application Manager で、[Overview (概要)] タブが開きます。
5. [Compliance] (コンプライアンス) タブを選択します。

CloudWatch Application Insights を使用したアプリケーションの監視

Application Manager の構成要素である AWS Systems Manager では、[Monitoring (モニタリング)] タブには、Amazon CloudWatch Application Insights とアプリケーションのリソースのアラーム詳細が表示されます。

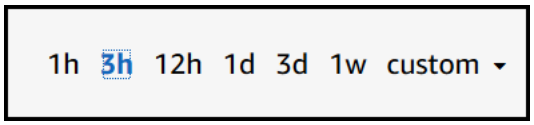
Application Insights について

CloudWatch Application Insights は、アプリケーションリソースとテクノロジースタック全体の主要なメトリクス、ログ、アラームを識別して設定します。また、メトリクスとログを継続的にモニタリングし、異常やエラーを検出して相互に関連付けます。エラーや異常が検出されると、Application Insights は CloudWatch Events を生成します。これを使用すると、通知を設定したり、アクションを実行したりできます。[モニタリング] タブで [設定の編集] ボタンを選択すると、CloudWatch Application Insights コンソールが開きます。Application Insights の詳細については、Amazon CloudWatch ユーザーガイドで「Amazon CloudWatch Application Insights とは」を参照してください。

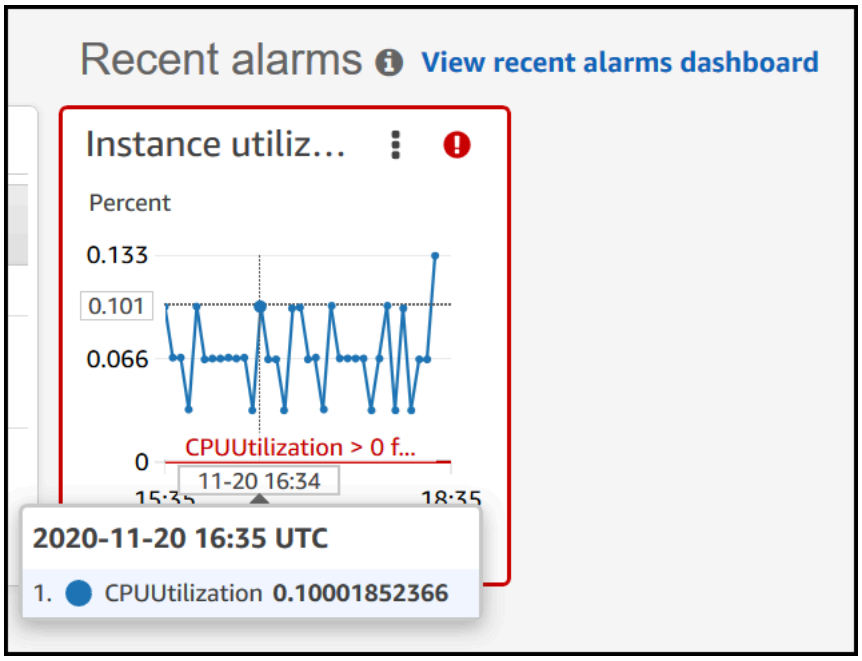
このページで実行できるアクション

このページでは、次のアクションを実行できます。

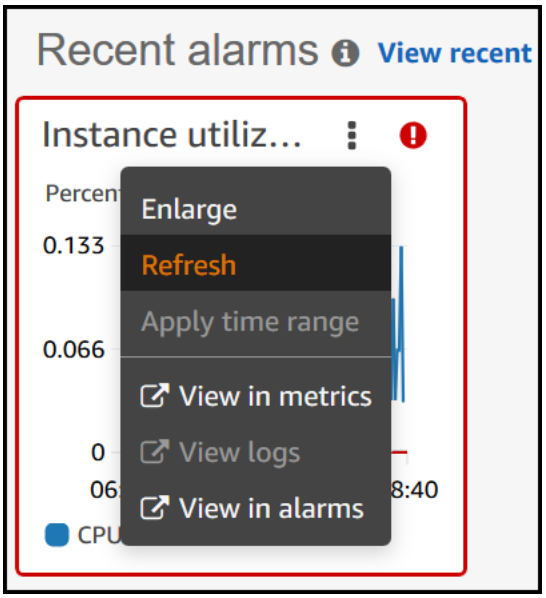
- [AWS のサービスによるアラーム] セクションでサービス名を選択して、CloudWatch を開いて選択したサービスとアラームを表示します。
- 定義済みの期間の値を 1 つ選択して、[Recent alarms (最近のアラーム)] セクションのウィジェットに表示されるデータの期間を調整します。[カスタム] を選択して、独自の期間を定義できます。



- [Recent alarms (最近のアラーム)] セクションのウィジェットの上にカーソルをホバリングすると、特定の時間のデータのポップアップが表示されます。

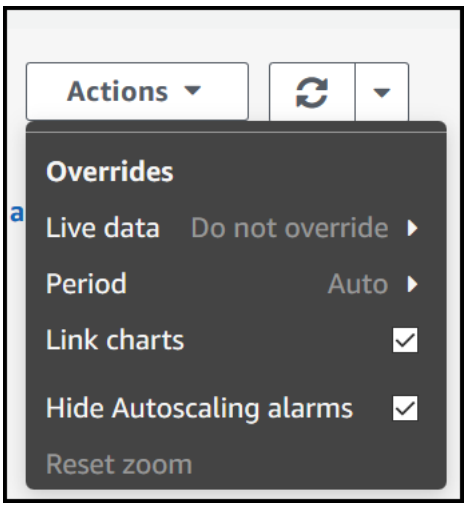


- ウィジェットのオプションメニューを選択して、表示オプションを表示します。[拡大] を選択して、ウィジェットを展開します。[Refresh] を選択して、ウィジェットのデータを更新します。ウィジェットのデータ表示で、カーソルをクリックおよびドラッグし、特定の範囲を選択します。次に、[Apply time range (時間範囲の適用)] を選択します。



- [Actions (アクション)] メニューを選択して、アラームデータの [Override (上書き)] オプションを表示します。このオプションには次のようなものがあります。
  - ウィジェットにライブデータを表示するかどうかを選択します。ライブデータとは、直近の 1 分以内に公開された、完全には集計されていないデータです。ライブデータをオフにすると、集計期間が 1 分以上経過したデータポイントのみが表示されます。たとえば、5 分の期間を使用すると、12 時 35 分のデータポイントは 12 時 35 分から 12 時 40 分まで集計され、12 時 41 分に表示されます。

    ライブデータをオンにすると、対応する集計期間にデータが公開されるとすぐに、最新のデータポイントが表示されます。表示を更新するたびに、その集計期間内に新しいデータが公開されると、最新のデータポイントが変わる場合があります。
  - ライブデータの期間を指定します。
  - [Recent alarms (最近のアラーム)] セクションでグラフをリンクすると、一方のグラフをズームインまたはズームアウトしたときに、もう一方のグラフが同時に拡大または縮小されます。グラフのリンクを解除し、拡大を 1 つのグラフに行うこともできます。
  - Auto Scaling アラームを非表示にします。



[モニタリング] タブを開くには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Application Manager] を選択します。
3. [Applications (アプリケーション)] セクションで、カテゴリを選択します。Application Manager で手動で作成したアプリケーションを開くには、[カスタムアプリケーション] を選択します。
4. リストからアプリケーションを選択します。Application Manager で、[Overview (概要)] タブが開きます。
5. モニタリングタブを選択します。

アプリケーションでの OpsItems の表示

AWS Systems Manager の構成要素である Application Manager で、[OpsItems] タブに選択したアプリケーションのリソースの運用作業項目 (OpsItems) が表示されます。Amazon CloudWatch アラームと Amazon EventBridge イベントから OpsItems を自動的に作成するように、Systems Manager OpsCenter を設定できます。手動で OpsItems を作成することもできます。

このタブで実行できるアクション

このページでは、次のアクションを実行できます。

- 検索フィールドを使用して OpsItems のリストをフィルタリングします。OpsItem の名前、ID、ソース ID、または重要度でフィルタリングできます。ステータスに基づいてリストをフィルタリ

ングすることもできます。OpsItems は、Open、In progress、Resolved、または All のいずれかのステータスをサポートします。

- その横にあるオプションボタンを選択し、[Set status] メニューのオプションを選択して、OpsItem のステータスを変更します。
- Systems Manager OpsCenter を開き、[Create OpsItem] を選択して OpsItem を作成します。

OpsItems タブを開くには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Application Manager] を選択します。
3. [Applications (アプリケーション)] セクションで、カテゴリを選択します。Application Manager で手動で作成したアプリケーションを開くには、[カスタムアプリケーション] を選択します。
4. リストからアプリケーションを選択します。Application Manager で、[Overview (概要)] タブが開きます。
5. [OpsItems] タブを選択します。

アプリケーションログの管理

AWS Systems Manager の構成要素である Application Manager で、[Logs (ログ)] タブには Amazon CloudWatch Logs のロググループのリストが表示されます。

このタブで実行できるアクション

このページでは、次のアクションを実行できます。

- ロググループ名を選択して CloudWatch Logs で開きます。その後、ログストリームを選択して、アプリケーションのコンテキストでリソースのログを表示できます。
- CloudWatch Logs でロググループを作成するには、[Create log grouops (ロググループの作成)] を選択します。

[Logs (ログ)] タブを開くには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Application Manager] を選択します。

3. [Applications (アプリケーション)] セクションで、カテゴリを選択します。Application Manager で手動で作成したアプリケーションを開くには、[カスタムアプリケーション] を選択します。
4. リストからアプリケーションを選択します。Application Manager で、[Overview (概要)] タブが開きます。
5. [ログ] タブを選択します。

Automation ランブックを使用してアプリケーション問題を修正する

Automation ランブックを使用して、AWS リソースに関する問題を AWS Systems Manager のツールである Application Manager から修復できます。オートメーションランブックは、オートメーションの実行時にマネージドインスタンスおよびその他の AWS リソースで Systems Manager が実行するアクションを定義します。Automation は AWS Systems Manager のツールです。ランブックには、順次実行されるステップが 1 つ以上含まれています。各ステップは、1 つのアクションを中心に構築されます。1 つのステップからの出力は、後のステップで入力として使用できます。

Application Manager アプリケーションまたはクラスターから [Start runbook (ランブックの起動)] を選択すると、アプリケーションまたはクラスター内のリソースのタイプに基づいてフィルターされた使用可能なランブックのリストが表示されます。起動するランブックを選択すると、Systems Manager により [Execute automation document (オートメーションドキュメントの実行)] ページが開きます。

Application Manager には、ランブックを使用するための以下の拡張機能が含まれています。

- Application Manager でリソースの名前を選択し、[Execute runbook (Runbook の実行)] を選ぶと、そのリソースタイプのランブックのフィルター処理されたリストが表示されます。
- 同じ種類のすべてのリソースでオートメーションを開始するには、リストでランブックを選択し、[Run for resources of same type (同じタイプのリソースに対して実行)] を選択します。

[開始する前に]

Application Manager からランブックを開始する前に、以下を実行してください。

- ランブックを開始するための適切なアクセス許可があることを確認してください。詳細については、「」を参照してくださいオートメーションの設定
- ランブックの開始に関するオートメーション手順のドキュメントを確認してください。詳細については、「Systems Manager Automation を使用した自動オペレーションを実行する」を参照してください。

Application Manager からランブックを開始するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Application Manager] を選択します。
3. [Applications (アプリケーション)] セクションで、カテゴリを選択します。Application Manager で手動で作成したアプリケーションを開くには、[カスタムアプリケーション] を選択します。
4. リストからアプリケーションを選択します。Application Manager で、[Overview (概要)] タブが開きます。
5. [ランブックを開始] を選択すると、Application Manager は [自動化ウィジェット] のポップアップを開きます。[自動化ウィジェット] のオプションについては、「Systems Manager Automation を使用した自動オペレーションを実行する」を参照してください。

Application Manager 内のリソースのタグ付け

アプリケーションと、Application Manager の AWS リソースでタグをすばやく追加または削除できます。アプリケーションと、そのアプリケーションのあらゆる AWS リソースにタグを追加するか削除するには、以下の手順を使用します。

アプリケーションおよびアプリケーション内のすべてのリソースにタグを追加または削除するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Application Manager] を選択します。
3. [Applications (アプリケーション)] セクションで、カテゴリを選択します。Application Manager で手動で作成したアプリケーションを開くには、[カスタムアプリケーション] を選択します。
4. リストからアプリケーションを選択します。Application Manager で、[Overview (概要)] タブが開きます。
5. [Application information (アプリケーション情報)] セクションの [Application tags (アプリケーションタグ)] の下で数字を選びます。アプリケーションにタグが割り当てられていない場合、数字はゼロになります。
6. タグを追加するには、[Add new tag (新しいタグの追加)] を選択します。キーとオプションの値を指定します。タグを削除するには、[Remove (削除)] を選択します。
7. [Save (保存)] を選択します。

Application Manager で、特定のリソースにタグを追加するか削除するには、以下の手順に従います。

リソースにタグを追加または削除するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Application Manager] を選択します。
3. [Applications (アプリケーション)] セクションで、カテゴリを選択します。Application Manager で手動で作成したアプリケーションを開くには、[カスタムアプリケーション] を選択します。
4. リストからアプリケーションを選択します。Application Manager で、[Overview (概要)] タブが開きます。
5. [リソース] タブを選択します。
6. リソース名を選択します。
7. [Tags (タグ)] セクションで [Edit (編集)] を選択します。
8. タグを追加するには、[Add new tag (新しいタグの追加)] を選択します。キーとオプションの値を指定します。タグを削除するには、[Remove (削除)] を選択します。
9. [Save] を選択します。

Application Manager での AWS CloudFormation テンプレートとスタックの使用

AWS Systems Manager のツールである Application Manager は、AWS CloudFormation と統合することで、アプリケーションのリソースのプロビジョニングと管理に役立ちます。Application Manager では、AWS CloudFormation テンプレートとスタックを作成、編集、削除できます。スタックは、単一のユニットとして管理できる AWS リソースのコレクションです。つまり、CloudFormation スタックを使用すると、一連の AWS リソースを作成、更新、または削除できます。テンプレートは、JSON または YAML でフォーマットされたテキストファイルで、スタックでプロビジョニングするリソースを指定します。

Application Manager には、テンプレートのクローン、作成、格納が可能なテンプレートライブラリも含まれています。Application Manager と CloudFormation には、スタックの現在のステータスに関する情報と同じ情報が表示されます。テンプレートとテンプレートの更新は、スタックをプロビジョニングするまで Systems Manager に格納されます。このとき、変更内容は CloudFormation にも表示されます。

Application Manager でスタックを作成すると、[CloudFormation stacks (CloudFormation スタック)] ページには有用な情報が表示されます。この情報には、作成に使用されたテンプレート、スタックのリソースの OpsItems 数、スタックのステータス、ドリフトのステータスが含まれます。

Cost Explorer について

Application Manager は、[Cost] (コスト) ウィジェットによって、AWS Cost Management の機能である AWS Cost Explorer と統合されています。コストマネジメントコンソールで Cost Explorer を有効にした後、Application Manager の [Cost] (コスト) ウィジェットに、特定の非コンテナアプリケーションまたはアプリケーションコンポーネントのコストデータが表示されます。ウィジェットでフィルターを使用して、棒グラフまたは折れ線グラフで、異なる期間、粒度、およびコストタイプに基づいてコストデータを表示できます。

この機能は、[Go to AWS Cost Management console] ボタンを選択すると有効化されます。デフォルトでは、データは過去 3 か月間でフィルタリングされています。非コンテナアプリケーションの場合は、[View all] (すべてを表示) ボタンを選択すると、Application Manager に [Resources] (リソース) タブが開きます。コンテナアプリケーションでは、[View all] (すべてを表示) ボタンで AWS Cost Explorerコンソールが開きます。

> **Note**
>
> Cost Explorer タグを使用してアプリケーションのコストを追跡できます。AWS CloudFormation スタックベースのアプリケーションに `AppManagerCFNStackKey` タグキーが設定されていない場合、Application Manager で Cost Explorer で正確なコストデータを表示できません。`AppManagerCFNStackKey` タグキーが検出されない場合、コンソールでタグを CloudFormation スタックに追加してコスト追跡を有効にするように求められます。追加すると、タグキーがスタックの Amazon リソースネーム (ARN) にマッピングされ、[Cost] (コスト) ウィジェットで正確なコストデータを表示できます。

> **Important**
>
> `AppManagerCFNStackKey` タグを追加すると、スタックの更新がトリガーされます。スタックが最初にデプロイされた後に実行された手動設定は、ユーザータグを追加した後には反映されません。リソースの更新動作の詳細については、「AWS CloudFormation ユーザーガイド」の「スタックリソースの更新動作」を参照してください。

[開始する前に]

Application Manager を使用して CloudFormation のテンプレートとスタックを作成、編集、または削除する前に、次のリンクを使用して CloudFormation の概念を確認してください。

- What is AWS CloudFormation?
- AWS CloudFormation のベストプラクティス
- テンプレートの基礎に関する説明
- AWS CloudFormation スタックの操作
- AWS CloudFormation テンプレートの操作
- サンプルテンプレート

トピック

- Application Manager を使用した AWS CloudFormation テンプレートの管理
- Application Manager を使用した AWS CloudFormation スタックの管理

Application Manager を使用した AWS CloudFormation テンプレートの管理

AWS Systems Manager のツールである Application Manager には、テンプレートライブラリやその他のツールが含まれており、AWS CloudFormation テンプレートの管理に役立ちます。このセクションでは、次の情報を紹介します。

トピック

- テンプレートライブラリの操作
- テンプレートの作成
- テンプレートの編集

テンプレートライブラリの操作

Application Manager のテンプレートライブラリには、テンプレートの表示、作成、編集、削除、およびクローン作成に役立つツールが用意されています。また、テンプレートライブラリから直接スタックをプロビジョニングすることもできます。テンプレートは、タイプ `CloudFormation` の Systems Manager (SSM) ドキュメントとして格納されます。テンプレートを SSM ドキュメントとして格納することで、バージョンコントロールを使用して、異なるバージョンのテンプレー

トを操作できます。アクセス許可を設定したり、テンプレートを共有したりすることもできます。スタックのプロビジョニングに成功すると、スタックとテンプレートは Application Manager と CloudFormation で使用できるようになります。

[開始する前に]

Application Manager で CloudFormation のテンプレートの操作を開始する前に、SSM ドキュメントの詳細について、次のトピックをお読みください。

- AWS Systems Manager ドキュメント
- SSM ドキュメントの共有
- 共有 SSM ドキュメントのベストプラクティス

Application Manager でテンプレートライブラリを表示するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Application Manager] を選択します。
3. [CloudFormation テンプレートライブラリ] を選択します。

テンプレートの作成

以下の手順では、Application Manager で CloudFormation のテンプレートを作成する方法について説明します。テンプレートを作成するときは、テンプレートのスタックの詳細を JSON または YAML で入力します。JSON や YAML に詳しくない場合は、テンプレートを視覚的に作成および変更するためのツール、AWS Infrastructure Composer を使用してください。詳細については、「AWS CloudFormationユーザーガイド」の「Infrastructure Composer でテンプレートを視覚的に作成する」を参照してください。テンプレートの構造の詳細については、AWS CloudFormation ユーザーガイドの「AWS CloudFormation テンプレートセクション」を参照してください。

複数のテンプレートスニペットからテンプレートを作成することもできます。テンプレートスニペットは、特定のリソースのテンプレートを作成する方法を示す例を提供しています。たとえば、Amazon Elastic Compute Cloud (Amazon EC2) インスタンス、Amazon Simple Storage Service (Amazon S3) ドメイン、AWS CloudFormation マッピングなどのスニペットを表示できます。スニペットはリソースごとにグループ化されます。AWS CloudFormation ユーザーガイドの「一般的なテンプレートスニペット」セクションでは、用途の広い AWS CloudFormation スニペットが紹介されています。

Application Manager (コンソール) で CloudFormation のテンプレートを作成

以下の手順に従い、AWS Management Console を使用して Application Manager で CloudFormation のテンプレートを作成します。

Application Manager で CloudFormation テンプレートを作成するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Application Manager] を選択します。
3. [CloudFormation テンプレートライブラリ] を選択し、[テンプレートを作成] を選択するか、既存のテンプレートを選択して [アクション]、[クローン] の順に選択します。
4. [Name] (名前) には、テンプレートが作成するリソース、もしくはスタックの目的を識別しやすくするテンプレートの名前を入力します。
5. (オプション) [Version name] (バージョン名) には、テンプレートのバージョンを識別する名前または番号を入力します。
6. [Code editor] (コードエディタ) セクションで、[YAML] または [JSON] をクリックし、テンプレートコードを入力するか、コピーして貼り付けます。
7. (オプション) [Tags] (タグ) セクションで、テンプレートにタグキーの名前/値ペアを 1 つ、または複数適用します。
8. (オプション) [Permissions] (アクセス許可) セクションで、AWS アカウント ID を入力し、[Add acount] (アカウントの追加) を選択します。このアクションで、テンプレートに読み取りのアクセス許可を付与します。アカウント所有者はテンプレートのプロビジョニングとクローン作成ができますが、テンプレートの編集や削除はできません。
9. [Create] を選択します。テンプレートは、Systems Manager (SSM) ドキュメントサービスに保存されます。

Application Manager (コマンドライン) で CloudFormation テンプレートを作成

JSON または YAML で CloudFormation のテンプレートのコンテンツを作成したら、AWS Command Line Interface (AWS CLI) または AWS Tools for PowerShell を使用して、テンプレートを SSM ドキュメントとして保存します。各##############をユーザー自身の情報に置き換えます。

[開始する前に]

まだ AWS CLI または AWS Tools for PowerShell をインストールして設定していない場合は、インストールして設定します。詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」および「AWS Tools for PowerShell のインストール」を参照してください。

Linux & macOS

```
aws ssm create-document \
    --content file://path/to/template_in_json_or_yaml \
    --name "a_name_for_the_template" \
    --document-type "CloudFormation" \
    --document-format "JSON_or_YAML" \
    --tags "Key=tag-key,Value=tag-value"
```

Windows

```
aws ssm create-document ^
    --content file://C:\path\to\template_in_json_or_yaml ^
    --name "a_name_for_the_template" ^
    --document-type "CloudFormation" ^
    --document-format "JSON_or_YAML" ^
    --tags "Key=tag-key,Value=tag-value"
```

PowerShell

```
$json = Get-Content -Path "C:\path\to\template_in_json_or_yaml | Out-String
New-SSMDocument `
    -Content $json `
    -Name "a_name_for_the_template" `
    -DocumentType "CloudFormation" `
    -DocumentFormat "JSON_or_YAML" `
    -Tags "Key=tag-key,Value=tag-value"
```

成功すると、コマンドは以下のような応答を返します。

```
{
    "DocumentDescription": {
        "Hash": "c1d9640f15fbdba6deb41af6471d6ace0acc22f213bdd1449f03980358c2d4fb",
        "HashType": "Sha256",
        "Name": "MyTestCFTemplate",
        "Owner": "428427166869",
        "CreatedDate": "2021-06-04T09:44:18.931000-07:00",
```

```
        "Status": "Creating",
        "DocumentVersion": "1",
        "Description": "My test template",
        "PlatformTypes": [],
        "DocumentType": "CloudFormation",
        "SchemaVersion": "1.0",
        "LatestVersion": "1",
        "DefaultVersion": "1",
        "DocumentFormat": "YAML",
        "Tags": [
            {
                "Key": "Templates",
                "Value": "Test"
            }
        ]
    }
```

テンプレートの編集

以下の手順に従って、Application Manager で CloudFormation テンプレートを編集します。テンプレートの変更は、更新されたテンプレートを使用するスタックをプロビジョニングした後、CloudFormation で行います。

Application Manager で CloudFormation テンプレートを編集するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Application Manager] を選択します。
3. [CloudFormation テンプレートライブラリ] を選択します。
4. テンプレートを選択してから、[Actions] (アクション)、[Edit] (編集) の順に選択します。テンプレートの名前は変更できませんが、他の詳細はすべて変更できます。
5. [Save] を選択します。テンプレートは、Systems Manager ドキュメントサービスに保存されます。

Application Manager を使用した AWS CloudFormation スタックの管理

AWS Systems Manager のツールである Application Manager は、AWS CloudFormation と統合することで、アプリケーションのリソースのプロビジョニングと管理に役立ちます。Application Manager で CloudFormation のテンプレートとスタックを作成、編集、削除できます。スタックは、

単一のユニットとして管理できる AWS リソースのコレクションです。つまり、CloudFormation スタックを使用すると、一連の AWS リソースを作成、更新、または削除できます。テンプレートは、JSON または YAML でフォーマットされたテキストファイルで、スタックでプロビジョニングするリソースを指定します。このセクションでは、次の情報を紹介します。

トピック

- スタックの作成
- スタックの更新

スタックの作成

以下の手順では、Application Manager を使用して CloudFormation のスタックを作成する方法について説明します。スタックはテンプレートに基づいています。スタックを作成するときは、既存のテンプレートを選択するか、新しいテンプレートを作成します。スタックの作成後、システムはスタック内で識別されたリソースの作成をただちに試みます。システムがリソースを正常にプロビジョニングすると、テンプレートとスタックは Application Manager と CloudFormation で表示および編集できるようになります。

> **Note**
>
> Application Manager を使用してスタックを作成する場合には料金はかかりませんが、スタックで作成した AWS リソースには料金が発生します。

Application Manager (コンソール) を使用して CloudFormation のスタックを作成するには

以下の手順に従い、AWS Management Console で Application Manager を使用してスタックを作成します。

CloudFormation のスタックを作成する

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Application Manager] を選択します。
3. [アプリケーションの作成、CloudFormation スタック] を選択します。
4. [Prepare a template] (テンプレートの準備) セクションで、オプションを選択します。[Use an existing template] (既存のテンプレートを使用) を選択する場合、[Choose a template] (テンプ

レートの選択) セクションのタブを使用して目的のテンプレートを見つけます。(他のオプションを選択した場合は、ウィザードを完了してテンプレートを準備します。)

5. テンプレート名の横にあるボタンを選択し、[次へ] を選択します。
6. [Specify template details] (テンプレートの詳細を指定) ページでテンプレートの詳細を確認し、必要なリソースが作成できるようにします。

   - (オプション) [Tags] (タグ) セクションで、テンプレートにタグキーの名前/値ペアを 1 つ、または複数適用します。
   - タグは、リソースに割り当てるオプションのメタデータです。タグを使用することで、目的、所有者、または環境などの異なる方法でリソースを分類できます。
   - [次へ] を選択します。
7. [Edit stack details] (スタック詳細の編集) ページでは、[Stack Name] (スタック名) には、テンプレートが作成するリソース、もしくはスタックの目的を識別しやすくするテンプレートの名前を入力します。

   - [Parameters] (パラメータ) セクションには、テンプレートで指定されたオプションおよび必須パラメータがすべて含まれています。各フィールドに 1 つ以上のパラメータを入力します。
   - (オプション) [Tags] (タグ) セクションでスタックにタグキーの名前/値ペアを 1 つ、または複数適用します。
   - (オプション) [Permissions] (アクセス許可) セクションで、AWS Identity and Access Management (IAM) ロール名または IAM Amazon リソースネーム (ARN) を指定します。システムは、指定されたサービスロールを使用して、スタックで指定されたすべてのリソースを作成します。IAM ロールを指定しなかった場合、AWS CloudFormation はユーザー認証情報からシステムが生成する一時的セッションを使用します。この IAM ロールの詳細については、AWS CloudFormation ユーザーガイドの「AWS CloudFormation サービスロール」を参照してください。
   - [Next] を選択します。
8. [Review and provision] (確認とプロビジョニング) ページで、スタックの詳細をすべて確認します。このページで [Edit] (編集) ボタンを選択して変更を行います。
9. [Provision stack] (スタックのプロビジョニング) を選択します。

Application Manager には、[CloudFormation stacks (CloudFormation のスタック)] ページと、スタックの作成とデプロイに関するステータスが表示されます。CloudFormation がスタックの作成とプロビジョニングに失敗した場合は、AWS CloudFormation ユーザーガイドで以下のトピックを参照してください。

- スタックステータスコード
- AWS CloudFormation のトラブルシューティング

スタックリソースがプロビジョニングされ、実行されると、ユーザーはリソースを作成した基盤となるサービスを使用してリソースを直接編集できます。例えば、Amazon Elastic Compute Cloud (Amazon EC2) コンソールを使用して、CloudFormation のスタックの一部として作成されたサーバーインスタンスを更新できます。一部の変更は偶発的になされますが、時間的制約のある操作上のイベントに対応するために意図的になされる場合もあります。しかし、CloudFormation の外部で行われた変更はスタックの更新または削除オペレーションを複雑にする可能性があります。ドリフト検出またはドリフトステータスを使用して、CloudFormation 管理外で設定変更がされたスタックリソースを識別できます。ドリフトステータスの詳細については、「スタックとリソースに対するアンマネージド型設定変更の検出」を参照してください。

Application Manager (コマンドライン) を使用して CloudFormationの スタックを作成

次の AWS Command Line Interface (AWS CLI) 手順を使用して、Systems Manager で SSM ドキュメントとして格納されている CloudFormation テンプレートを使用してスタックをプロビジョニングします。各###############をユーザー自身の情報に置き換えます。AWS CLIスタックを作成するその他の手順については、AWS CloudFormation ユーザーガイドの「スタックの作成」を参照してください。

開始する前に

まだ AWS CLI または AWS Tools for PowerShell をインストールして設定していない場合は、インストールして設定します。詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」および「AWS Tools for PowerShell のインストール」を参照してください。

Linux & macOS

```
aws cloudformation create-stack \
    --stack-name a_name_for_the_stack \
    --template-url "ssm-doc://arn:aws:ssm:Region:account_ID:document/template_name"
 \
```

Windows

```
aws cloudformation create-stack ^
     --stack-name a_name_for_the_stack ^
```

```
    --template-url "ssm-doc://arn:aws:ssm:Region:account_ID:document/template_name"
^
```

PowerShell

```
New-CFNStack `
    -StackName "a_name_for_the_stack" `
    -TemplateURL "ssm-doc://arn:aws:ssm:Region:account_ID:document/template_name" `
```

スタックの更新

Application Manager でスタックを直接編集することで、CloudFormation のスタックに更新をデプロイできます。直接更新する場合は、テンプレートまたは入力パラメータに対する更新を指定します。変更を保存してデプロイすると、CloudFormation が、指定された変更に応じて AWS リソースを変更します。

更新前に CloudFormation がスタックに加える変更をプレビューするには、変更セットを使用します。詳細については、AWS CloudFormation ユーザーガイドの「変更セットを使用したスタックの更新」を参照してください。

Application Manager で CloudFormation のスタックを更新するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Application Manager] を選択します。
3. アプリケーション名の横にあるラジオボタンを選択し、[アクション]、[スタックの更新] の順に選択します。
4. [Specify template source] (テンプレートのソースを指定) ページで、次のいずれかのオプションを選択し、[Next] (次へ) を選択します。
   - [Use the template code currently provisioned in the stack] (スタックで現在プロビジョニングされているテンプレートコードを使用) をクリックしてテンプレートを表示します。[Versions] (バージョン) リストを使用してテンプレートのバージョンを選択し、[Next] (次へ) を選択します。
   - [Switch to a different template] (別のテンプレートに切り替え) を選択して、スタックの新しいテンプレートを選択または作成します。
5. テンプレートの変更が完了したら、[Next] (次へ) を選択します。

6. [Edit stack details] (スタックの詳細の編集) ページでは、パラメータ、タグ、アクセス許可を編集できます。スタックの名前を変更することはできません。変更を行ってから、[Next] (次へ) を選択します。
7. [Review and provision] (確認とプロビジョニング) ページで、スタックのすべての詳細を確認し、[Provision stack] (スタックのプロビジョニング) を選択します。

Application Manager でのクラスターの操作

このセクションでは、AWS Systems Manager の構成要素である Application Manager で Amazon Elastic Container Service (Amazon ECS) および Amazon Elastic Kubernetes Service (Amazon EKS) コンテナクラスターの操作に役立つトピックを扱います

内容

- Application Manager での Amazon ECS の操作
- Application Manager での Amazon EKS の使用
- クラスター用のランブックの操作

Application Manager での Amazon ECS の操作

AWS Systems Manager のツールである Application Manager を使用すると、Amazon Elastic Container Service (Amazon ECS) クラスターインフラストラクチャを表示および管理できます。Application Manager は、クラスターの Amazon リソースネーム (ARN) をタグ値として使用して、タグを Amazon ECS クラスターに適用します。Application Manager は、クラスター内のコンピューティング、ネットワーキング、ストレージリソースのコンポーネントランタイムビューを提供します。

> **Note**
>
> Application Manager では、コンテナに関するオペレーション情報を管理および表示することはできません。管理および表示できるのは、Amazon ECS リソースをホストしているインフラストラクチャに関するオペレーション情報のみです。

このページで実行できるアクション

このページでは、次のアクションを実行できます。

- Amazon ECS でクラスターを開くには、[Manage cluster (クラスターの管理)] を選択します。

- クラスター内のリソースのリストを表示するには、[すべて表示] を選択します。
- Amazon CloudWatch でリソースアラームを表示するには、[View in CloudWatch (CloudWatch で表示)] を選択します。
- Amazon ECS でこれらのリソースを表示するには、[Manage nodes (ノードの管理)] または [Manager Fargate profiles (Manager Fargate プロファイル)] を選択します。
- リソースの詳細情報を作成されたコンソールに表示するには、リソース ID を選択します。
- クラスターに関連する OpsItems のリストを表示します。
- クラスター上で実行されたランブックの履歴を表示します。

ECS クラスターを開くには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Application Manager] を選択します。
3. [コンテナクラスター] セクションで、[ECS クラスター] を選択します。
4. リストからクラスターを選択します。Application Manager で、[Overview (概要)] タブが開きます。

Application Manager での Amazon EKS の使用

AWS Systems Manager のツールである Application Manager は、Amazon Elastic Kubernetes Service (Amazon EKS) と統合され、Amazon EKS クラスターのインフラストラクチャの正常性に関する情報を表示します。Application Manager は、クラスターの Amazon リソースネーム (ARN) をタグ値として使用して、タグを Amazon ECS クラスターに適用します。Application Manager は、クラスター内のコンピューティング、ネットワーキング、およびストレージリソースのコンポーネントランタイムビューを提供します。

> **Note**
>
> Application Manager では、Amazon EKS ポッドまたはコンテナに関するオペレーション情報を管理または表示することはできません。管理および表示できるのは、Amazon EKS リソースをホストしているインフラストラクチャに関するオペレーション情報のみです。

このページで実行できるアクション

このページでは、次のアクションを実行できます。

- Amazon EKS でクラスターを開くには、[Manage cluster (クラスターの管理)] を選択します。
- クラスター内のリソースのリストを表示するには、[すべて表示] を選択します。
- Amazon CloudWatch でリソースアラームを表示するには、[View in CloudWatch (CloudWatch で表示)] を選択します。
- Amazon EKS でこれらのリソースを表示するには、[Manage nodes (ノードの管理)] または [Manager Fargate profiles (Manager Fargate プロファイル)] を選択します。
- リソースの詳細情報を作成されたコンソールに表示するには、リソース ID を選択します。
- クラスターに関連する OpsItems のリストを表示します。
- クラスター上で実行されたランブックの履歴を表示します。

EKS クラスターのアプリケーションを開くには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Application Manager] を選択します。
3. [コンテナクラスター] セクションで、[EKS クラスター] を選択します。
4. リストからクラスターを選択します。Application Manager で、[Overview (概要)] タブが開きます。

クラスター用のランブックの操作

Systems Manager Automation ランブックを使用して、AWS Systems Manager のツールである Application Manager から AWS リソースに関する問題を修復できます。Application Manager クラスターから [Start runbook (ランブックの起動)] を選択すると、アプリケーション内のリソースのタイプに基づいて、ランブックのフィルタリングされたリストが表示されます。起動するランブックを選択すると、Systems Manager により [Execute automation document (オートメーションドキュメントの実行)] ページが開きます。

[開始する前に]

Application Manager からランブックを開始する前に、以下を実行してください。

- ランブックを開始するための適切なアクセス許可があることを確認してください。詳細については、「」を参照してくださいオートメーションの設定

- ランブックの開始に関するオートメーション手順のドキュメントを確認してください。詳細については、「Systems Manager Automation を使用した自動オペレーションを実行する」を参照してください。
- 複数のリソースでランブックを同時に開始する場合は、ターゲットとレート制御の使用に関するドキュメントを確認してください。詳細については、「自動オペレーションを大規模に実行する」を参照してください。

Application Manager からクラスターのランブックを開始するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Application Manager] を選択します。
3. [コンテナクラスター] セクションで、コンテナタイプを選択します。
4. リストからクラスターを選択します。Application Manager で、[Overview (概要)] タブが開きます。
5. [Runbooks] (ランブック) タブで [Start runbook] (ランブックの起動) をクリックします。Application Manager の新しいタブで [Execute automation document] (オートメーションドキュメントの実行) ページが開きます。[Execute automation document (オートメーションドキュメントの実行)] ページのオプションについては、Systems Manager Automation を使用した自動オペレーションを実行する を参照してください。

AWS Systems Manager Parameter Store

AWS Systems Manager のツールである Parameter Store は、設定データ管理と機密管理のための安全な階層型ストレージを提供します。パスワード、データベース文字列、Amazon Machine Image (AMI) ID、ライセンスコードなどのデータをパラメータ値として保存することができます。値はプレーンテキストまたは暗号化されたデータとして保存できます。パラメータの作成時に指定した一意の名前を使用して、スクリプト、コマンド、SSM ドキュメント、設定およびオートメーションワークフローの Systems Manager パラメータを参照できます。Parameter Store の使用を開始するには、Systems Manager コンソールを開きます。ナビゲーションペインで、[Parameter Store] を選択します。

Parameter Store も、Secrets Manager と統合されています。Parameter Store パラメータへの参照を既にサポートしている他の AWS のサービスを使用する際、Secrets Manager のシークレットを取得できます。詳しくは、「Parameter Store パラメータからの AWS Secrets Manager シークレットの参照」を参照してください。

> **Note**
>
> パスワードローテーションのライフサイクルを実装するには、 を使用しますAWS Secrets Manager Secrets Manager を使用すると、データベースの認証情報、API キー、その他のシークレットをそのライフサイクルを通してローテーション、管理、取得できます。詳細については、AWS Secrets Managerユーザーガイドの「AWS Secrets Manager とは」を参照してください。

Parameter Store はどのように組織にとってメリットになりますか?

Parameter Store は、以下の利点を提供します。

- セキュアでスケーラブルな、ホストされたシークレット管理サービスを使用します (管理が必要なサーバーはありません)。
- コードからデータを分離してセキュリティ体制を改善します。
- 設定データと暗号化された文字列を階層内に保存し、バージョンを追跡します。
- きめ細かいレベルでアクセスの制御と監査を行います。
- Parameter Store は AWS リージョン で複数のアベイラビリティーゾーンでホストされるため、パラメータは確実に保存してください。

Parameter Store はどのようなユーザーに適していますか?

- 設定データを一元的に管理したいすべての AWS のお客様。
- さまざまなログインや参照ストリームを保存したいソフトウェアデベロッパー。
- シークレットとパスワードが変更された場合、または変更されない場合に通知を受信する管理者。

Parameter Store の特徴は何ですか?

- 変更通知

  パラメータとパラメータポリシーの両方について、変更通知を設定し、自動化されたアクションを呼び出すことができます。詳しくは、「Parameter Store イベントに基づいた通知の設定またはアクションのトリガー」を参照してください。
- パラメータの整理

パラメータに個別にタグを付けると、そのタグに基づいてパラメータを識別できます。例えば、特定の環境または部門のパラメータをタグ付けできます。

- ラベルのバージョン

  ラベルを作成することで、パラメータのバージョンにエイリアスを関連付けることができます。ラベルは、バージョンが複数ある場合にパラメータバージョンの用途を覚えておくのに役立ちます。

- [Data validation] (データ検証)

  Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを指すパラメータを作成すると、Parameter Store がこれらのパラメータを検証して、期待されるリソースタイプを参照していること、リソースが存在すること、および顧客にリソースを使用するアクセス許可があることを確認します。例えば、`aws:ec2:image` データ型の値として Amazon Machine Image (AMI) ID を持つパラメータを作成すると、Parameter Store で非同期検証オペレーションが実行され、パラメータ値が AMI ID の書式設定要件を満たし、指定された AMI を AWS アカウント で使用できることが確認されます。

- シークレットの参照

  Parameter Store は AWS Secrets Manager と統合されたため、Parameter Store パラメータへの参照がすでにサポートされている他の AWS のサービスを使用する際に Secrets Manager のシークレットを取得できます。

- 他のアカウントとパラメータを共有

  オプションで、設定データを 1 つの AWS アカウント に一元管理し、パラメータにアクセスする必要のある他のアカウントとパラメータを共有できます。

- 他の AWS のサービスからアクセス可能

  他の Systems Manager ツールおよび AWS のサービスで Parameter Store パラメータを使用して、中央のストアからシークレットおよび設定データを取得できます。パラメータは、AWS Systems Manager のツールである Run Command、Automation、State Manager など、Systems Manager ツールで動作します。また、次のような他の多くの AWS のサービスでパラメータを参照することもできます。

  - Amazon Elastic Compute Cloud (Amazon EC2)
  - Amazon Elastic Container Service (Amazon ECS)
  - AWS Secrets Manager
  - AWS Lambda

  - AWS CloudFormation
  - AWS CodeBuild
  - AWS CodePipeline
  - AWS CodeDeploy
- 他の AWS のサービスとの統合

  暗号化、通知、モニタリング、監査のために、以下の AWS のサービスとの統合を設定します。

  - AWS Key Management Service (AWS KMS)
  - Amazon Simple Notification Service (Amazon SNS)
  - Amazon CloudWatch: 詳細については、「パラメータおよびパラメータポリシー用の EventBridge ルールを設定する」を参照してください。
  - Amazon EventBridge: 詳細については、「Amazon SNS 通知を使用した Systems Manager のステータス変更のモニタリング」および「リファレンス: Systems Manager 用の Amazon EventBridge イベントパターンとタイプ」を参照してください。
  - AWS CloudTrail詳細については、「」を参照してください。AWS Systems Manager による AWS CloudTrail API コールのログ記録

パラメータとは何ですか?

Parameter Store パラメータとは、テキストのブロック、名前のリスト、パスワード、AMI ID、ライセンスキーなど、Parameter Store に保存されるデータのことです。スクリプト、コマンド、SSM ドキュメントで、このデータを一元的かつ安全に参照できます。

パラメータを参照するときは、以下の規則を使用してパラメータ名を指定します。

{{ssm:*parameter-name*}}

> **Note**
>
> パラメータは、他のパラメータの値で参照またはネストすることはできません。パラメータ値に {{}} または {{ssm:*parameter-name*}} を含めることはできません。

Parameter Store では、String、StringList、SecureString という 3 タイプのパラメータがサポートされています。

1 つの例外を除いて、パラメータを作成または更新するときは、パラメータ値をプレーンテキストとして入力します。入力したテキストは Parameter Store によって検証されません。ただし、String パラメータの場合、データ型を aws:ec2:image として指定できます。Parameter Store によって、入力した値が Amazon EC2 AMI の適切な形式 (ami-12345abcdeEXAMPLE など) であることが検証されます。

パラメータタイプ: 文字列

デフォルトでは、String パラメータは、入力したテキストのブロックで構成されます。例：

- abc123
- Example Corp
-

パラメータタイプ: StringList

StringList パラメータには、以下の例に示すように、値のカンマ区切りリストを含めます。

Monday,Wednesday,Friday

CSV,TSV,CLF,ELF,JSON

パラメータタイプ: SecureString

SecureString パラメータは、セキュアな方法で保存および参照する必要がある機密データです。パスワードやライセンスキーなど、ユーザーがプレーンテキストで変更または参照しないデータがある場合は、SecureString データ型を使用してこれらのパラメータを作成します。

> **Important**
>
> String パラメータまたは StringList パラメータに機密データを保存しないでください。機密データを暗号化したままにする場合は、SecureString パラメータタイプのみを使用します。
> 詳細については、「」を参照してくださいAWS CLI を使用して SecureString パラメータを作成するには

次のシナリオでは SecureString パラメータを使用することをお勧めします。

- コマンド、関数、エージェントログ、または CloudTrail ログに値をプレーンテキストとして公開せずに、すべての AWS のサービスでデータ/パラメータを使用する。
- 機密データへのユーザーのアクセスを制御する。
- 機密データへのアクセスを監査する (CloudTrail)。
- 機密データの暗号化と独自の暗号化キーがアクセスの管理に必要である。

> **Important**
>
> SecureString パラメータの値のみが暗号化されます。パラメータ名、説明などのプロパティは暗号化されません。

SecureString パラメータタイプは、パスワード、アプリケーションシークレット、機密設定データ、保護するその他のタイプのデータなど、暗号化するテキストデータに使用できます。SecureString データは、AWS KMS キーを使用して暗号化および復号されます。AWS が提供するデフォルトの KMS キーを使用するか、独自の AWS KMS key を作成して使用することができます。(SecureString パラメータへのユーザーアクセスを制限する場合は自分の AWS KMS key を使用してください。 詳細については、「AWS のデフォルトキーとカスタマーマネージドキーを使用するための IAM アクセス権限」を参照してください。)

他の AWS のサービスと SecureString パラメータを使用することもできます。次の例では、GetParameters API を使用して Lambda 関数で SecureString パラメータを取得します。

```
import json
import boto3
ssm = boto3.client('ssm', 'us-east-2')
def get_parameters():
    response = ssm.get_parameters(
        Names=['LambdaSecureString'],WithDecryption=True
    )
    for parameter in response['Parameters']:
        return parameter['Value']

def lambda_handler(event, context):
    value = get_parameters()
    print("value1 = " + value)
    return value  # Echo back the first key value
```

AWS KMS の暗号化と料金

パラメータを作成するときに SecureString パラメータ型を選択すると、Systems Manager は AWS KMS を使用してパラメータ値を暗号化します。

> **Important**
>
> Parameter Store では、対称暗号化 KMS キーのみをサポートしています。非対称暗号化 KMS キーを使用してパラメータを暗号化することはできません。KMS キーが対称か非対称かを判断する方法については、「AWS Key Management Service デベロッパーガイド」の「対称キーと非対称 KMS キーの識別」を参照してください。

Parameter Store では、SecureString パラメータの作成には料金はかかりませんが、AWS KMS 暗号化の使用には料金がかかります。詳細については、「AWS Key Management Service の料金表」を参照してください。

AWS マネージドキーとカスタマー管理のキーの詳細については、AWS Key Management Service デベロッパーガイドの「AWS Key Management Service の概念」を参照してください。Parameter Store および AWS KMS の暗号化の詳細については、「AWS KMS で AWS Systems ManagerParameter Store を使用する方法」を参照してください。

> **Note**
>
> AWS マネージドキー を表示するには、AWS KMS DescribeKey オペレーションを使用します。この AWS Command Line Interface (AWS CLI) の例では、DescribeKey を使用して AWS マネージドキー を表示します。
>
> ```
> aws kms describe-key --key-id alias/aws/ssm
> ```

詳細情報

- Parameter Store で SecureString パラメータを作成して、ノードをドメインに結合する (PowerShell)
- Parameter Store を使用して CodeDeploy で機密情報と Config データに安全にアクセス
- Amazon EC2 Systems Manager Parameter Store についての興味深い記事

Parameter Store を設定する

AWS Systems Manager のツールである Parameter Store でパラメータを設定する前に、最初に AWS Identity and Access Management (IAM) ポリシーを設定して、アカウント内のユーザーに指定したアクションを実行するためのアクセス許可を付与します。

このセクションでは、IAM コンソールを使用してこれらのポリシーを手動で設定する方法、およびそれらをユーザーとユーザーグループに割り当てる方法について説明します。マネージドノード上で実行できるパラメータアクションを制御するためのポリシーを作成して割り当てることもできます。

また、このセクションでは、Systems Manager パラメータの変更に関する通知を受信するために Amazon EventBridge ルールを作成する方法についても説明します。さらに、Parameter Store の変更に基づき、AWS で他のアクションを呼び出す EventBridge ルールを使用することもできます。

内容

- IAM ポリシーを使用して Parameter Store パラメータへのアクセスを制限する
- パラメータ層の管理
- Parameter Store スループットの引き上げまたはリセット
- Parameter Store イベントに基づいた通知の設定またはアクションのトリガー

IAM ポリシーを使用して Parameter Store パラメータへのアクセスを制限する

AWS Identity and Access Management (IAM) を使用して、AWS Systems Manager パラメータへのアクセスを制限します。具体的には、次の API オペレーションへのアクセスを制限する IAM ポリシーを作成します。

- DeleteParameter
- DeleteParameters
- DescribeParameters
- GetParameter
- GetParameters
- GetParameterHistory
- GetParametersByPath
- PutParameter

IAM ポリシーを使用して Systems Manager パラメータへのアクセスを制限する場合は、制限付き IAM ポリシーを作成して使用することをお勧めします。たとえば、以下のポリシーでは、ユーザーは限られた一連のリソースに対して DescribeParameters および GetParameters API オペレーションを呼び出すことができます。つまり、prod-* で始まるすべてのパラメータに関する情報を取得し、使用することができます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeParameters"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:GetParameters"
            ],
            "Resource": "arn:aws:ssm:us-east-2:123456789012:parameter/prod-*"
        }
    ]
}
```

Important

ユーザーがパスへのアクセス許可を持つ場合、そのユーザーはそのパスのすべてのレベルにアクセスできます。たとえば、ユーザーがパス /a へのアクセス許可を持っている場合、ユーザーは /a/b にアクセスすることもできます。ユーザーが IAM でパラメータ /a/b へのアクセスを明示的に拒否された場合でも、/a に対して GetParametersByPath API オペレーションを再帰的に呼び出し、/a/b を表示できます。

信頼されている管理者には、以下の例のようなポリシーを使用することで、すべての Systems Manager パラメータ API オペレーションへのアクセスを許可できます。このポリシーにより、ユーザーは、dbserver-prod-* で始まるすべての本稼働パラメータにフルアクセスできます。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:PutParameter",
                "ssm:DeleteParameter",
                "ssm:GetParameterHistory",
                "ssm:GetParametersByPath",
                "ssm:GetParameters",
                "ssm:GetParameter",
                "ssm:DeleteParameters"
            ],
            "Resource": "arn:aws:ssm:us-east-2:123456789012:parameter/dbserver-prod-*"
        },
        {
            "Effect": "Allow",
            "Action": "ssm:DescribeParameters",
            "Resource": "*"
        }
    ]
}
```

アクセス許可を拒否する

各 API は一意であり、個別に許可または拒否できる個別の操作とアクセス許可があります。ポリシー内の明示的な拒否は、許可に優先します。

> **Note**
>
> デフォルトの AWS Key Management Service (AWS KMS) キーには、AWS アカウント 内のすべての IAM プリンシパルに対する `Decrypt` アクセス許可があります。アカウントの `SecureString` パラメータに対して異なるアクセスレベルを使用する場合は、デフォルトのキーを使用することはお勧めしません。

パラメータ値を取得するすべての API オペレーションの動作を同じにする場合は、ポリシーの `GetParameter*` ようなパターンを使用できます。次に、`GetParameter` で始まるすべてのパラメータについて、`GetParameters`、`GetParameterHistory`、`GetParametersByPath`、および `prod-*` を拒否する例を示します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ssm:GetParameter*"
            ],
            "Resource": "arn:aws:ssm:us-east-2:123456789012:parameter/prod-*"
        }
    ]
}
```

次に、prod-* で始まるすべてのパラメータに対してユーザーが他のコマンドを実行できるようにしながら、一部のコマンドを拒否する例を示します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ssm:PutParameter",
                "ssm:DeleteParameter",
                "ssm:DeleteParameters",
                "ssm:DescribeParameters"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:GetParametersByPath",
                "ssm:GetParameters",
                "ssm:GetParameter",
                "ssm:GetParameterHistory"
            ],
            "Resource": "arn:aws:ssm:us-east-2:123456789012:parameter/prod-*"
        }
    ]
}
```

> **Note**
>
> パラメータ履歴には、現在のパラメータを含むすべてのパラメータバージョンが含まれます。したがって、GetParameter、GetParameters、および GetParameterByPath に対するアクセス許可が拒否され、GetParameterHistory に対するアクセス許可が認められている場合、SecureString を使用して、GetParameterHistory パラメータを含む現在のパラメータを表示できます。

特定のパラメータのみノードでの実行を許可する

指定したパラメータのみをマネージドノードが実行できるようにアクセスをコントロールできます。

パラメータを作成するときに SecureString パラメータ型を選択した場合、Systems Manager は AWS KMS を使用してパラメータ値を暗号化します。AWS KMS は AWS マネージドキー または カスタマーマネージドキーを使用して値を暗号化します。AWS KMS と AWS KMS key の詳細については、「AWS Key Management Service デベロッパーガイド」を参照してください。

AWS マネージドキー を表示するには、以下のコマンドを AWS CLI から実行します。

```
aws kms describe-key --key-id alias/aws/ssm
```

以下の例では、「prod-」で始まるパラメータに対してのみ、ノードがパラメータの値を取得できるようにしています。パラメータが SecureString の場合、ノードは AWS KMS を使用してその文字列を復号化します。

> **Note**
>
> 以下の例のように、IAM でインスタンスポリシーはインスタンスロールに割り当てられます。ユーザーとインスタンスにポリシーを割り当てる方法を含め、Systems Manager の機能へのアクセスを設定する方法の詳細については、「Systems Manager を利用した EC2 インスタンスの管理」を参照してください。

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

```
            "Action": [
                "ssm:GetParameters"
            ],
            "Resource": [
                "arn:aws:ssm:us-east-2:123456789012:parameter/prod-*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": [
                "arn:aws:kms:us-east-2:123456789012:key/4914ec06-e888-4ea5-
a371-5b88eEXAMPLE"
            ]
        }
    ]
}
```

AWS のデフォルトキーとカスタマーマネージドキーを使用するための IAM アクセス権限

Parameter Store SecureString パラメータは、AWS KMS キーを使用して暗号化および復号化されます。AWS が提供する AWS KMS key またはデフォルトの KMS キーを使用して、SecureString パラメータを暗号化することを選択できます。

カスタマーマネージドキーを使用する場合、パラメータまたはパラメータパスへのユーザーアクセスを許可する IAM ポリシーによって、キーに対する明示的な kms:Encrypt アクセス許可を提供する必要があります。例えば、次のポリシーでは、指定した AWS リージョン と AWS アカウント で「prod-」で始まる SecureString パラメータを作成、更新、表示できます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:PutParameter",
                "ssm:GetParameter",
                "ssm:GetParameters"
            ],
            "Resource": [
                "arn:aws:ssm:us-east-2:111122223333:parameter/prod-*"
```

```
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:Encrypt",
                "kms:GenerateDataKey"
  1
            ],
            "Resource": [
                "arn:aws:kms:us-
east-2:111122223333:key/1234abcd-12ab-34cd-56ef-12345EXAMPLE"
            ]
        }
    ]
}
```

[1]指定されたカスタマーマネージドキーを使用して暗号化された詳細パラメータを作成するには、kms:GenerateDataKey アクセス許可が必要です。

対照的に、カスタマーアカウント内のすべてのユーザーは、デフォルトの AWS マネージドキーにアクセスできます。このデフォルトキーを使用して SecureString パラメータを暗号化し、ユーザーが SecureString パラメータを操作しないようにする場合は、次のポリシー例に示すように、IAM ポリシーでデフォルトキーへのアクセスを明示的に拒否する必要があります。

> **Note**
>
> デフォルトのキーの Amazon リソースネーム (ARN) は、AWS KMS コンソールの [AWS マネージドキー] ページで確認できます。デフォルトのキーは、[エイリアス] 列の aws/ssm で識別されるキーです。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
```

```
            ],
            "Resource": [
                "arn:aws:kms:us-east-2:111122223333:key/abcd1234-ab12-cd34-ef56-
abcdeEXAMPLE"
            ]
        }
    ]
}
```

アカウントの SecureString パラメータに対するきめ細かいアクセス制御が必要な場合は、カスタマーマネージドキーを使用して、これらのパラメータへのアクセスを保護および制限する必要があります。また、AWS CloudTrail を使用して SecureString パラメータのアクティビティを監視することをお勧めします。

詳細については、以下のトピックを参照してください。

- IAM ユーザーガイドの「ポリシー評価ロジック」
- 「AWS Key Management Service デベロッパーガイド」の「AWS KMS の主要ポリシーを使用する」
- AWS CloudTrail ユーザーガイドの「CloudTrail イベント履歴でのイベントの表示」

パラメータ層の管理

AWS Systems Manager のツールである Parameter Store には、スタンダードパラメータとアドバンストパラメータが含まれています。スタンダードパラメータ階層 (デフォルト階層) またはアドバンストパラメータ階層を使用するようパラメータを個別に設定します。

スタンダードパラメータをアドバンストパラメータに変更することはできますが、アドバンストパラメータをスタンダードパラメータに変更することはできません。アドバンストパラメータをスタンダードパラメータに戻すと、システムはパラメータのサイズを 8 KB から 4 KB に切り捨て、データが失われるためです。元に戻すと、パラメータにアタッチされたポリシーも削除されます。また、アドバンストパラメータはスタンダードパラメータよりもさまざまな暗号化形式を使用します。詳細については、AWS Key Management Service デベロッパーガイドの「AWS Systems ManagerParameter Store が AWS KMS を使用する方法」を参照してください。

アドバンストパラメータが不要になった場合、またはアドバンストパラメータの料金を抑えたい場合は、アドバンストパラメータを削除して新しいスタンダードパラメータとして再作成します。

以下の表では、階層の違いについて説明しています。

	スタンダード	アドバンスト
許可されるパラメータの合計数 (AWS アカウント および AWS リージョン あたり)	10,000	100,000
パラメータ値の最大サイズ	4 KB	8 KB
パラメータポリシーの使用可否	いいえ	はい 詳細については、Parameter Store でのパラメータポリシーの割り当てを参照してください
Cost	追加料金なし	料金対象 詳細については、「Parameter Store 向けの AWS Systems Manager 料金」を参照してください。

トピック

- デフォルトのパラメータ階層の指定
- スタンダードパラメータをアドバンストパラメータに変更する

デフォルトのパラメータ階層の指定

パラメータを作成または更新するリクエスト (つまり、`PutParameter` オペレーション) では、リクエストで使用するパラメータ階層を指定できます。以下に示しているのは、AWS Command Line Interface (AWS CLI) を使用した例です。

Linux & macOS

```
aws ssm put-parameter \
    --name "default-ami" \
```

```
    --type "String" \
    --value "t2.micro" \
    --tier "Standard"
```

Windows

```
aws ssm put-parameter ^
    --name "default-ami" ^
    --type "String" ^
    --value "t2.micro" ^
    --tier "Standard"
```

リクエストで階層を指定するたびに、Parameter Store はリクエストに応じてパラメータを作成または更新します。ただし、リクエストで階層を明示的に指定しない場合、デフォルトの Parameter Store 階層設定によって、パラメータが作成される階層が決まります。

スタンダードパラメータ階層は、Parameter Store の使用を開始するときのデフォルトの階層です。アドバンストパラメータ階層を使用する場合、デフォルトとして次のいずれかを指定できます。

- アドバンスト: このオプションでは、パラメータストアはすべてのリクエストをアドバンストパラメータとして評価します。
- Intelligent-Tiering: このオプションでは、Parameter Store は各リクエストを評価して、パラメータがスタンダードパラメータかアドバンストパラメータかを判断します。

  リクエストに詳細パラメータを必要とするオプションが含まれていない場合、パラメータは標準パラメータ階層で作成されます。アドバンストパラメータを必要とする 1 つ以上のオプションがリクエストに含まれている場合、Parameter Store はアドバンストパラメータ階層でパラメータを作成します。

Intelligent-Tiering の利点

以下は、デフォルトの階層として Intelligent-Tiering を選択する理由です。

コスト管理 - Intelligent-Tiering は、高度なパラメータが絶対に必要な場合を除き、常に標準パラメータを作成することで、パラメータ関連のコストを管理するのに役立ちます。

アドバンストパラメータ階層への自動アップグレード - 標準パラメータをアドバンストパラメータにアップグレードする必要があるコードに変更を加えると、Intelligent-Tiering によって変換が処理されます。アップグレードを処理するためにコードを変更する必要はありません。

自動アップグレードの例をいくつか示します。

- AWS CloudFormation テンプレートは、実行時に多数のパラメータをプロビジョニングします。このプロセスによって標準パラメータ階層で 10,000 個のパラメータのクォータに達した場合、Intelligent-Tiering によって自動的にアドバンストパラメータ階層にアップグレードされ、AWS CloudFormation プロセスは中断されません。
- 証明書値をパラメータに保存し、証明書値を定期的にローテーションします。コンテンツは標準パラメータ階層の 4 KB のクォータを下回ります。代替証明書の値が 4 KB を超える場合、Intelligent-Tiering は自動的にパラメータをアドバンストパラメータ階層にアップグレードします。
- 多数の既存の標準パラメータをパラメータポリシーに関連付ける必要があります。これには、アドバンストパラメータ階層が必要です。パラメータを更新するすべての呼び出しに `--tier Advanced` オプションを含める必要はなく、Intelligent-Tiering は自動的にパラメータをアドバンストパラメータ階層にアップグレードします。Intelligent-Tiering オプションは、アドバンストパラメータ階層の基準が導入されるたびに、パラメータを標準からアドバンストにアップグレードします。

アドバンストパラメータを必要とするオプションには、以下が含まれます。

- パラメータのコンテンツサイズが 4 KB を超えています。
- パラメータは、パラメータポリシーを使用します。
- 現在の AWS リージョン では、10,000 を超えるパラメータが既に AWS アカウント に存在します。

デフォルトの階層オプション

デフォルトとして指定できる階層オプションには、以下が含まれます。

- スタンダード – スタンダードパラメータ階層は、Parameter Store の使用を開始するときのデフォルトの階層です。スタンダードパラメータ階層を使用すると、AWS アカウント の AWS リージョン ごとに 10,000 個のパラメータを作成できます。各パラメータのコンテンツサイズは最大 4 KB と等しくできます。標準パラメータはパラメータポリシーをサポートしていません。標準パラメータ階層の使用に追加料金はかかりません。デフォルト階層として [標準] を選択すると、Parameter Store は常に、階層を指定しないリクエストに対して標準パラメータの作成を試みます。
- アドバンスト – アドバンストパラメータ階層を使用して、AWS アカウント の AWS リージョン ごとに最大 100,000 個のパラメータを作成します。各パラメータのコンテンツサイズは、最大 8 KB

と等しくできます。アドバンストパラメータはパラメータポリシーをサポートします。パラメータを共有するには、そのパラメータが詳細パラメータ階層に含まれている必要があります。アドバンストパラメータ階層の使用には料金が発生します。詳細については、「Parameter Store 向けの AWS Systems Manager 料金」を参照してください。デフォルト階層として [アドバンスト] を選択すると、Parameter Store は階層を指定しないリクエストに対して常にアドバンストパラメータの作成を試みます。

> **Note**
>
> アドバンストパラメータ階層を選択する場合、作成するアドバンストパラメータについて AWS がアカウントに課金することを明示的に承認します。

- Intelligent-Tiering – Intelligent-Tiering オプションを使用して、Parameter Store は、リクエストのコンテンツに基づいて、スタンダードパラメータ階層またはアドバンストパラメータ階層のどちらを使用するか決定します。例えば、4 KB 未満のコンテンツを持つパラメータを作成するコマンドを実行し、AWS アカウント の現在の AWS リージョン に存在するパラメータが 10,000 個未満であり、パラメータポリシーを指定しない場合、標準パラメータが作成されます。4 KB を超えるコンテンツを含むパラメータを作成するコマンドを実行する場合、AWS アカウント の現在の AWS リージョン に 10,000 個を超えるパラメータが既にある場合、またはパラメータポリシーを指定すると、アドバンストパラメータが作成されます。

  > **Note**
  >
  > Intelligent-Tiering を選択する場合、作成したアドバンストパラメータについて AWS がアカウントに課金することを明示的に承認する必要があります。

デフォルトの Parameter Store 階層設定はいつでも変更できます。

デフォルトの Parameter Store 階層を指定するアクセス許可の設定

次のいずれかを実行して、Parameter Store のデフォルトパラメータ階層を変更するアクセス許可が AWS Identity and Access Management (IAM) にあることを確認します。

- `AdministratorAccess` ポリシーが IAM エンティティ (ユーザー、グループ、ロールなど) にアタッチされていることを確認します。
- 次の API オペレーションを使用して、デフォルト階層設定を変更するアクセス権限があることを確認します。

- GetServiceSetting
- UpdateServiceSetting
- ResetServiceSetting

IAM エンティティに次のアクセス許可を付与して、ユーザーが AWS アカウント の特定の AWS リージョン でパラメータのデフォルト階層の設定を表示および変更できるようにします。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:GetServiceSetting"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:UpdateServiceSetting"
            ],
            "Resource": "arn:aws:ssm:region:account-id:servicesetting/ssm/parameter-
store/default-parameter-tier"
        }
    ]
}
```

管理者は、次のアクセス許可を割り当てることで、読み取り専用のアクセス許可を指定することができます。

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

```
        {
            "Effect": "Deny",
            "Action": [
                "ssm:ResetServiceSetting",
                "ssm:UpdateServiceSetting"
            ],
            "Resource": "*"
        }
    ]
}
```

アクセス権限を付与するにはユーザー、グループ、またはロールにアクセス許可を追加します。

- AWS IAM Identity Center のユーザーとグループ:

  アクセス許可セットを作成します。「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」の手順に従ってください。
- IAM 内で、ID プロバイダーによって管理されているユーザー:

  ID フェデレーションのロールを作成します。詳細については「IAM ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) 用のロールを作成する」を参照してください。
- IAM ユーザー:
  - ユーザーが担当できるロールを作成します。手順については「IAM ユーザーガイド」の「IAM ユーザーのロールの作成」を参照してください。
  - (お奨めできない方法) ポリシーをユーザーに直接アタッチするか、ユーザーをユーザーグループに追加します。詳細については「IAM ユーザーガイド」の「ユーザー (コンソール) へのアクセス権限の追加」を参照してください。

コンソールを使用してデフォルトの Parameter Store 階層を指定または変更する

次の手順は、Systems Manager コンソールを使用して、現在の AWS アカウント と AWS リージョン のデフォルトのパラメータ階層を指定または変更する方法を示しています。

> **Tip**
>
> まだパラメータを作成していない場合は、AWS Command Line Interface (AWS CLI) または AWS Tools for Windows PowerShell を使用してデフォルトのパラメータ層を変更できます。詳細については、「AWS CLI を使用したデフォルトの Parameter Store 階層の指定または変

更」および「デフォルトの Parameter Store 階層の指定または変更 (PowerShell)」を参照してください。

デフォルトの Parameter Store 階層を指定または変更するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Parameter Store] を選択します。
3. [Settings] タブを選択します。
4. [Change default tier (デフォルト階層の変更)] を選択します。
5. 次のいずれかのオプションを選択します。

   - スタンダード
   - アドバンスト
   - [Intelligent-Tiering]

   これらのオプションについては、「デフォルトのパラメータ階層の指定」を参照してください。
6. メッセージを確認したら、[確認] を選択します。

デフォルト階層の設定を後で変更する場合は、この手順を繰り返し、別のデフォルト階層オプションを指定します。

AWS CLI を使用したデフォルトの Parameter Store 階層の指定または変更

次の手順では、AWS CLI を使用して、現在の AWS アカウント と AWS リージョン のデフォルトのパラメータ階層の設定を変更する方法を示します。

AWS CLI を使用してデフォルトの Parameter Store 階層を指定または変更するには

1. AWS CLI を開き、次のコマンドを実行して、AWS アカウント の特定の AWS リージョン のデフォルトのパラメータ階層設定を変更します。

```
aws ssm update-service-setting --setting-id arn:aws:ssm:region:account-id:servicesetting/ssm/parameter-store/default-parameter-tier --setting-value tier-option
```

region は、米国東部 (オハイオ) リージョンの us-east-2 のように、AWS Systems Manager でサポートされている AWS リージョン の識別子を表します。サポートされている *region* 値の一覧については、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」にある Region 列を参照してください。

******* の値は、Standard、Advanced、および Intelligent-Tiering です。これらのオプションについては、「デフォルトのパラメータ階層の指定」を参照してください。

コマンドが成功した場合、出力はありません。

2. 次のコマンドを実行して、現在の AWS アカウント と AWS リージョン の Parameter Store で現在のデフォルトパラメータ層のサービス設定を表示します。

```
aws ssm get-service-setting --setting-id arn:aws:ssm:region:account-
id:servicesetting/ssm/parameter-store/default-parameter-tier
```

システムは以下のような情報を返します。

```
{
    "ServiceSetting": {
        "SettingId": "/ssm/parameter-store/default-parameter-tier",
        "SettingValue": "Advanced",
        "LastModifiedDate": 1556551683.923,
        "LastModifiedUser": "arn:aws:sts::123456789012:assumed-role/Administrator/
Jasper",
        "ARN": "arn:aws:ssm:us-east-2:123456789012:servicesetting/ssm/parameter-
store/default-parameter-tier",
        "Status": "Customized"
    }
}
```

デフォルトの階層設定を再び変更する場合は、この手順を繰り返し、別の SettingValue オプションを指定します。

デフォルトの Parameter Store 階層の指定または変更 (PowerShell)

次の手順では、Tools for Windows PowerShell を使用して、Amazon Web Services アカウントの特定の AWS リージョン のデフォルトのパラメータ階層の設定を変更する方法を示します。

PowerShell を使用してデフォルトの Parameter Store 階層を指定または変更するには

1. AWS Tools for PowerShell (Tools for PowerShell) を使用して、現在の AWS アカウント と AWS リージョン の Parameter Store のデフォルト階層を変更します。

```
Update-SSMServiceSetting -SettingId "arn:aws:ssm:region:account-id:servicesetting/
ssm/parameter-store/default-parameter-tier" -SettingValue "tier-option" -
Region region
```

   region は、米国東部 (オハイオ) リージョンの us-east-2 のように、AWS Systems Manager でサポートされている AWS リージョン の識別子を表します。サポートされている *region* 値の一覧については、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」にある Region 列を参照してください。

   ******* の値は、Standard、Advanced、および Intelligent-Tiering です。これらのオプションについては、「デフォルトのパラメータ階層の指定」を参照してください。

   コマンドが成功した場合、出力はありません。

2. 次のコマンドを実行して、現在の AWS アカウント と AWS リージョン の Parameter Store で現在のデフォルトパラメータ層のサービス設定を表示します。

```
Get-SSMServiceSetting -SettingId "arn:aws:ssm:region:account-id:servicesetting/ssm/
parameter-store/default-parameter-tier" -Region region
```

   region は、米国東部 (オハイオ) リージョンの us-east-2 のように、AWS Systems Manager でサポートされている AWS リージョン の識別子を表します。サポートされている *region* 値の一覧については、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」にある Region 列を参照してください。

   システムは以下のような情報を返します。

```
ARN : arn:aws:ssm:us-east-2:123456789012:servicesetting/ssm/parameter-store/
default-parameter-tier
LastModifiedDate : 4/29/2019 3:35:44 PM
LastModifiedUser : arn:aws:sts::123456789012:assumed-role/Administrator/Jasper
SettingId        : /ssm/parameter-store/default-parameter-tier
SettingValue     : Advanced
Status           : Customized
```

デフォルトの階層設定を再び変更する場合は、この手順を繰り返し、別の `SettingValue` オプションを指定します。

スタンダードパラメータをアドバンストパラメータに変更する

既存のスタンダードパラメータをアドバンストパラメータに変更するには、次の手順を使用します。新しい詳細パラメータの作成方法については、「Systems Manager での Parameter Store パラメータの作成」を参照してください。

スタンダードパラメータをアドバンストパラメータに変更するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Parameter Store] を選択します。
3. パラメータを選択してから、[編集] を選択します。
4. [説明] に、このパラメータに関する情報を入力します。
5. [Advanced] を選択します。
6. [値]に、このパラメータの値を入力します。アドバンストパラメータの最大値は 8 KB に制限されます。
7. [Save changes] を選択します。

Parameter Store スループットの引き上げまたはリセット

Parameter Store のスループットを増やすと、AWS Systems Manager のツールである Parameter Store が処理できる 1 秒あたりのトランザクション (TPS) の最大数が増加します。スループットが引き上げられると、複数のパラメータに同時アクセスが必要なアプリケーションとワークロードをサポートするため、高いボリュームで Parameter Store を運用できます。[Settings] (設定) タブでは、最大スループットまでクォータを引き上げることができます。

Parameter Store のスループット設定は、現在の AWS アカウント と AWS リージョン におけるすべての (IAM) ユーザーによって作成されたすべてのトランザクションに適用されます。スループット設定は、スタンダードおよびアドバンストのパラメータに適用されます。

> **Note**
>
> 通常、更新は Service Quotas にすぐに表示されます。まれに、更新が反映されるまでに最大 24 時間かかることがあります。

最大スループットのデフォルトと上限の詳細については、「AWS Systems Manager エンドポイントとクォータ」を参照してください。

スループットのクォータを引き上げると、AWS アカウント に追加料金が発生します。詳細については、AWS Systems Manager 料金を参照してください。

トピック

- Parameter Store のスループットを変更するアクセス許可を設定する
- コンソールを使用したスループットの引き上げまたはリセット
- AWS CLI を使用したスループットの引き上げまたはリセット
- スループットの引き上げまたはリセット (PowerShell)

Parameter Store のスループットを変更するアクセス許可を設定する

次のいずれかを実行して、Parameter Store のスループットを変更する IAM のアクセス許可があることを確認します。

- `AdministratorAccess` ポリシーが、IAM エンティティ (ユーザー、グループ、またはロール) にアタッチされていることを確認します。
- 次の API オペレーションを使用して、スループットサービス設定を変更する権限があることを確認します。
  - GetServiceSetting
  - UpdateServiceSetting
  - ResetServiceSetting

IAM エンティティに次のアクセス許可を付与して、ユーザーが AWS アカウント の特定の AWS リージョン でパラメータのスループット設定を表示および変更できるようにします。

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

```
        {
            "Effect": "Allow",
            "Action": [
                "ssm:UpdateServiceSetting"
            ],
            "Resource": "arn:aws:ssm:region:account-id:servicesetting/ssm/parameter-
store/high-throughput-enabled"
        }
    ]
}
```

管理者は、次のアクセス許可を割り当てることで、読み取り専用のアクセス許可を指定することができます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:GetServiceSetting"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "ssm:ResetServiceSetting",
                "ssm:UpdateServiceSetting"
            ],
            "Resource": "*"
        }
    ]
}
```

アクセス権限を付与するにはユーザー、グループ、またはロールにアクセス許可を追加します。

- AWS IAM Identity Center のユーザーとグループ:

  アクセス許可セットを作成します。「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」の手順に従ってください。
- IAM 内で、ID プロバイダーによって管理されているユーザー:

ID フェデレーションのロールを作成します。詳細については「IAM ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) 用のロールを作成する」を参照してください。

- IAM ユーザー:
  - ユーザーが担当できるロールを作成します。手順については「IAM ユーザーガイド」の「IAM ユーザーのロールの作成」を参照してください。
  - (お奨めできない方法) ポリシーをユーザーに直接アタッチするか、ユーザーをユーザーグループに追加します。詳細については「IAM ユーザーガイド」の「ユーザー (コンソール) へのアクセス権限の追加」を参照してください。

コンソールを使用したスループットの引き上げまたはリセット

次の手順では、Systems Manager コンソールを使用して Parameter Store が現在の AWS アカウント と AWS リージョン に対して処理できる 1 秒あたりのトランザクション数を引き上げる方法を示します。スループットの向上が不要になった場合や追加の料金を回避したい場合に標準の設定に戻す方法も示します。

コンソールを使用して Parameter Store スループットを増加またはリセットするには

> **Tip**
>
> パラメータをまだ作成していない場合は、AWS Command Line Interface (AWS CLI) または AWS Tools for Windows PowerShell を使用してスループットを増加することができます。詳細については、「AWS CLI を使用したスループットの引き上げまたはリセット」および「スループットの引き上げまたはリセット (PowerShell)」を参照してください。

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Parameter Store] を選択します。
3. [Settings] (設定) タブを選択します。
4. スループットを上げるには、[上限をセットする] を選択します。

   -または-

   デフォルトの上限に戻すには、[上限をリセットする] を選択します。
5. 上限を上げる場合は、次の手順を実行します。

- [この設定を変更すると AWS アカウント に料金が発生することを承諾します] のチェックボックスを選択します。
- [Set limit (制限の設定)] を選択します。

-または-

上限をデフォルトにリセットする場合は、次の手順を実行します。

- [デフォルトのスループット上限にリセットすると、Parameter Store で 1 秒あたりに処理されるトランザクションが少なくなることを承諾します] のチェックボックスを選択します。
- [上限をリセットする] を選択します。

AWS CLI を使用したスループットの引き上げまたはリセット

次の手順では、AWS CLI を使用して、Parameter Store が現在の AWS アカウント と AWS リージョン に対して処理できる 1 秒あたりのトランザクションの数を増やす方法を示します。デフォルトの上限に戻すこともできます。

AWS CLI を使用して Parameter Store のスループットを向上させるには

1. AWS CLI を開き、次のコマンドを実行して、現在の AWS アカウント と AWS リージョン で Parameter Store が処理できる 1 秒あたりのトランザクション数を増やします。

```
aws ssm update-service-setting --setting-id arn:aws:ssm:region:account-
id:servicesetting/ssm/parameter-store/high-throughput-enabled --setting-value true
```

   コマンドが成功した場合、出力はありません。

2. 次のコマンドを実行して、現在の AWS アカウント と AWS リージョン の Parameter Store で現在のスループットサービス設定を表示します。

```
aws ssm get-service-setting --setting-id arn:aws:ssm:region:account-
id:servicesetting/ssm/parameter-store/high-throughput-enabled
```

   システムは以下のような情報を返します。

```
{
    "ServiceSetting": {
```

```
        "SettingId": "/ssm/parameter-store/high-throughput-enabled",
        "SettingValue": "true",
        "LastModifiedDate": 1556551683.923,
        "LastModifiedUser": "arn:aws:sts::123456789012:assumed-role/Administrator/
Jasper",
        "ARN": "arn:aws:ssm:us-east-2:123456789012:servicesetting/ssm/parameter-
store/high-throughput-enabled",
        "Status": "Customized"
    }
}
```

スループットの向上が不要になった場合や追加の料金を節約したい場合は、標準の設定に戻すことができます。設定を元に戻すには、次のコマンドを実行します。

```
aws ssm reset-service-setting --setting-id arn:aws:ssm:region:account-
id:servicesetting/ssm/parameter-store/high-throughput-enabled
```

```
{
    "ServiceSetting": {
        "SettingId": "/ssm/parameter-store/high-throughput-enabled",
        "SettingValue": "false",
        "LastModifiedDate": 1555532818.578,
        "LastModifiedUser": "System",
        "ARN": "arn:aws:ssm:us-east-2:123456789012:servicesetting/ssm/parameter-store/
high-throughput-enabled",
        "Status": "Default"
    }
}
```

スループットの引き上げまたはリセット (PowerShell)

次の手順は、Tools for Windows PowerShell を使用して、現在の AWS アカウント と AWS リージョン に対して Parameter Store が処理できる 1 秒あたりのトランザクション数を引き上げる増やす方法を示しています。デフォルトの上限に戻すこともできます。

PowerShell を使用して Parameter Store のスループットを向上させるには

1. AWS Tools for PowerShell (Tools for PowerShell) を使用して、現在の AWS アカウント と AWS リージョン の Parameter Store のスループットを引き上げます。

```
Update-SSMServiceSetting -SettingId "arn:aws:ssm:region:account-id:servicesetting/
ssm/parameter-store/high-throughput-enabled" -SettingValue "true" -Region region
```

コマンドが成功した場合、出力はありません。

2. 次のコマンドを実行して、現在の AWS アカウント と AWS リージョン の Parameter Store で現在のスループットサービス設定を表示します。

```
Get-SSMServiceSetting -SettingId "arn:aws:ssm:region:account-id:servicesetting/ssm/
parameter-store/high-throughput-enabled" -Region region
```

システムは以下のような情報を返します。

```
ARN              : arn:aws:ssm:us-east-2:123456789012:servicesetting/ssm/parameter-
store/high-throughput-enabled
LastModifiedDate : 4/29/2019 3:35:44 PM
LastModifiedUser : arn:aws:sts::123456789012:assumed-role/Administrator/Jasper
SettingId        : /ssm/parameter-store/high-throughput-enabled
SettingValue     : true
Status           : Customized
```

スループットの向上が不要になった場合や追加の料金を節約したい場合は、標準の設定に戻すことができます。設定を元に戻すには、次のコマンドを実行します。

```
Reset-SSMServiceSetting -SettingId "arn:aws:ssm:region:account-id:servicesetting/ssm/
parameter-store/high-throughput-enabled" -Region region
```

システムは以下のような情報を返します。

```
ARN              : arn:aws:ssm:us-east-2:123456789012:servicesetting/ssm/parameter-
store/high-throughput-enabled
LastModifiedDate : 4/17/2019 8:26:58 PM
LastModifiedUser : System
SettingId        : /ssm/parameter-store/high-throughput-enabled
SettingValue     : false
Status           : Default
```

Parameter Store イベントに基づいた通知の設定またはアクションのトリガー

このセクションのトピックでは、Amazon EventBridge および Amazon Simple Notification Service (Amazon SNS) を使用して、AWS Systems Manager のパラメータに変更があったことの通知を受け取る方法について説明します。パラメータまたはパラメータラベルのバージョンが作成、更新、または削除されたときに通知する EventBridge ルールを作成できます。イベントは、ベストエフォートベースで出力されます。パラメータの有効期限切れ、期限切れ間近、または指定された期間中に変更されていないなど、パラメータポリシーに関する変更またはステータスに関する通知を受信することができます。

> **Note**
>
> パラメータポリシーは、高度なパラメータ階層を使用するパラメータに利用できます。料金が適用されます。詳細については、「Parameter Store でのパラメータポリシーの割り当て」および「パラメータ層の管理」を参照してください。

本セクションのトピックでは、特定のパラメータイベントに対してターゲット上で他のアクションを開始する方法も説明しています。たとえば、有効期限が切れたか、削除された場合に、そのパラメータを自動的に再作成する AWS Lambda 関数を実行することができます。また、データベースパスワードが更新された際に Lambda 関数を起動する通知をセットアップすることもできます。Lambda 関数は、データベース接続のリセットまたは新しいパスワードでの再接続を強制できます。EventBridge は、Run Command コマンドの実行と Automation の実行、およびその他多くの AWS のサービスでのアクションもサポートしています。Run Command と Automation はどちらも AWS Systems Manager のツールです。詳細については、「Amazon EventBridge ユーザーガイド」を参照してください。

開始する前に

作成したルールのターゲットアクションを指定するために必要なリソースを作成します。例えば、作成したルールが通知の送信用である場合は、まず Amazon SNS トピックを作成します。詳細については、「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNS の使用開始」を参照してください。

パラメータおよびパラメータポリシー用の EventBridge ルールを設定する

このトピックは、次のセクションで構成されています。

- AWS アカウント の 1 つ以上のパラメータに発生したイベントに基づき、ターゲットを呼び出す EventBridge ルールを作成する方法。

- AWS アカウント の 1 つ以上のパラメータポリシーに発生したイベントに基づき、ターゲットを呼び出す EventBridge ルールを作成する方法。詳細パラメータを作成する際、パラメータの失効日、パラメータの有効期限の失効前に通知を受信するタイミング、パラメータが変更されていないことを示す通知を送信するまでの時間を指定します。次の手順を使用して、これらのイベントの通知を設定します。詳細については、Parameter Store でのパラメータポリシーの割り当ておよびパラメータ層の管理を参照してください。

Systems Manager パラメータまたはパラメータポリシー用に EventBridge を設定するには

1. Amazon EventBridge コンソール のhttps://console.aws.amazon.com/events/ を開いてください。
2. ナビゲーションペインで、[Rules (ルール)] を選択し、[Create rule (ルールの作成)] を選択します。

   -または-

   EventBridge ホームページが最初に開く場合は、[Create rule (ルールの作成)] を選択します。
3. ルールの名前と説明を入力します。

   ルールには同じリージョン内および同じイベントバス上の別のルールと同じ名前を付けることはできません。
4. [イベントバス] で、このルールに関連付けるイベントバスを選択します。このルールをユーザー自身の AWS アカウント の一致するイベントで開始する場合は、[Default] (デフォルト) 選択します。アカウントの AWS のサービスで発生したイベントは、常にアカウントのデフォルトのイベントバスに移動します。
5. [Rule type] (ルールタイプ) で、デフォルトの [Rule with an event pattern] (イベントパターンを持つルール) を選択したままにします。
6. [Next] を選択します。
7. [イベントソース] で、デフォルトの [AWS イベントまたは EventBridge パートナーイベント] を選択したままにします。[Sample event] (サンプルイベント) セクションはスキップできます。
8. [Event pattern] (イベントパターン) の場合は次のいずれかを実行します。

   - [Custom pattern (JSON editor)] (カスタムパターン (JSON エディター)) を選択します。
   - [Event pattern] (イベントパターン) で、パラメータまたはパラメータポリシーのどちらのルールを作成するかに応じて、次のいずれかの内容をボックスに貼り付けます。

Parameter

```
{
    "source": [
        "aws.ssm"
    ],
    "detail-type": [
        "Parameter Store Change"
    ],
    "detail": {
        "name": [
            "parameter-1-name",
            "/parameter-2-name/level-2",
            "/parameter-3-name/level-2/level-3"
        ],
        "operation": [
            "Create",
            "Update",
            "Delete",
            "LabelParameterVersion"
        ]
    }
}
```

Parameter policy

```
{
    "source": [
        "aws.ssm"
    ],
    "detail-type": [
        "Parameter Store Policy Action"
    ],
    "detail": {
        "parameter-name": [
            "parameter-1-name",
            "/parameter-2-name/level-2",
            "/parameter-3-name/level-2/level-3"
        ],
        "policy-type": [
            "Expiration",
            "ExpirationNotification",
            "NoChangeNotification"
```

```
        ]
    }
}
```

- 次の例に示されているように、アクションを行うパラメータやオペレーションの内容を変更します。

  Parameter

  この例では、Oncall と /Project/Teamlead という名前のいずれかのパラメータが更新されると、アクションが実行されます。

```
{
    "source": [
        "aws.ssm"
    ],
    "detail-type": [
        "Parameter Store Change"
    ],
    "detail": {
        "name": [
            "/Oncall",
            "/Project/Teamlead"
        ],
        "operation": [
            "Update"
        ]
    }
}
```

  Parameter policy

  この例では、OncallDuties という名前のパラメータが失効し、削除されると、アクションが実行されます。

```
{
    "source": [
        "aws.ssm"
    ],
    "detail-type": [
        "Parameter Store Policy Action"
    ],
    "detail": {
```

```
        "parameter-name": [
            "/OncallDuties"
        ],
        "policy-type": [
            "Expiration"
        ]
    }
}
```

9. [Next] を選択します。
10. [Target 1] (ターゲット 1) で、ターゲットタイプとサポートされているリソースを選択します。たとえば、[SNS トピック] を選択した場合は、[トピック] に対して選択を行います。[CodePipeline] を選択した場合は、[Pipeline ARN] (パイプライン ARN) にパイプライン ARN を入力します。必要に応じて、追加の設定値を指定します。

> **Tip**
>
> ルールに追加のターゲットが必要な場合は、[Add another target] (別のターゲットを追加) を選択します。

11. [Next] を選択します。
12. (オプション) ルールに 1 つ以上のタグを入力します。詳細については、Amazon EventBridge ユーザーガイドのAmazon EventBridge のタグを参照してください。
13. [Next] を選択します。
14. ルールの作成を選択します。

詳細情報

- 環境全体での設定更新を容易にするためにパラメーターラベルを使用する
- 「Amazon EventBridge ユーザーガイド」の「Tutorial: Use EventBridge to relay events to AWS Systems ManagerRun Command」
- Amazon EventBridge ユーザーガイドの「チュートリアル: AWS Systems Manager Automation を EventBridge のターゲットとして設定する」

「Parameter Store」 の使用

このセクションでは、タグパラメータを編成および作成する方法と、パラメータの異なるバージョンを作成する方法について説明します。

AWS Systems Manager コンソール、AWS Command Line Interface (AWS CLI)、AWS Tools for PowerShell、AWS SDK を使用して、パラメータを作成して操作できます。パラメータの詳細については、「パラメータとは何ですか?」を参照してください。

トピック

- Systems Manager での Parameter Store パラメータの作成
- Systems Manager での Parameter Store パラメータの検索
- Parameter Store でのパラメータポリシーの割り当て
- Parameter Store でのパラメータ階層の使用
- Parameter Store API オペレーションへのアクセスの防止
- Parameter Store でのパラメータラベルの操作
- Parameter Store でのパラメータバージョンの使用
- Parameter Store での共有パラメータの使用
- Run Command コマンドを使用した Parameter Store でのパラメータの操作
- Amazon マシンイメージ ID の Parameter Store でのパラメータのネイティブサポートの利用
- Parameter Store からのパラメータの削除

Systems Manager での Parameter Store パラメータの作成

以下のトピックの情報は、AWS Systems Manager コンソール、AWS Command Line Interface (AWS CLI)、AWS Tools for Windows PowerShell (Tools for Windows PowerShell) を使用して Systems Manager パラメータを作成するのに役立ちます。

このセクションでは、テスト環境で Parameter Store を使用してパラメータを作成、保存、実行する方法について説明します。また、他の Systems Manager ツールや AWS のサービスで Parameter Store を使用する方法についても説明します。詳細については、「パラメータとは何ですか?」を参照してください。

パラメータ名の要件と制約を理解する

このトピックの情報を使用して、パラメータの作成時にパラメータ名に有効な値を指定します。

この情報は AWS Systems Manager API リファレンス のトピック PutParameter の詳細を補完し、AllowedPattern、Description、KeyId、Overwrite、Type、Value の値についての詳細も提供します。

パラメータ名の要件と制約には次のようなものがあります。

- 大文字と小文字の区別: パラメータ名では大文字と小文字が区別されます。
- スペース: パラメータ名に空白を含めることはできません。
- 有効な文字: パラメータ名には、記号と文字として `a-zA-Z0-9_.-` のみを使用できます。

  さらに、スラッシュ文字 (/) は、パラメータ名の階層を表すために使用されます。例: `/Dev/Production/East/Project-ABC/MyParameter`
- 有効な AMI 形式: `aws:ec2:image` パラメータのデータ型として `String` を選択した場合、入力する ID は AMI ID 形式 `ami-12345abcdeEXAMPLE` に対して検証される必要があります。
- 完全修飾: 階層内でパラメータを作成または参照する場合は、スラッシュ文字 (/) を先頭に含めます。階層の一部であるパラメータを参照する場合は、先頭のスラッシュ (/) を含む階層パス全体を指定します。
  - 完全修飾パラメータ名:`MyParameter1` 、`/MyParameter2`、`/Dev/Production/East/Project-ABC/MyParameter`
  - 完全に修飾されていないパラメータ名: `MyParameter3/L1`
- 長さ: 指定するパラメータ名の最大文字数は 1,011 文字です。この 1,011 文字数には、指定した名前の前にある ARN 内の文字 (`arn:aws:ssm:us-east-2:111122223333:parameter/` の 45 文字など) が含まれます。
- プレフィックス: パラメータ名には、プレフィックスとして「`aws`」または「`ssm`」(大文字と小文字は区別しない) を付けることはできません。たとえば、以下のパラメータ名を作成しようとすると、例外によりエラーになります。
  - `awsTestParameter`
  - `SSM-testparameter`
  - `/aws/testparam1`

  > **Note**
  >
  > SSM ドキュメント、コマンド、またはスクリプトでパラメータを指定する場合、構文の一部として `ssm` を含めます。例: {{ssm:*parameter-name*}} および {{ ssm:*parameter-name* }} (例: `{{ssm:MyParameter}}`、および `{{ ssm:MyParameter }}`.)
- 一意性: パラメータ名は AWS リージョン 内で一意であることが必要です。例えば、以下が同じリージョン内にある場合、Systems Manager では個別のパラメータとして扱われます。
  - `/Test/TestParam1`

- /TestParam1

次の例も、一意です。

- /Test/TestParam1/Logpath1
- /Test/TestParam1

ただし、次の例は同じリージョン内にある場合、一意ではありません。

- /TestParam1
- TestParam1

- 階層の深さ: パラメータ階層を指定する場合、階層は最大 15 レベルの深さを持つことができます。階層のあらゆるレベルでパラメータを定義できます。次の例はいずれも、構造的に有効です。
  - /Level-1/L2/L3/L4/L5/L6/L7/L8/L9/L10/L11/L12/L13/L14/parameter-name
  - parameter-name

  次のパラメータの作成を試みると、HierarchyLevelLimitExceededException 例外で失敗します。
  - /Level-1/L2/L3/L4/L5/L6/L7/L8/L9/L10/L11/L12/L13/L14/L15/L16/parameter-name

> **Important**
>
> ユーザーがパスへのアクセス許可を持つ場合、そのユーザーはそのパスのすべてのレベルにアクセスできます。たとえば、ユーザーがパス /a へのアクセス許可を持っている場合、ユーザーは /a/b にアクセスすることもできます。ユーザーが AWS Identity and Access Management (IAM) でパラメータ /a/b で明示的にアクセスを拒否された場合でも、/a に対して GetParametersByPath API オペレーションを再帰的に呼び出して /a/b を表示できます。

トピック

- コンソールを使用して Parameter Store パラメータを作成する
- AWS CLI を使用して Parameter Store パラメータを作成する
- Tools for Windows PowerShell を使用して Parameter Store パラメータを作成する

コンソールを使用して Parameter Store パラメータを作成する

AWS Systems Manager コンソールを使用して、String、StringList、SecureString パラメータタイプを作成して実行できます。パラメータを削除したら、30 秒以上待ってから同じ名前のパラメータを作成します。

> **Note**
>
> パラメータは、パラメータを作成した AWS リージョン でのみ使用できます。

以下の手順では、Parameter Store コンソールでパラメータを作成するプロセスについて説明します。コンソールでは、String、StringList、および SecureString のパラメータタイプを作成できます。

パラメータを作成するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Parameter Store] を選択します。
3. [Create parameter] を選択します。
4. [Name (名前)] ボックスに、階層と名前を入力します。たとえば、「**/Test/helloWorld**」と入力します。

   パラメータ階層の詳細については、「Parameter Store でのパラメータ階層の使用」を参照してください。
5. [Description] ボックスに、このパラメータをテストパラメータとして識別するための説明を入力します。
6. [Parameter tier] で、[スタンダード] または [アドバンスト] を選択します。詳細パラメータの詳細については、「パラメータ層の管理」を参照してください。
7. [Type] として、[String]、[StringList]、[SecureString] のいずれかを選択します。

   - [String] を選択した場合は、[Data type (データ型)] フィールドが表示されます。Amazon Machine Image (AMI) のリソース ID を保持するパラメータを作成する場合は、「aws:ec2:image」を選択します。それ以外の場合は、デフォルトの text を選択したままにします。

- [SecureString] を選択すると、[KMS Key ID] フィールドが表示されます。AWS Key Management Service AWS KMS key ID、AWS KMS key Amazon リソースネーム (ARN)、エイリアス名、またはエイリアス ARN を指定しない場合、システムは Systems Manager の AWS マネージドキー である `alias/aws/ssm` を使用します。このキーを使用しない場合は、カスタマーマネージドキーを使用することもできます。AWS マネージドキーとカスタマー管理のキーの詳細については、AWS Key Management Service デベロッパーガイドの「AWS Key Management Service の概念」を参照してください。Parameter Store および AWS KMS の暗号化の詳細については、「AWS KMS で AWS Systems ManagerParameter Store を使用する方法」を参照してください。

  > **Important**
  >
  > Parameter Store では、対称暗号化 KMS キーのみをサポートしています。非対称暗号化 KMS キーを使用してパラメータを暗号化することはできません。KMS キーが対称か非対称かを判断する方法については、「AWS Key Management Service デベロッパーガイド」の「対称キーと非対称 KMS キーの識別」を参照してください。

- カスタマーマネージドキーエイリアス名またはエイリアス ARN のいずれかと `key-id` パラメータを使用してコンソールで `SecureString` パラメータを作成する場合は、そのエイリアスの前にプレフィックスの `alias/` を付けます。ARN の例を次に示します。

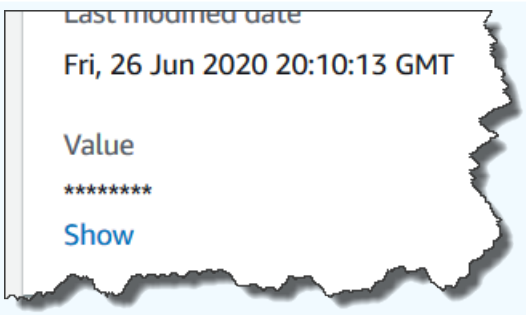
  ```
  arn:aws:kms:us-east-2:123456789012:alias/abcd1234-ab12-cd34-ef56-abcdeEXAMPLE
  ```

  エイリアス名の例を次に示します。

  ```
  alias/MyAliasName
  ```

8. [Value] ボックスに、値を入力します。たとえば、「**`This is my first parameter`**」または「**`ami-0dbf5ea29aEXAMPLE`**」と入力します。

   > **Note**
   >
   > パラメータは、他のパラメータの値で参照またはネストすることはできません。パラメータ値に `{{}}` または `{{ssm:parameter-name}}` を含めることはできません。
   > 次の図で示すように、[SecureString] を選択した場合、後でパラメータの [概要] タブで表示すると、パラメータの値はデフォルトでマスキングされます (「******」)。[表示] を選択して、パラメータ値を表示します。



9. (オプション) [タグ] 領域で、タグキーと値のペアを 1 つ以上パラメータに適用します。

   タグは、リソースに割り当てるオプションのメタデータです。タグを使用すると、目的、所有者、環境などのさまざまな方法でリソースを分類できます。たとえば、Systems Manager パラメータにタグを付けて、それが適用されるリソースのタイプ、環境、パラメータによって参照される設定データのタイプを識別できます。この場合、以下のキーと値のペアを指定します。

   - `Key=Resource,Value=S3bucket`
   - `Key=OS,Value=Windows`
   - `Key=ParameterType,Value=LicenseKey`

10. [Create parameter] を選択します。
11. パラメータリストで、先ほど作成したパラメータの名前を選択します。[Overview] タブで詳細を確認します。`SecureString` パラメータを作成した場合、[表示] を選択して、非暗号化された値を表示します。

> **Note**
>
> アドバンストパラメータをスタンダードパラメータに変更することはできません。アドバンストパラメータが不要になった場合、またはアドバンストパラメータの料金を抑えたい場合は、アドバンストパラメータを削除して新しいスタンダードパラメータとして再作成します。

AWS CLI を使用して Parameter Store パラメータを作成する

AWS Command Line Interface (AWS CLI) を使用して、`String`、`StringList`、および `SecureString` パラメータタイプを作成できます。パラメータを削除したら、30 秒以上待ってから同じ名前のパラメータを作成します。

パラメータは、他のパラメータの値で参照またはネストすることはできません。パラメータ値に {{}} または {{ssm:*parameter-name*}} を含めることはできません。

> **Note**
>
> パラメータは、パラメータを作成した AWS リージョン でのみ使用できます。

トピック

- AWS CLI を使用して String パラメータを作成する
- AWS CLI を使用して StringList パラメータを作成する
- AWS CLI を使用して SecureString パラメータを作成するには
- AWS CLI を使用して複数行パラメータを作成する

AWS CLI を使用して **String** パラメータを作成する

1. まだ AWS Command Line Interface (AWS CLI) をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」を参照してください。

2. 以下のコマンドを実行して String タイプのパラメータを作成します。各*###############*をユーザー自身の情報に置き換えます。

   Linux & macOS

   ```
   aws ssm put-parameter \
       --name "parameter-name" \
       --value "parameter-value" \
       --type String \
       --tags "Key=tag-key,Value=tag-value"
   ```

   Windows

   ```
   aws ssm put-parameter ^
       --name "parameter-name" ^
       --value "parameter-value" ^
       --type String ^
   ```

```
    --tags "Key=tag-key,Value=tag-value"
```

-または-

次のコマンドを実行して、パラメータ値として Amazon Machine Image (AMI) ID を含むパラメータを作成します。

Linux & macOS

```
aws ssm put-parameter \
    --name "parameter-name" \
    --value "an-AMI-id" \
    --type String \
    --data-type "aws:ec2:image" \
    --tags "Key=tag-key,Value=tag-value"
```

Windows

```
aws ssm put-parameter ^
    --name "parameter-name" ^
    --value "an-AMI-id" ^
    --type String ^
    --data-type "aws:ec2:image" ^
    --tags "Key=tag-key,Value=tag-value"
```

`--name` オプションは階層をサポートしています。階層については、「Parameter Store でのパラメータ階層の使用」を参照してください。

`--data-type` オプションは、AMI ID を含むパラメータを作成する場合にのみ指定する必要があります。入力したパラメータ値が、適切に書式設定された Amazon Elastic Compute Cloud (Amazon EC2) AMI ID であることを確認します。他のすべてのパラメータの場合、デフォルトのデータ型は `text` であり、値の指定はオプションです。詳細については、「」を参照してくださいAmazon マシンイメージ ID の Parameter Store でのパラメータのネイティブサポートの利用

> **Important**
>
> 成功すると、コマンドはパラメータのバージョン番号を返します。例外: データ型として aws:ec2:image を指定した場合、レスポンスの新しいバージョン番号が意味するのは、パラメータ値が未検証であるということです。詳細については、「」を参照してくださいAmazon マシンイメージ ID の Parameter Store でのパラメータのネイティブサポートの利用

以下の例では、キーと値のペアのタグ 2 つをパラメータに追加します。

Linux & macOS

```
aws ssm put-parameter \
    --name parameter-name \
    --value "parameter-value" \
    --type "String" \
    --tags '[{"Key":"Region","Value":"East"},{"Key":"Environment",
 "Value":"Production"}]'
```

Windows

```
aws ssm put-parameter ^
    --name parameter-name ^
    --value "parameter-value" ^
    --type "String" ^
    --tags [{\"Key\":\"Region1\",\"Value\":\"East1\"},{\"Key\":\"Environment1\",
\"Value\":\"Production1\"}]
```

次の例では、名前にパラメータ階層を使用して、プレーンテキストの String パラメータを作成します。パラメータのバージョン番号を返します。パラメータ階層の詳細については、「Parameter Store でのパラメータ階層の使用」を参照してください。

Linux & macOS

階層にないパラメータ

```
aws ssm put-parameter \
```

```
    --name "golden-ami" \
    --type "String" \
    --value "ami-12345abcdeEXAMPLE"
```

階層内のパラメータ

```
aws ssm put-parameter \
    --name "/amis/linux/golden-ami" \
    --type "String" \
    --value "ami-12345abcdeEXAMPLE"
```

Windows

階層にないパラメータ

```
aws ssm put-parameter ^
    --name "golden-ami" ^
    --type "String" ^
    --value "ami-12345abcdeEXAMPLE"
```

階層内のパラメータ

```
aws ssm put-parameter ^
    --name "/amis/windows/golden-ami" ^
    --type "String" ^
    --value "ami-12345abcdeEXAMPLE"
```

3. 次のコマンドを実行して、最新のパラメータ値を表示し、新しいパラメータの詳細を確認します。

```
aws ssm get-parameters --names "/Test/IAD/helloWorld"
```

システムが以下のような情報を返します。

```
{
    "InvalidParameters": [],
    "Parameters": [
        {
            "Name": "/Test/IAD/helloWorld",
            "Type": "String",
            "Value": "My updated parameter value",
```

```
            "Version": 2,
            "LastModifiedDate": "2020-02-25T15:55:33.677000-08:00",
            "ARN": "arn:aws:ssm:us-east-2:123456789012:parameter/Test/IAD/
helloWorld"
        }
    ]
}
```

以下のコマンドを実行して、パラメータの値を変更します。パラメータのバージョン番号を返します。

```
aws ssm put-parameter --name "/Test/IAD/helloWorld" --value "My updated 1st parameter"
 --type String --overwrite
```

以下のコマンドを実行して、パラメータ値の履歴を表示します。

```
aws ssm get-parameter-history --name "/Test/IAD/helloWorld"
```

以下のコマンドを実行して、このパラメータをコマンドで使用します。

```
aws ssm send-command --document-name "AWS-RunShellScript" --parameters '{"commands":
["echo {{ssm:/Test/IAD/helloWorld}}"]}' --targets "Key=instanceids,Values=instance-ids"
```

パラメータ Value のみを取得する場合は、次のコマンドを実行します。

```
aws ssm get-parameter --name testDataTypeParameter --query "Parameter.Value"
```

get-parameters を使用してパラメータ Value だけを取得する場合は、次のコマンドを実行します。

```
aws ssm get-parameters --names "testDataTypeParameter" --query "Parameters[*].Value"
```

以下のコマンドを実行して、パラメータのメタデータを表示します。

```
aws ssm describe-parameters --filters "Key=Name,Values=/Test/IAD/helloWorld"
```

> **Note**
>
> [Name] は大文字である必要があります。

システムが以下のような情報をレスポンスします。

```
{
    "Parameters": [
        {
            "Name": "helloworld",
            "Type": "String",
            "LastModifiedUser": "arn:aws:iam::123456789012:user/JohnDoe",
            "LastModifiedDate": 1494529763.156,
            "Version": 1,
            "Tier": "Standard",
            "Policies": []
        }
    ]
}
```

AWS CLI を使用して StringList パラメータを作成する

1. まだ AWS Command Line Interface (AWS CLI) をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」を参照してください。

2. 以下のコマンドを実行してパラメータを作成します。各*##############*をユーザー自身の情報に置き換えます。

   Linux & macOS

   ```
   aws ssm put-parameter \
       --name "parameter-name" \
       --value "a-comma-separated-list-of-values" \
       --type StringList \
       --tags "Key=tag-key,Value=tag-value"
   ```

Windows

```
aws ssm put-parameter ^
    --name "parameter-name" ^
    --value "a-comma-separated-list-of-values" ^
    --type StringList ^
    --tags "Key=tag-key,Value=tag-value"
```

> **Note**
>
> 成功すると、コマンドはパラメータのバージョン番号を返します。

この例では、キーと値のペアのタグ 2 つをパラメータに追加します。(ローカルマシンのオペレーティングシステムのタイプに応じて、次のいずれかのコマンドを実行します。ローカル Windows マシンから実行するバージョンには、コマンドラインツールからコマンドを実行するために必要なエスケープ文字 (「\」) が含まれます)。

以下に示しているのは、パラメータ階層を使用する StringList の例です。

Linux & macOS

```
aws ssm put-parameter \
    --name /IAD/ERP/Oracle/addUsers \
    --value "Milana,Mariana,Mark,Miguel" \
    --type StringList
```

Windows

```
aws ssm put-parameter ^
    --name /IAD/ERP/Oracle/addUsers ^
    --value "Milana,Mariana,Mark,Miguel" ^
    --type StringList
```

> **Note**
>
> StringList の項目はカンマ (,) で区切る必要があります。他の句読点または特殊文字を使用してリスト内の項目をエスケープすることはできません。カンマを必要とするパラメータ値がある場合は、String 型を使用してください。

3. パラメータの詳細を確認するには、get-parameters コマンドを実行します。例：

```
aws ssm get-parameters --name "/IAD/ERP/Oracle/addUsers"
```

AWS CLI を使用して SecureString パラメータを作成するには

SecureString パラメータを作成するには、次の手順を使用します。各##############をユーザー自身の情報に置き換えます。

> **Important**
>
> SecureString パラメータの値のみが暗号化されます。パラメータ名、説明などのプロパティは暗号化されません。

> **Important**
>
> Parameter Store では、対称暗号化 KMS キーのみをサポートしています。非対称暗号化 KMS キーを使用してパラメータを暗号化することはできません。KMS キーが対称か非対称かを判断する方法については、「AWS Key Management Service デベロッパーガイド」の「対称キーと非対称 KMS キーの識別」を参照してください。

1. まだ AWS Command Line Interface (AWS CLI) をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」を参照してください。
2. 以下のコマンドのいずれかを実行して、SecureString データ型を使用するパラメータを作成します。

Linux & macOS

デフォルトの AWS マネージドキーを使用して **SecureString** パラメータを作成する

```
aws ssm put-parameter \
    --name "parameter-name" \
    --value "parameter-value" \
    --type "SecureString"
```

カスタマーマネージドキーを使用する **SecureString** パラメータを作成する

```
aws ssm put-parameter \
    --name "parameter-name" \
    --value "a-parameter-value, for example P@ssW%rd#1" \
    --type "SecureString"
    --tags "Key=tag-key,Value=tag-value"
```

カスタム AWS KMS キーを使用する **SecureString** パラメータを作成する

```
aws ssm put-parameter \
    --name "parameter-name" \
    --value "a-parameter-value, for example P@ssW%rd#1" \
    --type "SecureString" \
    --key-id "your-account-ID/the-custom-AWS KMS-key" \
    --tags "Key=tag-key,Value=tag-value"
```

Windows

デフォルトの AWS マネージドキーを使用して **SecureString** パラメータを作成する

```
aws ssm put-parameter ^
    --name "parameter-name" ^
    --value "parameter-value" ^
    --type "SecureString"
```

カスタマーマネージドキーを使用する **SecureString** パラメータを作成する

```
aws ssm put-parameter ^
    --name "parameter-name" ^
    --value "a-parameter-value, for example P@ssW%rd#1" ^
```

```
    --type "SecureString" ^
    --tags "Key=tag-key,Value=tag-value"
```

カスタム AWS KMS キーを使用する **SecureString** パラメータを作成する

```
aws ssm put-parameter ^
    --name "parameter-name" ^
    --value "a-parameter-value, for example P@ssW%rd#1" ^
    --type "SecureString" ^
    --key-id " ^
    --tags "Key=tag-key,Value=tag-value"account-ID/the-custom-AWS KMS-key"
```

アカウントとリージョンで AWS マネージドキーを使用して SecureString パラメータを作成する場合、--key-id パラメータの値を指定する必要はありません。

> **Note**
>
> AWS アカウント と AWS リージョン に割り当てられた AWS KMS key を使用するには、コマンドから key-id パラメータを削除します。AWS KMS keys の詳細については、AWS Key Management Serviceデベロッパーガイドの「AWS Key Management Service の概念」を参照してください。

アカウントに割り当てられた AWS マネージドキー の代わりにカスタマーマネージドキーを使用するには、--key-id パラメータを使用してキーを指定します。パラメータは以下の KMS パラメータ形式をサポートします。

- キーの Amazon リソースネーム (ARN) の例:

  arn:aws:kms:us-east-2:123456789012:key/*key-id*

- エイリアス ARN の例:

  arn:aws:kms:us-east-2:123456789012:alias/*alias-name*

- キー ID の例:

  12345678-1234-1234-1234-123456789012

- エイリアス名の例:

```
alias/MyAliasName
```

カスタマーマネージドキーを作成するには、AWS Management Console または AWS KMS API を使用します。以下の AWS CLI コマンドは、AWS アカウント の現在の AWS リージョン でカスタマーマネージドキーを作成します。

```
aws kms create-key
```

先ほど作成したキーを使用して、SecureString パラメータを作成するには、以下の形式のコマンドを使用します。

以下の例では、パスワードパラメータと AWS KMS key 向けに難読化された名前(3l3vat3131)を使用しています。

Linux & macOS

```
aws ssm put-parameter \
    --name /Finance/Payroll/3l3vat3131 \
    --value "P@sSwW)rd" \
    --type SecureString \
    --key-id arn:aws:kms:us-
east-2:123456789012:key/1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4d5e
```

Windows

```
aws ssm put-parameter ^
    --name /Finance/Payroll/3l3vat3131 ^
    --value "P@sSwW)rd" ^
    --type SecureString ^
    --key-id arn:aws:kms:us-
east-2:123456789012:key/1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4d5e
```

3. パラメータの詳細を確認するには、以下のコマンドを実行します。

with-decryption パラメータを指定しない場合、または no-with-decryption パラメータを指定した場合、コマンドは暗号化された GUID を返します。

Linux & macOS

```
aws ssm get-parameters \
    --name "the-parameter-name-you-specified" \
    --with-decryption
```

Windows

```
aws ssm get-parameters ^
    --name "the-parameter-name-you-specified" ^
    --with-decryption
```

4. 以下のコマンドを実行して、パラメータのメタデータを表示します。

Linux & macOS

```
aws ssm describe-parameters \
    --filters "Key=Name,Values=the-name-that-you-specified"
```

Windows

```
aws ssm describe-parameters ^
    --filters "Key=Name,Values=the-name-that-you-specified"
```

5. カスタマーマネージド AWS KMS key を使用していない場合は、以下のコマンドを実行してパラメータ値を変更します。

Linux & macOS

```
aws ssm put-parameter \
    --name "the-name-that-you-specified" \
    --value "a-new-parameter-value" \
    --type "SecureString" \
    --overwrite
```

Windows

```
aws ssm put-parameter ^
    --name "the-name-that-you-specified" ^
    --value "a-new-parameter-value" ^
```

```
    --type "SecureString" ^
    --overwrite
```

-または-

カスタマーマネージド AWS KMS key を使用している場合は、以下のいずれかのコマンドを実行してパラメータ値を変更します。

Linux & macOS

```
aws ssm put-parameter \
    --name "the-name-that-you-specified" \
    --value "a-new-parameter-value" \
    --type "SecureString" \
    --key-id "the-KMSkey-ID" \
    --overwrite
```

```
aws ssm put-parameter \
    --name "the-name-that-you-specified" \
    --value "a-new-parameter-value" \
    --type "SecureString" \
    --key-id "account-alias/the-KMSkey-ID" \
    --overwrite
```

Windows

```
aws ssm put-parameter ^
    --name "the-name-that-you-specified" ^
    --value "a-new-parameter-value" ^
    --type "SecureString" ^
    --key-id "the-KMSkey-ID" ^
    --overwrite
```

```
aws ssm put-parameter ^
    --name "the-name-that-you-specified" ^
    --value "a-new-parameter-value" ^
    --type "SecureString" ^
    --key-id "account-alias/the-KMSkey-ID" ^
    --overwrite
```

6. 以下のコマンドを実行して、最新のパラメータ値を表示します。

   Linux & macOS

   ```
   aws ssm get-parameters \
       --name "the-name-that-you-specified" \
       --with-decryption
   ```

   Windows

   ```
   aws ssm get-parameters ^
       --name "the-name-that-you-specified" ^
       --with-decryption
   ```

7. 以下のコマンドを実行して、パラメータ値の履歴を表示します。

   Linux & macOS

   ```
   aws ssm get-parameter-history \
       --name "the-name-that-you-specified"
   ```

   Windows

   ```
   aws ssm get-parameter-history ^
       --name "the-name-that-you-specified"
   ```

> **Note**
>
> 暗号化された値でパラメータを手動で作成できます。この場合、値は既に暗号化されているため、SecureString パラメータタイプを選択する必要はありません。SecureString を選択した場合、パラメータは二重に暗号化されます。

デフォルトでは、すべての SecureString 値が暗号化テキストとして表示されます。SecureString 値を復号するには、AWS KMS の Decrypt API オペレーションを呼び出すためのアクセス権限が必要です。AWS KMS アクセスコントロールの設定方法については、「AWS Key Management Service デベロッパーガイド」の「AWS KMS に対する認証とアクセスコントロール」を参照してください。

> **Important**
>
> パラメータの暗号化に使用される KMS キーの KMS キーエイリアスを変更する場合は、パラメータが AWS KMS の参照で使用するキーエイリアスも更新する必要があります。これは KMS キーエイリアスにのみ適用されます。エイリアスがアタッチするキー ID は、キー全体を削除しない限り、同じままになります。

AWS CLI を使用して複数行パラメータを作成する

AWS CLI を使用して、改行を含むパラメータを作成できます。改行すると、長いパラメータ値のテキストを分割して読みやすくすることができ、たとえば、ウェブページの複数段落のパラメータコンテンツを更新できます。次の例に示すように、JSON ファイルにコンテンツを含めると、`--cli-input-json` のような改行文字を使用して \n オプションを使用できます。

1. まだ AWS Command Line Interface (AWS CLI) をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」を参照してください。

2. 次のコマンドを実行して、複数行のパラメータを作成します。

   Linux & macOS

   ```
   aws ssm put-parameter \
       --name "MultiLineParameter" \
       --type String \
       --cli-input-json file://MultiLineParameter.json
   ```

   Windows

   ```
   aws ssm put-parameter ^
       --name "MultiLineParameter" ^
       --type String ^
       --cli-input-json file://MultiLineParameter.json
   ```

   次の例では、`MultiLineParameter.json` ファイルの内容を示します。

```
{
    "Value": "<para>Paragraph One</para>\n<para>Paragraph Two</para>
\n<para>Paragraph Three</para>"
}
```

保存されたパラメータ値は、次のように保存されます。

```
<para>Paragraph One</para>
<para>Paragraph Two</para>
<para>Paragraph Three</para>
```

Tools for Windows PowerShell を使用して Parameter Store パラメータを作成する

AWS Tools for Windows PowerShell を使用して、String、StringList、SecureString パラメータタイプを作成できます。パラメータを削除したら、30 秒以上待ってから同じ名前のパラメータを作成します。

パラメータは、他のパラメータの値で参照またはネストすることはできません。パラメータ値に {{}} または {{ssm:*parameter-name*}} を含めることはできません。

> **Note**
>
> パラメータは、パラメータを作成した AWS リージョン でのみ使用できます。

トピック

- String パラメータを作成する (Tools for Windows PowerShell)
- StringList パラメータを作成する (Tools for Windows PowerShell)
- SecureString パラメータを作成する (Tools for Windows PowerShell)

String パラメータを作成する (Tools for Windows PowerShell)

1. AWS Tools for PowerShell (Tools for Windows PowerShell) をインストールして設定します (まだインストールしていない場合)。

   詳細については、「AWS Tools for PowerShell のインストール」を参照してください。

2. 以下のコマンドを実行して、プレーンテキスト値を含むパラメータを作成します。各*########*をユーザー自身の情報に置き換えます。

```
Write-SSMParameter `
    -Name "parameter-name" `
    -Value "parameter-value" `
    -Type "String"
```

-または-

次のコマンドを実行して、パラメータ値として Amazon Machine Image (AMI) ID を含むパラメータを作成します。

> **Note**
>
> タグ付きのパラメータを作成するには、変数として手前で service.model.tag を作成します。以下はその例です。
>
> ```
> $tag = New-Object Amazon.SimpleSystemsManagement.Model.Tag
> $tag.Key = "tag-key"
> $tag.Value = "tag-value"
> ```

```
Write-SSMParameter `
    -Name "parameter-name" `
    -Value "an-AMI-id" `
    -Type "String" `
    -DataType "aws:ec2:image" `
    -Tags $tag
```

-DataType オプションは、AMI ID を含むパラメータを作成する場合にのみ指定する必要があります。他のすべてのパラメータでは、デフォルトのデータ型は `text` です。詳細については、「」を参照してくださいAmazon マシンイメージ ID の Parameter Store でのパラメータのネイティブサポートの利用

以下に示しているのは、パラメータ階層の使用例です。

```
Write-SSMParameter `
    -Name "/IAD/Web/SQL/IPaddress" `
```

```
    -Value "99.99.99.999" `
    -Type "String" `
    -Tags $tag
```

3. パラメータの詳細を確認するには、以下のコマンドを実行します。

```
(Get-SSMParameterValue -Name "the-parameter-name-you-specified").Parameters
```

StringList パラメータを作成する (Tools for Windows PowerShell)

1. AWS Tools for PowerShell (Tools for Windows PowerShell) をインストールして設定します (まだインストールしていない場合)。

   詳細については、「AWS Tools for PowerShell のインストール」を参照してください。

2. 以下のコマンドを実行して、StringList パラメータを作成します。各##############をユーザー自身の情報に置き換えます。

> **Note**
>
> タグ付きのパラメータを作成するには、変数として手前で service.model.tag を作成します。以下はその例です。
>
> ```
> $tag = New-Object Amazon.SimpleSystemsManagement.Model.Tag
> $tag.Key = "tag-key"
> $tag.Value = "tag-value"
> ```

```
Write-SSMParameter `
    -Name "parameter-name" `
    -Value "a-comma-separated-list-of-values" `
    -Type "StringList" `
    -Tags $tag
```

成功すると、コマンドはパラメータのバージョン番号を返します。

以下はその例です。

```
Write-SSMParameter `
```

```
    -Name "stringlist-parameter" `
    -Value "Milana,Mariana,Mark,Miguel" `
    -Type "StringList" `
    -Tags $tag
```

> **Note**
>
> StringList の項目はカンマ (,) で区切る必要があります。他の句読点または特殊文字を使用してリスト内の項目をエスケープすることはできません。カンマを必要とするパラメータ値がある場合は、String 型を使用してください。

3. パラメータの詳細を確認するには、以下のコマンドを実行します。

```
(Get-SSMParameterValue -Name "the-parameter-name-you-specified").Parameters
```

SecureString パラメータを作成する (Tools for Windows PowerShell)

SecureString パラメータを作成する前に、このタイプのパラメータに関する前提要件を確認してください。詳細については、「AWS CLI を使用して SecureString パラメータを作成するには」を参照してください。

> **Important**
>
> SecureString パラメータの値のみが暗号化されます。パラメータ名、説明などのプロパティは暗号化されません。

> **Important**
>
> Parameter Store では、対称暗号化 KMS キーのみをサポートしています。非対称暗号化 KMS キーを使用してパラメータを暗号化することはできません。KMS キーが対称か非対称かを判断する方法については、「AWS Key Management Service デベロッパーガイド」の「対称キーと非対称 KMS キーの識別」を参照してください。

1. AWS Tools for PowerShell (Tools for Windows PowerShell) をインストールして設定します (まだインストールしていない場合)。

詳細については、「AWS Tools for PowerShell のインストール」を参照してください。

2. 以下のコマンドを実行してパラメータを作成します。各##############をユーザー自身の情報に置き換えます。

> **Note**
>
> タグ付きのパラメータを作成するには、まず service.model.tag を変数として作成します。以下はその例です。
>
> ```
> $tag = New-Object Amazon.SimpleSystemsManagement.Model.Tag
> $tag.Key = "tag-key"
> $tag.Value = "tag-value"
> ```

```
Write-SSMParameter `
    -Name "parameter-name" `
    -Value "parameter-value" `
    -Type "SecureString"  `
    -KeyId "an AWS KMS key ID, an AWS KMS key ARN, an alias name, or an alias ARN"
 `
    -Tags $tag
```

成功すると、コマンドはパラメータのバージョン番号を返します。

> **Note**
>
> アカウントに割り当てられた AWS マネージドキーを使用するには、コマンドから -KeyId パラメータを削除します。

難読化された名前 (3l3vat3131) をパスワードパラメータとして使用し、AWS マネージドキーを使用する例を次に示します。

```
Write-SSMParameter `
    -Name "/Finance/Payroll/3l3vat3131" `
    -Value "P@sSwW)rd" `
    -Type "SecureString"`
```

```
    -Tags $tag
```

3. パラメータの詳細を確認するには、以下のコマンドを実行します。

```
(Get-SSMParameterValue -Name "the-parameter-name-you-specified" -WithDecryption
 $true).Parameters
```

デフォルトでは、すべての SecureString 値が暗号化テキストとして表示されます。SecureString 値を復号するには、AWS KMS の Decrypt API オペレーションを呼び出すためのアクセス権限が必要です。AWS KMS アクセスコントロールの設定方法については、「AWS Key Management Service デベロッパーガイド」の「AWS KMS に対する認証とアクセスコントロール」を参照してください。

> **Important**
>
> パラメータの暗号化に使用される KMS キーの KMS キーエイリアスを変更する場合は、パラメータが AWS KMS の参照で使用するキーエイリアスも更新する必要があります。これは KMS キーエイリアスにのみ適用されます。エイリアスがアタッチするキー ID は、キー全体を削除しない限り、同じままになります。

Systems Manager での Parameter Store パラメータの検索

アカウントに多数のパラメータがある場合、一度に1つまたは複数のパラメータに関する情報を見つけるのが難しい場合があります。このような場合は、フィルタツールを使用して検索条件を指定することで、必要な情報を検索できます。AWS Systems Manager コンソール、AWS Command Line Interface (AWS CLI)、AWS Tools for PowerShell、または DescribeParameters API を使用してパラメータを検索できます。

トピック

- コンソールを使用してパラメータを検索する
- AWS CLI を使用してパラメータを検索する

コンソールを使用してパラメータを検索する

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。

2. ナビゲーションペインで、[Parameter Store] を選択します。
3. 検索ボックスを選択し、検索方法を選択します。例えば、Type、Name などです。
4. 選択した検索タイプの情報を入力します。以下に例を示します。

   - Type で検索する場合は、String、StringList、SecureString から選択します。
   - Name で検索する場合は、contains、equals、または begins-with を選択し、パラメータ名のすべてまたは一部を入力します。

   > **Note**
   >
   > コンソールでは、Name のデフォルトの検索タイプは contains です。

5. [Enter] キーを押します。

パラメータのリストが検索結果で更新されます。

AWS CLI を使用してパラメータを検索する

describe-parameters の 1 つ以上のパラメータに関する情報を表示するには、AWS CLI コマンドを使用します。

以下の例は、 のパラメータに関する情報を表示するために使用できるさまざまなオプションを示していますAWS アカウント これらのオプションの詳細については、「AWS Command Line Interface ユーザーガイド」の「describe-parameters」を参照してください。

1. まだ AWS Command Line Interface (AWS CLI) をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」を参照してください。

2. 以下のコマンドのサンプル値を、アカウントで作成されたパラメータを反映した値に置き換えます。

   Linux & macOS

   ```
   aws ssm describe-parameters \
       --parameter-filters "Key=Name,Values=MyParameterName"
   ```

Windows

```
aws ssm describe-parameters ^
    --parameter-filters "Key=Name,Values=MyParameterName"
```

> **Note**
>
> describe-parameters の場合、Name のデフォルトの検索タイプは Equals です。パラメータフィルタで、"Key=Name,Values=*MyParameterName*" を指定することは、"Key=Name,Option=Equals,Values=*MyParameterName*" を指定することと同じです。

```
aws ssm describe-parameters \
    --parameter-filters "Key=Name,Option=Contains,Values=Product"
```

```
aws ssm describe-parameters \
    --parameter-filters "Key=Type,Values=String"
```

```
aws ssm describe-parameters \
    --parameter-filters "Key=Path,Values=/Production/West"
```

```
aws ssm describe-parameters \
    --parameter-filters "Key=Tier,Values=Standard"
```

```
aws ssm describe-parameters \
    --parameter-filters "Key=tag:tag-key,Values=tag-value"
```

```
aws ssm describe-parameters \
    --parameter-filters "Key=KeyId,Values=key-id"
```

> **Note**
>
> 最後の例の *key-id* は、アカウントで作成された AWS Key Management Service パラメータの暗号化に使用される AWS KMS (SecureString) キーの ID を表します。ま

た、**alias/aws/ssm** を入力して、アカウントのデフォルトの AWS KMS キーを使用することもできます。詳細については、「」を参照してくださいAWS CLI を使用して SecureString パラメータを作成するには

成功すると、コマンドは以下のような出力を返します。

```
{
    "Parameters": [
        {
            "Name": "/Production/West/Manager",
            "Type": "String",
            "LastModifiedDate": 1573438580.703,
            "LastModifiedUser": "arn:aws:iam::111122223333:user/Mateo.Jackson",
            "Version": 1,
            "Tier": "Standard",
            "Policies": []
        },
        {
            "Name": "/Production/West/TeamLead",
            "Type": "String",
            "LastModifiedDate": 1572363610.175,
            "LastModifiedUser": "arn:aws:iam::111122223333:user/Mateo.Jackson",
            "Version": 1,
            "Tier": "Standard",
            "Policies": []
        },
        {
            "Name": "/Production/West/HR",
            "Type": "String",
            "LastModifiedDate": 1572363680.503,
            "LastModifiedUser": "arn:aws:iam::111122223333:user/Mateo.Jackson",
            "Version": 1,
            "Tier": "Standard",
            "Policies": []
        }
    ]
}
```

Parameter Store でのパラメータポリシーの割り当て

パラメータポリシーを使用すると、有効期限終了日または有効期限などの特定の条件をパラメータに割り当てることができ、増え続けるパラメータのセットを管理できます。パラメータポリシーは、AWS Systems Manager のツールである Parameter Store に保存されたパスワードと設定データを強制的に更新または削除するのに役立ちます。Parameter Store には、`Expiration`、`ExpirationNotification`、`NoChangeNotification` というタイプのポリシーがあります。

> **Note**
>
> パスワードローテーションのライフサイクルを実装するには、 を使用しますAWS Secrets Manager Secrets Manager を使用すると、データベースの認証情報、API キー、その他のシークレットをそのライフサイクルを通してローテーション、管理、取得できます。詳細については、AWS Secrets Managerユーザーガイドの「AWS Secrets Manager とは」を参照してください。

Parameter Store は、非同期の定期的なスキャンを使用してパラメータポリシーを適用します。ポリシーを作成したら、追加のアクションを実行する必要はありません。Parameter Store は指定した条件に基づいて、ポリシーで定義されたアクションを個別に実行します。

> **Note**
>
> パラメータポリシーは、高度なパラメータ階層を使用するパラメータに利用できます。詳細については、「」を参照してくださいパラメータ層の管理

パラメータポリシーは、次の表に示すように、JSON 配列です。新しいアドバンストパラメータを作成するときにポリシーを割り当てることも、パラメータを更新することでポリシーを適用することもできます。以下のタイプのパラメータポリシーが Parameter Store でサポートされています。

ポリシー	詳細	例
有効期限	このポリシーは、パラメータを削除します。`ISO_INSTANT` または `ISO_OFFSET_DATE_TIME` のいずれか	`{ "Type": "Expiration", "Version": "1.0",`

ポリシー	詳細	例

	の形式を使用して、特定の日時を指定できます。パラメータを削除するタイミングを変更する場合は、ポリシーを更新します。パラメータを更新しても、アタッチされているポリシーの有効期限日または時刻には影響しません。有効期限日または時刻に達すると、Parameter Store はパラメータを削除します。
	
	Note
	この例では、ISO_INSTANT 形式を使用しています。ISO_OFFSET_DATE_TIME 形式を使用して、日時を指定することもできます。たとえば、2019-11-01T22:13:48.87+10:30:00 と指定します。
		<pre>"Attributes": {
		"Timestamp": "2018-12-02T21:34:33.000Z"
		}
		}</pre>

ポリシー	詳細	例
ExpirationNotification	このポリシーは、有効期限を通知するイベントを Amazon EventBridge (EventBridge) で開始します。このポリシーを使用することで、有効期限に達する前に日数または時間単位で通知を受け取ることができます。	`{ "Type": "ExpirationNotification", "Version": "1.0", "Attributes": { "Before": "15", "Unit": "Days" } }`
NoChangeNotification	このポリシーは、指定された期間内にパラメータが変更されていない場合、EventBridge でイベントを開始します。このポリシータイプが役立つのは、たとえば、ある期間内にパスワードを変更する必要がある場合です。 このポリシーでは、パラメータの `LastModifiedTime` 属性を読み取ることで、通知を送信するタイミングを決定します。パラメータを変更または編集した場合、システムは `LastModifiedTime` の新しい値に基づいて通知する期間をリセットします。	`{ "Type": "NoChangeNotification", "Version": "1.0", "Attributes": { "After": "20", "Unit": "Days" } }`

複数のポリシーをパラメータに割り当てることもできます。例えば、`Expiration` および `ExpirationNotification` のポリシーを割り当て、システムが EventBridge イベントを開始して、パラメータが間もなく削除される通知を受け取ることができます。最大 10 個のポリシーをパラメータに割り当てることができます。

以下の例では、SecureString という名前の新しい ProdDB3 パラメータに 4 つのポリシーを割り当てる PutParameter API リクエストのリクエスト構文を示しています。

```
{
    "Name": "ProdDB3",
    "Description": "Parameter with policies",
    "Value": "P@ssW*rd21",
    "Type": "SecureString",
    "Overwrite": "True",
    "Policies": [
        {
            "Type": "Expiration",
            "Version": "1.0",
            "Attributes": {
                "Timestamp": "2018-12-02T21:34:33.000Z"
            }
        },
        {
            "Type": "ExpirationNotification",
            "Version": "1.0",
            "Attributes": {
                "Before": "30",
                "Unit": "Days"
            }
        },
        {
            "Type": "ExpirationNotification",
            "Version": "1.0",
            "Attributes": {
                "Before": "15",
                "Unit": "Days"
            }
        },
        {
            "Type": "NoChangeNotification",
            "Version": "1.0",
            "Attributes": {
                "After": "20",
                "Unit": "Days"
            }
        }
    ]
}
```

既存のパラメータにポリシーを追加する

このセクションには、AWS Systems Manager コンソール、AWS Command Line Interface (AWS CLI)、AWS Tools for Windows PowerShell を使用して既存のパラメータにポリシーを追加する方法についての情報が含まれています。ポリシーが含まれている新しいパラメータの作成方法については、「Systems Manager での Parameter Store パラメータの作成」を参照してください。

トピック

- コンソールを使用して既存のパラメータにポリシーを追加する
- AWS CLI を使用して既存のパラメータにポリシーを追加する
- 既存のパラメータにポリシーを追加する (Tools for Windows PowerShell)

コンソールを使用して既存のパラメータにポリシーを追加する

以下の手順に従って、Systems Manager コンソールを使用して既存のパラメータにポリシーを追加します。

既存のパラメータにポリシーを追加するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Parameter Store] を選択します。
3. ポリシーを含めるために更新するパラメータの横にあるオプションを選択し、[編集] を選択します。
4. [Advanced] を選択します。
5. (オプション) [Parameter policies (パラメータポリシー)] セクションで、[有効] を選択します。このパラメータには、有効期限と 1 つ以上の通知ポリシーを指定できます。
6. [Save changes] を選択します。

> **Important**
>
> - Parameter Store は、新しいポリシーでポリシーを上書きするか、ポリシーを削除するまでパラメータのポリシーを保持します。
> - 既存のパラメータからすべてのポリシーを削除するには、パラメータを編集し、次のように角括弧と中括弧 [{}] を使用して空のポリシーを適用します。

- 既にポリシーが設定されているパラメータに新しいポリシーを追加すると、Systems Manager はそのパラメータにアタッチされているポリシーを上書きします。既存のポリシーが削除されます。すでに 1 つ以上のポリシーがあるパラメータに新しいポリシーを追加する場合は、元のポリシーをコピーして貼り付け、新しいポリシーを入力してから変更を保存します。

AWS CLI を使用して既存のパラメータにポリシーを追加する

以下の手順を使用して、既存のパラメータに AWS CLI を使用してポリシーを追加します。

既存のパラメータにポリシーを追加するには

1. まだ AWS Command Line Interface (AWS CLI) をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」を参照してください。

2. 次のコマンドを実行して、既存のパラメータにポリシーを追加します。各##############をユーザー自身の情報に置き換えます。

   Linux & macOS

   ```
   aws ssm put-parameter
       --name "parameter name" \
       --value 'parameter value' \
       --type parameter type \
       --overwrite \
       --policies "[{policies-enclosed-in-brackets-and-curly-braces}]"
   ```

   Windows

   ```
   aws ssm put-parameter
       --name "parameter name" ^
       --value 'parameter value' ^
       --type parameter type ^
       --overwrite ^
       --policies "[{policies-enclosed-in-brackets-and-curly-braces}]"
   ```

以下に示しているのは、15 日後にパラメータを削除する有効期限ポリシーを含む例です。この例では、パラメータが削除される 5 日前に EventBridge イベントを生成する通知ポリシーも含まれます。最後に、60 日後にこのパラメータが変更されない場合のNoChangeNotificationポリシーが含まれます。この例では、パスワードに難読化された名前 (3l3vat3131)、および AWS Key Management Service AWS KMS key を使用しています。AWS KMS keys の詳細については、AWS Key Management Serviceデベロッパーガイドの「AWS Key Management Service の概念」を参照してください。

Linux & macOS

```
aws ssm put-parameter \
    --name "/Finance/Payroll/3l3vat3131" \
    --value "P@sSwW)rd" \
    --type "SecureString" \
    --overwrite \
    --policies "[{\"Type\":\"Expiration\",\"Version\":\"1.0\",\"Attributes\":
{\"Timestamp\":\"2020-05-13T00:00:00.000Z\"}},{\"Type\":\"ExpirationNotification
\",\"Version\":\"1.0\",\"Attributes\":{\"Before\":\"5\",\"Unit\":\"Days\"}},
{\"Type\":\"NoChangeNotification\",\"Version\":\"1.0\",\"Attributes\":{\"After
\":\"60\",\"Unit\":\"Days\"}}]"
```

Windows

```
aws ssm put-parameter ^
    --name "/Finance/Payroll/3l3vat3131" ^
    --value "P@sSwW)rd" ^
    --type "SecureString" ^
    --overwrite ^
    --policies "[{\"Type\":\"Expiration\",\"Version\":\"1.0\",\"Attributes\":
{\"Timestamp\":\"2020-05-13T00:00:00.000Z\"}},{\"Type\":\"ExpirationNotification
\",\"Version\":\"1.0\",\"Attributes\":{\"Before\":\"5\",\"Unit\":\"Days\"}},
{\"Type\":\"NoChangeNotification\",\"Version\":\"1.0\",\"Attributes\":{\"After
\":\"60\",\"Unit\":\"Days\"}}]"
```

3. パラメータの詳細を確認するには、以下のコマンドを実行します。*parameter name* を自分の情報に置き換えます。

Linux & macOS

```
aws ssm describe-parameters  \
```

```
    --parameter-filters "Key=Name,Values=parameter name"
```

Windows

```
aws ssm describe-parameters  ^
    --parameter-filters "Key=Name,Values=parameter name"
```

Important

- Parameter Store では、新しいポリシーでポリシーを上書きするまで、またはポリシーを削除するまでパラメータのポリシーが保持されます。
- 既存のパラメータからすべてのポリシーを削除するには、パラメータを編集し、空の角括弧と中括弧のポリシーを適用します。各###############をユーザー自身の情報に置き換えます。例:

  Linux & macOS

  ```
  aws ssm put-parameter \
      --name parameter name \
      --type parameter type  \
      --value 'parameter value' \
      --policies "[{}]"
  ```

  Windows

  ```
  aws ssm put-parameter ^
      --name parameter name ^
      --type parameter type  ^
      --value 'parameter value' ^
      --policies "[{}]"
  ```

- 既にポリシーが設定されているパラメータに新しいポリシーを追加すると、Systems Manager はそのパラメータにアタッチされているポリシーを上書きします。既存のポリシーが削除されます。すでに 1 つ以上のポリシーがあるパラメータに新しいポリシーを追加する場合は、元のポリシーをコピーして貼り付け、新しいポリシーを入力してから変更を保存します。

既存のパラメータにポリシーを追加する (Tools for Windows PowerShell)

Tools for Windows PowerShell を使用して既存のパラメータにポリシーを追加するには、次の手順に従います。各##############をユーザー自身の情報に置き換えます。

既存のパラメータにポリシーを追加するには

1. Tools for Windows PowerShell を開き、次のコマンドを実行して認証情報を指定します。Amazon Elastic Compute Cloud (Amazon EC2) で管理者権限を持っているか、AWS Identity and Access Management (IAM) で適切なアクセス許可が付与されている必要があります。

```
Set-AWSCredentials `
    -AccessKey access-key-name `
    -SecretKey secret-key-name
```

2. 次のコマンドを実行して、PowerShell セッションのリージョンを設定します。この例では、米国東部 (オハイオ) リージョン (us-east-2) を使用しています。

```
Set-DefaultAWSRegion `
    -Region us-east-2
```

3. 次のコマンドを実行して、既存のパラメータにポリシーを追加します。各##############をユーザー自身の情報に置き換えます。

```
Write-SSMParameter `
    -Name "parameter name" `
    -Value "parameter value" `
    -Type "parameter type" `
    -Policies "[{policies-enclosed-in-brackets-and-curly-braces}]" `
    -Overwrite
```

以下に示しているのは、2020 年 5 月 13 日深夜 0 時 (GMT) にパラメータを削除する有効期限ポリシーを含む例です。この例では、パラメータが削除される 5 日前に EventBridge イベントを生成する通知ポリシーも含まれます。最後に、60 日後にこのパラメータが変更されない場合のNoChangeNotification ポリシーが含まれます。この例では、パスワードに難読化された名前 (3l3vat3131)、および AWS マネージドキー を使用しています。

```
Write-SSMParameter `
    -Name "/Finance/Payroll/3l3vat3131" `
    -Value "P@sSwW)rd" `
    -Type "SecureString" `
```

```
    -Policies "[{\"Type\":\"Expiration\",\"Version\":\"1.0\",\"Attributes\":
{\"Timestamp\":\"2018-05-13T00:00:00.000Z\"}},{\"Type\":\"ExpirationNotification
\",\"Version\":\"1.0\",\"Attributes\":{\"Before\":\"5\",\"Unit\":\"Days\"}},{\"Type
\":\"NoChangeNotification\",\"Version\":\"1.0\",\"Attributes\":{\"After\":\"60\",
\"Unit\":\"Days\"}}]" `
    -Overwrite
```

4. パラメータの詳細を確認するには、以下のコマンドを実行します。*parameter name* を自分の情報に置き換えます。

```
(Get-SSMParameterValue -Name "parameter name").Parameters
```

Important

- Parameter Store は、新しいポリシーでポリシーを上書きするか、ポリシーを削除するまでパラメータのポリシーを保持します。
- 既存のパラメータからすべてのポリシーを削除するには、パラメータを編集し、空の角括弧と中括弧のポリシーを適用します。以下に例を示します。

```
Write-SSMParameter `
    -Name "parameter name" `
    -Value "parameter value" `
    -Type "parameter type" `
    -Policies "[{}]"
```

- 既にポリシーが設定されているパラメータに新しいポリシーを追加すると、Systems Manager はそのパラメータにアタッチされているポリシーを上書きします。既存のポリシーが削除されます。すでに 1 つ以上のポリシーがあるパラメータに新しいポリシーを追加する場合は、元のポリシーをコピーして貼り付け、新しいポリシーを入力してから変更を保存します。

Parameter Store でのパラメータ階層の使用

数十または数百のパラメータをフラットリストで管理することは、時間がかかり、エラーの原因となります。また、タスクに合ったパラメータを特定することが難しくなります。これは、誤って間違ったパラメータを使用したり、同じ設定データを使用するパラメータを複数作成する可能性があることを意味します。

パラメータ階層を使用すると、パラメータの編成や管理がしやすくなります。階層は、スラッシュを使用して定義するパスを含むパラメータ名です。

トピック

- 例を介してパラメータ階層を理解する
- 階層でパラメータへのクエリを実行する
- AWS CLI を使用して階層でパラメータを管理する

例を介してパラメータ階層を理解する

以下の例では、名前に 3 つの階層レベルを使用しています。

```
/Environment/Type of computer/Application/Data
```

```
/Dev/DBServer/MySQL/db-string13
```

最大で 15 のレベルを持つ階層を作成できます。次の例で示されているように、ユーザーの環境にすでに存在する階層構造を反映した階層を作成することをお勧めします。

- 継続的統合および継続的デリバリー環境 (CI/CD ワークフロー)

  ```
  /Dev/DBServer/MySQL/db-string
  ```

  ```
  /Staging/DBServer/MySQL/db-string
  ```

  ```
  /Prod/DBServer/MySQL/db-string
  ```

- コンテナを使用するアプリケーション

  ```
  /MyApp/.NET/Libraries/my-password
  ```

- ユーザーの企業

  ```
  /Finance/Accountants/UserList
  ```

  ```
  /Finance/Analysts/UserList
  ```

  ```
  /HR/Employees/EU/UserList
  ```

パラメータ階層は、パラメータを作成する方法を標準化し、時間とともにパラメータの管理が容易になります。階層パラメータはまた、設定タスクに合ったパラメータを特定するのに役立ちます。つまり、同じ設定データを持つパラメータを複数作成することを防ぎます。

開発およびステージング環境でパスワードを使用する次の例に示されているように、異なる環境間でパラメータを共有できる階層を作成することができます。

/DevTest/MyApp/database/*my-password*

続いて、次の例に示されているように、本番環境の一意のパスワードを作成できます。

/prod/MyApp/database/*my-password*

パラメータ階層を指定する必要はありません。レベル 1 でパラメータを作成できます。これらはルートパラメータと呼ばれます。下位互換性のため、階層をリリースする前に Parameter Store で作成されたすべてのパラメータは、ルートパラメータではありません。システムは、次のパラメータの両方をルートパラメータとして扱います。

/parameter-name

parameter-name

階層でパラメータへのクエリを実行する

階層を使用するもう 1 つの利点は、GetParametersByPath API オペレーションを使用して、階層内の特定のレベル以下の、すべてのパラメータをクエリする機能です。例えば、AWS Command Line Interface (AWS CLI) で次のコマンドを実行すると、システムは `Oncall` レベル以下のすべてのパラメータを返します。

```
aws ssm get-parameters-by-path --path /Dev/Web/Oncall
```

サンプル出力:

```
{
    "Parameters": [
        {
            "Name": "/Dev/Web/Oncall/Week1",
            "Type": "String",
            "Value": "John Doe",
            "Version": 1,
```

```
            "LastModifiedDate": "2024-11-22T07:18:53.510000-08:00",
            "ARN": "arn:aws:ssm:us-east-2:123456789012:parameter/Dev/Web/Oncall/Week1",
            "DataType": "text"
        },
        {
            "Name": "/Dev/Web/Oncall/Week2",
            "Type": "String",
            "Value": "Mary Major",
            "Version": 1,
            "LastModifiedDate": "2024-11-22T07:21:25.325000-08:00",
            "ARN": "arn:aws:ssm:us-east-2:123456789012:parameter/Dev/Web/Oncall/Week2",
            "DataType": "text"
        }
    ]
}
```

復号化された SecureString パラメータを階層で表示するには、次の例に示されているように、パスおよび --with-decryption パラメータを指定します。

```
aws ssm get-parameters-by-path --path /Prod/ERP/SAP --with-decryption
```

AWS CLI を使用して階層でパラメータを管理する

この手順では、AWS CLI を使用してパラメータおよびパラメータ階層を使用する方法について説明します。

階層を使用してパラメータを管理するには

1. まだ AWS Command Line Interface (AWS CLI) をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」を参照してください。
2. 以下のコマンドを実行して、allowedPattern パラメータおよび String パラメータタイプを使用するパラメータを作成します。この例の許容されているパターンは、パラメータの値が 1 ~ 4 桁である必要があることを意味します。

   Linux & macOS

   ```
   aws ssm put-parameter \
       --name "/MyService/Test/MaxConnections" \
   ```

```
    --value 100 --allowed-pattern "\d{1,4}" \
    --type String
```

Windows

```
aws ssm put-parameter ^
    --name "/MyService/Test/MaxConnections" ^
    --value 100 --allowed-pattern "\d{1,4}" ^
    --type String
```

コマンドはパラメータのバージョン番号を返します。

3. 次のコマンドを実行して、先ほど新しい値で作成したパラメータの上書きを試みます。

Linux & macOS

```
aws ssm put-parameter \
    --name "/MyService/Test/MaxConnections" \
    --value 10,000 \
    --type String \
    --overwrite
```

Windows

```
aws ssm put-parameter ^
    --name "/MyService/Test/MaxConnections" ^
    --value 10,000 ^
    --type String ^
    --overwrite
```

システムは、新しい値が前のステップで指定した許容されるパターンの要件を満たしていないため、次のエラーを返します。

```
An error occurred (ParameterPatternMismatchException) when calling the PutParameter
 operation: Parameter value, cannot be validated against allowedPattern: \d{1,4}
```

4. 次のコマンドを実行して、AWS マネージドキー を使用する SecureString パラメータを作成します。この例の許容されているパターンは、ユーザーが任意の文字を指定でき、値が 8～20 文字である必要があることを意味します。

Linux & macOS

```
aws ssm put-parameter \
    --name "/MyService/Test/my-password" \
    --value "p#sW*rd33" \
    --allowed-pattern ".{8,20}" \
    --type SecureString
```

Windows

```
aws ssm put-parameter ^
    --name "/MyService/Test/my-password" ^
    --value "p#sW*rd33" ^
    --allowed-pattern ".{8,20}" ^
    --type SecureString
```

5. 次のコマンドを実行し、前のステップの階層構造を使用するパラメータをさらに作成します。

Linux & macOS

```
aws ssm put-parameter \
    --name "/MyService/Test/DBname" \
    --value "SQLDevDb" \
    --type String
```

```
aws ssm put-parameter \
    --name "/MyService/Test/user" \
    --value "SA" \
    --type String
```

```
aws ssm put-parameter \
    --name "/MyService/Test/userType" \
    --value "SQLuser" \
    --type String
```

Windows

```
aws ssm put-parameter ^
    --name "/MyService/Test/DBname" ^
    --value "SQLDevDb" ^
```

```
    --type String
```

```
aws ssm put-parameter ^
    --name "/MyService/Test/user" ^
    --value "SA" ^
    --type String
```

```
aws ssm put-parameter ^
    --name "/MyService/Test/userType" ^
    --value "SQLuser" ^
    --type String
```

6. 次のコマンドを実行して、2 つのパラメータの値を取得します。

   Linux & macOS

   ```
   aws ssm get-parameters \
       --names "/MyService/Test/user" "/MyService/Test/userType"
   ```

   Windows

   ```
   aws ssm get-parameters ^
       --names "/MyService/Test/user" "/MyService/Test/userType"
   ```

7. 次のコマンドを実行して、単一レベル以下のすべてのパラメータをクエリします。

   Linux & macOS

   ```
   aws ssm get-parameters-by-path \
       --path "/MyService/Test"
   ```

   Windows

   ```
   aws ssm get-parameters-by-path ^
       --path "/MyService/Test"
   ```

8. 次のコマンドを実行して、2 つのパラメータを削除します。

Linux & macOS

```
aws ssm delete-parameters \
    --names "/IADRegion/Dev/user" "/IADRegion/Dev/userType"
```

Windows

```
aws ssm delete-parameters ^
    --names "/IADRegion/Dev/user" "/IADRegion/Dev/userType"
```

Parameter Store API オペレーションへのアクセスの防止

AWS Identity and Access Management (IAM) ポリシーに Systems Manager がサポートするサービス固有の条件を使用することで、Parameter Store API オペレーションとコンテンツへのアクセスを明示的に許可または拒否することができます。これらの条件を使用すると、組織内の特定の IAM エンティティ (ユーザーとロール) のみに特定の API アクションの呼び出しを許可したり、特定の IAM エンティティがアクションを実行できないようにしたりすることができます。これには、Parameter Store コンソール、AWS Command Line Interface (AWS CLI) 、および SDK 経由でのアクションが含まれます。

Systems Manager は現在、Parameter Store に固有の 3 つの条件をサポートしています。

トピック

- ssm:Overwrite を使用して既存のパラメータの変更を防止する
- ssm:Policies を使用してパラメータポリシーを使用するパラメータの作成または更新を禁止する
- ssm:Recursive を使用して階層的パラメータ内のレベルへのアクセスを禁止する

`ssm:Overwrite` を使用して既存のパラメータの変更を防止する

`ssm:Overwrite` 条件を使用して、IAM エンティティが既存のパラメータを更新できるかどうかを制御します。

以下のサンプルポリシーでは、`"Allow"` ステートメントは、米国東部 (オハイオ) リージョン (us-east-2) にある AWS アカウント 123456789012 で `PutParameter` API オペレーションを実行してパラメータを作成する許可を付与します。

その一方で、"Deny" ステートメントはエンティティが既存のパラメータの値を変更するのを禁止しています。これは、PutParameter オペレーションについての Overwrite オプションが明示的に拒否されているためです。このため、このポリシーが割り当てられているエンティティは、パラメータを作成することはできても、既存のパラメータを変更することはできません。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:PutParameter"
            ],
            "Resource": "arn:aws:ssm:us-east-2:123456789012:parameter/*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "ssm:PutParameter"
            ],
            "Condition": {
                "StringEquals": {
                    "ssm:Overwrite": [
                        "true"
                    ]
                }
            },
            "Resource": "arn:aws:ssm:us-east-2:123456789012:parameter/*"
        }
    ]
}
```

ssm:Policies を使用してパラメータポリシーを使用するパラメータの作成または更新を禁止する

パラメータポリシーを含むパラメータの作成と、パラメータポリシーを含む既存のパラメータの更新をエンティティに許可するかどうかを制御する ssm:Policies 条件を使用します。

次のポリシー例では、"Allow" ステートメントはパラメータを作成する一般的なアクセス許可を付与しますが、"Deny" ステートメントは、エンティティが米国東部 (オハイオ) リージョン (us-east-2) の AWS アカウント 123456789012 にパラメータポリシーを含むパラメータを作成または更新することを禁止します。エンティティは、パラメータポリシーが割り当てられていないパラメータを作成または更新できます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:PutParameter"
            ],
            "Resource": "arn:aws:ssm:us-east-2:123456789012:parameter/*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "ssm:PutParameter"
            ],
            "Condition": {
                "StringEquals": {
                    "ssm:Policies": [
                        "true"
                    ]
                }
            },
            "Resource": "arn:aws:ssm:us-east-2:123456789012:parameter/*"
        }
    ]
}
```

ssm:Recursive を使用して階層的パラメータ内のレベルへのアクセスを禁止する

ssm:Recursive 条件を使用して、IAM エンティティが階層的パラメータ内のレベルを表示または参照できるかどうかを制御します。特定の階層レベルを超えるすべてのパラメータへのアクセスを提供または制限することができます。

以下のサンプルポリシーでは、"Allow" ステートメントは、米国東部 (オハイオ) リージョン (us-east-2) にある AWS アカウント 123456789012 のパス /Code/Departments/Finance/* 内のすべてのパラメータに対する Parameter Store オペレーションへのアクセスを提供します。

その後に続く "Deny" ステートメントは、IAM エンティティが /Code/Departments/* レベルもしくはそれ以下のパラメータデータを閲覧または取得することを禁止しています。ただし、エンティティは引き続きそのパス内のパラメータを作成または更新できます。このサンプルは、特定のパラメータ階層レベルより下のレベルへのアクセスを再帰的に拒否することが、同じポリシー内にある許容度の高いアクセスよりも優先されることを説明するために構築されています。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:*"
            ],
            "Resource": "arn:aws:ssm:us-east-2:123456789012:parameter/*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "ssm:GetParametersByPath"
            ],
            "Condition": {
                "StringEquals": {
                    "ssm:Recursive": [
                        "true"
                    ]
                }
            },
            "Resource": "arn:aws:ssm:us-east-2:123456789012:parameter/Code/Departments/
*"
        }
    ]
}
```

Important

ユーザーがパスへのアクセス許可を持つ場合、そのユーザーはそのパスのすべてのレベルにアクセスできます。たとえば、ユーザーがパス /a へのアクセス許可を持っている場合、ユーザーは /a/b にアクセスすることもできます。ただし、上記のように、ユーザーが IAM でパラメータ /b へのアクセスを明示的に拒否されている場合は例外となります。

Parameter Store でのパラメータラベルの操作

パラメータラベルは、ユーザー定義のエイリアスであり、異なるバージョンのパラメータの管理に役立ちます。パラメータを変更すると、AWS Systems Manager は自動的に新しいバージョンを保

存し、そのバージョン番号を 1 つ増やします。ラベルは、バージョンが複数ある場合にパラメータバージョンの用途を覚えておくのに役立ちます。

例えば、/MyApp/DB/ConnectionString というパラメータがあるとします。このパラメータの値は、テスト環境のローカルデータベースでの MySQL サーバーへの接続文字列です。アプリケーションの更新が完了したら、そのパラメータでプロダクションデータベースへの接続文字列を使用します。/MyApp/DB/ConnectionString の値を変更します。Systems Manager は、新しい接続文字列でバージョン 2 を自動的に作成します。各バージョンの用途がすぐ思い出せるように、各パラメータにラベルをアタッチします。バージョン 1 にラベル Test をアタッチし、バージョン 2 にラベル Production をアタッチします。

パラメータのラベルは同じパラメータの別のバージョンに移動できます。例えば、新しい本稼働データベース用の接続文字列を使用して /MyApp/DB/ConnectionString パラメータのバージョン 3 を作成した場合、Production ラベルをパラメータのバージョン 2 からバージョン 3 に移動できます。

パラメータラベルは、パラメータタグの軽量の代替です。組織によっては、さまざまな AWS リソースに適用される必要があるタグに対する厳格なガイドラインが存在することがあります。一方、ラベルはパラメータの特定のバージョンに対するテキストの関連付けにすぎません。

タグと同様に、ラベルを使用してパラメータをクエリできます。GetParametersByPath API オペレーションを使用してパラメータセットをクエリする場合に、同じラベルを使用している特定のパラメータバージョンのリストを表示できます (このセクションで後述しています)。

> **Note**
>
> 存在しないパラメータのバージョンを指定するコマンドを実行すると、コマンドは失敗します。パラメータの最新値やデフォルト値にはフォールバックしません。

ラベルの要件と制約

パラメータラベルには以下の要件と制約があります。

- 1 つのパラメータの 1 つのバージョンにアタッチできるラベルは最大 10 個です。
- 同じパラメータの別のバージョンに同じラベルをアタッチすることはできません。例えば、パラメータのバージョン 1 にラベル Production がアタッチされている場合、バージョン 2 にラベル Production をアタッチすることはできません。
- パラメータのラベルは同じパラメータの別のバージョンに移動できます。

- パラメータの作成時にラベルを作成することはできません。ラベルはパラメータの特定のバージョンにアタッチする必要があります。
- パラメータラベルが不要になった場合は、そのラベルをパラメータの別のバージョンに移動したり、削除したりできます。
- ラベルに使用できるのは最大 100 文字です。
- ラベルでは英字 (大文字と小文字が区別される)、数字、ピリオド (.)、ハイフン (-)、アンダースコア (_) を使用できます。
- 数字、「aws」または「ssm」(大文字と小文字は区別されない) で始まるラベルは使用できません。ラベルが上記の要件を満たしていない場合、そのラベルはパラメータバージョンにアタッチされず、そのラベルはシステムによって `InvalidLabels` のリストに表示されます。

トピック

- コンソールを使用したパラメータラベルの操作
- AWS CLI を使用したパラメータラベルの操作

コンソールを使用したパラメータラベルの操作

このセクションでは、Systems Manager コンソールを使用して以下のタスクを実行する方法について説明します。

- コンソールを使用してパラメータラベルを作成する
- コンソールを使用してパラメータにアタッチされているラベルを表示する
- コンソールを使用してパラメータラベルを移動する
- コンソールを使用してパラメータラベルを削除する

コンソールを使用してパラメータラベルを作成する

次の手順では、Systems Manager コンソールを使用して、既存のパラメータの特定のバージョンにラベルをアタッチする方法について説明します。新しいパラメータの作成時にラベルをアタッチすることはできません。

パラメータバージョンにラベルをアタッチするには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。

2. ナビゲーションペインで、[Parameter Store] を選択します。
3. パラメータの名前を選択して、そのパラメータ詳細ページを開きます。
4. [History] タブを選択します。
5. ラベルをアタッチするパラメータバージョンを選択します。
6. [Manage labels] (ラベルを管理) を選択します。
7. [Add new label] (新しいラベルを追加) を選択します。
8. テキストボックスにラベル名を入力します。ラベルを追加するには、[Add new label] (新しいラベルを追加) を選択します。1 つのバージョンに最大 10 個のラベルをアタッチできます。
9. 完了したら、[変更の保存] を選択します。

コンソールを使用してパラメータにアタッチされているラベルを表示する

1 つのパラメータバージョンにアタッチできるラベルは最大 10 個です。次の手順では、Systems Manager コンソールを使用して、1 つのパラメータバージョンにアタッチされているすべてのラベルを表示する方法について説明します。

パラメータバージョンにアタッチされているラベルを表示するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Parameter Store] を選択します。
3. パラメータの名前を選択して、そのパラメータ詳細ページを開きます。
4. [History] タブを選択します。
5. アタッチされているすべてのラベルを表示するパラメータバージョンを見つけます。そのパラメータバージョンにアタッチされているすべてのラベルが [Labels (ラベル)] 列に表示されます。

コンソールを使用してパラメータラベルを移動する

次の手順では、Systems Manager コンソールを使用して、パラメータラベルを同じパラメータの別のバージョンに移動する方法について説明します。

ラベルを別のパラメータバージョンに移動するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。

2. ナビゲーションペインで、[Parameter Store] を選択します。
3. パラメータの名前を選択して、そのパラメータ詳細ページを開きます。
4. [History] タブを選択します。
5. ラベルを移動するパラメータバージョンを選択します。
6. [Manage labels] (ラベルを管理) を選択します。
7. [Add new label] (新しいラベルを追加) を選択します。
8. テキストボックスにラベル名を入力します。
9. 完了したら、[変更の保存] を選択します。

コンソールを使用してパラメータラベルを削除する

次の手順では、Systems Manager コンソールを使用して 1 つまたは複数のパラメータラベルを削除する方法について説明します。

パラメータからラベルを削除するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Parameter Store] を選択します。
3. パラメータの名前を選択して、そのパラメータ詳細ページを開きます。
4. [History] タブを選択します。
5. ラベルを削除するパラメータバージョンを選択します。
6. [Manage labels] (ラベルを管理) を選択します。
7. 削除する各ラベルの横にある [Remove] (削除) を選択します。
8. 完了したら、[変更の保存] を選択します。
9. 変更が正しいことを確認し、テキストボックスに `Confirm` と入力し、[Confirm] (確認) を選択します。

AWS CLI を使用したパラメータラベルの操作

このセクションでは、AWS Command Line Interface (AWS CLI) を使用して以下のタスクを実行する方法について説明します。

- AWS CLI を使用してパラメータラベルを作成する

- AWS CLI を使用してパラメータのラベルを表示する
- AWS CLI を使用してラベルが割り当てられているパラメータのリストを表示する
- AWS CLI を使用してパラメータラベルを移動する
- AWS CLI を使用してパラメータラベルを削除する

AWS CLI を使用してパラメータラベルを作成する

次の手順では、AWS CLI を使用して、既存のパラメータの特定のバージョンにラベルをアタッチする方法について説明します。新しいパラメータの作成時にラベルをアタッチすることはできません。

パラメータラベルを作成するには

1. まだ AWS Command Line Interface (AWS CLI) をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」を参照してください。
2. 次のコマンドを実行すると、ラベルをアタッチするためのアクセス許可があるパラメータのリストが表示されます。

   > **Note**
   >
   > パラメータは、パラメータを作成した AWS リージョン でのみ使用できます。ラベルをアタッチするパラメータが表示されていない場合は、リージョンが正しいかどうかを確認します。

   ```
   aws ssm describe-parameters
   ```

   ラベルをアタッチするパラメータの名前をメモします。
3. パラメータのすべてのバージョンを確認するには、次のコマンドを実行します。

   ```
   aws ssm get-parameter-history --name "parameter-name"
   ```

   ラベルをアタッチするパラメータバージョンをメモします。
4. 次のコマンドを実行して、パラメータに関する情報をバージョン番号別に取得します。

```
aws ssm get-parameters --names "parameter-name:version-number"
```

以下はその例です。

```
aws ssm get-parameters --names "/Production/SQLConnectionString:3"
```

5. 以下のいずれかのコマンドを実行して、1 つのパラメータの 1 つのバージョンにラベルをアタッチします。複数のラベルをアタッチする場合は、ラベル名をスペースで区切ります。

   パラメータの最新バージョンにラベルをアタッチする

   ```
   aws ssm label-parameter-version --name parameter-name  --labels label-name
   ```

   パラメータの特定のバージョンにラベルをアタッチする

   ```
   aws ssm label-parameter-version --name parameter-name --parameter-version version-number --labels label-name
   ```

   次に例を示します。

   ```
   aws ssm label-parameter-version --name /config/endpoint --labels production east-region finance
   ```

   ```
   aws ssm label-parameter-version --name /config/endpoint --parameter-version 3 --labels MySQL-test
   ```

   > **Note**
   >
   > 作成したラベルが InvalidLabels リストに表示されている場合、そのラベルはこのトピックで前述した要件を満たしていません。要件を確認してからもう一度試してください。InvalidLabels リストが空であれば、パラメータのバージョンにラベルが正常に適用されています。

6. バージョン番号またはラベル名を使用することによって、パラメータの詳細を表示できます。前の手順で作成したラベルを指定して、次のコマンドを実行します。

```
aws ssm get-parameter --name parameter-name:label-name --with-decryption
```

このコマンドによって以下のような情報が返されます。

```
{
    "Parameter": {
        "Version": version-number,
        "Type": "parameter-type",
        "Name": "parameter-name",
        "Value": "parameter-value",
        "Selector": ":label-name"
    }
}
```

> **Note**
>
> 出力にある Selector は、Name 入力フィールドで指定したバージョン番号またはラベル名です。

AWS CLI を使用してパラメータのラベルを表示する

GetParameterHistory API オペレーションを使用して、指定したパラメータの完全な履歴とアタッチされているすべてのラベルを表示できます。または、GetParametersByPath API オペレーションを使用して、特定のラベルが割り当てられているすべてのパラメータのリストを表示できます。

GetParameterHistory API オペレーションを使用してパラメータのラベルを表示するには

1. 次のコマンドを実行すると、ラベルを表示できるパラメータのリストが表示されます。

> **Note**
>
> パラメータは、パラメータを作成したリージョンでのみ使用できます。ラベルを表示するパラメータが表示されていない場合は、リージョンが正しいかどうかを確認します。

```
aws ssm describe-parameters
```

ラベルを表示するパラメータの名前を書き留めます。

2. パラメータのすべてのバージョンを確認するには、次のコマンドを実行します。

```
aws ssm get-parameter-history --name parameter-name --with-decryption
```

システムが以下のような情報をレスポンスします。

```
{
    "Parameters": [
        {
            "Name": "/Config/endpoint",
            "LastModifiedDate": 1528932105.382,
            "Labels": [
                "Deprecated"
            ],
            "Value": "MyTestService-June-Release.example.com",
            "Version": 1,
            "LastModifiedUser": "arn:aws:iam::123456789012:user/test",
            "Type": "String"
        },
        {
            "Name": "/Config/endpoint",
            "LastModifiedDate": 1528932111.222,
            "Labels": [
                "Current"
            ],
            "Value": "MyTestService-July-Release.example.com",
            "Version": 2,
            "LastModifiedUser": "arn:aws:iam::123456789012:user/test",
            "Type": "String"
        }
    ]
}
```

AWS CLI を使用してラベルが割り当てられているパラメータのリストを表示する

GetParametersByPath API オペレーションを使用して、特定のラベルが割り当てられている、パス内のすべてのパラメータのリストを表示できます。

次のコマンドを実行すると、特定のラベルが割り当てられている、パス内のパラメータのリストが表示されます。各###############をユーザー自身の情報に置き換えます。

```
aws ssm get-parameters-by-path \
    --path parameter-path \
    --parameter-filters Key=Label,Values=label-name,Option=Equals \
    --max-results a-number \
    --with-decryption --recursive
```

システムが以下のような情報をレスポンスします。次の例では、ユーザーが/Config パス内を検索していました。

```
{
    "Parameters": [
        {
            "Version": 3,
            "Type": "SecureString",
            "Name": "/Config/DBpwd",
            "Value": "MyS@perGr&pass33"
        },
        {
            "Version": 2,
            "Type": "String",
            "Name": "/Config/DBusername",
            "Value": "TestUserDB"
        },
        {
            "Version": 2,
            "Type": "String",
            "Name": "/Config/endpoint",
            "Value": "MyTestService-July-Release.example.com"
        }
    ]
}
```

AWS CLI を使用してパラメータラベルを移動する

次の手順では、パラメータラベルを同じパラメータの別のバージョンに移動する方法について説明します。

パラメータラベルを移動するには

1. パラメータのすべてのバージョンを確認するには、次のコマンドを実行します。*parameter name* を自分の情報に置き換えます。

```
aws ssm get-parameter-history \
    --name "parameter name"
```

   ラベルの移動先と移動元となるパラメータのバージョンを書き留めます。

2. 既存のラベルを別のバージョンのパラメータに割り当てるには、次のコマンドを実行します。各###############をユーザー自身の情報に置き換えます。

```
aws ssm label-parameter-version \
    --name parameter name \
    --parameter-version version number \
    --labels name-of-existing-label
```

> **Note**
>
> 既存のラベルをパラメータの最新バージョンに移動する場合は、上記のコマンドで `--parameter-version` を削除します。

AWS CLI を使用してパラメータラベルを削除する

次の手順では、AWS CLI を使用してパラメータラベルを削除する方法について説明します。

パラメータラベルを削除するには

1. パラメータのすべてのバージョンを確認するには、次のコマンドを実行します。*parameter name* を自分の情報に置き換えます。

```
aws ssm get-parameter-history \
    --name "parameter name"
```

   システムが以下のような情報をレスポンスします。

```
{
    "Parameters": [
```

```
        {
            "Name": "foo",
            "DataType": "text",
            "LastModifiedDate": 1607380761.11,
            "Labels": [
                "l3",
                "l2"
            ],
            "Value": "test",
            "Version": 1,
            "LastModifiedUser": "arn:aws:iam::123456789012:user/test",
            "Policies": [],
            "Tier": "Standard",
            "Type": "String"
        },
        {
            "Name": "foo",
            "DataType": "text",
            "LastModifiedDate": 1607380763.11,
            "Labels": [
                "l1"
            ],
            "Value": "test",
            "Version": 2,
            "LastModifiedUser": "arn:aws:iam::123456789012:user/test",
            "Policies": [],
            "Tier": "Standard",
            "Type": "String"
        }
    ]
}
```

1 つまたは複数のラベルを削除するパラメータのバージョンを書き留めます。

2. 次のコマンドを実行して、そのパラメータから選択したラベルを削除します。各*##########*####をユーザー自身の情報に置き換えます。

```
aws ssm unlabel-parameter-version \
    --name parameter name \
    --parameter-version version \
    --labels label 1,label 2,label 3
```

システムが以下のような情報をレスポンスします。

```
{
    "InvalidLabels": ["invalid"],
    "DeletedLabels" : ["Prod"]
 }
```

Parameter Store でのパラメータバージョンの使用

パラメータの値を編集するたびに、AWS Systems Manager のツールである Parameter Store は、パラメータの新しいバージョンを作成し、以前のバージョンを保持します。最初にパラメータを作成すると、Parameter Store はそのパラメータにバージョン 1 を割り当てます。パラメータの値を変更すると、Parameter Store により自動的にバージョン番号が 1 つ上がります。パラメータの履歴にあるすべてのバージョンの詳細 (値を含む) を表示できます。

API コマンドおよび SSM ドキュメントで使用するパラメータのバージョンを指定することもできます (例: `ssm:MyParameter:3`) 。API コールと SSM ドキュメントでは、パラメータ名と特定のバージョン番号を指定できます。バージョン番号を指定しない場合は、自動的に最新バージョンが使用されます。存在しないバージョンの番号を指定すると、システムはパラメータの最新バージョンまたはデフォルトバージョンにフォールバックするのではなく、エラーを返します。

パラメータバージョンを使用して、一定期間にわたるパラメータの変更回数を確認することもできます。パラメータバージョンでは、パラメータ値が誤って変更された場合、保護のレイヤーも提供されます。

パラメータは最大 100 バージョンまで作成および保守できます。100 バージョンのパラメータを作成した後は、新しいバージョンを作成するたびに、履歴から最も古いバージョンのパラメータが削除され、新しいバージョン用のスペースが作成されます。

この例外は、履歴にすでに 100 個のパラメータバージョンがあり、パラメータの最も古いバージョンにパラメータラベルが割り当てられている場合です。この場合、そのバージョンは履歴から削除されず、新しいパラメータバージョンを作成する要求は失敗します。この保護は、ミッションクリティカルラベルが割り当てられているパラメータバージョンが削除されないようにするためです。新しいパラメータの作成を続行するには、最初に最も古いバージョンのパラメータから、操作で使用するために、ラベルを新しいバージョンのパラメータに移動します。パラメータラベルの移動については、「コンソールを使用してパラメータラベルを移動する」および「AWS CLI を使用してパラメータラベルを移動する」を参照してください。

次の手順では、パラメータを編集し、新しいバージョンが作成されたことを確認する方法を示します。`get-parameter` コマンドと `get-parameters` コマンドを使用して、パラメータバージョン

を表示できます。これらのコマンドの使用例については、AWS Systems Manager API リファレンスの GetParameter と GetParameters を参照してください。

トピック

- コンソールを使用してパラメータの新しいバージョンを作成する
- パラメータバージョンを参照する

コンソールを使用してパラメータの新しいバージョンを作成する

Systems Manager コンソールを使用して、パラメータの新しいバージョンを作成し、パラメータのバージョン履歴を表示できます。

パラメータの新しいバージョンを作成するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Parameter Store] を選択します。
3. 前に作成したパラメータの名前を選択します。新しいパラメータの作成については、「Systems Manager での Parameter Store パラメータの作成」を参照してください。
4. [Edit] を選択します。
5. [Value] ボックスに、新しい値を入力し、[Save changes] を選択します。
6. 更新したパラメータの名前を選択します。[Overview] タブで、バージョン番号が 1 つ増えたことを確認し、新しい値を確認します。
7. パラメータのすべてのバージョンの履歴を表示するには、[履歴] タブを選択します。

パラメータバージョンを参照する

コマンド、API コール、SSM ドキュメントで特定のパラメータバージョンを参照するには、ssm:*parameter-name*:*version-number* という形式を使用できます。

次の例では、`run-instances command` パラメータのバージョン 3 が Amazon Elastic Compute Cloud (Amazon EC2) `golden-ami` で使用されています。

Linux & macOS

```
aws ec2 run-instances \
    --image-id resolve:ssm:/golden-ami:3 \
    --count 1 \
```

```
    --instance-type t2.micro \
    --key-name my-key-pair \
    --security-groups my-security-group
```

Windows

```
aws ec2 run-instances ^
    --image-id resolve:ssm:/golden-ami:3 ^
    --count 1 ^
    --instance-type t2.micro ^
    --key-name my-key-pair ^
    --security-groups my-security-group
```

> **Note**
>
> resolve とパラメータ値は、--image-id オプション、および Amazon Machine Image (AMI) を値として含むパラメータと共にのみ使用できます。詳細については、「」を参照してくださいAmazon マシンイメージ ID の Parameter Store でのパラメータのネイティブサポートの利用

次に、SSM ドキュメント内の MyRunCommandParameter という名前のパラメータのバージョン 2 を指定する例を示します。

YAML

```
---
schemaVersion: '2.2'
description: Run a shell script or specify the commands to run.
parameters:
  commands:
    type: String
    description: "(Required) Specify a shell script or a command to run."
    displayType: textarea
    default: "{{ssm:MyRunCommandParameter:2}}"
mainSteps:
- action: aws:runShellScript
  name: RunScript
  inputs:
    runCommand:
```

```
    - "{{commands}}"
```

JSON

```
{
    "schemaVersion": "2.2",
    "description": "Run a shell script or specify the commands to run.",
    "parameters": {
        "commands": {
            "type": "String",
            "description": "(Required) Specify a shell script or a command to run.",
            "displayType": "textarea",
            "default": "{{ssm:MyRunCommandParameter:2}}"
        }
    },
    "mainSteps": [
        {
            "action": "aws:runShellScript",
            "name": "RunScript",
            "inputs": {
                "runCommand": [
                    "{{commands}}"
                ]
            }
        }
    ]
}
```

Parameter Store での共有パラメータの使用

詳細パラメータを共有することで、マルチアカウント環境での設定データ管理が簡単になります。パラメータは、一元的に保存および管理し、これらのパラメータを参照する必要がある他の AWS アカウント と共有できます。

Parameter Store を AWS Resource Access Manager (AWS RAM) と統合することで、詳細パラメータの共有が可能になります。AWS RAM は、リソースを他の AWS アカウント と共有したり、AWS Organizations を介して共有したりできるようにするサービスです。

AWS RAM を使用したリソース共有。これにより、自身が所有するリソースを共有できます。リソース共有では、共有するリソース、付与するアクセス許可、および共有先のコンシューマーを指定します。コンシューマーには以下が含まれます。

- AWS Organizations の特定の AWS アカウント の組織の内部または外部
- AWS Organizations の組織内の組織単位
- AWS Organizations の組織全体

AWS RAM については、「AWS RAM User Guide」を参照してください。

このトピックでは、所有しているパラメータの共有方法と、共有されているパラメータの使用方法を説明します。

内容

- パラメータを共有するための前提条件
- パラメータの共有
- 共有パラメータの共有を停止する
- 共有パラメータの特定
- 共有パラメータへのアクセス
- パラメータを共有するためのアクセス許可のセット
- 共有パラメータの最大スループット
- 共有パラメータの料金
- 閉鎖された AWS アカウント に対するクロスアカウントアクセス

パラメータを共有するための前提条件

アカウントからパラメータを共有するには、次の前提条件が満たされている必要があります。

- パラメータを共有するには、AWS アカウント でそのパラメータを所有している必要があります。共有を受けているパラメータを共有することはできません。
- パラメータを共有するには、そのパラメータが詳細パラメータ階層に含まれている必要があります。パラメータ階層の詳細については、「パラメータ層の管理」を参照してください。既存の標準パラメータを詳細パラメータに変更する方法については、「スタンダードパラメータをアドバンストパラメータに変更する」を参照してください。
- `SecureString` パラメータを共有するには、カスタマーマネージドキーで暗号化されている必要があります。また、キーは AWS Key Management Service を介して別途共有する必要があります。AWS マネージドキー を共有することはできません。ただし、デフォルトの AWS マネージドキー で暗号化されたパラメータを、カスタマーマネージドキーを使用するように更新することは

できます。AWS KMS キー定義については、「AWS Key Management Service 開発者ガイド」の「AWS KMS の概念」を参照してください。

- 組織、または AWS Organizations 内の組織単位とパラメータを共有するには、AWS Organizations との共有を有効にする必要があります。詳細については、「AWS RAM ユーザーガイド」の「AWS Organizations で共有を有効化する」を参照してください。

パラメータの共有

パラメータを共有するには、リソース共有に追加する必要があります。リソース共有とは、AWS アカウント間で自身のリソースを共有するための AWS RAM リソースです。リソース共有では、共有対象のリソースと、共有先のコンシューマーを指定します。

所有しているパラメータを他のAWS アカウントと共有する場合、2 つの AWS マネージドアクセス許可から選択してコンシューマーに付与できます。詳細については、「パラメータを共有するためのアクセス許可のセット」を参照してください。

AWS Organizations の組織の一員であり、組織内での共有が有効になっている場合は、組織内のコンシューマーに AWS RAM コンソールから共有パラメータへのアクセス権を許可付与できます。これに該当しない場合、コンシューマーはリソース共有への参加の招待を受け取り、その招待を受け入れると、共有パラメータに対するアクセス権が付与されます。

AWS RAM コンソールまたは AWS CLI を使用して、所有しているパラメータを共有できます。

> **Note**
>
> Systems Manager の PutResourcePolicy API オペレーションを使用してパラメータを共有することもできますが、そうではなく AWS Resource Access Manager (AWS RAM) を使用することをお勧めします。これは、`PutResourcePolicy` を使用する場合、AWS RAM PromoteResourceShareCreatedFromPolicy API オペレーションを使用してパラメータを標準リソース共有にプロモートするという追加の手順が必要になるためです。そうしないと、`--shared` オプションを使用する Systems Manager の DescribeParameters API オペレーションによってパラメータが返されません。

AWS RAM コンソールを使用して、自身が所有するパラメータを共有するには

「AWS RAM ユーザーガイド」の「Creating a resource share in AWS RAM」を参照してください。

以下の項目を選択し、手順を完了させてください。

- ステップ 1 ページの [リソース] で Parameter Store Advanced Parameter を選択し、共有する詳細パラメータ階層の各パラメータのボックスを選択します。
- ステップ 2 ページの [マネージドアクセス許可] で、このトピック後半の パラメータを共有するためのアクセス許可のセット で説明されているように、コンシューマーに付与するアクセス許可を選択します。

パラメータ共有の目的に基づいてその他のオプションを選択します。

AWS CLI を使用して、自身が所有するパラメータを共有するには

create-resource-share コマンドを使用して、新しいリソース共有にパラメータを追加します。

associate-resource-share コマンドを使用して、既存のリソース共有にパラメータを追加します。

次の例では、新しいリソース共有を作成して、組織内および個人アカウントのコンシューマーとパラメータを共有します。

```
aws ram create-resource-share \
    --name "MyParameter" \
    --resource-arns "arn:aws:ssm:us-east-2:123456789012:parameter/MyParameter" \
    --principals "arn:aws:organizations::123456789012:ou/o-63bEXAMPLE/ou-46xi-rEXAMPLE"
 "987654321098"
```

共有パラメータの共有を停止する

共有パラメータの共有を停止すると、コンシューマーアカウントはそのパラメータにアクセスできなくなります。

所有しているパラメータの共有を停止するには、リソース共有から削除する必要があります。この操作は、Systems Manager コンソール、AWS RAM コンソール、または AWS CLI を使用して行うことができます。

AWS RAM コンソールを使用して、所有しているパラメータの共有を停止するには

「AWS RAM ユーザーガイド」の「AWS RAM 内のリソース共有を更新する」を参照してください。

AWS CLI を使用して、所有しているパラメータの共有を停止するには

disassociate-resource-share コマンドを使用します。

共有パラメータの特定

所有者とコンシューマーは、AWS CLI を使用して共有パラメータを特定できます。

AWS CLI を使用して共有パラメータを特定するには

AWS CLI を使用して共有パラメータを特定するには、Systems Manager `describe-parameters` コマンドと AWS RAM `list-resources` コマンドから選択できます。

`--shared` オプションを `describe-parameters` とともに使用すると、コマンドは共有されているパラメータを返します。

以下に例を示します。

```
aws ssm describe-parameters --shared
```

共有パラメータへのアクセス

コンシューマーは、AWS コマンドラインツールと AWS SDK を使用して共有パラメータにアクセスできます。コンシューマーアカウントの場合、そのアカウントと共有されているパラメータは [マイパラメータ] ページには含まれません。

CLI の例: AWS CLI を使用して共有パラメータの詳細にアクセスする

AWS CLI を使用して共有パラメータの詳細にアクセスするには、get-parameter または get-parameters コマンドを使用できます。別のアカウントからパラメータを取得するには、`--name` として完全なパラメータ ARN を指定する必要があります。

以下に例を示します。

```
aws ssm get-parameter \
    --name arn:aws:ssm:us-east-2:123456789012:parameter/MySharedParameter
```

共有パラメータがサポートされている統合とサポートされていない統合

現在、共有パラメータは次の統合シナリオで使用できます。

- AWS CloudFormation テンプレートパラメータ
- AWS パラメータとシークレットの Lambda 拡張機能
- Amazon Elastic Compute Cloud (EC2) 起動テンプレート
- Amazon Machine Image (AMI) からインスタンスを作成するための EC2 RunInstances コマンドの `ImageID` の値

- Systems Manager のツールである Automation 用のランブックのパラメータ値の取得

次のシナリオと統合サービスは、現在、共有パラメータの使用をサポートしていません。

- Systems Manager のツールである Run Command のコマンド内のパラメータ
- AWS CloudFormation 動的参照
- AWS CodeBuild の環境変数の値
- AWS App Runner の環境変数の値
- Amazon Elastic Container Service のシークレットの値

パラメータを共有するためのアクセス許可のセット

コンシューマーアカウントには、共有するパラメータへの読み取り専用アクセス権が付与されます。コンシューマーはパラメータの更新や削除ができません。コンシューマーはパラメータを第 3 のアカウントと共有できません。

AWS Resource Access Manager でリソース共有を作成してパラメータを共有する場合、2 つの AWS マネージドアクセス許可セットから選択して、この読み取り専用アクセスを許可できます。

AWSRAMDefaultPermissionSSMParameterReadOnly

実行可能なアクション: `DescribeParameters`、`GetParameter`、`GetParameters`

AWSRAMPermissionSSMParameterReadOnlyWithHistory

実行可能なアクション: `DescribeParameters`、`GetParameter`、`GetParameters`、`GetParameterHistory`

「AWS RAM ユーザーガイド」の「Creating a resource share in AWS RAM」のステップに従う場合は、リソースタイプとして `Parameter Store Advanced Parameters` を選択し、ユーザーがパラメータ履歴を表示するかどうかに応じて、これらのマネージドアクセス許可のいずれかを選択します。

> **Note**
>
> 共有パラメータをプログラムで取得する場合 (例えば AWS Lambda を使用する)、AWS Resource Access Manager API アクションを呼び出す IAM ロールに

`ssm:GetResourcePolicies` と `ssm:PutResourcePolicy` のアクセス許可を追加する必要がある場合があります。

共有パラメータの最大スループット

Systems Manager は、GetParameter オペレーションおよび GetParameters オペレーションの最大スループット (1 秒あたりのトランザクション数) を制限します。スループットは個々のアカウントレベルで適用されます。そのため、共有パラメータを使用する各アカウントは、他のアカウントの影響を受けずに、許容される最大スループットを使用できます。パラメータの最大スループットの詳細については、次のトピックを参照してください。

- Parameter Store スループットの向上
- Amazon Web Services 全般のリファレンス の Systems Manager Service Quotas

共有パラメータの料金

アカウント間の共有は詳細パラメータ階層でのみ利用可能です。詳細パラメータについては、各詳細パラメータのストレージと API の使用量について、現在の価格で料金が発生します。所有しているアカウントには、詳細パラメータのストレージに対して課金されます。共有の詳細パラメータに API コールを行うコンシューマーアカウントには、そのパラメータの使用料が課金されます。

例えば、アカウント A が詳細パラメータ `MyAdvancedParameter` を作成した場合、そのアカウントにはパラメータの保管料として 1 か月あたり 0.05 USD が課金されます。

その後、アカウント A はアカウント B およびアカウント C と `MyAdvancedParameter` を共有します。1 か月の間に、3 つのアカウントが `MyAdvancedParameter` を呼び出すとします。次の表は、それぞれの呼び出し回数に対して発生する料金を示しています。

> **Note**
>
> 次の表の料金は説明のみを目的としています。現在の料金を確認するには、「Parameter Store に対する AWS Systems Manager の料金」を参照してください。

アカウント	呼び出し回数	料金
アカウント A (所有アカウント)	10,000 回の呼び出し	• 1 か月間の詳細パラメータの保存: 0.05 USD • `MyAdvancedParameter` に対する 10,000 回の呼び出し: 0.05 USD • 合計: 0.10 USD
アカウント B (コンシューマーアカウント)	20,000 回の呼び出し	• `MyAdvancedParameter` に対する 20,000 回の呼び出し: 0.10 USD • 合計: 0.10 USD
アカウント C (コンシューマーアカウント)	30,000 回の呼び出し	• `MyAdvancedParameter` に対する 30,000 回の呼び出し: 0.15 USD • 合計: 0.15 USD

閉鎖された AWS アカウント に対するクロスアカウントアクセス

共有パラメータを所有する AWS アカウント が閉鎖されると、すべてのコンシューマーアカウントは共有パラメータにアクセスできなくなります。所有アカウントが閉鎖されてから 90 日以内にアカウントが再開されると、コンシューマーアカウントは以前に共有されていたパラメータに再びアクセスできるようになります。閉鎖後の期間中にアカウントを再開する方法の詳細については、「AWS アカウント管理 リファレンスガイド」の「閉鎖後の AWS アカウント へのアクセス」を参照してください。

Run Command コマンドを使用した Parameter Store でのパラメータの操作

AWS Systems Manager のツールである Run Command でパラメータを使用できます。詳細については、「AWS Systems Manager Run Command」を参照してください。

コンソールを使用して String パラメータを実行する

次の手順では、`String` パラメータを使用するコマンドを実行するプロセスを順を追って説明します。

Parameter Store を使用して文字列パラメータを実行するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Run Command] を選択します。
3. [Run command (コマンドの実行)] を選択します。
4. [コマンドのドキュメント] リストで、[AWS-RunPowerShellScript] (Windows) または [AWS-RunShellScript] (Linux) を選択します。
5. [コマンドパラメータ] で、**echo {{ssm:*parameter-name*}}** と入力します。例: **echo {{ssm:/Test/helloWorld}}**。
6. [Targets] (ターゲット) セクションで、タグの指定、インスタンスやエッジデバイスの手動選択、リソースグループの指定により、このオペレーションを実行するマネージドノードを選択します。

   > **Tip**
   >
   > 表示されるはずのマネージドノードが表示されない場合は、トラブルシューティングのヒントについて「マネージドノードの可用性のトラブルシューティング」を参照してください。

7. [その他のパラメータ] で、以下の操作を行います。
   - [コメント] に、このコマンドに関する情報を入力します。
   - [タイムアウト (秒)] に、コマンドの実行全体が失敗するまでにシステムが待機する秒数を指定します。
8. [レート制御] の場合:
   - [同時実行数] の場合、コマンドを同時に実行するマネージドノードの数または割合を指定します。

     > **Note**
     >
     > マネージドノードに適用されるタグを指定するか、AWS リソースグループを指定してターゲットを選択し、ターゲットとなるマネージドノードの数が不明な場合は、割合を指定してドキュメントを同時に実行できるターゲットの数を制限します。

- [エラーのしきい値] で、ノードの数または割合のいずれかで失敗した後、他のマネージドノードでのコマンドの実行をいつ停止するか指定します。例えば、3 つのエラーを指定した場合、4 番目のエラーが受信されると、システムマネージャー はコマンドの送信を停止します。コマンドを処理しているマネージドノードもエラーを送信する可能性があります。

9. (オプション) コマンド出力をファイルに保存する場合は、[出力オプション] の [S3 バケットにコマンド出力を書き込む] ボックスを選択します。ボックスにバケット名とプレフィックス (フォルダ) 名を入力します。

> **Note**
>
> S3 バケットにデータを書き込む機能を許可する S3 許可は、このタスクを実行する IAM ユーザーのものではなく、インスタンスに割り当てられたインスタンスプロファイル (EC2 インスタンスの場合) または IAM サービスロール (ハイブリッドアクティベーションマシン) のものです。詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」または「ハイブリッド環境に IAM サービスロールを作成する」を参照してください。さらに、指定された S3 バケットが別の AWS アカウント にある場合は、マネージドノードに関連付けられたインスタンスプロファイルまたは IAM サービスロールが、そのバケットへの書き込みに必要なアクセス許可があることを確認してください。

10. [SNS Notifications (SNS 通知)] セクションで、コマンドの実行状態に関する通知を受け取る場合は、[Enable SNS notifications (SNS 通知を有効にする)] チェックボックスをオンにします。

    Run Command 用の Amazon SNS 通知の設定の詳細については、「Amazon SNS 通知を使用した Systems Manager のステータス変更のモニタリング」を参照してください。

11. [Run (実行)] を選択します。

12. [Command ID] (コマンド ID) ページの [Targets and outputs] (ターゲットと出力) エリアで、コマンドを実行したノードの ID の横にあるボタンを選択し、[View output] (出力の表示) を選択します。コマンドの出力が、パラメータに指定した値 (**`This is my first parameter`** など) であることを確認します。

AWS CLI を使用してパラメータを実行する

例 1: シンプルコマンド

次のコマンドの例には、DNS-IP という名前の Systems Manager パラメータが含まれています。このパラメータの値は単純なノードの IP アドレスです。この例では、AWS Command Line Interface (AWS CLI) コマンドを使用してパラメータ値を エコーします。

Linux & macOS

```
aws ssm send-command \
    --document-name "AWS-RunShellScript" \
    --document-version "1" \
    --targets "Key=instanceids,Values=i-02573cafcfEXAMPLE" \
    --parameters "commands='echo {{ssm:DNS-IP}}'" \
    --timeout-seconds 600 \
    --max-concurrency "50" \
    --max-errors "0" \
    --region us-east-2
```

Windows

```
aws ssm send-command ^
    --document-name "AWS-RunPowerShellScript" ^
    --document-version "1" ^
    --targets "Key=instanceids,Values=i-02573cafcfEXAMPLE" ^
    --parameters "commands='echo {{ssm:DNS-IP}}'" ^
    --timeout-seconds 600 ^
    --max-concurrency "50" ^
    --max-errors "0" ^
    --region us-east-2
```

このコマンドによって以下のような情報が返されます。

```
{
    "Command": {
        "CommandId": "c70a4671-8098-42da-b885-89716EXAMPLE",
        "DocumentName": "AWS-RunShellScript",
        "DocumentVersion": "1",
        "Comment": "",
        "ExpiresAfter": "2023-12-26T15:19:17.771000-05:00",
        "Parameters": {
            "commands": [
                "echo {{ssm:DNS-IP}}"
            ]
```

```
        },
        "InstanceIds": [],
        "Targets": [
            {
                "Key": "instanceids",
                "Values": [
                    "i-02573cafcfEXAMPLE"
                ]
            }
        ],
        "RequestedDateTime": "2023-12-26T14:09:17.771000-05:00",
        "Status": "Pending",
        "StatusDetails": "Pending",
        "OutputS3Region": "us-east-2",
        "OutputS3BucketName": "",
        "OutputS3KeyPrefix": "",
        "MaxConcurrency": "50",
        "MaxErrors": "0",
        "TargetCount": 0,
        "CompletedCount": 0,
        "ErrorCount": 0,
        "DeliveryTimedOutCount": 0,
        "ServiceRole": "",
        "NotificationConfig": {
            "NotificationArn": "",
            "NotificationEvents": [],
            "NotificationType": ""
        },
        "CloudWatchOutputConfig": {
            "CloudWatchLogGroupName": "",
            "CloudWatchOutputEnabled": false
        },
        "TimeoutSeconds": 600,
        "AlarmConfiguration": {
            "IgnorePollAlarmFailure": false,
            "Alarms": []
        },
        "TriggeredAlarms": []
    }
}
```

コマンドの実行が完了したら、以下のコマンドを使ってそのコマンドに関する詳細情報を表示できます。

- get-command-invocation — コマンドの実行に関する詳細情報を表示します。
- list-command-invocations — 特定のマネージドノードにおけるコマンドの実行ステータスを表示します。
- list-commands — 複数のマネージドノードにおけるコマンドの実行ステータスを表示します。

例 2: **SecureString** パラメータ値を復号する

次のコマンド例では、SecurePassword という名前の SecureString パラメータを使用します。parameters フィールドで使用されるコマンドは、SecureString パラメータの値を取得および復号化した後、クリアテキストでパスワードを渡すことなくローカル管理者パスワードをリセットします。

Linux

```
aws ssm send-command \
        --document-name "AWS-RunShellScript" \
        --document-version "1" \
        --targets "Key=instanceids,Values=i-02573cafcfEXAMPLE" \
        --parameters '{"commands":["secure=$(aws ssm get-parameters --names
 SecurePassword --with-decryption --query Parameters[0].Value --output text --region
 us-east-2)","echo $secure | passwd myuser --stdin"]}' \
        --timeout-seconds 600 \
        --max-concurrency "50" \
        --max-errors "0" \
        --region us-east-2
```

Windows

```
aws ssm send-command ^
        --document-name "AWS-RunPowerShellScript" ^
        --document-version "1" ^
        --targets "Key=instanceids,Values=i-02573cafcfEXAMPLE" ^
        --parameters "commands=['$secure = (Get-SSMParameterValue -Names
 SecurePassword -WithDecryption $True).Parameters[0].Value','net user administrator
 $secure']" ^
        --timeout-seconds 600 ^
        --max-concurrency "50" ^
        --max-errors "0" ^
        --region us-east-2
```

例 3: SSM ドキュメント内のパラメータを参照する

また、以下の例に示すように、SSM ドキュメントの Parameters セクションで Systems Manager パラメータを参照することもできます。

```
{
   "schemaVersion":"2.0",
   "description":"Sample version 2.0 document v2",
   "parameters":{
      "commands" : {
        "type": "StringList",
        "default": ["{{ssm:parameter-name}}"]
      }
    },
    "mainSteps":[
       {
          "action":"aws:runShellScript",
          "name":"runShellScript",
          "inputs":{
             "runCommand": "{{commands}}"
          }
       }
    ]
}
```

SSM ドキュメントの `runtimeConfig` セクションで使用されている ローカルパラメータと同様の構文を、Parameter Store パラメータと混同しないでください。ローカルパラメータは、Systems Manager のパラメータと同じではありません。「`ssm:`」というプレフィックスを付けないことで、ローカルパラメータを Systems Manager パラメータから区別できます。

```
"runtimeConfig":{
        "aws:runShellScript":{
            "properties":[
                {
                    "id":"0.aws:runShellScript",
                    "runCommand":"{{ commands }}",
                    "workingDirectory":"{{ workingDirectory }}",
                    "timeoutSeconds":"{{ executionTimeout }}"
```

Note

SSM ドキュメントは、SecureString パラメータへのリファレンスをサポートしていません。たとえば、Run Command で SecureString パラメータを使用するには、以下の例に示すように、Run Command に渡す前にパラメータ値を取得する必要があります。

Linux & macOS

```
value=$(aws ssm get-parameters --names parameter-name --with-decryption)
```

```
aws ssm send-command \
    --name AWS-JoinDomain \
    --parameters password=$value \
    --instance-id instance-id
```

Windows

```
aws ssm send-command ^
    --name AWS-JoinDomain ^
    --parameters password=$value ^
    --instance-id instance-id
```

Powershell

```
$secure = (Get-SSMParameterValue -Names parameter-name -WithDecryption
 $True).Parameters[0].Value | ConvertTo-SecureString -AsPlainText -Force
```

```
$cred = New-Object System.Management.Automation.PSCredential -
argumentlist user-name,$secure
```

Amazon マシンイメージ ID の Parameter Store でのパラメータのネイティブサポートの利用

String パラメータを作成するときに、データ型を aws:ec2:image として指定して、入力するパラメータ値が有効な Amazon Machine Image (AMI) ID 形式に確実になるようにできます。

AMI ID 形式のサポートにより、プロセスで使用する AMI が変更されるたびに、すべてのスクリプトとテンプレートを新しい ID で更新する必要がなくなりました。データ型 aws:ec2:image のパラ

メータを作成し、その値として、AMI の ID を入力できます。これは、新しいインスタンスの作成元となる AMI です。このパラメータをテンプレート、コマンド、スクリプトで参照します。

例えば、Amazon Elastic Compute Cloud (Amazon EC2) AMI コマンドを実行するときに、希望の `run-instances` ID を含むパラメータを指定できます。

> **Note**
>
> このコマンドを実行するユーザーには、パラメータ値が検証されるように、`ssm:GetParameters` API オペレーションを含む AWS Identity and Access Management (IAM) アクセス許可が必要です。このアクセス許可がない場合、パラメータ作成プロセスは失敗します。

Linux & macOS

```
aws ec2 run-instances \
    --image-id resolve:ssm:/golden-ami \
    --count 1 \
    --instance-type t2.micro \
    --key-name my-key-pair \
    --security-groups my-security-group
```

Windows

```
aws ec2 run-instances ^
    --image-id resolve:ssm:/golden-ami ^
    --count 1 ^
    --instance-type t2.micro ^
    --key-name my-key-pair ^
    --security-groups my-security-group
```

Amazon EC2 コンソールを使用してインスタンスを作成するときに、希望する AMI を選択することもできます。詳細については、「Amazon EC2 ユーザーガイド」の「Systems Manager パラメータを使用して AMI を検索する」を参照してください。

インスタンス作成ワークフローで別の AMI を使用するときは、パラメータを新しい AMI 値で更新するだけです。正しい形式で ID を入力したことが Parameter Store によって再度検証されます。

aws:ec2:image データ型のパラメータを作成するアクセス許可を付与する

AWS Identity and Access Management (IAM) ポリシーを使用すると、Parameter Store API オペレーションおよびコンテンツへのユーザーアクセスを提供または制限できます。

aws:ec2:image データ型パラメータを作成するには、ユーザーには ssm:PutParameter と ec2:DescribeImages の両方のアクセス許可が必要です。

次のポリシー例では、PutParameter の aws:ec2:image API オペレーションを呼び出すアクセス権限をユーザーに付与します。これは、ユーザーがデータタイプ aws:ec2:image のパラメータをシステムに追加できることを意味します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ssm:PutParameter",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeImages",
            "Resource": "*"
        }
    ]
}
```

AMI 形式の検証の仕組み

パラメータのデータ型として aws:ec2:image を指定した場合、Systems Manager によってパラメータはすぐには作成されません。代わりに、非同期検証オペレーションが実行され、パラメータ値が AMI ID の書式設定要件を満たし、指定された AMI が AWS アカウント で使用可能であることが確認されます。

パラメータのバージョン番号は、検証操作が完了する前に生成されることがあります。パラメータバージョン番号が生成されても、操作が完了しない場合があります。

create および update パラメータのオペレーションに関する通知により、パラメータが正常に作成されたかどうかをモニタリングするには、Amazon EventBridge を使用することをお勧めします。これらの通知は、パラメータのオペレーションが成功したかどうかをレポートします。オペレーションが失敗した場合、通知には失敗の理由を示すエラーメッセージが含まれます。

```
{
    "version": "0",
    "id": "eed4a719-0fa4-6a49-80d8-8ac65EXAMPLE",
    "detail-type": "Parameter Store Change",
    "source": "aws.ssm",
    "account": "111122223333",
    "time": "2020-05-26T22:04:42Z",
    "region": "us-east-2",
    "resources": [
        "arn:aws:ssm:us-east-2:111122223333:parameter/golden-ami"
    ],
    "detail": {
        "exception": "Unable to Describe Resource",
        "dataType": "aws:ec2:image",
        "name": "golden-ami",
        "type": "String",
        "operation": "Create"
    }
}
```

EventBridge での Parameter Store イベントのサブスクライブについては、「Parameter Store イベントに基づいた通知の設定またはアクションのトリガー」を参照してください。

Parameter Store からのパラメータの削除

このトピックでは、AWS Systems Manager のツールである Parameter Store で作成したパラメータを削除する方法について説明します。

> **Warning**
>
> パラメータを削除すると、パラメータのすべてのバージョンが削除されます。一度削除されると、パラメータとそのバージョンを復元することはできません。

コンソールを使用してパラメータを削除するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Parameter Store] を選択します。
3. [マイパラメーター] タブで、削除する各パラメータの横にあるチェックボックスを選択します。

4. [削除] を選択します。
5. 確認ダイアログボックスで、[パラメータを削除] を選択します。

AWS CLI を使用してパラメータを削除するには

- 次のコマンドを実行してください。

```
aws ssm delete-parameter --name "my-parameter"
```

my-parameter は、削除するパラメータの名前に置き換えます。

delete-parameter コマンドで使用できるすべてのオプションについては、AWS CLI コマンドリファレンスの「AWS Systems Manager」セクションの「delete-parameter」を参照してください。

Parameter Store でのパブリックパラメータの使用

一部の AWS のサービスでは、共通のアーティファクトを AWS Systems Manager パブリックパラメータとして公開します。例えば、Amazon Elastic Compute Cloud (Amazon EC2) サービスは、Amazon Machine Images (AMIs) に関する情報をパブリックパラメータとして公開しています。

このガイドのトピック

- Parameter Store でのパブリックパラメータの検出
- Parameter Store で AMI パブリックパラメータを呼び出す
- Parameter Store で ECS 最適化 AMI パブリックパラメータを呼び出す
- Parameter Store で EKS 最適化 AMI パブリックパラメータを呼び出す
- Parameter Store における、AWS のサービス、リージョン、エンドポイント、アベイラビリティーゾーン、Local Zones、Wavelength Zones のパブリックパラメータの呼び出し

関連する AWS ブログ記事

- Query for AWS リージョン, Endpoints, and More Using AWS Systems ManagerParameter Store
- Query for the latest Amazon Linux AMI IDs using AWS Systems ManagerParameter Store
- Query for the Latest Windows AMI Using AWS Systems ManagerParameter Store

Parameter Store でのパブリックパラメータの検出

Parameter Store コンソールまたは AWS Command Line Interface を使用して、パブリックパラメータを検索できます。

パブリックパラメータ名は `aws/service/list` で始まります。名前の次の部分は、そのパラメータを所有するサービスに対応しています。

以下は、パブリックパラメータを提供する AWS のサービスおよびその他のリソースの、一部を記したリストです。

- `ami-amazon-linux-latest`
- `ami-windows-latest`
- `ec2-macos`
- `appmesh`
- `aws-for-fluent-bit`
- `aws-sdk-pandas`
- `bottlerocket`
- `canonical`
- `cloud9`
- `datasync`
- `debian`
- `deeplearning`
- `ecs`
- `eks`
- `fis`
- `freebsd`
- `global-infrastructure`
- `marketplace`
- `neuron`
- `powertools`
- `sagemaker-distribution`
- `storagegateway`

すべてのパブリックパラメータがすべての AWS リージョン に公開されるわけではありません。

Parameter Store コンソールを使用してパブリックパラメータを検索する

コンソールを使用してパブリックパラメータを検索するには、AWS アカウント と AWS リージョン に少なくとも 1 つのパラメータが必要です。

コンソールを使用してパブリックパラメータを検索する

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Parameter Store] を選択します。
3. [Public parameters] (パブリックパラメータ) タブを選択します。
4. [Select a service] (サービスを選択) のドロップダウンを選択します。パラメータを使用するサービスを選択します。
5. (オプション) 検索バーに詳細情報を入力して、選択したサービスが所有するパラメータをフィルタリングします。
6. 使用するパブリックパラメータを選択します。

AWS CLI を使用してパブリックパラメータを検索する

パブリックパラメータの検出に `describe-parameters` を使用します。

`get-parameters-by-path` にリストされているサービスの実際のパスを取得するときに `/aws/service/list` を使用します。サービスのパスを取得するには、パスから `/list` を削除します。例えば、`/aws/service/list/ecs` は `/aws/service/ecs` になります。

Parameter Store で異なるサービスが所有するパブリックパラメータのリストを取得するには、次のコマンドを実行します。

```
aws ssm get-parameters-by-path --path /aws/service/list
```

このコマンドによって以下のような情報が返されます。この例は、スペースの都合上、一部を省略しています。

```
{
    "Parameters": [
        {
            "Name": "/aws/service/list/ami-al-latest",
```

```
            "Type": "String",
            "Value": "/aws/service/ami-al-latest/",
            "Version": 1,
            "LastModifiedDate": "2021-01-29T10:25:10.902000-08:00",
            "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/list/ami-al-latest",
            "DataType": "text"
        },
        {
            "Name": "/aws/service/list/ami-windows-latest",
            "Type": "String",
            "Value": "/aws/service/ami-windows-latest/",
            "Version": 1,
            "LastModifiedDate": "2021-01-29T10:25:12.567000-08:00",
            "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/list/ami-windows-
latest",
            "DataType": "text"
        },
        {
            "Name": "/aws/service/list/aws-storage-gateway-latest",
            "Type": "String",
            "Value": "/aws/service/aws-storage-gateway-latest/",
            "Version": 1,
            "LastModifiedDate": "2021-01-29T10:25:09.903000-08:00",
            "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/list/aws-storage-
gateway-latest",
            "DataType": "text"
        },
        {
            "Name": "/aws/service/list/global-infrastructure",
            "Type": "String",
            "Value": "/aws/service/global-infrastructure/",
            "Version": 1,
            "LastModifiedDate": "2021-01-29T10:25:11.901000-08:00",
            "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/list/global-
infrastructure",
            "DataType": "text"
        }
    ]
}
```


特定のサービスが所有するパラメータを表示する場合は、前のコマンドの実行後に生成されたサービスをリストから選択します。その後、目的のサービスの名前を使用して get-parameters-by-path コールを実行します。

例えば、/aws/service/global-infrastructure と指定します。パスは、1 レベル (指定された値と完全に一致するパラメータのみを呼び出す) または再帰的 (指定した値を超えるパス内の要素を含む) にすることができます。

> **Note**
>
> /aws/service/global-infrastructure パスはすべてのリージョンのクエリでサポートされているわけではありません。詳細については、Parameter Store における、AWS のサービス、リージョン、エンドポイント、アベイラビリティーゾーン、Local Zones、Wavelength Zones のパブリックパラメータの呼び出し を参照してください。

指定したサービスの結果が返されない場合は、--recursive フラグを追加してコマンドを再実行してください。

```
aws ssm get-parameters-by-path --path /aws/service/global-infrastructure
```

これは、global-infrastructure が所有するすべてのパラメータを返します。以下に例を示します。

```
{
    "Parameters": [
        {
            "Name": "/aws/service/global-infrastructure/current-region",
            "Type": "String",
            "LastModifiedDate": "2019-06-21T05:15:34.252000-07:00",
            "Version": 1,
            "Tier": "Standard",
            "Policies": [],
            "DataType": "text"
        },
        {
            "Name": "/aws/service/global-infrastructure/version",
            "Type": "String",
            "LastModifiedDate": "2019-02-04T06:59:32.875000-08:00",
            "Version": 1,
            "Tier": "Standard",
            "Policies": [],
            "DataType": "text"
        }
    ]
```

```
}
```

Option:BeginsWith フィルターを使用して、特定のサービスが所有するパラメータを表示することもできます。

```
aws ssm describe-parameters --parameter-filters "Key=Name, Option=BeginsWith, Values=/
aws/service/ami-amazon-linux-latest"
```

このコマンドによって以下のような情報が返されます。この例では、出力はスペースの都合上、表示されていません。

```
{
    "Parameters": [
        {
            "Name": "/aws/service/ami-amazon-linux-latest/amzn-ami-hvm-x86_64-ebs",
            "Type": "String",
            "LastModifiedDate": "2021-01-26T13:39:40.686000-08:00",
            "Version": 25,
            "Tier": "Standard",
            "Policies": [],
            "DataType": "text"
        },
        {
            "Name": "/aws/service/ami-amazon-linux-latest/amzn-ami-hvm-x86_64-gp2",
            "Type": "String",
            "LastModifiedDate": "2021-01-26T13:39:40.807000-08:00",
            "Version": 25,
            "Tier": "Standard",
            "Policies": [],
            "DataType": "text"
        },
        {
            "Name": "/aws/service/ami-amazon-linux-latest/amzn-ami-hvm-x86_64-s3",
            "Type": "String",
            "LastModifiedDate": "2021-01-26T13:39:40.920000-08:00",
            "Version": 25,
            "Tier": "Standard",
            "Policies": [],
            "DataType": "text"
        }
    ]
}
```

> **Note**
>
> Option=BeginsWith では、別の検索パターンが使用されるため、返されるパラメータが異なる場合があります。

Parameter Store で AMI パブリックパラメータを呼び出す

Amazon Elastic Compute Cloud (Amazon EC2) Amazon Machine Image (AMI) パブリックパラメータは、Amazon Linux 1、Amazon Linux 2、Amazon Linux 2023 (AL2023)、macOS、Windows Server の次のパスから入手できます。

- Amazon Linux 1、Amazon Linux 2、Amazon Linux 2023: `/aws/service/ami-amazon-linux-latest`
- macOS: `/aws/service/ec2-macos`
- Windows Server: `/aws/service/ami-windows-latest`

Amazon Linux 1、Amazon Linux 2、および Amazon Linux 2023 の AMI パブリックパラメータを呼び出す

AWS Command Line Interface (AWS CLI) で次のコマンドを使用して、現在の AWS リージョン にあるすべての Amazon Linux 1、Amazon Linux 2、および Amazon Linux 2023 (AL2023) AMIs のリストを表示できます。

Linux & macOS

```
aws ssm get-parameters-by-path \
    --path /aws/service/ami-amazon-linux-latest \
    --query 'Parameters[].Name'
```

Windows

```
aws ssm get-parameters-by-path ^
    --path /aws/service/ami-amazon-linux-latest ^
    --query Parameters[].Name
```

このコマンドによって以下のような情報が返されます。

```
[
    "/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-6.1-arm64",
    "/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-6.1-x86_64",
    "/aws/service/ami-amazon-linux-latest/al2023-ami-minimal-kernel-6.1-arm64",
    "/aws/service/ami-amazon-linux-latest/al2023-ami-minimal-kernel-6.1-x86_64",
    "/aws/service/ami-amazon-linux-latest/al2023-ami-minimal-kernel-default-arm64",
    "/aws/service/ami-amazon-linux-latest/amzn-ami-hvm-x86_64-gp2",
    "/aws/service/ami-amazon-linux-latest/amzn-ami-hvm-x86_64-s3",
    "/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-ebs",
    "/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2",
    "/aws/service/ami-amazon-linux-latest/amzn2-ami-kernel-5.10-hvm-x86_64-ebs",
    "/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-default-arm64",
    "/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-default-x86_64",
    "/aws/service/ami-amazon-linux-latest/al2023-ami-minimal-kernel-default-x86_64",
    "/aws/service/ami-amazon-linux-latest/amzn-ami-hvm-x86_64-ebs",
    "/aws/service/ami-amazon-linux-latest/amzn-ami-minimal-hvm-x86_64-ebs",
    "/aws/service/ami-amazon-linux-latest/amzn-ami-minimal-hvm-x86_64-s3",
    "/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-arm64-gp2",
    "/aws/service/ami-amazon-linux-latest/amzn2-ami-kernel-5.10-hvm-arm64-gp2",
    "/aws/service/ami-amazon-linux-latest/amzn2-ami-kernel-5.10-hvm-x86_64-gp2",
    "/aws/service/ami-amazon-linux-latest/amzn2-ami-minimal-hvm-arm64-ebs",
    "/aws/service/ami-amazon-linux-latest/amzn2-ami-minimal-hvm-x86_64-ebs"
]
```

AMIs ID と Amazon リソースネーム (ARN) を含むこれらの AMI の詳細を表示するには、次のコマンドを使用します。

Linux & macOS

```
aws ssm get-parameters-by-path \
    --path "/aws/service/ami-amazon-linux-latest" \
    --region region
```

Windows

```
aws ssm get-parameters-by-path ^
    --path "/aws/service/ami-amazon-linux-latest" ^
    --region region
```

*#####*は、米国東部 (オハイオ) リージョンの us-east-2 のように、AWS Systems Manager でサポートされている AWS リージョン の識別子を表します。サポートされている *region* 値の一覧に

ついては、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」にある Region 列を参照してください。

このコマンドによって以下のような情報が返されます。この例では、出力はスペースの都合上、表示されていません。

```
{
    "Parameters": [
         {
            "Name": "/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-6.1-arm64",
            "Type": "String",
            "Value": "ami-0b1b8b24a6c8e5d8b",
            "Version": 69,
            "LastModifiedDate": "2024-03-13T14:05:09.583000-04:00",
            "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/ami-amazon-linux-
latest/al2023-ami-kernel-6.1-arm64",
            "DataType": "text"
        },
        {
            "Name": "/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-6.1-
x86_64",
            "Type": "String",
            "Value": "ami-0e0bf53f6def86294",
            "Version": 69,
            "LastModifiedDate": "2024-03-13T14:05:09.890000-04:00",
            "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/ami-amazon-linux-
latest/al2023-ami-kernel-6.1-x86_64",
            "DataType": "text"
        },
        {
            "Name": "/aws/service/ami-amazon-linux-latest/al2023-ami-minimal-
kernel-6.1-arm64",
            "Type": "String",
            "Value": "ami-09951bb66f9e5b5a5",
            "Version": 69,
            "LastModifiedDate": "2024-03-13T14:05:10.197000-04:00",
            "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/ami-amazon-linux-
latest/al2023-ami-minimal-kernel-6.1-arm64",
            "DataType": "text"
        }
    ]
}
```

特定の AMI の詳細を表示するには、パスを含む完全な AMI 名を指定した GetParameters API オペレーションを使用します。コマンドの例を次に示します。

Linux & macOS

```
aws ssm get-parameters \
    --names /aws/service/ami-amazon-linux-latest/al2023-ami-kernel-6.1-arm64 \
    --region us-east-2
```

Windows

```
aws ssm get-parameters ^
    --names /aws/service/ami-amazon-linux-latest/al2023-ami-kernel-6.1-arm64 ^
    --region us-east-2
```

コマンドは次の情報を返します。

```
{
    "Parameters": [
        {
            "Name": "/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-6.1-arm64",
            "Type": "String",
            "Value": "ami-0b1b8b24a6c8e5d8b",
            "Version": 69,
            "LastModifiedDate": "2024-03-13T14:05:09.583000-04:00",
            "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/ami-amazon-linux-
latest/al2023-ami-kernel-6.1-arm64",
            "DataType": "text"
        }
    ],
    "InvalidParameters": []
}
```

AMI 用の macOS パブリックパラメータを呼び出す

現在の AWS リージョン リージョンで、すべての macOS AMIs のリストを表示するには、AWS CLI で次のコマンドを使用します。

Linux & macOS

```
aws ssm get-parameters-by-path \
```

```
    --path /aws/service/ec2-macos\
    --query 'Parameters[].Name'
```

Windows

```
aws ssm get-parameters-by-path ^
    --path /aws/service/ec2-macos ^
    --query Parameters[].Name
```

このコマンドによって以下のような情報が返されます。

```
[
    "/aws/service/ec2-macos/sonoma/x86_64_mac/latest/image_id",
    "/aws/service/ec2-macos/ventura/x86_64_mac/latest/image_id",
    "/aws/service/ec2-macos/monterey/x86_64_mac/latest/image_id",
    "/aws/service/ec2-macos/sonoma/arm64_mac/latest/image_id",
    "/aws/service/ec2-macos/ventura/arm64_mac/latest/image_id",
    "/aws/service/ec2-macos/monterey/arm64_mac/latest/image_id"
]
```

AMIs ID と Amazon リソースネーム (ARN) を含むこれらの AMI の詳細を表示するには、次のコマンドを使用します。

Linux & macOS

```
aws ssm get-parameters-by-path \
    --path "/aws/service/ec2-macos" \
    --region region
```

Windows

```
aws ssm get-parameters-by-path ^
    --path "/aws/service/ec2-macos" ^
    --region region
```

*#####*は、米国東部 (オハイオ) リージョンの `us-east-2` のように、AWS Systems Manager でサポートされている AWS リージョン の識別子を表します。サポートされている *region* 値の一覧については、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」にある Region 列を参照してください。

このコマンドによって以下のような情報が返されます。この例では、出力はスペースの都合上、表示されていません。

```
{
    "Parameters": [
        ...sample results pending...
    ]
}
```

特定の AMI の詳細を表示するには、パスを含む完全な AMI 名を指定した GetParameters API オペレーションを使用します。コマンドの例を次に示します。

Linux & macOS

```
aws ssm get-parameters \
    --names /aws/service/ec2-macos/...pending... \
    --region us-east-2
```

Windows

```
aws ssm get-parameters ^
     --names /aws/service/ec2-macos/...pending... ^
    --region us-east-2
```

コマンドは次の情報を返します。

```
{
    "Parameters": [
         ...sample results pending...
    ],
    "InvalidParameters": []
}
```

AMI 用の Windows Server パブリックパラメータを呼び出す

現在の AWS リージョン リージョンで、すべての Windows Server AMIs のリストを表示するには、AWS CLI で次のコマンドを使用します。

Linux & macOS

```
aws ssm get-parameters-by-path \
    --path /aws/service/ami-windows-latest \
    --query 'Parameters[].Name'
```

Windows

```
aws ssm get-parameters-by-path ^
    --path /aws/service/ami-windows-latest ^
    --query Parameters[].Name
```

このコマンドによって以下のような情報が返されます。この例では、出力はスペースの都合上、表示されていません。

```
[
    "/aws/service/ami-windows-latest/EC2LaunchV2-Windows_Server-2016-English-Full-
Base",
    "/aws/service/ami-windows-latest/Windows_Server-2016-English-Full-
SQL_2014_SP3_Enterprise",
    "/aws/service/ami-windows-latest/Windows_Server-2016-German-Full-Base",
    "/aws/service/ami-windows-latest/Windows_Server-2016-Japanese-Full-
SQL_2016_SP3_Standard",
    "/aws/service/ami-windows-latest/Windows_Server-2016-Japanese-Full-SQL_2017_Web",
    "/aws/service/ami-windows-latest/Windows_Server-2019-English-Core-
EKS_Optimized-1.25",
    "/aws/service/ami-windows-latest/Windows_Server-2019-Italian-Full-Base",
    "/aws/service/ami-windows-latest/Windows_Server-2022-Japanese-Full-
SQL_2019_Enterprise",
    "/aws/service/ami-windows-latest/Windows_Server-2022-Portuguese_Brazil-Full-Base",
    "/aws/service/ami-windows-latest/amzn2-ami-hvm-2.0.20191217.0-x86_64-gp2-mono",
    "/aws/service/ami-windows-latest/Windows_Server-2016-English-Deep-Learning",
    "/aws/service/ami-windows-latest/Windows_Server-2016-Japanese-Full-
SQL_2016_SP3_Web",
    "/aws/service/ami-windows-latest/Windows_Server-2016-Korean-Full-Base",
    "/aws/service/ami-windows-latest/Windows_Server-2019-English-STIG-Core",
    "/aws/service/ami-windows-latest/Windows_Server-2019-French-Full-Base",
    "/aws/service/ami-windows-latest/Windows_Server-2019-Japanese-Full-
SQL_2017_Enterprise",
    "/aws/service/ami-windows-latest/Windows_Server-2019-Korean-Full-Base",
    "/aws/service/ami-windows-latest/Windows_Server-2022-English-Full-SQL_2022_Web",
    "/aws/service/ami-windows-latest/Windows_Server-2022-Italian-Full-Base",
```

```
    "/aws/service/ami-windows-latest/amzn2-x86_64-SQL_2019_Express",
    "/aws/service/ami-windows-latest/EC2LaunchV2-Windows_Server-2016-English-Core-
Base",
    "/aws/service/ami-windows-latest/Windows_Server-2016-English-Full-
SQL_2019_Enterprise",
    "/aws/service/ami-windows-latest/Windows_Server-2016-English-Full-
SQL_2019_Standard",
    "/aws/service/ami-windows-latest/Windows_Server-2016-Portuguese_Portugal-Full-
Base",
    "/aws/service/ami-windows-latest/Windows_Server-2019-English-Core-
EKS_Optimized-1.24",
    "/aws/service/ami-windows-latest/Windows_Server-2019-English-Deep-Learning",
    "/aws/service/ami-windows-latest/Windows_Server-2019-English-Full-SQL_2017_Web",
    "/aws/service/ami-windows-latest/Windows_Server-2019-Hungarian-Full-Base
]
```

AMIs ID と Amazon リソースネーム (ARN) を含むこれらの AMI の詳細を表示するには、次のコマンドを使用します。

Linux & macOS

```
aws ssm get-parameters-by-path \
    --path "/aws/service/ami-windows-latest" \
    --region region
```

Windows

```
aws ssm get-parameters-by-path ^
    --path "/aws/service/ami-windows-latest" ^
    --region region
```

*#####*は、米国東部 (オハイオ) リージョンの us-east-2 のように、AWS Systems Manager でサポートされている AWS リージョン の識別子を表します。サポートされている *region* 値の一覧については、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」にある Region 列を参照してください。

このコマンドによって以下のような情報が返されます。この例では、出力はスペースの都合上、表示されていません。

```
{
```

```
    "Parameters": [
        {
            "Name": "/aws/service/ami-windows-latest/EC2LaunchV2-Windows_Server-2016-
English-Full-Base",
            "Type": "String",
            "Value": "ami-0a30b2e65863e2d16",
            "Version": 36,
            "LastModifiedDate": "2024-03-15T15:58:37.976000-04:00",
            "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/ami-windows-latest/
EC2LaunchV2-Windows_Server-2016-English-Full-Base",
            "DataType": "text"
        },
        {
            "Name": "/aws/service/ami-windows-latest/Windows_Server-2016-English-Full-
SQL_2014_SP3_Enterprise",
            "Type": "String",
            "Value": "ami-001f20c053dd120ce",
            "Version": 69,
            "LastModifiedDate": "2024-03-15T15:53:58.905000-04:00",
            "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/ami-windows-latest/
Windows_Server-2016-English-Full-SQL_2014_SP3_Enterprise",
            "DataType": "text"
        },
        {
            "Name": "/aws/service/ami-windows-latest/Windows_Server-2016-German-Full-
Base",
            "Type": "String",
            "Value": "ami-063be4935453e94e9",
            "Version": 102,
            "LastModifiedDate": "2024-03-15T15:51:12.003000-04:00",
            "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/ami-windows-latest/
Windows_Server-2016-German-Full-Base",
            "DataType": "text"
        }
    ]
}
```

特定の AMI の詳細を表示するには、パスを含む完全な AMI 名を指定した GetParameters API オペレーションを使用します。コマンドの例を次に示します。

Linux & macOS

```
aws ssm get-parameters \
```

```
    --names /aws/service/ami-windows-latest/EC2LaunchV2-Windows_Server-2016-English-
Full-Base \
    --region us-east-2
```

Windows

```
aws ssm get-parameters ^
    --names /aws/service/ami-windows-latest/EC2LaunchV2-Windows_Server-2016-English-
Full-Base ^
    --region us-east-2
```

コマンドは次の情報を返します。

```
{
    "Parameters": [
        {
            "Name": "/aws/service/ami-windows-latest/EC2LaunchV2-Windows_Server-2016-
English-Full-Base",
            "Type": "String",
            "Value": "ami-0a30b2e65863e2d16",
            "Version": 36,
            "LastModifiedDate": "2024-03-15T15:58:37.976000-04:00",
            "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/ami-windows-latest/
EC2LaunchV2-Windows_Server-2016-English-Full-Base",
            "DataType": "text"
        }
    ],
    "InvalidParameters": []
}
```

Parameter Store で ECS 最適化 AMI パブリックパラメータを呼び出す

Amazon Elastic Container Service (Amazon ECS) サービスは、最新の Amazon ECS 最適化 Amazon Machine Images (AMIs) の名前をパブリックパラメータとして公開します。最適化された AMI にはバグ修正および機能のアップデートが含まれているため、Amazon ECS 用の新しい Amazon Elastic Compute Cloud (Amazon EC2) クラスターを作成するときにこの AMIs を使用することをお勧めします。

次のコマンドを使用して、Amazon Linux 2 用の最新の Amazon ECS 最適化 AMI の名前を表示します。他のオペレーティングシステムのコマンドについては、Amazon Container Service デベロッパーガイドの「Amazon ECS で最適化された AMI メタデータを取得する」を参照してください。

Linux & macOS

```
aws ssm get-parameters \
    --names /aws/service/ecs/optimized-ami/amazon-linux-2/recommended
```

Windows

```
aws ssm get-parameters ^
    --names /aws/service/ecs/optimized-ami/amazon-linux-2/recommended
```

このコマンドによって以下のような情報が返されます。

```
{
    "Parameters": [
        {
            "Name": "/aws/service/ecs/optimized-ami/amazon-linux-2/recommended",
            "Type": "String",
            "Value": "{\"schema_version\":1,\"image_name\":\"amzn2-ami-ecs-
hvm-2.0.20210929-x86_64-ebs\",\"image_id\":\"ami-0c38a2329ed4dae9a\",\"os\":\"Amazon
 Linux 2\",\"ecs_runtime_version\":\"Docker version 20.10.7\",\"ecs_agent_version\":
\"1.55.4\"}",
            "Version": 73,
            "LastModifiedDate": "2021-10-06T16:35:10.004000-07:00",
            "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/ecs/optimized-ami/
amazon-linux-2/recommended",
            "DataType": "text"
        }
    ],
    "InvalidParameters": []
}
```

Parameter Store で EKS 最適化 AMI パブリックパラメータを呼び出す

Amazon Elastic Kubernetes Service (Amazon EKS) サービスは、最新の Amazon EKS 最適化 Amazon Machine Image (AMI) の名前をパブリックパラメータとして公開します。新しいリリースには Kubernetes パッチとセキュリティアップデートが含まれているため、Amazon EKS クラスターにノードを追加するときは、この AMI を使用することをお勧めします。これまでは、最新の AMI を確実に使用しているようにするには、Amazon EKS ドキュメントをチェックしたり、新しい AMI ID を使用してデプロイテンプレートやリソースを手動で更新したりする必要がありました。

次のコマンドを使用して、Amazon Linux 2 用の最新の Amazon EKS 最適化 AMI の名前を表示します。

Linux & macOS

```
aws ssm get-parameters \
    --names /aws/service/eks/optimized-ami/1.14/amazon-linux-2/recommended
```

Windows

```
aws ssm get-parameters ^
    --names /aws/service/eks/optimized-ami/1.14/amazon-linux-2/recommended
```

このコマンドによって以下のような情報が返されます。

```
{
    "Parameters": [
        {
            "Name": "/aws/service/eks/optimized-ami/1.14/amazon-linux-2/recommended",
            "Type": "String",
            "Value": "{\"schema_version\":\"2\",\"image_id\":\"ami-08984d8491de17ca0\",
\"image_name\":\"amazon-eks-node-1.14-v20201007\",\"release_version\":
\"1.14.9-20201007\"}",
            "Version": 24,
            "LastModifiedDate": "2020-11-17T10:16:09.971000-08:00",
            "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/eks/optimized-
ami/1.14/amazon-linux-2/recommended",
            "DataType": "text"
        }
    ],
    "InvalidParameters": []
}
```

Parameter Store における、AWS のサービス、リージョン、エンドポイント、アベイラビリティーゾーン、Local Zones、Wavelength Zones のパブリックパラメータの呼び出し

以下のパスを使用して、パブリックパラメータの AWS リージョン、サービス、エンドポイント、アベイラビリティーゾーン、および Wavelength Zones を呼び出すことができます。

`/aws/service/global-infrastructure`

Note

現在、パス `/aws/service/global-infrastructure` は次の AWS リージョン のクエリについてのみサポートされています:

- 米国東部 (バージニア北部) (us-east-1)
- 米国東部 (オハイオ) (us-east-2)
- 米国西部 (北カリフォルニア) (us-west-1)
- 米国西部 (オレゴン) (us-west-2)
- アジアパシフィック (香港) (ap-east-1)
- アジアパシフィック (ムンバイ) (ap-south-1)
- アジアパシフィック (ソウル) (ap-northeast-2)
- アジアパシフィック (シンガポール) (ap-southeast-1)
- アジアパシフィック (シドニー) (ap-southeast-2)
- アジアパシフィック (東京) (ap-northeast-1)
- カナダ (中部) (ca-central-1)
- ヨーロッパ (フランクフルト) (eu-central-1)
- 欧州 (アイルランド) (eu-west-1)
- ヨーロッパ (ロンドン) (eu-west-2)
- 欧州 (パリ) (eu-west-3)
- 欧州 (ストックホルム) (eu-north-1)
- 南米 (サンパウロ) (sa-east-1)

別の商用リージョンで作業している場合は、クエリでサポートされているリージョンを指定して結果を表示できます。例えば、カナダ西部 (カルガリー) (ca-west-1) リージョンで作業している場合は、クエリでカナダ (中部) (ca-central-1) を指定できます。

```
aws ssm get-parameters-by-path \
    --path /aws/service/global-infrastructure/regions \
    --region ca-central-1
```

アクティブな を表示AWS リージョン

すべてのアクティブな AWS リージョン の一覧を表示するには、AWS Command Line Interface (AWS CLI) で次のコマンドを使用します。

Linux & macOS

```
aws ssm get-parameters-by-path \
    --path /aws/service/global-infrastructure/regions \
    --query 'Parameters[].Name'
```

Windows

```
aws ssm get-parameters-by-path ^
    --path /aws/service/global-infrastructure/regions ^
    --query Parameters[].Name
```

このコマンドによって以下のような情報が返されます。

```
[
    "/aws/service/global-infrastructure/regions/af-south-1",
    "/aws/service/global-infrastructure/regions/ap-east-1",
    "/aws/service/global-infrastructure/regions/ap-northeast-3",
    "/aws/service/global-infrastructure/regions/ap-south-2",
    "/aws/service/global-infrastructure/regions/ca-central-1",
    "/aws/service/global-infrastructure/regions/eu-central-2",
    "/aws/service/global-infrastructure/regions/eu-west-2",
    "/aws/service/global-infrastructure/regions/eu-west-3",
    "/aws/service/global-infrastructure/regions/us-east-1",
    "/aws/service/global-infrastructure/regions/us-gov-west-1",
    "/aws/service/global-infrastructure/regions/ap-northeast-2",
    "/aws/service/global-infrastructure/regions/ap-southeast-1",
    "/aws/service/global-infrastructure/regions/ap-southeast-2",
    "/aws/service/global-infrastructure/regions/ap-southeast-3",
    "/aws/service/global-infrastructure/regions/cn-north-1",
    "/aws/service/global-infrastructure/regions/cn-northwest-1",
    "/aws/service/global-infrastructure/regions/eu-south-1",
    "/aws/service/global-infrastructure/regions/eu-south-2",
    "/aws/service/global-infrastructure/regions/us-east-2",
    "/aws/service/global-infrastructure/regions/us-west-1",
    "/aws/service/global-infrastructure/regions/ap-northeast-1",
    "/aws/service/global-infrastructure/regions/ap-south-1",
    "/aws/service/global-infrastructure/regions/ap-southeast-4",
    "/aws/service/global-infrastructure/regions/ca-west-1",
```

```
    "/aws/service/global-infrastructure/regions/eu-central-1",
    "/aws/service/global-infrastructure/regions/il-central-1",
    "/aws/service/global-infrastructure/regions/me-central-1",
    "/aws/service/global-infrastructure/regions/me-south-1",
    "/aws/service/global-infrastructure/regions/sa-east-1",
    "/aws/service/global-infrastructure/regions/us-gov-east-1",
    "/aws/service/global-infrastructure/regions/eu-north-1",
    "/aws/service/global-infrastructure/regions/eu-west-1",
    "/aws/service/global-infrastructure/regions/us-west-2"
]
```

利用可能な AWS のサービスを表示する

すべての利用可能な AWS のサービスの一覧を表示するには、次のコマンドを使用してアルファベット順にソートします。この例では、出力はスペースの都合上、表示されていません。

Linux & macOS

```
aws ssm get-parameters-by-path \
    --path /aws/service/global-infrastructure/services \
    --query 'Parameters[].Name | sort(@)'
```

Windows

```
aws ssm get-parameters-by-path ^
    --path /aws/service/global-infrastructure/services ^
    --query "Parameters[].Name | sort(@)"
```

このコマンドによって以下のような情報が返されます。この例は、スペースの都合上、一部を省略しています。

```
[
     "/aws/service/global-infrastructure/services/accessanalyzer",
    "/aws/service/global-infrastructure/services/account",
    "/aws/service/global-infrastructure/services/acm",
    "/aws/service/global-infrastructure/services/acm-pca",
    "/aws/service/global-infrastructure/services/ahl",
    "/aws/service/global-infrastructure/services/aiq",
    "/aws/service/global-infrastructure/services/amazonlocationservice",
    "/aws/service/global-infrastructure/services/amplify",
    "/aws/service/global-infrastructure/services/amplifybackend",
```

```
    "/aws/service/global-infrastructure/services/apigateway",
    "/aws/service/global-infrastructure/services/apigatewaymanagementapi",
    "/aws/service/global-infrastructure/services/apigatewayv2",
    "/aws/service/global-infrastructure/services/appconfig",
    "/aws/service/global-infrastructure/services/appconfigdata",
    "/aws/service/global-infrastructure/services/appflow",
    "/aws/service/global-infrastructure/services/appintegrations",
    "/aws/service/global-infrastructure/services/application-autoscaling",
    "/aws/service/global-infrastructure/services/application-insights",
    "/aws/service/global-infrastructure/services/applicationcostprofiler",
    "/aws/service/global-infrastructure/services/appmesh",
    "/aws/service/global-infrastructure/services/apprunner",
    "/aws/service/global-infrastructure/services/appstream",
    "/aws/service/global-infrastructure/services/appsync",
    "/aws/service/global-infrastructure/services/aps",
    "/aws/service/global-infrastructure/services/arc-zonal-shift",
    "/aws/service/global-infrastructure/services/artifact",
    "/aws/service/global-infrastructure/services/athena",
    "/aws/service/global-infrastructure/services/auditmanager",
    "/aws/service/global-infrastructure/services/augmentedairuntime",
    "/aws/service/global-infrastructure/services/aurora",
    "/aws/service/global-infrastructure/services/autoscaling",
    "/aws/service/global-infrastructure/services/aws-appfabric",
    "/aws/service/global-infrastructure/services/awshealthdashboard",
```

AWS のサービスでサポートされているリージョンの表示

サービスが利用可能な AWS リージョン の一覧を表示できます。この例では AWS Systems Manager (ssm) を使用します。

Linux & macOS

```
aws ssm get-parameters-by-path \
    --path /aws/service/global-infrastructure/services/ssm/regions \
    --query 'Parameters[].Value'
```

Windows

```
aws ssm get-parameters-by-path ^
    --path /aws/service/global-infrastructure/services/ssm/regions ^
    --query Parameters[].Value
```

このコマンドによって以下のような情報が返されます。

```
[
    "ap-south-1",
    "eu-central-1",
    "eu-central-2",
    "eu-west-1",
    "eu-west-2",
    "eu-west-3",
    "il-central-1",
    "me-south-1",
    "us-east-2",
    "us-gov-west-1",
    "af-south-1",
    "ap-northeast-3",
    "ap-southeast-1",
    "ap-southeast-4",
    "ca-central-1",
    "ca-west-1",
    "cn-north-1",
    "eu-north-1",
    "eu-south-2",
    "us-west-1",
    "ap-east-1",
    "ap-northeast-1",
    "ap-northeast-2",
    "ap-southeast-2",
    "ap-southeast-3",
    "cn-northwest-1",
    "eu-south-1",
    "me-central-1",
    "us-gov-east-1",
    "us-west-2",
    "ap-south-2",
    "sa-east-1",
    "us-east-1"
]
```

サービスのリージョンのエンドポイントを表示する

サービスのリージョンのエンドポイントを表示するには、次のコマンドを使用します。このコマンドは、米国東部 (オハイオ) (us-east-2) リージョンをクエリします。

Linux & macOS

```
aws ssm get-parameter \
    --name /aws/service/global-infrastructure/regions/us-east-2/services/ssm/
endpoint \
    --query 'Parameter.Value'
```

Windows

```
aws ssm get-parameter ^
    --name /aws/service/global-infrastructure/regions/us-east-2/services/ssm/
endpoint ^
    --query Parameter.Value
```

このコマンドによって以下のような情報が返されます。

```
"ssm.us-east-2.amazonaws.com"
```

アベイラビリティーゾーンの詳細をすべて表示する

以下のコマンドを使用して、アベイラビリティーゾーンを表示できます。

Linux & macOS

```
aws ssm get-parameters-by-path \
    --path /aws/service/global-infrastructure/availability-zones/
```

Windows

```
aws ssm get-parameters-by-path ^
    --path /aws/service/global-infrastructure/availability-zones/
```

このコマンドによって以下のような情報が返されます。この例は、スペースの都合上、一部を省略しています。

```
{
    "Parameters": [
        {
```

```
            "Name": "/aws/service/global-infrastructure/availability-zones/afs1-az3",
            "Type": "String",
            "Value": "afs1-az3",
            "Version": 1,
            "LastModifiedDate": "2020-04-21T12:05:35.375000-04:00",
            "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/
availability-zones/afs1-az3",
            "DataType": "text"
        },
        {
            "Name": "/aws/service/global-infrastructure/availability-zones/aps1-az2",
            "Type": "String",
            "Value": "aps1-az2",
            "Version": 1,
            "LastModifiedDate": "2020-04-03T16:13:57.351000-04:00",
            "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/
availability-zones/aps1-az2",
            "DataType": "text"
        },
        {
            "Name": "/aws/service/global-infrastructure/availability-zones/apse3-az1",
            "Type": "String",
            "Value": "apse3-az1",
            "Version": 1,
            "LastModifiedDate": "2021-12-13T08:51:38.983000-05:00",
            "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/
availability-zones/apse3-az1",
            "DataType": "text"
        }
    ]
}
```

アベイラビリティーゾーンの名前のみを表示する

以下のコマンドを使用して、アベイラビリティーゾーンの名前を表示できます。

Linux & macOS

```
aws ssm get-parameters-by-path \
    --path /aws/service/global-infrastructure/availability-zones \
    --query 'Parameters[].Name | sort(@)'
```

Windows

```
aws ssm get-parameters-by-path ^
    --path /aws/service/global-infrastructure/availability-zones ^
    --query "Parameters[].Name | sort(@)"
```

このコマンドによって以下のような情報が返されます。この例は、スペースの都合上、一部を省略しています。

```
[
    "/aws/service/global-infrastructure/availability-zones/afs1-az1",
    "/aws/service/global-infrastructure/availability-zones/afs1-az2",
    "/aws/service/global-infrastructure/availability-zones/afs1-az3",
    "/aws/service/global-infrastructure/availability-zones/ape1-az1",
    "/aws/service/global-infrastructure/availability-zones/ape1-az2",
    "/aws/service/global-infrastructure/availability-zones/ape1-az3",
    "/aws/service/global-infrastructure/availability-zones/apne1-az1",
    "/aws/service/global-infrastructure/availability-zones/apne1-az2",
    "/aws/service/global-infrastructure/availability-zones/apne1-az3",
    "/aws/service/global-infrastructure/availability-zones/apne1-az4"
```

1 つのリージョンのアベイラビリティーゾーンの名前を表示する

以下のコマンドを使用して、1 つのリージョン (この例では us-east-2) のアベイラビリティーゾーンの名前を表示できます。

Linux & macOS

```
aws ssm get-parameters-by-path \
    --path /aws/service/global-infrastructure/regions/us-east-2/availability-zones \
    --query 'Parameters[].Name | sort(@)'
```

Windows

```
aws ssm get-parameters-by-path ^
    --path /aws/service/global-infrastructure/regions/us-east-2/availability-zones ^
    --query "Parameters[].Name | sort(@)"
```

このコマンドによって以下のような情報が返されます。

```
[
    "/aws/service/global-infrastructure/regions/us-east-2/availability-zones/use2-az1",
    "/aws/service/global-infrastructure/regions/us-east-2/availability-zones/use2-az2",
    "/aws/service/global-infrastructure/regions/us-east-2/availability-zones/use2-az3"
```

アベイラビリティーゾーンの ARN のみを表示する

以下のコマンドを使用して、アベイラビリティーゾーンの Amazon リソースネーム (ARN) のみを表示できます。

Linux & macOS

```
aws ssm get-parameters-by-path \
    --path /aws/service/global-infrastructure/availability-zones \
    --query 'Parameters[].ARN | sort(@)'
```

Windows

```
aws ssm get-parameters-by-path ^
    --path /aws/service/global-infrastructure/availability-zones ^
    --query "Parameters[].ARN | sort(@)"
```

このコマンドによって以下のような情報が返されます。この例は、スペースの都合上、一部を省略しています。

```
[
    "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/availability-
zones/afs1-az1",
    "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/availability-
zones/afs1-az2",
    "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/availability-
zones/afs1-az3",
    "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/availability-
zones/ape1-az1",
    "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/availability-
zones/ape1-az2",
    "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/availability-
zones/ape1-az3",
    "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/availability-
zones/apne1-az1",
```

ローカルゾーンの詳細を表示する

以下のコマンドを使用して、ローカルゾーンを表示できます。

Linux & macOS

```
aws ssm get-parameters-by-path \
    --path /aws/service/global-infrastructure/local-zones
```

Windows

```
aws ssm get-parameters-by-path ^
    --path /aws/service/global-infrastructure/local-zones
```

このコマンドによって以下のような情報が返されます。この例は、スペースの都合上、一部を省略しています。

```
{
    "Parameters": [
        {
            "Name": "/aws/service/global-infrastructure/local-zones/afs1-los1-az1",
            "Type": "String",
            "Value": "afs1-los1-az1",
            "Version": 1,
            "LastModifiedDate": "2023-01-25T11:53:11.690000-05:00",
            "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/
local-zones/afs1-los1-az1",
            "DataType": "text"
        },
        {
            "Name": "/aws/service/global-infrastructure/local-zones/apne1-tpe1-az1",
            "Type": "String",
            "Value": "apne1-tpe1-az1",
            "Version": 1,
            "LastModifiedDate": "2024-03-15T12:35:41.076000-04:00",
            "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/
local-zones/apne1-tpe1-az1",
            "DataType": "text"
        },
        {
            "Name": "/aws/service/global-infrastructure/local-zones/aps1-ccu1-az1",
            "Type": "String",
```

```
            "Value": "aps1-ccu1-az1",
            "Version": 1,
            "LastModifiedDate": "2022-12-19T11:34:43.351000-05:00",
            "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/
local-zones/aps1-ccu1-az1",
            "DataType": "text"
        }
    ]
}
```

Wavelength Zone の詳細を表示する

次のコマンドを使用して、Wavelength Zone を表示することができます。

Linux & macOS

```
aws ssm get-parameters-by-path \
    --path /aws/service/global-infrastructure/wavelength-zones
```

Windows

```
aws ssm get-parameters-by-path ^
    --path /aws/service/global-infrastructure/wavelength-zones
```

このコマンドによって以下のような情報が返されます。この例は、スペースの都合上、一部を省略しています。

```
{
    "Parameters": [
        {
            "Name": "/aws/service/global-infrastructure/wavelength-zones/apne1-wl1-nrt-
wlz1",
            "Type": "String",
            "Value": "apne1-wl1-nrt-wlz1",
            "Version": 3,
            "LastModifiedDate": "2020-12-15T17:16:04.715000-05:00",
            "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/
wavelength-zones/apne1-wl1-nrt-wlz1",
            "DataType": "text"
        },
        {
```

```
            "Name": "/aws/service/global-infrastructure/wavelength-zones/apne2-wl1-sel-
wlz1",
            "Type": "String",
            "Value": "apne2-wl1-sel-wlz1",
            "Version": 1,
            "LastModifiedDate": "2022-05-25T12:29:13.862000-04:00",
            "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/
wavelength-zones/apne2-wl1-sel-wlz1",
            "DataType": "text"
        },
        {
            "Name": "/aws/service/global-infrastructure/wavelength-zones/cac1-wl1-yto-
wlz1",
            "Type": "String",
            "Value": "cac1-wl1-yto-wlz1",
            "Version": 1,
            "LastModifiedDate": "2022-04-26T09:57:44.495000-04:00",
            "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/
wavelength-zones/cac1-wl1-yto-wlz1",
            "DataType": "text"
        }
    ]
}
```

ローカルゾーンのすべてのパラメータと値を表示する

以下のコマンドを使用して、ローカルゾーンのすべてのパラメータデータを表示できます。

Linux & macOS

```
aws ssm get-parameters-by-path \
    --path "/aws/service/global-infrastructure/local-zones/usw2-lax1-az1/"
```

Windows

```
aws ssm get-parameters-by-path ^
    --path "/aws/service/global-infrastructure/local-zones/use1-bos1-az1"
```

このコマンドによって以下のような情報が返されます。この例は、スペースの都合上、一部を省略しています。

```
{
```

```
    "Parameters": [
        {
            "Name": "/aws/service/global-infrastructure/local-zones/use1-bos1-az1/
geolocationCountry",
            "Type": "String",
            "Value": "US",
            "Version": 3,
            "LastModifiedDate": "2020-12-15T14:16:17.641000-08:00",
            "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/
local-zones/use1-bos1-az1/geolocationCountry",
            "DataType": "text"
        },
        {
            "Name": "/aws/service/global-infrastructure/local-zones/use1-bos1-az1/
geolocationRegion",
            "Type": "String",
            "Value": "US-MA",
            "Version": 3,
            "LastModifiedDate": "2020-12-15T14:16:17.794000-08:00",
            "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/
local-zones/use1-bos1-az1/geolocationRegion",
            "DataType": "text"
        },
        {
            "Name": "/aws/service/global-infrastructure/local-zones/use1-bos1-az1/
location",
            "Type": "String",
            "Value": "US East (Boston)",
            "Version": 1,
            "LastModifiedDate": "2021-01-11T10:53:24.634000-08:00",
            "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/
local-zones/use1-bos1-az1/location",
            "DataType": "text"
        },
        {
            "Name": "/aws/service/global-infrastructure/local-zones/use1-bos1-az1/
network-border-group",
            "Type": "String",
            "Value": "us-east-1-bos-1",
            "Version": 3,
            "LastModifiedDate": "2020-12-15T14:16:20.641000-08:00",
            "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/
local-zones/use1-bos1-az1/network-border-group",
            "DataType": "text"
```

```
        },
        {
            "Name": "/aws/service/global-infrastructure/local-zones/use1-bos1-az1/
parent-availability-zone",
            "Type": "String",
            "Value": "use1-az4",
            "Version": 3,
            "LastModifiedDate": "2020-12-15T14:16:20.834000-08:00",
            "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/
local-zones/use1-bos1-az1/parent-availability-zone",
            "DataType": "text"
        },
        {
            "Name": "/aws/service/global-infrastructure/local-zones/use1-bos1-az1/
parent-region",
            "Type": "String",
            "Value": "us-east-1",
            "Version": 3,
            "LastModifiedDate": "2020-12-15T14:16:20.721000-08:00",
            "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/
local-zones/use1-bos1-az1/parent-region",
            "DataType": "text"
        },
        {
            "Name": "/aws/service/global-infrastructure/local-zones/use1-bos1-az1/zone-
group",
            "Type": "String",
            "Value": "us-east-1-bos-1",
            "Version": 3,
            "LastModifiedDate": "2020-12-15T14:16:17.983000-08:00",
            "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/global-infrastructure/
local-zones/use1-bos1-az1/zone-group",
            "DataType": "text"
        }
    ]
}
```

ローカルゾーンのパラメータの名前のみを表示する

以下のコマンドを使用して、ローカルゾーンのパラメータの名前のみを表示できます。

Linux & macOS

```
aws ssm get-parameters-by-path \
```

```
    --path /aws/service/global-infrastructure/local-zones/usw2-lax1-az1 \
    --query 'Parameters[].Name | sort(@)'
```

Windows

```
aws ssm get-parameters-by-path ^
    --path /aws/service/global-infrastructure/local-zones/use1-bos1-az1 ^
    --query "Parameters[].Name | sort(@)"
```

このコマンドによって以下のような情報が返されます。

```
[
    "/aws/service/global-infrastructure/local-zones/use1-bos1-az1/geolocationCountry",
    "/aws/service/global-infrastructure/local-zones/use1-bos1-az1/geolocationRegion",
    "/aws/service/global-infrastructure/local-zones/use1-bos1-az1/location",
    "/aws/service/global-infrastructure/local-zones/use1-bos1-az1/network-border-
group",
    "/aws/service/global-infrastructure/local-zones/use1-bos1-az1/parent-availability-
zone",
    "/aws/service/global-infrastructure/local-zones/use1-bos1-az1/parent-region",
    "/aws/service/global-infrastructure/local-zones/use1-bos1-az1/zone-group"
]
```

Parameter Store のチュートリアル

このセクションのチュートリアルでは、AWS Systems Manager のツールである Parameter Store をテスト環境で使用してパラメータを作成、保存、実行する方法について説明します。さらに、他の Systems Manager ツールで Parameter Store を使用する方法についても説明します。Parameter Store は、他の AWS のサービスで使用することもできます。詳細については、「パラメータとは何ですか?」を参照してください。

内容

- Parameter Store で SecureString パラメータを作成して、ノードをドメインに結合する (PowerShell)

Parameter Store で SecureString パラメータを作成して、ノードをドメインに結合する (PowerShell)

このチュートリアルでは、 AWS Systems Manager `SecureString` パラメータと Run Command を使用して Windows Server ノードをドメインに結合する方法を示します。チュートリアルでは、ドメ

イン名やドメインユーザー名など一般的なドメインパラメータを使用します。これらの値は、暗号化されていない文字列値として渡されます。ドメインパスワードは、AWS マネージドキー を使用して暗号化され、暗号化された文字列として渡されます。

前提条件

このチュートリアルでは、Amazon VPC に関連付けられた DHCP オプションセットでドメイン名と DNS サーバーの IP アドレスを既に指定していることを前提としています。詳細については、Amazon VPC ユーザーガイドの「DHCP オプションセットを使用する」を参照してください。

SecureString パラメータを作成し、ノードをドメインに結合するには

1. AWS Tools for Windows PowerShell を使用してシステムにパラメータを入力します。

   次のコマンドでは、*###############*をユーザー自身の情報で置き換えます。

   ```
   Write-SSMParameter -Name "domainName" -Value "DOMAIN-NAME" -Type String
   Write-SSMParameter -Name "domainJoinUserName" -Value "DOMAIN\USERNAME" -Type String
   Write-SSMParameter -Name "domainJoinPassword" -Value "PASSWORD" -Type SecureString
   ```

   > **Important**
   >
   > SecureString パラメータの値のみが暗号化されます。パラメータ名、説明などのプロパティは暗号化されません。

2. ノードに IAM ロールのアクセス許可をするために、次の AWS Identity and Access Management (IAM) ポリシーを添付します。

   - AmazonSSMManagedInstanceCore – 必須。この AWS 管理ポリシーにより、マネージドノードは Systems Manager サービスのコア機能を使用できます。
   - AmazonSSMDirectoryServiceAccess – 必須。AWS 管理ポリシーでは、マネージドノードによるドメインの結合リクエストに対して、SSM Agent による AWS Directory Service へのアクセスをお客様の代わりに許可します。
   - S3 バケットアクセスのカスタムポリシー – 必須。ノードにあり、Systems Manager タスクを実行する SSM Agent は、Amazon 所有の特有の Amazon Simple Storage Service (Amazon S3) バケットへのアクセスが必要です。作成したカスタムの S3 バケットポリシーで、Systems Manager オペレーションに必要な独自の S3 バケットへのアクセス権も付与します。

例: Run Command コマンドまたは Session Manager セッションの出力を S3 バケットに書き込んだ後、この出力を監査またはトラブルシューティングに使用できます。アクセススクリプトまたはカスタムパッチベースラインリストを S3 バケットに格納してから、コマンドを実行する場合、またはパッチベースラインが適用される場合にスクリプトまたはリストを参照します。

Amazon S3 バケットアクセスのカスタムポリシーの作成の詳細については、「インスタンスプロファイルのカスタム S3 バケットポリシーを作成する」を参照してください。

> **Note**
>
> S3 バケットに出力ログデータを保存することはオプションですが、使用することを決定した場合は、Systems Manager 設定プロセスの最初に設定することをお勧めします。詳細については、Amazon Simple Storage Service ユーザーガイドの「バケットの作成」を参照してください。

- CloudWatchAgentServerPolicy – オプション。この AWS 管理ポリシーでは、マネージドノードで CloudWatch エージェントを実行できます。このポリシーでは、ノードの情報を読み込み、Amazon CloudWatch に書き込むことができます。このポリシーは、Amazon EventBridge や CloudWatch Logs などのサービスを使用する場合にのみ、インスタンスプロファイルに必要です。

> **Note**
>
> CloudWatch と EventBridge 機能の使用はオプションですが、使用することにした場合は、Systems Manager 設定プロセスの開始時にそれらを設定することをお勧めします。詳細については、Amazon EventBridge ユーザーガイドおよび Amazon CloudWatch Logs ユーザーガイドを参照してください。

3. ノードにアタッチされた IAM ロールを編集し、次のポリシーを追加します。このポリシーは、`kms:Decrypt` と `ssm:CreateDocument` API を呼び出すためのアクセス許可をノードに付与します。

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

```
            "Action": [
                "kms:Decrypt",
                "ssm:CreateDocument"
            ],
            "Resource": [
                "arn:aws:kms:region:account-id:key/kms-key-id"
            ]
        }
    ]
}
```

4. 以下の json テキストをコピーしてテキストエディタに貼り付け、ファイルを JoinInstanceToDomain.json として c:\temp\JoinInstanceToDomain.json に保存します。

```
{
    "schemaVersion": "2.2",
    "description": "Run a PowerShell script to securely join a Windows Server
 instance to a domain",
    "mainSteps": [
        {
            "action": "aws:runPowerShellScript",
            "name": "runPowerShellWithSecureString",
            "precondition": {
                "StringEquals": [
                    "platformType",
                    "Windows"
                ]
            },
            "inputs": {
                "runCommand": [
                    "$domain = (Get-SSMParameterValue -Name
 domainName).Parameters[0].Value",
                    "if ((gwmi Win32_ComputerSystem).domain -eq $domain){write-host
 \"Computer is part of $domain, exiting\"; exit 0}",
                    "$username = (Get-SSMParameterValue -Name
 domainJoinUserName).Parameters[0].Value",
                    "$password = (Get-SSMParameterValue -Name domainJoinPassword -
WithDecryption $True).Parameters[0].Value | ConvertTo-SecureString -asPlainText -
Force",
                    "$credential = New-Object
 System.Management.Automation.PSCredential($username,$password)",
```

```
                    "Add-Computer -DomainName $domain -Credential $credential -
ErrorAction SilentlyContinue -ErrorVariable domainjoinerror",
                    "if($?){Write-Host \"Instance joined to domain successfully.
 Restarting\"; exit 3010}else{Write-Host \"Instance failed to join domain with
 error:\" $domainjoinerror; exit 1 }"
                ]
            }
        }
    ]
}
```

5. Tools for Windows PowerShell で次のコマンドを実行して、新しい SSM ドキュメントを作成します。

```
$json = Get-Content C:\temp\JoinInstanceToDomain | Out-String
New-SSMDocument -Name JoinInstanceToDomain -Content $json -DocumentType Command
```

6. Tools for Windows PowerShell で次のコマンドを実行して、ノードをドメインに結合します。

```
Send-SSMCommand -InstanceId instance-id -DocumentName JoinInstanceToDomain
```

コマンドが成功すると、システムは以下のような情報を返します。

```
WARNING: The changes will take effect after you restart the computer EC2ABCD-
EXAMPLE.
Domain join succeeded, restarting
Computer is part of example.local, exiting
```

コマンドが失敗した場合、システムは以下のような情報を返します。

```
Failed to join domain with error:
Computer 'EC2ABCD-EXAMPLE' failed to join domain 'example.local'
from its current workgroup 'WORKGROUP' with following error message:
The specified domain either does not exist or could not be contacted.
```

Parameter Store アクティビティの監査とログ記録

AWS CloudTrail は AWS Systems Manager コンソール、AWS Command Line Interface (AWS CLI)、および Systems Manager SDK で行われた API コールをキャプチャします。CloudTrail コンソールまたは Amazon Simple Storage Service (Amazon S3) バケットで情報を表示できます。ア

カウントのすべての CloudTrail ログは 1 つのバケットを使用します。Systems Manager アクティビティの CloudTrail ログの表示と使用の詳細については、「AWS Systems Manager による AWS CloudTrail API コールのログ記録」を参照してください。Systems Manager の監査と口グ記録のオプションに関する詳細については、「AWS Systems Manager でのログ記録とモニタリング」を参照してください。

Parameter Store のトラブルシューティング

AWS Systems Manager のツールである Parameter Store を使用したトラブルシューティングでは、以下の情報を使用します。

aws:ec2:image パラメータ作成のトラブルシューティング

以下の情報は、aws:ec2:image データ型のパラメータの作成に関する問題のトラブルシューティングに役立ちます。

インスタンスを作成するアクセス許可がない

問題: aws:ec2:image パラメータを使用してインスタンスを作成しようとすると、「このオペレーションを実行する権限がありません」などのエラーメッセージが発生します。

- 解決策: ec2:RunInstances、ec2:DescribeImages、ssm:GetParameter やその他のアクセス許可など、パラメータ値を使用して EC2 インスタンスを作成するのに必要なアクセス許可がすべて揃っていません。組織で管理者アクセス許可を持つユーザーに連絡して、必要なアクセス許可をリクエストしてください。

EventBridge からエラーメッセージ「リソースの定義を取得できません」がレポートされる

問題: aws:ec2:image パラメータを作成するコマンドを実行しましたが、パラメータの作成に失敗しました。「リソースの定義を取得できません」という例外をレポートする通知が Amazon EventBridge から届きます。

解決策: このメッセージは以下のことを示している可能性があります。

- ec2:DescribeImages API オペレーションに必要なすべてのアクセス許可を持っていないか、パラメータで参照される特定のイメージに対するアクセス許可が付与されていません。組織で管理者アクセス許可を持つユーザーに連絡して、必要なアクセス許可をリクエストしてください。
- パラメータ値として入力した Amazon Machine Image (AMI) ID が無効です。作業中の現在の AWS リージョン とアカウントで使用可能な AMI の ID を入力していることを確認してください。

新しい **aws:ec2:image** パラメータを使用できない

問題: aws:ec2:image パラメータを作成するコマンドを実行したところ、バージョン番号がレポートされましたが、そのパラメータは使用できません。

- 解決策: aws:ec2:image データ型を使用するパラメータを作成するコマンドを実行すると、パラメータのバージョン番号がすぐに生成されますが、そのパラメータが使用可能になる前に、パラメータの形式が検証される必要があります。このプロセスには数分かかることがあります。パラメータの作成および検証プロセスをモニタリングするために、以下の操作を行うことができます。
  - EventBridge を使用すると、create および update パラメータのオペレーションに関する通知を受け取ることができます。これらの通知は、パラメータのオペレーションが成功したかどうかをレポートします。EventBridge での Parameter Store イベントのサブスクライブについては、「Parameter Store イベントに基づいた通知の設定またはアクションのトリガー」を参照してください。
  - Systems Manager コンソールの Parameter Store セクションで、パラメータのリストを定期的に更新し、新しいパラメータまたは更新されたパラメータの詳細を検索します。
  - GetParameter コマンドを使用して、新しいパラメータまたは更新されたパラメータを確認します。例えば、AWS Command Line Interface (AWS CLI) で以下のように指定します。

    ```
    aws ssm get-parameter name MyParameter
    ```

    新しいパラメータの場合、パラメータが検証されるまで ParameterNotFound メッセージが返されます。更新する既存のパラメータの場合、パラメータが検証されるまで、新しいバージョンに関する情報は含まれません。

  検証プロセスが完了する前にパラメータを作成または更新しようとすると、システムから検証がまだ進行中であることがレポートされます。パラメータが作成または更新されない場合は、最初の試行から 5 分後に再試行できます。

AWS Systems Manager 運用ツール

運用ツールは、AWS リソースの管理に便利な一連の機能です。

- Systems Manager によってホストされる Amazon CloudWatch ダッシュボード は、CloudWatch コンソールのカスタマイズ可能なホームページであり、単一のビューで AWS リージョン 全体でリソースをモニタリングするために使用できます。

- Explorer は、AWS リソースに関する情報の報告に使用するカスタマイズ可能なオペレーションダッシュボードです。Explorer には、AWS アカウント および AWS リージョン 全体のオペレーションデータ (OpsData) の集約的なビューが表示されます。
- Incident Manager は、AWS でホストされているアプリケーションに影響を与えるインシデントを軽減し、そこから回復するのに役立ちます。
- OpsCenter を利用すると、オペレーションエンジニアや IT プロフェッショナルは AWS リソースに関連した運用上の作業項目 (OpsItems) の表示、調査、解決を一元的に行えます。

トピック

- AWS Systems Manager Incident Manager
- AWS Systems Manager Explorer
- AWS Systems Manager OpsCenter
- Systems Manager がホストする Amazon CloudWatch ダッシュボードの使用

AWS Systems Manager Incident Manager

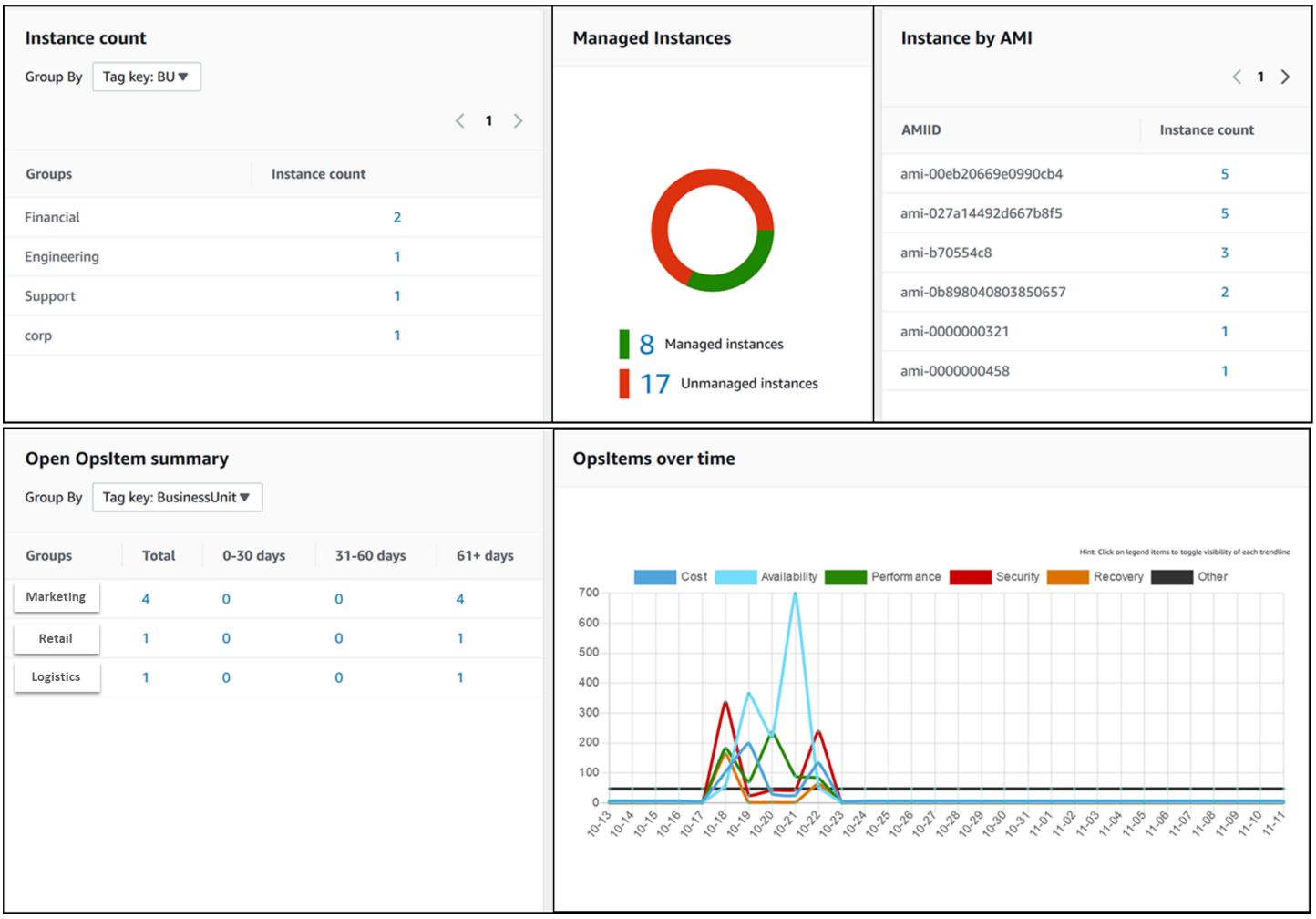
AWS Systems Manager のツールである Incident Manager を使用すると、AWS でホストされたアプリケーションで発生するインシデントを管理できます。Incident Manager は、ユーザーエンゲージメント、エスカレーション、ランブック、対応プラン、チャットチャネル、インシデント後の分析を組み合わせて、チームがインシデントを迅速にトリアージし、アプリケーションを正常に戻すのに役立ちます。Incident Manager の詳細については、Incident Manager ユーザーガイドを参照してください。

AWS Systems Manager Explorer

AWS Systems Manager Explorer は、AWS リソースに関する情報の報告に使用するカスタマイズ可能なオペレーションダッシュボードです。Explorer には、AWS アカウント および AWS リージョン 全体のオペレーションデータ (OpsData) の集約的なビューが表示されます。Explorer では、OpsData にはハイブリッドおよびマルチクラウド環境のマネージドノードに関するメタデータが含まれています。OpsData は、Patch Manager のパッチコンプライアンスや State Manager での関連付けコンプライアンスの詳細など、他の Systems Manager ツールによって提供される情報も含みます。OpsData へのアクセス方法をさらに簡略化するために、Explorer では AWS Config、AWS Trusted Advisor、AWS Compute Optimizer、および AWS サポート (サポートケース) など、これらを使用する AWS のサービスからの情報を表示します。

運用上の認識を上げるために、Explorer は運用作業項目 (OpsItems) も表示します。Explorer では、OpsItems がビジネスユニットまたはアプリケーション全体にどのように分散されているか、それらが時間の経過とともにどのような傾向を示すか、およびカテゴリによってどのように異なるかに関するコンテキストが提供されます。Explorer で情報をグループ化およびフィルタリングすると、自身に関連する項目や、アクションが必要な項目に注目することができます。優先度の高い問題を特定したら、Systems Manager OpsCenter を使用してオートメーションランブックを実行すると、問題をすばやく解決できます。Explorer の使用を開始するには、Systems Manager コンソールを開きます。ナビゲーションペインで、[Explorer] を選択します。

次の図は、Explorer で使用できるウィジェットと呼ばれる個別のレポートボックスの一部を示しています。



Explorer の特徴は何ですか?

Explorer には、以下の特徴があります。

- 実用的な情報のカスタマイズ可能な表示: Explorer には、AWS リソースに関する実用的な情報を自動的に表示するドラッグアンドドロップウィジェットが含まれています。Explorer では、2 種類のウィジェットに情報が表示されます。
  - 情報ウィジェット: これらのウィジェットは、Amazon EC2、Patch Manager、State Manager のほか、AWS Trusted Advisor、AWS、Compute Optimizer、サポート のようなサポートされる AWS のサービスの情報を要約します。これらのウィジェットは、AWS リソースの状態および運用上のリスクを理解するのに役立つ重要なコンテキストを提供します。情報ウィジェットの例としては、[Instance count] (インスタンス数)、[Instance by AMI] (AMI 別インスタンス)、[Total noncompliant nodes] (非準拠ノードの合計数) (パッチ時)、[Noncompliant associations] (非準拠の関連付け)、および [Support Center cases] (サポートセンターのケース) などがあります。
  - OpsItem ウィジェット: OpsItem は、1 つ以上の AWS リソースに関連するオペレーション作業項目です。OpsItems は、Systems Manager OpsCenter の機能です。OpsItems では、DevOps エンジニアが問題を調査し、潜在的に修正しなければならない場合があります。OpsItems の例としては、EC2 インスタンスの CPU 使用率が高いこと、Amazon Elastic Block Store (Amazon EBS) ボリュームのデタッチ、 AWS CodeDeployのデプロイの障害、Systems Manager Automation の実行の障害などがあります。OpsItem ウィジェットの例としては、[Open OpsItem summary (OpsItem のオープンサマリー)]、[OpsItem by status (ステータス別の OpsItem)]、[OpsItems over time (一定期間の OpsItem)] などがあります。
- フィルター: 各ウィジェットは、AWS アカウント、AWS リージョン、タグに基づいて情報をフィルタリングする機能を提供します。フィルターを使用すると、Explorer に表示される情報をすばやく絞り込むことができます。
- サービス画面への直接リンク: AWS リソースの問題を調査しやすくするため、Explorer ウィジェットには、関連するサービス画面への直接リンクが含まれています。ウィジェットに適用されたフィルタは、関連するサービス画面に移動しても引き続き有効です。
- グループ: 組織全体の運用上の問題の種類を理解しやすくするために、一部のウィジェットでは、アカウント、リージョン、タグに基づいてデータをグループ化できます。
- レポートタグキー: Explorer をセットアップするときに、最大 5 つのタグキーを指定できます。これらのキーは、Explorer でデータをグループ化およびフィルタリングするのに役立ちます。指定されたキーが OpsItem を生成するリソースのキーと一致する場合は、キーと値が OpsItems に含まれます。
- AWS アカウント および AWS リージョン 表示の 3 つのモード: Explorer には、AWS アカウント と AWS リージョン での OpsData および OpsItems の次の表示モードが含まれています。
  - 単一アカウント/単一リージョン: これはデフォルトのビューです。このモードでは、ユーザーは自身のアカウントと現在のリージョンからデータと OpsItems を表示できます。

- 単一アカウント/複数リージョン: このモードでは、Explorer の [設定] ページを使用して、1 つ以上のリソースデータ同期を作成する必要があります。リソースデータ同期では、1 つ以上のリージョンから OpsData が集約されます。リソースデータ同期を作成した後、Explorer ダッシュボードで使用する同期を切り替えることができます。その後、リージョンに基づいてデータをフィルタリングおよびグループ化できます。
- 複数アカウント/複数リージョン: このモードでは、組織または会社が、[All features (すべての機能)] を有効にして AWS Organizations を使用する必要があります。コンピューティング環境で AWS Organizations を設定したら、管理アカウントのすべてのアカウントデータを集約できます。その後、リソースデータ同期を作成して、リージョンに基づいてデータをフィルタリングおよびグループ化することができます。Organizations の [すべての機能] モードの詳細については、「組織内のすべての機能の有効化」を参照してください。

- レポート: Explorer レポートをカンマ区切り (.csv) ファイルとして Amazon Simple Storage Service (Amazon S3) バケットにエクスポートできます。エクスポートが完了すると、Amazon Simple Notification Service (Amazon SNS) からアラートを受け取ります。

Explorer と OpsCenter にはどのような関連性がありますか?

Systems Manager OpsCenter は、運用エンジニアや IT プロフェッショナルが AWS リソースに関連する OpsItems を表示、調査、および解決するための一元的な場所を提供します。Explorer はレポートハブであり、DevOps マネージャーによって、AWS リージョン とアカウント全体の運用データ (OpsItems を含む) の集約サマリーが表示されます。Explorer ではユーザーが、傾向やパターンを検出し、必要に応じて Systems Manager オートメーションランブックを使用して問題を迅速に解決することができます。

OpsCenter のセットアップが Explorer のセットアップと統合されました。すでに OpsCenter をセットアップしている場合、Explorer には、OpsItems について集約された情報を含む運用データが自動的に表示されます。OpsCenter をセットアップしていない場合は、Explorer のセットアップを使用して、両方のツールを開始できます。詳細については、「Systems Manager Explorer と OpsCenter の開始方法」を参照してください。

OpsData とは何ですか?

OpsData は、Systems Manager Explorer ダッシュボードに表示されるオペレーションデータです。Explorer は以下のソースから OpsData を取得します。

- Amazon Elastic Compute Cloud (Amazon EC2)

Explorer に表示されるデータには、ノードの総数、マネージドノードとアンマネージドノードの総数、特定の Amazon Machine Image (AMI) を使用するノードの数が含まれます。

- Systems Manager OpsCenter

  Explorer に表示されるデータには、ステータス別の OpsItems の数、重要度別の OpsItems の数、グループ全体で 30 日間にわたって開かれた OpsItems の数、OpsItems の長期の履歴データが含まれます。

- Systems Manager Patch Manager

  Explorer に表示されるデータにより、通常の非準拠ノードと、重大な非準拠ノードの数を確認できます。

- AWS Trusted Advisor

  Explorer に表示されるデータには、コストの最適化、セキュリティ、耐障害性、パフォーマンス、サービス制限の各分野における、EC2 リザーブドインスタンスのためのベストプラクティスチェックに関するステータスが含まれます。

- AWS Compute Optimizer

  Explorer に表示されるデータには、アンダープロビジョニングおよびオーバープロビジョニングされた EC2 インスタンスの数、最適化の結果、オンデマンド料金の詳細、インスタンスタイプと価格の推奨事項が含まれます。

- サポート センターのケース

  Explorer に表示されるデータには、ケース ID、重大度、ステータス、作成時刻、件名、サービス、カテゴリが含まれます。

- AWS Config

  Explorerに表示されるデータには、準拠および非準拠の AWS Config ルールの全体的な要約、準拠および非準拠のリソースの数、そして各リソースに関する具体的な詳細情報 (非準拠のルールまたはリソースをドリルダウンする場合) が含まれます。

- AWS Security Hub

  Explorer に表示されるデータには、Security Hub の結果の全体的な概要、重要度別にグループ化された各検出の数、および検索に関する詳細情報が含まれます。

> **Note**
>
> Explorer で AWS Trusted Advisor および サポート Center のケースを表示するには、AWS サポート を使用してエンタープライズアカウントまたはビジネスアカウントを設定する必要があります。

OpsData ソースの表示や管理は Explorer の [Settings (設定)] ページから行えます。Explorer ウィジェットに OpsData を入力するサービスのセットアップと設定については、「Explorer のための関連サービスのセットアップ」を参照してください。

Explorer の使用料金はかかりますか?

はい。統合セットアップ中に OpsItems を作成するためのデフォルトルールを有効にすると、OpsItems を自動的に作成するプロセスが開始されます。アカウントには、月ごとに作成された OpsItems の数に基づいて課金されます。アカウントは、月ごとに実行された `GetOpsItem`、`DescribeOpsItem`、`UpdateOpsItem`、`GetOpsSummary` API コールの数に基づいて課金されます。さらに、関連する診断情報を公開する他のサービスへのパブリック API コールに対して課金される場合があります。詳細については、AWS Systems Manager 料金を参照してください。

トピック

- Systems Manager Explorer と OpsCenter の開始方法
- Explorer の使用
- Systems Manager Explorer から OpsData をエクスポートする
- Systems Manager Explorer のトラブルシューティング

Systems Manager Explorer と OpsCenter の開始方法

AWS Systems Manager では、統合セットアップエクスペリエンスを使用して、Systems Manager Explorer と Systems Manager OpsCenter の利用を開始できます。このドキュメントでは、Explorer と OpsCenter のセットアップは統合セットアップと呼ばれます。すでに OpsCenter をセットアップしている場合は、統合セットアップを完了して、設定とオプションを確認する必要があります。OpsCenter をセットアップしていない場合は、統合セットアップを使用することで両方のツールの使用を開始できます。

> **Note**
>
> 統合セットアップは、Systems Manager コンソールでのみ使用できます。ExplorerまたはOpsCenter をプログラム的にセットアップすることはできません。

統合セットアップでは、以下のタスクを実行します。

- ロールとアクセス権限を設定する: 統合セットアップでは、AWS Identity and Access Management (IAM)ロールを作成します。このロールを使用すると、Amazon EventBridge OpsItemsがデフォルトのルールに基づいて OpsItems を自動的に作成できます。設定後、このセクションの説明に従って、OpsCenter のユーザー、グループ、ロールのアクセス許可を設定する必要があります。
- OpsItem 作成のデフォルトルールを許可: 統合セットアップでは、EventBridge にデフォルトルールが作成されます。これらのルールに従って、イベントに応じて OpsItems が自動的に作成されます。これらのイベントの例としては、AWS リソースの状態の変更、セキュリティ設定の変更、サービス使用不可などがあります。
- OpsData ソースのアクティブ化: 統合セットアップでは、Explorer ウィジェットに入力される次のデータソースがアクティブ化されます。
  - サポート センター (このソースをアクティブにするには、ビジネスまたはエンタープライズサポートプランが必要です)。
  - AWS Compute Optimizer (このソースをアクティブにするには、ビジネスまたはエンタープライズサポートプランが必要です)。
  - Systems Manager State Manager の関連付けのコンプライアンス
  - AWS Config Compliance
  - Systems Manager OpsCenter
  - Systems Manager Patch Manager のパッチコンプライアンス
  - Amazon Elastic Compute Cloud (Amazon EC2)
  - Systems Manager Inventory
  - AWS Trusted Advisor (このソースをアクティブにするには、ビジネスまたはエンタープライズサポートプランが必要です)。
  - AWS Security Hub

> **Note**
>
> セットアップ設定は、[設定] ページでいつでも変更できます。

統合セットアップが完了したら、複数のリージョンおよびアカウントのデータを表示するように Explorer をセットアップすることをお勧めします。Explorer と OpsCenter は、統合セットアップの完了時に使用した AWS アカウント と AWS リージョン の OpsData と OpsItems を自動的に同期します。他のアカウントやリージョンから OpsData と OpsItems を集約するには、リソースデータ同期を作成します。

Explorer のための関連サービスのセットアップ

AWS Systems Manager Systems Manager Explorer と AWS Systems Manager OpsCenter は、他の AWS のサービスおよび Systems Manager ツールから情報を収集するか、またはインタラクションします。統合セットアップを使用する前に、これらの他のサービスやツールをセットアップおよび設定することをお勧めします。

次の表には、Explorer と OpsCenter が他の AWS のサービスや Systems Manager ツールから情報を収集したり、それらと対話したりできるようにするタスクが含まれています。

タスク	情報
Systems Manager Automation でアクセス許可を確認する	Explorer と OpsCenter では、Systems Manager Automation ランブックを使用して AWS リソースに関する問題を修復できます。この修復ツールを使用するには、Systems Manager Automation ランブックを実行するためのアクセス許可が必要です。詳細については、「オートメーションの設定」を参照してください。
Systems Manager Patch Manager をセットアップして設定する	Explorer には、パッチのコンプライアンスに関する情報を提供するウィジェットが含まれています。Explorer でこのデータを表示するには、パッチ適用を設定する必要があります。詳細については、「AWS Systems Manager Patch Manager」を参照してください。

タスク	情報
Systems Manager State Manager をセットアップして設定する	Explorer には、Systems Manager State Manager 関連付けのコンプライアンスに関する情報を提供するウィジェットが含まれています。Explorer でこのデータを表示するには、State Manager を設定する必要があります。詳細については、「AWS Systems Manager State Manager」を参照してください。
AWS Config 設定レコーダーの有効化	Explorer は、AWS Config 設定レコーダーから提供されるデータを使用して、EC2 インスタンスに関する情報をウィジェットに入力します。Explorer でこのデータを表示するには、AWS Config 設定レコーダーを有効にします。詳細については、「設定レコーダーの管理」を参照してください。 **Note** 設定レコーダーを有効にした後、Systems Manager が EC2 インスタンスに関する情報を表示する Explorer ウィジェットにデータを表示できるようになるまでに、最大 6 時間かかる場合があります。

タスク	情報
AWS Trusted Advisor をオンにする	Explorer では、Amazon EC2 リザーブドインスタンスのベストプラクティスチェックでの (コストの最適化、セキュリティ、耐障害性、パフォーマンス、サービスの制限に関する) ステータスを表示するために、Trusted Advisor によって提供されるデータを使用します。Explorer でこのデータを表示するには、ビジネスサポートプランまたはエンタープライズサポートプランが必要です。詳細については、「サポート」を参照してください。
AWS Compute Optimizer をオンにする	Explorer は、Compute Optimizer によって提供されるデータを使用して、アンダープロビジョニングおよびオーバープロビジョニングされた EC2 インスタンスの数、最適化の結果、オンデマンド料金の詳細、インスタンスタイプと料金の推奨事項を表示します。Explorer でこのデータを表示するには、Compute Optimizer を有効にします。詳細については、「AWS Compute Optimizer の使用開始」を参照してください。
AWS Security Hub をオンにする	Explorer は、Security Hub から提供されたデータを使用して、セキュリティ検出結果に関する情報をウィジェットに入力します。このデータを Explorer で表示するには、Security Hub の統合を有効にします。詳細については、「AWS Security Hub とは」を参照してください。

Systems Manager Explorer のロールとアクセス許可の設定

統合セットアップは、AWS Systems Manager Explorer と AWS Systems Manager OpsCenter の AWS Identity and Access Management (IAM) ロールを自動的に作成および設定します。統合セットアップを完了した場合、Explorer のロールとアクセス権限を設定するために追加のタスクを実行する

必要はありません。ただし、このトピックで後述するように、OpsCenter のアクセス権限を設定する必要があります。

統合セットアップでは、Explorer および OpsCenter を操作するための以下のロールが作成、設定されます。

- `AWSServiceRoleForAmazonSSM`: Systems Manager が管理または使用する AWS リソースへのアクセスを提供します。
- `OpsItem-CWE-Role`: 一般的なイベントに応答して、CloudWatch Events と EventBridge が OpsItems を作成することを許可します。
- `AWSServiceRoleForAmazonSSM_AccountDiscovery`: Systems Manager が、データの同期時に他の AWS のサービスを呼び出して AWS アカウント 情報を検出できるようにします。このロールの詳細については、「ロールを使用した OpsCenter および Explorer の AWS アカウント 情報の収集」を参照してください。
- `AmazonSSMExplorerExport`: Explorer が OpsData をカンマ区切り値 (CSV) ファイルにエクスポートできるようにします。

AWS Organizations とリソースデータ同期を使用して複数のアカウントとリージョンのデータを表示するように Explorer を設定すると、Systems Manager が `AWSServiceRoleForAmazonSSM_AccountDiscovery` サービスにリンクされたロールを作成します。Systems Manager は、このロールを使用して、AWS Organizations の AWS アカウント に関する情報を取得します。ロールは以下のアクセス権限ポリシーを使用します。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "organizations:DescribeAccount",
            "organizations:DescribeOrganization",
            "organizations:ListAccounts",
            "organizations:ListAWSServiceAccessForOrganization",
            "organizations:ListChildren",
            "organizations:ListParents"
         ],
         "Resource":"*"
      }
   ]
```

```
}
```

AWSServiceRoleForAmazonSSM_AccountDiscovery ロールの詳細については、「ロールを使用した OpsCenter および Explorer の AWS アカウント 情報の収集」を参照してください。

Systems Manager OpsCenter のアクセス許可を設定する

統合セットアップを完了したら、ユーザーが OpsCenter でアクションを実行できるように、ユーザー、グループ、ロールのアクセス許可を設定する必要があります。

[開始する前に]

OpsCenter では、OpsItems を 1 つのアカウントのみで作成および管理するように設定することも、あるいは複数のアカウントにわたって作成および管理するように設定することもできます。複数のアカウントにわたって OpsItems を作成および管理するように OpsCenter を設定した場合、Systems Manager 委任管理者アカウントまたは AWS Organizations 管理アカウントから他のアカウントの OpsItems を手動で作成、表示、編集することができます。Systems Manager 委任管理者アカウントの詳細については、「Explorer のための委任された管理者の設定」を参照してください。

ただし、1 つのアカウントのみで作成および管理するよう OpsCenter を設定した場合は、OpsItems を作成したアカウントでのみ OpsItems を表示または編集できます。AWS アカウント 間で OpsItems を共有または転送することはできません。そのため、AWS ワークロードの実行に使用している AWS アカウント で、OpsCenter のアクセス権限を設定することをお勧めします。これで、そのアカウントで ユーザーまたはグループを作成することができます。このように、複数のオペレーションエンジニアまたは IT プロフェッショナルが同じ AWS アカウント で OpsItems を作成、表示、編集することができます。

Explorer と OpsCenter では、次の API オペレーションを使用します。ユーザー、グループ、ロールにこれらのアクションへのアクセス権がある場合は、Explorer および OpsCenter のすべての機能を使用できます。このセクションで後述するように、より制限的なアクセスを作成することもできます。

- CreateOpsItem
- CreateResourceDataSync
- DescribeOpsItems
- DeleteResourceDataSync
- GetOpsItem
- GetOpsSummary

- ListResourceDataSync
- UpdateOpsItem
- UpdateResourceDataSync

必要に応じて次のインラインポリシーをアカウント、グループ、ロールに追加することで、読み取り専用のアクセス許可を指定できます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:GetOpsItem",
        "ssm:GetOpsSummary",
        "ssm:DescribeOpsItems",
        "ssm:GetServiceSetting",
        "ssm:ListResourceDataSync"
      ],
      "Resource": "*"
    }
  ]
}
```

IAM ユーザーポリシーの作成と編集の詳細については、IAM ユーザーガイドの「IAM ポリシーの作成」を参照してください。このポリシーを IAM グループに割り当てる方法については、「IAM グループへのポリシーのアタッチ」を参照してください。

以下を使用してアクセス許可を作成し、ユーザー、グループ、ロールに追加します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:GetOpsItem",
        "ssm:UpdateOpsItem",
        "ssm:DescribeOpsItems",
        "ssm:CreateOpsItem",
        "ssm:CreateResourceDataSync",
```

```
        "ssm:DeleteResourceDataSync",
        "ssm:ListResourceDataSync",
        "ssm:UpdateResourceDataSync"

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

組織で使用しているアイデンティティアプリケーションに応じて、次のオプションのいずれかを選択し、ユーザーアクセスを設定できます。

アクセス権限を付与するにはユーザー、グループ、またはロールにアクセス許可を追加します。

- AWS IAM Identity Center のユーザーとグループ:

  アクセス許可セットを作成します。「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」の手順に従ってください。
- IAM 内で、ID プロバイダーによって管理されているユーザー:

  ID フェデレーションのロールを作成します。詳細については「IAM ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) 用のロールを作成する」を参照してください。
- IAM ユーザー:
  - ユーザーが担当できるロールを作成します。手順については「IAM ユーザーガイド」の「IAM ユーザーのロールの作成」を参照してください。
  - (お奨めできない方法) ポリシーをユーザーに直接アタッチするか、ユーザーをユーザーグループに追加します。詳細については「IAM ユーザーガイド」の「ユーザー (コンソール) へのアクセス権限の追加」を参照してください。

タグを使用した OpsItems へのアクセスの制限

また、タグを指定するインライン IAM ポリシーを使用して、OpsItems へのアクセスを制限することもできます。タグキー Department とタグ値 Finance を指定する例を以下に示します。このポリシーでは、ユーザーは GetOpsItem API オペレーションを呼び出して、以前、Key=Department および Value=Finance とタグ付けされていた OpsItems のみを表示できます。それ以外の OpsItems を表示することはできません。

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:GetOpsItem"
             ],
      "Resource": "*"
      ,
      "Condition": { "StringEquals": { "ssm:resourceTag/Department": "Finance" } }
    }
  ]
}
```

OpsItems を表示し、更新するための API オペレーションを指定する例を以下に示します。このポリシーでは、タグキーと値の 2 組のペア (Department-Finance と Project-Unity) も指定します。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "ssm:GetOpsItem",
            "ssm:UpdateOpsItem"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "ssm:resourceTag/Department":"Finance",
               "ssm:resourceTag/Project":"Unity"
            }
         }
      }
   ]
}
```

OpsItem へのタグの追加については、「OpsItems を手動で作成する」を参照してください。

統合セットアップで作成されたデフォルト EventBridge ルールを理解する

Explorer と OpsCenter の統合セットアッププロセス中に、Amazon EventBridge によって検出されたイベントに基づいて特定のデフォルトルールを有効にすることができます。これらのイベントが検

出されると、システムは自動的に AWS Systems Manager の OpsCenter 内に OpsItems を作成します。

例えば、EC2 自動スケーリング インスタンスの終了が失敗すると、ルール `SSMOpsItems-Autoscaling-instance-termination-failure` によって OpsItem が作成されます。

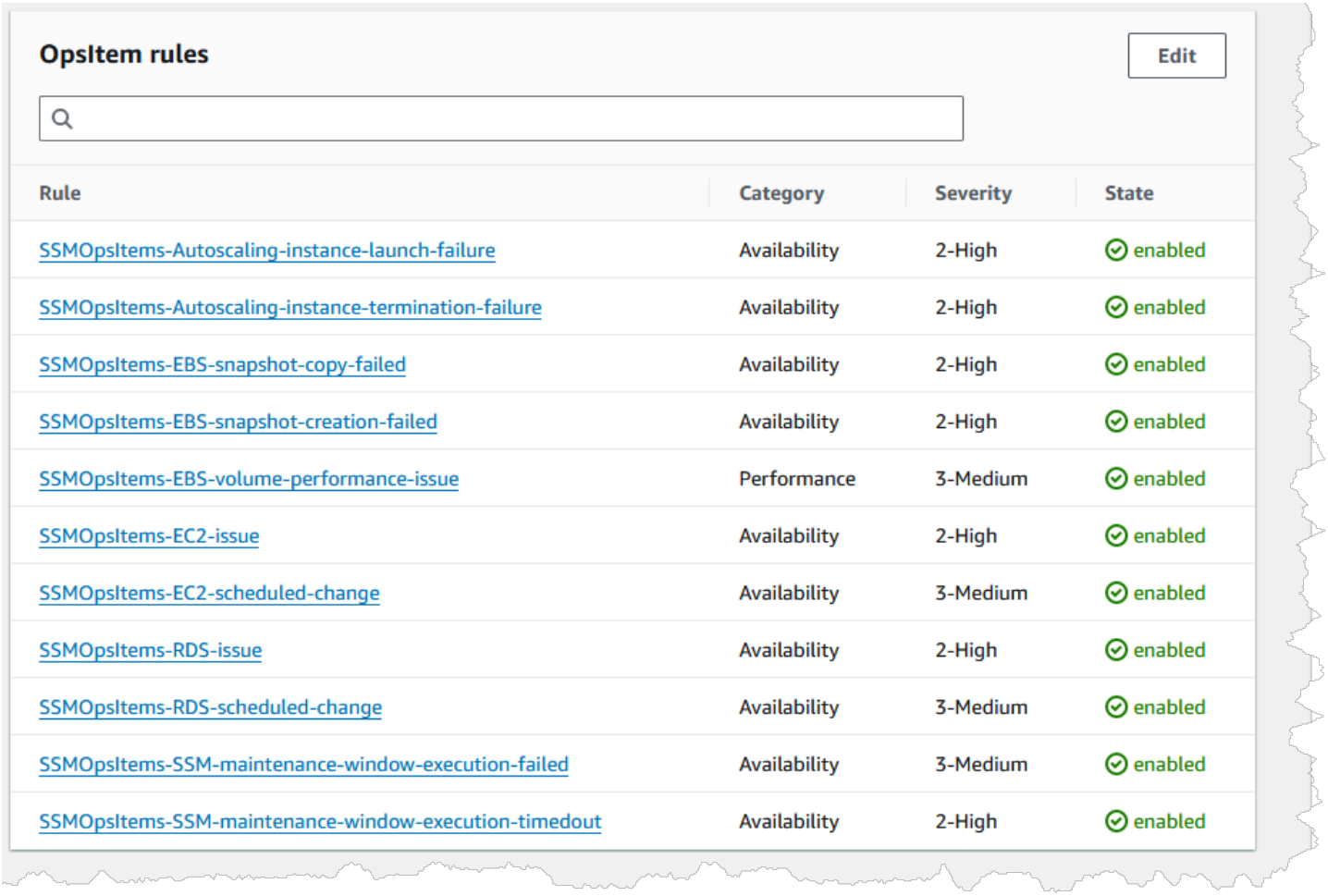
このルール `SSMOpsItems-SSM-maintenance-window-execution-failed` は、Systems Manager のメンテナンスウィンドウが正常に完了しなかった場合に OpsItem を作成します。

セットアップ手順と、セットアッププロセス中に有効にできるすべての EventBridge ルールの詳細については、OpsCenter を設定する を参照してください。

EventBridge でこれらのイベントの OpsItems を作成しないようにするには、「統合セットアップ」でこのオプションをオフにすることができます。必要に応じて、特定の EventBridge イベントのターゲットとして OpsCenter を指定できます。詳細については、「EventBridge ルールを設定して OpsItems を作成する」を参照してください。

デフォルトのルールを無効にするか、もしくは OpsCenter の [設定] ページで [OpsCenter 設定] を選択してカテゴリと重要度レベルを変更してから [OpsItem ルール] エリアで [編集] を選択します。

または、Systems Manager コンソールで、これらのルールから作成された個別の OpsItem に割り当てられたカテゴリまたは重要度を編集することもできます。詳細については、OpsItem の編集 を参照してください。



Explorer のための委任された管理者の設定

AWS Organizations とのリソースデータの同期を使用して、複数の AWS リージョン とアカウントから AWS Systems Manager Explorer データを集約する場合は、Explorer の委任管理者を設定することをお勧めします。

代理管理者は、以下のコンソール、SDK、AWS Command Line Interface (AWS CLI) または AWS Tools for Windows PowerShell を使用して次の Explorer リソースデータ同期 API を使用できます。

- CreateResourceDataSync
- DeleteResourceDataSync
- ListResourceDataSync
- UpdateResourceDataSync

委任管理者は、組織全体または組織単位のサブセットに対してリソースデータの同期を最大 5 つ作成できます。委任管理者によって作成されたリソースデータ同期は、委任管理者アカウントでのみ使用できます。AWS Organizations 管理アカウントで同期や集計データを表示することはできません。

リソースデータ同期の詳細については、「複数のアカウントおよびリージョンのデータを表示するように Systems Manager Explorer を設定する」を参照してください。AWS Organizations の詳細については、AWS Organizations ユーザーガイドのAWS Organizations とはを参照してください。

トピック

- Explorer 委任管理者の設定
- Explorer 委任管理者の登録解除

Explorer 委任管理者の設定

Explorer 委任管理者を登録するには、次の手順に従います。

Explorer 委任管理者を登録するには

1. AWS Organizations 管理アカウントにログインします。
2. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
3. ナビゲーションペインで、[Explorer] を選択します。
4. [設定] を選択します。
5. [Explorer の委任管理者] セクションで、サービスにリンクされた必要なロールとサービスアクセスオプションを設定したことを確認します。必要に応じて、[Create role (ロールの作成)] ボタンと [Enable access (アクセスの有効化)] ボタンを選択して、これらのオプションを設定します。
6. [アカウント ID] に AWS アカウント ID を入力します。このアカウントは、AWS Organizations のメンバーアカウントである必要があります。
7. [Register delegated administrator (委任管理者の登録)] を選択します。

委任管理者は、[リソースデータ同期の作成] ページの [AWS Organizations の設定からすべてのアカウントを含める] および [AWS Organizations の組織単位を選択する] オプションにアクセスできるようになりました。

Explorer 委任管理者の登録解除

Explorer 委任管理者の登録を解除するには、次の手順に従います。委任管理者アカウントは、AWS Organizations 管理アカウントでのみ登録解除できます。委任管理者アカウントが登録解除されると、委任管理者によって作成されたすべての AWS Organizations リソースデータの同期が削除されます。

Explorer の委任管理者の登録を解除するには

1. AWS Organizations 管理アカウントにログインします。
2. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
3. ナビゲーションペインで、[Explorer] を選択します。
4. [設定] を選択します。
5. [Explorer の委任管理者]セクションで、[登録解除] を選択します。警告が表示されます。
6. アカウント ID を入力し、[削除] を選択します。

アカウントは、AWS Organizations リソースデータの同期 API オペレーションにアクセスできなくなりました。アカウントによって作成されたすべての AWS Organizations リソースデータの同期が削除されます。

複数のアカウントおよびリージョンのデータを表示するように Systems Manager Explorer を設定する

AWS Systems Manager は、統合セットアップエクスペリエンスによって、AWS Systems Manager Explorer と AWS Systems Manager OpsCenter の使用開始を支援します。統合セットアップが完了すると、Explorer と OpsCenter は自動でデータを同期します。より具体的には、これらのツールは、統合セットアップの完了時に使用した AWS アカウントおよび AWS リージョンの OpsData と OpsItems を同期化します。他のアカウントやリージョンの OpsData と OpsItems を集約するには、このトピックの説明に従ってリソースデータの同期を作成する必要があります。

> **Note**
>
> 統合セットアップの詳細については、「Systems Manager Explorer と OpsCenter の開始方法」を参照してください。

トピック

- Explorer のリソースデータ同期について
- 複数のアカウントとリージョンのリソースデータの同期について
- リソースデータ同期の作成

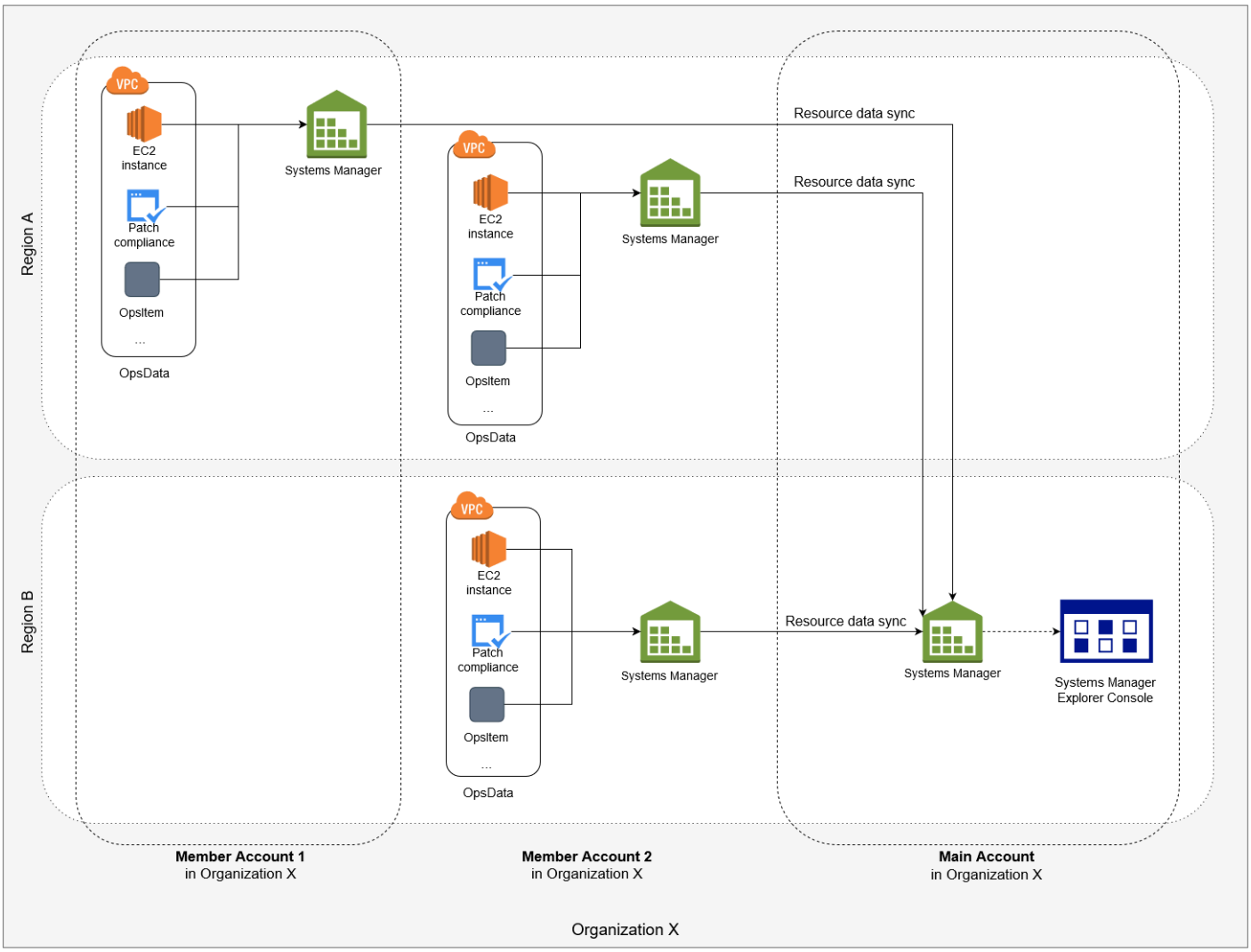
Explorer のリソースデータ同期について

Explorer のリソースデータの同期では、次の 2 つの集約オプションが提供されています。

- 単一アカウント/複数リージョン: 複数の AWS リージョン から OpsItems および OpsData データを集約するように Explorer を設定できます。ただし、データセットは現在の AWS アカウント に制限されます。
- 複数アカウント/複数リージョン: 複数の AWS リージョン とアカウントのデータを集約するように Explorer を設定できます。このオプションでは、AWS Organizations をセットアップおよび設定する必要があります。AWS Organizations をセットアップして設定した後、Explorer で組織単位 (OU) 別または組織全体のデータを集約できます。Systems Manager は、データをAWS Organizations 管理アカウントに集約してから Explorer に表示します。詳細については、『AWS Organizations ユーザーガイド』の「What is AWS Organizations? (とは ?)」 を参照してください。

> **Warning**
>
> AWS Organizations の組織からデータを集約するよう Explorer を設定する場合、組織内のすべてのメンバーアカウントで OpsData が有効になります。すべてのメンバーアカウントで OpsData ソースを有効にすると、CreateOpsItem や GetOpsSummary のような OpsCenter API への呼び出し回数が増えます。これらの API アクションへの呼び出しに対して課金されます。

次の図に、AWS Organizations を使用して設定されたリソースデータの同期を示します。このシナリオでは、ユーザーには AWS Organizations で定義された 2 つのアカウントがあります。リソースデータの同期により、両方のアカウントと複数の AWS リージョン のデータが AWS Organizations 管理アカウントに集約されてから Explorer に表示されます。



複数のアカウントとリージョンのリソースデータの同期について

このセクションでは、AWS Organizations を使用する複数のアカウントおよび複数のリージョンリソースデータ同期に関する重要な詳細について説明します。具体的には、このセクションの情報は、[Create resource data sync] (リソースデータの同期を作成する) のページで次のいずれかのオプションを選択した場合に適用されます。

- AWS Organizations の設定からすべてのアカウントを含める
- AWS Organizations の組織単位を選択する

これらのオプションのいずれかを使用する予定がない場合は、このセクションを省略できます。

SSM コンソールでリソースデータ同期を作成するときに、AWS Organizations オプションのいずれかを選択すると、Systems Manager は、組織内 (または選択した組織単位内) のすべての

AWS アカウント について、選択したリージョンのすべての OpsData ソースを自動的に有効にします。例えば、リージョンで Explorer を有効にしていない場合でも、リソースデータ同期で AWS Organizations オプションを選択すると、Systems Manager はそのリージョンから OpsData を自動的に収集します。OpsData ソースを許可せずにリソースデータ同期を作成するには、データ同期を作成するときに EnableAllOpsDataSources を false に指定します。詳細については、「Amazon EC2 Systems Manager API リファレンス」のResourceDataSyncSource データ型の `EnableAllOpsDataSources` パラメータの詳細を参照してください。

リソースデータ同期の AWS Organizations オプションのいずれかを選択しない場合は、Explorer がデータにアクセスするアカウントとリージョンごとに、統合セットアップを完了する必要があります。この作業を行っていない場合は、統合セットアップを完了しなかったアカウントとリージョンの OpsData と OpsItems が Explorer に表示されません。

組織に子アカウントを追加すると、Explorer はそのアカウントのすべての OpsData ソースを自動的に有効にします。後で組織から子アカウントを削除した場合、Explorer は引き続きアカウントから OpsData を収集します。

AWS Organizations オプションのいずれかを使用する既存のリソースデータ同期を更新すると、変更の影響を受けるすべてのアカウントおよびリージョンのすべての OpsData ソースの収集を承認するよう求められます。

AWS アカウント に新しいサービスを追加し、Explorer がそのサービスの OpsData を収集する場合、Systems Manager はその OpsData を収集するように Explorer を自動的に設定します。例えば、以前にリソースデータ同期を作成したときに AWS Trusted Advisor を使用せず、組織がこのサービスにサインアップする場合、Explorer はリソースデータ同期を自動的に更新してこの OpsData を収集します。

Important

複数のアカウントおよびリージョンのリソースデータ同期に関する次の重要な情報を書き留めます。

- リソースデータ同期を削除しても、Explorer の OpsData ソースは無効になりません。
- 複数のアカウントからの OpsData と OpsItems を表示するには、AWS Organizations の [All features (すべての機能)] モードを有効にし、AWS Organizations 管理アカウントにサインインする必要があります。

リソースデータ同期の作成

Explorer のリソースデータ同期を設定する前に、次の詳細を書き留めます。

- Explorer は、最大 5 つのリソースデータ同期をサポートしています。
- リージョンのリソースデータ同期を作成した後、その同期のアカウントオプションを変更することはできません。例えば、us-east-2 (オハイオ) リージョンで同期を作成し、[現在のアカウントのみを含める)] オプションを選択した場合、後でその同期を編集して [自分用の AWS Organizations 設定のすべてのアカウントを含める] オプションを選択することはできません。代わりに、最初のリソースデータ同期を削除し、新しいリソースデータ同期を作成する必要があります。
- Explorer で表示される OpsData は読み取り専用です。

以下の手順を使用して、Explorer のリソースデータ同期を作成します。

リソースデータの同期を作成するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Explorer] を選択します。
3. [設定] を選択します。
4. [Configure resource data sync (リソースデータ同期の設定)] セクションで、[Create resource data sync (リソースデータ同期の作成)] を選択します。
5. [Resource data sync name (リソースデータ同期名)] に名前を入力します。
6. [Add accounts (アカウントの追加)] セクションでオプションを選択します。

> **Note**
>
> いずれかの AWS Organizations オプションを使用するには、AWS Organizations 管理アカウント、または Explorer の委任管理者アカウントにログインしている必要があります。委任管理者アカウントの詳細については、「Explorer のための委任された管理者の設定」を参照してください。

7. [Regions to include (含めるリージョン)] セクションで、以下のいずれかのオプションを選択します。

- [All current and future regions] (現在および将来のすべてのリージョン) を選択すると、現在のすべての AWS リージョン と将来オンラインになる新しいリージョンのデータが自動的に同期されます。
- [All regions] (すべてのリージョン) を選択すると、現在のすべての AWS リージョン リージョンからのデータが自動的に同期されます。
- 含めるリージョンを個別に選択します。

8. [Create resource data sync (リソースデータ同期の作成)] を選択します。

リソースデータ同期を作成した後、Explorer にデータが入力されるまで、数分かかる場合があります。同期を表示するには、Explorer で [Select a resource data sync (リソースデータ同期を選択)] リストから同期を選択します。

Explorer の使用

このセクションでは、ウィジェットレイアウトおよびダッシュボードに表示されるデータを変更することによって AWS Systems Manager Explorer をカスタマイズする方法について説明します。

内容

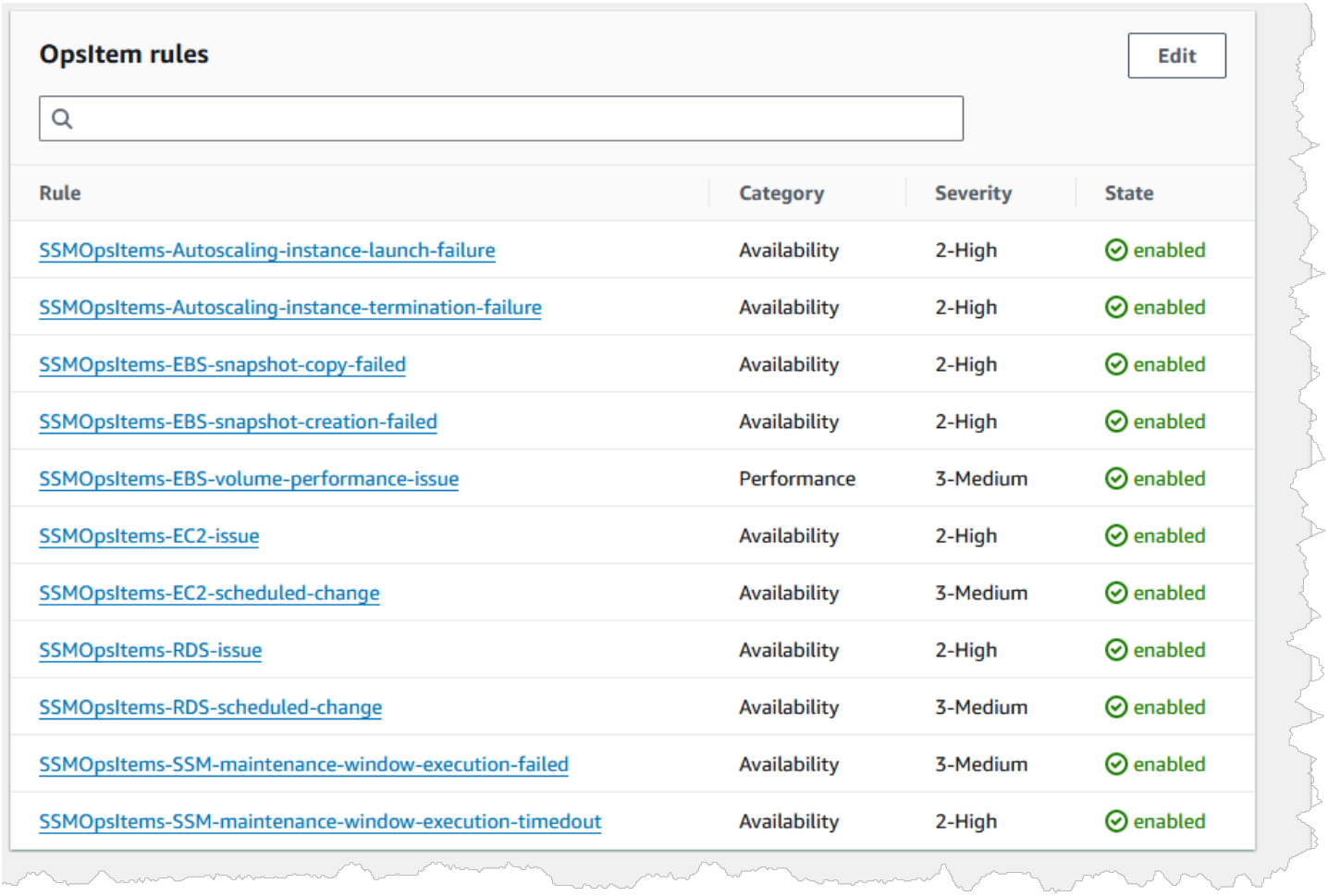
- Explorer のために作成された EventBridge ルールの編集
- Systems Manager Explorer のデータソースを編集する
- Explorer 表示のカスタマイズ
- Explorer の AWS Security Hub から結果を受け取る
- Systems Manager Explorer のリソースデータ同期を削除する

Explorer のために作成された EventBridge ルールの編集

統合セットアップを完了すると、Amazon EventBridge で多数のルールが有効になります。これらのルールにより、AWS Systems Manager OpsCenter でOpsItems が自動的に作成されます。AWS Systems Manager Explorer には、OpsItems に関する集約情報が表示されます。

各ルールには、事前設定された [カテゴリ] と [重要度] の値が含まれています。イベントから OpsItems が作成されるときに、事前設定された [カテゴリ] と [重要度] が自動的に割り当てられます。

> **Important**
>
> デフォルトルールの [カテゴリ] と [重要度] の値は編集できませんが、デフォルトルールから作成された OpsItems でこれらの値を編集できます。



OpsItems を作成するためのデフォルトルールを編集するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Explorer] を選択します。
3. [設定] を選択します。
4. [OpsItems rules (OpsItems ルール)] セクションで [編集] を選択します。
5. [CWE rules (CWE ルール)] を展開します。

6. 使用しないルールの横のチェックボックスをオフにします。
7. [カテゴリ] および [重要度] リストを使用して、ルールのこの情報を変更します。
8. [Save] を選択します。

変更は、OpsItem の次回作成時に有効になります。

Systems Manager Explorer のデータソースを編集する

AWS Systems Manager Explorer は、以下のソースからのデータを表示します。データソースを追加または削除できるように Explorer の設定を編集できます。

- Amazon Elastic Compute Cloud (Amazon EC2)
- AWS Systems Manager OpsCenter
- AWS Systems Manager Patch Manager パッチコンプライアンス
- AWS Systems Manager State Manager の関連付けのコンプライアンス
- AWS Trusted Advisor
- AWS Compute Optimizer
- AWS サポート センターのケース
- AWS Config のルールとリソースコンプライアンス
- AWS Security Hub の結果

> **Note**
>
> - Explorerで サポートセンターのケースを表示するには、サポートでエンタープライズアカウントまたはビジネスアカウントをセットアップする必要があります。
> - OpsCenter OpsItem データの表示を停止するように Explorer を設定することはできません。

開始する前に

Explorerウィジェットにデータを入力するサービスをセットアップして設定したことを確認します。詳細については、「Explorer のための関連サービスのセットアップ」を参照してください。

データソースを編集するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Explorer] を選択します。
3. [設定] を選択して、[ダッシュボードの設定] タブを選択します。
4. [OpsData ソース] セクション [ステータス] 列で、表示するデータに従ってソースをオンまたはオフにします。

Explorer 表示のカスタマイズ

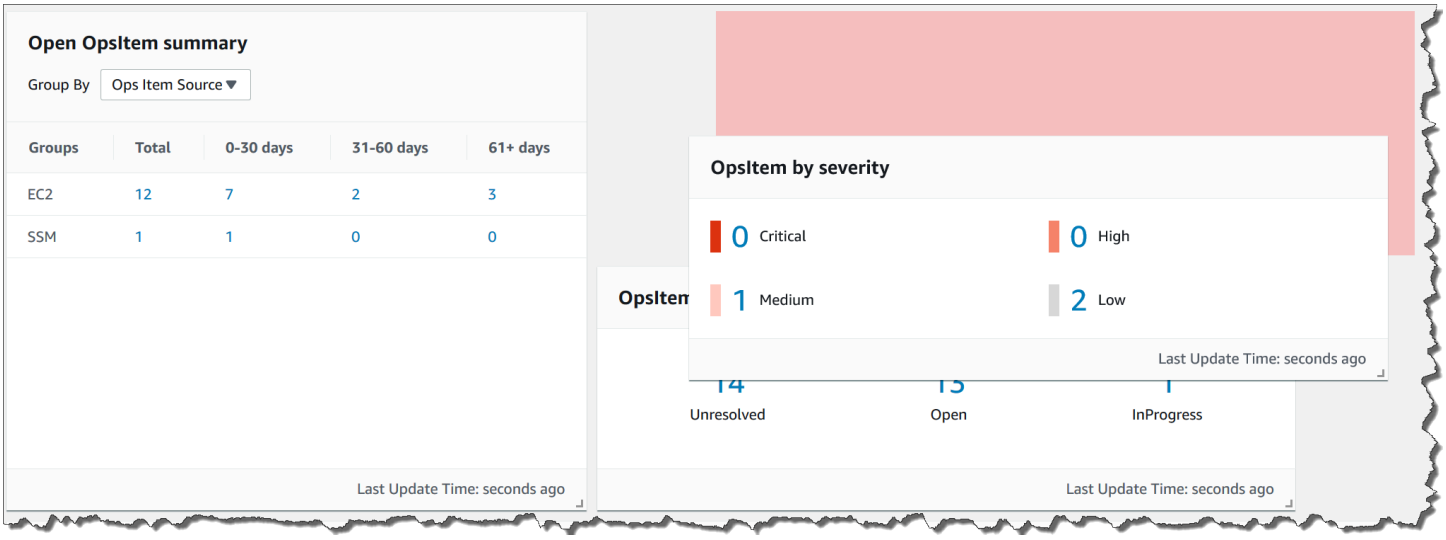
AWS Systems Manager Explorer でウィジェットのレイアウトをカスタマイズするには、ドラッグアンドドロップ機能を使用します。このトピックで説明するように、フィルターを使用して、Explorer に表示される OpsData および OpsItems をカスタマイズすることもできます。

ウィジェットのレイアウトをカスタマイズする前に、表示対象のウィジェットが、現在、Explorer 内に表示中であることを確認してください。ウィジェットを Explorer (AWS Config コンプライアンスウィジェットなど) 内に表示するには、[Configure dashboard] (ダッシュボードの設定) ページで、それらのウィジェットを有効にする必要があります。

Explorer でのウィジェットの表示を有効にするには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Explorer] を選択します。
3. [Dashboard actions] (ダッシュボードのアクション)、[Configure dashboard] (ダッシュボードの設定) の順に選択します。
4. [Configure Dashboard] (ダッシュボードの設定) タブを開きます。
5. [Enable all] (すべて有効化) を選択するか、ウィジェットまたはデータソースを個別に有効化します。
6. [Explorer] を選択して変更を表示します。

Explorer でウィジェットのレイアウトをカスタマイズするには、移動するウィジェットを選択します。ウィジェットの名前をクリックしたまま、新しい場所までドラッグします。



再配置するウィジェットごとにこのプロセスを繰り返します。

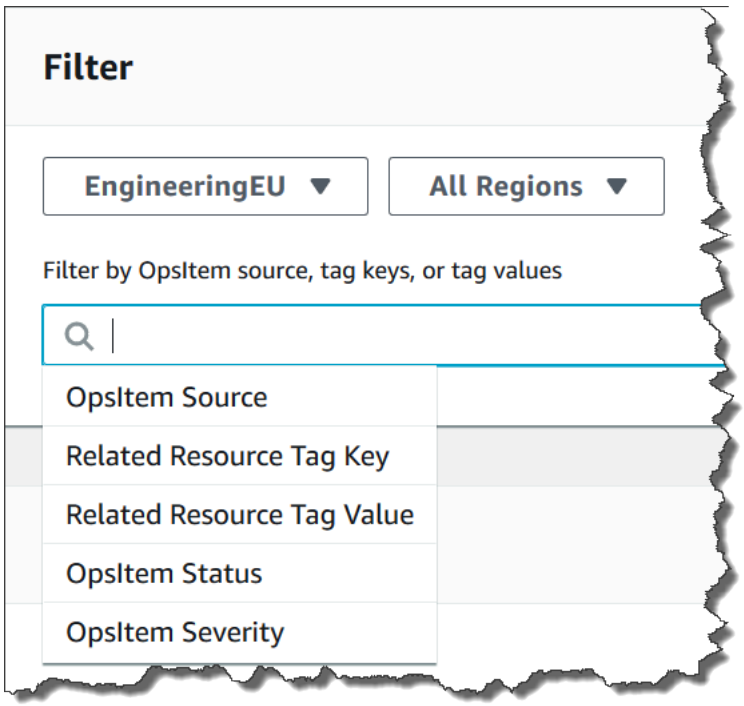
新しいレイアウトが気に入らない場合は、[Reset layout (レイアウトをリセット)] を選択してすべてのウィジェットを元の場所に戻します。

フィルターを使用して Explorer に表示されるデータを変更

Explorer にはデフォルトで、現在の AWS アカウント と現在のリージョンのデータが表示されます。1 つ以上のリソースデータ同期を作成した場合は、フィルターを使用して、アクティブな同期を変更できます。その後、特定のリージョンまたはすべてのリージョンのデータを表示するように選択できます。また、検索バーを使用して、さまざまな OpsItem およびキータグ条件でフィルタリングすることもできます。

フィルターを使用して Explorer に表示されるデータを変更するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Explorer] を選択します。
3. [フィルタ] セクションの [Select a resource data sync (リソースデータ同期を選択)] リストを使用して同期を選択します。
4. [Regions] (リージョン) リストを使用して、特定の AWS リージョン を選択するか、[All Regions] (すべてのリージョン) を選択します。
5. 検索バーを選択し、データをフィルタリングする条件を選択します。



6. [Enter] キーを押します。

ページをいったん閉じてから開いても、Explorer には選択したフィルタオプションがそのまま保持されています。

Explorer の AWS Security Hub から結果を受け取る

AWS Security Hub は、AWS のセキュリティ状態の包括的なビューを提供します。このサービスは AWS アカウント 全体、サービス、およびサポートされているサードパーティ製品から検出結果と呼ばれるセキュリティデータを収集します。Security Hub の検出結果は、セキュリティ業界標準とベストプラクティスに照らして環境をチェックしたり、セキュリティの傾向を分析し、最も優先度の高いセキュリティ問題を特定したりするのに役立ちます。

Security Hub は Amazon EventBridge に結果を送信し、Amazon EventBridge はイベントルールを使用して検出結果を Explorer に送信します。こちらの説明に従って統合を有効にすると、Security Hub の検出結果を Explorer ウィジェットで表示し、検出結果の詳細を OpsCenter OpsItems で表示できます。ウィジェットには、Security Hub のすべての検出結果の概要が重要度に基づいて表示されます。Security Hub の新しい検出結果は、通常、数秒以内に作成され、Explorer で表示されます。

> **Warning**
>
> 次の重要な情報に注意してください。

- Explorer は Systems Manager のツールである OpsCenter と統合されています。Security Hub と Explorer の統合を有効化したあと、OpsCenter は Security Hub の検出結果用に OpsItems を自動的に作成します。ご使用の AWS 環境によって、統合を有効にすることで、大量の OpsItems が発生する場合があります。これは有料です。

  続行する前に、Security Hub と OpsCenter の統合についてお読みください。このトピックでは、検出結果および OpsItems への変更と更新がどのようにお客様のアカウントに請求されるかについて解説しています。詳細については、「OpsCenter と AWS Security Hub の統合について」を参照してください。OpsCenter 料金情報については、「AWS Systems Manager の料金表」を参照してください。
- Explorer でリソースデータの同期を作成すると、データが同期されます。管理者アカウントにログインすると、管理者と同期中のすべてのメンバーアカウントの Security Hub 統合が自動的に有効になります。有効になると、OpsCenter は Security Hub の検出結果に OpsItems を自動的に作成します。この処理は有料です。リソースデータ同期の作成の詳細については、「複数のアカウントおよびリージョンのデータを表示するように Systems Manager Explorer を設定する」を参照してください。

Explorer が受け取る検出結果の種類

Explorer は、Security Hub からすべての結果を受け取ります。Security Hub のデフォルト設定を有効にすると、Explorer ウィジェットで重要度に基づくすべての結果を確認できます。デフォルトでは、Explorer は重大かつ重大度の高い検出結果に OpsItems を作成します。重要度が Medium および Low の検出結果に対して OpsItems を作成するために、手動で Explorer を設定できます。

Explorer は情報提供の検出結果に対しては OpsItems を作成しないものの、Security Hub の調査結果概要ウィジェットに情報操作データ (OpsData) を表示できます。Explorer 重大度に関係なく、すべての調査結果の OpsData を作成します。Security Hub 重大度レベルの詳細については、「AWS Security Hub API リファレンス」の「重大度」を参照してください。

統合の有効化

このセクションでは、Explorer が Security Hub の検出結果の受信を開始できるように、有効化し、設定する方法について説明します。

[開始する前に]

Explorer を設定して Security Hub の検出結果の受信を開始する前に、次のタスクを完了します。

- Security Hub を有効にして設定します。詳細については、AWS Security Hub ユーザーガイドの「Security Hub の設定」を参照してください。
- AWS Organizations 管理アカウントにログインします。Systems Manager では、Security Hub の検出結果から OpsItems を作成するには、AWS Organizations へのアクセスが必要です。管理アカウントにログインした後、次の手順で説明するように、Explorer の [ダッシュボードの設定] タブで [アクセスを有効にする] ボタンをクリックするよう求められます。AWS Organizations 管理アカウントにログインしないと、アクセスを有効にすることができず、Explorer は Security Hub の検出結果から OpsItems を作成できません。

Security Hub の検出結果の受信を開始するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Explorer] を選択します。
3. [設定] を選択します。
4. [ダッシュボードの設定] タブを選択します。
5. AWS Security Hub を選択します。
6. [Disabled (無効)] スライダーを選択して AWS Security Hub を有効にします。

   デフォルトでは、Critical と High の重大度の検出結果が表示されます。Medium と Low の重大度検出結果を表示するには、Medium、Low の横にある [無効] スライダーを選択します。
7. [Security Hub の検出結果によって作成された OpsItems] セクションで、[アクセスを有効にする] を選択します。このボタンが表示されない場合は、AWS Organizations 管理アカウントにログインし、このページに戻ってボタンを選択します。

Security Hub の検出結果を表示する方法

次の手順では、Security Hub の検出結果を表示する方法について説明します。

Security Hub の検出結果を表示するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Explorer] を選択します。
3. AWS Security Hub 結果の概要ウィジェットを検索します。これにより、Security Hub の検出結果が表示されます。重要度を選択すると、対応する OpsItem の詳細な説明を表示できます。

検出結果の受け取りを停止する方法

次の手順では、Security Hub の検出結果の受信を停止する方法について説明します。

Security Hub の検出結果の受信を停止するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Explorer] を選択します。
3. [設定] を選択します。
4. [ダッシュボードの設定] タブを選択します。
5. [Enabled (有効)] スライダーを選択して AWS Security Hub を無効にします。

> **Important**
>
> コンソールで Security Hub の検出結果を無効にするオプションがグレー表示になっている場合は、AWS CLI で次のコマンドを実行して、この設定を無効にすることができます。コマンドは、AWS Organizations 管理アカウントまたは Systems Manager の委任された管理者アカウントにログイン中に実行する必要があります。`region` パラメータでは、Explorer で Security Hub の検出結果の受信を停止する AWS リージョン を指定します。
>
> ```
> aws ssm update-service-setting --setting-id /ssm/opsdata/SecurityHub --setting-value Disabled --region AWS #####
> ```
>
> 以下に例を示します。
>
> ```
> aws ssm update-service-setting --setting-id /ssm/opsdata/SecurityHub --setting-value Disabled --region us-east-1
> ```

Systems Manager Explorer のリソースデータ同期を削除する

AWS Systems Manager Explorer では、リソースデータ同期を作成することによって、他のアカウントやリージョンから OpsData と OpsItems を集約することができます。

リソースデータ同期のアカウントオプションは変更できません。例えば、us-east-2 (オハイオ) リージョンで同期を作成し、[現在のアカウントのみを含める] オプションを選択した場合、後でその同期を編集して [自分用の AWS Organizations 設定のすべてのアカウントを含める] オプションを選択することはできません。代わりに、以下の手順の説明に従って、リソースデータ同期を削除し、新しいリソースデータ同期を作成する必要があります。

リソースデータ同期を削除するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Explorer] を選択します。
3. [設定] を選択します。
4. [Configure resource data sync (リソースデータ同期の設定)] セクションで、削除するリソースデータ同期を選択します。
5. [削除] を選択します。

Systems Manager Explorer から OpsData をエクスポートする

カンマ区切り (.csv) ファイルとして、5,000 の OpsData のアイテムを AWS Systems Manager Explorer から Amazon Simple Storage Service (Amazon S3) バケットにエクスポートできます。Explorer は AWS-ExportOpsDataToS3 オートメーションランブックを使用して OpsData をエクスポートします。OpsData をエクスポートすると、システムは assumeRole、Amazon S3 バケット名、SNS トピック ARN、エクスポートするフィールドなどの詳細を指定できる自動化ランブックページを表示します。

OpsData をエクスポートするには

- ステップ 1: SNS トピックを指定する
- ステップ 2: (オプション) データエクスポートを設定する
- ステップ 3: OpsData をエクスポートする

ステップ 1: SNS トピックを指定する

データエクスポートを設定するときは、データをエクスポートするのと同じ AWS リージョン に存在する Amazon Simple Notification Service (Amazon SNS) トピックを指定する必要があります。エクスポートが完了すると、Systems Manager から Amazon SNS トピックに通知が送信されま

す。Amazon SNS トピックの作成の詳細については、「Amazon SNS トピックの作成」を参照してください。

ステップ 2: (オプション) データエクスポートを設定する

データエクスポート設定は、[設定] ページまたは [S3 バケットに Ops データをエクスポート] ページから設定できます。

Explorer からのデータエクスポートを設定するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Explorer] を選択します。
3. [設定] を選択します。
4. [Configure data export (データエクスポートの設定)] セクションで [編集] を選択します。
5. データエクスポートファイルを既存の Amazon S3 バケットにアップロードするには、[既存の S3 バケットを選択] を選択し、リストからバケットを選択します。

   データエクスポートファイルを新しい Amazon S3 バケットにアップロードするには、[新しい S3 バケットを作成] を選択し、新しいバケットに使用する名前を入力します。

   > **Note**
   >
   > Amazon S3 バケット名と Amazon SNS トピック ARN は、次の Explorer で初めて設定したページからのみ編集できます。[設定] ページから Amazon S3 バケットと Amazon SNS トピック ARN をセットアップした場合、それらの設定は [設定] ページからのみ変更できます。

6. [Amazon SNS トピック ARN を選択] では、エクスポートの完了時に通知するトピックを選択します。
7. [Create] (作成) を選択します。

ステップ 3: OpsData をエクスポートする

Explorer のデータをエクスポートすると、Systems Manager は `AmazonSSMExplorerExportRole` という名前の AWS Identity and Access Management (IAM) ロールを作成します。このロールは以下の IAM ポリシーを使用します。

```
{
      "Version": "2012-10-17",
      "Statement": [
          {
              "Sid": "OpsSummaryExportAutomationServiceRoleStatement1",
              "Effect": "Allow",
              "Action": [
                  "s3:PutObject"
              ],
              "Resource": [
                 "arn:aws:s3:::{{ExportDestinationS3BucketName}}/*"
              ]
          },
          {
              "Sid": "OpsSummaryExportAutomationServiceRoleStatement2",
              "Effect": "Allow",
              "Action": [
                  "s3:GetBucketAcl",
                  "s3:GetBucketLocation"
              ],
              "Resource": [
                 "arn:aws:s3:::{{ExportDestinationS3BucketName}}"
              ]
          },
          {
              "Sid": "OpsSummaryExportAutomationServiceRoleStatement3",
              "Effect": "Allow",
              "Action": [
                  "sns:Publish"
              ],
              "Resource": [
                  "{{SnsTopicArn}}"
              ]
          },
          {
              "Sid": "OpsSummaryExportAutomationServiceRoleStatement4",
              "Effect": "Allow",
              "Action": [
                  "logs:DescribeLogGroups",
                  "logs:DescribeLogStreams"
              ],
              "Resource": [
                  "*"
```

```
            ]
        },
        {
            "Sid": "OpsSummaryExportAutomationServiceRoleStatement5",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup",
                "logs:PutLogEvents",
                "logs:CreateLogStream"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "OpsSummaryExportAutomationServiceRoleStatement6",
            "Effect": "Allow",
            "Action": [
                "ssm:GetOpsSummary"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

ロールには、次の信頼エンティティが含まれています。

```
{
      "Version": "2012-10-17",
      "Statement": [
        {
          "Sid": "OpsSummaryExportAutomationServiceRoleTrustPolicy",
          "Effect": "Allow",
          "Principal": {
            "Service": "ssm.amazonaws.com"
          },
          "Action": "sts:AssumeRole"
        }
      ]
    }
```

Explorer から OpsData をエクスポートするには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Explorer] を選択します。
3. Explorer ウィジェットでデータリンクを選択します。例えば、[ステータス別 OpsItems] のウィジェットで [未解決] または [未解決の問題] を選択します。あるいは、[重要度別 OpsItem] のウィジェットで [最重要] または [高] のデータリンクを選択します。Explorer で、選択したデータセットの OpsData ページが開きます。
4. [テーブルのエクスポート] を選択します。

   > **Note**
   >
   > OpsData を初めてエクスポートすると、システムがエクスポート用ロールを引き受けます。デフォルトの引き受けロールは変更できません。

5. [S3 バケット名] で、既存のバケットを選択します。必要に応じて、[作成] を選択して Amazon S3 バケットを作成できます。

   S3 バケット名を変更できない場合は、[設定] ページでバケット名を設定したことを意味します。バケット名は [設定] ページからのみ変更できます。

   > **Note**
   >
   > Amazon S3 バケット名と Amazon SNS トピック ARN は、次の Explorer で初めて設定したページからのみ編集できます。

6. [SNS トピック ARN] の場合、ダウンロードの完了時に通知する既存の Amazon SNS トピック ARN を選択します。

   Amazon SNS トピック ARN を変更できない場合は、[設定] ページから Amazon SNS トピック ARN を設定したことを意味します。トピック ARN は、[設定] ページからのみ変更できます。

7. (オプション) [SNS 成功メッセージ] には、エクスポートが正常に完了したときに表示する成功メッセージを指定します。
8. [送信] を選択します。システムは前のページに移動し、[クリックしてエクスポートプロセスのステータスを表示] というメッセージを表示します。[詳細を表示]。

[詳細を表示] を選択すると、Systems Manager Automation でランブックのステータスとの進行状況を表示できます。

これで、Explorer から指定された Amazon S3 バケットに OpsData をエクスポートできるようになりました。

この手順を使用してデータをエクスポートできない場合は、ユーザー、グループ、ロールに `iam:CreatePolicyVersion` および `iam:DeletePolicyVersion` アクションが含まれていることを確認してください。これらのアクションをユーザー、グループ、ロールに追加する方法については、「IAM ユーザーガイド」の「IAM ポリシーの編集」を参照してください。

Systems Manager Explorer のトラブルシューティング

このトピックでは、AWS Systems Manager Explorer の一般的な問題のトラブルシューティング方法について説明します。

[Settings] (設定) ページでタグを更新した後、Explorer 上の AWS リソースをフィルタリングできない

Explorer でタグキーやその他のデータ設定を更新すると、変更に基づいてデータが同期されるまでに最大 6 時間かかる場合があります。

[Create resource data sync (リソースデータの同期の作成)] ページの AWS Organizations オプションがグレー表示される

[リソースデータ同期の作成] ページの [AWS Organizations の設定からすべてのアカウントを含める] オプションと [AWS Organizations 内の組織単位を選択する] オプションは、AWS Organizations をセットアップして設定した場合にのみ利用できます。AWS Organizations をセットアップして設定した場合、AWS Organizations 管理アカウントまたは Explorer 委任管理者のいずれかが、これらのオプションを使用するリソースデータの同期を作成できます。

詳細については、複数のアカウントおよびリージョンのデータを表示するように Systems Manager Explorer を設定するおよびExplorer のための委任された管理者の設定を参照してください。

Explorer にデータが表示されない

- Explorer でデータにアクセスして表示する各アカウントおよびリージョンで統合セットアップが完了していることを確認します。この作業を行っていない場合は、統合セットアップを完了しなかっ

たアカウントとリージョンの OpsData と OpsItems が Explorer に表示されません。詳細については、「Systems Manager Explorer と OpsCenter の開始方法」を参照してください。

- Explorer を使用して複数のアカウントとリージョンからのデータを表示するときは、AWS Organizations 管理アカウント、または Explorer 委任管理者アカウントにログインしていることを確認してください。複数のアカウントとリージョンからの OpsData と OpsItems を表示するには、このアカウントにサインインする必要があります。

Amazon EC2 インスタンスに関するウィジェットにデータが表示されない

Amazon Elastic Compute Cloud (Amazon EC2) インスタンスに関するウィジェット ([インスタンス数]、[マネージドインスタンス]、[AMI 別のインスタンス] など) でデータが表示されない場合は、以下を確認してください。

- 数分待ったことを確認します。統合セットアップの完了後、OpsData が Explorer に表示されるまでに数分かかる場合があります。
- AWS Config 設定レコーダーを設定したことを確認します。Explorer は、AWS Config 設定レコーダーから提供されるデータを使用して、ウィジェットに EC2 インスタンスに関する情報を入力します。詳細については、「設定レコーダーの管理」を参照してください。
- [Settings (設定)] ページで Amazon EC2 OpsData ソースが有効になっていることを確認します。また、設定レコーダーをアクティベーションしてから、またはインスタンスに変更を加えてから 6 時間以上経過したことを確認します。Systems Manager は、最初に設定レコーダーをアクティベーションするか、インスタンスに変更を加えてから、Explorer EC2 ウィジェットに AWS Config からのデータが表示されるのに最大 6 時間かかる場合があります。
- インスタンスが停止または終了した場合、Explorer では 24 時間後にそれらのインスタンスの表示が停止されることに注意してください。
- Amazon EC2 インスタンスを設定した正しい AWS リージョン で作業していることを確認します。Explorer には、オンプレミスインスタンスに関するデータは表示されません。
- 複数のアカウントおよびリージョンのリソースデータ同期を設定した場合は、Organizations 管理アカウント、または Explorer 委任管理者アカウントにサインインしていることを確認してください。

パッチウィジェットにデータが表示されない

[Non-compliant instances for patching (パッチの非準拠インスタンス)] ウィジェットでは、準拠していないパッチインスタンスに関するデータのみが表示されます。インスタンスが準拠している場合、このウィジェットではデータが表示されません。非準拠インスタンスがあると考えられる

場合は、Systems Manager のパッチをセットアップして設定し、AWS Systems Manager Patch Manager を使用してパッチのコンプライアンスを確認します。詳細については、「AWS Systems Manager Patch Manager」を参照してください。

その他の問題

Explorer で OpsItems を編集または修正できない: アカウントまたはリージョン間で表示される OpsItems は読み取り専用です。これらは、ホームアカウントまたはリージョンからのみ更新、修正できます。

AWS Systems Manager OpsCenter

AWS Systems Manager のツールである OpsCenter は、オペレーションエンジニアや IT プロフェッショナルが AWS リソースに関連するオペレーション作業項目 (OpsItems) を一元的に確認、調査、および解決できる場所を提供します。OpsCenter は、AWS リソースに影響を与える問題の解決にかかる平均時間を短縮するよう設計されています。OpsCenter は、複数のサービスの OpsItems を集約および標準化するとともに、各 OpsItem および関連の OpsItems と関連するリソースに関するコンテキスト調査データを提供します。さらに OpsCenter も、迅速な問題の解決に役立つ Systems Manager Automation ランブックを提供します。検索可能なカスタムデータを OpsItem ごとに指定することができます。OpsItems に関する自動的に生成された概要レポートは、ステータスおよびソース別に表示することもできます。OpsCenter の使用を開始するには、Systems Manager コンソールを開きます。ナビゲーションペインで、[OpsCenter] を選択します。

OpsCenter は Amazon EventBridge および Amazon CloudWatch と統合されています。つまり、CloudWatch アラームが ALARM の状態になったとき、または EventBridge がイベントを発行する AWS のサービスからのイベントを処理するときに、OpsCenter で OpsItem を自動的に作成するようにこれらのサービスを設定できます。CloudWatch アラームと EventBridge イベントが自動的に OpsItems を作成するように構成すると、1 つのコンソールから AWS リソースに関する問題を迅速に診断および修正できます。

問題の診断に役立つように、各 OpsItem には、OpsItem を生成した AWS リソースの名前と ID、アラームまたはイベントの詳細、アラーム履歴、アラームタイムライングラフなど、状況に応じた関連情報が含まれています。

AWS リソースに対し、OpsCenter は AWS Config、AWS CloudTrail ログおよび Amazon CloudWatch Events の情報を集約するため、調査中に複数のコンソールページ間を移動する必要がありません。

次のリストは、OpsItems を作成する CloudWatch アラームを設定するお客様の AWS リソースとメトリックスのタイプを示しています。

- Amazon DynamoDB: データベースの読み取りおよび書き込みアクションがしきい値に達する
- Amazon EC2: CPU 使用率がしきい値に達する
- AWS 請求: 推定請求額がしきい値に達する
- Amazon EC2: インスタンスがステータスチェックに失敗する
- Amazon Elastic Block Store (EBS): ディスク領域の使用率がしきい値に達する

次のリストには、OpsItems を作成するためにお客様が設定する EventBridge ルールの種類を示します。

- AWS Security Hub: セキュリティアラートが発行されました
- DynamoDB: スロットリングイベント
- Amazon EC2 Auto Scaling: インスタンスの起動に失敗しました
- Systems Manager: オートメーションを実行できませんでした
- AWS Health: スケジュールされたメンテナンスのアラート
- EC2: インスタンスの状態が `Running` から `Stopped` に変わる

OpsCenter は、.NET および SQL Server 用の Amazon CloudWatch Application Insights とも統合されています。つまり、アプリケーションで検出された問題に対して自動的に OpsItems を作成できます。また、OpsCenter を AWS Security Hub と統合して、Systems Manager のセキュリティ、パフォーマンス、運用上の問題を集約し、アクションを実行することもできます。

オペレーションエンジニアおよび IT プロフェッショナルは、AWS Systems Manager コンソールの OpsCenter ページ、パブリック API オペレーション、AWS Command Line Interface (AWS CLI)、AWS Tools for Windows PowerShell、または AWS SDK を使用して、OpsItems を作成、表示、および編集できます。OpsCenter パブリック API アクションを使用すると、OpsCenter をケース管理システムおよび正常性ダッシュボードと統合することも可能です。

OpsCenter はどのように組織にとってメリットになりますか?

OpsCenter では、AWS リソースに関する問題を表示、対応、修正するための統一された標準エクスペリエンスを提供します。統一された標準エクスペリエンスによって、問題の解決やその問題の調査、新しいオペレーションエンジニアと IT プロフェッショナルのトレーニングにかかる時間は短縮されます。また、統一された標準エクスペリエンスでは、問題を管理して修正するシステムに対する手動エラーの数が低下します。

具体的には、OpsCenter は、オペレーションエンジニアや組織にとって、次のような利点があります。

- AWS リソースに関連する OpsItems を表示、調査、解決するために複数のコンソールページを移動する必要はありません。OpsItems は、サービス全体の中心の場所に集約されます。
- CloudWatch アラーム、EventBridge イベント、および .NET および SQL Server 用の CloudWatch Application Insights によって自動的に生成される OpsItems のサービス固有のデータおよびコンテキストに関連するデータを表示できます。
- OpsItem に関するリソースの Amazon リソースネーム (ARN) を指定することができます。関連リソースを指定することで、OpsCenter は、組み込みロジックを使用して、OpsItems が重複しないようにします。
- 同様の OpsItems の詳細や解決方法に関する情報を確認することができます。
- 問題を解決するには、Systems Manager Automation ランブック に関する情報をすばやく表示して実行します。

OpsCenter の特徴は何ですか?

- 自動スナップショットと手動 OpsItem 作成

  OpsCenter は Amazon CloudWatch と統合されています。つまり、アラームが ALARM 状態になったとき、または Amazon EventBridge がイベントを発行する AWS のサービスからのイベントを処理するときに、OpsCenter で OpsItem を自動的に作成するように CloudWatch を設定できます。手動で OpsItems を作成することもできます。

  OpsCenter は、.NET および SQL Server 用の Amazon CloudWatch Application Insights とも統合されています。つまり、アプリケーションで検出された問題に対して自動的に OpsItems を作成できます。

- 詳細で検索可能な OpsItems

  各 OpsItem には、情報の複数のフィールドを含みます。たとえば、OpsItem のタイトル、ID、優先度、説明のほか、最終更新日時などがあります。各 OpsItem には、次の設定可能な機能も含まれます。

  - ステータス: Open、In progress、Resolved、または Open and In progress。
  - 関連リソース: 関連リソースは、影響を受けるリソース、または OpsItem を作成した EventBridge イベントを開始したリソースです。各 OpsItem には、[関連リソース] セクションを含みます。OpsCenter によって、関連リソースの Amazon リソースネーム (ARN) が自動的に

表示されます。また、関連リソースの ARN を手動で指定することもできます。一部の ARN タイプでは、その情報を表示するために他のコンソールページにアクセスしなくても、OpsCenter によって、リソースに関する詳細を表示するディープリンクが自動的に作成されます。たとえば、EC2 インスタンスの ARN を指定すると、OpsCenter のそのインスタンスに関する EC2 提供の詳細をすべて表示できます。その他の関連リソースの ARN は手動で追加することができます。各 OpsItem セクションには、最大 100 個の関連リソースの ARN を表示できます。詳細については、「関連リソースを OpsItem に追加する」を参照してください。

- 関連および同様の OpsItems: [関連 OpsItems (Related)] 機能を使用すると、現在の OpsItem に関連する OpsItems の ID を指定できます。[同様の OpsItem] 機能によって、OpsItem のタイトルや説明が自動的に確認されてから、関連する、またはその他のユーザー向けの他の OpsItems が一覧表示されます。
- 検索可能でプライベートな運用データ: 運用データは、OpsItem に関する有用なリファレンスの詳細を提供するカスタムデータです。たとえば、ログファイル、エラー文字列、ライセンスキー、トラブルシューティングのヒント、その他の関連データを指定することができます。キーと値のペアで、運用データを入力します。キーの最大長は 128 文字です。値の最大サイズは 20 KB です。

  このカスタムデータは検索可能ですが、制限があります。[Searchable operational data (検索可能な運用データ)] 機能で (DescribeOpsItems API オペレーションによって提供)、OpsItem 概要ページにアクセスできるユーザーは誰でも、指定されたデータを表示および検索することができます。[Private operational data (プライベートな運用データ)] 機能で、(GetOpsItem API オペレーションと同様) OpsItem にアクセスできるユーザーのみがデータに表示できます。
- 重複排除機能: 関連リソースを指定することにより、OpsCenterは、組み込みロジックを使用して、OpsItems が重複しないようにします。OpsCenter にはオペレーションインサイトという機能も含まれており、重複した OpsItems に関する情報が表示されます。アカウントで重複する OpsItems の数をさらに制限するには、EventBridge イベントルールに重複排除文字列を手動で指定できます。詳細については、「OpsItems の重複を管理する」を参照してください。

- 一括編集OpsItems: OpsCenter で複数の OpsItems を選択し、次のフィールドのいずれかを編集します。ステータス、優先度、重要度、カテゴリ。
- ランブックを使用した簡単な修復

  各 OpsItem には、AWS リソースに関する一般的な問題を自動的に修正するために使用できる Systems Manager Automation ランブックのリストを含む [Runbooks (ランブック)] セクションがあります。OpsItem を開き、その OpsItem の AWS リソースを選択し、コンソールで [Run automation (自動化を実行)] ボタンを選択すると、OpsCenter に OpsItem を生成した AWS リソースで実行できる自動化ドキュメントのリストが表示されます。OpsItem から Automation ランブッ

クを実行したら、ランブックは、将来の参照を目的として、OpsItem の関連リソースに自動的に関連付けられます。さらに、OpsCenter を使用して EventBridge で OpsItem ルールを自動的に設定した場合は、一般的なイベントのランブックは、EventBridge によって自動的に関連付けられます。OpsCenter は、特定の OpsItem に対して実行された Automation ランブックのレコードを 30 日間保持します。詳細については、「OpsItem の問題を修正する」を参照してください。

- 変更通知: OpsItem が変更または編集されたときはいつでも、Amazon Simple Notification Service (SNS) トピックの ARN を指定して通知を発行できます。SNSトピックは、OpsItem と同じ AWS リージョン に存在する必要があります。
- 包括的な OpsItem の検索機能: OpsCenter では、OpsItems を速やかに見つけやすいように、複数の検索オプションが提供されています。検索方法の例は次のとおりです: ランブック実行の OpsItem ID、タイトル、最終更新日時、運用データ値、ソース、および自動化 ID。検索結果を絞り込むには、ステータスフィルターを使用します。
- OpsItem 概要レポート

  OpsCenter には、概要レポートページが含まれており、次のセクションが自動的に表示されます。

  - ステータスの概要: OpsItems の概要 (ステータス別: Open、In progress、Resolved、Open and In progress)。
  - Sources with most open OpsItems: オープン OpsItems が含まれている上位の AWS サービスの内訳。
  - OpsItems by source and age: ソースから作成された日数までにグループ化された OpsItems の数。

  OpsCenter 概要レポートの表示の詳細については、「OpsCenter 概要レポートの表示」を参照してください。
- ログ記録および監査機能のサポート

  他の AWS サービスとの統合を使用して、AWS アカウント の OpsCenter ユーザーアクションの監査およびログ記録ができます。詳細については、「OpsCenter ログとレポートを表示する」を参照してください。
- コンソール、CLI、PowerShell、および SDK の OpsCenter ツールへのアクセス

  AWS Systems Manager コンソール、AWS Command Line Interface (AWS CLI)、AWS Tools for PowerShell、または AWS SDK を使用すると OpsCenter を操作できます。

OpsCenter は既存のケース管理システムと統合できますか?

OpsCenter は既存のケース管理システムを補完するように設計されています。パブリック API オペレーションを使用して、OpsItems を既存のケース管理システムに統合できます。現在のシステムで手動のライフサイクルワークフローを維持し、OpsCenter を調査および修復のハブとして使用することもできます。

OpsCenter パブリック API オペレーションの詳細については、AWS Systems Manager API リファレンスの次の API オペレーションをご覧ください。

- CreateOpsItem
- DescribeOpsItems
- GetOpsItem
- GetOpsSummary
- UpdateOpsItem

OpsCenter の使用料金はかかりますか?

はい。詳細については、AWS Systems Manager 料金を参照してください。

OpsCenter はオンプレミスおよびハイブリッドマネージドノードと連携しますか ?

はい。Systems Manager を使用するように設定されているオンプレミスのマネージドノードに関する問題を調査して修正するには、OpsCenter を使用できます。Systems Manager 用のオンプレミスサーバーおよび仮想マシンのセットアップおよび設定に関する詳細については、「Systems Manager を利用したハイブリッド環境およびマルチクラウド環境でのノードの管理」を参照してください。

OpsCenter のクォータとは?

すべての Systems Manager ツールのクォータは、「Amazon Web Services 全般のリファレンス」の「Systems Manager Service Quotas」で確認できます。特に明記していない限り、クォータはリージョン固有です。

OpsCenter を設定する

AWS Systems Manager では、Systems Manager のツールである統合セットアップエクスペリエンスを使用して、OpsCenter と Explorer の利用を開始できます。Explorer は、AWS リソースに関する

情報をレポートするカスタマイズ可能な運用ダッシュボードです。このドキュメントでは、Explorer と OpsCenter のセットアップは統合セットアップと呼ばれます。

OpsCenter を Explorer でセットアップするには、統合セットアップを使用する必要があります。統合セットアップは、AWS Systems Manager コンソールでのみ使用できます。Explorer と OpsCenter をプログラムで設定することはできません。詳細については、「Systems Manager Explorer と OpsCenter の開始方法」を参照してください。

[開始する前に]

OpsCenter のセットアップ時に、OpsItems を自動的に作成する Amazon EventBridge のデフォルトルールを有効にします。次の表では、OpsItems を自動的に作成する、デフォルトの EventBridge ルールについて説明します。EventBridge のルールは、[OpsItem ルール] の下にある OpsCenter の [設定] ページで無効にできます。

> **Important**
>
> アカウントには、デフォルトルールで作成された OpsItems の料金も請求されます。詳細については、AWS Systems Manager 料金を参照してください。

ルール名	説明
SSMOpsItems-Autoscaling-instance-launch-failure	このルールは、EC2 自動スケーリングインスタンスの起動が失敗した場合に OpsItems を作成します。
SSMOpsItems-Autoscaling-instance-termination-failure	このルールは、EC2 自動スケーリングインスタンスの終了が失敗した場合に OpsItems を作成します。
SSMOpsItems-EBS-snapshot-copy-failed	このルールは、Amazon Elastic Block Store (Amazon EBS) スナップショットをコピーできなかったときに OpsItems を作成します。
SSMOpsItems-EBS-snapshot-creation-failed	このルールは、システムが Amazon EBS スナップショットを作成できなかったときに OpsItems を作成します。

ルール名	説明
SSMOpsItems-EBS-volume-performance-issue	このルールは AWS Health 追跡ルールに対応しています。このルールは、Amazon EBS ボリューム (health event = `AWS_EBS_DEGRADED_EBS_VOLUME_PERFORMANCE`) にパフォーマンス上の問題があるたびに OpsItems を作成します。
SSMOpsItems-EC2-issue	このルールは、AWS サービスやリソースに影響する予期しないイベントの AWS Health 追跡ルールに対応しています。このルールは、サービスの低下を引き起こしているオペレーション上の問題、またはローカライズされたリソースレベルの問題に関する認識を高めるために、サービスが通信を送信するときに OpsItems を作成します。例えば、このルールでは次のイベントに OpsItem を作成します: `AWS_EC2_OPERATIONAL_ISSUE` 。
SSMOpsItems-EC2-scheduled-change	このルールは AWS Health 追跡ルールに対応しています。AWS は、再起動、停止、またはインスタンスの開始など、インスタンスのイベントを予定できます。このルールは EC2 の予定されたイベントに OpsItems を作成します。予定されたイベントの詳細については、「Amazon EC2 ユーザーガイド」の「インスタンスの予定されたイベント」を参照してください。

ルール名	説明
SSMOpsItems-RDS-issue	このルールは、AWS サービスやリソースに影響する予期しないイベントの AWS Health 追跡ルールに対応しています。このルールは、サービスの低下を引き起こしているオペレーション上の問題、またはローカライズされたリソースレベルの問題に関する認識を高めるために、サービスが通信を送信するときに OpsItems を作成します。例えば、このルールでは次のイベントに OpsItem を作成します: `AWS_RDS_MYSQL_DATABASE_CRASHING_REPEATEDLY` 、`AWS_RDS_EXPORT_TASK_FAILED` 、および `AWS_RDS_CONNECTIVITY_ISSUE` 。
SSMOpsItems-RDS-scheduled-change	このルールは AWS Health 追跡ルールに対応しています。このルールは Amazon RDS の予定されたイベントに OpsItems を作成します。これらのイベントは、Amazon RDS サービスへの今後の変更に関する情報を提供します。サービスの中断を回避するためにアクションの実行を推奨するイベントもあります。ユーザー側のアクションなしで自動的に発生するイベントもあります。予定された変更アクティビティの間、リソースが一時的に利用できないことがあります。例えば、このルールでは次のイベントに OpsItem を作成します: `AWS_RDS_SYSTEM_UPGRADE_SCHEDULED` および `AWS_RDS_MAINTENANCE_SCHEDULED` 。予定されているイベントについて詳しくは、「AWS Health ユーザーガイド」の「イベントタイプのカテゴリ」を参照してください。
SSMOpsItems-SSM-maintenance-window-execution-failed	このルールは、Systems Manager メンテナンスウィンドウの処理が失敗したときに OpsItems を作成します。

ルール名	説明
SSMOpsItems-SSM-maintenance-window-execution-timedout	このルールは、Systems Manager のメンテナンスウィンドウのローンチがタイムアウトになったときに OpsItems を作成します。

次の手順に従って、OpsCenter を設定します。

OpsCenter をセットアップする

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[OpsCenter] を選択します。
3. OpsCenter ホームページで、[開始] を選択します。
4. OpsCenter セットアップページで、[このオプションを有効にすると、Explorer で AWS Config および Amazon CloudWatch Events が設定され、一般的に使用されるルールとイベントに基づいて OpsItems が自動的に作成されるようになります] を選択します。このオプションを選択しない場合、OpsCenter は無効のままになります。

   > **Note**
   >
   > Amazon EventBridge (以前の Amazon CloudWatch Events) は、CloudWatch Events のすべての機能の他に、カスタムイベントバス、サードパーティーのイベントソース、スキーマレジストリなどのいくつかの新機能を提供します。

5. [有効化]OpsCenter を選択します。

OpsCenter を有効にすると、[設定] から以下のことを実行できます。

- [CloudWatch コンソールを開く] ボタンをクリックして、CloudWatch アラームを作成します。詳細については、「OpsItems を作成するように CloudWatch を設定する」を参照してください。
- 運用上のインサイトを無効にします。詳細については、「OpsItems を減らすために運用上のインサイトを分析する」を参照してください。
- AWS Security Hub の検出結果のアラームを有効にします。詳細については、「OpsCenter と AWS Security Hub の統合について」を参照してください。

内容

- (オプション)OpsCenter を設定して、複数のアカウント間で OpsItems を一元管理する
- (オプション) OpsItems に関する通知を受け取るように Amazon SNS を設定する

(オプション)OpsCenter を設定して、複数のアカウント間で OpsItems を一元管理する

Systems Manager OpsCenter を使用すると、選択した AWS リージョン 内の複数の AWS アカウント 間で OpsItems を一元管理できます。この機能は AWS Organizations にお客様の組織をセットアップした後に利用可能になります。AWS Organizations は、作成し一元管理する組織に、複数の AWS アカウントを統合するためのアカウント管理サービスです。AWS Organizations には、お客様のビジネスの予算、セキュリティ、コンプライアンスのニーズをより適切に満たすアカウント管理および一括請求機能が備わっています。詳細については、AWS Organizations ユーザーガイドの「AWS Organizations とは何か」を参照してください。

AWS Organizations 管理アカウントに属するユーザーは、Systems Manager の委任管理者をセットアップできます。OpsCenter のコンテキストでは、委任管理者はメンバーアカウントで OpsItems を作成、編集、表示できます。委任管理者は Systems Manager Automation ランブックを使用して、OpsItems を生成している AWS リソースに関する OpsItems を一括解決または問題を修復することもできます。

> **Note**
>
> Systems Manager に対して、委任管理者を 1 人だけ割り当てることができます。詳細については、「Systems Manager 用の AWS Organizations 委任された管理者の作成」を参照してください。

Systems Manager では、OpsCenter複数の AWS アカウント 間で OpsItems を一元管理するための設定方法として、次の方法が用意されています。

- Quick Setup: Systems Manager ツールの 1 つであるクイックセットアップを使用すると、Systems Manager ツールのセットアップタスクと設定タスクを簡略化できます。詳細については、「AWS Systems Manager Quick Setup」を参照してください。

  OpsCenter の Quick Setup を使用すると、複数のアカウント間で OpsItems を管理するために次のタスクを実行できます。

  - アカウントを委任管理者として登録する (委任管理者がまだ指定されていない場合)

- 必要な AWS Identity and Access Management (IAM) ポリシーとロールを作成する
- 委任管理者が複数のアカウント間で OpsItems を管理できる AWS Organizations 組織または組織単位 (OU) を指定する

詳細については、「(オプション) Quick Setup を使用して、複数のアカウント間で OpsItems を管理するように OpsCenter を設定」を参照してください。

> **Note**
>
> Quick Setup は、Systems Manager が現在利用可能なすべての AWS リージョン 地域で利用できるわけではありません。複数のアカウント間で OpsItems を一元管理するように OpsCenter を設定したいリージョンで Quick Setup を利用できない場合は、手動で対応する必要があります。Quick Setup を利用できる AWS リージョン のリストを表示するには、AWS リージョン に Quick Setup の可用性 を参照してください。

- 手動セットアップ: 複数のアカウント間で OpsItems を一元管理するように OpsCenter を設定したいリージョンで Quick Setup を利用できない場合は、手動手順で対応できます。詳細については、「(オプション) OpsCenter の手動設定により、複数のアカウント間で OpsItems を一元管理する」を参照してください。

(オプション) Quick Setup を使用して、複数のアカウント間で OpsItems を管理するように OpsCenter を設定

AWS Systems Manager のツールである Quick Setup により、Systems Manager ツールの設定タスクと構成タスクが簡略化されます。OpsCenter 用の Quick Setup は、複数のアカウント間で OpsItems を管理するための次のタスクの実行に有用です。

- 委任された管理者のアカウントを指定する
- 必要な AWS Identity and Access Management (IAM) ポリシーとロールを作成する
- 委任管理者が複数のアカウント間で OpsItems を管理できる AWS Organizations 組織、またはメンバーアカウントのサブセットを指定する

Quick Setup を使用して複数のアカウント間で OpsItems を管理するように OpsCenter を設定すると、Quick Setup は指定されたアカウントに次のリソースを作成します。これらのリソースは、OpsItems を生成する AWS リソース生成に関する問題を解決するため、OpsItems をで作業し、オートメーションランブックを使用する権限を指定されたアカウントに付与します。

リソース	アカウント
`AWSServiceRoleForAmazonSSM_AccountDiscovery` AWS Identity and Access Management (IAM) サービスリンクロール このロールの詳細については、「ロールを使用した OpsCenter および Explorer の AWS アカウント 情報の収集」を参照してください。	AWS Organizations 管理アカウントと委任された管理者アカウント
`OpsItem-CrossAccountManagementRole` IAM ロール `AWS-SystemsManager-AutomationAdministrationRole` IAM ロール	委任された管理者アカウント
`OpsItem-CrossAccountExecutionRole` IAM ロール `AWS-SystemsManager-AutomationExecutionRole` IAM ロール デフォルトの OpsItem グループ (`OpsItemGroup`) に対する `AWS::SSM::ResourcePolicy` Systems Manager リソースポリシー	すべての AWS Organizations メンバーアカウント

> **Note**
>
> 手動で複数のアカウント間で OpsItems を管理するように OpsCenter を設定していた場合は、そのプロセスのステップ 4 と 5 で作成された AWS CloudFormation スタックまたはスタックセットを削除する必要があります。以下の手順を実行したときにそれらのリソースがアカウントに存在する場合、Quick Setup はクロスアカウント OpsItem 管理を適切に設定できません。

Quick Setup を使用して複数のアカウント間で OpsItems を管理するように OpsCenter を設定するには

1. AWS Organizations 管理アカウントを使用して AWS Management Console にログインします。
2. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
3. ナビゲーションペインで、[Quick Setup] を選択します。
4. [ライブラリ] タブを選択します。
5. 一番下までスクロールして、OpsCenter 設定タイルを探します。[作成] を選択します。
6. Quick SetupOpsCenter ページの [委任管理者] セクションに、アカウント ID を入力します。このフィールドを編集できない場合は、Systems Manager の委任管理者アカウントがすでに指定されています。
7. [ターゲット] セクションで、オプションを選択してください。[カスタム] を選択した場合は、複数のアカウント間で OpsItems を管理する組織単位 (OU) を選択します。
8. [作成] を選択します。

Quick Setup は OpsCenter 設定を作成し、必要な AWS リソースを指定された OU にデプロイします。

> **Note**
>
> 複数のアカウント間で OpsItems を管理しない場合は、Quick Setup から設定を削除できます。設定を削除すると、Quick Setup は設定が最初にデプロイされたときに作成された次の IAM ポリシーとロールを削除します。
>
> - 委任された管理者のアカウントからの `OpsItem-CrossAccountManagementRole`
> - `OpsItem-CrossAccountExecutionRole` と `SSM::ResourcePolicy` をすべての Organizations のメンバーアカウントから
>
> Quick Setup は、すべての組織単位および設定が最初にデプロイされた AWS リージョン から、設定を削除します。

OpsCenter に対する Quick Setupの設定に関する問題のトラブルシューティング

このセクションには、Quick Setup を使用してクロスアカウント OpsItem 管理を設定する場合の問題のトラブルシューティングに役立つ情報が含まれています。

トピック

- 次の StackSet へのデプロイに失敗しました: delegatedAdmin
- Quick Setup 設定ステータスが [失敗] となっている

次の StackSet へのデプロイに失敗しました: delegatedAdmin

OpsCenter 設定を作成するときに、Quick Setup が Organizations 管理アカウントに 2 つの AWS CloudFormation スタックセットをデプロイします。スタックセットには次のプレフィックス: `AWS-QuickSetup-SSMOpsCenter` を使用します。Quick Setup が次のエラー「`Deployment to these StackSets failed: delegatedAdmin`」表示する場合は、次の手順を使用してこの問題を解決してください。

StackSets failed:delegatedAdmin エラーをトラブルシューティングするには

1. Quick Setup コンソールに赤いバナーで `Deployment to these StackSets failed: delegatedAdmin` エラーが表示された場合は、委任された管理者アカウントと、Quick Setup ホームリージョンとして指定された AWS リージョン にサインインします。
2. https://console.aws.amazon.com/cloudformation で AWS CloudFormation コンソール を開きます。
3. Quick Setup 設定で作成されたスタックを選択します。スタック名に AWS-QuickSetup-SSMOpsCenter が含まれています。

   > **Note**
   >
   > CloudFormation は、失敗したスタックのデプロイを削除することがあります。スタックが [Stacks] (スタック) テーブルに表示されない場合は、フィルターリストから [Deleted] (削除済み) を選択します。

4. [Status] (ステータス) と [Status reason] (ステータス理由) を表示します。スタックのステータスの詳細については、「AWS CloudFormationユーザーガイド」の「スタックステータスコード」を参照してください。

5. 失敗したステップを正確に把握するには、[Events] (イベント) タブを開き、各イベントの [Status] (ステータス) を確認します。詳細については、「AWS CloudFormation ユーザーガイド」の「トラブルシューティング」を参照してください。

> **Note**
>
> CloudFormation のトラブルシューティングに関するステップによりデプロイの失敗を解決できない場合は、設定を削除したうえで再試行します。

Quick Setup 設定ステータスが [失敗] となっている

[構成の詳細] ページの [構成の詳細] テーブルに設定ステータスが `Failed` と表示されている場合は、障害が発生した AWS アカウント およびリージョンにサインインします。

Quick Setup が OpsCenter 設定の作成に失敗した場合のトラブルシューティングを行うには

1. 障害が発生した AWS アカウントと AWS リージョンにサインインしてください。
2. https://console.aws.amazon.com/cloudformation で AWS CloudFormation コンソール を開きます。
3. Quick Setup 設定で作成されたスタックを選択します。スタック名に AWS-QuickSetup-SSMOpsCenter が含まれています。

   > **Note**
   >
   > CloudFormation は、失敗したスタックのデプロイを削除することがあります。スタックが [Stacks] (スタック) テーブルに表示されない場合は、フィルターリストから [Deleted] (削除済み) を選択します。

4. [Status] (ステータス) と [Status reason] (ステータス理由) を表示します。スタックのステータスの詳細については、「AWS CloudFormationユーザーガイド」の「スタックステータスコード」を参照してください。
5. 失敗したステップを正確に把握するには、[Events] (イベント) タブを開き、各イベントの [Status] (ステータス) を確認します。詳細については、「AWS CloudFormation ユーザーガイド」の「トラブルシューティング」を参照してください。

メンバーアカウント設定で ResourcePolicyLimitExceededException と表示されている

スタックのステータスが `ResourcePolicyLimitExceededException` と示されている場合、アカウントは手動で、以前 OpsCenter クロスアカウント管理にオンボーディングされたことがあります。この問題を解決するには、手動オンボーディングプロセスのステップ 4 と 5 で作成された AWS CloudFormation スタックまたはスタックセットを削除する必要があります。詳細については、「AWS CloudFormation ユーザーガイド」の「スタックセットの削除」と「AWS CloudFormation コンソールでスタックを削除する」を参照してください。

(オプション) OpsCenter の手動設定により、複数のアカウント間で OpsItems を一元管理する

このセクションでは、クロスアカウント OpsItem 管理の OpsCenter を手動で設定する方法について説明します。このプロセスは引き続きサポートされていますが、Systems Manager Quick Setup を使用する新しいプロセスに置き換えられています。詳細については、「(オプション) Quick Setup を使用して、複数のアカウント間で OpsItems を管理するように OpsCenter を設定」を参照してください。

中央アカウントを設定して、メンバーアカウントの OpsItems 手動を作成し、それらの OpsItems を管理および修正することができます。中央アカウントには、AWS Organizations 管理アカウントか、AWS Organizations 管理アカウントと Systems Manager 委任管理者アカウントの両方を使用することができます。Systems Manager 委任管理者アカウントを中央アカウントとして使用することをお勧めします。この機能は、AWS Organizations を設定した後にのみ使用できます。

AWS Organizations では、ユーザーが作成して一元管理する組織に、複数の AWS アカウント を統合することができます。セントラルアカウントユーザーは、選択したすべてのメンバーアカウント用の OpsItems を同時に作成して、これらの OpsItems を管理できます。

このセクションの手順を使用して、Organizations の Systems Manager サービスプリンシパルを有効にし、アカウント間で OpsItems を操作するための AWS Identity and Access Management (IAM) アクセス許可を設定します。

トピック

- [開始する前に]
- ステップ 1: リソースデータの同期を作成する
- ステップ 2: AWS Organizations で Systems Manager のサービスプリンシパルを有効にする
- ステップ 3: サービスにリンクされたロール AWSServiceRoleForAmazonSSM_AccountDiscovery を作成する
- タスク 4: アカウント間で OpsItems を操作するためのアクセス許可を設定する

- タスク 5: アカウント間で関連リソースを使用するためのアクセス許可を設定する

> **Note**
>
> アカウント間で OpsCenter を使用する場合、`/aws/issue` タイプの OpsItems のみがサポートされます。

[開始する前に]

アカウント間で OpsItems を操作するように OpsCenter を設定する前に、以下を設定してください。

- Systems Manager の委任管理者アカウント 詳細については、「Explorer のための委任された管理者の設定」を参照してください。
- Organizations 内で 1 つの組織をセットアップして設定します。詳細については、「AWS Organizations ユーザーガイド」の「組織の作成と管理」を参照してください。
- 複数の AWS リージョン アカウントと AWS にわたって自動化ランブックを実行するように Systems Manager Automation を設定しました。詳細については、「複数の AWS リージョン とアカウントでのオートメーションの実行」を参照してください。

ステップ 1: リソースデータの同期を作成する

AWS Organizations のセットアップと設定の完了後、リソースデータ同期を作成することで、組織全体について OpsCenter の OpsItems を集計できるようになります。詳細については、「リソースデータ同期の作成」を参照してください。同期を作成するときは、[アカウントの追加] セクションで、必ず [AWS Organizations 設定のすべてのアカウントを含める] オプションを選択します。

ステップ 2: AWS Organizations で Systems Manager のサービスプリンシパルを有効にする

ユーザーがアカウントをまたいで OpsItems を使用できるようにするには、AWS Organizations で Systems Manager サービスプリンシパルを有効にしておく必要があります。以前に、他のツールを使用してマルチアカウントシナリオ用に Systems Manager を設定済みの場合は、Organizations 内で、既に Systems Manager サービスプリンシパルの設定が完了している場合があります。これを確認するには、 AWS Command Line Interface (AWS CLI) から以下のコマンドを実行します。他のマルチアカウントシナリオで Systems Manager を設定していない場合は、次の「AWS Organizations で Systems Manager サービスプリンシパルを有効にする」の手順に進んでください。

Systems Manager サービスプリンシパルが AWS Organizations で有効になっていることを確認するには

1. 最新バージョンの をローカルマシンにダウンロードAWS CLIします。
2. AWS CLI を開いて次のコマンドを実行し、認証情報と AWS リージョン リージョンを指定します。

```
aws configure
```

以下を指定するよう求められます。次の例では、各 ############## を独自の情報に置き換えます。

```
AWS Access Key ID [None]: key_name
AWS Secret Access Key [None]: key_name
Default region name [None]: region
Default output format [None]: ENTER
```

3. 次のコマンドを実行して、AWS Organizations のために Systems Manager サービスプリンシパルが有効になっていることを確認します。

```
aws organizations list-aws-service-access-for-organization
```

このコマンドは、下記の例のような情報を返します。

```
{
    "EnabledServicePrincipals": [
        {
            "ServicePrincipal":
 "member.org.stacksets.cloudformation.amazonaws.com",
            "DateEnabled": "2020-12-11T16:32:27.732000-08:00"
        },
        {
            "ServicePrincipal": "opsdatasync.ssm.amazonaws.com",
            "DateEnabled": "2022-01-19T12:30:48.352000-08:00"
        },
        {
            "ServicePrincipal": "ssm.amazonaws.com",
            "DateEnabled": "2020-12-11T16:32:26.599000-08:00"
        }
    ]
```

```
}
```

AWS Organizations で Systems Manager サービスプリンシパルを有効化する

まだ、Systems Manager サービスプリンシパルを Organizations 用に設定していない場合は、次に説明する手順に従って設定します。このコマンドの詳細については、「AWS CLI コマンドリファレンス」の「enable-aws-service-access」を参照してください。

1. まだ AWS Command Line Interface (AWS CLI) をインストールして設定していない場合は、インストールして設定します。詳細については、「CLI のインストール」および「CLI の設定」を参照してください。
2. 最新バージョンの をローカルマシンにダウンロードAWS CLIします。
3. AWS CLI を開いて次のコマンドを実行し、認証情報と AWS リージョン リージョンを指定します。

   ```
   aws configure
   ```

   以下を指定するよう求められます。次の例では、各 ############## を独自の情報に置き換えます。

   ```
   AWS Access Key ID [None]: key_name
   AWS Secret Access Key [None]: key_name
   Default region name [None]: region
   Default output format [None]: ENTER
   ```

4. 以下のコマンドを実行して、AWS Organizations 用に Systems Manager サービスプリンシパルを有効にします。

   ```
   aws organizations enable-aws-service-access --service-principal "ssm.amazonaws.com"
   ```

ステップ 3: サービスにリンクされたロール **AWSServiceRoleForAmazonSSM_AccountDiscovery** を作成する

AWSServiceRoleForAmazonSSM_AccountDiscovery ロールなどサービスにリンクされたロールは、AWS のサービス (例えば Systems Manager) に直接リンクされた、一意のタイプの IAM ロールです。サービスにリンクされたロールはサービスによって事前定義されており、サービスがお客様の代わりに他の AWS のサービス サービスを呼び出す際に必要な、すべてのアクセス許可が含まれ

ています。AWSServiceRoleForAmazonSSM_AccountDiscovery サービスにリンクされたロールの詳細については、Systems Manager アカウント検出のためのサービスにリンクされたロールの許可を参照してください。

AWS CLI を使用してサービスにリンクされたロール AWSServiceRoleForAmazonSSM_AccountDiscovery を作成するためには、次の手順を実行します。この手順で使用するコマンドの詳細については、「AWS CLI コマンドリファレンス」の「create-service-linked-role」を参照してください。

AWSServiceRoleForAmazonSSM_AccountDiscovery のサービスにリンクされたロールを作成するには

1. AWS Organizations 管理アカウントにサインインします。
2. Organizations の管理アカウントにサインインした状態で、次のコマンドを実行します。

```
aws iam create-service-linked-role \
    --aws-service-name accountdiscovery.ssm.amazonaws.com \
    --description "Systems Manager account discovery for AWS Organizations service-linked role"
```

タスク 4: アカウント間で OpsItems を操作するためのアクセス許可を設定する

AWS CloudFormation スタックセットを使用して、アカウント間で OpsItems を操作するアクセス許可をユーザーに付与する OpsItemGroup リソースポリシーと IAM 実行ロールを作成します。これを開始するには、OpsCenterCrossAccountMembers.zip ファイルをダウンロードしてそれを zip 解凍します。このファイルには、OpsCenterCrossAccountMembers.yaml AWS CloudFormation テンプレートファイルが含まれています。このテンプレートを使用してスタックセットを作成すると、CloudFormation は、アカウント内で、自動的に OpsItemCrossAccountResourcePolicy リソースポリシーと OpsItemCrossAccountExecutionRole 実行ロールを作成します。シークレットを作成する方法については、「AWS CloudFormation ユーザーガイド」の「スタックセットの作成」を参照してください。

> **Important**
>
> このタスクに関しては、次の重要事項に留意してください。
>
> - このスタックセットは、AWS Organizations 管理アカウントにサインインした状態でデプロイする必要があります。

- この手順は、代理管理者アカウントを含むアカウント間で OpsItems を操作するすべてのアカウントにサインインして、繰り返し実行する必要があります。
- 別の AWS リージョン でクロスアカウントの OpsItems 管理を有効にする場合は、テンプレートの [Specify regions] (リージョンの指定) セクションで、[Add all regions] (すべてのリージョンを追加) を選択します。クロスアカウントの OpsItem 管理は、オプトインリージョンではサポートされていません。

タスク 5: アカウント間で関連リソースを使用するためのアクセス許可を設定する

OpsItem には、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスや Amazon Simple Storage Service (Amazon S3) バケットなど、影響を受けたリソースの詳細情報を含めることができます。前のステップ 4 で作成した `OpsItemCrossAccountExecutionRole` 実行ロールにより、メンバーアカウントの関連リソースを表示するための読み取り専用のアクセス許可が OpsCenter に付与されます。これと同時に、管理アカウントが関連リソースを表示したり操作したりするための許可を付与する、IAM ロールを作成する必要があります。この処理はこのタスクで完了します。

これを開始するには、`OpsCenterCrossAccountManagementRole.zip` ファイルをダウンロードしてそれを zip 解凍します。このファイルには、`OpsCenterCrossAccountManagementRole.yaml` AWS CloudFormation テンプレートファイルが含まれています。このテンプレートを使用してスタックを作成すると、CloudFormation はアカウント内で、自動的に `OpsCenterCrossAccountManagementRole` IAM ロールを作成します。スタック作成の詳細については、「AWS CloudFormation ユーザーガイド」の「AWS CloudFormation コンソールでのスタックの作成」 を参照してください。

Important

このタスクに関しては、次の重要事項に留意してください。

- アカウントを、OpsCenter の委任管理者として指定する予定の場合は、スタックの作成時に必ずその AWS アカウント を指定してください。
- この手順は、AWS Organizations の管理アカウントにログインした状態で実行し、委任管理者アカウントに再度ログインした後にも実行する必要があります。

(オプション) OpsItems に関する通知を受け取るように Amazon SNS を設定する

システムが OpsItem を作成するか、既存の OpsItem を更新したときに、Amazon Simple Notification Service (Amazon SNS) トピックで通知を受け取るように OpsCenter を設定できます。

OpsItems の通知を受信するには、次のステップを実行します。

- ステップ 1: Amazon SNS トピックを作成してサブスクライブする
- ステップ 2: Amazon SNS アクセスポリシーを更新する
- ステップ 3: AWS KMS のアクセスポリシーを更新する

> **Note**
>
> ステップ 2 で AWS Key Management Service (AWS KMS) サーバー側の暗号化をオンにした場合は、ステップ 3 を完了する必要があります。それ以外の場合は、ステップ 3 をスキップできます。

- ステップ 4: デフォルトの OpsItems ルールを有効にして新しい OpsItems の通知を送信する

ステップ 1: Amazon SNS トピックを作成してサブスクライブする

通知を受け取るには、Amazon SNS トピックを作成してサブスクライブする必要があります。詳細については、Amazon Simple Notification Service デベロッパーガイドの「Amazon SNS トピックを作成する」および「Amazon SNS トピックへサブスクライブする」を参照してください。

> **Note**
>
> OpsCenter を複数の AWS リージョン またはアカウントで使用している場合は、OpsItem 通知を受け取る各リージョンまたはアカウントで Amazon SNS トピックを作成してサブスクライブする必要があります。

ステップ 2: Amazon SNS アクセスポリシーを更新する

Amazon SNS トピックを OpsItems に関連付ける必要があります。以下の手順を使用して Amazon SNS アクセスポリシーをセットアップし、Systems Manager がステップ 1 で作成した Amazon SNS トピックに OpsItems 通知を発行できるようにします。

1. AWS Management Console にサインインして Amazon SNS コンソール (https://console.aws.amazon.com/sns/v3/home) を開きます。
2. ナビゲーションペインで、[トピック] を選択します。
3. ステップ 1 で作成したトピックを選択し、[編集] をクリックします。
4. [アクセスポリシー] を展開します。
5. 既存のポリシーに次の Sid ブロックを追加します。各##############をユーザー自身の情報に置き換えます。

```
{
      "Sid": "Allow OpsCenter to publish to this topic",
      "Effect": "Allow",
      "Principal": {
        "Service": "ssm.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account ID:topic name", // Account ID of the
 SNS topic owner
      "Condition": {
      "StringEquals": {
        "AWS:SourceAccount": "account ID" //  Account ID of the OpsItem owner
      }
   }
}
```

> **Note**
>
> 混乱した代理シナリオから保護する aws:SourceAccount グローバル条件キー。この条件キーを使用するには、値を OpsItem 所有者のアカウント ID に設定します。詳細については、「IAM ユーザーガイド」の「混乱した代理問題」を参照してください。

6. [Save changes] (変更の保存) をクリックします。

OpsItems が作成または更新されると、システムは Amazon SNS トピックに通知を送信するようになります。

> **Important**
>
> ステップ 2 で AWS Key Management Service (AWS KMS) サーバー側暗号化キーを使用して Amazon SNS トピックを設定した場合は、ステップ 3 を完了します。それ以外の場合は、ステップ 3 をスキップできます。

ステップ 3: AWS KMS のアクセスポリシーを更新する

Amazon SNS トピックの AWS KMS サーバー側の暗号化をオンにした場合、トピックを設定したときに選択した AWS KMS key のアクセスポリシーも更新する必要があります。以下の手順を使用してアクセスポリシーを更新し、Systems Manager がステップ 1 で作成した Amazon SNS トピックに OpsItem 通知を発行できるようにします。

> **Note**
>
> OpsCenter は、AWS マネージドキー を使用して設定された Amazon SNS トピックへの OpsItems の発行をサポートしていません。

1. AWS KMS コンソール (https://console.aws.amazon.com/kms) を開きます。
2. AWS リージョン を変更するには、ページの右上隅にあるリージョンセレクターを使用します。
3. ナビゲーションペインで、[カスタマーマネージドキー] を選択します。
4. トピックの作成時に選択した KMS キーの ID を選択します。
5. [Key Policy] (キーポリシー) セクションで、[Switch to policy view] (ポリシービューへの切り替え) を選択します。
6. [Edit] を選択します。
7. 既存のポリシーに次の `Sid` ブロックを追加します。各`###############`をユーザー自身の情報に置き換えます。

```
{
      "Sid": "Allow OpsItems to decrypt the key",
      "Effect": "Allow",
      "Principal": {
        "Service": "ssm.amazonaws.com"
      },
      "Action": ["kms:Decrypt", "kms:GenerateDataKey*"],
```

```
        "Resource": "arn:aws:kms:region:account ID:key/key ID"
    }
```

次の例では、新しいブロックが行 14 に入力されています。

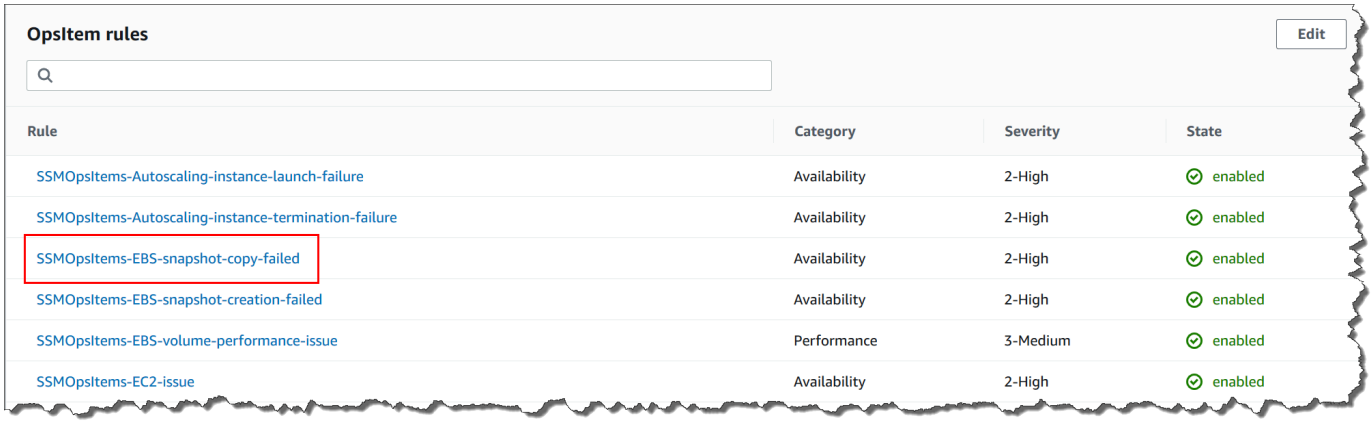
8. [Save changes] (変更の保存) をクリックします。

ステップ 4: デフォルトの OpsItems ルールを有効にして新しい OpsItems の通知を送信する

Amazon EventBridge のデフォルトの OpsItems ルールには、Amazon SNS 通知の Amazon リソースネーム (ARN) が設定されていません。次の手順に従って EventBridge でルールを編集し、`notifications` ブロックを入力します。

デフォルトの OpsItem ルールに通知ブロックを追加するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[OpsCenter] を選択します。
3. [OpsItems] タブを選択し、[Configure sources (ソースの設定)] を選択します。
4. 次の例に示すように、`notifications` ブロックを使用して設定するソースルールの名前を選択します。



ルールは Amazon EventBridge で開きます。

5. ルールの詳細ページの [Targets] (ターゲット) タブで [Edit] (編集) を選択します。
6. [Additional settings] (追加設定) セクションの [Configure target input] (ターゲット入力の設定) を選択します。
7. [テンプレート] ボックスに、次の形式で notifications ブロックを追加します。

```
"notifications":[{"arn":"arn:aws:sns:region:account ID:topic name"}],
```

以下に例を示します。

```
"notifications":[{"arn":"arn:aws:sns:us-west-2:1234567890:MySNSTopic"}],
```

米国西部 (オレゴン) (us-west-2) リージョンについての次の例に示すように、resources ブロックの前に通知ブロックを入力します。

```
{
    "title": "EBS snapshot copy failed",
    "description": "CloudWatch Event Rule SSMOpsItems-EBS-snapshot-copy-failed was
 triggered. Your EBS snapshot copy has failed. See below for more details.",
    "category": "Availability",
    "severity": "2",
    "source": "EC2",
    "notifications": [{
        "arn": "arn:aws:sns:us-west-2:1234567890:MySNSTopic"
    }],
    "resources": <resources>,
    "operationalData": {
        "/aws/dedup": {
```

```
            "type": "SearchableString",
            "value": "{\"dedupString\":\"SSMOpsItems-EBS-snapshot-copy-failed\"}"
        },
        "/aws/automations": {
            "value": "[ { \"automationType\": \"AWS:SSM:Automation\",
 \"automationId\": \"AWS-CopySnapshot\" } ]"
        },
        "failure-cause": {
            "value": <failure - cause>
        },
        "source": {
            "value": <source>
        },
        "start-time": {
            "value": <start - time>
        },
        "end-time": {
            "value": <end - time>
        }
    }
}
```

8. [確認] を選択します。
9. [Next] を選択します。
10. [Next] を選択します。
11. [ルールの更新] を選択します。

次回システムがデフォルトルールの OpsItem を作成するときに、Amazon SNS トピックに通知を発行します。

OpsCenter と他の AWS のサービス との統合

AWS Systems Manager のツールである OpsCenter は、複数の AWS のサービスを統合して、AWS リソースに関する問題を診断して修正します。OpsCenter と統合する前に、AWS のサービス を設定する必要があります。

デフォルトでは、次の AWS のサービス が OpsCenter と統合されており、OpsItems を自動的に作成できます。

- Amazon CloudWatch
- Amazon CloudWatch Application Insights

- Amazon EventBridge
- AWS Config
- AWS Systems Manager Incident Manager

OpsItems を自動的に作成するには、次のサービスを OpsCenter と統合する必要があります。

- Amazon DevOps Guru
- AWS Security Hub

これらのサービスのいずれかが OpsItem を作成すると、OpsCenter から OpsItem を管理および修正できます。詳細については、OpsItems を管理するおよびOpsItem の問題を修正するを参照してください。

AWS のサービス の詳細および OpsCenter との統合方法については、以下のトピックを参照してください。

トピック

- OpsCenter と Amazon CloudWatch の統合について
- OpsCenter と Amazon CloudWatch Application Insights の統合について
- OpsCenter と Amazon DevOps Guru の統合について
- OpsCenter と Amazon EventBridge の統合について
- OpsCenter と AWS Config の統合について
- OpsCenter と AWS Security Hub の統合について
- OpsCenter と Incident Manager の統合について

OpsCenter と Amazon CloudWatch の統合について

Amazon CloudWatch は AWS リソースとサービスをモニタリングし、使用しているすべての AWS のサービス でメトリクスを表示します。アラームがアラーム状態になると、CloudWatch は OpsItem を作成します。例えば、Application Load Balancer によって生成された HTTP エラーが急増した場合に、OpsItem を自動的に作成するようにアラームを設定できます。

CloudWatch で OpsItems を作成するように設定できるアラームを以下のリストに示します。

- Amazon DynamoDB: データベースの読み取りおよび書き込みアクションがしきい値に達する
- Amazon EC2: CPU 使用率がしきい値に達する

- AWS 請求: 推定請求額がしきい値に達する
- Amazon EC2: インスタンスがステータスチェックに失敗する
- Amazon Elastic Block Store (EBS): ディスク領域の使用率がしきい値に達する

アラームを作成するか、既存のアラームを編集して OpsItem を作成できます。詳細については、「OpsItems を作成するように CloudWatch を設定する」を参照してください。

統合セットアップ使用して OpsCenter を有効にすると、CloudWatch が OpsCenterと統合されます。

OpsCenter と Amazon CloudWatch Application Insights の統合について

Amazon CloudWatch Application Insights を使用すると、アプリケーションのリソースをモニタリングする最適な条件を設定し、データを継続的に分析してアプリケーションの問題の徴候を検出できます。CloudWatch Application Insights でアプリケーションリソースを設定する際に、システムが OpsCenter で OpsItems を作成するように選択できます。アプリケーションで検出された問題ごとに、OpsCenter コンソールに 1 つの OpsItem が作成されます。詳細については、「Amazon CloudWatch ユーザーガイド」の「モニタリングするアプリケーションをセットアップ、設定、管理する」を参照してください。

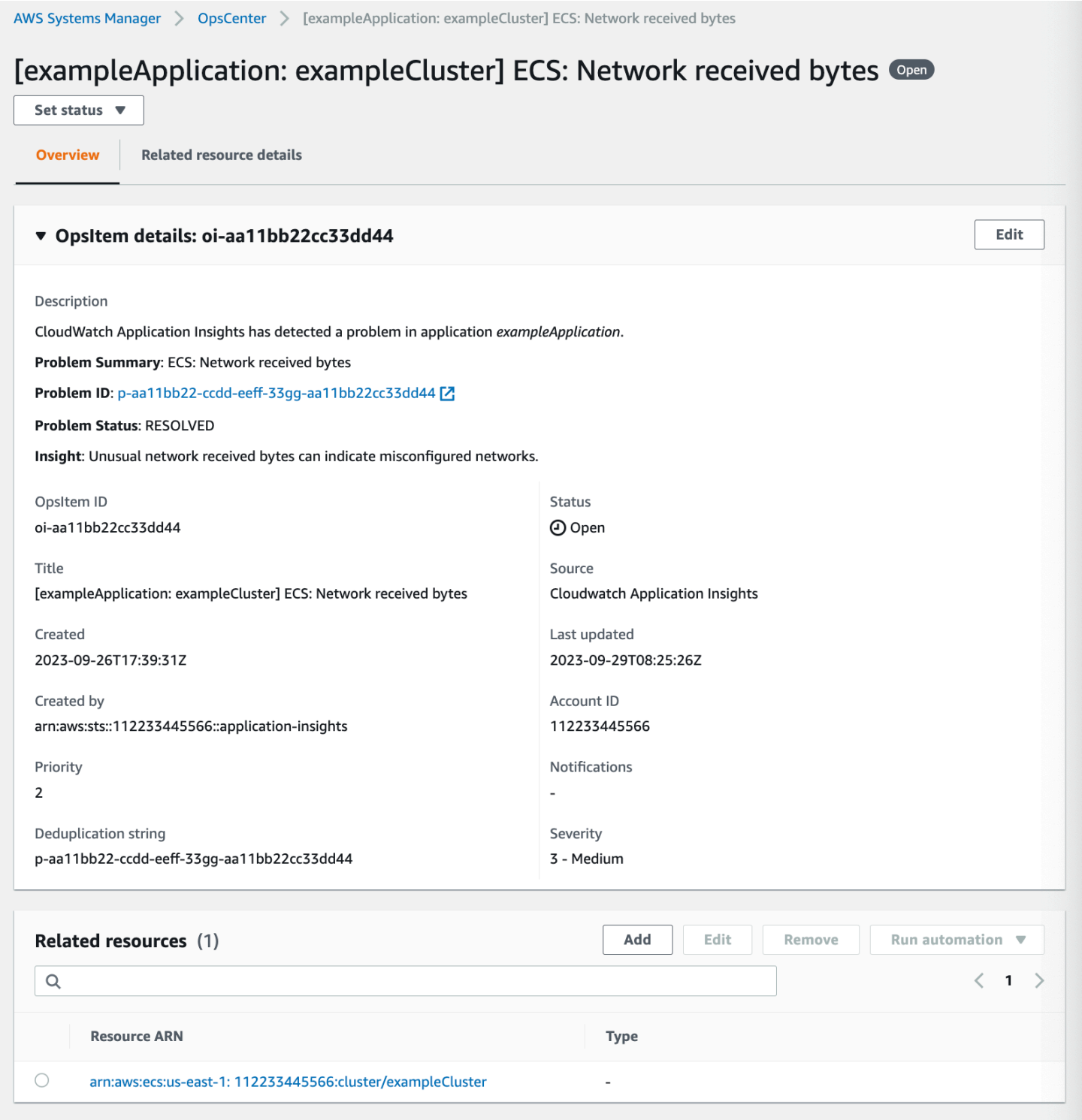
> **Note**
>
> 2023 年 10 月 16 日以降、CloudWatch Application Insights によって作成された OpsItems のタイトルと説明は、以下の改良されたフォーマットを使用するようになりました。

```
OpsItem title: [<APPLICATION NAME>: <RESOURCE ID>] <PROBLEM SUMMARY>

OpsItem description:

CloudWatch Application Insights has detected a problem in application <APPLICATION
 NAME>.
Problem summary: <PROBLEM SUMMARY>
Problem ID: <PROBLEM ID> (hyperlinks to the Application Insights problem summary page)
Problem Status: <PROBLEM STATUS>
Insight: <INSIGHT>
```

以下がその例です。



OpsCenter と Amazon DevOps Guru の統合について

Amazon DevOps Guru は、機械学習を適用して、運用データ、アプリケーションのメトリクス、およびアプリケーションのイベントを分析し、通常の運用パターンから逸脱する動作を特定しま

す。DevOps Guru を有効にして OpsCenter で OpsItem を生成すると、各インサイトが新しい OpsItem を生成します。OpsItems は OpsCenter を使用して管理することができます。

DevOps Guru は自動的に OpsItems を作成します。Systems Manager のツールである Quick Setup を使用すると、Amazon DevOps Guru が OpsItems を作成できるようになります。システムは、AWSServiceRoleForDevOpsGuru AWS Identity and Access Management (IAM) サービスにリンクされたロールを使用して OpsItems を作成します。

OpsCenter とDevOps Guru を統合するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Quick Setup] を選択します。
3. [DevOps Guru 設定オプションのカスタマイズ] ページで、[ライブラリ] タブをクリックします。
4. [DevOps Guru] ペインで [作成] をクリックします。
5. [設定オプション] で、[AWS Systems Manager OpsItems を有効化] をクリックします。
6. セットアップが完了したら、[作成] をクリックします。

OpsCenter と Amazon EventBridge の統合について

Amazon EventBridge は、AWS リソースの変更を記述するイベントのストリームを配信します。統合セットアップを使用して OpsCenter を有効にすると、EventBridge と OpsCenter が統合され、デフォルトの EventBridge ルールが有効になります。これらのルールに基づいて、EventBridge が OpsItems を作成します。ルールを使用すると、イベントをフィルターして OpsCenter に振り分けて、調査や修正を行うことができます。

> **Note**
>
> Amazon EventBridge (以前の Amazon CloudWatch Events) は、CloudWatch Events のすべての機能の他に、カスタムイベントバス、サードパーティーのイベントソース、スキーマレジストリなどのいくつかの新機能を提供します。

OpsItem を作成するために EventBridge で 設定できるルールは次のとおりです。

- Security Hub: セキュリティアラートが発行されました

- Amazon DynamoDB: スロットリングイベント
- Amazon Elastic Compute Cloud Auto Scaling: インスタンスの起動に失敗しました
- Systems Manager: オートメーションを実行できませんでした
- AWS Health: スケジュールされたメンテナンスのアラート
- Amazon EC2: インスタンスの状態が実行中から停止に変わりました

必要に応じて、ルールを作成するか、既存のルールを編集して OpsItems ルールを作成できます。ルールを編集して OpsItem を作成する方法については、「EventBridge ルールを設定して OpsItems を作成する」を参照してください。

OpsCenter と AWS Config の統合について

AWS Config は、AWS アカウント にある AWS リソースの設定詳細ビューを提供します。

AWS Config は OpsCenter と直接統合されません。代わりに、AWS Config が非準拠インスタンスを検出した場合などに、Amazon EventBridge にイベントを送信する AWS Config ルールを作成します。次に、EventBridge は、作成した EventBridge ルールと照らし合わせてそのイベントを評価します。ルールが一致すると、EventBridge はイベントを OpsItem に変換し、宛先 OpsCenter に送信します。

この OpsItem を使用すると、非準拠のリソースの詳細を追跡して、調査アクションを記録し、一貫した改善措置へのアクセスを提供できます。

関連情報

EventBridge ルールを設定して OpsItems を作成する

AWS Systems Manager、OpsCenter、AWS Config を使用してコンプライアンスモニタリングを行う

OpsCenter と AWS Security Hub の統合について

AWS Security Hub は AWS アカウント やさまざまなサービスからセキュリティデータ、呼び出された検出結果を収集します。Security Hub は、一連のルールを使用して検出結果を検出して生成することで、管理するリソースのセキュリティ問題の特定、優先順位付け、修正を支援します。このトピックで説明されているように統合を設定すると、Systems Manager は OpsCenter の Security Hub 検出結果に対する OpsItems を作成します。

> **Note**
>
> OpsCenter は、Security Hub との双方向の統合を実現しています。つまり、セキュリティの検出結果に基づいて、OpsItem の [ステータス] または [重大度] フィールドを更新すると、システムはその変更を Security Hub と同期します。同様に、検出結果に変更を加えると、OpsCenter の対応する OpsItems 項目に自動的に更新されます。
> Security Hub 検出結果から OpsItem を作成すると、Security Hub メタデータが OpsItem の運用データフィールドに自動的に追加されます。このメタデータが削除されると、双方向更新は機能しなくなります。

デフォルトでは、Systems Manager は重大度が Critical と High の検出結果に OpsItems を作成します。また、重要度が Medium および Low の検出結果に対して OpsItems を作成するように OpsCenter を設定することもできます。OpsCenter では、情報提供のための検出結果に対する OpsItems は、修正が必要ないため作成されません。Security Hub 重大度レベルの詳細については、「AWS Security Hub API リファレンス」の「重大度」を参照してください。

[開始する前に]

Security Hub の検出結果をもとに、OpsItems を作成するよう OpsCenter を設定する前に、Security Hub セットアップタスクを完了したことを確認します。詳細については、AWS Security Hub ユーザーガイドの「Security Hub の設定」を参照してください。

Security Hub と OpsCenter を統合すると、システムは `AWSServiceRoleForSystemsManagerOpsDataSync` IAM サービスにリンクされたロールを使用して OpsItems を作成します。このロールの詳細については、「ロールを使用して、Explorer の OpsData および OpsItems を作成」を参照してください。

> **Warning**
>
> Security Hub と OpsCenter の統合の価格設定に関する重要な情報に注意してください。
>
> - 設定時に Security Hub 管理者アカウントにログインしていて、OpsCenter と Security Hub の統合を設定すると、システムは管理者とすべてのメンバーアカウントの検出結果に OpsItems を作成します。OpsItems は管理者アカウントですべて作成されます。さまざまな要因によっては、これにより AWS から予想外に多額の請求が発生する可能性があります。

統合を設定するときにログインしていたのがメンバーアカウントであった場合、システムは個人のアカウントの検出結果にのみ OpsItems を作成します。Security Hub 管理者アカウント、メンバーアカウント、および検出結果の EventBridge イベントフィードとの関係の詳細については、「AWS Security Hubユーザーガイド」で「EventBridge との Security Hub 統合のタイプ」を参照してください。

- 検出結果が OpsItem を作成するたびに、OpsItem の作成には通常料金がかかります。また、OpsItem を編集した場合や、対応する検出結果が Security Hub で更新された (OpsItem がトリガーされる) 場合にも課金されます。
- AWS Security Hub との統合によって作成された OpsItems は現在、リージョンのアカウントあたり 500,000 OpsItems の最大クォータによって制限されていません。そのため、Security Hub アラートによって、アカウント内の各リージョンで 500,000 を超える課金対象の OpsItems が作成される可能性があります。

  高負荷の本番環境では、Security Hub の検出結果の範囲を重要度の高い問題のみに制限することをお勧めします。

Security Hub の調査結果に対し OpsCenter を作成するために OpsItems を設定するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[OpsCenter] を選択します。
3. [設定] を選択します。
4. [Security Hub の検出結果] セクションで、[編集] を選択します。
5. スライダーを選択して [無効] を [有効] に変更します。
6. 重大度の検出結果が Medium または Low に対して、システムで OpsItems を作成するには、これらのオプションを切り替えます。
7. [Save (保存)] を選択して設定を保存します。

Security Hub の検出結果に対し、システムで OpsItems を作成する必要がなければ、次の手順を使用してください。

Security Hub の検出結果に対する OpsItems の受信を停止するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[OpsCenter] を選択します。
3. [設定] を選択します。
4. [Security Hub の検出結果] セクションで、[編集] を選択します。
5. スライダーを選択して [有効] を [無効] に変更します。スライダーを切り替えられない場合は、AWS アカウント の Security Hub が有効になっていません。
6. [保存] を選択して設定を保存します。OpsCenter は Security Hub の検出結果に基づいて OpsItems を作成しなくなります。

> **Important**
>
> Systems Manager の委任管理者または AWS Organizations 管理アカウントは、Explorer でリソースデータ同期を作成して、複数のアカウントまたは AWS リージョン に対して OpsCenter の Security Hub 検出結果を有効にできます。Explorer で Security Hub ソースが有効になっていて、Security Hub 統合を無効にしたメンバーアカウントをターゲットとするリソースデータ同期が存在する場合、管理者が選択した設定が優先されます。OpsCenter は、Security Hub 検出結果に対して引き続き OpsItems を作成します。リソースデータ同期のターゲットとなるメンバーアカウントで Security Hub 検出結果に対する OpsItems の作成を停止するには、管理者に連絡してリソースデータ同期からアカウントを削除するよう依頼するか、Explorer の Security Hub ソースをオフにします。Explorer での設定の変更については、「Systems Manager Explorer のデータソースを編集する」を参照してください。

OpsCenter と Incident Manager の統合について

AWS Systems Manager のツールである Incident Manager は、AWS でホストされたアプリケーションに影響を与えるインシデントを軽減し、回復させるのに役立つインシデント管理コンソールを提供します。インシデントとは、サービスの品質の計画外の中断または低下です。Incident Manager をセットアップして設定すると、システムが OpsCenter で OpsItems を自動的に作成します。

システムが Incident Manager でインシデントを作成すると、OpsCenter で OpsItem も作成され、そのインシデントが関連アイテムとして表示されます。OpsItem が既に存在する場合、Incident Manager は OpsItem を作成しません。この最初の OpsItem は、親 OpsItem と呼ばれます。イン

シデントの規模と範囲が大きくなる場合は、インシデントを既存の OpsItem に追加できます。必要に応じて、OpsItem のインシデントを手動で作成することができます。インシデントを閉じた後、Incident Manager で分析を作成し、類似した問題に対する改善プロセスの見直しを行い、改善することができます。

デフォルトでは、OpsCenter は Incident Manager と統合されています。Incident Manager が設定されていない場合、OpsCenter ページには Incident Manager を設定するためのメッセージが表示されます。Incident Manager が OpsItem を作成すると、OpsCenter から OpsItem を管理および修正できます。OpsItem のインシデントを作成する手順については、「OpsItem のインシデントを作成する」を参照してください。

OpsItems の作成

AWS Systems Manager のツールである OpsCenter をセットアップして AWS のサービスと統合すると、AWS のサービスがデフォルトのルール、イベント、またはアラームに基づいて OpsItems を自動的に作成します。

デフォルトの Amazon EventBridge ルールのステータスと重要度レベルを表示できます。必要に応じて、Amazon EventBridge からこれらのルールを作成または編集できます。Amazon CloudWatch からアラームを表示したり、作成または編集したりすることもできます。ルールとアラームを使用して、OpsItems を自動的に生成するためのイベントを設定できます。

システムが OpsItem を作成すると、ステータスが [未解決] になります。OpsItem の調査を開始するときは、ステータスを [進行中] に変更し、OpsItem を修正したら [解決済み] に変更できます。OpsItems を作成するように AWS のサービス でアラームとルールを設定する方法と、OpsItems を手動で作成する方法の詳細については、次のトピックを参照してください。

トピック

- EventBridge ルールを設定して OpsItems を作成する
- OpsItems を作成するように CloudWatch を設定する
- OpsItems を手動で作成する

EventBridge ルールを設定して OpsItems を作成する

Amazon EventBridge がイベントを受信すると、デフォルトのルールに基づいて 新しい OpsItem を作成します。ルールを作成するか、既存のルールを編集して、OpsCenter を EventBridge イベントのターゲットとして設定できます。新しいイベントルールの作成方法については、「Amazon EventBridge ユーザーガイド」の「AWS のサービス のルールを作成する」を参照してください。

OpsCenter に OpsItems を作成する EventBridge ルールを設定するには

1. Amazon EventBridge コンソール (https://console.aws.amazon.com/events/) を開きます。
2. ナビゲーションペインで ルール] を選択します。
3. [ルール] ページの [イベントバス] で [default] (デフォルト) を選択します。
4. [ルール] で、ルールの名前の横にあるチェックボックスをオンにしてルールを選択します。
5. ルールの名前を選択して、その詳細ページを開きます。[ルールの詳細] セクションで、[ステータス] が [有効] に設定されていることを確認します。

   > **Note**
   >
   > 必要に応じて、ページの右上隅にある [編集] を使用してステータスを更新できます。

6. [Targets] タブを選択します。
7. [Targets] タブで、[Edit] を選択します。
8. [ターゲットタイプ] で [AWS のサービス] を選択します。
9. [Select a target] (ターゲットを選択) では、[Systems Manager OpsItem] を選択します。
10. 多くのターゲットタイプで、EventBridge はターゲットにイベントを送信するためのアクセス許可が必要です。これらの場合、EventBridge は、イベントの実行に必要な AWS Identity and Access Management (IAM) ロールを作成できます。

    - 自動的に IAM ロールを作成するには、[Create a new role for this specific resource (この特定のリソースに対して新しいロールを作成する)] を選択します。
    - OpsCenter で OpsItems を作成する EventBridge アクセス許可を付与するために作成した IAM ロールを使用するには、[既存のロールの使用] を選択します。

11. [追加設定] セクションの [ターゲット入力の設定] で [入力トランスフォーマー] を選択します。

    [入力トランスフォーマー] オプションを使用すると、重複排除文字列と、タイトルや重要度など、OpsItems のその他の重要な情報を指定できます。

12. 入力トランスフォーマーの設定 を選択します。
13. [ターゲット入力トランスフォーマー] の [入力パス] で、トリガーするイベントから解析する値を指定します。例えば、ルールをトリガーするイベントの開始時刻、終了時刻、およびその他の詳細を解析するには、次の JSON を使用します。

```
{
    "end-time": "$.detail.EndTime",
```

```
    "failure-cause": "$.detail.cause",
    "resources": "$.resources[0]",
    "source": "$.detail.source",
    "start-time": "$.detail.StartTime"
}
```

14. [Template] (テンプレート) で、ターゲットに送信する情報を指定します。例えば、次の JSON を使用して OpsCenter に情報を渡します。この情報は、OpsItem を作成するために使用されます。

> **Note**
>
> 入力テンプレートが JSON 形式の場合、テンプレート内のオブジェクト値に引用符を含めることはできません。たとえば、リソース、障害原因、ソース、開始時刻、終了時刻の値を引用符で囲むことはできません。

```
{
    "title": "EBS snapshot copy failed",
    "description": "CloudWatch Event Rule SSMOpsItems-EBS-snapshot-copy-failed was
 triggered. Your EBS snapshot copy has failed. See below for more details.",
    "category": "Availability",
    "severity": "2",
    "source": "EC2",
    "operationalData": {
        "/aws/dedup": {
            "type": "SearchableString",
            "value": "{\"dedupString\":\"SSMOpsItems-EBS-snapshot-copy-failed\"}"
        },
        "/aws/automations": {
            "value": "[ { \"automationType\": \"AWS:SSM:Automation\",
 \"automationId\": \"AWS-CopySnapshot\" } ]"
        },
        "failure-cause": {
            "value": <failure-cause>
        },
        "source": {
            "value": <source>
        },
        "start-time": {
            "value": <start-time>
        },
```

```
        "end-time": {
            "value": <end-time>
        },
         },
        "resources": {
            "value": <resources>
        }
    }
}
```

これらのフィールドの詳細については、Amazon EventBridge ユーザーガイド の「ターゲット入力を変換する」を参照してください。

15. [確認] を選択します。
16. [Next] を選択します。
17. [Next] を選択します。
18. [ルールの更新] を選択します。

イベントから OpsItem が作成されたら、OpsItem を開いて、[Private operational data (プライベート運用データ)] セクションまで下にスクロールして、イベントの詳細を表示することができます。OpsItem でオプションを設定する方法については、「OpsItems を管理する」を参照してください。

OpsItems を作成するように CloudWatch を設定する

AWS Systems Manager のツールである OpsCenter の統合セットアップ中に、Amazon CloudWatch を有効にして、一般的なアラームに基づいて OpsItems を自動的に作成します。アラームを作成するか、既存のアラームを編集して、OpsCenter に OpsItems を作成できます。

OpsItems を作成するアラームを設定すると、CloudWatch は AWS Identity and Access Management (IAM) でサービスにリンクされた新しいロールを自動的に作成します。新しいロールの名前は `AWSServiceRoleForCloudWatchAlarms_ActionSSM` です。CloudWatch サービスにリンクされたロールの詳細については、「Amazon CloudWatch ユーザーガイド」の「CloudWatch のサービスにリンクされたロールの使用」を参照してください。

CloudWatch アラームが OpsItem を生成すると、OpsItem に [CloudWatch アラーム - '***alarm_name***' はアラーム状態です] が表示されます。

特定の OpsItem の詳細を表示するには、[OpsItem] を選択し、[関連リソースの詳細] タブを選択します。OpsItems を手動で編集して、重要度やカテゴリなどの詳細を変更できます。ただし、ア

ラームの重要度やカテゴリを編集する場合、そのアラームから既に作成されている OpsItems の重要度やカテゴリは Systems Manager で更新することができません。アラームによって OpsItem が作成され、重複排除文字列を指定した場合、CloudWatch でアラームを編集しても、アラームは追加の OpsItems を作成しません。OpsItem が OpsCenter で解決された場合、CloudWatch は新しい OpsItem を作成します。

CloudWatch アラームの詳細については、次のトピックを参照してください。

トピック

- OpsItems (コンソール) を作成するように CloudWatch を設定する
- OpsItems を (プログラムで) 作成するように既存の CloudWatch アラームを設定する

OpsItems (コンソール) を作成するように CloudWatch を設定する

アラームを手動で作成するか、既存のアラームを更新して、OpsItems を Amazon CloudWatch から作成できます。

CloudWatch アラームを作成して、アラームのターゲットとして Systems Manager を設定するには

1. 「Amazon CloudWatch ユーザーガイド」の「静的しきい値に基づいて CloudWatch アラームを作成する」で指定されているように、ステップ 1 ~ 9 を完了します。
2. [Systems Manager] セクションで、[Systems Manager OpsCenter アクションの追加] をクリックします。
3. [OpsItems] をクリックします。
4. [重要度] は、1 ~ 4 の中から指定できます。
5. (オプション) [カテゴリ] に、OpsItem のカテゴリを選択します。
6. 「Amazon CloudWatch ユーザーガイド」「静的しきい値に基づいて CloudWatch アラームを作成する」で指定されているように、ステップ 11 ~ 13 を完了します。
7. [次] を選択し、ウィザードを完了します。

既存のアラームを編集し、アラームのターゲットとして Systems Manager を設定するには

1. CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) を開きます。
2. ナビゲーションペインで、[Alarms] を選択します。
3. アラームを選択してから、[アクション]、[編集] の順に選択します。
4. (オプション) [メトリクス] セクションと [条件] セクションの設定を変更し、[次] を選択します。

5. [Systems Manager] セクションで、[Add Systems Manager OpsCenter action (Systems Manager OpsCenter アクションの追加)]を選択します。
6. [重大度] で、数値を選択します。

> **Note**
>
> 重大度は、ユーザー定義の値です。各重要度値の意味、各重要度に関連するサービスレベルアグリーメントは、お客様または組織が決定します。

7. (オプション) [カテゴリ] で、オプションを選択します。
8. [次] を選択し、ウィザードを完了します。

OpsItems を (プログラムで) 作成するように既存の CloudWatch アラームを設定する

AWS Command Line Interface (AWS CLI)、AWS CloudFormation テンプレート、または Java コードスニペットを使用して、OpsItems をプログラムで作成するように Amazon CloudWatch アラームを設定できます。

トピック

- 始める前に
- OpsItems (AWS CLI) を作成するように CloudWatch アラームを設定する
- OpsItems (CloudFormation) を作成または更新するように CloudWatch アラームを設定する
- OpsItems (Java) を作成または更新するように CloudWatch アラームを設定する

始める前に

既存のアラームをプログラムで編集するか、OpsItems を作成する新しいアラームを作成する場合は、Amazon リソースネーム (ARN) を指定する必要があります。この ARN により、Systems Manager OpsCenter はアラームから作成された OpsItems のターゲットとして識別されます。アラームから作成された OpsItems に重大度やカテゴリなどの特定の情報が含まれるように、ARN をカスタマイズできます。各 ARN には、次の表に示す情報が含まれています。

Parameter	詳細
`Region` (必須)	アラームが存在する AWS リージョン。例: `us-west-2` 。OpsCenter を使用できる AWS リー

Parameter	詳細
	ジョン については、「AWS Systems Manager エンドポイントとクォータ」を参照照してください。
account_ID (必須)	アラームの作成に使用したのと同じ AWS アカウント ID。例: 123456789012 。以下の例に示すように、アカウント ID の後にはコロン (:) とパラメータ opsitem を指定する必要があります。
severity (必須)	アラームから作成された OpsItems のユーザー定義の重大度。有効な値: 1、2、3、4
Category (オプション)	アラームから作成された OpsItems のカテゴリ。有効な値: Availability 、Cost、Performance 、Recovery、および Security。

次の構文を使用して ARN を作成します。この ARN には、オプションの Category パラメータは含まれません。

```
arn:aws:ssm:Region:account_ID:opsitem:severity
```

次に例を示します。

```
arn:aws:ssm:us-west-2:123456789012:opsitem:3
```

オプションの Category パラメータを使用する ARN を作成するには、次の構文を使用します。

```
arn:aws:ssm:Region:account_ID:opsitem:severity#CATEGORY=category_name
```

次に例を示します。

```
arn:aws:ssm:us-west-2:123456789012:opsitem:3#CATEGORY=Security
```

OpsItems (AWS CLI) を作成するように CloudWatch アラームを設定する

このコマンドでは、alarm-actions パラメータの ARN を指定する必要があります。ARN を作成する方法については、「始める前に」を参照してください。

OpsItems (AWS CLI) を作成するように CloudWatch アラームを設定するには

1. まだ AWS Command Line Interface (AWS CLI) をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」を参照してください。

2. 次のコマンドを実行して、設定するアラームに関する情報を収集します。

```
aws cloudwatch describe-alarms --alarm-names "alarm name"
```

3. 次のコマンドを実行してアラームを更新します。各###############をユーザー自身の情報に置き換えます。

```
aws cloudwatch put-metric-alarm --alarm-name name \
--alarm-description "description" \
--metric-name name --namespace namespace \
--statistic statistic --period value --threshold value \
--comparison-operator value \
--dimensions "dimensions" --evaluation-periods value \
    --alarm-actions
 arn:aws:ssm:Region:account_ID:opsitem:severity#CATEGORY=category_name \
--unit unit
```

   以下に例を示します。

   Linux & macOS

```
aws cloudwatch put-metric-alarm --alarm-name cpu-mon \
--alarm-description "Alarm when CPU exceeds 70 percent" \
--metric-name CPUUtilization --namespace AWS/EC2 \
--statistic Average --period 300 --threshold 70 \
--comparison-operator GreaterThanThreshold \
--dimensions "Name=InstanceId,Value=i-12345678" --evaluation-periods 2 \
--alarm-actions arn:aws:ssm:us-east-1:123456789012:opsitem:3#CATEGORY=Security \
```

```
--unit Percent
```

Windows

```
aws cloudwatch put-metric-alarm --alarm-name cpu-mon ^
--alarm-description "Alarm when CPU exceeds 70 percent" ^
--metric-name CPUUtilization --namespace AWS/EC2 ^
--statistic Average --period 300 --threshold 70 ^
--comparison-operator GreaterThanThreshold ^
--dimensions "Name=InstanceId,Value=i-12345678" --evaluation-periods 2 ^
--alarm-actions arn:aws:ssm:us-east-1:123456789012:opsitem:3#CATEGORY=Security ^
--unit Percent
```

OpsItems (CloudFormation) を作成または更新するように CloudWatch アラームを設定する

このセクションでは、OpsItems を自動的に作成または更新するように CloudWatch アラームを設定する際に使用できる AWS CloudFormation テンプレートを紹介します。各テンプレートでは、`AlarmActions` パラメータの ARN を指定する必要があります。ARN を作成する方法については、「始める前に」を参照してください。

メトリクスアラーム – CloudWatch メトリクスアラームを作成または更新するには、以下の CloudFormation テンプレートを使用します。このテンプレートで指定されたアラームは、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのステータスチェックをモニタリングします。アラームが `ALARM` ステートになると、OpsCenter で OpsItem が作成されます。

```
   {
     "AWSTemplateFormatVersion": "2010-09-09",
     "Parameters" : {
       "RecoveryInstance" : {
         "Description" : "The EC2 instance ID to associate this alarm with.",
         "Type" : "AWS::EC2::Instance::Id"
       }
     },
     "Resources": {
       "RecoveryTestAlarm": {
         "Type": "AWS::CloudWatch::Alarm",
         "Properties": {
           "AlarmDescription": "Run a recovery action when instance status check fails
for 15 consecutive minutes.",
```

```
            "Namespace": "AWS/EC2" ,
            "MetricName": "StatusCheckFailed_System",
            "Statistic": "Minimum",
            "Period": "60",
            "EvaluationPeriods": "15",
            "ComparisonOperator": "GreaterThanThreshold",
            "Threshold": "0",
            "AlarmActions": [ {"Fn::Join" : ["",
["arn:arn:aws:ssm:Region:account_ID:opsitem:severity#CATEGORY=category_name",
{ "Ref" : "AWS::Partition" }, ":ssm:", { "Ref" : "AWS::Region" }, { "Ref" : "AWS::
AccountId" }, ":opsitem:3" ]]} ],
            "Dimensions": [{"Name": "InstanceId","Value": {"Ref": "RecoveryInstance"}}]
          }
        }
      }
    }
```

複合アラーム – 複合アラームを作成または更新するには、以下の CloudFormation テンプレートを使用します。複合アラームは、複数のメトリクスアラームで構成されます。アラームが ALARM ステートになると、OpsCenter で OpsItem が作成されます。

```
"Resources":{
       "HighResourceUsage":{
          "Type":"AWS::CloudWatch::CompositeAlarm",
          "Properties":{
             "AlarmName":"HighResourceUsage",
             "AlarmRule":"(ALARM(HighCPUUsage) OR ALARM(HighMemoryUsage)) AND NOT
 ALARM(DeploymentInProgress)",

 "AlarmActions":"arn:aws:ssm:Region:account_ID:opsitem:severity#CATEGORY=category_name",
             "AlarmDescription":"Indicates that the system resource usage is high while
 no known deployment is in progress"
          },
          "DependsOn":[
             "DeploymentInProgress",
             "HighCPUUsage",
             "HighMemoryUsage"
          ]
       },
       "DeploymentInProgress":{
          "Type":"AWS::CloudWatch::CompositeAlarm",
          "Properties":{
             "AlarmName":"DeploymentInProgress",
```

```
            "AlarmRule":"FALSE",
            "AlarmDescription":"Manually updated to TRUE/FALSE to disable other
alarms"
         }
      },
      "HighCPUUsage":{
         "Type":"AWS::CloudWatch::Alarm",
         "Properties":{
            "AlarmDescription":"CPUusageishigh",
            "AlarmName":"HighCPUUsage",
            "ComparisonOperator":"GreaterThanThreshold",
            "EvaluationPeriods":1,
            "MetricName":"CPUUsage",
            "Namespace":"CustomNamespace",
            "Period":60,
            "Statistic":"Average",
            "Threshold":70,
            "TreatMissingData":"notBreaching"
         }
      },
      "HighMemoryUsage":{
         "Type":"AWS::CloudWatch::Alarm",
         "Properties":{
            "AlarmDescription":"Memoryusageishigh",
            "AlarmName":"HighMemoryUsage",
            "ComparisonOperator":"GreaterThanThreshold",
            "EvaluationPeriods":1,
            "MetricName":"MemoryUsage",
            "Namespace":"CustomNamespace",
            "Period":60,
            "Statistic":"Average",
            "Threshold":65,
            "TreatMissingData":"breaching"
         }
      }
   }
```

OpsItems (Java) を作成または更新するように CloudWatch アラームを設定する

このセクションでは、OpsItems を自動的に作成または更新する CloudWatch アラームの設定に使用できる Java コードスニペットについて説明します。各スニペットでは、`validSsmActionStr` パラメータの ARN を指定する必要があります。ARN を作成する方法については、「始める前に」を参照してください。

特定のアラーム – 次の Java コードスニペットを使用して、CloudWatch アラームを作成または更新します。このテンプレートで指定されたアラームは、Amazon EC2 インスタンスのステータスチェックをモニタリングします。アラームが ALARM ステートになると、OpsCenter で OpsItem が作成されます。

```
import com.amazonaws.services.cloudwatch.AmazonCloudWatch;
    import com.amazonaws.services.cloudwatch.AmazonCloudWatchClientBuilder;
    import com.amazonaws.services.cloudwatch.model.ComparisonOperator;
    import com.amazonaws.services.cloudwatch.model.Dimension;
    import com.amazonaws.services.cloudwatch.model.PutMetricAlarmRequest;
    import com.amazonaws.services.cloudwatch.model.PutMetricAlarmResult;
    import com.amazonaws.services.cloudwatch.model.StandardUnit;
    import com.amazonaws.services.cloudwatch.model.Statistic;

    private void putMetricAlarmWithSsmAction() {
        final AmazonCloudWatch cw =
                AmazonCloudWatchClientBuilder.defaultClient();

        Dimension dimension = new Dimension()
                .withName("InstanceId")
                .withValue(instanceId);

        String validSsmActionStr =
 "arn:aws:ssm:Region:account_ID:opsitem:severity#CATEGORY=category_name";

        PutMetricAlarmRequest request = new PutMetricAlarmRequest()
                .withAlarmName(alarmName)
                .withComparisonOperator(
                        ComparisonOperator.GreaterThanThreshold)
                .withEvaluationPeriods(1)
                .withMetricName("CPUUtilization")
                .withNamespace("AWS/EC2")
                .withPeriod(60)
                .withStatistic(Statistic.Average)
                .withThreshold(70.0)
                .withActionsEnabled(false)
                .withAlarmDescription(
                        "Alarm when server CPU utilization exceeds 70%")
                .withUnit(StandardUnit.Seconds)
                .withDimensions(dimension)
                .withAlarmActions(validSsmActionStr);

        PutMetricAlarmResult response = cw.putMetricAlarm(request);
```

```
    }
```

すべてのアラームを更新する – 次の Java コードスニペットを使用して、アラームが ALARM 状態になったときに OpsItems を作成するように、AWS アカウント 内のすべての CloudWatch アラームを更新します。

```
import com.amazonaws.services.cloudwatch.AmazonCloudWatch;
    import com.amazonaws.services.cloudwatch.AmazonCloudWatchClientBuilder;
    import com.amazonaws.services.cloudwatch.model.DescribeAlarmsRequest;
    import com.amazonaws.services.cloudwatch.model.DescribeAlarmsResult;
    import com.amazonaws.services.cloudwatch.model.MetricAlarm;

    private void listMetricAlarmsAndAddSsmAction() {
        final AmazonCloudWatch cw = AmazonCloudWatchClientBuilder.defaultClient();

        boolean done = false;
        DescribeAlarmsRequest request = new DescribeAlarmsRequest();

        String validSsmActionStr =
 "arn:aws:ssm:Region:account_ID:opsitem:severity#CATEGORY=category_name";

        while(!done) {

            DescribeAlarmsResult response = cw.describeAlarms(request);

            for(MetricAlarm alarm : response.getMetricAlarms()) {
                // assuming there are no alarm actions added for the metric alarm
                alarm.setAlarmActions(ImmutableList.of(validSsmActionStr));
            }

            request.setNextToken(response.getNextToken());

            if(response.getNextToken() == null) {
                done = true;
            }
        }
    }
```

OpsItems を手動で作成する

オペレーション時の問題が見つかった場合は、AWS Systems Manager のツールである OpsCenter から OpsItem を手動で作成して、その問題を管理および解決することができます。

アカウント間管理のために OpsCenter を設定すると、Systems Manager の委任管理者または AWS Organizations の管理アカウントが、メンバーアカウントの OpsItems を作成することができます。詳細については、「(オプション) OpsCenter の手動設定により、複数のアカウント間で OpsItems を一元管理する」を参照してください。

OpsItems は、AWS Systems Manager コンソール、AWS Command Line Interface (AWS CLI)、または AWS Tools for Windows PowerShell を使用して作成できます。

トピック

- OpsItems の手動作成 (コンソール)
- OpsItems の手動作成 (AWS CLI)
- OpsItems を手動で作成する (PowerShell)

OpsItems の手動作成 (コンソール)

AWS Systems Manager コンソールを使用して OpsItems を手動で作成できます。OpsItem を作成すると、OpsCenter アカウントに表示されます。クロスアカウント管理のために OpsCenter を設定した場合、OpsCenter では委任管理者または管理アカウントに、選択したメンバーアカウントの OpsItems を作成するオプションが提供されます。詳細については、「(オプション) OpsCenter の手動設定により、複数のアカウント間で OpsItems を一元管理する」を参照してください。

AWS Systems Manager コンソールを使用して OpsItem を作成するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[OpsCenter] を選択します。
3. [作成]OpsItem を選択します。このボタンが表示されない場合は、[OpsItems] タブを選択してから [OpsItem の作成] を選択します。
4. (オプション) [その他のアカウント] を選択し、OpsItem を作成するアカウントを選択します。

   > **Note**
   >
   > このステップは、メンバーアカウントの OpsItems を作成する場合に必要です。

5. [タイトル] に、OpsItem の目的を示すわかりやすい名前を入力します。
6. [Source] (ソース) に、影響を受ける AWS リソースのタイプなど、ソースの情報を指定して、ユーザーが OpsItem のオリジンをわかるようにします。

> **Note**
>
> OpsItem の作成後に [ソース] フィールドを編集することはできません。

7. (オプション) [優先度] で、優先度レベルを選択します。
8. (オプション) [重大度] で、重大度レベルを選択します。
9. (オプション) [カテゴリ] で、カテゴリを選択します。
10. [説明] に、問題を再現するための手順など、この OpsItem に関する情報 (該当する場合) を入力します。

> **Note**
>
> コンソールは OpsItem 説明フィールドのほとんどの Markdown フォーマットをサポートしています。詳細については、「AWS Management Console 入門ガイド」の「コンソールでの Markdown の使用」を参照してください。

11. [重複排除文字列] に、システムが重複する OpsItems をチェックするために使用できる単語を入力します。重複排除文字列の詳細については、「OpsItems の重複を管理する」を参照してください。
12. (オプション) [通知] で、OpsItem の更新時に通知を送信する Amazon SNS トピックの Amazon リソースネーム (ARN) を指定します。OpsItem と同じ AWS リージョン にある Amazon SNS ARN を指定する必要があります。
13. (オプション) [関連リソース] で、[追加] を選択して、影響を受けるリソースおよび関連リソースの ID または ARN を指定します。
14. [作成]OpsItem を選択します。

成功すると、ページに OpsItem が表示されます。委任された管理者または管理アカウントが、選択したメンバーアカウントの OpsItem を作成すると、新しい OpsItems が管理者アカウントとメンバーアカウントの OpsCenter に表示されます。OpsItem でオプションを設定する方法については、「OpsItems を管理する」を参照してください。

OpsItems の手動作成 (AWS CLI)

次の手順では、AWS Command Line Interface (AWS CLI) を使用して OpsItem を作成する方法について説明します。

AWS CLI を使用して OpsItem を作成するには

1. まだ AWS Command Line Interface (AWS CLI) をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」を参照してください。

2. AWS CLI を開き、以下のコマンドを実行して OpsItem を作成します。各##############をユーザー自身の情報に置き換えます。

```
aws ssm create-ops-item \
    --title "Descriptive_title" \
    --description "Information_about_the_issue" \
    --priority Number_between_1_and_5 \
    --source Source_of_the_issue \
    --operational-data Up_to_20_KB_of_data_or_path_to_JSON_file \
    --notifications Arn="SNS_ARN_in_same_Region" \
    --tags "Key=key_name,Value=a_value"
```

   ファイルから運用データを指定する

   OpsItem を作成する場合、ファイルから運用データを指定することができます。ファイルは JSON ファイルで、ファイルの内容には、次の形式を使用する必要があります。

```
{
  "key_name": {
    "Type": "SearchableString",
    "Value": "Up to 20 KB of data"
  }
}
```

   以下はその例です。

```
aws ssm create-ops-item ^
    --title "EC2 instance disk full" ^
    --description "Log clean up may have failed which caused the disk to be full" ^
    --priority 2 ^
    --source ec2 ^
    --operational-data file:///Users/TestUser1/Desktop/OpsItems/opsData.json ^
    --notifications Arn="arn:aws:sns:us-west-1:12345678:TestUser1" ^
```

```
    --tags "Key=EC2,Value=Production"
```

> **Note**
>
> さまざまなローカルオペレーティングシステムでコマンドラインに JSON 形式のパラメータを入力する方法については、AWS Command Line Interface ユーザーガイドの「AWS CLI で文字列に引用符を使用する」を参照してください。

システムが以下のような情報をレスポンスします。

```
{
    "OpsItemId": "oi-1a2b3c4d5e6f"
}
```

3. 以下のコマンドを実行して、作成した OpsItem の詳細を表示します。

```
aws ssm get-ops-item --ops-item-id ID
```

システムが以下のような情報をレスポンスします。

```
{
    "OpsItem": {
        "CreatedBy": "arn:aws:iam::12345678:user/TestUser",
        "CreatedTime": 1558386334.995,
        "Description": "Log clean up may have failed which caused the disk to be
 full",
        "LastModifiedBy": "arn:aws:iam::12345678:user/TestUser",
        "LastModifiedTime": 1558386334.995,
        "Notifications": [
            {
                "Arn": "arn:aws:sns:us-west-1:12345678:TestUser"
            }
        ],
        "Priority": 2,
        "RelatedOpsItems": [],
        "Status": "Open",
        "OpsItemId": "oi-1a2b3c4d5e6f",
        "Title": "EC2 instance disk full",
        "Source": "ec2",
        "OperationalData": {
```

```
            "EC2": {
                "Value": "12345",
                "Type": "SearchableString"
            }
        }
    }
}
```

4. 次のコマンドを実行して OpsItem を更新します。このコマンドでは、ステータスを Open (デフォルト) から InProgress に変更します。

```
aws ssm update-ops-item --ops-item-id ID --status InProgress
```

コマンドには出力がありません。

5. 次のコマンドを再度実行し、ステータスが InProgress に変更されていることを確認します。

```
aws ssm get-ops-item --ops-item-id ID
```

OpsItem の作成例

次のコード例は、Linux 管理ポータルmacOS、または Windows を使用して OpsItem を作成する方法を示します。

Linux 管理ポータル、または macOS

次のコマンドは、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスディスクがいっぱいになったときに OpsItem を作成します。

```
aws ssm create-ops-item \
    --title "EC2 instance disk full" \
    --description "Log clean up may have failed which caused the disk to be full" \
    --priority 2 \
    --source ec2 \
    --operational-data '{"EC2":{"Value":"12345","Type":"SearchableString"}}' \
    --notifications Arn="arn:aws:sns:us-west-1:12345678:TestUser1" \
    --tags "Key=EC2,Value=ProductionServers"
```

次のコマンドは、OperationalData の /aws/resources キーを使用して、Amazon DynamoDB 関連リソースを持つ OpsItem を作成します。

```
aws ssm create-ops-item \
    --title "EC2 instance disk full" \
    --description "Log clean up may have failed which caused the disk to be full" \
    --priority 2 \
    --source ec2 \
    --operational-data '{"/aws/resources":{"Value":"[{\"arn\": \"arn:aws:dynamodb:us-
west-2:12345678:table/OpsItems\"}]","Type":"SearchableString"}}' \
    --notifications Arn="arn:aws:sns:us-west-2:12345678:TestUser"
```

以下のコマンドは、OperationalData の /aws/automations キーを使用して、関連付けられた Automation ランブックとして AWS-ASGEnterStandby ドキュメントを指定する OpsItem を作成します。

```
aws ssm create-ops-item \
    --title "EC2 instance disk full" \
    --description "Log clean up may have failed which caused the disk to be full" \
    --priority 2 \
    --source ec2 \
    --operational-data '{"/aws/automations":{"Value":"[{\"automationId
\": \"AWS-ASGEnterStandby\", \"automationType\": \"AWS::SSM::Automation
\"}]","Type":"SearchableString"}}' \
    --notifications Arn="arn:aws:sns:us-west-2:12345678:TestUser"
```

Windows

次のコマンドは、Amazon Relational Database Service (Amazon RDS) インスタンスが応答しない場合に OpsItem を作成します。

```
aws ssm create-ops-item ^
    --title "RDS instance not responding" ^
    --description "RDS instance not responding to ping" ^
    --priority 1 ^
    --source RDS ^
    --operational-data={\"RDS\":{\"Value\":\"abcd\",\"Type\":\"SearchableString\"}} ^
    --notifications Arn="arn:aws:sns:us-west-1:12345678:TestUser1" ^
    --tags "Key=RDS,Value=ProductionServers"
```

以下のコマンドは、OperationalData の /aws/resources キーを使用して、Amazon EC2 インスタンスの関連リソースを持つ OpsItem を作成します。

```
aws ssm create-ops-item ^
```

```
    --title "EC2 instance disk full" ^
    --description "Log clean up may have failed which caused the disk to be full" ^
    --priority 2 ^
    --source ec2 ^
    --operational-data={\"/aws/resources\":{\"Value\":\"[{\\\"""arn\\\""":\
\"""arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0\\\"""}]\",\"Type\":
\"SearchableString\"}}
```

次のコマンドは、OperationalData の /aws/automations キーを使用して、関連付けられた Automation ランブックとして AWS-RestartEC2Instance ランブックを指定する OpsItem を作成します。

```
aws ssm create-ops-item ^
    --title "EC2 instance disk full" ^
    --description "Log clean up may have failed which caused the disk to be full" ^
    --priority 2 ^
    --source ec2 ^
    --operational-data={\"/aws/automations\":{\"Value\":\"[{\\\"""automationId\\\""":
\\\"""AWS-RestartEC2Instance\\”"",\\\"""automationType\\\""":\\\"""AWS::SSM::Automation\
\\"""}]\",\"Type\":\"SearchableString\"}}
```

OpsItems を手動で作成する (PowerShell)

次の手順では、(AWS Tools for Windows PowerShell) を使用して OpsItem を作成する方法について説明します。

AWS Tools for Windows PowerShell を使用して OpsItem を作成するには

1. AWS Tools for Windows PowerShell を開き、次のコマンドを実行して認証情報を指定します。

   ```
   Set-AWSCredentials -AccessKey key-name -SecretKey key-name
   ```

2. 次のコマンドを実行して、PowerShell セッションの AWS リージョン を設定します。

   ```
   Set-DefaultAWSRegion -Region Region
   ```

3. 次のコマンドを実行して、新しい OpsItem を作成します。各##############をユーザー自身の情報に置き換えます。このコマンドは、OpsItem を修復するために Systems Manager Automation ランブックを指定します。

   ```
   $opsItem = New-Object Amazon.SimpleSystemsManagement.Model.OpsItemDataValue
   ```

```
$opsItem.Type = [Amazon.SimpleSystemsManagement.OpsItemDataType]::SearchableString
$opsItem.Value = '[{\"automationId\":\"runbook_name\",\"automationType\":
\"AWS::SSM::Automation\"}]'
$newHash = @{" /aws/
automations"=[Amazon.SimpleSystemsManagement.Model.OpsItemDataValue]$opsItem}

New-SSMOpsItem `
    -Title "title" `
    -Description "description" `
    -Priority priority_number `
    -Source AWS_service `
    -OperationalData $newHash
```

成功すると、コマンドは、新しい OpsItem の ID を出力します。

次の例では、障害が発生した Amazon Elastic Compute Cloud (Amazon EC2) インスタンスの Amazon リソースネーム (ARN) を指定しています。

```
$opsItem = New-Object Amazon.SimpleSystemsManagement.Model.OpsItemDataValue
$opsItem.Type = [Amazon.SimpleSystemsManagement.OpsItemDataType]::SearchableString
$opsItem.Value = '[{\"arn\":\"arn:aws:ec2:us-east-1:123456789012:instance/
i-1234567890abcdef0\"}]'
$newHash = @{" /aws/
resources"=[Amazon.SimpleSystemsManagement.Model.OpsItemDataValue]$opsItem}
New-SSMOpsItem -Title "EC2 instance disk full still" -Description "Log clean up may
 have failed which caused the disk to be full" -Priority 2 -Source ec2 -OperationalData
 $newHash
```

OpsItems を管理する

AWS Systems Manager のツールである OpsCenter は、OpsItems の作成から解決までを追跡します。クロスアカウント管理のために OpsCenter を設定すると、委任管理者または管理アカウントが自分のアカウントから OpsItems を管理できます。詳細については、「(オプション) OpsCenter の手動設定により、複数のアカウント間で OpsItems を一元管理する」を参照してください。

Systems Manager コンソールの次のページを使用して OpsItems を表示および管理できます。

- 概要 — 未解決かつ進行中の OpsItems の数、ソース別、経過時間別の OpsItems の数、運用上のインサイトが表示されます。ソース別および OpsItems のステータス別に OpsItems をフィルターできます。

- OpsItems — タイトル、ID、優先度、説明、OpsItem のソース、最終更新日時など、複数のフィールドの情報が含まれる OpsItems のリストを表示します。このページを使用して、OpsItems の手動作成、ソースの設定、OpsItem のステータスの変更、新しいインシデントによる OpsItems のフィルタリングを行うことができます。OpsItem をクリックして、[OpsItems の詳細] ページを表示できます。

- OpsItem の詳細 — OpsItem の管理に使用できる詳細なインサイトとツールを提供します。OpsItems の詳細ページには、次のタブが表示されます。
  - [概要] — 関連リソース、過去 30 日間に実行されたランブック、実行可能なランブックのリストが表示されます。同様の OpsItems の情報を表示したり、運用データを追加したり、関連する OpsItems のデータを追加したりすることもできます。
  - [関連リソースの詳細] - AWS のいくつかのサービスから提供されるリソースに関する情報が表示されます。ホスト元の AWS のサービスから提供されるこのリソースに関する情報を表示するには、[リソースの詳細] のセクションを展開します。[関連リソース] リストを使用して、この OpsItem に関連付けられている他の関連リソース間を切り替えることもできます。

OpsItems の管理方法については、次のトピックを参照してください。

トピック

- OpsItem の詳細を表示する
- OpsItem の編集
- 関連リソースを OpsItem に追加する
- 関連する OpsItems を OpsItem に追加する
- 運用データを OpsItem に追加する
- OpsItem のインシデントを作成する
- OpsItems の重複を管理する
- OpsItems を減らすために運用上のインサイトを分析する
- OpsCenter ログとレポートを表示する

OpsItem の詳細を表示する

OpsItem の包括的なビューを表示するには、OpsCenter コンソールの [OpsItem の詳細] ページを使用します。[概要] ページには、次の情報が表示されます。

- OpsItems の詳細 — 選択した OpsItem の一般情報を表示します。
- 関連リソース - 関連リソースは、影響を受けるリソース、またはイベントを開始して OpsItem を作成したリソースです。
- 過去 30 日間の自動化の実行 — 過去 30 日間に実行されたランブックのリスト。
- ランブック — 利用可能なランブックのリストからランブックを選択できます。
- 類似する OpsItems - ユーザーに関連している、または関心のある OpsItems のリスト。リストを生成するために、システムはすべての OpsItems のタイトルと説明をスキャンし、同様の用語を使用している OpsItems を返します。
- 運用データ – OpsItem に関する有用なリファレンスの詳細を提供するカスタムデータ。例えば、ログファイル、エラー文字列、ライセンスキー、トラブルシューティングのヒント、その他の関連データを指定することができます。
- 関連する OpsItems - 現在の OpsItem 何らかの関係がある OpsItems の ID を指定できます。
- 関連リソースの詳細 - Amazon CloudWatch メトリクスとアラーム、AWS CloudTrail ログ、AWS Config の詳細などを含む、データプロバイダーを表示します。

OpsItem の詳細を表示するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[OpsCenter] を選択します。
3. OpsItem を選択して、詳細を表示します。

OpsItem の編集

[OpsItem の詳細] セクションには、OpsItem に関する情報 (説明、タイトル、ソース、OpsItem ID、ステータスなど) が含まれています。
OpsItem を個別に編集するか、複数のOpsItems を選択して、[ステータス]、[優先度]、[重要度]、[カテゴリ] フィールドを編集できます。

Amazon EventBridge が OpsItem を作成すると、[タイトル]、[ソース]、[説明] の各フィールドにデータが入力されます。[タイトル] および [説明] フィールドは編集できますが、[ソース] フィールドは編集できません。

> **Note**
>
> コンソールは OpsItem 説明フィールドのほとんどの Markdown フォーマットをサポートしています。詳細については、「AWS Management Console 入門ガイド」の「コンソールでの Markdown の使用」を参照してください。

通常は、以下の OpsItem の設定可能なデータを編集することができます。

- タイトル — OpsItem の名前。ソースが OpsItem のタイトルを作成します。
- 説明 - 問題を再現するための手順など、この OpsItem に関する情報。
- ステータス – OpsItem のステータス。有効なステータスの値のリストについては、「AWS Systems Manager API リファレンス」の「OpsItem のステータス」を参照してください。
- 優先度 — OpsItem の優先度は 1 ~ 5 の範囲で指定できます。各優先度の意味と、各レベルに対応するサービスレベルアグリーメントは組織で決定することをお勧めします。
- 重要度 — OpsItem の重要度は 1 ~ 4 の範囲で指定します。1 は「重大」、2 は「高い」、3 は「中程度」、4 は「低い」です。
- カテゴリ — OpsItem のカテゴリには、可用性、コスト、パフォーマンス、リカバリ、セキュリティなどがあります。
- 通知 — OpsItem の編集時に [通知] フィールドで、Amazon Simple Notification Service (SNS) トピックの Amazon リソースネーム (ARN) を指定できます。ARN を指定することで、OpsItem が編集されると、ステータス変更を含むすべての関係者に通知が送信されるようにします。詳細については、「Amazon Simple Notification Service デベロッパーガイド」を参照してください。

> **Important**
>
> Amazon SNS トピックは、OpsItem と同じ AWS リージョン にある必要があります。トピックと OpsItem のリージョンが異なる場合は、システムはエラーを返します。

OpsCenter は AWS Security Hub と双方向に統合しています。セキュリティ結果に関連する OpsItem ステータスと重要度を更新すると、変更内容が自動的に Security Hub に送信され、常に最新で正しい情報が表示されます。

Security Hub 検出結果から OpsItem を作成すると、Security Hub メタデータが OpsItem の運用データフィールドに自動的に追加されます。このメタデータが削除されると、双方向更新は機能しなくなります。

OpsItem の詳細を編集するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[OpsCenter] を選択します。
3. OpsItem ID を選択して、詳細ページを開くか、複数の OpsItems を選択します。複数の OpsItems 選択した場合、ステータス、優先度、重大度、またはカテゴリのみを編集できます。複数の OpsItems を編集する場合、OpsCenter は新しいステータス、優先度、重大度、またはカテゴリを選択すると、すぐに変更内容を更新、保存します。
4. [OpsItem の詳細] セクションで、[編集] を選択します。
5. 組織で指定された要件やガイドラインに応じて、OpsItem の詳細を編集します。
6. 完了したら、[保存] を選択します。

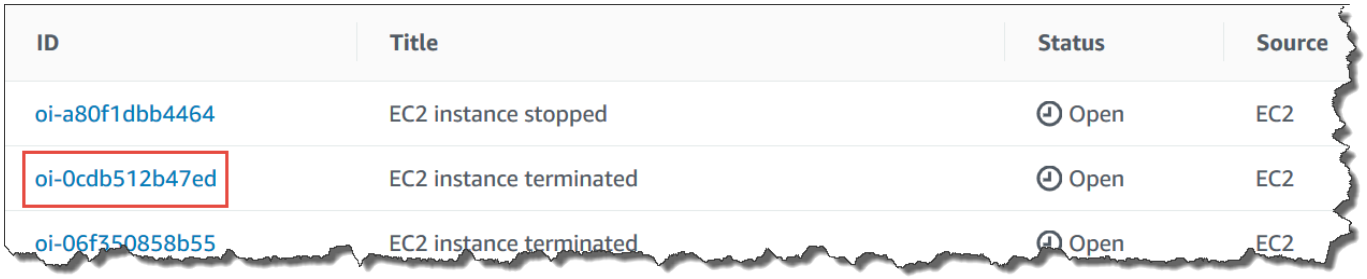
関連リソースを OpsItem に追加する

各 OpsItem には、[関連リソース] セクションが含まれ、関連リソースの Amazon リソースネーム (ARN) の一覧が表示されます。[関連リソース] とは、調査行う必要がある影響を受けた AWS リソースです。

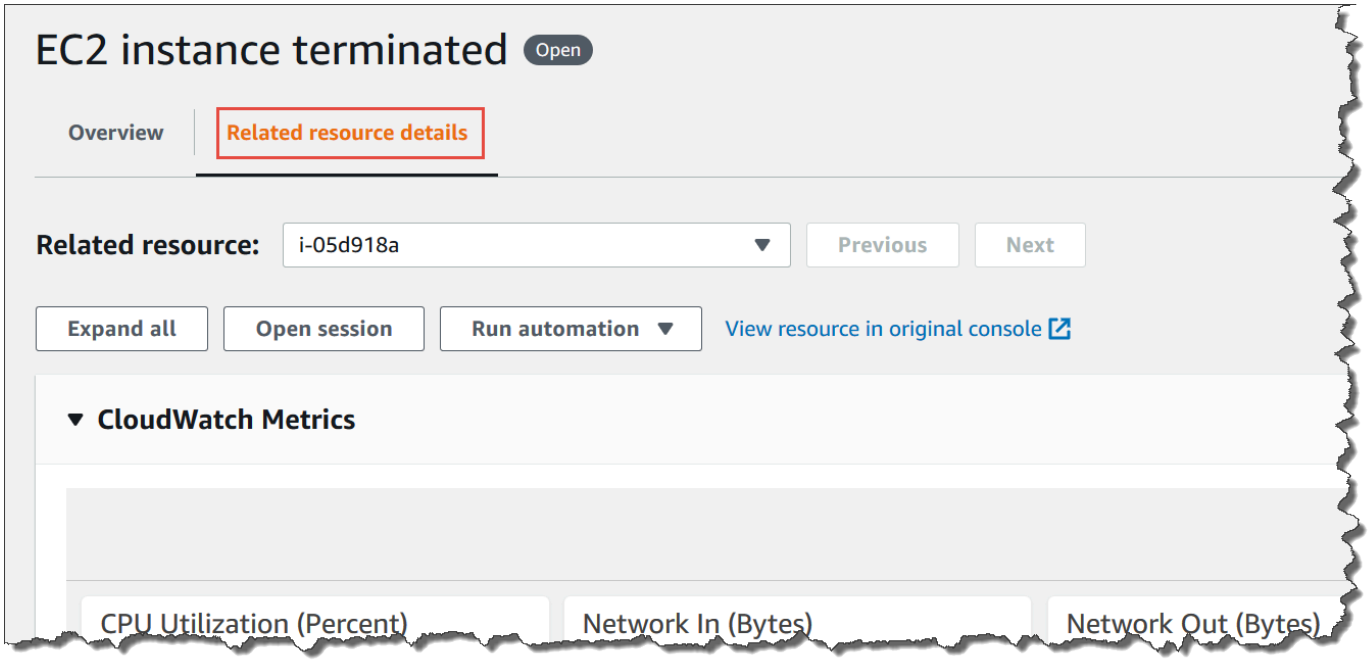
Amazon EventBridge が OpsItem を作成すると、システムは自動的にリソースの ARN を OpsItem に入力します。また、関連リソースの ARN を手動で指定することもできます。特定の ARN タイプでは、OpsCenter が、リソースに関する詳細を表示するディープリンクを OpsCenter コンソールに自動的に作成します。例えば、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスの ARN を指定すると、OpsCenter がその EC2 インスタンスに関する詳細を取得できます。これにより、影響を受ける AWS リソースに感する詳細な情報を表示することができます。OpsCenter を離れる必要はありません。

関連リソースを表示して OpsItem に追加するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[OpsCenter] を選択します。
3. [OpsItems] タブを選択します。
4. OpsItem ID を選択します。



5. 影響を受けるリソースに関する情報を表示するには、[関連リソースの詳細] タブを選択します。



このタブには、いくつかの AWS のサービスから提供されるリソースに関する情報が表示されます。ホスト元の AWS のサービスから提供されるこのリソースに関する情報を表示するには、[Resource details] (リソースの詳細) のセクションを展開します。[関連リソース] リストを使用して、この OpsItem に関連付けられている他の関連リソース間を切り替えることもできます。

6. その他の関連リソースを追加するには、[概要] タブを選択します。
7. [関連リソース] セクションで、[追加] を選択します。
8. [リソースタイプ] で、リストからリソースを選択します。
9. [リソース ID] に、ID または Amazon リソースネーム (ARN) を入力します。選択する情報のタイプは、前のステップで選択したリソースによって異なります。

> **Note**
>
> その他の関連リソースの ARN は手動で追加することができます。各 OpsItem セクションには、最大 100 個の関連リソースの ARN を表示できます。

次の表は、関連するリソースへのディープリンクを自動的に作成するリソースタイプの一覧です。

サポートされているリソースタイプ

リソース名	ARN 形式
AWS Certificate Manager 証明書	`arn:aws:acm: region:account-id :certificate/ certificate-id`
Amazon EC2 Auto Scaling グループ	`arn:aws:autoscaling: region:account-id :autoScalingGroup: groupid:autoScalingGroupName/ groupfriendlyname`
Amazon CloudFront ディストリビューション	`arn:aws:cloudfront:: account-id :*`
AWS CloudFormation スタック	`arn:aws:cloudformation: region:account-id :stack/stackname /additionalidentifier`
Amazon CloudWatch アラーム	`arn:aws:cloudwatch: region:account-id :alarm:alarm-name`
AWS CloudTrail 証跡	`arn:aws:cloudtrail: region:account-id :trail/trailname`
AWS CodeBuild プロジェクト	`arn:aws:codebuild: region:account-id :resourcetype /resource`

リソース名	ARN 形式
AWS CodePipeline	`arn:aws:codepipeline:  region:account-id :resource-specifier`
Amazon DevOps Guru のインサイト	`arn:aws:devops-guru:  region:account-id :insight/ proactive or reactive/resource-id`
Amazon DynamoDB テーブル	`arn:aws:dynamodb: region:account-id :table/tablename`
Amazon Elastic Compute Cloud (Amazon EC2) カスタマーゲートウェイ	`arn:aws:ec2: region:account-id :customer-gateway/  cgw-id`
Amazon EC2 elastic IP	`arn:aws:ec2: region:account-id :eip/eipalloc-id`
Amazon EC2 Dedicated Host	`arn:aws:ec2: region:account-id :dedicated-host/ host-id`
Amazon EC2 インスタンス	`arn:aws:ec2: region:account-id :instance/ instance-id`
Amazon EC2 インターネットゲートウェイ	`arn:aws:ec2: region:account-id :internet-gateway/  igw-id`
Amazon EC2 ネットワークアクセスコントロールリスト (ネットワーク ACL)	`arn:aws:ec2: region:account-id :network-acl/ nacl-id`
Amazon EC2 ネットワークインターフェイス	`arn:aws:ec2: region:account-id :network-interface/  eni-id`

リソース名	ARN 形式
Amazon EC2 ルートテーブル	`arn:aws:ec2: region:account-id :route-table/ route-table-id`
Amazon EC2 セキュリティグループ	`arn:aws:ec2: region:account-id :security-group/ security-group-id`
Amazon EC2 サブネット	`arn:aws:ec2: region:account-id :subnet/subnet-id`
Amazon EC2 ボリューム	`arn:aws:ec2: region:account-id :volume/volume-id`
Amazon EC2 VPC	`arn:aws:ec2: region:account-id :vpc/vpc-id`
Amazon EC2 VPN 接続	`arn:aws:ec2: region:account-id :vpn-connection/ vpn-id`
Amazon EC2 VPN ゲートウェイ	`arn:aws:ec2: region:account-id :vpn-gateway/ vgw-id`
AWS Elastic Beanstalk アプリケーション	`arn:aws:elasticbeanstalk: region:account-id :application/ applicationname`
Elastic Load Balancing (Classic Load Balancer)	`arn:aws:elasticloadbalancing: region:account-id :loadbalancer/ name`

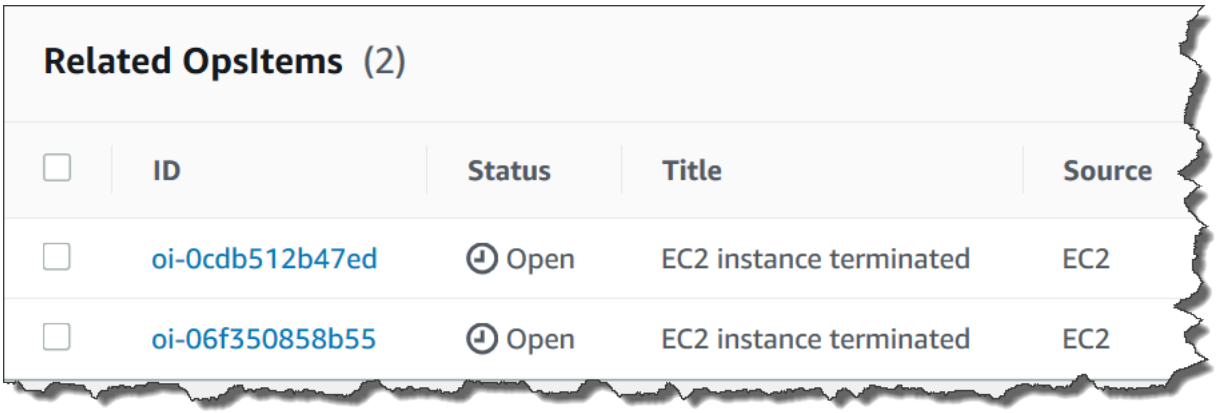
リソース名	ARN 形式
Elastic Load Balancing (Application Load Balancer)	`arn:aws:elasticloadbalancing: region:account-id :loadbalancer/app/ load-balancer-name /load-balancer-id`
Elastic Load Balancing (Network Load Balancer)	`arn:aws:elasticloadbalancing: region:account-id :loadbalancer/net/ load-balancer-name /load-balancer-id`
AWS Identity and Access Management (IAM) グループ	`arn:aws:iam:: account-id :group/group-name`
IAM ポリシー	`arn:aws:iam:: account-id :policy/policy-name`
IAM ロール	`arn:aws:iam:: account-id :role/role-name`
IAM ユーザー	`arn:aws:iam:: account-id :user/user-name`
AWS Lambda 関数	`arn:aws:lambda: region:account-id :function: function-name`
Amazon Relational Database Service (Amazon RDS) クラスター	`arn:aws:rds: region:account-id :cluster: db-cluster-name`
Amazon RDS データベースインスタンス	`arn:aws:rds: region:account-id :db:db-instance-name`

リソース名	ARN 形式
Amazon RDS サブスクリプション	`arn:aws:rds: region:account-id :es:subscription-name`
Amazon RDS セキュリティグループ	`arn:aws:rds: region:account-id :secgrp:security-group-name`
Amazon RDS クラスターのスナップショット	`arn:aws:rds: region:account-id :cluster-snapshot: cluster-snapshot-name`
Amazon RDS サブネットグループ	`arn:aws:rds: region:account-id :subgrp:subnet-group-name`
Amazon Redshift クラスター	`arn:aws:redshift: region:account-id :cluster: cluster-name`
Amazon Redshift パラメータグループ	`arn:aws:redshift: region:account-id :parametergroup: parameter-group-name`
Amazon Redshift セキュリティグループ	`arn:aws:redshift: region:account-id :securitygroup: security-group-name`
Amazon Redshift クラスターのスナップショット	`arn:aws:redshift: region:account-id :snapshot: cluster-name /snapshot-name`
Amazon Redshift サブネットグループ	`arn:aws:redshift: region:account-id :subnetgroup: subnet-group-name`
Amazon Simple Storage Service (Amazon S3) バケット	`arn:aws:s3::: bucket_name`

リソース名	ARN 形式
AWS Systems Manager マネージドノードのインベントリの AWS Config の記録	`arn:aws:ssm:region:account-id:managed-instance-inventory/node_id`
Systems Manager State Manager の関連付け	`arn:aws:ssm:region:account-id:association/association_ID`

関連する OpsItems を OpsItem に追加する

[OpsItems 詳細] ページの [関連する OpsItems] を使用すると、運用上の問題を調査し、問題の背景情報を取得できます。OpsItems は、OpsItems 間の親子関係、根本原因、または重複など、さまざまな方法で関連付けることができます。ある OpsItem を他の OpsItems と関連付けて、[関連する OpsItem] セクションに表示することができます。現在の OpsItem に関連する他の OpsItems の ID は、最大 10 個まで指定できます。

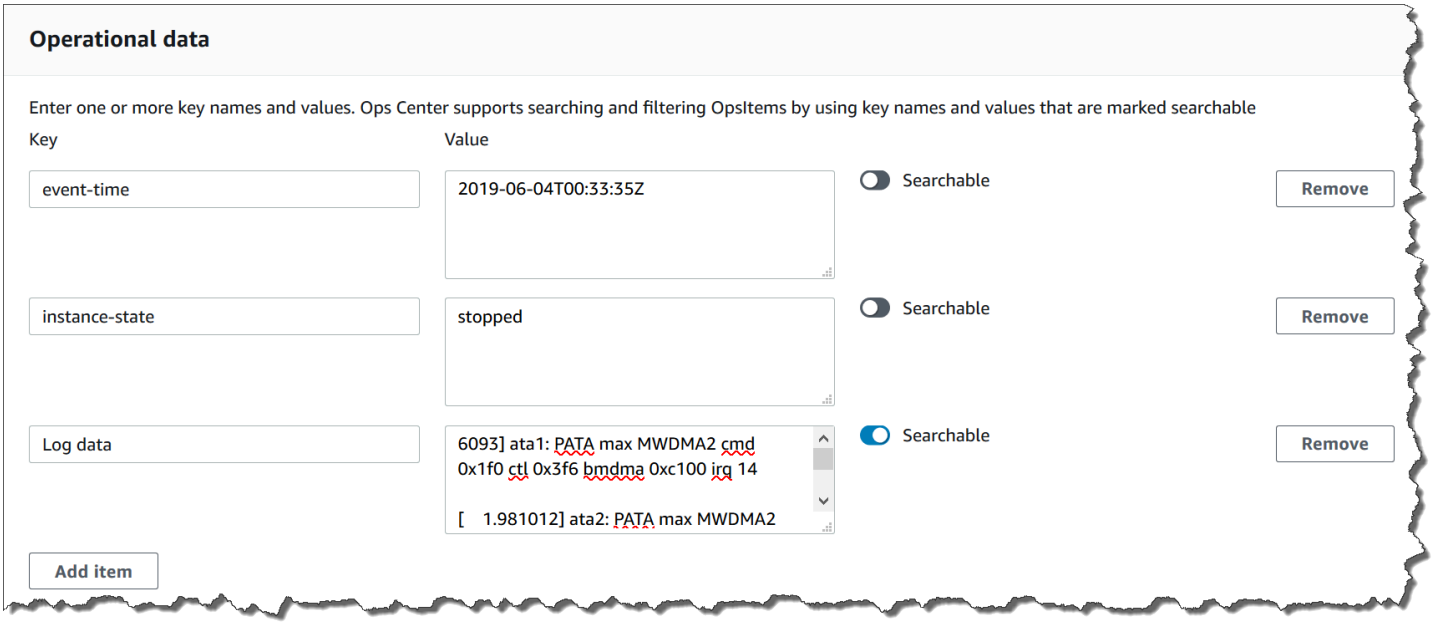


関連のある OpsItem を追加するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[OpsCenter] を選択します。
3. OpsItem ID を選択して、詳細ページを開きます。
4. [関連 OpsItem] セクションで、[追加] を選択します。
5. [OpsItem ID] で、ID を指定します。
6. [追加] を選択します。

運用データを OpsItem に追加する

運用データは、OpsItem に関する有用なリファレンスの詳細を提供するカスタムデータです。運用データの複数のキーと値のペアを入力できます。例えば、ログファイル、エラー文字列、ライセンスキー、トラブルシューティングのヒント、その他の関連データを指定することができます。キーの最大長は 128 文字、値の最大サイズは 20 KB になる可能性があります。



アカウント内の他のユーザーがデータを検索できるようにしたり、検索アクセスを制限したりすることもできます。検索可能なデータとは、OpsItem の [概要] ページ (Describe OpsItems API オペレーションによって提供) にアクセスできるすべてのユーザーが特定のデータを表示および検索できるということです。検索可能でない運用データは、OpsItem (GetOpsItem API オペレーションによって提供) にアクセスできるユーザーが表示のみできます。

運用データを OpsItem に追加するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[OpsCenter] を選択します。
3. OpsItem ID を選択して、詳細ページを開きます。
4. [運用データ] を展開します。
5. 運用データが OpsItem に存在しない場合は、[追加] をクリックします。運用データが OpsItem に既に存在する場合は、[管理] を選択します。

運用データを作成したら、[管理] を選択して、キーと値の編集、運用データの削除、その他キーと値のペアの追加を行うことができます。

6. [キー] で、データの目的を示すわかりやすい用語を指定します。

> **Important**
>
> オペレーションデータキーは、amazon、aws、amzn、ssm、/amazon、/aws、/amzn、/ssm で始まることはできません。

7. [値] で、データを指定します。
8. [Save] を選択します。

> **Note**
>
> OpsItems ページで [Operational data (運用データ)] 演算子を使用して OpsItems をフィルタ処理できます。[検索] ボックスで、[運用データ] をクリックし、キーと値のペアを JSON で入力します。次の形式を使用してキーと値のペアを入力する必要があります。`{"key":"key_name","value":"a_value"}`

OpsItem のインシデントを作成する

以下の手順で、OpsItem のインシデントを手動で作成して、AWS Systems Manager のツールである AWS Systems Manager Incident Manager でインシデントの追跡と管理を行います。インシデントとは、サービスの品質の計画外の中断または低下です。インシデントマネージャーの詳細については、「the section called “OpsCenter と他の AWS のサービス との統合”」を参照してください。

OpsItem のインシデントを手動で作成するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[OpsCenter] を選択します。
3. Incident Manager が OpsItem を作成した場合は、それを選択してステップ 5 に進みます。そうでない場合は、[OpsItem の作成] を選択し、フォームに記入します。このボタンが表示されない場合は、[OpsItems] タブを選択してから [OpsItem の作成)] を選択します。
4. 新しい OpsItem を作成した場合は、それを開きます。

5. [インシデントの開始] を選択します。
6. [対応プラン] で、このインシデントに割り当てるインシデントマネージャーの対応プランを選択します。
7. (オプション) [タイトル] に、他のチームメンバーがインシデントの性質を理解するのに役立つわかりやすい名前を入力します。新しいタイトルを入力しない場合、OpsCenter は対応プランのタイトルを使用して、Incident Manager に OpsItem と対応するインシデントを作成します。
8. (オプション) [インシデントの影響] では、このインシデントの影響レベルを選択します。影響レベルを選択しない場合、OpsCenter は、対応プランの影響レベルを使用して、Incident Manager で OpsItem および対応するインシデントを作成します。
9. [開始] を選択します。

OpsItems の重複を管理する

OpsCenter は、1 つのソースに対して複数の AWS のサービス から複数の重複する OpsItems を受け取ることができます。OpsCenter は、組み込みロジックと設定可能な重複排除文字列の組み合わせを使用して、重複する OpsItems を作成しないようにします。AWS Systems Manager は、CreateOpsItem API オペレーションが呼び出されると、重複排除の組み込みロジックを適用します。

AWS Systems Manager は、次の重複排除ロジックを使用します。

1. OpsItem を作成するとき、Systems Manager は重複排除文字列と OpsItem を開始したリソースに基づいてハッシュを作成して保存します。
2. OpsItem を作成するリクエストを受け取ると、システムは新しいリクエストの重複排除文字列をチェックします。
3. この重複排除文字列に一致するハッシュが存在する場合、Systems Manager は既存の OpsItem をチェックします。既存の OpsItem のステータスが未解決または進行中の場合、OpsItem は作成されません。既存の OpsItem が解決されると、Systems Manager は新しい OpsItem を作成します。

OpsItem を作成した後、その OpsItem で重複排除文字列を編集または変更することはできません。

OpsItems の重複を管理するには、次の操作を行います。

- OpsCenter をターゲットにする Amazon EventBridge ルールの重複排除文字列を編集します。詳細については、「デフォルトの EventBridge ルールの重複排除文字列を編集する」を参照してください。

- OpsItem を手動で作成するときに、重複排除文字列を指定します。詳細については、「AWS CLI を使用して重複排除文字列を指定する」を参照してください。
- 運用インサイトを使用して、重複する OpsItems を確認して解決します。重複する OpsItems は、ランブックを使用して解決できます。

  重複する OpsItems を解決し、ソースによって作成される OpsItems の数を減らすために、Systems Manager では自動化ランブックが提供されています。詳細については、インサイトに基づく重複 OpsItems の解決 を参照してください。

デフォルトの EventBridge ルールの重複排除文字列を編集する

OpsCenter をターゲットとする EventBridge ルールに重複排除文字列を指定するには、次の手順を使用します。

デフォルトの EventBridge ルールの重複排除文字列を編集するには

1. AWS Management Console にサインインし、Amazon EventBridge コンソール (https://console.aws.amazon.com/events/) を開きます。
2. ナビゲーションペインで [ルール] を選択します。
3. ルールを選択し、[編集] を選択します。
4. [Select target(s)] (ターゲットの選択) ページに移動します。
5. [Additional settings] (追加設定) セクションの [Configure input transformer] (入力トランスフォーマーの設定) を選択します。
6. [Template] (テンプレート) ボックスで、編集する `"operationalData": { "/aws/dedup"` JSON エントリと重複排除文字列を見つけます。

   EventBridge ルールの重複排除文字列を入力する際は、以下の JSON 形式を使用します。

   ```
   "operationalData": { "/aws/dedup": {"type": "SearchableString","value":
    "{\"dedupString\":\"Words the system should use to check for duplicate
    OpsItems\"}"}}
   ```

   以下はその例です。

   ```
   "operationalData": { "/aws/dedup": {"type": "SearchableString","value":
    "{\"dedupString\":\"SSMOpsCenter-EBS-volume-performance-issue\"}"}}
   ```
7. 重複排除文字列を編集し、[確認] をクリックします。

8. [Next] を選択します。
9. [Next] を選択します。
10. [ルールの更新] を選択します。

AWS CLI を使用して重複排除文字列を指定する

重複排除文字列は、AWS Systems Manager コンソールまたは AWS CLI のいずれかを使用して、新しい OpsItem を手動で作成するときに指定することができます。コンソールで OpsItem を手動で作成するときに重複排除文字列を入力する方法については、「OpsItems を手動で作成する」を参照してください。AWS CLI を使用している場合、OperationalData パラメータに重複排除文字列を入力できます。次の例に示すように、パラメータの構文では JSON を使用します。

```
--operational-data '{"/aws/dedup":{"Value":"{\"dedupString\": \"Words the system should
 use to check for duplicate OpsItems\"}","Type":"SearchableString"}}'
```

以下に示しているのは、`disk full` の重複排除文字列を指定するコマンドの例です。

Linux & macOS

```
aws ssm create-ops-item \
    --title "EC2 instance disk full" \
    --description "Log clean up may have failed which caused the disk to be full" \
    --priority 1 \
    --source ec2 \
    --operational-data '{"/aws/dedup":{"Value":"{\"dedupString\": \"disk full
\"}","Type":"SearchableString"}}' \
    --tags "Key=EC2,Value=ProductionServers" \
    --notifications Arn="arn:aws:sns:us-west-1:12345678:TestUser"
```

Windows

```
aws ssm create-ops-item ^
    --title "EC2 instance disk full" ^
    --description "Log clean up may have failed which caused the disk to be full" ^
    --priority 1 ^
    --source EC2 ^
    --operational-data={\"/aws/dedup\":{\"Value\":\"{\\\"""dedupString\\""":\\"""disk
 full\\"""}\",\"Type\":\"SearchableString\"}} ^
    --tags "Key=EC2,Value=ProductionServers" --notifications Arn="arn:aws:sns:us-
west-1:12345678:TestUser"
```

OpsItems を減らすために運用上のインサイトを分析する

OpsCenter の運用上のインサイトには、重複する OpsItems に関する情報が表示されます。OpsCenter はアカウント内で自動的に OpsItems を分析し、3 種類のインサイトを生成します。この情報は OpsCenter [概要] タブの [運用上のインサイト] セクションで確認できます。

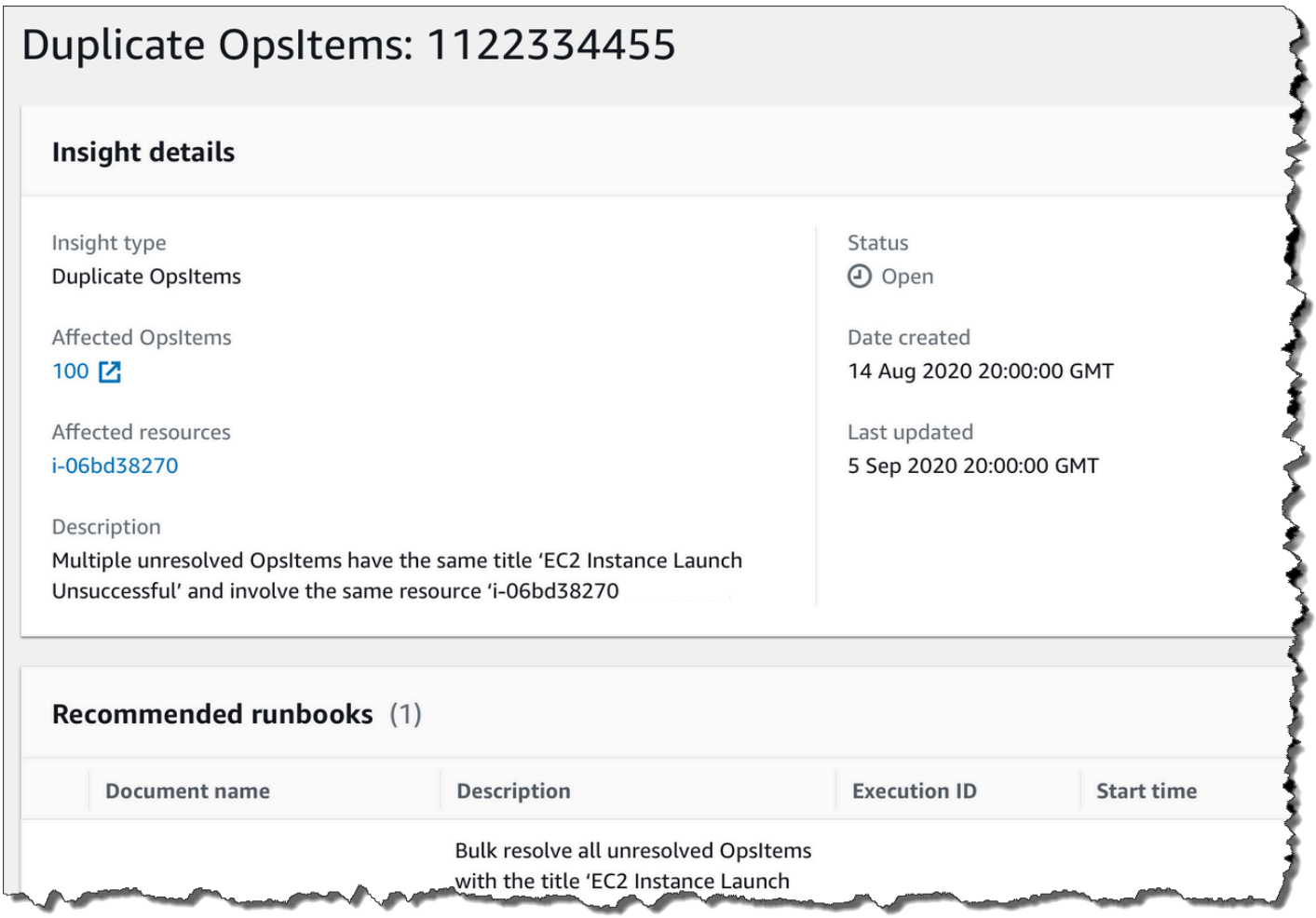
- OpsItems を複製 – このフィールドには、同じリソースに同じタイトルの OpsItems が 8 個以上ある場合に、インサイトが 1 件生成されます。
- 最も一般的なタイトル — 同じタイトルの OpsItems が 50 件を超えるとインサイトが 1 件生成されます。
- OpsItems を最も多く生成するリソース — AWS 件のリソースに OpsItems が 10 件以上開いているときにインサイトが 1 件生成されます。これらのインサイトとそれに対応するリソースが、OpsCenter [概要] タブの [OpsItems を最も多く生成するリソース] テーブルに表示されます。リソースは OpsItem の数の多い順に一覧表示されます。

> **Note**
>
> OpsCenter は以下のリソースタイプについて [OpsItems を最も多く生成するリソース] インサイトを作成します。
>
> - Amazon Elastic Compute Cloud (Amazon EC2) インスタンス
> - Amazon EC2 セキュリティグループ
> - Amazon EC2 Auto Scaling グループ
> - Amazon Relational Database Service (Amazon RDS) データベース
> - Amazon RDS クラスター
> - AWS Lambda 関数
> - Amazon DynamoDB テーブル
> - Elastic Load Balancing ロードバランサー
> - Amazon Redshift クラスター
> - AWS Certificate Manager 証明書
> - Amazon Elastic Block Store ボリューム

OpsCenter は 1 つのタイプにつきインサイト 15 件までという上限を設けています。タイプがこの上限に達すると、OpsCenter はそのタイプのインサイトの表示を停止します。追加のインサイトを表

示するには、そのタイプの OpsInsight に関連付けられた OpsItems をすべて解決する必要があります。15 件のインサイトの上限により、保留中のインサイトがコンソールに表示されない場合、そのインサイトは他のインサイトが閉じられた後に表示されます。

インサイトを選択すると、影響を受ける OpsItems とリソースに関する情報が OpsCenter に表示されます。次のスクリーンショットは、重複している OpsItem インサイトの詳細を示した例です。



運用上のインサイトは、デフォルトで無効になっています。運用上のインサイトの使用に関する詳細については、以下のトピックを参照してください。

トピック

- 運用上のインサイトを無効化する
- インサイトに基づく重複 OpsItems の解決
- オペレーションインサイトの無効化

運用上のインサイトを無効化する

Systems Manager コンソールの OpsCenter ページで運用上のインサイトを有効にできます。運用上のインサイトを有効にすると、Systems Manager は `AWSServiceRoleForAmazonSSM_OpsInsights` という名前の AWS Identity and Access Management (IAM) サービスリンクロールを作成します。サービスにリンクされたロールは、Systems Manager に直接リンクされた一意のタイプの IAM ロールです。サービスにリンクされたロールは事前定義されており、サービスがユーザーに代わって他の AWS のサービス を呼び出すために必要なすべてのアクセス許可が含まれています。`AWSServiceRoleForAmazonSSM_OpsInsights` サービスにリンクされたロールの詳細については、ロールを使用して Systems Manager OpsCenter で運用上のインサイト OpsItems を作成するを参照してください。

> **Note**
>
> 次の重要な情報に注意してください。
>
> - 運用上のインサイトは、お客様の AWS アカウントに課金されます。詳細については、AWS Systems Manager 料金を参照してください。
> - OpsCenter は、バッチプロセスを使用してインサイトを定期的に更新します。つまり、OpsCenter に表示されるインサイトの一覧は同期されていない可能性があります。

OpsCenter で運用上のインサイトを有効にして表示するには、次の手順を使用します。

運用上のインサイトを有効にして表示するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[OpsCenter] を選択します。
3. [運用上のインサイトが利用可能です] メッセージボックスで、[有効化] を選択します。このメッセージが表示されない場合は、[運用上のインサイト] セクションまで下にスクロールして [有効化] を選択します。
4. この機能を有効にしたら、[概要] タブの [運用上のインサイト] セクションまで下にスクロールします。
5. フィルター処理されたインサイトのリンクを表示するには、[OpsItems を重複]、[最も一般的なタイトル]、または[OpsItems を最も多く生成するリソース] の隣にあるリンクを選択します。す

べてのインサイトを表示するには、[運用に関するすべてのインサイトを表示] を選択してください。

6. 詳細情報を表示するには、インサイト ID を選択します。

インサイトに基づく重複 OpsItems の解決

インサイトを解決するには、まず、インサイトに関連付けられている OpsItems をすべて解決する必要があります。インサイトに関連付けられている OpsItems を解決するため、`AWS-BulkResolveOpsItemsForInsight` ランブックを使用できます。

重複する OpsItems を解決し、ソースによって作成された OpsItems の数を減らすために、Systems Manager では、以下のような自動化ランブックが提供されています。

- `AWS-BulkResolveOpsItems` ランブックは、特定のフィルターに一致する OpsItems を解決します。
- `AWS-AddOpsItemDedupStringToEventBridgeRule` ランブックは、特定の Amazon EventBridge ルールに関連付けられたすべての OpsItem ターゲットの重複解除文字列を追加します。ルールが既に存在する場合、このランブックは重複解除文字列を追加しません。
- EventBridge のルールが数十から数百の OpsItems を生成している場合、`AWS-DisableEventBridgeRule` によってそのルールがオフになります。

オペレーションに関するインサイトを解決するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[OpsCenter] を選択します。
3. [概要] タブで下にスクロールして、[オペレーションインサイト]までスクロールダウンします。
4. [オペレーションに関するすべてのインサイトを表示] を選択します。
5. 詳細情報を表示するには、インサイト ID を選択します。
6. ランブックを選択し、[実行] を選択します。

オペレーションインサイトの無効化

運用上のインサイトを無効にすると、システムは新しいインサイトの作成を停止し、コンソールでのインサイトの表示を停止します。アクティブなインサイトは、コンソールに表示されることはありませんが、システム内では変更されないままになっています。この機能を再度有効にすると、システム

は未解決のインサイトを表示し、新しいインサイトの作成を開始します。運用上のインサイトをオフにするには、次の手順に従います。

運用上のインサイトをオフにするには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[OpsCenter] を選択します。
3. [設定] を選択します。
4. [オペレーションインサイト] セクションで [編集] を選択してから、[無効化] オプションにトグルします。
5. [保存] を選択します。

OpsCenter ログとレポートを表示する

AWS CloudTrail は、コンソール、AWS Command Line Interface (AWS CLI)、および SDK への AWS Systems Manager OpsCenter API コールをログに記録します。CloudTrail コンソールまたは Amazon Simple Storage Service (Amazon S3) バケットで情報を表示できます。Amazon S3 は、1 つのバケットを使用して、アカウントのすべての CloudTrail ログを保存します。

OpsCenter アクションのログには、OpsItem アクティビティの作成、更新、取得、および説明が含まれます。Systems Manager アクティビティの CloudTrail ログの表示と使用の詳細については、「AWS Systems Manager による AWS CloudTrail API コールの口グ記録」を参照してください。

AWS Systems Manager OpsCenter は、OpsItems に関する情報を提供します。

- OpsItem ステータスの概要 - ステータス別 (未解決で進行中、未解決、進行中) の OpsItems の概要。
- 未解決の上位 OpsItems を含むソース - 未解決の OpsItems が含まれている上位の AWS のサービス の内訳。
- ソース別および経過日数別の OpsItems - ソース別および経過日数別にグループ化した OpsItems の数。

OpsCenter の概要レポートを表示するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。

2. ナビゲーションペインで、[OpsCenter] を選択します。
3. OpsItems の [概要] ページで、[概要] をクリックします。
4. [OpsItems by source and age (ソース別および経過時間別の OpsItems)] で検索バーを選択し、[Source (ソース)] に基づいて OpsItems をフィルター処理します。リストを使用して、[Status (ステータス)] に基づいてフィルタ処理します。

OpsItems を削除する

AWS Command Line Interface または AWS SDK を使用して DeleteOpsItem API 操作を呼び出すと、個々の OpsItem を削除できます。AWS Management Console で OpsItem を削除することはできません。OpsItem を削除するには、AWS Identity and Access Management (IAM) ユーザー、グループ、またはロールに管理者アクセス許可があるか、`DeleteOpsItem` API 操作を呼び出すアクセス許可が付与されている必要があります。

Important

この操作に関しては、次の重要事項に留意してください。

- OpsItem を削除すると元に戻せません。削除された OpsItem を復元することはできません。
- この操作では結果整合性モデルが使用されるため、システムがこの操作を完了するまでに数分かかることがあります。OpsItem を削除し、GetOpsItem などをすぐに呼び出しても、削除した OpsItem が応答に表示されることがあります。
- このオペレーションはべき等です。同じ OpsItem に対してこの操作を繰り返し呼び出しても、システムは例外を発生させません。最初の呼び出しが成功すると、それ以降のすべての呼び出しは最初の呼び出しと同じ成功応答を返します。
- この操作ではアカウント間呼び出しをサポートしていません。OpsCenter がアカウント間管理用にセットアップされている場合、委任管理者または管理アカウントは、他のアカウントで OpsItems を削除できません。アカウント間管理の詳細については、「(オプション)OpsCenter を設定して、複数のアカウント間で OpsItems を一元管理する」を参照してください。
- `OpsItemLimitExceededException` が表示された場合は、OpsItems を 1 つ以上削除して、OpsItems の合計数をクォータ制限以下に減らします。この例外の詳細については、「OpsCenter で問題のトラブルシューティング」を参照してください。

OpsItem の削除

以下の手順に従って、OpsItem を削除します。

OpsItem を削除するには

1. まだ AWS CLI をインストールして設定していない場合はインストールして設定します。詳細については、「Installing or updating the latest version of the AWS CLI」を参照してください。
2. 以下のコマンドを実行してください。削除する OpsItem の ID で *[ID]* を置き換えます。

```
aws ssm delete-ops-item --ops-item-id ID
```

正常終了すると、コマンドは何も返しません。

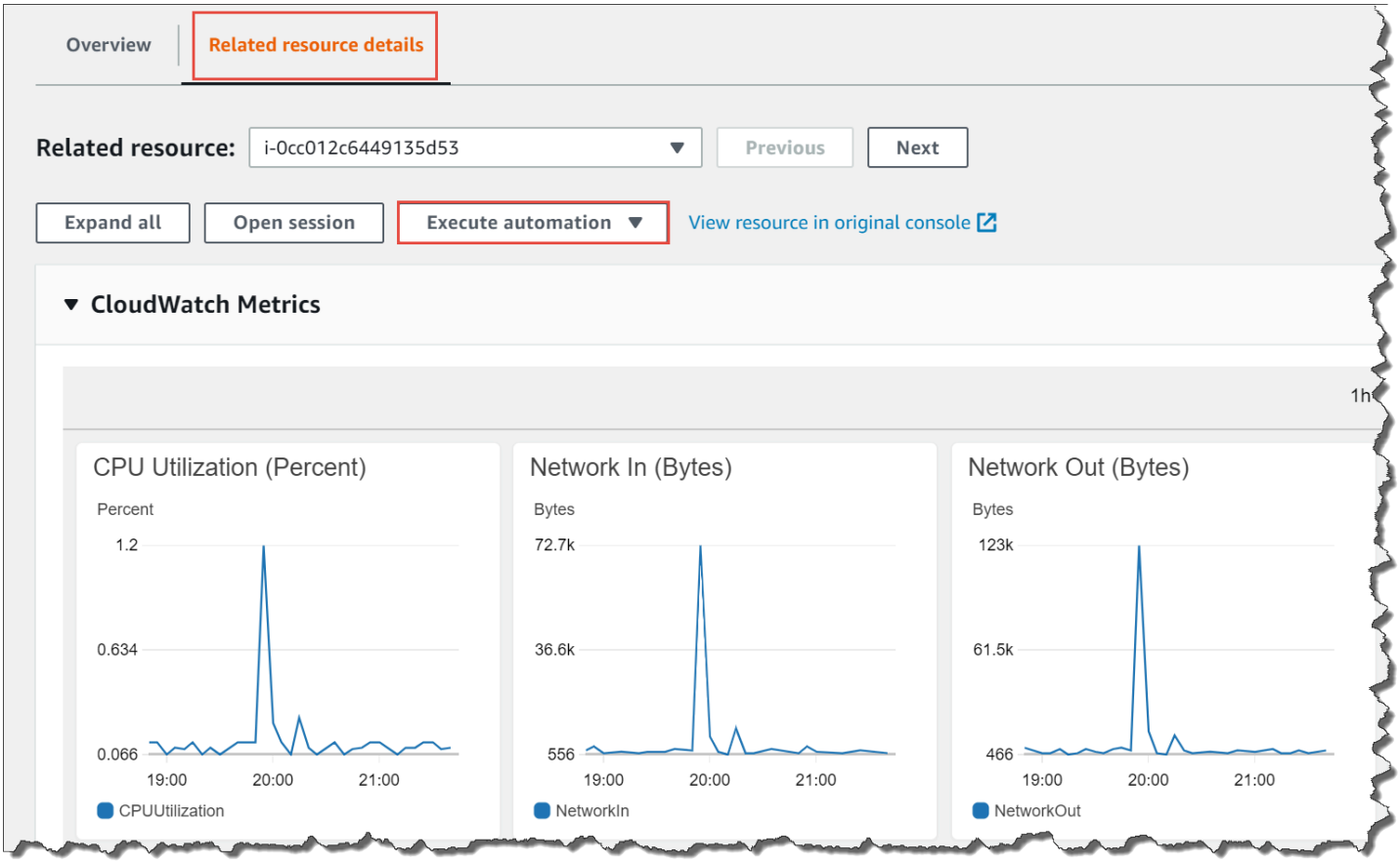
OpsItem の問題を修正する

AWS Systems Manager 自動化ランブックを使用して、OpsItem で特定した AWS リソースに関する問題を修正できます。オートメーションは、事前定義されたランブックを使用して、AWS リソースに関する一般的な問題を修正します。

各 OpsItem には [ランブック] セクションがあり、修正に使用できるランブックがリストされています。リストから自動化ランブックを選択すると、OpsCenter がドキュメントの実行に必要なフィールドの一部を自動的に表示します。自動化ランブックを実行すると、システムはランブックを OpsItem の関連リソースに自動的に関連付けます。Amazon EventBridge が OpsItem を作成すると、ランブックが OpsItem に関連付けられます。OpsCenter は、OpsItem の自動化ランブックを 30 日間記録します。

次の例に示すように、オートメーションが失敗した理由、失敗したときに実行されていた自動化ランブックのステップなど、その実行に関する重要な詳細を表示するステータスを選択できます。

選択した OpsItem の [関連リソースの詳細] ページには、[Run automation] リストが含まれます。最近使用した自動化ランブックまたはリソース固有の自動化ランブックを選択して、問題を修正できます。このページには、Amazon CloudWatch メトリクスとアラーム、AWS CloudTrail ログ、AWS Config の詳細など、役立つデータプロバイダーも含まれています。



Automation ランブックに関する情報を表示するには、コンソールでその名前を選択するか、Systems Manager Automation ランブックのリファレンス を使用します。

ランブックを使用して OpsItem を修正する

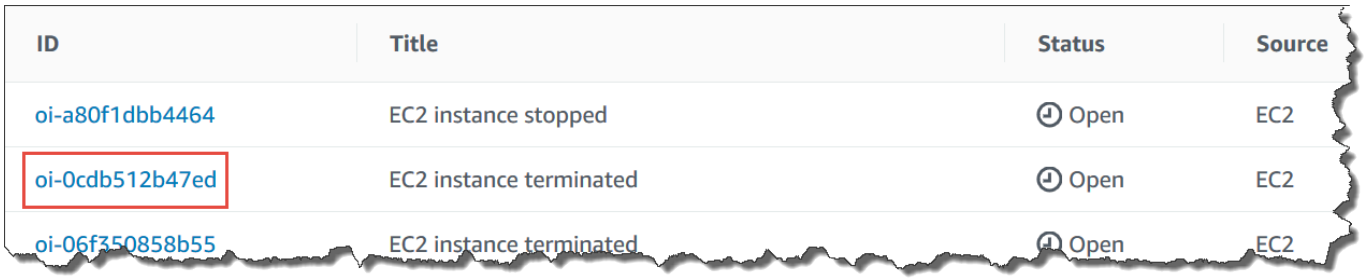
自動化ランブックを使用して OpsItem の問題を修正する前に、次の操作を行います。

- Systems Manager Automation ランブックを実行するためのアクセス許可があることを確認します。詳細については、「」を参照してくださいオートメーションの設定
- 実行する自動化のリソース固有の ID 情報を収集します。例えば、EC2 インスタンスを再起動するオートメーションを実行する場合、再起動する EC2 インスタンスの ID を指定する必要があります。

Automation ランブックを実行して OpsItem の問題を修復するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[OpsCenter] を選択します。

3. OpsItem ID を選択して、詳細ページを開きます。



4. [ランブック] セクションまでスクロールします。
5. 検索バー、または右上の数字を使用して、実行する自動化ランブックを検索します。
6. ランブックを選択し、[実行] を選択します。
7. ランブックの必要な情報を入力し、[送信] を選択します。

   ランブックを起動すると、システムは前の画面に戻り、ステータスを表示します。
8. [過去 30 日間の自動化] セクションで、[実行 ID] リンクを選択して、実行のステップとステータスを表示します。

関連するランブックを使用して、OpsItem を修正する

OpsItem から自動化ランブックを実行すると、OpsCenter がランブックを OpsItem に関連付けます。関連付けられたランブックは、[ランブック] リストの他のランブックよりも上位にランク付けされます。

次の手順に従って、OpsItem の関連リソースに既に関連付けられている Automation ランブックを実行します。関連リソースの追加については、「OpsItems を管理する」を参照してください。

リソースに関連付けられたランブックを実行して OpsItem の問題を修復するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[OpsCenter] を選択します。
3. OpsItemを開きます。
4. [関連リソース] セクションで、 Automation ランブックを実行するリソースを選択します。
5. [Run automation (自動化を実行)] を選択し、実行する関連付けられた Automation ランブックを選択します。
6. ランブックの必要な情報を入力し、[実行] を選択します。

ランブックを起動すると、システムは前の画面に戻り、ステータスを表示します。

7. [過去 30 日間の自動化] セクションで、[実行 ID] リンクを選択して、実行のステップとステータスを表示します。

OpsCenter 概要レポートの表示

AWS Systems Manager OpsCenter には、概要ページが含まれており、以下の情報が自動的に表示されます。

- OpsItem ステータス概要 – `Open` や `In progress` といった、ステータス別の OpsItems の概要。
- 最もオープンな OpsItems を持つソース – OpsItems が最も多く開かれた AWS のサービス の内訳。
- ソースと経過日数別の OpsItems - ソース別および経過日数別にグループ化した OpsItems の数。

OpsCenter 概要レポートを表示するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで OpsCenter を選択し、次に [概要] タブを選択します。
3. ソースと経過日数別の OpsItems セクションで、以下の操作を行います。

    1. (オプション) フィルターフィールドで、[ソース] を選択したら、`Equal`、`Begin With`、または `Not Equal` を選択し、検索パラメータを入力します。
    2. 隣接するリストで、次のいずれかのステータス値を選択します。
        - `Open`
        - `In progress`
        - `Resolved`
        - `Open and in progress`
        - `All`

OpsCenter で問題のトラブルシューティング

このトピックには、OpsCenter の一般的なエラーや問題のトラブルシューティングに役立つ情報が収められています。

OpsItemLimitExceededException の発生

CreateOpsItem API オペレーションを呼び出したときに、AWS アカウント が許可されている OpsItems の最大数に達すると、`OpsItemLimitExceededException` を受け取ります。OpsCenter は呼び出しが以下のいずれかのクォータの OpsItems の最大数を超えると、例外を返します。

- リージョンの AWS アカウント あたりの `Open` 総数 (OpsItems および `Resolved` OpsItems を含む): 500,000
- 1 か月の AWS アカウント あたりの OpsItems の最大数: 10,000

これらのクォータは、以下を除くすべてのソースから作成された OpsItems に適用されます。

- AWS Security Hub の検出結果により作成された OpsItems
- Incident Manager のインシデントが開かれると自動生成される OpsItems

これらのソースから作成された OpsItems は OpsItem クォータにはカウントされませんが、OpsItem ごとに課金されます。

`OpsItemLimitExceededException` を受け取った場合は、OpsItem の新規作成を妨げるクォータより少なくなるまで、OpsItems を手動で削除できます。繰り返しになりますが、Security Hub の検出結果または Incident Manager のインシデント用に作成された OpsItems を削除しても、クォータによって適用される OpsItems の総数は減りません。他のソースから OpsItems を削除する必要があります。OpsItem を削除する方法については、「OpsItems を削除する」を参照してください。

AWS から自動生成された大量の OpsItems に対し高額な請求書が届く

AWS Security Hub との統合を設定した場合、OpsCenter は Security Hub の検出結果に OpsItems を作成します。Security Hub が生成する検出結果の数と、統合を設定したときに口グインしていたアカウントによっては、OpsCenter は OpsItems を大量に生成する可能性があります。これには料金が発生します。Security Hub の調査結果によって生成される OpsItems に関連する具体的な詳細は次のとおりです。

- 設定時に Security Hub 管理者アカウントに口グインしていて、OpsCenter と Security Hub の統合を設定すると、システムは管理者とすべてのメンバーアカウントの検出結果に OpsItems を作成します。OpsItems は管理者アカウントですべて作成されます。さまざまな要因によっては、これにより AWS から予想外に多額の請求が発生する可能性があります。

統合を設定するときにログインしていたのがメンバーアカウントであった場合、システムは個人のアカウントの検出結果にのみ OpsItems を作成します。Security Hub 管理者アカウント、メンバーアカウント、および検出結果の EventBridge イベントフィードとの関係の詳細については、「AWS Security Hubユーザーガイド」で「EventBridge との Security Hub 統合のタイプ」を参照してください。

- 検出結果が OpsItem を作成するたびに、OpsItem の作成には通常料金がかかります。また、OpsItem を編集した場合や、対応する検出結果が Security Hub で更新された (OpsItem がトリガーされる) 場合にも課金されます。
- AWS Security Hub との統合によって作成された OpsItems は現在、リージョンのアカウントあたり 500,000 OpsItems の最大クォータによって制限されていません。そのため、Security Hub アラートによって、アカウント内の各リージョンで 500,000 を超える課金対象の OpsItems が作成される可能性があります。

  高負荷の本番環境では、Security Hub の検出結果の範囲を重要度の高い問題のみに制限することをお勧めします。

> **Important**
>
> OpsItems の多くが誤って作成されたもので、AWS の請求内容が不当であると思われる場合は、サポート にお問い合わせください。

Security Hub の検出結果に対し、システムで OpsItems を作成する必要がなければ、次の手順を使用してください。

Security Hub の検出結果に対する OpsItems の受信を停止するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[OpsCenter] を選択します。
3. [設定] を選択します。
4. [Security Hub の検出結果] セクションで、[編集] を選択します。
5. スライダーを選択して [有効] を [無効] に変更します。スライダーを切り替えられない場合は、AWS アカウント の Security Hub が有効になっていません。

6. [保存] を選択して設定を保存します。OpsCenter は Security Hub の検出結果に基づいて OpsItems を作成しなくなります。

> **Important**
>
> OpsCenter が設定を [有効] に戻し、検出結果の OpsItems の作成を続行する場合は、Systems Manager の委任管理者アカウントまたは AWS Organizations 管理アカウントにログインして、この手順を繰り返します。これらのアカウントにログインするアクセス許可がない場合は、管理者に連絡し、この手順を繰り返してアカウントの統合を無効にするよう依頼してください。

Systems Manager がホストする Amazon CloudWatch ダッシュボードの使用

Amazon CloudWatch ダッシュボードは、CloudWatch コンソールにあるカスタマイズ可能なホームページであり、ダッシュボードを使用すれば、異なる AWS リージョン にまたがっているリソースでも、1 つのビューでモニタリングできます。CloudWatch ダッシュボードを使用して、AWS のリソースのメトリクスおよびアラームをカスタマイズした状態で表示することができます。ダッシュボードでは、以下を作成することが可能です。

- 選択されたメトリクスとアラームのための単一ビュー。これは、1 つ、または複数の AWS リージョン 全体のリソースとアプリケーションの正常性を評価するために役立ちます。各グラフのメトリクスごとに使用する色を選択できるため、複数のグラフにわたる同一のメトリクスを追跡できます。
- 操作イベント中の特定の問題への対処法に関して、チームのメンバーにガイダンスを提供する運営計画。
- 重要なリソースとアプリケーション測定の共通表示。これをチームメンバー間で共有して操作イベント中のコミュニケーションフローを円滑化できます。

ダッシュボードを作成するには、コンソール、AWS Command Line Interface (AWS CLI)、または CloudWatch `PutDashboard` API を使用します。詳細については、「Amazon CloudWatch ユーザーガイド」の「Amazon CloudWatch ダッシュボードの使用」を参照してください。

「SSM Agent」 の使用

AWS Systems Manager エージェント (SSM Agent) は、Amazon Elastic Compute Cloud (Amazon EC2) インスタンス、エッジデバイス、オンプレミスサーバー、仮想マシン (VM) で実行される Amazon のソフトウェアです。SSM Agent を使用すると、Systems Manager でこれらのリソースを更新、管理、設定できるようになります。エージェントは、AWS クラウド で Systems Manager サービスからのリクエストを処理し、リクエストで指定されたとおりに実行します。SSM Agent は、Amazon Message Gateway Service (ssmmessages) を使用して、Systems Manager サービスにステータスと実行情報を返します。(2024 年より前にローンチされた AWS リージョン では、ステータスと実行情報が Amazon Message Delivery Service (サービスプレフィックス: ec2messages) によって返される場合があります。)

トラフィックをモニタリングすると、マネージドノードが ssmmessages.* エンドポイントか、場合によっては ec2messages.* エンドポイントと通信していることがわかります。詳細については、「リファレンス: ec2messages、ssmmessages およびその他の API オペレーション」を参照してください。SSM Agent ログを Amazon CloudWatch Logs に移植する方法については、「AWS Systems Manager でのログ記録とモニタリング」を参照してください。

内容

- SSM Agent に関する技術的な詳細を知る
- SSM Agent がプリインストールされている AMIs を見つける
- Linux 用 EC2 インスタンスで SSM Agent を使用する
- macOS 用 EC2 インスタンスで SSM Agent を使用する
- Windows Server 用 EC2 インスタンスで SSM Agent を使用する
- SSM Agent ステータスの確認とエージェントの起動
- SSM Agent バージョン番号の確認
- SSM Agent ログの表示
- SSM Agent を介してルートレベルコマンドへのアクセスを制限する
- SSM Agent への更新の自動化
- SSM Agent 通知にサブスクライブする
- SSM Agent のトラブルシューティング

SSM Agent に関する技術的な詳細を知る

このトピックの情報を使用して、AWS Systems Manager Agent (SSM Agent) を実装し、エージェントの仕組みを理解するのに役立ちます。

トピック

- SSM Agent バージョン 3.2.x.x 認証情報の動作
- SSM Agent 認証情報の優先順位
- 連邦情報処理規格 (FIPS) での使用のための SSM Agent の設定
- ローカル ssm-user アカウントについて
- SSM Agentと Instance Metadata Service (IMDS)
- SSM Agent を最新の状態に維持
- SSM Agent インストールディレクトリが変更、移動、削除されていないことの確認
- AWS リージョン による SSM Agent のローリング更新
- SSM Agent と AWS マネージド S3 バケットとの通信

SSM Agent バージョン 3.2.x.x 認証情報の動作

インスタンスが、Quick Setup のデフォルトのホスト管理設定を使用してオンボーディングされた場合、SSM Agent は一時的な認証情報のセットを `/var/lib/amazon/ssm/credentials` (Linux と macOS の場合)、または `%PROGRAMFILES%\Amazon\SSM\credentials` (Windows Server の場合) に格納します。一時的な認証情報には、デフォルトのホスト管理設定で選択した IAM ロールに指定した許可が含まれます。Linux では、これらの認証情報にアクセスできるのは、root アカウントだけです。Windows Server では、SYSTEM アカウントとローカル管理者のみがこれらの認証情報にアクセスできます。

SSM Agent 認証情報の優先順位

このトピックは SSM Agent がリソースにアクションを実行するためにどのようにアクセス許可が付与されるか、重要な情報について説明します。

> **Note**
>
> エッジデバイスのサポートは少し異なります。AWS IoT Greengrass コアソフトウェアを使用できようにエッジデバイスを設定、AWS Identity and Access Management (IAM) サービス

ロールを設定、AWS IoT Greengrass を使って SSM Agent をデバイスに展開する必要があります。詳細については、「Systems Manager を利用したエッジデバイスの管理」を参照してください。

SSM Agent がマシンにインストールされている場合、Systems Manager サービスと通信するにはアクセス許可が必要です。Amazon Elastic Compute Cloud (Amazon EC2) インスタンスでは、このようなアクセス許可は、インスタンスにアタッチされたインスタンスプロファイルで提供されます。非 EC2 マシンの場合、SSM Agent は通常、必要な許可を共有認証情報ファイルから取得し、`/root/.aws/credentials` (Linux と macOS) または `%USERPROFILE%\.aws\credentials` (Windows Server) に保存されています。必要な許可は、ハイブリッドアクティベーションプロセス中にこのファイルに追加されます。

ただし、まれに、SSM Agent がタスクを実行するための許可をチェックする複数の場所に、マシンの許可が追加されてしまうことがあります。

例えば、Systems Manager によって管理されるように EC2 インスタンスを設定したとします。その設定にはインスタンスプロファイルのアタッチが含まれます。しかし、そのインスタンスをデベロッパーまたはエンドユーザーのタスクにも使用し、そのインスタンス に AWS Command Line Interface (AWS CLI) をインストールすることにしました。このインストールでは、インスタンス上の認証情報ファイルに追加のアクセス許可が追加されます。

インスタンスで Systems Manager コマンドを実行すると、SSM Agent は、インスタンスプロファイルではなく認証情報ファイルからの認証情報など、使用する想定とは異なる認証情報を使用しようとすることがあります。これは、SSM Agent がデフォルトの資格情報プロバイダーチェーンに規定された順序で資格情報を検索するためです。

> **Note**
>
> Linux と macOS では、SSM Agent はルートユーザーとして実行されます。したがって、このプロセスで SSM Agent が検索する環境変数と認証情報ファイルは、ルートユーザーのみのものです (`/root/.aws/credentials`)。SSM Agent は、認証情報の検索中に、インスタンス上の他のユーザーの環境変数や認証情報ファイルを参照しません。

デフォルトのプロバイダーチェーンは、次の順序で認証情報を検索します。

1. 環境変数 (設定されている場合) (`AWS_ACCESS_KEY_ID` および `AWS_SECRET_ACCESS_KEY`)。

2. ハイブリッド環境のアクティベーションや AWS CLI のインストールなどによって提供されるアクセス許可を持つ共有認証情報ファイル (Linux と macOS の場合は `$HOME/.aws/credentials`、Windows Server の場合は `%USERPROFILE%\.aws\credentials`)。
3. Amazon Elastic Container Service (Amazon ECS) タスク定義または RunTask API オペレーションを使用するアプリケーションが存在する場合、タスクの AWS Identity and Access Management (IAM) ロール。
4. Amazon EC2 インスタンスにアタッチされたインスタンスプロファイル。
5. デフォルトのホスト管理構成用に選択された IAM ロール。

関連情報については、次のトピックを参照してください。

- EC2 インスタンスのインスタンスプロファイル — Systems Manager に必要なインスタンスのアクセス許可を設定する
- ハイブリッドアクティベーション – ハイブリッドアクティベーションを作成して、Systems Manager にノードを登録する
- AWS CLI クレデンシャルファイル – AWS Command Line Interface ユーザーガイドの「設定と認証情報ファイルの設定」
- デフォルトの認証情報プロバイダーチェーン – AWS SDK for Go デベロッパーガイドの「認証情報の指定」

> **Note**
>
> AWS SDK for Go デベロッパーガイドのこのトピックでは、SDK for Go に関するデフォルトのプロバイダーチェーンについて説明します。ただし、SSM Agent の認証情報の評価にも同じ原則が適用されます。

連邦情報処理規格 (FIPS) での使用のための SSM Agent の設定

Systems Manager を連邦情報処理規格 (FIPS) 140-3 検証済み暗号化モジュールで使用する必要がある場合は、サポートされているリージョン内の FIPS エンドポイントを使用するように AWS Systems Manager Agent (SSM Agent) を設定することができます。

FIPS 140-3 エンドポイントに接続するように SSM Agent を設定する

1. マネージドノードに接続します。

2. amazon-ssm-agent.json ファイルが格納されているディレクトリに移動します。

   - Linux: /etc/amazon/ssm/
   - macOS: /opt/aws/ssm/
   - Windows Server: C:\Program Files\Amazon\SSM\

3. 編集する amazon-ssm-agent.json という名前のファイルを開きます。

   > **Tip**
   >
   > amazon-ssm-agent.json ファイルがまだ存在していない場合は、amazon-ssm-agent.json.template のコンテンツを amazon-ssm-agent.json という名前の新しいファイルにコピーします。amazon-ssm-agent.json.template と同じディレクトリに amazon-ssm-agent.json を保存します。

4. ファイルに次のコンテンツを追加します。*region* のプレースホルダー値を、パーティションに適したリージョンコードに置き換えます:

```
{
    ---Existing file content, if any---
    "Mds": {
        "Endpoint": "ec2messages-fips.region.amazonaws.com",
    },
    "Ssm": {
        "Endpoint": "ssm-fips.region.amazonaws.com",
    },
    "Mgs": {
        "Endpoint": "ssmmessages-fips.region.amazonaws.com",
        "Region": "region"
    },
    "S3": {
        "Endpoint": "s3-fips.dualstack.region.amazonaws.com",
        "Region": region"
    },
    "Kms": {
        "Endpoint": "kms-fips.region.amazonaws.com"
    }
}
```

   サポートされるリージョンには以下が含まれます。

- us-east-1 (米国東部 (バージニア北部) リージョンの場合)
- us-east-2 (米国東部 (オハイオ) リージョンの場合)
- us-west-1 (米国西部 (北カリフォルニア) リージョンの場合)
- us-west-2 (米国西部 (オレゴン) リージョンの場合)
- ca-west-1 (カナダ西部 (カルガリー) リージョンの場合)

5. ファイルを保存して、SSM Agent を再起動します。

設定を変更するたびに、SSM Agent を再起動します。

同じ手順を使用して、SSM Agent の他の機能をカスタマイズできます。利用可能な設定プロパティとそのデフォルト値の最新リストについては、GitHub の amazon-ssm-agent リポジトリで「Config Property Definitions」を参照してください。

FIPS に対する AWS サポートの詳細については、「連邦情報処理規格 (FIPS) 140-3」を参照してください。

ローカル ssm-user アカウントについて

SSM Agent バージョン 2.3.50.0 以降では、エージェントは ssm-user という名前のローカルユーザーアカウントを作成し、/etc/sudoers.d ディレクトリ (Linux と macOS) または、管理者グループ (Windows Server) に追加します。2.3.612.0 より前のエージェントバージョンでは、アカウントはインストール後に SSM Agent が最初に起動または再起動するときに作成されます。バージョン 2.3.612.0 以降では、ssm-user アカウントは、インスタンスでセッションが最初に開始されたときに作成されます。この ssm-user は、AWS Systems Manager のツールである Session Manager でセッションが開始されたときのデフォルトの OS ユーザーです。ssm-user を特権の少ないグループに移動するか、sudoers ファイルを変更することで、アクセス許可を変更できます。SSM Agent がアンインストールされるときに、ssm-user アカウントはシステムから削除されません。

Windows Server では、SSM Agent は各セッションの開始時に ssm-user アカウントの新しいパスワードの設定を処理します。Linux マネージドインスタンスで ssm-user にはパスワードは設定されていません。

SSM Agent 2.3.612.0 バージョンから、ssm-user アカウントは、ドメインコントローラーとして使用されている Windows Server マシンに自動的には作成されません。Session Manager ドメインコントローラーで Windows Server を使用するには、ssm-user アカウントが存在しない場合は手動でアカウントを作成し、ドメイン管理者のアクセス許可をユーザーに割り当てます。

> **Important**
>
> `ssm-user` アカウントを作成するには、インスタンスに添付されたインスタンスプロファイルによって、必要なアクセス許可が付与される必要があります。詳細については、「ステップ 2: Session Managerのインスタンスのアクセス権限の確認または追加」を参照してください。

SSM Agentと Instance Metadata Service (IMDS)

Systems Manager の正常な機能は、EC2 インスタンスメタデータに左右されます。Systems Manager は、Instance Metadata Service (IMDSv1 および IMDSv2) のバージョン 1 またはバージョン 2 を使用して、インスタンスメタデータにアクセスできます。インスタンスはインスタンスメタデータサービスの IPv4 アドレスにアクセスできる必要があります: 169.254.169.254。詳細については「アマゾン EC2 ユーザーガイド」の「Instance metadata and user data」(インスタンスメタデータとユーザーデータ) を参照してください。

SSM Agent を最新の状態に維持

新しいツールが Systems Manager に追加されるか、既存のツールが更新されると必ず、更新されたバージョンの SSM Agent がリリースされます。最新バージョンのエージェントを使用しないと、マネージドノードが Systems Manager の各種ツールや機能を使用できなくなる可能性があります。このため、マシン上で SSM Agent を最新状態に維持するプロセスを自動化することをお勧めします。詳細については、「SSM Agent への更新の自動化」を参照してください。GitHub の「SSM Agent リリースノート」ページをサブスクライブすると、SSM Agent の更新に関する通知を受け取ることができます。

> **Note**
>
> 新しいツールが Systems Manager に追加されるか、既存のツールが更新されると必ず、更新されたバージョンの SSM Agent がリリースされます。最新バージョンのエージェントを使用しないと、マネージドノードが Systems Manager の各種ツールや機能を使用できなくなる可能性があります。このため、マシン上で SSM Agent を最新状態に維持するプロセスを自動化することをお勧めします。詳細については、「SSM Agent への更新の自動化」を参照してください。GitHub の「SSM Agent リリースノート」ページをサブスクライブすると、SSM Agent の更新に関する通知を受け取ることができます。

デフォルトで SSM Agentが含まれている Amazon Machine Images (AMIs) は、最新バージョンの SSM Agentで更新されるまでに最大 2 週間かかります。SSM Agent に対するさらに頻繁な自動更新を設定することをお勧めします。

SSM Agent インストールディレクトリが変更、移動、削除されていないことの確認

SSM Agent は `/var/lib/amazon/ssm/` (Linux と macOS) および `%PROGRAMFILES%\Amazon\SSM\` (Windows Server) にインストールされます。これらのインストールディレクトリには、認証情報ファイル、プロセス間通信 (IPC) 用リソース、オーケストレーションフォルダなど、SSM Agent が使用する重要なファイルやフォルダが含まれています。インストールディレクトリ内のものは変更、移動、削除しないでください。そうでないと、SSM Agent が正しく機能しなくなる可能性があります。

AWS リージョン による SSM Agent のローリング更新

GitHub リポジトリで SSM Agent 更新が使用可能になった後、更新されたバージョンは各 AWS リージョン に異なる時間にロールアウトされ、すべてにロールアウトされるまで、最大 2 週間かかることがあります。このため、リージョンに SSM Agent の新しいバージョンをデプロイしようとすると、「Unsupported on current platform (現在のプラットフォームでサポートされていません)」または「updating amazon-ssm-agent to an older version, please turn on allow downgrade to proceed (amazon-ssm-agent を古いバージョンに更新しています。ダウングレードを許可してください)」というエラーが表示されることがあります。

使用可能な SSM Agent のバージョンを確認するには、`curl` コマンドを実行します。

グローバルダウンロードバケットで利用できるエージェントのバージョンを表示するには、次のコマンドを実行します。

```
curl https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/VERSION
```

特定のリージョンで使用可能なエージェントのバージョンを表示するには、次のコマンドを実行します。*`region`* を(米国東部 (オハイオ) リージョンでは `us-east-2` などの作業しているリージョンに置き換えます。

```
curl https://s3.region.amazonaws.com/amazon-ssm-region/latest/VERSION
```

VERSION コマンドなしでブラウザで curl ファイルを直接開くこともできます。

SSM Agent と AWS マネージド S3 バケットとの通信

さまざまな Systems Manager のオペレーションを実行する過程で、AWS Systems Manager Agent (SSM Agent) は多数の Amazon Simple Storage Service (Amazon S3) バケットにアクセスします。これらの S3 バケットはパブリックにアクセス可能です。デフォルトで、SSM Agent は HTTP 呼び出しを使用してこれに接続します。

ただし、Systems Manager のオペレーションで仮想プライベートクラウド (VPC) エンドポイントを使用している場合は、Systems Manager の Amazon Elastic Compute Cloud (Amazon EC2) インスタンスプロファイル、またはハイブリッドおよびマルチクラウド環境の非 EC2 マシンのサービスロールで、明示的なアクセス許可を付与する必要があります。それ以外の場合、リソースからこれらのパブリックバケットにアクセスすることはできません。

VPC エンドポイントの使用中にこれらのバケットへのマネージドノードアクセスを許可するには、カスタム Amazon S3 許可ポリシーを作成し、それをインスタンスプロファイル (EC2 インスタンスの場合) またはサービスロール (非 EC2 ノードの場合) にアタッチします。

Systems Manager オペレーションで仮想プライベートクラウド (VPC) エンドポイントを使用する方法については、「Systems Manager のために VPC エンドポイントを使用して EC2 インスタンスのセキュリティを強化する」を参照してください。

> **Note**
>
> これらのアクセス許可では、SSM Agent が必要とする AWS マネージドバケットへのアクセスのみが付与されます。また、その他の Amazon S3 オペレーションに必要なアクセス許可は付与されません。また、独自の S3 バケットへのアクセス許可は付与されません。

詳細については、以下の各トピックを参照してください。

- Systems Manager に必要なインスタンスのアクセス許可を設定する
- ハイブリッドおよびマルチクラウド環境で Systems Manager に必要な IAM サービスロールを作成する
- 参照: パッチ適用オペレーション用の Amazon S3 バケット

内容

- 必要なバケットアクセス許可
- 例
- ハードウェアフィンガープリントを使用したハイブリッドアクティベーションマシンの検証
- SSM AgentGitHub での

必要なバケットアクセス許可

次の表は、各 S3 バケットについて説明しています。SSM Agent は Systems Manager のオペレーションで、このようなバケットにアクセスする必要があるかもしれません。

> **Note**
>
> *region* は、米国東部 (オハイオ) リージョンの us-east-2 のように、AWS Systems Manager でサポートされている AWS リージョン の識別子を表します。サポートされている *region* 値の一覧については、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」にある Region 列を参照してください。

SSM Agent が必要とする Amazon S3 のアクセス許可

S3 バケット ARN	説明
arn:aws:s3:::aws-windows-downloads- *region*/*	Windows Server オペレーティングシステムのみをサポートする一部の SSM ドキュメントに必要です。さらに、AWSEC2-ConfigureSTIG などのクロスプラットフォームサポート用のドキュメントもあります。
arn:aws:s3:::amazon-ssm- *region*/*	SSM Agent インストールの更新のために必須です。これらのバケットには SSM Agent インストールパッケージ、および AWS-UpdateSSMAgent ドキュメントとプラグインによって参照されるインストールマニフェストが含まれています。これらのアクセス許可が提供されていない場合、SSM Agent は HTTP コールを実行して更新プログラムをダウンロードします。

S3 バケット ARN	説明
`arn:aws:s3:::aws-ssm-` *region*`/*`	パッチ適用以外の Systems Manager ドキュメント (SSM Command ドキュメント) での使用に必要なモジュールが含まれる S3 バケットへのアクセスを提供します。例: `arn:aws:s3:::aws-ssm-us-east-2/*` 。 以下は、これらのバケットに格納されている一般的に使用される SSM ドキュメントの一部です。 • `AWS-ConfigureWindowsUpdate` • `AWS-FindWindowsUpdates` • `AWS-UpdateSSMAgent` • `AWS-UpdateEC2Config`

S3 バケット ARN	説明
arn:aws:s3:::patch-baseline-snapshot- *region*/* -または- arn:aws:s3:::patch-baseline-snapshot- *region-unique-suffix* /*	パッチベースラインのスナップショットを含む S3 バケットへのアクセスを提供します。これは、以下の SSM Command ドキュメントのいずれかを使用する場合に必要です。 • AWS-RunPatchBaseline • AWS-RunPatchBaselineAssociation • AWS-RunPatchBaselineWithHooks • AWS-ApplyPatchBaseline (レガシーの SSM ドキュメント) ほとんどのサポート対象 AWS リージョンのバケットは、以下の形式を使用しています。 arn:aws:s3:::patch-baseline-snapshot- *region* 一部のリージョンでは、バケット名に一意のサフィックスが追加されています。例えば、中東 (バーレーン) リージョン (me-south-1) のバケット名は以下のようになります。 • patch-baseline-snapshot-me-south-1-uduvl7q8 パッチベースラインスナップショットのバケット名の完全なリストについては、「AWS が管理するパッチベースラインのスナップショットが含まれるバケット」を参照してください。 **Note** オンプレミスのファイアウォールを使用していて Patch Manager を使用する

S3 バケット ARN	説明
	場合は、そのファイアウォールでパッチベースラインのエンドポイントへの適切なアクセスを許可する必要もあります。

S3 バケット ARN	説明
Linux と Windows Server マネージドノードの場合: `arn:aws:s3:::aws-patch-manager-` *region*`-`*unique-suffix*` /*` macOS の Amazon EC2 インスタンスの場合: `arn:aws:s3:::aws-patchmanager-macos-` *region*`-`*unique-suffix*` /*`	Patch Manager でのパッチ適用オペレーション用 SSM Command ドキュメントを含む S3 バケットへのアクセスを提供します。各バケット名には、米国東部 (オハイオ) (us-east-2) リージョンにあるバケットの 552881074　など、一意のサフィックスが含まれています。 • `arn:aws:s3:::aws-patch-manager-us-east-2-552881074/*` • `arn:aws:s3::: aws-patchmanager-macos-us-east-2-552881074/*` SSM ドキュメント 以下は、これらのバケットに格納されている一般的に使用される SSM ドキュメントの一部です。 • `AWS-RunPatchBaseline` • `AWS-RunPatchBaselineAssociation` • `AWS-RunPatchBaselineWithHooks` • `AWS-InstanceRebootWithHooks` • `AWS-PatchAsgInstance` • `AWS-PatchInstanceWithRollback` パッチ適用オペレーション用の AWS マネージド S3 バケットの完全なリストについては、以下のトピックを参照してください。 • パッチ適用オペレーション用の SSM Command ドキュメントが含まれるバケット (Linux および Windows Server)

S3 バケット ARN	説明
	• パッチ適用オペレーション用の SSM Command ドキュメントが含まれるバケット (macOS)

例

次の例は、米国東部 (オハイオ) リージョン (us-east-2) で Systems Manager の使用に必要な S3 バケットへのアクセス権を付与する方法を示しています。ほとんどの場合、VPC エンドポイントを使用する場合にのみ、インスタンスプロファイルまたはサービスロールでこれらのアクセス許可を明示的に指定する必要があります。

> **Important**
>
> このポリシーの特定のリージョンの代わりにワイルドカード文字 (*) を使用しないことをお勧めします。例えば、`arn:aws:s3:::aws-ssm-us-east-2/*` を使用して、`arn:aws:s3:::aws-ssm-*/*` は使用しないでください。ワイルドカードを使用すると、アクセスを付与する S3 バケットへのアクセス権が付与される場合があります。複数のリージョンでインスタンスプロファイルを使用する場合は、各リージョンの最初の `Statement` ブロックを繰り返すことをお勧めします。

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Effect": "Allow",
                "Action": "s3:GetObject",
                "Resource": [
                    "arn:aws:s3:::aws-windows-downloads-us-east-2/*",
                    "arn:aws:s3:::amazon-ssm-us-east-2/*",
                    "arn:aws:s3:::aws-ssm-us-east-2/*",
                    "arn:aws:s3:::patch-baseline-snapshot-us-east-2/*",
                    "arn:aws:s3:::aws-patch-manager-us-east-2-552881074/*",
                    "arn:aws:s3:::aws-patchmanager-macos-us-east-2-552881074/*"
                ]
            }
        ]
```

```
    }
```

ハードウェアフィンガープリントを使用したハイブリッドアクティベーションマシンの検証

ハイブリッドおよびマルチクラウド環境で非 EC2 を実行する場合、SSM Agent は多数のシステム属性 (ハードウェアハッシュと呼ばれます) を収集し、これらの属性を使用してフィンガープリントを計算します。フィンガープリントは、エージェントが特定の Systems Manager API に渡す不透明な文字列です。この固有のフィンガープリントは、発信者を特定のハイブリッドアクティベーションマネージドノードに関連付けます。エージェントは、フィンガープリントとハードウェアハッシュをローカルディスク上の Vault と呼ばれる場所に保存します。

エージェントは、マシンが Systems Manager で使用するために登録されると、ハードウェアハッシュとフィンガープリントを計算します。エージェントが `RegisterManagedInstance` コマンドを送信すると、フィンガープリントが Systems Manager サービスに戻されます。

その後、`RequestManagedInstanceRoleToken` コマンドを送信するときに、エージェントは Vault 内のフィンガープリントとハードウェアハッシュをチェックして、現在のマシン属性が保存されているハードウェアハッシュと一致することを確認します。現在のマシン属性が Vault に保存されているハードウェアハッシュと一致する場合、エージェントはフィンガープリントを Vault から `RegisterManagedInstance` に渡し、呼び出しが成功します。

現在のマシン属性が保存されているハードウェアハッシュと一致しない場合、SSM Agent は新しいフィンガープリントを計算し、新しいハードウェアハッシュとフィンガープリントを Vault に保存し、新しいフィンガープリントを `RequestManagedInstanceRoleToken` に渡します。これにより *`RequestManagedInstanceRoleToken`* が失敗し、エージェントは Systems Manager サービスに接続するためのロールトークンを取得できません。

この障害は設計上のものであり、複数のマネージドノードが同じマネージドノードとして Systems Manager サービスと通信することを防ぐための検証手順として使用されます。

現在のマシン属性を Vault に保存されているハードウェアハッシュと比較すると、エージェントは次のロジックを使用して、古いハッシュと新しいハッシュが一致するかどうかを判断します。

- SID (システム/マシン ID) が異なる場合は、一致しません。
- 同じ場合は、IP アドレスが同じであれば一致します。
- それ以外の場合は、一致するマシン属性の割合が計算され、ユーザー設定の類似度しきい値と比較され、一致があるかどうかが判断されます。

類似度のしきい値は、ハードウェアハッシュの一部として Vault に保存されます。

類似度のしきい値は、インスタンスの登録後に次のようなコマンドを使用して設定できます。

Linux マシンの場合:

```
sudo amazon-ssm-agent -fingerprint -similarityThreshold 1
```

PowerShell を使用している Windows Server マシンの場合:

```
cd "C:\Program Files\Amazon\SSM\" `
    .\amazon-ssm-agent.exe -fingerprint -similarityThreshold 1
```

> **Important**
>
> フィンガープリントの計算に使用されるコンポーネントの 1 つが変更されると、エージェントが休止状態になる可能性があります。この休止状態を回避するには、類似度のしきい値を低い値 (**1** など) に設定します。

SSM AgentGitHub での

SSM Agent のソースコードが GitHub に用意されているので、ニーズに応じてエージェントを調整できます。含めることを希望する変更について、プルリクエストを送信することをお勧めします。ただし、Amazon Web Services はこのソフトウェアの変更されたコピーの実行をサポートしていません。

SSM Agent がプリインストールされている AMIs を見つける

AWS Systems Manager Agent (SSM Agent) は、AWS および信頼できるサードパーティが提供している一部の Amazon Machine Images (AMIs) にプリインストールされています。

たとえば、次のいずれかのオペレーティングシステムで AMI から作成された Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを起動すると、SSM Agent がすでにインストールされている場合があります。

- AlmaLinux
- 2017 年 9 月以降の Amazon Linux 1 Base AMI
- Amazon Linux 2

- Amazon Linux 2 ECS に最適化されたベース AMIs
- Amazon Linux 2023 (AL2023)
- Amazon EKS 最適化 Amazon Linux AMIs
- macOS 10.14.x (Mojave)、10.15.x (Catalina)、11.x (Big Sur)、12.x (Monterey)、13.x (Ventura)、14.x (Sonoma)、および 15.x (Sequoia)
- SUSE Linux Enterprise Server(SLES) 12 と 15
- Ubuntu Server 16.04、18.04、20.04、および 22.04
- 2016 年 11 月以降に公開された Windows Server 2008-2012 R2 AMIs
- Windows Server 2016、2019、2022 (Nano バージョンを除く)、および 2025

> **Note**
>
> AMI にプリインストールされている SSM Agent のバージョンが利用可能な最新バージョンではない可能性があります。ベストプラクティスとして、マネージドノードで常に最新バージョンの SSM Agent を使用することをお勧めします。SSM Agent 更新の自動化の詳細については、「SSM Agent への更新の自動化」を参照してください。
> このリストに含まれていない AWS マネージド AMIs には、SSM Agent が事前インストールされている場合があります。つまり一般的には、Systems Manager のすべてのツールで、オペレーティングシステム (OS) が完全にサポートされているわけではないことになります。また、AWS Marketplace またはコミュニティ AMIs リポジトリにある AMIs に、SSM Agent が事前インストールされている場合もあります。ただし AWS では、これらの AMIs をサポートしていません。

SSM Agent のステータスを確認する

上記のリストにある AMI から作成されたインスタンスには、その初期化の時期によって、SSM Agent が事前インストールされていない場合があります。さらに、インスタンスにエージェントが事前インストールされていても、そのエージェントが実行されていない場合もあり得ます。そのため、インスタンスで Systems Manager を初めて使用する際には、先に SSM Agent のステータスを確認することをお勧めします。

SSM Agent がインストール済みで、かつインスタンスで実行されていることを確認するには、次の手順を使用します。インストール済みのエージェントがみつからない場合は、手動で、Linux、macOS、および Windows Server のインスタンスにインストールできます。

インスタンスで SSM Agent のインストールを確認するには

1. 新しいインスタンスを起動すると、初期化されるまで数分待ちます。
2. 好みの方法を使用してインスタンスに接続します。たとえば、SSH を使用して Linux インスタンスに接続したり、リモートデスクトップを使用して Windows Server インスタンスに接続したりできます。
3. インスタンスのオペレーティングシステムタイプに対応するコマンドを実行し、SSM Agent の状態を確認します。

オペレーティングシステム	コマンド
Amazon Linux 1	`sudo status amazon-ssm-agent`
Amazon Linux 2 および Amazon Linux 2023	`sudo systemctl status amazon-ssm-agent`
macOS	macOS で SSM Agent 状態を確認するコマンドはありません。エージェント ログファイル `/var/log/amazon/ssm/amazon-ssm-agent.log` を見つけて評価することでステータスを確認できます。
SUSE Linux Enterprise Server	`sudo systemctl status amazon-ssm-agent`
Ubuntu Server (32 ビット)	`sudo status amazon-ssm-agent`
Ubuntu Server (64 ビット - Deb)	`sudo systemctl status amazon-ssm-agent`
Ubuntu Server (64 ビット - Snap)	`sudo systemctl status snap.amazon-ssm-agent.amazon-ssm-agent.service`
Windows Server	`Get-Service AmazonSSMAgent`

> **Tip**
>
> Systems Manager でサポートされているすべてのオペレーティングシステムタイプの SSM Agent 状態を確認するコマンドを表示するには、「SSM Agent ステータスの確認とエージェントの起動」を参照してください。

4. コマンド出力を評価して、SSM Agent の状態を確認します。

   状態: インストール済みおよび実行中

   ほとんどの場合、コマンド出力は、エージェントがインストールされ、実行中であることを示します。

   次の例は、SSM Agent が Amazon Linux 2 インスタンスにインストールされ、実行されていることを示しています。

   ```
   amazon-ssm-agent.service - amazon-ssm-agent
   Loaded: loaded (/usr/lib/systemd/system/amazon-ssm-agent.service; enabled; vendor
    preset: enabled)
   Active: active (running) since Wed 2021-10-20 19:09:29 UTC; 4min 6s ago
   --truncated--
   ```

   次の例は、SSM Agent が Windows Server インスタンスにインストールされ、実行されていることを示しています。

   ```
   Status   Name               DisplayName
   ------   ----               -----------
   Running  AmazonSSMAgent     Amazon SSM Agent
   ```

   状態: インストール済みですが、実行されていません

   場合によっては、コマンド出力は、エージェントがインストールされているが、実行されていないことを示します。

   次の例は、SSM Agent が Amazon Linux 2 インスタンスにインストールされているが、実行されていないことを示しています。

```
amazon-ssm-agent.service - amazon-ssm-agent
Loaded: loaded (/usr/lib/systemd/system/amazon-ssm-agent.service; enabled; vendor
 preset: enabled)
Active: inactive (dead) since Wed 2021-10-20 22:16:41 UTC; 18s ago
--truncated--
```

次の例は、SSM Agent が Windows Server インスタンスにインストールされているが実行されていないことを示しています。

```
Status   Name               DisplayName
------   ----               -----------
Stopped  AmazonSSMAgent     Amazon SSM Agent
```

エージェントがインストールされていても実行されていない場合は、インスタンスのオペレーティングシステムタイプのコマンドを使用して、手動でアクティブ化できます。

オペレーティングシステム	コマンド
Amazon Linux 1	`sudo start amazon-ssm-agent`

Amazon Linux 2 および Amazon Linux 2023	`sudo systemctl enable amazon-ssm-agent`
	
	`sudo systemctl start amazon-ssm-agent`

macOS	`sudo launchctl load -w /Library/LaunchDaemons/com.amazon.aws.ssm.plist`
	
	`sudo launchctl start com.amazon.aws.ssm`

オペレーティングシステム	コマンド

SUSE Linux Enterprise Server	`sudo systemctl enable amazon-ssm-agent`
	
	`sudo systemctl start amazon-ssm-agent`

Ubuntu Server (32 ビット)	`sudo start amazon-ssm-agent`

Ubuntu Server (64 ビット - Deb)	`sudo systemctl enable amazon-ssm-agent`
	
	`sudo systemctl start amazon-ssm-agent`

Ubuntu Server (64 ビット - Snap)	`sudo snap start amazon-ssm-agent`
Windows Server	PowerShell で、次のコマンドを実行します。 `Start-Service AmazonSSMAgent`

状態: インストールされていません

場合によっては、コマンド出力は、エージェントがインストールされていないことを示します。

次の例は、SSM Agent が Amazon Linux 2 インスタンスにインストールされていないことを示しています。

```
Unit amazon-ssm-agent.service could not be found.
```

次の例は、SSM Agent が Windows Server インスタンスにインストールされていないことを示しています。

```
Get-Service : Cannot find any service with service name 'AmazonSSMAgent'.
--truncated--
```

エージェントがインストールされていない場合は、オペレーティングシステムタイプの手順を使用して、手動でインストールできます。

- Linux 用 EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする
- macOS 用の EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする
- Windows Server 用の EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする

Linux 用 EC2 インスタンスで SSM Agent を使用する

AWS Systems Manager Agent (SSM Agent) は Systems Manager リクエストを処理し、リクエストに指定されたとおりにマシンを設定します。次のトピックの手順を使用して、Linux オペレーティングシステムで SSM Agent のインストール、設定、アンインストールを実行します。

トピック

- SSM Agent の署名の確認
- Linux 用 EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする
- Linux ノードでプロキシを使用するための SSM Agent の設定

SSM Agent の署名の確認

Linux インスタンス用の AWS Systems Manager Agent (SSM Agent) deb および rpm インストーラーパッケージは、暗号化で署名されています。パブリックキーを使用して、エージェントのパッケージがオリジナルであり、変更されていないことを確認できます。ファイルが損傷していたり、改変されていた場合、検証は失敗します。RPM または GPG を使用して、インストーラーパッケージの署名を確認できます。以下の情報は SSM Agent バージョン 3.1.1141.0 以降のものです。

インスタンスのアーキテクチャとオペレーティングシステムに適した署名ファイルを検索するには、次の表を参照してください。

region は、米国東部 (オハイオ) リージョンの `us-east-2` のように、AWS Systems Manager でサポートされている AWS リージョン の識別子を表します。サポートされている *region* 値の一覧については、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」にある Region 列を参照してください。

アーキテクチャ	オペレーティングシステム	署名ファイルの URL	エージェントダウンロードファイル名

x86_64	AlmaLinux、Amazon Linux 1、Amazon Linux 2、Amazon Linux 2023、CentOS、CentOS Stream、RHEL、Oracle Linux、Rocky Linux、SLES	`https://s3.region.amazonaws.com/amazon-ssm-region/latest/linux_amd64/amazon-ssm-agent.rpm.sig`
		
		`https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/linux_amd64/amazon-ssm-agent.rpm.sig`
			`amazon-ssm-agent.rpm`

x86_64	Debian Server, Ubuntu Server	`https://s3.region.amazonaws.com/amazon-ssm-region/latest/debian_amd64/amazon-ssm-agent.deb.sig`
		
		`https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/`
			`amazon-ssm-agent.deb`

アーキテクチャ	オペレーティングシステム	署名ファイルの URL	エージェントダウンロードファイル名
		debian_amd64/amazon-ssm-agent.deb.sig	
x86	Amazon Linux 1、Amazon Linux 2、Amazon Linux 2023、CentOS、RHEL	https://s3.*region*.amazonaws.com/amazon-ssm-*region*/latest/linux_386/amazon-ssm-agent.rpm.sig https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/linux_386/amazon-ssm-agent.rpm.sig	amazon-ssm-agent.rpm

アーキテクチャ	オペレーティングシステム	署名ファイルの URL	エージェントダウンロードファイル名
x86	Ubuntu Server	https://s3. *region*.amazonaws.com/amazon-ssm-*region*/latest/debian_386/amazon-ssm-agent.deb.sig https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/debian_386/amazon-ssm-agent.deb.sig	amazon-ssm-agent.deb

アーキテクチャ	オペレーティングシステム	署名ファイルの URL	エージェントダウンロードファイル名

ARM64	Amazon Linux 1、Amazon Linux 2、Amazon Linux 2023、CentOS、RHEL	`https://s3.region.amazonaws.com/amazon-ssm-region/latest/linux_arm64/amazon-ssm-agent.rpm.sig`
		
		`https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/linux_arm64/amazon-ssm-agent.rpm.sig`
			`amazon-ssm-agent.rpm`

Linux サーバーでの SSM Agent パッケージの検証 (v3.3.1802.0 以降)

[開始する前に]

このセクションの GPG と RPM の手順は、SSM Agent バージョン 3.3.1802.0 以降に適用されます。以下の手順を使用して SSM Agent の署名を検証する前に、オペレーティングシステム用の最新のエージェントパッケージがダウンロードされていることを確認してください。例えば、`https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/linux_arm64/amazon-ssm-agent.rpm` と指定します。SSM Agent パッケージのダウンロードの詳細については、「Linux 用 EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする」を参照してください。

エージェントバージョン 3.3.1611.0 以前を引き続き使用する理由がある場合は、代わりに「Linux サーバー (v3.3.1611.0 以前) での SSM Agent パッケージの検証」の手順に従います。

GPG

Linux サーバー (v3.3.1802.0 以降) で SSM Agent パッケージを検証するには

1. 次のパブリックキーの 1 つをコピーし、amazon-ssm-agent.gpg という名前のファイルに保存します。

> **Important**
>
> 次のパブリックキーは 2026-07-15 (2026 年 7 月 15 日) に期限切れになります。Systems Manager は、古いパブリックキーの有効期限が切れる前に、このトピックで新しいパブリックキーを発行します。このトピックの RSS フィードにサブスクライブして、新しいキーが利用可能になったときに通知を受け取ることをお勧めします。

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2.0.22 (GNU/Linux)

mQINBGeRNq4BEACrlf5h6Pz+k+M+QCJJ2LfK7d2Tn9J8iJ9qBK2Vwvuxco1rpSO+
KEI3nTeysPuheximps8WOCADX4VlbsKxMZQLjQM4mA26m1Tiw9nAI4kod4bKjiuM
BMUTCD1wfnjH3zQi4kDUdbpfAEMiPgNLVLH85Wf+lhK+Zm+V38DYzLyVj03kX4wK
iG6RMoxzOBZa5gNsVq+j+oCUITGz/URxH713Rgo8WeoEegI0+7iCBLKg+PM0b7GV
2nzkwWJz796HdkqSg8BwXsYaLTrHxa2P1IpwPCisAkyO7gZaMd6Uj69dtMFO+V8a
Qee6b57qGuFKZw7h1Vvc85PbF1Gy/wNIpary57kUHBFUg1vYep/roJuEbJCq97r5
I2liLl4NAyrWb9r/TAVxlXvqM4iZUhxm8GAp0FywMdBr9ZECClKa5HxuVmlm0Wgl
TXoYTOZKeDg6ZoCvyhNxWneCNip74fohXymeFF5L/budhBwy5wuwSniOgTGLo/4C
VgZHWCcN+d0Q3bx/sl2QNqPg5/xzsxEtymXLdVdwLIsLdEQUnIvy8KTs5jol3Dwi
nnEEyhly6wdaw+qDOhkSOT/VnErrSMkYF8VJfa5GjhCBWKw9JVSkaP2CI/VHOgHM
MKROnulq0hRQBR7RmLYt98xu38BHJWMmF8Ga/HJuIxzD1VmkZOPvDDESUwARAQAB
tCdTU00gQWdlbnQgPHNzbS1hZ2VudC1zaWduZXJAYW1hem9uLmNvbT6JAj8EEwEC
ACkFAmeRNq4CGy8FCQLGmIAHCwkIBwMCAQYVCAIJCgsEFgIDAQIeAQIXgAAKCRBR
qOBQ0AUuXTdND/9qldQ1E3dYjBVXOnbhiUQL594bkS5VoEX7D4fZ5UMVZa5pGiz+
husnoRUS9rH1cSeq7aHJu9hSCMuMdvRpuoo0CwLB+7HtzJvAO2M01hcEkUYa6Qdj
njTzP0ZjnoenJmqF9SYmVqAI/VPa9mNQ1OJ+HQ3qh5i6w+FoWlVqEdXjZGrWijub
TqyN33i1Y26t7Os/x8I9fUeNx37y/7Kama8LTdtv9GhWiMVBg2IuVf27HCMYofrQ
m2uCGe61IhtsnhsYaYupmljl+6qgdiuCiS9BAsoIGtqTnu8lnKcGyGz6YnRszN+U
1bNE4w+UFpXWJF8ogpYcghJ06aW/LhjZnQSx3VliLdW8eOJzou41yWmiuL3ZY8eW
KAlD+7eYKS6N6fEJCeNO2VX2lcKtDfaOX+lqGIVyexKayMfpi+0frNzt/92YCpF5
3jkeS77vMMVqKIUiIp1OCGv3XsFpIr6Bt2c2throYPDoQL3zvq6vvG40BKeRQ4tT
Y+5vTc8MeNn3LdzTl9pusxTcKifrJq7f5FIsL2CpAX8uQ+Qz+XWsYQQ5PvyUDtOz
```

```
nU/MRZaP6HnqY42bzI9ZlKgXi9IE3MXIwoET9YyzFjkIDvat7SlB4uJCpeIqp/KM
OIrTMb7paGLYmBU6YqxNBkDWItNG7NeZzyhh/R/Qqb4vJaf4S+ZqD1RZXokCHAQQ
AQIABgUCZ5E2rwAKCRB90Jej2tf1/CdnD/46It+RNoE00TesZK5n2bijH5Eljw0E
4/UpMi1SV6t2zY7lIm7TcKNn18tynJNFqB6YXXOwSbBG/fbN2E9RaoUCZw23TmAv
amuHwrfsDqsHb7zzPF0bISYjqEDLQJj/gtEugUc6XY1dEpFSlWJIOvgryG04cFXI
uD2KY87ya4s1R+sEVAJ14K4RlUCiMmzJdR0NJNYJOwBi1gkLEp6jG86ttiG2U7fY
pE2ibV+c0GeIFq8PIzqqENsn9KBuRH5EcbdBwfnsj2XfM4aR3ZtRIdWXkKkdP9Rs
yU5dTF/Y7XPId5h8/gp00+DMlXFBinQ1jE7A7eDYviEFd1ba8P7dIom3Q3gzKiWu
KTGpnykShs5NvpQmvGUF6JqDHI4RK9s3kLqsNyZkhenJfRBrJ/45fQAuP4CRedkF
7PSfX0Xp7kDnKuyK6wEUEfXXrqmuLGDmigTXblO5qgdyMwkOLjiY9znBZbHoKs76
VplOoNgGnN19i3nuMcPf2npFICJv7kTIyn5Fh7pjWDCahl3U/PwoLjrrlEzpyStU
oXSZrK3kiAADEdSODXJl8KYU0Pb27JbRr1ZbWnxb+O39TOhtssstulkR0v+IDGDQ
rQE1b12sKgcNFSzInzWrNGu4S06WN8DYzlrTZ9aSHj+37ZqpXAevi8WOFXKPV3PA
E6+O8RI2451Dcg==
=aDkv
-----END PGP PUBLIC KEY BLOCK-----
```

2. パブリックキーをキーリングにインポートし、返されたキー値をメモします。

```
gpg --import amazon-ssm-agent.gpg
```

3. フィンガープリントを確認します。*key-value* は、前の手順の値に置き換えてください。RPM を使用してインストーラーパッケージを確認する場合でも、GPG を使用してフィンガープリントを確認することをお勧めします。

```
gpg --fingerprint key-value
```

このコマンドは、次のような出力を返します：

```
pub   4096R/D0052E5D 2025-01-22 [expires: 2026-07-15]
      Key fingerprint = 4855 A9E6 8332 16D6 A77D  8FE4 51A8 E050 D005 2E5D
uid                  SSM Agent <ssm-agent-signer@amazon.com>
```

フィンガープリントは、次のものと一致する必要があります。

```
4855 A9E6 8332 16D6 A77D 8FE4 51A8 E050 D005 2E5D
```

フィンガープリントが一致しない場合は、エージェントをインストールしないでください。に連絡しますAWS サポート

4. インスタンスのアーキテクチャとオペレーティングシステムに従って署名ファイルをダウンロードします (まだ実行していない場合)。

5. インストーラパッケージの署名を確認します。*signature-filename* および *agent-download-filename* は、このトピックで前述したように、署名ファイルおよびエージェントをダウンロードするときに指定した値に置き換えてください。

```
gpg --verify signature-filename agent-download-filename
```

例えば、Amazon Linux 2 の x86_64 アーキテクチャ:

```
gpg --verify amazon-ssm-agent.rpm.sig amazon-ssm-agent.rpm
```

このコマンドは、次のような出力を返します :

```
gpg: Signature made Sat 08 Feb 2025 12:05:08 AM UTC using RSA key ID D0052E5D
gpg: Good signature from "SSM Agent <ssm-agent-signer@amazon.com>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 4855 A9E6 8332 16D6 A77D  8FE4 51A8 E050 D005 2E5D
```

出力結果に「BAD signature」という句が含まれる場合、手順が正しいことをもう一度確認してください。この応答が続く場合は、サポート に連絡し、エージェントをインストールしないでください。信頼に関する警告メッセージは、署名が無効であることを意味するものではなく、パブリックキーを検証していないことを示すだけです。キーは、自分や信頼する人が署名した場合にのみ信頼できます。出力にフレーズ Can't check signature: No public key が含まれている場合、SSM Agent バージョン 3.1.1141.0 以降をダウンロードしたことを確認します。

RPM

Linux サーバー (v3.3.1802.0 以降) で SSM Agent パッケージを検証するには

1. 次のパブリックキーをコピーし、amazon-ssm-agent.gpg という名前のファイルに保存します。

> **Important**
>
> 次のパブリックキーは 2026-07-15 (2026 年 7 月 15 日) に期限切れになります。Systems Manager は、古いパブリックキーの有効期限が切れる前に、このトピックで新しいパブリックキーを発行します。このトピックの RSS フィードにサブ

スクライブして、新しいキーが利用可能になったときに通知を受け取ることをお勧めします。

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2.0.22 (GNU/Linux)

mQINBGeRNq4BEACrlf5h6Pz+k+M+QCJJ2LfK7d2Tn9J8iJ9qBK2Vwvuxco1rpSO+
KEI3nTeysPuheximps8WOCADX4VlbsKxMZQLjQM4mA26m1Tiw9nAI4kod4bKjiuM
BMUTCD1wfnjH3zQi4kDUdbpfAEMiPgNLVLH85Wf+lhK+Zm+V38DYzLyVj03kX4wK
iG6RMoxzOBZa5gNsVq+j+oCUITGz/URxH713Rgo8WeoEegI0+7iCBLKg+PM0b7GV
2nzkwWJz796HdkqSg8BwXsYaLTrHxa2P1IpwPCisAkyO7gZaMd6Uj69dtMFO+V8a
Qee6b57qGuFKZw7h1Vvc85PbF1Gy/wNIpary57kUHBFUg1vYep/roJuEbJCq97r5
I2liLl4NAyrWb9r/TAVxlXvqM4iZUhxm8GAp0FywMdBr9ZECClKa5HxuVmlm0Wgl
TXoYTOZKeDg6ZoCvyhNxWneCNip74fohXymeFF5L/budhBwy5wuwSniOgTGLo/4C
VgZHWCcN+d0Q3bx/sl2QNqPg5/xzsxEtymXLdVdwLIsLdEQUnIvy8KTs5jol3Dwi
nnEEyhly6wdaw+qDOhkSOT/VnErrSMkYF8VJfa5GjhCBWKw9JVSkaP2CI/VHOgHM
MKROnulq0hRQBR7RmLYt98xu38BHJWMmF8Ga/HJuIxzD1VmkZOPvDDESUwARAQAB
tCdTU00gQWdlbnQgPHNzbS1hZ2VudC1zaWduZXJAYW1hem9uLmNvbT6JAj8EEwEC
ACkFAmeRNq4CGy8FCQLGmIAHCwkIBwMCAQYVCAIJCgsEFgIDAQIeAQIXgAAKCRBR
qOBQ0AUuXTdND/9qldQ1E3dYjBVXOnbhiUQL594bkS5VoEX7D4fZ5UMVZa5pGiz+
husnoRUS9rH1cSeq7aHJu9hSCMuMdvRpuoo0CwLB+7HtzJvAO2M01hcEkUYa6Qdj
njTzP0ZjnoenJmqF9SYmVqAI/VPa9mNQ1OJ+HQ3qh5i6w+FoWlVqEdXjZGrWijub
TqyN33i1Y26t7Os/x8I9fUeNx37y/7Kama8LTdtv9GhWiMVBg2IuVf27HCMYofrQ
m2uCGe61IhtsnhsYaYupmljl+6qgdiuCiS9BAsoIGtqTnu8lnKcGyGz6YnRszN+U
1bNE4w+UFpXWJF8ogpYcghJ06aW/LhjZnQSx3VliLdW8eOJzou41yWmiuL3ZY8eW
KAlD+7eYKS6N6fEJCeNO2VX2lcKtDfaOX+lqGIVyexKayMfpi+0frNzt/92YCpF5
3jkeS77vMMVqKIUiIp1OCGv3XsFpIr6Bt2c2throYPDoQL3zvq6vvG40BKeRQ4tT
Y+5vTc8MeNn3LdzTl9pusxTcKifrJq7f5FIsL2CpAX8uQ+Qz+XWsYQQ5PvyUDtOz
nU/MRZaP6HnqY42bzI9ZlKgXi9IE3MXIwoET9YyzFjkIDvat7SlB4uJCpeIqp/KM
OIrTMb7paGLYmBU6YqxNBkDWItNG7NeZzyhh/R/Qqb4vJaf4S+ZqD1RZXokCHAQQ
AQIABgUCZ5E2rwAKCRB90Jej2tf1/CdnD/46It+RNoE00TesZK5n2bijH5Eljw0E
4/UpMi1SV6t2zY7lIm7TcKNn18tynJNFqB6YXXOwSbBG/fbN2E9RaoUCZw23TmAv
amuHwrfsDqsHb7zzPF0bISYjqEDLQJj/gtEugUc6XY1dEpFSlWJIOvgryG04cFXI
uD2KY87ya4s1R+sEVAJ14K4RlUCiMmzJdR0NJNYJOwBi1gkLEp6jG86ttiG2U7fY
pE2ibV+c0GeIFq8PIzqqENsn9KBuRH5EcbdBwfnsj2XfM4aR3ZtRIdWXkKkdP9Rs
yU5dTF/Y7XPId5h8/gp00+DMlXFBinQ1jE7A7eDYviEFd1ba8P7dIom3Q3gzKiWu
KTGpnykShs5NvpQmvGUF6JqDHI4RK9s3kLqsNyZkhenJfRBrJ/45fQAuP4CRedkF
7PSfX0Xp7kDnKuyK6wEUEfXXrqmuLGDmigTXblO5qgdyMwkOLjiY9znBZbHoKs76
VplOoNgGnN19i3nuMcPf2npFICJv7kTIyn5Fh7pjWDCahl3U/PwoLjrrlEzpyStU
oXSZrK3kiAADEdSODXJl8KYU0Pb27JbRr1ZbWnxb+O39TOhtssstulkR0v+IDGDQ
rQE1b12sKgcNFSzInzWrNGu4S06WN8DYzlrTZ9aSHj+37ZqpXAevi8WOFXKPV3PA
```

```
E6+08RI2451Dcg==
=aDkv
-----END PGP PUBLIC KEY BLOCK-----
```

2. パブリックキーをキーリングにインポートし、返されたキー値をメモします。

```
rpm --import amazon-ssm-agent.gpg
```

3. フィンガープリントを確認します。RPM を使用してインストーラーパッケージを確認する場合でも、GPG を使用してフィンガープリントを確認することをお勧めします。

```
rpm -qa gpg-pubkey --qf '%{Description}' | gpg --with-fingerprint | grep -A 1
 "ssm-agent-signer@amazon.com"
```

このコマンドは、次のような出力を返します：

```
pub  4096R/D0052E5D 2025-01-22 SSM Agent <ssm-agent-signer@amazon.com>
      Key fingerprint = 4855 A9E6 8332 16D6 A77D  8FE4 51A8 E050 D005 2E5D
```

フィンガープリントは、次のものと一致する必要があります。

```
4855 A9E6 8332 16D6 A77D 8FE4 51A8 E050 D005 2E5D
```

フィンガープリントが一致しない場合は、エージェントをインストールしないでください。に連絡しますAWS サポート

4. インストーラパッケージの署名を確認します。*agent-download-filename* は、このトピックの表で前述したように、エージェントをダウンロードするときに指定した値に置き換えてください。

```
rpm --checksig agent-download-filename
```

例えば、Amazon Linux 2 の x86_64 アーキテクチャ:

```
rpm --checksig amazon-ssm-agent.rpm
```

このコマンドは、次のような出力を返します。

```
amazon-ssm-agent.rpm: rsa sha1 md5 OK
```

pgp が出力に存在せず、パブリックキーをインポートした場合、エージェントは署名されません。出力にフレーズ NOT OK (MISSING KEYS: (MD5) *key-id*) が含まれている場合、手順が正しいことを再度確認し、SSM Agent バージョン 3.1.1141.0 以降をダウンロードしたことを確認します。この応答が続く場合は、サポート に連絡し、エージェントをインストールしないでください。

Linux サーバー (v3.3.1611.0 以前) での SSM Agent パッケージの検証

[開始する前に]

このセクションの GPG および RPM の手順は、SSM Agent バージョン 3.3.1611.0 以前のバージョンに適用されます。常に、エージェントの最新バージョンを使用することをお勧めします。詳細については、Linux サーバーでの SSM Agent パッケージの検証 (v3.3.1802.0 以降) を参照してください。ただし、エージェントバージョン 3.3.1611.0 以前を引き続き使用する特別な理由がある場合は、次のいずれかの手順に従います。

GPG

Linux サーバー (v3.3.1611.0 以前) で SSM Agent パッケージを検証するには

1. 次のパブリックキーをコピーし、amazon-ssm-agent.gpg という名前のファイルに保存します。

> **Important**
>
> 以下に示すパブリックキーは 2025-02-17 (2025 年 2 月 17 日) に有効期限が切れ、バージョン 3.3.1611.0 以前のバージョン 3.2.1542.0 までで動作します。これは、以前にエージェントの署名を検証するために使用されていた場合のみです。Systems Manager は、古いパブリックキーの有効期限が切れる前に、このトピックで新しいパブリックキーを発行します。このトピックの RSS フィードにサブスクライブして、新しいキーが利用可能になったときに通知を受け取ることをお勧めします。

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2.0.22 (GNU/Linux)

mQENBGTtIoIBCAD2M1aoGIE0FXynAHM/jtuvdAVVaX3Q4ZejTqrX+Jq8ElAMhxyO
GzHu2CDtCYxtVxXK3unptLVt2kGgJwNbhYC393jDeZx5dCda4Nk2YXX1UK3P461i
```

```
axuuXRzMYvfM4RZn+7bJTu635tA07q9Xm6MGD4TCTvsjBfViOxbrxOg5ozWbJdSw
fSR8MwUrRfmFpAefRlYfCEuZ8FHywa9U6jLeWt2O/kqrZliJOAGjGzXtB7EZkqKb
faCCxikjjvhF1awdEqSK4DQorC/OvQc4I5kP5y2CJbtXvXO73QH2yE75JMDIIx9x
rOsIRUoSfK3UrWaOVuAnEEn5ueKzZNqGG1J1ABEBAAG0J1NTTSBBZ2VudCA8c3Nt
LWFnZW50LXNpZ25lckBhbWF6b24uY29tPokBPwQTAQIAKQUCZO0iggIbLwUJAsaY
gAcLCQgHAwIBBhUIAgkKCwQWAgMBAh4BAheAAAoJELwfSVyX3QTt+icH/A//tJsW
I+7Ay8FGJh8dJPNy++HIBjVSFdGNJFWNbw1Z8uZcazHEcUCH3FhW4CLQLTZ3OVPz
qvFwzDtRDVIN/Y9EGDhLMFvimrE+/z4olWsJ5DANf6BnX8I5UNIcRt5d8SWH1BEJ
2FWIBZFgKyTDI6XzRC5x4ahtgpOVAGeeKDehs+wh6Ga4W0/K4GsviP1Kyr+Ic2br
NAIq0q0IHyN1q9zam3Y0+jKwEuNmTj+Bjyzshyv/X8S0JWWoXJhkexkOvWeBYNNt
5wI4QcSteyfIzp6KlQF8q11Hzz9D9WaPfcBEYyhq7vLEARobkbQMBzpkmaZua241
0RaWG50HRvrgm4aJAhwEEAECAAYFAmTtIoMACgkQfdCXo9rX9fwwqBAAzkTgYJ38
sWgxpn7Ux/81F2BWR1sVkmP79i++fXyJlKI8xtcJFQZhzeUos69KBUCy7mgx5bYU
P7NA5o9DUbwz/QS0i1Cqm4+jtFlX0MXe4FikXcqfDPnnzN8mVB2H+fa43iHR1PuH
GgUWuNdxzSoIYRmLZXWmeN5YXPcmixlhLzcE2TOQn1mOKcu2fKdLtBQ8KiEkmjiu
naoLxnUcyk1zMhaha+LzEkQdOyasix0ggylN2ViWVnlmfy0niuXDxW0qZWPdLStF
OODiX3iqGmkH3rDfy6nvxxBR4GIs+MGD72fpWzzrINDgkGI2i2t1+0AX/mps3aTy
+ftlgrim8stYWB58XXDAb0vad06sNye5/zDzfr0I9HupJrTzFhaYJQjWPaSlINto
LDJnBXohiUIPRYRcy/k012oFHDWZHT3H6CyjK9UD5UlxA9H7dsJurANs6FOVRe+7
34uJyxDZ/W7zLG4AVG0zxibrUSoaJxwcOjVPVsQAlrwG/GTs7tcAccsJqbJ1Py/w
9AgJl8VU2qc8POsHNXk348gjP7C8PDnGMpZFzr9f5INctRushpiv7onX+aWJVX7T
n2uX/TP3LCyH/MsrNJrJOQnMYFRLQitciP0E+F+eA3v9CY6mDuyb8JSx5HuGGUsG
S4bKBOcA8vimEpwPoT8CE7fdsZ3Qkwdu+pw=
=zr5w
-----END PGP PUBLIC KEY BLOCK-----
```

2. パブリックキーをキーリングにインポートし、返されたキー値をメモします。

```
gpg --import amazon-ssm-agent.gpg
```

3. フィンガープリントを確認します。*key-value* は、前の手順の値に置き換えてください。RPM を使用してインストーラーパッケージを確認する場合でも、GPG を使用してフィンガープリントを確認することをお勧めします。

```
gpg --fingerprint key-value
```

このコマンドは、次のような出力を返します。

```
pub   2048R/97DD04ED 2023-08-28 [expired: 2025-02-17]
      Key fingerprint = DE92 C7DA 3E56 E923 31D6 2A36 BC1F 495C 97DD 04ED
uid                  SSM Agent <ssm-agent-signer@amazon.com>
```

フィンガープリントは、次のものと一致する必要があります。

```
DE92 C7DA 3E56 E923 31D6 2A36 BC1F 495C 97DD 04ED
```

フィンガープリントが一致しない場合は、エージェントをインストールしないでください。に連絡しますAWS サポート

4. インスタンスのアーキテクチャとオペレーティングシステムに従って署名ファイルをダウンロードします (まだ実行していない場合)。
5. インストーラパッケージの署名を確認します。*signature-filename* および *agent-download-filename* は、このトピックで前述したように、署名ファイルおよびエージェントをダウンロードするときに指定した値に置き換えてください。

```
gpg --verify signature-filename agent-download-filename
```

例えば、Amazon Linux 2 の x86_64 アーキテクチャ:

```
gpg --verify amazon-ssm-agent.rpm.sig amazon-ssm-agent.rpm
```

このコマンドは、次のような出力を返します :

```
gpg: Signature made Fri 10 Jan 2025 01:54:18 AM UTC using RSA key ID 97DD04ED
gpg: Good signature from "SSM Agent <ssm-agent-signer@amazon.com>"
gpg: Note: This key has expired!
Primary key fingerprint: DE92 C7DA 3E56 E923 31D6  2A36 BC1F 495C 97DD 04ED
```

出力結果に「BAD signature」という句が含まれる場合、手順が正しいことをもう一度確認してください。この応答が続く場合は、サポート に連絡し、エージェントをインストールしないでください。信頼に関する警告メッセージは、署名が無効であることを意味するものではなく、パブリックキーを検証していないことを示すだけです。キーは、自分や信頼する人が署名した場合にのみ信頼できます。出力にフレーズ Can't check signature: No public key が含まれている場合、SSM Agent バージョン 3.1.1141.0 以降をダウンロードしたことを確認します。

RPM

Linux サーバー (v3.3.1611.0 以前) で SSM Agent パッケージを検証するには

1. 次のパブリックキーをコピーし、amazon-ssm-agent.gpg という名前のファイルに保存します。

> **Important**
>
> 以下に示すパブリックキーは 2025-02-17 (2025 年 2 月 17 日) に有効期限が切れ、バージョン 3.3.1611.0 以前のバージョン 3.2.1542.0 までで動作します。これは、以前にエージェントの署名を検証するために使用されていた場合のみです。Systems Manager は、古いパブリックキーの有効期限が切れる前に、このトピックで新しいパブリックキーを発行します。このトピックの RSS フィードにサブスクライブして、新しいキーが利用可能になったときに通知を受け取ることをお勧めします。

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2.0.22 (GNU/Linux)

mQENBGTtIoIBCAD2M1aoGIE0FXynAHM/jtuvdAVVaX3Q4ZejTqrX+Jq8ElAMhxyO
GzHu2CDtCYxtVxXK3unptLVt2kGgJwNbhYC393jDeZx5dCda4Nk2YXX1UK3P461i
axuuXRzMYvfM4RZn+7bJTu635tA07q9Xm6MGD4TCTvsjBfViOxbrxOg5ozWbJdSw
fSR8MwUrRfmFpAefRlYfCEuZ8FHywa9U6jLeWt2O/kqrZliJOAGjGzXtB7EZkqKb
faCCxikjjvhF1awdEqSK4DQorC/OvQc4I5kP5y2CJbtXvXO73QH2yE75JMDIIx9x
rOsIRUoSfK3UrWaOVuAnEEn5ueKzZNqGG1J1ABEBAAG0J1NTTSBBZ2VudCA8c3Nt
LWFnZW50LXNpZ25lckBhbWF6b24uY29tPokBPwQTAQIAKQUCZO0iggIbLwUJAsaY
gAcLCQgHAwIBBhUIAgkKCwQWAgMBAh4BAheAAAoJELwfSVyX3QTt+icH/A//tJsW
I+7Ay8FGJh8dJPNy++HIBjVSFdGNJFWNbw1Z8uZcazHEcUCH3FhW4CLQLTZ3OVPz
qvFwzDtRDVIN/Y9EGDhLMFvimrE+/z4olWsJ5DANf6BnX8I5UNIcRt5d8SWH1BEJ
2FWIBZFgKyTDI6XzRC5x4ahtgpOVAGeeKDehs+wh6Ga4W0/K4GsviP1Kyr+Ic2br
NAIq0q0IHyN1q9zam3Y0+jKwEuNmTj+Bjyzshyv/X8S0JWWoXJhkexkOvWeBYNNt
5wI4QcSteyfIzp6KlQF8q11Hzz9D9WaPfcBEYyhq7vLEARobkbQMBzpkmaZua241
0RaWG50HRvrgm4aJAhwEEAECAAYFAmTtIoMACgkQfdCXo9rX9fwwqBAAzkTgYJ38
sWgxpn7Ux/81F2BWR1sVkmP79i++fXyJlKI8xtcJFQZhzeUos69KBUCy7mgx5bYU
P7NA5o9DUbwz/QS0i1Cqm4+jtFlX0MXe4FikXcqfDPnnzN8mVB2H+fa43iHR1PuH
GgUWuNdxzSoIYRmLZXWmeN5YXPcmixlhLzcE2TOQn1mOKcu2fKdLtBQ8KiEkmjiu
naoLxnUcyk1zMhaha+LzEkQdOyasix0ggylN2ViWVnlmfy0niuXDxW0qZWPdLStF
OODiX3iqGmkH3rDfy6nvxxBR4GIs+MGD72fpWzzrINDgkGI2i2t1+0AX/mps3aTy
+ftlgrim8stYWB58XXDAb0vad06sNye5/zDzfr0I9HupJrTzFhaYJQjWPaSlINto
LDJnBXohiUIPRYRcy/k012oFHDWZHT3H6CyjK9UD5UlxA9H7dsJurANs6FOVRe+7
```

```
34uJyxDZ/W7zLG4AVG0zxibrUSoaJxwcOjVPVsQAlrwG/GTs7tcAccsJqbJ1Py/w
9AgJl8VU2qc8POsHNXk348gjP7C8PDnGMpZFzr9f5INctRushpiv7onX+aWJVX7T
n2uX/TP3LCyH/MsrNJrJOQnMYFRLQitciP0E+F+eA3v9CY6mDuyb8JSx5HuGGUsG
S4bKBOcA8vimEpwPoT8CE7fdsZ3Qkwdu+pw=
=zr5w
-----END PGP PUBLIC KEY BLOCK-----
```

2. パブリックキーをキーリングにインポートし、返されたキー値をメモします。

```
rpm --import amazon-ssm-agent.gpg
```

3. フィンガープリントを確認します。RPM を使用してインストーラーパッケージを確認する場合でも、GPG を使用してフィンガープリントを確認することをお勧めします。

```
rpm -qa gpg-pubkey --qf '%{Description}' | gpg --with-fingerprint | grep -A 1
 "ssm-agent-signer@amazon.com"
```

このコマンドは、次のような出力を返します：

```
pub  2048R/97DD04ED 2023-08-28 SSM Agent <ssm-agent-signer@amazon.com>
      Key fingerprint = DE92 C7DA 3E56 E923 31D6 2A36 BC1F 495C 97DD 04ED
```

フィンガープリントは、次のものと一致する必要があります。

DE92 C7DA 3E56 E923 31D6 2A36 BC1F 495C 97DD 04ED

フィンガープリントが一致しない場合は、エージェントをインストールしないでください。に連絡しますAWS サポート

4. インストーラパッケージの署名を確認します。*agent-download-filename* は、このトピックの表で前述したように、エージェントをダウンロードするときに指定した値に置き換えてください。

```
rpm --checksig agent-download-filename
```

例えば、Amazon Linux 2 の x86_64 アーキテクチャ:

```
rpm --checksig amazon-ssm-agent.rpm
```

このコマンドは、次のような出力を返します。

```
amazon-ssm-agent.rpm: rsa sha1 md5 OK
```

pgp が出力に存在せず、パブリックキーをインポートした場合、エージェントは署名されません。出力にフレーズ NOT OK (MISSING KEYS: (MD5) *key-id*) が含まれている場合、手順が正しいことを再度確認し、SSM Agent バージョン 3.1.1141.0 以降をダウンロードしたことを確認します。この応答が続く場合は、サポート に連絡し、エージェントをインストールしないでください。

Linux 用 EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする

Amazon Elastic Compute Cloud (Amazon EC2) Linux オペレーティングシステムに AWS Systems Manager Agent (SSM Agent) を手動でインストールする前に、次の情報を確認してください。

SSM Agent インストールファイルの URL

任意のコマーシャル AWS リージョン に保存されている SSM Agent 用インストールファイルにアクセスできます。また、代替ファイルまたはバックアップソースファイルとしてグローバルに利用可能な Amazon Simple Storage Service (Amazon S3) バケットで、インストールファイルを提供しています。

エージェントを 1 つまたは 2 つのインスタンスに手動でインストールする場合は、クイックインストール手順のコマンドを使用して、時間を節約することができます。これらの手順で提供されるコマンドは、ユーザーデータを介してスクリプトとして Amazon EC2 インスタンスに渡すこともできます。

複数のインスタンスにエージェントをインストールするために使用するスクリプトまたはテンプレートを作成する場合は、ユーザーが地理的に位置する AWS リージョン またはその付近でインストールファイルを使用することをお勧めします。一括インストールの場合、これによりダウンロード速度が上がり、レイテンシーが短縮されます。一括インストールの場合、インストールトピックの「カスタムインストールコマンドの作成」手順に従うことをお勧めします。

エージェントがプリインストールされた Amazon Machine Images

SSM Agent は AWS が提供するいくつかの Amazon Machine Images (AMIs) にプリインストールされています。詳細については、SSM Agent がプリインストールされている AMIs を見つける を参照してください。

他のマシンタイプへのインストール

Systems Manager で使用できるようにエージェントをオンプレミスサーバーまたは仮想マシン (VM) にインストールする必要がある場合は、「ハイブリッド Linux ノードに SSM Agent をインストールする方法」を参照してください。エッジデバイスへのエージェントのインストールの詳細については、「Systems Manager を利用したエッジデバイスの管理」を参照してください。

エージェントを最新状態に保つ

新しいツールが Systems Manager に追加されるか、既存のツールが更新されると必ず、更新されたバージョンの SSM Agent がリリースされます。最新バージョンのエージェントを使用しないと、マネージドノードが Systems Manager の各種ツールや機能を使用できなくなる可能性があります。このため、マシン上で SSM Agent を最新状態に維持するプロセスを自動化することをお勧めします。詳細については、SSM Agent への更新の自動化 を参照してください。GitHub の「SSM Agent リリースノート」ページをサブスクライブすると、SSM Agent の更新に関する通知を受け取ることができます。

オペレーティングシステムの選択

指定したオペレーティングシステムに手動で SSM Agent をインストールする手順を確認するには、次のリストからリンクを選択してください。

> **Note**
>
> 以下の各オペレーティングシステムのサポート対象のバージョンのリストについては、「System Manager でサポートされているオペレーティングシステム」を参照してください。

- AlmaLinux
- Amazon Linux 2 および Amazon Linux 2023
- Amazon Linux 1
- CentOS
- CentOS Stream
- Debian Server
- Oracle Linux
- Red Hat Enterprise Linux

- Rocky Linux
- SUSE Linux Enterprise Server
- Ubuntu Server

Linux インスタンスから SSM Agent をアンインストールする

Linux インスタンスから SSM Agent をアンインストールするには、オペレーティングシステムのパッケージマネージャーを使用します。オペレーティングシステムによって多少異なりますが、アンインストールコマンドは次の例のようになります。

```
sudo dpkg -r amazon-ssm-agent
```

AlmaLinux インスタンスに SSM Agent を手動でインストールする

このセクションの情報に従って、AlmaLinux インスタンスに SSM Agent を手動でインストールまたは再インストールできます。

[開始する前に]

AlmaLinux インスタンスに SSM Agent をインストールする前に、次の点に注意してください。

- Python 3 が AlmaLinux インスタンスにインストールされていることを確認します。これは、SSM Agent が適切に動作するための必要条件です。
- すべての Linux ベースのオペレーティングシステムに SSM Agent をインストールする際に適用される重要な情報については、「Linux 用 EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする」を参照してください。

トピック

- AlmaLinux の SSM Agent 用クイックインストールコマンド
- ユーザーのリージョンで AlmaLinux 用のカスタムエージェントインストールコマンドを作成する

AlmaLinux の SSM Agent 用クイックインストールコマンド

次のステップに従って、シングルインスタンスに SSM Agent を手動でインストールします。この手順では、グローバルに利用可能なインストールファイルを使用します。

[開始する前に]

AlmaLinux インスタンスに SSM Agent をインストールする前に、次の点に注意してください。

- Python 3 が AlmaLinux インスタンスにインストールされていることを確認します。これは、SSM Agent が適切に動作するための必要条件です。

AlmaLinux で SSM Agent をインストールするには

1. SSH など、任意の方法を使用して AlmaLinux インスタンスに接続します。
2. インスタンスのアーキテクチャのコマンドをコピーして、インスタンスで実行します。

> **Note**
>
> 次のコマンドの URL には ec2-downloads-windows ディレクトリが含まれていますが、これらは AlmaLinux 用の正しいグローバルインストールファイルです。

x86_64 インスタンス

```
sudo dnf install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/
latest/linux_amd64/amazon-ssm-agent.rpm
```

ARM64 インスタンス

```
sudo dnf install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/
latest/linux_arm64/amazon-ssm-agent.rpm
```

3. (推奨事項) エージェントが実行されていることを確認するには、次のコマンドを実行します。

```
sudo systemctl status amazon-ssm-agent
```

ほとんどの場合、次の例に示されているように、コマンドは、エージェントが実行中であることを報告します。

```
# amazon-ssm-agent.service - amazon-ssm-agent
   Loaded: loaded (/etc/systemd/system/amazon-ssm-agent.service; enabled; vendo>
   Active: active (running) since Tue 2022-04-19 16:40:41 UTC; 9s ago
 Main PID: 4898 (amazon-ssm-agen)
    Tasks: 14 (limit: 4821)
   Memory: 34.6M
```

```
   CGroup: /system.slice/amazon-ssm-agent.service
           ##4898 /usr/bin/amazon-ssm-agent
           ##4954 /usr/bin/ssm-agent-worker
            --truncated--
```

まれに、次の例に示されているように、コマンドは、エージェントがインストールされているにも関わらず実行されていないことを報告します。

```
# amazon-ssm-agent.service - amazon-ssm-agent
   Loaded: loaded (/etc/systemd/system/amazon-ssm-agent.service; enabled; vendo>
   Active: inactive (dead) since Tue 2022-04-19 16:42:05 UTC; 2s ago
            --truncated--
```

このような場合、エージェントをアクティブ化するには、次のコマンドを実行します。

```
sudo systemctl enable amazon-ssm-agent
```

```
sudo systemctl start amazon-ssm-agent
```

ユーザーのリージョンで AlmaLinux 用のカスタムエージェントインストールコマンドを作成する

スクリプトまたはテンプレートを使用する複数のインスタンスで SSM Agent をインストールする場合は、作業中の AWS リージョンに保存されているインストールファイルを使用することが推奨されます。

次のコマンドでは、米国東部 (オハイオ) リージョン (us-east-2) で、パブリックアクセス可能な S3 バケットを使用する例を示します。

> **Tip**
>
> このトピックで前述した手順 AlmaLinux の SSM Agent 用クイックインストールコマンド のグローバル URLは、構築したカスタムリージョン URL に置き換えることもできます。

次のコマンドで、*[Region]* (リージョン) をユーザー自身の情報に置き換えます。サポートされている *region* 値の一覧については、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」にある Region 列を参照してください。

x86_64

```
sudo dnf install -y https://s3.region.amazonaws.com/amazon-ssm-region/latest/
linux_amd64/amazon-ssm-agent.rpm
```

次の例を参照してください。

```
sudo dnf install -y https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/
linux_amd64/amazon-ssm-agent.rpm
```

ARM64

```
sudo dnf install -y https://s3.region.amazonaws.com/amazon-ssm-region/latest/
linux_arm64/amazon-ssm-agent.rpm
```

次の例を参照してください。

```
sudo dnf install -y https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/
linux_arm64/amazon-ssm-agent.rpm
```

Amazon Linux 2 および Amazon Linux 2023 インスタンスに SSM Agent を手動でインストールする

Important

このトピックでは、Amazon Linux 2 および Amazon Linux 2023 インスタンスで SSM Agent を使用するためのコマンドについて説明します。これらのコマンドの一部は、Amazon Linux 1 インスタンスではサポートされていません。続行する前に、インスタンスタイプに適切なトピックが表示されていることを確認してください。Amazon Linux 1 インスタンスで実行するコマンドについては、「Amazon Linux 1 インスタンスに SSM Agent を手動でインストールする」を参照してください。

ほとんどの場合、AWS が提供する Amazon Linux 2 用および Amazon Linux 2023 用 Amazon Machine Images (AMIs) には、デフォルトで AWS Systems Manager エージェント (SSM Agent) がプリインストールされています。詳細については、「SSM Agent がプリインストールされている AMIs を見つける」を参照してください。

新しい Amazon Linux 2 または Amazon Linux 2023 インスタンスに SSM Agent がプリインストールされていない場合や、エージェントを手動で再インストールする必要がある場合は、このページの情報を参考にしてください。

[開始する前に]

Amazon Linux 2 または Amazon Linux 2023 インスタンスに SSM Agent をインストールする前に、次の点に注意してください。

- すべての Linux ベースのオペレーティングシステムに SSM Agent をインストールする際に適用される重要な情報については、「Linux 用 EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする」を参照してください。
- SSM ドキュメント `AWS-UpdateSSMAgent` を使用してエージェントがインストールまたは更新された後、マネージドノードで `yum` コマンドを使用して SSM Agent を更新する場合、「警告: RPMDB が yum 外で変更されました」というメッセージが表示されることがあります。このメッセージは正常であり、無視してもかまいません。

トピック

- Amazon Linux 2 または Amazon Linux 2023 の SSM Agent 用クイックインストールコマンド
- ユーザーのリージョンで Amazon Linux 2 用または Amazon Linux 2023 用のカスタムエージェントインストールコマンドを作成する

Amazon Linux 2 または Amazon Linux 2023 の SSM Agent 用クイックインストールコマンド

次のステップに従って、シングルインスタンスに SSM Agent を手動でインストールします。この手順では、グローバルに利用可能なインストールファイルを使用します。

クイックコピーアンドペーストコマンドを使用して Amazon Linux 2 または Amazon Linux 2023 に SSM Agent をインストールするには

1. SSH など、任意の方法を使用して Amazon Linux 2 または Amazon Linux 2023 インスタンスに接続します。
2. インスタンスのアーキテクチャのコマンドをコピーして、インスタンスで実行します。

> **Note**
>
> 次のコマンドの URL には ec2-downloads-windows ディレクトリが含まれていますが、これらは Amazon Linux 2 用 および Amazon Linux 2023 用の正しいグローバルインストールファイルです。

x86_64

```
sudo yum install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/
latest/linux_amd64/amazon-ssm-agent.rpm
```

ARM64

```
sudo yum install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/
latest/linux_arm64/amazon-ssm-agent.rpm
```

3. (推奨事項) エージェントが実行されていることを確認するには、次のコマンドを実行します。

```
sudo systemctl status amazon-ssm-agent
```

ほとんどの場合、次の例に示されているように、コマンドは、エージェントが実行中であることを報告します。

```
amazon-ssm-agent.service - amazon-ssm-agent
Loaded: loaded (/usr/lib/systemd/system/amazon-ssm-agent.service; enabled; vendor
 preset: enabled)
Active: active (running) since Wed 2021-10-20 19:09:29 UTC; 4min 6s ago
            --truncated--
```

まれに、次の例に示されているように、コマンドは、エージェントがインストールされているにも関わらず実行されていないことを報告します。

```
amazon-ssm-agent.service - amazon-ssm-agent
Loaded: loaded (/usr/lib/systemd/system/amazon-ssm-agent.service; enabled; vendor
 preset: enabled)
Active: inactive (dead) since Wed 2021-10-20 22:16:41 UTC; 18s ago
            --truncated--
```

このような場合、エージェントをアクティブ化するには、次のコマンドを実行します。

```
sudo systemctl start amazon-ssm-agent
```

ユーザーのリージョンで Amazon Linux 2 用または Amazon Linux 2023 用のカスタムエージェントインストールコマンドを作成する

スクリプトまたはテンプレートを使用する複数のインスタンスで SSM Agent をインストールする場合は、作業中の AWS リージョン に保存されているインストールファイルを使用することが推奨されます。

次のコマンドでは、米国東部 (オハイオ) リージョン (us-east-2) で、パブリックアクセス可能な S3 バケットを使用する例を示します。

> **Tip**
>
> このトピックで前述した手順 Amazon Linux 1 の SSM Agent 用クイックインストールコマンド のグローバル URLは、構築したカスタムリージョン URL に置き換えることもできます。

次のコマンドで、*[Region]* (リージョン) をユーザー自身の情報に置き換えます。サポートされている *region* 値の一覧については、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」にある Region 列を参照してください。

x86_64

```
sudo yum install -y https://s3.region.amazonaws.com/amazon-ssm-region/latest/
linux_amd64/amazon-ssm-agent.rpm
```

次の例を参照してください。

```
sudo yum install -y https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/
linux_amd64/amazon-ssm-agent.rpm
```

ARM64

```
sudo yum install -y https://s3.region.amazonaws.com/amazon-ssm-region/latest/
linux_arm64/amazon-ssm-agent.rpm
```

次の例を参照してください。

```
sudo yum install -y https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/
linux_arm64/amazon-ssm-agent.rpm
```

Amazon Linux 1 インスタンスに SSM Agent を手動でインストールする

> **Important**
>
> Amazon Linux 1 は、2020 年 12 月 31 日に標準サポートが終了し、2023 年 12 月 31 日に廃止されました。これは、「AWS ニュースブログ」の「Amazon Linux AMI 廃止に関するアップデート」でお知らせしています。AWS では、このオペレーティングシステム向けの Amazon Machine Images (AMIs) の提供を終了しました。ただし、AWS Systems Manager では、既存の Amazon Linux 1 インスタンスは引き続きサポートします。
> このトピックでは、Amazon Linux 1 インスタンスで SSM Agent を使用するためのコマンドについて説明します。これらのコマンドの一部は、Amazon Linux 2 および Amazon Linux 2023 インスタンスではサポートされていません。続行する前に、インスタンスタイプに対する正しいトピックを参照していることを確認してください。Amazon Linux 2 または Amazon Linux 2023 インスタンスで実行するコマンドについては、「Amazon Linux 2 および Amazon Linux 2023 インスタンスに SSM Agent を手動でインストールする」を参照してください。

ほとんどの場合、AWS が提供する Amazon Linux 1 用 Amazon Machine Images (AMIs) には、デフォルトで AWS Systems Manager エージェント (SSM Agent) がプリインストールされています。詳細については、「SSM Agent がプリインストールされている AMIs を見つける」を参照してください。

エージェントを Amazon Linux 1 に手動で再インストールする必要がある場合は、このページの情報を参考にしてください。

[開始する前に]

Amazon Linux 1 インスタンスに SSM Agent をインストールする前に、次の点に注意してください。

- すべての Linux ベースのオペレーティングシステムに SSM Agent をインストールする際に適用される重要な情報については、「Linux 用 EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする」を参照してください。
- SSM ドキュメント `AWS-UpdateSSMAgent` を使用してエージェントがインストールまたは更新された後、マネージドノードで yum コマンドを使用して SSM Agent を更新する場合、「警告: RPMDB が yum 外で変更されました」というメッセージが表示されることがあります。このメッセージは正常であり、無視してもかまいません。

トピック

- Amazon Linux 1 の SSM Agent 用クイックインストールコマンド
- 自身のリージョンで Amazon Linux 1 用のカスタムエージェントインストールコマンドを作成する

Amazon Linux 1 の SSM Agent 用クイックインストールコマンド

次のステップに従って、シングルインスタンスに SSM Agent を手動でインストールします。この手順では、グローバルに利用可能なインストールファイルを使用します。

クイックコピーアンドペーストコマンドを使用して Amazon Linux 1 に SSM Agent をインストールするには

1. SSH など、任意の方法を使用して Amazon Linux 1 インスタンスに接続します。
2. インスタンスのアーキテクチャのコマンドをコピーして、インスタンスで実行します。

> **Note**
>
> 次のコマンドの URL には `ec2-downloads-windows` ディレクトリが含まれていますが、これらは Amazon Linux 1 用の正しいグローバルインストールファイルです。

x86_64

```
sudo yum install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/
latest/linux_amd64/amazon-ssm-agent.rpm
```

x86

```
sudo yum install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/
latest/linux_386/amazon-ssm-agent.rpm
```

ARM64

```
sudo yum install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/
latest/linux_arm64/amazon-ssm-agent.rpm
```

3. (推奨事項) インスタンスのアーキテクチャのコマンドを実行して、エージェントが実行中であることを確認します。

   x86_64 および x86

   ```
   sudo status amazon-ssm-agent
   ```

   ARM64

   ```
   sudo systemctl status amazon-ssm-agent
   ```

   ほとんどの場合、次の例に示されているように、コマンドは、エージェントが実行中であることを報告します。

   x86_64 および x86

   ```
   amazon-ssm-agent start/running, process 12345
   ```

   ARM64

   ```
   amazon-ssm-agent.service - amazon-ssm-agent
   Loaded: loaded (/usr/lib/systemd/system/amazon-ssm-agent.service; enabled;
    vendor preset: enabled)
   Active: active (running) since Wed 2021-10-20 19:09:29 UTC; 4min 6s ago
              --truncated--
   ```

まれに、次の例に示されているように、コマンドは、エージェントがインストールされているにも関わらず実行されていないことを報告します。

x86_64 および x86

```
amazon-ssm-agent stop/waiting
```

ARM64

```
amazon-ssm-agent.service - amazon-ssm-agent
Loaded: loaded (/usr/lib/systemd/system/amazon-ssm-agent.service; enabled;
 vendor preset: enabled)
Active: inactive (dead) since Wed 2021-10-20 22:16:41 UTC; 18s ago
            --truncated--
```

このような場合にエージェントをアクティブ化するには、インスタンスのアーキテクチャのコマンドを実行します。

x86_64 および x86

```
sudo start amazon-ssm-agent
```

ARM64

```
sudo systemctl start amazon-ssm-agent
```

自身のリージョンで Amazon Linux 1 用のカスタムエージェントインストールコマンドを作成する

スクリプトまたはテンプレートを使用する複数のインスタンスで SSM Agent をインストールする場合は、作業中の AWS リージョンに保存されているインストールファイルを使用することが推奨されます。

次のコマンドでは、米国東部 (オハイオ) リージョン (us-east-2) で、パブリックアクセス可能な S3 バケットを使用する例を示します。

> **Tip**
>
> このトピックで前述した手順 Amazon Linux 1 の SSM Agent 用クイックインストールコマンド のグローバル URLは、構築したカスタムリージョン URL に置き換えることもできます。

次のコマンドで、*[Region]* (リージョン) をユーザー自身の情報に置き換えます。サポートされている *region* 値の一覧については、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」にある Region 列を参照してください。

x86_64

```
sudo yum install -y https://s3.region.amazonaws.com/amazon-ssm-region/latest/
linux_amd64/amazon-ssm-agent.rpm
```

次の例を参照してください。

```
sudo yum install -y https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/
linux_amd64/amazon-ssm-agent.rpm
```

x86

```
sudo yum install -y https://s3.region.amazonaws.com/amazon-ssm-region/latest/
linux_386/amazon-ssm-agent.rpm
```

次の例を参照してください。

```
sudo yum install -y https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/
linux_386/amazon-ssm-agent.rpm
```

ARM64

```
sudo yum install -y https://s3.region.amazonaws.com/amazon-ssm-region/latest/
linux_arm64/amazon-ssm-agent.rpm
```

次の例を参照してください。

```
sudo yum install -y https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/
linux_arm64/amazon-ssm-agent.rpm
```

CentOS インスタンスに SSM Agent を手動でインストールする

AWS が提供する CentOS 用 Amazon Machine Images (AMIs) には、デフォルトでは AWS Systems Manager エージェント (SSM Agent) がプリインストールされていません。エージェントがプリインストールされている可能性のある AWS マネージド AMIs のリストについては、「SSM Agent がプリインストールされている AMIs を見つける」を参照してください。

このセクションの情報に従って、CentOS インスタンスに SSM Agent を手動でインストールまたは再インストールできます。

開始する前に

CentOS インスタンスに SSM Agent をインストールする前に、次の点に注意してください。

- すべての Linux ベースのオペレーティングシステムに SSM Agent をインストールする際に適用される重要な情報については、「Linux 用 EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする」を参照してください。
- SSM ドキュメント `AWS-UpdateSSMAgent` を使用してエージェントがインストールまたは更新された後、マネージドノードで `yum` コマンドを使用して SSM Agent を更新する場合、「警告: RPMDB が yum 外で変更されました」 というメッセージが表示されることがあります。このメッセージは正常であり、無視してもかまいません。

トピック

- CentOS 8.x に SSM Agent をインストールする
- CentOS 7.x に SSM Agent をインストールする
- CentOS 6.x に SSM Agent をインストールする

CentOS 8.x に SSM Agent をインストールする

AWS が提供する CentOS 8 用 Amazon Machine Images (AMIs) には、デフォルトでは AWS Systems Manager エージェント (SSM Agent) がプリインストールされていません。このセクションの情報に従って、CentOS 8 インスタンスにエージェントをインストールまたは再インストールできます。

[開始する前に]

CentOS 8 インスタンスに SSM Agent をインストールする前に、次の点に注意してください。

- Python 2 または Python 3 のいずれかが CentOS 8 インスタンスにインストールされていることを確認します。これは、SSM Agent が適切に動作するための必要条件です。

トピック

- CentOS 8 の SSM Agent 用クイックインストールコマンド
- ユーザーのリージョンで CentOS 8 用のカスタムエージェントインストールコマンドを作成する

CentOS 8 の SSM Agent 用クイックインストールコマンド

次のステップに従って、シングルインスタンスに SSM Agent を手動でインストールします。この手順では、グローバルに利用可能なインストールファイルを使用します。

CentOS 8.x に SSM Agent をインストールするには

1. SSH など、任意の方法を使用して CentOS 8 インスタンスに接続します。
2. インスタンスのアーキテクチャのコマンドをコピーして、インスタンスで実行します。

> **Note**
>
> 次のコマンドの URL には `ec2-downloads-windows` ディレクトリが含まれていますが、これらは CentOS 8 用の正しいグローバルインストールファイルです。

x86_64 インスタンス

```
sudo dnf install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/
latest/linux_amd64/amazon-ssm-agent.rpm
```

ARM64 インスタンス

```
sudo dnf install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/
latest/linux_arm64/amazon-ssm-agent.rpm
```

3. (推奨事項) エージェントが実行されていることを確認するには、次のコマンドを実行します。

```
sudo systemctl status amazon-ssm-agent
```

ほとんどの場合、次の例に示されているように、コマンドは、エージェントが実行中であることを報告します。

```
# amazon-ssm-agent.service - amazon-ssm-agent
   Loaded: loaded (/etc/systemd/system/amazon-ssm-agent.service; enabled; vendo>
   Active: active (running) since Tue 2022-04-19 15:48:54 UTC; 19s ago
            --truncated--
```

まれに、次の例に示されているように、コマンドは、エージェントがインストールされているにも関わらず実行されていないことを報告します。

```
# amazon-ssm-agent.service - amazon-ssm-agent
   Loaded: loaded (/etc/systemd/system/amazon-ssm-agent.service; disabled; vend>
   Active: inactive (dead)
            --truncated--
```

このような場合、エージェントをアクティブ化するには、次のコマンドを実行します。

```
sudo systemctl enable amazon-ssm-agent
```

```
sudo systemctl start amazon-ssm-agent
```

ユーザーのリージョンで CentOS 8 用のカスタムエージェントインストールコマンドを作成する

スクリプトまたはテンプレートを使用する複数のインスタンスで SSM Agent をインストールする場合は、作業中の AWS リージョンに保存されているインストールファイルを使用することが推奨されます。

次のコマンドでは、米国東部 (オハイオ) リージョン (us-east-2) で、パブリックアクセス可能な S3 バケットを使用する例を示します。

> **Tip**
>
> このトピックで前述した手順 CentOS 8 の SSM Agent 用クイックインストールコマンド のグローバル URLは、構築したカスタムリージョン URL に置き換えることもできます。

次のコマンドで、*[Region]* (リージョン) をユーザー自身の情報に置き換えます。サポートされている *region* 値の一覧については、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」にある Region 列を参照してください。

x86_64

```
sudo dnf install -y https://s3.region.amazonaws.com/amazon-ssm-region/latest/
linux_amd64/amazon-ssm-agent.rpm
```

次の例を参照してください。

```
sudo dnf install -y https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/
linux_amd64/amazon-ssm-agent.rpm
```

ARM64

```
sudo dnf install -y https://s3.region.amazonaws.com/amazon-ssm-region/latest/
linux_arm64/amazon-ssm-agent.rpm
```

次の例を参照してください。

```
sudo dnf install -y https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/
linux_arm64/amazon-ssm-agent.rpm
```

CentOS 7.x に SSM Agent をインストールする

AWS が提供する CentOS 7 用 Amazon Machine Images (AMIs) には、デフォルトでは AWS Systems Manager エージェント (SSM Agent) がプリインストールされていません。このページの情報に従って、CentOS 7 インスタンスにエージェントをインストールまたは再インストールできます。

トピック

- CentOS 7 の SSM Agent 用クイックインストールコマンド
- ユーザーのリージョンで CentOS 7 用のカスタムエージェントインストールコマンドを作成する

CentOS 7 の SSM Agent 用クイックインストールコマンド

次のステップに従って、シングルインスタンスに SSM Agent を手動でインストールします。この手順では、グローバルに利用可能なインストールファイルを使用します。

CentOS 7.x に SSM Agent をインストールするには

1. SSH など、任意の方法を使用して CentOS 7 インスタンスに接続します。
2. インスタンスのアーキテクチャのコマンドをコピーして、インスタンスで実行します。

> **Note**
>
> 次のコマンドの URL には ec2-downloads-windows ディレクトリが含まれていますが、これらは CentOS 7 用の正しいグローバルインストールファイルです。

x86_64 インスタンス

```
sudo yum install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/
latest/linux_amd64/amazon-ssm-agent.rpm
```

ARM64 インスタンス

```
sudo yum install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/
latest/linux_arm64/amazon-ssm-agent.rpm
```

3. (推奨事項) エージェントが実行されていることを確認するには、次のコマンドを実行します。

```
sudo systemctl status amazon-ssm-agent
```

ほとんどの場合、次の例に示されているように、コマンドは、エージェントが実行中であることを報告します。

```
# amazon-ssm-agent.service - amazon-ssm-agent
   Loaded: loaded (/etc/systemd/system/amazon-ssm-agent.service; enabled; vendor
 preset: disabled)
   Active: active (running) since Tue 2022-04-19 15:57:27 UTC; 6s ago
           --truncated--
```

まれに、次の例に示されているように、コマンドは、エージェントがインストールされているにも関わらず実行されていないことを報告します。

```
# amazon-ssm-agent.service - amazon-ssm-agent
   Loaded: loaded (/etc/systemd/system/amazon-ssm-agent.service; enabled; vendor
 preset: disabled)
   Active: inactive (dead) since Tue 2022-04-19 15:58:44 UTC; 2s ago
            --truncated--
```

このような場合、エージェントをアクティブ化するには、次のコマンドを実行します。

```
sudo systemctl enable amazon-ssm-agent
```

```
sudo systemctl start amazon-ssm-agent
```

ユーザーのリージョンで CentOS 7 用のカスタムエージェントインストールコマンドを作成する

スクリプトまたはテンプレートを使用する複数のインスタンスで SSM Agent をインストールする場合は、作業中の AWS リージョン に保存されているインストールファイルを使用することが推奨されます。

次のコマンドでは、米国東部 (オハイオ) リージョン (us-east-2) で、パブリックアクセス可能な S3 バケットを使用する例を示します。

> **Tip**
>
> このトピックで前述した手順 CentOS 7 の SSM Agent 用クイックインストールコマンド のグローバル URLは、構築したカスタムリージョン URL に置き換えることもできます。

次のコマンドで、*[Region]* (リージョン) をユーザー自身の情報に置き換えます。サポートされている *region* 値の一覧については、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」にある Region 列を参照してください。

x86_64

```
sudo yum install -y https://s3.region.amazonaws.com/amazon-ssm-region/latest/
linux_amd64/amazon-ssm-agent.rpm
```

次の例を参照してください。

```
sudo yum install -y https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/
linux_amd64/amazon-ssm-agent.rpm
```

ARM64

```
sudo yum install -y https://s3.region.amazonaws.com/amazon-ssm-region/latest/
linux_arm64/amazon-ssm-agent.rpm
```

次の例を参照してください。

```
sudo yum install -y https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/
linux_arm64/amazon-ssm-agent.rpm
```

CentOS 6.x に SSM Agent をインストールする

AWS が提供する CentOS 6 用 Amazon Machine Images (AMIs) には、デフォルトでは AWS Systems Manager エージェント (SSM Agent) がプリインストールされていません。このページの情報に従って、CentOS 6 インスタンスにエージェントをインストールまたは再インストールできます。

トピック

- CentOS 6 の SSM Agent 用クイックインストールコマンド
- ユーザーのリージョンで CentOS 6 用のカスタムエージェントインストールコマンドを作成する

CentOS 6 の SSM Agent 用クイックインストールコマンド

次のステップに従って、シングルインスタンスに SSM Agent を手動でインストールします。この手順では、グローバルに利用可能なインストールファイルを使用します。

CentOS 6.x に SSM Agent をインストールするには

1. SSH など、任意の方法を使用して CentOS 6 インスタンスに接続します。

2. インスタンスのアーキテクチャのコマンドをコピーして、インスタンスで実行します。

> **Note**
>
> 次のコマンドの URL には ec2-downloads-windows ディレクトリが含まれていますが、これらは CentOS 6 用の正しいグローバルインストールファイルです。
> 次のコマンドは、latest ディレクトリの代わりにバージョンディレクトリ 3.0.1479.0 を指定します。これは、SSM Agent バージョン 3.1 以降では、CentOS 6 がサポートされていないためです。

x86_64 インスタンス

```
sudo yum install -y https://s3.amazonaws.com/ec2-downloads-windows/
SSMAgent/3.0.1479.0/linux_amd64/amazon-ssm-agent.rpm
```

x86 インスタンス

```
sudo yum install -y https://s3.amazonaws.com/ec2-downloads-windows/
SSMAgent/3.0.1479.0/linux_386/amazon-ssm-agent.rpm
```

3. (推奨事項) エージェントが実行されていることを確認するには、次のコマンドを実行します。

```
sudo status amazon-ssm-agent
```

ほとんどの場合、次の例に示されているように、コマンドは、エージェントが実行中であることを報告します。

```
amazon-ssm-agent start/running, process 1744
```

まれに、次の例に示されているように、コマンドは、エージェントがインストールされているにも関わらず実行されていないことを報告します。

```
amazon-ssm-agent stop/waiting
```

このような場合、エージェントをアクティブ化するには、次のコマンドを実行します。

```
sudo start amazon-ssm-agent
```

ユーザーのリージョンで CentOS 6 用のカスタムエージェントインストールコマンドを作成する

スクリプトまたはテンプレートを使用する複数のインスタンスで SSM Agent をインストールする場合は、作業中の AWS リージョンに保存されているインストールファイルを使用することが推奨されます。

次のコマンドでは、米国東部 (オハイオ) リージョン (us-east-2) で、パブリックアクセス可能な S3 バケットを使用する例を示します。

> **Tip**
>
> このトピックで前述した手順 CentOS 6 の SSM Agent 用クイックインストールコマンド のグローバル URLは、構築したカスタムリージョン URL に置き換えることもできます。

次のコマンドで、*[Region]* (リージョン) をユーザー自身の情報に置き換えます。サポートされている *region* 値の一覧については、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」にある Region 列を参照してください。

> **Note**
>
> 次のコマンドは、latest ディレクトリの代わりにバージョンディレクトリ 3.0.1479.0 を指定します。これは、SSM Agent バージョン 3.1 以降では、CentOS 6 がサポートされていないためです。

x86_64

```
sudo yum install -y https://s3.region.amazonaws.com/amazon-ssm-region/3.0.1479.0/
linux_amd64/amazon-ssm-agent.rpm
```

次の例を参照してください。

```
sudo yum install -y https://s3.us-east-2.amazonaws.com/amazon-ssm-us-
east-2/3.0.1479.0/linux_amd64/amazon-ssm-agent.rpm
```

x86

```
sudo yum install -y https://s3.region.amazonaws.com/amazon-ssm-region/3.0.1479.0/
linux_386/amazon-ssm-agent.rpm
```

次の例を参照してください。

```
sudo yum install -y https://s3.us-east-2.amazonaws.com/amazon-ssm-us-
east-2/3.0.1479.0/linux_386/amazon-ssm-agent.rpm
```

CentOS Stream インスタンスに SSM Agent を手動でインストールする

AWS が提供する CentOS Stream 用 Amazon Machine Images (AMIs) には、デフォルトでは AWS Systems Manager エージェント (SSM Agent) がプリインストールされていません。エージェントがプリインストールされている可能性のある AWS マネージド AMIs のリストについては、「SSM Agent がプリインストールされている AMIs を見つける」を参照してください。

このセクションの情報に従って、CentOS Stream インスタンスに SSM Agent を手動でインストールまたは再インストールできます。

[開始する前に]

CentOS Stream インスタンスに SSM Agent をインストールする前に、次の点に注意してください。

- すべての Linux ベースのオペレーティングシステムに SSM Agent をインストールする際に適用される重要な情報については、「Linux 用 EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする」を参照してください。

トピック

- CentOS Stream の SSM Agent 用クイックインストールコマンド
- ユーザーのリージョンで CentOS Stream 用のカスタムエージェントインストールコマンドを作成する

CentOS Stream の SSM Agent 用クイックインストールコマンド

次のステップに従って、シングルインスタンスに SSM Agent を手動でインストールします。この手順では、グローバルに利用可能なインストールファイルを使用します。

[開始する前に]

CentOS Stream インスタンスに SSM Agent をインストールする前に、次の点に注意してください。

- Python 2 または Python 3 のいずれかが CentOS Stream 8 インスタンスにインストールされていることを確認します。これは、SSM Agent が適切に動作するための必要条件です。

CentOS Stream に SSM Agent をインストールするには

1. SSH など、任意の方法を使用して CentOS Stream インスタンスに接続します。
2. インスタンスのアーキテクチャのコマンドをコピーして、インスタンスで実行します。

> **Note**
>
> 次のコマンドの URL には ec2-downloads-windows ディレクトリが含まれていますが、これらは CentOS Stream 用の正しいグローバルインストールファイルです。

x86_64 インスタンス

```
sudo dnf install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/
latest/linux_amd64/amazon-ssm-agent.rpm
```

ARM64 インスタンス

```
sudo dnf install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/
latest/linux_arm64/amazon-ssm-agent.rpm
```

3. (推奨事項) エージェントが実行されていることを確認するには、次のコマンドを実行します。

```
sudo systemctl status amazon-ssm-agent
```

ほとんどの場合、次の例に示されているように、コマンドは、エージェントが実行中であることを報告します。

```
# amazon-ssm-agent.service - amazon-ssm-agent
   Loaded: loaded (/etc/systemd/system/amazon-ssm-agent.service; enabled; vendo>
   Active: active (running) since Tue 2022-04-19 16:40:41 UTC; 9s ago
 Main PID: 4898 (amazon-ssm-agen)
    Tasks: 14 (limit: 4821)
   Memory: 34.6M
   CGroup: /system.slice/amazon-ssm-agent.service
           ##4898 /usr/bin/amazon-ssm-agent
           ##4954 /usr/bin/ssm-agent-worker
            --truncated--
```

まれに、次の例に示されているように、コマンドは、エージェントがインストールされているにも関わらず実行されていないことを報告します。

```
# amazon-ssm-agent.service - amazon-ssm-agent
   Loaded: loaded (/etc/systemd/system/amazon-ssm-agent.service; enabled; vendo>
   Active: inactive (dead) since Tue 2022-04-19 16:42:05 UTC; 2s ago
            --truncated--
```

このような場合、エージェントをアクティブ化するには、次のコマンドを実行します。

```
sudo systemctl enable amazon-ssm-agent
```

```
sudo systemctl start amazon-ssm-agent
```

ユーザーのリージョンで CentOS Stream 用のカスタムエージェントインストールコマンドを作成する

スクリプトまたはテンプレートを使用する複数のインスタンスで SSM Agent をインストールする場合は、作業中の AWS リージョンに保存されているインストールファイルを使用することが推奨されます。

次のコマンドでは、米国東部 (オハイオ) リージョン (us-east-2) で、パブリックアクセス可能な S3 バケットを使用する例を示します。

> **Tip**
>
> このトピックで前述した手順 CentOS Stream の SSM Agent 用クイックインストールコマンド のグローバル URLは、構築したカスタムリージョン URL に置き換えることもできます。

次のコマンドで、*[Region]* (リージョン) をユーザー自身の情報に置き換えます。サポートされている *region* 値の一覧については、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」にある Region 列を参照してください。

x86_64

```
sudo dnf install -y https://s3.region.amazonaws.com/amazon-ssm-region/latest/
linux_amd64/amazon-ssm-agent.rpm
```

次の例を参照してください。

```
sudo dnf install -y https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/
linux_amd64/amazon-ssm-agent.rpm
```

ARM64

```
sudo dnf install -y https://s3.region.amazonaws.com/amazon-ssm-region/latest/
linux_arm64/amazon-ssm-agent.rpm
```

次の例を参照してください。

```
sudo dnf install -y https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/
linux_arm64/amazon-ssm-agent.rpm
```

Debian Server インスタンスに SSM Agent を手動でインストールする

AWS が提供する Debian Server 用 Amazon Machine Images (AMIs) には、デフォルトでは AWS Systems Manager エージェント (SSM Agent) がプリインストールされていません。エージェントがプリインストールされている可能性のある AWS マネージド AMIs のリストについては、「SSM Agent がプリインストールされている AMIs を見つける」を参照してください。

このセクションの情報に従って、Debian Server インスタンスに SSM Agent を手動でインストールまたは再インストールできます。

[開始する前に]

Debian Server インスタンスに SSM Agent をインストールする前に、次の点に注意してください。

- すべての Linux ベースのオペレーティングシステムに SSM Agent をインストールする際に適用される重要な情報については、「Linux 用 EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする」を参照してください。

トピック

- Debian Server の SSM Agent 用クイックインストールコマンド
- ユーザーのリージョンで Debian Server 用のカスタムエージェントインストールコマンドを作成する

Debian Server の SSM Agent 用クイックインストールコマンド

次のステップに従って、シングルインスタンスに SSM Agent を手動でインストールします。この手順では、グローバルに利用可能なインストールファイルを使用します。

Debian Server に SSM Agent をインストールするには

1. SSH など、任意の方法を使用して Debian Server インスタンスに接続します。
2. 次のコマンドを実行して、インスタンスに一時ディレクトリを作成します。

```
mkdir /tmp/ssm
```

3. 次のコマンドを実行して、一時ディレクトリに変更します。

```
cd /tmp/ssm
```

4. インスタンスのアーキテクチャのコマンドをコピーして、インスタンスで実行します。

> **Note**
>
> 次のコマンドの URL には ec2-downloads-windows ディレクトリが含まれていますが、これらは Debian Server 用の正しいグローバルインストールファイルです。Debian Server 8 では、x86_64 アーキテクチャのみがサポートされています。

x86_64 インスタンス

```
wget https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/
debian_amd64/amazon-ssm-agent.deb
```

ARM64 インスタンス

```
wget https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/
debian_arm64/amazon-ssm-agent.deb
```

5. 以下のコマンドを実行してください。

```
sudo dpkg -i amazon-ssm-agent.deb
```

6. (推奨事項) エージェントが実行されていることを確認するには、次のコマンドを実行します。

```
sudo systemctl status amazon-ssm-agent
```

ほとんどの場合、次の例に示されているように、コマンドは、エージェントが実行中であることを報告します。

```
# amazon-ssm-agent.service - amazon-ssm-agent
   Loaded: loaded (/lib/systemd/system/amazon-ssm-agent.service; enabled; vendor
   Active: active (running) since Tue 2022-04-19 16:25:03 UTC; 4s ago
 Main PID: 628 (amazon-ssm-agen)
   CGroup: /system.slice/amazon-ssm-agent.service
           ##628 /usr/bin/amazon-ssm-agent
           ##650 /usr/bin/ssm-agent-worker
            --truncated--
```

まれに、次の例に示されているように、コマンドは、エージェントがインストールされているにも関わらず実行されていないことを報告します。

```
# amazon-ssm-agent.service - amazon-ssm-agent
   Loaded: loaded (/lib/systemd/system/amazon-ssm-agent.service; enabled; vendor
   Active: inactive (dead) since Tue 2022-04-19 16:26:30 UTC; 5s ago
 Main PID: 628 (code=exited, status=0/SUCCESS)
            --truncated--
```

このような場合、エージェントをアクティブ化するには、次のコマンドを実行します。

```
sudo systemctl enable amazon-ssm-agent
```

```
sudo systemctl start amazon-ssm-agent
```

ユーザーのリージョンで Debian Server 用のカスタムエージェントインストールコマンドを作成する

スクリプトまたはテンプレートを使用する複数のインスタンスで SSM Agent をインストールする場合は、作業中の AWS リージョンに保存されているインストールファイルを使用することが推奨されます。

次のコマンドでは、米国東部 (オハイオ) リージョン (us-east-2) で、パブリックアクセス可能な S3 バケットを使用する例を示します。

> **Tip**
>
> このトピックで前述した手順 Debian Server の SSM Agent 用クイックインストールコマンド のグローバル URLは、構築したカスタムリージョン URL に置き換えることもできます。

次のコマンドで、*[Region]* (リージョン) をユーザー自身の情報に置き換えます。サポートされている *region* 値の一覧については、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」にある Region 列を参照してください。

> **Note**
>
> Debian Server 8 では、x86_64 アーキテクチャのみがサポートされています。

x86_64

```
wget https://s3.region.amazonaws.com/amazon-ssm-region/latest/debian_amd64/amazon-ssm-agent.deb
```

```
sudo dpkg -i amazon-ssm-agent.deb
```

次の例を参照してください。

```
wget https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/debian_amd64/amazon-ssm-agent.deb
```

```
sudo dpkg -i amazon-ssm-agent.deb
```

ARM64

```
wget https://s3.region.amazonaws.com/amazon-ssm-region/latest/debian_arm64/amazon-ssm-agent.deb
```

```
sudo dpkg -i amazon-ssm-agent.deb
```

次の例を参照してください。

```
wget https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/debian_arm64/amazon-ssm-agent.deb
```

```
sudo dpkg -i amazon-ssm-agent.deb
```

Oracle Linux インスタンスに SSM Agent を手動でインストールする

AWS が提供する Oracle Linux 用 Amazon Machine Images (AMIs) には、デフォルトでは AWS Systems Manager エージェント (SSM Agent) がプリインストールされていません。エージェントがプリインストールされている可能性のある AWS マネージド AMIs のリストについては、「SSM Agent がプリインストールされている AMIs を見つける」を参照してください。

このセクションの情報に従って、Oracle Linux インスタンスに SSM Agent を手動でインストールまたは再インストールできます。

[開始する前に]

Oracle Linux インスタンスに SSM Agent をインストールする前に、次の点に注意してください。

- すべての Linux ベースのオペレーティングシステムに SSM Agent をインストールする際に適用される重要な情報については、「Linux 用 EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする」を参照してください。
- SSM ドキュメント `AWS-UpdateSSMAgent` を使用してエージェントがインストールまたは更新された後、マネージドノードで yum コマンドを使用して SSM Agent を更新する場合、「警告: RPMDB が yum 外で変更されました」というメッセージが表示されることがあります。このメッセージは正常であり、無視してもかまいません。

トピック

- Oracle Linux の SSM Agent 用クイックインストールコマンド
- ユーザーのリージョンで Oracle Linux 用のカスタムエージェントインストールコマンドを作成する

Oracle Linux の SSM Agent 用クイックインストールコマンド

次のステップに従って、シングルインスタンスに SSM Agent を手動でインストールします。この手順では、グローバルに利用可能なインストールファイルを使用します。

クイックコピーアンドペーストコマンドを使用して Oracle Linux に SSM Agent をインストールするには

1. SSH など、任意の方法を使用して Oracle Linux インスタンスに接続します。
2. 次のコマンドをコピーして、インスタンスで実行します。

> **Note**
>
> 次のコマンドの URL には `ec2-downloads-windows` ディレクトリが含まれていますが、これらは Oracle Linux 用の正しいグローバルインストールファイルです。

x86_64

```
sudo yum install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/
latest/linux_amd64/amazon-ssm-agent.rpm
```

3. (推奨事項) エージェントが実行されていることを確認するには、次のコマンドを実行します。

```
sudo systemctl status amazon-ssm-agent
```

ほとんどの場合、次の例に示されているように、コマンドは、エージェントが実行中であることを報告します。

```
amazon-ssm-agent.service - amazon-ssm-agent
Loaded: loaded (/usr/lib/systemd/system/amazon-ssm-agent.service; enabled; vendor
 preset: enabled)
Active: active (running) since Wed 2021-10-20 19:09:29 UTC; 4min 6s ago
            --truncated--
```

まれに、次の例に示されているように、コマンドは、エージェントがインストールされているにも関わらず実行されていないことを報告します。

```
amazon-ssm-agent.service - amazon-ssm-agent
Loaded: loaded (/usr/lib/systemd/system/amazon-ssm-agent.service; enabled; vendor
 preset: enabled)
Active: inactive (dead) since Wed 2021-10-20 22:16:41 UTC; 18s ago
            --truncated--
```

このような場合、エージェントをアクティブ化するには、次のコマンドを実行します。

```
sudo systemctl enable amazon-ssm-agent
```

```
sudo systemctl start amazon-ssm-agent
```

ユーザーのリージョンで Oracle Linux 用のカスタムエージェントインストールコマンドを作成する

スクリプトまたはテンプレートを使用する複数のインスタンスで SSM Agent をインストールする場合は、作業中の AWS リージョンに保存されているインストールファイルを使用することが推奨されます。

次のコマンドでは、米国東部 (オハイオ) リージョン (us-east-2) で、パブリックアクセス可能な S3 バケットを使用する例を示します。

> **Tip**
>
> このトピックで前述した手順 Oracle Linux の SSM Agent 用クイックインストールコマンドのグローバル URLは、構築したカスタムリージョン URL に置き換えることもできます。

次のコマンドで、*[Region]* (リージョン) をユーザー自身の情報に置き換えます。サポートされている *region* 値の一覧については、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」にある Region 列を参照してください。

x86_64

```
sudo yum install -y https://s3.region.amazonaws.com/amazon-ssm-region/latest/
linux_amd64/amazon-ssm-agent.rpm
```

次の例を参照してください。

```
sudo yum install -y https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/
linux_amd64/amazon-ssm-agent.rpm
```

Red Hat Enterprise Linux インスタンスに SSM Agent を手動でインストールする

AWS が提供する Red Hat Enterprise Linux (RHEL) 用 Amazon Machine Images (AMIs) には、デフォルトでは AWS Systems Manager エージェント (SSM Agent) がプリインストールされていません。エージェントがプリインストールされている可能性のある AWS マネージド AMIs のリストについては、「SSM Agent がプリインストールされている AMIs を見つける」を参照してください。

このセクションの情報に従って、RHEL インスタンスに SSM Agent を手動でインストールまたは再インストールできます。

開始する前に

RHEL インスタンスに SSM Agent をインストールする前に、次の点に注意してください。

- すべての Linux ベースのオペレーティングシステムに SSM Agent をインストールする際に適用される重要な情報については、「Linux 用 EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする」を参照してください。
- SSM ドキュメント `AWS-UpdateSSMAgent` を使用してエージェントがインストールまたは更新された後、マネージドノードで yum コマンドを使用して SSM Agent を更新する場合、「警告: RPMDB が yum 外で変更されました」というメッセージが表示されることがあります。このメッセージは正常であり、無視してもかまいません。

トピック

- RHEL 8.x および 9.x を SSM Agent にインストール
- RHEL 7.x に SSM Agent をインストールする
- RHEL 6.x に SSM Agent をインストールする

RHEL 8.x および 9.x を SSM Agent にインストール

AWS が提供する RHEL 8 および 9 用 Amazon Machine Images (AMIs) には、デフォルトでは AWS Systems Manager エージェント (SSM Agent) がプリインストールされていません。このページの情報に従って、RHEL 8 および 9 インスタンスにエージェントをインストールまたは再インストールできます。

[開始する前に]

RHEL 8 および 9 インスタンスに SSM Agent をインストールする前に、次の点に注意してください。

- Python 2 または Python 3 のいずれかが RHEL 8 および 9 インスタンスにインストールされていることを確認します。これは、SSM Agent が適切に動作するための必要条件です。

トピック

- RHEL 8 または 9 の SSM Agent 用クイックインストールコマンド
- ユーザーのリージョンで RHEL 8 および 9 用のカスタムエージェントインストールコマンドを作成する

RHEL 8 または 9 の SSM Agent 用クイックインストールコマンド

次のステップに従って、シングルインスタンスに SSM Agent を手動でインストールします。この手順では、グローバルに利用可能なインストールファイルを使用します。

RHEL 8.x または 9.x に SSM Agent をインストールするには

1. SSH など、任意の方法を使用して RHEL 8 および 9 インスタンスに接続します。
2. インスタンスのアーキテクチャのコマンドをコピーして、インスタンスで実行します。

> **Note**
>
> 次のコマンドの URL には `ec2-downloads-windows` ディレクトリが含まれていますが、これらは RHEL 8 および 9 用の正しいグローバルインストールファイルです。

x86_64 インスタンス

```
sudo dnf install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/
latest/linux_amd64/amazon-ssm-agent.rpm
```

ARM64 インスタンス

```
sudo dnf install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/
latest/linux_arm64/amazon-ssm-agent.rpm
```

3. (推奨事項) エージェントが実行されていることを確認するには、次のコマンドを実行します。

```
sudo systemctl status amazon-ssm-agent
```

ほとんどの場合、次の例に示されているように、コマンドは、エージェントが実行中であることを報告します。

```
# amazon-ssm-agent.service - amazon-ssm-agent
   Loaded: loaded (/etc/systemd/system/amazon-ssm-agent.service; enabled; vendo>
   Active: active (running) since Tue 2022-04-19 16:40:41 UTC; 9s ago
 Main PID: 4898 (amazon-ssm-agen)
    Tasks: 14 (limit: 4821)
   Memory: 34.6M
   CGroup: /system.slice/amazon-ssm-agent.service
           ##4898 /usr/bin/amazon-ssm-agent
           ##4954 /usr/bin/ssm-agent-worker
            --truncated--
```

まれに、次の例に示されているように、コマンドは、エージェントがインストールされているにも関わらず実行されていないことを報告します。

```
# amazon-ssm-agent.service - amazon-ssm-agent
   Loaded: loaded (/etc/systemd/system/amazon-ssm-agent.service; enabled; vendo>
   Active: inactive (dead) since Tue 2022-04-19 16:42:05 UTC; 2s ago
           --truncated--
```

このような場合、エージェントをアクティブ化するには、次のコマンドを実行します。

```
sudo systemctl enable amazon-ssm-agent
```

```
sudo systemctl start amazon-ssm-agent
```

ユーザーのリージョンで RHEL 8 および 9 用のカスタムエージェントインストールコマンドを作成する

スクリプトまたはテンプレートを使用する複数のインスタンスで SSM Agent をインストールする場合は、作業中の AWS リージョンに保存されているインストールファイルを使用することが推奨されます。

次のコマンドでは、米国東部 (オハイオ) リージョン (us-east-2) で、パブリックアクセス可能な S3 バケットを使用する例を示します。

> **Tip**
>
> このトピックで前述した手順 RHEL 8 または 9 の SSM Agent 用クイックインストールコマンド のグローバル URLは、構築したカスタムリージョン URL に置き換えることもできます。

次のコマンドで、*[Region]* (リージョン) をユーザー自身の情報に置き換えます。サポートされている *region* 値の一覧については、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」にある Region 列を参照してください。

x86_64

```
sudo dnf install -y https://s3.region.amazonaws.com/amazon-ssm-region/latest/
linux_amd64/amazon-ssm-agent.rpm
```

次の例を参照してください。

```
sudo dnf install -y https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/
linux_amd64/amazon-ssm-agent.rpm
```

ARM64

```
sudo dnf install -y https://s3.region.amazonaws.com/amazon-ssm-region/latest/
linux_arm64/amazon-ssm-agent.rpm
```

次の例を参照してください。

```
sudo dnf install -y https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/
linux_arm64/amazon-ssm-agent.rpm
```

RHEL 7.x に SSM Agent をインストールする

AWS が提供する RHEL 7 用 Amazon Machine Images (AMIs) には、デフォルトでは AWS Systems Manager エージェント (SSM Agent) がプリインストールされていません。このページの情報に従って、RHEL 7 インスタンスにエージェントをインストールまたは再インストールできます。

トピック

- RHEL 7 の SSM Agent 用クイックインストールコマンド
- ユーザーのリージョンで RHEL 7 用のカスタムエージェントインストールコマンドを作成する

RHEL 7 の SSM Agent 用クイックインストールコマンド

次のステップに従って、シングルインスタンスに SSM Agent を手動でインストールします。この手順では、グローバルに利用可能なインストールファイルを使用します。

RHEL 7.x に SSM Agent をインストールするには

1. SSH など、任意の方法を使用して RHEL 7 インスタンスに接続します。
2. インスタンスのアーキテクチャのコマンドをコピーして、インスタンスで実行します。

> **Note**
>
> 次のコマンドの URL には `ec2-downloads-windows` ディレクトリが含まれていますが、これらは RHEL 7 用の正しいグローバルインストールファイルです。

x86_64 インスタンス

```
sudo yum install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/
latest/linux_amd64/amazon-ssm-agent.rpm
```

ARM64 インスタンス

```
sudo yum install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/
latest/linux_arm64/amazon-ssm-agent.rpm
```

3. (推奨事項) エージェントが実行されていることを確認するには、次のコマンドを実行します。

```
sudo systemctl status amazon-ssm-agent
```

ほとんどの場合、次の例に示されているように、コマンドは、エージェントが実行中であることを報告します。

```
# amazon-ssm-agent.service - amazon-ssm-agent
   Loaded: loaded (/etc/systemd/system/amazon-ssm-agent.service; enabled; vendor
 preset: disabled)
   Active: active (running) since Tue 2022-04-19 16:47:36 UTC; 22s ago
 Main PID: 1342 (amazon-ssm-agen)
   CGroup: /system.slice/amazon-ssm-agent.service
           ##1342 /usr/bin/amazon-ssm-agent
           ##1362 /usr/bin/ssm-agent-worker
            --truncated--
```

まれに、次の例に示されているように、コマンドは、エージェントがインストールされているにも関わらず実行されていないことを報告します。

```
# amazon-ssm-agent.service - amazon-ssm-agent
   Loaded: loaded (/etc/systemd/system/amazon-ssm-agent.service; enabled; vendor
 preset: disabled)
   Active: inactive (dead) since Tue 2022-04-19 16:48:56 UTC; 5s ago
  Process: 1342 ExecStart=/usr/bin/amazon-ssm-agent (code=exited, status=0/SUCCESS)
 Main PID: 1342 (code=exited, status=0/SUCCESS)
            --truncated--
```

このような場合、エージェントをアクティブ化するには、次のコマンドを実行します。

```
sudo systemctl enable amazon-ssm-agent
```

```
sudo systemctl start amazon-ssm-agent
```

ユーザーのリージョンで RHEL 7 用のカスタムエージェントインストールコマンドを作成する

スクリプトまたはテンプレートを使用する複数のインスタンスで SSM Agent をインストールする場合は、作業中の AWS リージョンに保存されているインストールファイルを使用することが推奨されます。

次のコマンドでは、米国東部 (オハイオ) リージョン (us-east-2) で、パブリックアクセス可能な S3 バケットを使用する例を示します。

> **Tip**
>
> このトピックで前述した手順 RHEL 7 の SSM Agent 用クイックインストールコマンド のグローバル URLは、構築したカスタムリージョン URL に置き換えることもできます。

次のコマンドで、*[Region]* (リージョン) をユーザー自身の情報に置き換えます。サポートされている *region* 値の一覧については、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」にある Region 列を参照してください。

x86_64

```
sudo yum install -y https://s3.region.amazonaws.com/amazon-ssm-region/latest/
linux_amd64/amazon-ssm-agent.rpm
```

次の例を参照してください。

```
sudo yum install -y https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/
linux_amd64/amazon-ssm-agent.rpm
```

ARM64

```
sudo yum install -y https://s3.region.amazonaws.com/amazon-ssm-region/latest/
linux_arm64/amazon-ssm-agent.rpm
```

次の例を参照してください。

```
sudo yum install -y https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/
linux_arm64/amazon-ssm-agent.rpm
```

RHEL 6.x に SSM Agent をインストールする

AWS が提供する RHEL 6 用 Amazon Machine Images (AMIs) には、デフォルトでは AWS Systems Manager エージェント (SSM Agent) がプリインストールされていません。このページの情報に従って、RHEL 6 インスタンスにエージェントをインストールまたは再インストールできます。

トピック

- RHEL 6 の SSM Agent 用クイックインストールコマンド
- ユーザーのリージョンで RHEL 6 用のカスタムエージェントインストールコマンドを作成する

RHEL 6 の SSM Agent 用クイックインストールコマンド

次のステップに従って、シングルインスタンスに SSM Agent を手動でインストールします。この手順では、グローバルに利用可能なインストールファイルを使用します。

RHEL 6.x に SSM Agent をインストールするには

1. SSH など、任意の方法を使用して RHEL 6 インスタンスに接続します。
2. インスタンスのアーキテクチャのコマンドをコピーして、インスタンスで実行します。

> **Note**
>
> 次のコマンドの URL には `ec2-downloads-windows` ディレクトリが含まれていますが、これらは RHEL 6 用の正しいグローバルインストールファイルです。
> 次のコマンドは、`latest` ディレクトリの代わりにバージョンディレクトリ `3.0.1479.0` を指定します。これは、SSM Agent バージョン 3.1 以降では、RHEL 6 がサポートされていないためです。

x86_64 インスタンス

```
sudo yum install -y https://s3.amazonaws.com/ec2-downloads-windows/
SSMAgent/3.0.1479.0/linux_amd64/amazon-ssm-agent.rpm
```

x86 インスタンス

```
sudo yum install -y https://s3.amazonaws.com/ec2-downloads-windows/
SSMAgent/3.0.1479.0/linux_386/amazon-ssm-agent.rpm
```

3. (推奨事項) エージェントが実行されていることを確認するには、次のコマンドを実行します。

```
sudo status amazon-ssm-agent
```

ほとんどの場合、次の例に示されているように、コマンドは、エージェントが実行中であることを報告します。

```
amazon-ssm-agent start/running, process 1788
```

まれに、次の例に示されているように、コマンドは、エージェントがインストールされているにも関わらず実行されていないことを報告します。

```
amazon-ssm-agent stop/waiting
```

このような場合、エージェントをアクティブ化するには、次のコマンドを実行します。

```
sudo start amazon-ssm-agent
```

ユーザーのリージョンで RHEL 6 用のカスタムエージェントインストールコマンドを作成する

スクリプトまたはテンプレートを使用する複数のインスタンスで SSM Agent をインストールする場合は、作業中の AWS リージョンに保存されているインストールファイルを使用することが推奨されます。

次のコマンドでは、米国東部 (オハイオ) リージョン (us-east-2) で、パブリックアクセス可能な S3 バケットを使用する例を示します。

> **Tip**
>
> このトピックで前述した手順 RHEL 6 の SSM Agent 用クイックインストールコマンド のグローバル URLは、構築したカスタムリージョン URL に置き換えることもできます。

次のコマンドで、*[Region]* (リージョン) をユーザー自身の情報に置き換えます。サポートされている *region* 値の一覧については、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」にある Region 列を参照してください。

> **Note**
>
> 次のコマンドは、`latest` ディレクトリの代わりにバージョンディレクトリ `3.0.1479.0` を指定します。これは、SSM Agent バージョン 3.1 以降では、RHEL 6 がサポートされていないためです。

x86_64

```
sudo yum install -y https://s3.region.amazonaws.com/amazon-ssm-region/3.0.1479.0/
linux_amd64/amazon-ssm-agent.rpm
```

次の例を参照してください。

```
sudo yum install -y https://s3.us-east-2.amazonaws.com/amazon-ssm-us-
east-2/3.0.1479.0/linux_amd64/amazon-ssm-agent.rpm
```

x86

```
sudo yum install -y https://s3.region.amazonaws.com/amazon-ssm-region/3.0.1479.0/
linux_386/amazon-ssm-agent.rpm
```

次の例を参照してください。

```
sudo yum install -y https://s3.us-east-2.amazonaws.com/amazon-ssm-us-
east-2/3.0.1479.0/linux_386/amazon-ssm-agent.rpm
```

Rocky Linux インスタンスに SSM Agent を手動でインストールする

AWS が提供する Rocky Linux 用 Amazon Machine Images (AMIs) には、デフォルトでは AWS Systems Manager エージェント (SSM Agent) がプリインストールされていません。エージェントがプリインストールされている可能性のある AWS マネージド AMIs のリストについては、「SSM Agent がプリインストールされている AMIs を見つける」を参照してください。

このセクションの情報に従って、Rocky Linux インスタンスに SSM Agent を手動でインストールまたは再インストールできます。

[開始する前に]

Rocky Linux インスタンスに SSM Agent をインストールする前に、次の点に注意してください。

- すべての Linux ベースのオペレーティングシステムに SSM Agent をインストールする際に適用される重要な情報については、「Linux 用 EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする」を参照してください。

トピック

- Rocky Linux の SSM Agent 用クイックインストールコマンド
- ユーザーのリージョンで Rocky Linux 用のカスタムエージェントインストールコマンドを作成する

Rocky Linux の SSM Agent 用クイックインストールコマンド

次のステップに従って、シングルインスタンスに SSM Agent を手動でインストールします。この手順では、グローバルに利用可能なインストールファイルを使用します。

[開始する前に]

Rocky Linux インスタンスに SSM Agent をインストールする前に、次の点に注意してください。

- Python 2 または Python 3 のいずれかが Rocky Linux インスタンスにインストールされていることを確認します。これは、SSM Agent が適切に動作するための必要条件です。

Rocky Linux に SSM Agent をインストールするには

1. SSH など、任意の方法を使用して Rocky Linux インスタンスに接続します。
2. インスタンスのアーキテクチャのコマンドをコピーして、インスタンスで実行します。

> **Note**
>
> 次のコマンドの URL には ec2-downloads-windows ディレクトリが含まれていますが、これらは Rocky Linux 用の正しいグローバルインストールファイルです。

x86_64 インスタンス

```
sudo dnf install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/
latest/linux_amd64/amazon-ssm-agent.rpm
```

ARM64 インスタンス

```
sudo dnf install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/
latest/linux_arm64/amazon-ssm-agent.rpm
```

3. (推奨事項) エージェントが実行されていることを確認するには、次のコマンドを実行します。

```
sudo systemctl status amazon-ssm-agent
```

ほとんどの場合、次の例に示されているように、コマンドは、エージェントが実行中であることを報告します。

```
# amazon-ssm-agent.service - amazon-ssm-agent
   Loaded: loaded (/etc/systemd/system/amazon-ssm-agent.service; enabled; vendo>
   Active: active (running) since Tue 2022-04-19 16:40:41 UTC; 9s ago
 Main PID: 4898 (amazon-ssm-agen)
    Tasks: 14 (limit: 4821)
   Memory: 34.6M
   CGroup: /system.slice/amazon-ssm-agent.service
           ##4898 /usr/bin/amazon-ssm-agent
           ##4954 /usr/bin/ssm-agent-worker
            --truncated--
```

まれに、次の例に示されているように、コマンドは、エージェントがインストールされているにも関わらず実行されていないことを報告します。

```
# amazon-ssm-agent.service - amazon-ssm-agent
   Loaded: loaded (/etc/systemd/system/amazon-ssm-agent.service; enabled; vendo>
```

```
   Active: inactive (dead) since Tue 2022-04-19 16:42:05 UTC; 2s ago
          --truncated--
```

このような場合、エージェントをアクティブ化するには、次のコマンドを実行します。

```
sudo systemctl enable amazon-ssm-agent
```

```
sudo systemctl start amazon-ssm-agent
```

ユーザーのリージョンで Rocky Linux 用のカスタムエージェントインストールコマンドを作成する

スクリプトまたはテンプレートを使用する複数のインスタンスで SSM Agent をインストールする場合は、作業中の AWS リージョンに保存されているインストールファイルを使用することが推奨されます。

次のコマンドでは、米国東部 (オハイオ) リージョン (us-east-2) で、パブリックアクセス可能な S3 バケットを使用する例を示します。

> **Tip**
>
> このトピックで前述した手順 Rocky Linux の SSM Agent 用クイックインストールコマンドのグローバル URLは、構築したカスタムリージョン URL に置き換えることもできます。

次のコマンドで、*[Region]* (リージョン) をユーザー自身の情報に置き換えます。サポートされている *region* 値の一覧については、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」にある Region 列を参照してください。

x86_64

```
sudo dnf install -y https://s3.region.amazonaws.com/amazon-ssm-region/latest/
linux_amd64/amazon-ssm-agent.rpm
```

次の例を参照してください。

```
sudo dnf install -y https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/
linux_amd64/amazon-ssm-agent.rpm
```

ARM64

```
sudo dnf install -y https://s3.region.amazonaws.com/amazon-ssm-region/latest/
linux_arm64/amazon-ssm-agent.rpm
```

次の例を参照してください。

```
sudo dnf install -y https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/
linux_arm64/amazon-ssm-agent.rpm
```

SUSE Linux Enterprise Server インスタンスに SSM Agent を手動でインストールする

ほとんどの場合、AWS が提供する SUSE Linux Enterprise Server (SLES) 用 Amazon Machine Images (AMIs) には、デフォルトで AWS Systems Manager エージェント (SSM Agent) がプリインストールされています。詳細については、「SSM Agent がプリインストールされている AMIs を見つける」を参照してください。

新しい SLES インスタンスに SSM Agent がプリインストールされていない場合や、エージェントを手動で再インストールする必要がある場合は、このページの情報を参考にしてください。

[開始する前に]

SLES インスタンスに SSM Agent をインストールする前に、次の点に注意してください。

- すべての Linux ベースのオペレーティングシステムに SSM Agent をインストールする際に適用される重要な情報については、「Linux 用 EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする」を参照してください。

トピック

- SLES の SSM Agent 用クイックインストールコマンド
- ユーザーのリージョンで SLES 用のカスタムエージェントインストールコマンドを作成する

SLES の SSM Agent 用クイックインストールコマンド

次のステップに従って、シングルインスタンスに SSM Agent を手動でインストールします。この手順では、グローバルに利用可能なインストールファイルを使用します。

クイックコピーアンドペーストコマンドを使用して SLES に SSM Agent をインストールするには

1. SSH など、任意の方法を使用して SLES インスタンスに接続します。
2. オプション 1: zypperコマンドを使用します:

   - 次のコマンドを実行してください。

     ```
     sudo zypper install amazon-ssm-agent
     ```

   - プロンプトに対応して y を入力します。

   オプション 2: rpmコマンドを使用します。

   - インスタンスに一時ディレクトリを作成します。

     ```
     mkdir /tmp/ssm
     ```

   - 一時ディレクトリに変更します。

     ```
     cd /tmp/ssm
     ```

   - SSM Agent インストーラをダウンロードして実行するには、次のコマンドを一度に 1 つずつ実行します。

     > **Note**
     >
     > 次のコマンドの URL には ec2-downloads-windows ディレクトリが含まれていますが、これらは SLES 用の正しいグローバルインストールファイルです。

     x86_64 インスタンス:

     ```
     wget https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/linux_amd64/
     amazon-ssm-agent.rpm
     ```

     ARM64 インスタンス:

     ```
     wget https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/linux_arm64/
     amazon-ssm-agent.rpm
     ```

- 以下のコマンドを実行してください。

```
sudo rpm --install amazon-ssm-agent.rpm
```

- (推奨事項) エージェントが実行されていることを確認するには、次のコマンドを実行します。

```
sudo systemctl status amazon-ssm-agent
```

ほとんどの場合、次の例に示されているように、コマンドは、エージェントが実行中であることを報告します。

```
# amazon-ssm-agent.service - amazon-ssm-agent
 Loaded: loaded (/usr/lib/systemd/system/amazon-ssm-agent.service; enabled;
 vendor preset: disabled)
 Active: active (running) since Mon 2022-02-21 23:13:28 UTC; 7s ago
 Main PID: 2102 (amazon-ssm-agen)
 Tasks: 15 (limit: 512)
 CGroup: /system.slice/amazon-ssm-agent.service
 ##2102 /usr/sbin/amazon-ssm-agent
 ##2107 /usr/sbin/ssm-agent-worker
            --truncated--
```

まれに、次の例に示されているように、コマンドは、エージェントがインストールされているにも関わらず実行されていないことを報告します。

```
# amazon-ssm-agent.service - amazon-ssm-agent
   Loaded: loaded (/usr/lib/systemd/system/amazon-ssm-agent.service; disabled;
 vendor preset: disabled)
   Active: inactive (dead)
            --truncated--
```

このような場合、エージェントをアクティブ化するには、次のコマンドを実行します。

```
sudo systemctl enable amazon-ssm-agent
```

```
sudo systemctl start amazon-ssm-agent
```

ユーザーのリージョンで SLES 用のカスタムエージェントインストールコマンドを作成する

スクリプトまたはテンプレートを使用する複数のインスタンスで SSM Agent をインストールする場合は、作業中の AWS リージョンに保存されているインストールファイルを使用することが推奨されます。

次のコマンドでは、米国東部 (オハイオ) リージョン (us-east-2) で、パブリックアクセス可能な S3 バケットを使用する例を示します。

> **Tip**
>
> このトピックで前述した手順 Amazon Linux 1 の SSM Agent 用クイックインストールコマンド のグローバル URLは、構築したカスタムリージョン URL に置き換えることもできます。

次のコマンドで、*[Region]* (リージョン) をユーザー自身の情報に置き換えます。サポートされている *region* 値の一覧については、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」にある Region 列を参照してください。

x86_64

```
wget https://s3.region.amazonaws.com/amazon-ssm-region/latest/linux_amd64/amazon-ssm-agent.rpm
```

```
sudo rpm --install amazon-ssm-agent.rpm
```

次の例を参照してください。

```
wget https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/linux_amd64/amazon-ssm-agent.rpm
```

```
sudo rpm --install amazon-ssm-agent.rpm
```

ARM64

```
wget https://s3.region.amazonaws.com/amazon-ssm-region/latest/linux_arm64/amazon-ssm-agent.rpm
```

```
sudo rpm --install amazon-ssm-agent.rpm
```

次の例を参照してください。

```
wget https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/linux_arm64/
amazon-ssm-agent.rpm
```

```
sudo rpm --install amazon-ssm-agent.rpm
```

Ubuntu Server インスタンスに SSM Agent を手動でインストールする

> **Important**
>
> 64 ビットバージョンの Ubuntu Server に SSM Agent をインストールする前に、正しいインストールツールを使用していることを確認してください。識別番号が 20180627 以降の Amazon マシンイメージ (AMI) では、SSM Agent は Snap パッケージを使用してバージョン 16.04 にプリインストールされています。以前の AMI から作成されたインスタンスでは、deb インストーラパッケージを使用して SSM Agent をインストールする必要があります。詳細については、「正しい SSM Agent バージョンを特定して、64 ビット Ubuntu Server 16.04 インスタンスにインストールする」を参照してください。

ほとんどの場合、AWS が提供する Ubuntu Server 用 Amazon Machine Images (AMIs) には、デフォルトで AWS Systems Manager エージェント (SSM Agent) がプリインストールされています。詳細については、「SSM Agent がプリインストールされている AMIs を見つける」を参照してください。

新しい Ubuntu Server インスタンスに SSM Agent がプリインストールされていない場合や、エージェントを手動で再インストールする必要がある場合は、このセクションの情報を参考にしてください。

開始する前に

Ubuntu Server インスタンスに SSM Agent をインストールする前に、次の点に注意してください。

- すべての Linux ベースのオペレーティングシステムに SSM Agent をインストールする際に適用される重要な情報については、「Linux 用 EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする」を参照してください。

トピック

- Ubuntu Server 22.04 LTS、20.10 STR および 20.04、18.04、16.04 LTS 64 ビット (Snap) に SSM Agent をインストールする
- Ubuntu Server 16.04 および 14.04 64 ビット (deb) に SSM Agent をインストールする
- Ubuntu Server 16.04 および 14.04 32 ビットに SSM Agent をインストールする
- 正しい SSM Agent バージョンを特定して、64 ビット Ubuntu Server 16.04 インスタンスにインストールする

Ubuntu Server 22.04 LTS、20.10 STR および 20.04、18.04、16.04 LTS 64 ビット (Snap) に SSM Agent をインストールする

[開始する前に]

Ubuntu Server 22.04 LTS、20.10 STR および 20.04、18.04、16.04 LTS 64 ビット (Snap) に SSM Agent をインストールする前に、次の点に注意してください。

Snap または deb インストーラによるバージョン 16.04 のインストール

Ubuntu Server 16.04 では、SSM Agentは 16.04 AMI のバージョンに応じて、Snap または deb インストールパッケージのいずれかを使用してインストールされます。

SSM Agent インストーラファイルの場所

Ubuntu Server 22.04 LTS、20.10 STR および 20.04、18.04、16.04 LTS (Snap 付き) の場合、SSM Agent インストーラファイル (エージェントバイナリや設定ファイルなど) は `/snap/amazon-ssm-agent/current/` ディレクトリに保存されています。このディレクトリで設定ファイルに変更を加えた場合、これらのファイルを `/snap` ディレクトリから `/etc/amazon/ssm/` ディレクトリにコピーする必要があります。ログファイルおよびライブラリファイルは変更されていません (`/var/lib/amazon/ssm`、`/var/log/amazon/ssm`)。

Snap `candidate` チャンネルの使用

Snap ストアの候補チャネル (安定チャネルではなく) には、SSM Agent の最新バージョン (最新のバグ修正のすべてを含む) が含まれています。候補チャネルと安定チャネルの違いの詳細については、https://snapcraft.io/docs/channels の「リスクレベル」を参照してください。

候補チャンネルの SSM Agent バージョン情報を追跡する場合は、Ubuntu Server 20.10 STR および 20.04、18.04、16.04 LTS 64 ビットインスタンスで次のコマンドを実行します。

```
sudo snap switch --channel=candidate amazon-ssm-agent
```

バージョン 18.04 以降で推奨される Snap

Ubuntu Server 22.04 LTS、20.10 STR および 20.04、18.04 LTS では、Snap のみを使用することをお勧めします。また、エージェントの 1 つのインスタンスのみがインスタンスにインストールされて実行されていることを確認してください。Snap なしで SSM Agent を使用する場合は、SSM Agent をアンインストールします。続いて、SSM Agent を Ubuntu Server 16.04 および 14.04 64 ビット (deb) にインストールする手順に従って、SSM Agent を Debian パッケージとしてインストールします。インストールする前に、debian パッケージとして管理するパッケージのリストと重複する Snap がインストールされていないことを確認します。

`Maximum timeout exceeded` エラーメッセージ

Snap の既知の問題により、`Maximum timeout exceeded` コマンドの使用時に `snap` エラーが表示される場合があります。このエラーが表示された場合は、以下のコマンドを一度に 1 つずつ実行してエージェントの起動、停止、およびステータスの確認を行います。

```
sudo systemctl start snap.amazon-ssm-agent.amazon-ssm-agent.service
```

```
sudo systemctl stop snap.amazon-ssm-agent.amazon-ssm-agent.service
```

```
sudo systemctl status snap.amazon-ssm-agent.amazon-ssm-agent.service
```

Ubuntu Server 22.04 LTS、20.10 STR および 20.04、18.04、16.04 LTS 64 ビットインスタンス (Snap パッケージ付き) に SSM Agent をインストールするには

1. 識別子が 20180627 以降の Ubuntu Server 22.04 LTS、20.04、18.04、16.04 LTS 64 ビット AMIs では、SSM Agent はデフォルトでインストールされます。

   SSM Agent オンプレミスサーバーにインストールする場合やエージェントを再インストールする場合は、次のスクリプトを使用できます。ダウンロードの URL を指定する必要はありません。`snap` コマンドでは、エージェントが Snap アプリストア https://snapcraft.io から自動的にダウンロードされます。

   ```
   sudo snap install amazon-ssm-agent --classic
   ```

2. SSM Agent が実行中であるかどうかを判断するために次のコマンドを実行します。

   ```
   sudo snap list amazon-ssm-agent
   ```

3. 前のコマンドから、amazon-ssm-agent is stopped、inactive、disabled が返された場合は、以下のコマンドを実行してサービスを開始します。

```
sudo snap start amazon-ssm-agent
```

4. エージェントのステータスを確認します。

```
sudo snap services amazon-ssm-agent
```

Ubuntu Server 16.04 および 14.04 64 ビット (deb) に SSM Agent をインストールする

> **Important**
>
> 64 ビットバージョンの Ubuntu Server に SSM Agent をインストールする前に、正しいインストールツールを使用していることを確認してください。識別番号が 20180627 以降の Amazon マシンイメージ (AMI) では、SSM Agent は Snap パッケージを使用してバージョン 16.04 にプリインストールされています。以前の AMI から作成されたインスタンスでは、deb インストーラパッケージを使用して SSM Agent をインストールする必要があります。詳細については、「正しい SSM Agent バージョンを特定して、64 ビット Ubuntu Server 16.04 インスタンスにインストールする」を参照してください。SSM Agent が Snap と連動したインスタンスにインストールされた状態で、deb インストーラパッケージを使用して SSM Agent をインストールまたは更新すると、インストールまたは SSM Agent オペレーションは失敗する可能性があります。

ほとんどの場合、AWS が提供する Amazon Machine Images (AMIs) Ubuntu Server 16.04 には、デフォルトで AWS Systems Manager エージェント (SSM Agent) がプリインストールされています。詳細については、「SSM Agent がプリインストールされている AMIs を見つける」を参照してください。

バージョン 20180627 以前の新しい Ubuntu Server 16.04 インスタンスに SSM Agent がプリインストールされていない状態で、Ubuntu Server 14.04 にエージェントをインストールする場合や、手動で再インストールする必要がある場合は、このページの情報を参考にしてください。

Ubuntu Server 16.04 および 14.04 64 ビット (deb) の SSM Agent 用クイックインストールコマンド

次のステップに従って、シングルインスタンスに SSM Agent を手動でインストールします。この手順では、グローバルに利用可能なインストールファイルを使用します。

クイックコピーアンドペーストコマンドを使用して Ubuntu Server 16.04 および 14.04 64 ビット (deb) に SSM Agent をインストールするには

1. SSH など、任意の方法を使用して Ubuntu Server インスタンスに接続します。
2. 次のコマンドを実行して、インスタンスに一時ディレクトリを作成します。

```
mkdir /tmp/ssm
```

3. 一時ディレクトリに変更します。

```
cd /tmp/ssm
```

4. 以下のコマンドを実行します。

> **Note**
>
> 次のコマンドの URL には `ec2-downloads-windows` ディレクトリが含まれていますが、これらは Ubuntu Server 16.04 および 14.04 64 ビット用の正しいグローバルインストールファイルです。

```
wget https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/debian_amd64/
amazon-ssm-agent.deb
```

```
sudo dpkg -i amazon-ssm-agent.deb
```

5. (推奨事項) 以下のコマンドのいずれかを実行し、SSM Agent が実行中であるかどうかを特定します。

   Ubuntu Server 16.04

   ```
   sudo systemctl status amazon-ssm-agent
   ```

   Ubuntu Server 14.04

   ```
   sudo status amazon-ssm-agent
   ```

   ほとんどの場合、コマンドは、エージェントが実行中であることを報告します。

まれに、次の例に示されているように、コマンドは、エージェントがインストールされているにも関わらず実行されていないことを報告します。

6. 前のコマンドから、`amazon-ssm-agent is stopped`、`inactive`、`disabled` が返された場合は、次のいずれかのコマンドを実行してサービスを開始します。

   Ubuntu Server 16.04:

   ```
   sudo systemctl enable amazon-ssm-agent
   ```

   Ubuntu Server 14.04:

   ```
   sudo start amazon-ssm-agent
   ```

ユーザーのリージョンの Ubuntu Server 16.04 および 14.04 64 ビット (deb) で SSM Agent 用のカスタムインストールコマンドを作成する

スクリプトまたはテンプレートを使用する複数のインスタンスで SSM Agent をインストールする場合は、作業中の AWS リージョンに保存されているインストールファイルを使用することが推奨されます。

次のコマンドでは、米国東部 (オハイオ) リージョン (`us-east-2`) で、パブリックアクセス可能な S3 バケットを使用する例を示します。

> **Tip**
>
> このトピックで前述した手順 Ubuntu Server 16.04 および 14.04 64 ビット (deb) の SSM Agent 用クイックインストールコマンド のグローバル URL は、構築したカスタムリージョン URL に置き換えることもできます。

次のコマンドで、*`[Region]`* (リージョン) をユーザー自身の情報に置き換えます。サポートされている *`region`* 値の一覧については、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」にある Region 列を参照してください。

```
wget https://s3.region.amazonaws.com/amazon-ssm-region/latest/debian_amd64/amazon-ssm-agent.deb
```

```
sudo dpkg -i amazon-ssm-agent.deb
```

次の例を参照してください。

```
wget https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/debian_amd64/
amazon-ssm-agent.deb
```

```
sudo dpkg -i amazon-ssm-agent.deb
```

Ubuntu Server 16.04 および 14.04 32 ビットに SSM Agent をインストールする

ほとんどの場合、AWS が提供する Amazon Machine Images (AMIs) Ubuntu Server 16.04 には、デフォルトで AWS Systems Manager エージェント (SSM Agent) がプリインストールされています。詳細については、「SSM Agent がプリインストールされている AMIs を見つける」を参照してください。

新しい Ubuntu Server 16.04 インスタンスに SSM Agent がプリインストールされていない状態で Ubuntu Server 14.04 にエージェントをインストールする場合や、手動で再インストールする必要がある場合は、このページの情報を参考にしてください。

Ubuntu Server 16.04 および 14.04 の 32 ビット (deb) の SSM Agent 用クイックインストールコマンド

次のステップに従って、シングルインスタンスに SSM Agent を手動でインストールします。この手順では、グローバルに利用可能なインストールファイルを使用します。

クイックコピーアンドペーストコマンドを使用して Ubuntu Server 16.04 および 14.04 32 ビット (deb) に SSM Agent をインストールするには

1. SSH など、任意の方法を使用して Ubuntu Server インスタンスに接続します。
2. 次のコマンドを実行して、インスタンスに一時ディレクトリを作成します。

   ```
   mkdir /tmp/ssm
   ```

3. 一時ディレクトリに変更します。

   ```
   cd /tmp/ssm
   ```

4. 以下のコマンドを実行します。

> **Note**
>
> 次のコマンドの URL には ec2-downloads-windows ディレクトリが含まれていますが、これらは Ubuntu Server 16.04 および 14.04 の 32 ビット用の正しいグローバルインストールファイルです。

```
wget https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/debian_386/
amazon-ssm-agent.deb
```

```
sudo dpkg -i amazon-ssm-agent.deb
```

5. (推奨事項) 以下のコマンドのいずれかを実行し、SSM Agent が実行中であるかどうかを特定します。

   Ubuntu Server 16.04

   ```
   sudo systemctl status amazon-ssm-agent
   ```

   Ubuntu Server 14.04

   ```
   sudo status amazon-ssm-agent
   ```

   ほとんどの場合、コマンドは、エージェントが実行中であることを報告します。

   まれに、次の例に示されているように、コマンドは、エージェントがインストールされているにも関わらず実行されていないことを報告します。

6. 前のコマンドから、amazon-ssm-agent is stopped、inactive、disabled が返された場合は、次のいずれかのコマンドを実行してサービスを開始します。

   Ubuntu Server 16.04:

   ```
   sudo systemctl enable amazon-ssm-agent
   ```

   Ubuntu Server 14.04:

```
sudo start amazon-ssm-agent
```

ユーザーのリージョンの Ubuntu Server 16.04 および 14.04 32 ビット (deb) で SSM Agent 用のカスタムインストールコマンドを作成する

スクリプトまたはテンプレートを使用する複数のインスタンスで SSM Agent をインストールする場合は、作業中の AWS リージョンに保存されているインストールファイルを使用することが推奨されます。

次のコマンドでは、米国東部 (オハイオ) リージョン (us-east-2) で、パブリックアクセス可能な S3 バケットを使用する例を示します。

> **Tip**
>
> このトピックで前述した手順 Ubuntu Server 16.04 および 14.04 の 32 ビット (deb) の SSM Agent 用クイックインストールコマンド のグローバル URL は、構築したカスタムリージョン URL に置き換えることもできます。

次のコマンドで、*[Region]* (リージョン) をユーザー自身の情報に置き換えます。サポートされている *region* 値の一覧については、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」にある Region 列を参照してください。

```
wget https://s3.region.amazonaws.com/amazon-ssm-region/latest/debian_386/amazon-ssm-agent.deb
```

```
sudo dpkg -i amazon-ssm-agent.deb
```

次の例を参照してください。

```
wget https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/debian_386/amazon-ssm-agent.deb
```

```
sudo dpkg -i amazon-ssm-agent.deb
```

正しい SSM Agent バージョンを特定して、64 ビット Ubuntu Server 16.04 インスタンスにインストールする

> **Important**
>
> 64 ビットバージョンの Ubuntu Server に SSM Agent をインストールする前に、正しいインストールツールを使用していることを確認してください。識別番号が 20180627 以降の Amazon マシンイメージ (AMI) では、SSM Agent は Snap パッケージを使用してバージョン 16.04 にプリインストールされています。以前の AMI から作成されたインスタンスでは、deb インストーラパッケージを使用して SSM Agent をインストールする必要があります。詳細については、「正しい SSM Agent バージョンを特定して、64 ビット Ubuntu Server 16.04 インスタンスにインストールする」を参照してください。
> インスタンスに SSM Agent のインストールが複数ある場合は注意してください (たとえば、1 つは Snap を使用してインストールされ、1 つは deb インストーラを使用してインストールされている場合)。エージェントのオペレーションは正しく機能しません。

インスタンスのソースの AMI ID の作成日は、以下のいずれかの方法で確認できます。これらの手順は、AWS マネージド AMIs にのみ適用されます。

ソースの AMI ID の作成日を確認する (コンソール)

1. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
2. 左のナビゲーションペインで、[Instances] (インスタンス) をクリックします。
3. インスタンスを選択します。
4. [詳細] タブで、[AMI 名] フィールドの下にある値の YYYYMMDD 識別子をチェックします。例: `ubuntu/images/hvm-ssd/ubuntu-xenial-16.04-amd64-server-20180627`。

ソースの AMI ID の作成日の確認 (AWS CLI)

- 次のコマンドを実行します。

  ```
  aws ec2 describe-images --image-ids ami-id
  ```

  ami-id は、AMI から提供されている AWS の ID を表します (`ami-07c8bc5c1ce9598c3` など)。

正常に終了すると、コマンドは次のような情報が返され、ここでは、CreationDate フィールドと Name フィールドで情報を確認できます。

```
{
    "Images": [
        {
            "Architecture": "x86_64",
            "CreationDate": "2020-07-24T20:40:27.000Z",
            "ImageId": "ami-07c8bc5c1ce9598c3",
-- truncated --
            "ImageOwnerAlias": "amazon",
            "Name": "amzn2-ami-hvm-2.0.20200722.0-x86_64-gp2",
            "RootDeviceName": "/dev/xvda",
            "RootDeviceType": "ebs",
            "SriovNetSupport": "simple",
            "VirtualizationType": "hvm"
        }
    ]
}
```

Linux ノードでプロキシを使用するための SSM Agent の設定

オーバーライド設定ファイルを作成してhttp_proxy、https_proxy、no_proxy、 の設定をファイルに追加することで、HTTP プロキシ経由で通信するように AWS Systems Manager Agent (SSM Agent) を設定できます。より新しいバージョンまたはより古いバージョンの SSM Agent をインストールすると、オーバーライドファイルにもプロキシ設定が保持されます。このセクションには、upstart 環境および systemd 環境の両方で上書きファイルを作成するための手順が含まれています。Session Manager を使用する予定の場合は、HTTPS プロキシサーバーはサポートされていないことに注意してください。

トピック

- プロキシを使用するように SSM Agent を設定する (Upstart)
- プロキシを使用するように SSM Agent を設定する (systemd)

プロキシを使用するように SSM Agent を設定する (Upstart)

upstart 環境のオーバーライド設定ファイルを作成するには、以下の手順に従います。

SSM Agent がプロキシ (Upstart) を使用するように設定する

1. SSM Agent をインストールした先のマネージドインスタンスに接続します。
2. VIM などの単純なエディタを開き、HTTP プロキシサーバーと HTTPS プロキシサーバーのどちらを使用しているかに応じて、以下のいずれかの設定オプションを追加します。

   HTTP プロキシサーバーの場合:

   ```
   env http_proxy=http://hostname:port
   env https_proxy=http://hostname:port
   env no_proxy=IP address for instance metadata services (IMDS)
   ```

   HTTPS プロキシサーバーの場合:

   ```
   env http_proxy=http://hostname:port
   env https_proxy=https://hostname:port
   env no_proxy=IP address for instance metadata services (IMDS)
   ```

   > **Important**
   >
   > no_proxy 設定をファイルに追加し、その IP アドレスを指定します。no_proxy の IP アドレスは、Systems Manager のインスタンスメタデータサービス (IMDS) エンドポイントです。no_proxy を指定しない場合、Systems Manager への呼び出しによってプロキシサービスからアイデンティティを引き受けるか (IMDSv1 フォールバックが有効の場合)、Systems Manager への呼び出しが失敗します (IMDSv2 が強制されている場合)。
   >
   > - IPv4 の場合は、no_proxy=169.254.169.254 を指定します。
   > - IPv6 の場合は、no_proxy=[fd00:ec2::254] を指定します。インスタンスメタデータサービスの IPv6 アドレスは、IMDSv2 コマンドと互換性があります。IPv6 アドレスは、AWS Nitro System 上に構築されたインスタンスでのみアクセス可能です。詳細については、「Amazon EC2 ユーザーガイド」の「インスタンスメタデータサービスバージョン 2 の仕組み」を参照してください。

3. amazon-ssm-agent.override という名前のファイルを次の場所に保存します: /etc/init/
4. 次のコマンドを使用して SSM Agent を停止し、再起動します。

   ```
   sudo service stop amazon-ssm-agent
   sudo service start amazon-ssm-agent
   ```

> **Note**
>
> Upstart 環境で `.override` ファイルを使用する詳しい方法については、「init: Upstart init daemon job configuration」を参照してください。

プロキシを使用するように SSM Agent を設定する (systemd)

`systemd` 環境内でプロキシを使用するように SSM Agent を設定するには、次の手順に従います。

> **Note**
>
> この手順のステップの一部には、SSM Agent が Snap を使用してインストールされた Ubuntu Server インスタンス用の明示的な手順が含まれています。

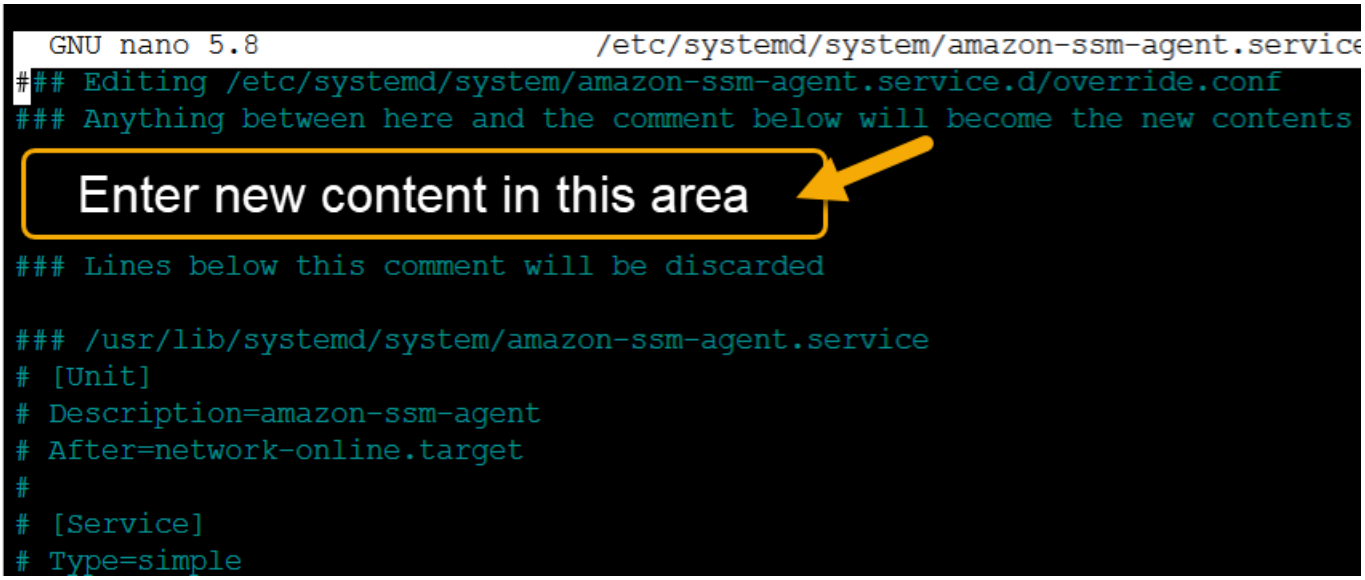
1. SSM Agent をインストールした先のインスタンスに接続します。
2. オペレーティングシステムの種類に応じて、次のいずれかのコマンドを実行します。
   - スナップを使用して SSM Agent がインストールされる Ubuntu Server インスタンスでは、次の操作を行います。

     ```
     sudo systemctl edit snap.amazon-ssm-agent.amazon-ssm-agent
     ```

     他のオペレーティングシステムで以下の手順を実行します。

     ```
     sudo systemctl edit amazon-ssm-agent
     ```
3. VIM などの単純なエディタを開き、HTTP プロキシサーバーと HTTPS プロキシサーバーのどちらを使用しているかに応じて、以下のいずれかの設定オプションを追加します。

   次の図に示すように、情報は必ず「`### Lines below this comment will be discarded`」というコメントより上に入力してください。



HTTP プロキシサーバーの場合:

```
[Service]
Environment="http_proxy=http://hostname:port"
Environment="https_proxy=http://hostname:port"
Environment="no_proxy=IP address for instance metadata services (IMDS)"
```

HTTPS プロキシサーバーの場合:

```
[Service]
Environment="http_proxy=http://hostname:port"
Environment="https_proxy=https://hostname:port"
Environment="no_proxy=IP address for instance metadata services (IMDS)"
```

Important

no_proxy 設定をファイルに追加し、その IP アドレスを指定します。no_proxy の IP アドレスは、Systems Manager のインスタンスメタデータサービス (IMDS) エンドポイントです。no_proxy を指定しない場合、Systems Manager への呼び出しによってプロキシサービスからアイデンティティを引き受けるか (IMDSv1 フォールバックが有効の場合)、Systems Manager への呼び出しが失敗します (IMDSv2 が強制されている場合)。

- IPv4 の場合は、no_proxy=169.254.169.254 を指定します。
- IPv6 の場合は、no_proxy=[fd00:ec2::254] を指定します。インスタンスメタデータサービスの IPv6 アドレスは、IMDSv2 コマンドと互換性があります。IPv6 ア

ドレスは、AWS Nitro System 上に構築されたインスタンスでのみアクセス可能です。詳細については、「Amazon EC2 ユーザーガイド」の「インスタンスメタデータサービスバージョン 2 の仕組み」を参照してください。

4. 変更を保存します。オペレーティングシステムの種類に応じて、次のいずれかのファイルが自動的に作成されます。

   - スナップを使用して SSM Agent がインストールされる Ubuntu Server インスタンスでは、次の操作を行います。

     `/etc/systemd/system/snap.amazon-ssm-agent.amazon-ssm-agent.service.d/override.conf`

   - Amazon Linux 2 および Amazon Linux 2023 インスタンスの場合:

     `/etc/systemd/system/amazon-ssm-agent.service.d/override.conf`

   - 他のオペレーティングシステムで以下の手順を実行します。

     `/etc/systemd/system/amazon-ssm-agent.service.d/amazon-ssm-agent.override`

5. オペレーティングシステムの種類に応じて、次のいずれかの SSM Agent コマンドを使用して再起動します。

   - スナップを使用してインストールされた Ubuntu Server インスタンスで、次の操作を行います。

     ```
     sudo systemctl daemon-reload && sudo systemctl restart snap.amazon-ssm-agent.amazon-ssm-agent
     ```

   - 他のオペレーティングシステムで以下の手順を実行します。

     ```
     sudo systemctl daemon-reload && sudo systemctl restart amazon-ssm-agent
     ```

> **Note**
>
> systemd 環境で `.override` ファイルを使用する方法については、Red Hat Enterprise Linux 7 システム管理者ガイドの「既存のユニットファイルの変更」を参照してください。

macOS 用 EC2 インスタンスで SSM Agent を使用する

AWS Systems Manager (SSM Agent) は Systems Manager リクエストを処理し、リクエストで指定されたとおりにマシンを設定します。macOS の SSM Agent をインストール、設定、またはアンインストールには、次の手順を使用します。

> **Note**
>
> macOS の場合、SSM Agent はデフォルトで Amazon Machine Images (AMIs) にプレインストールされています。アンインストールされていない限り、macOS の Amazon Elastic Compute Cloud (Amazon EC2) インスタンスに SSM Agent をインストールする必要はありません。

SSM Agent のソースコードが GitHub に用意されているので、ニーズに応じてエージェントを調整できます。含めることを希望する変更について、プルリクエストを送信することをお勧めします。ただし、AWS はこのソフトウェアの変更されたコピーの実行をサポートしていません。

> **Note**
>
> SSM Agent エージェントのバージョン別の詳細を確認するには、リリースノートを参照してください。

macOSオペレーティングシステムに手動で SSM Agent をインストールする前に、次の情報を確認してください。

- SSM Agent は EC2 インスタンスにデフォルトでインストールされ、Amazon Machine Images は Systems Manager でサポートされています。詳細については、macOS でサポートされているオペレーティングシステムのリストを参照してください。

  SSM Agent は、アンインストールしない限り、macOS EC2 インスタンスに手動でインストールする必要はありません。
- macOS EC2 インスタンスは、どの AWS リージョンでもサポートされていません。x86 ベースおよび M1 の EC2 インスタンスが、macOS 向けとしてサポートされているリージョンのリストについては、Amazon EC2 のよくある質問の「macOS ワークロード」を参照してください。
- 新しいツールが Systems Manager に追加されるか、既存のツールが更新されると必ず、更新されたバージョンの SSM Agent がリリースされます。最新バージョンのエージェントを使用しない

と、マネージドノードが Systems Manager の各種ツールや機能を使用できなくなる可能性があります。このため、マシン上で SSM Agent を最新状態に維持するプロセスを自動化することをお勧めします。詳細については、SSM Agent への更新の自動化 を参照してください。GitHub の「SSM Agent リリースノート」ページをサブスクライブすると、SSM Agent の更新に関する通知を受け取ることができます。

トピック

- macOS 用の EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする

macOS 用の EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする

macOS インスタンスに接続し、次の手順を実行して、AWS Systems Manager Agent (SSM Agent) をインストールします。Systems Manager を使用してコマンドを実行するインスタンスごとに以下の手順を実行します。この手順で提供されるコマンドは、ユーザーデータを通じてスクリプトとして Amazon EC2 インスタンスに渡すこともできます。

[開始する前に]

Homebrew を使用して `wget` をインストールします。

macOS に SSM Agent をインストールするには

1. 次のコマンドを使用して、x86_64 インスタンスのエージェントインストーラをダウンロードします。

   次のコマンドで、*[Region]* (リージョン) をユーザー自身の情報に置き換えます。サポートされている *region* 値の一覧については、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」にある Region 列を参照してください。

   ```
   sudo wget https://s3.region.amazonaws.com/amazon-ssm-region/latest/darwin_amd64/amazon-ssm-agent.pkg
   ```

   Apple silicon インスタンスには次のコマンドを使用します。

   ```
   sudo wget https://s3.region.amazonaws.com/amazon-ssm-region/latest/darwin_arm64/amazon-ssm-agent.pkg
   ```

以下はその例です。

```
sudo wget https://s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/latest/
darwin_amd64/amazon-ssm-agent.pkg
```

2. SSM Agent インストーラを実行するには、次のコマンドを使用します。

   x86_64:

   ```
   sudo installer -pkg amazon-ssm-agent.pkg -target /
   ```

3. エージェントのステータスを確認します。

   SSM Agent が実行中かどうかを確認するには、エージェントログを `/var/log/amazon/ssm/amazon-ssm-agent.log` で確認します。

4. エージェントログに「amazon-ssm-agent is stopped」と表示される場合は、以下のコマンドを実行してサービスを開始します。

   ```
   sudo launchctl load -w /Library/LaunchDaemons/com.amazon.aws.ssm.plist && sudo
    launchctl start com.amazon.aws.ssm
   ```

> **Important**
>
> 新しいツールが Systems Manager に追加されるか、既存のツールが更新されると必ず、更新されたバージョンの SSM Agent がリリースされます。最新バージョンのエージェントを使用しないと、マネージドノードが Systems Manager の各種ツールや機能を使用できなくなる可能性があります。このため、マシン上で SSM Agent を最新状態に維持するプロセスを自動化することをお勧めします。詳細については、SSM Agent への更新の自動化 を参照してください。GitHub の「SSM Agent リリースノート」ページをサブスクライブすると、SSM Agent の更新に関する通知を受け取ることができます。

macOSインスタンスから SSM Agent をアンインストール

macOS は PKG ファイルのアンインストールをネイティブでサポートしていません。AWS Systems Manager Agent (SSM Agent) を macOS v 用の Amazon Elastic Compute Cloud (Amazon EC2) イン

スタンスからアンインストールするには、次の場所から AWS マネージドスクリプトを使用できます。

https://github.com/aws/amazon-ssm-agent/blob/mainline/Tools/src/update/darwin/uninstall.sh

Windows Server 用 EC2 インスタンスで SSM Agent を使用する

AWS が提供する Windows Server 用の Amazon Machine Images (AMIs) には、デフォルトで AWS Systems Manager エージェント (SSM Agent) がプリインストールされています。以下のオペレーティングシステム (OS) のバージョンに、サポートが提供されます。

- 2016 年 11 月以降に公開された Windows Server 2008-2012 R2 AMIs
- Windows Server 2016、2019、2022 (Nano バージョンを除く)、および 2025

以前のバージョンのサポートに関する注意

2016 年 11 月より前に公開された Windows Server AMIs は、リクエストの処理とインスタンスの設定に EC2Config サービスを使用します。

EC2Config サービスまたは以前のバージョンの SSM Agent を使用して Systems Manager リクエストを処理する理由が特にない限り、ハイブリッドおよびマルチクラウド環境で Systems Manager 用に設定された各 Amazon Elastic Compute Cloud (Amazon EC2) インスタンスまたは非 EC2 マシンに、SSM Agent の最新バージョンをダウンロードしてインストールすることをお勧めします。

2020 年 1 月 14 日以降、Windows Server 2008 は Microsoft の機能更新プログラムまたはセキュリティ更新プログラムでサポートされなくなりました。Windows Server 2008 および 2008 R2 のレガシー Amazon Machine Images (AMIs) には、依然としてバージョン 2 の SSM Agent がプリインストールされていますが、Systems Manager は 2008 バージョンを正式にサポートしなくなり、これらのバージョンの Windows Server のエージェントを更新しなくなりました。さらに、SSM Agent のバージョン 3 は、Windows Server 2008 および 2008 R2 のいずれのオペレーションとも互換性がない場合があります。Windows Server 2008 バージョンで正式にサポートされている最後の SSM Agent のバージョンは 2.3.1644.0 です。

SSM Agent を最新の状態に維持

新しいツールが Systems Manager に追加されるか、既存のツールが更新されると必ず、更新されたバージョンの SSM Agent がリリースされます。最新バージョンのエージェントを使用しないと、マネージドノードが Systems Manager の各種ツールや機能を使用できなくなる可能性があります。こ

のため、マシン上で SSM Agent を最新状態に維持するプロセスを自動化することをお勧めします。詳細については、「SSM Agent への更新の自動化」を参照してください。GitHub の「SSM Agent リリースノート」ページをサブスクライブすると、SSM Agent の更新に関する通知を受け取ることができます。

SSM Agent エージェントのバージョン別の詳細を確認するには、リリースノートを参照してください。

トピック

- Windows Server 用の EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする
- SSM Agent が Windows Server インスタンス用にプロキシを使用するように設定する

Windows Server 用の EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする

AWS Systems Manager エージェント (SSM Agent) は、Amazon が提供する以下の Windows Server 用 Amazon Machine Images (AMIs) にデフォルトでプリインストールされています。

- 2016 年 11 月以降に公開された Windows Server 2008-2012 R2 AMIs
- Windows Server 2016、2019、2022 (Nano バージョンを除く)、および 2025

Windows Server 用の EC2 インスタンスに SSM Agent を手動でインストールする

必要に応じて、以下の手順を使用して、Windows Server の Amazon Elastic Compute Cloud (Amazon EC2) インスタンスに最新バージョンの SSM Agent を手動でダウンロードしてインストールできます。この手順で提供されるコマンドは、ユーザーデータを通じてスクリプトとして Amazon EC2 インスタンスに渡すこともできます。

SSM Agent では、Windows Server インスタンス (レガシー `AWS-ApplyPatchBaseline` など) で特定の AWS Systems Manager ドキュメント (SSM ドキュメントなど) を実行する場合、Windows PowerShell 3.0 以降が必要です。Windows Server インスタンスで Windows Management Framework 3.0 以降を実行していることを確認します。このフレームワークには Windows PowerShell が含まれています。詳細については、「Windows 管理フレームワーク 3.0」を参照してください。

> **Note**
>
> この手順は、Windows Server の EC2 インスタンスへの SSM Agent のインストールまたは再インストールに適用されます。Systems Manager で使用できるようにエージェントをオンプレミスサーバーまたは仮想マシン (VM) にインストールする必要がある場合は、「ハイブリッド Windows ノードに SSM Agent をインストールする方法」を参照してください。

最新バージョンの SSM Agent を Windows Server の EC2 インスタンスに手動でインストールするには

1. リモートデスクトップまたは Windows PowerShell を使用して、インスタンスに接続します。詳細については、「Amazon EC2 ユーザーガイド」の「Linux インスタンスへの接続」を参照してください。
2. 最新バージョンの SSM Agent をインスタンスにダウンロードします。PowerShell コマンドまたは直接ダウンロードリンクを使用してダウンロードできます。

   > **Note**
   >
   > このステップの URL では、すべての AWS リージョン から SSM Agent をダウンロードできます。特定のリージョンからエージェントをダウンロードする場合は、代わりにリージョン固有の URL を使用します。
   > `https://amazon-ssm-region.s3.region.amazonaws.com/latest/windows_amd64/AmazonSSMAgentSetup.exe`
   > *region* は、米国東部 (オハイオ) リージョンの `us-east-2` のように、AWS Systems Manager でサポートされている AWS リージョン の識別子を表します。サポートされている *region* 値の一覧については、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」にある Region 列を参照してください。

   PowerShell

   次の 3 つの PowerShell コマンドを順番に実行します。これらのコマンドを使用すると、Internet Explorer (IE) のセキュリティ強化の設定を調整せずに SSM Agent をダウンロードし、エージェントをインストールしてインストールファイルを削除できます。

64-bit

```
[System.Net.ServicePointManager]::SecurityProtocol = 'TLS12'
$progressPreference = 'silentlyContinue'
Invoke-WebRequest `
    https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/
windows_amd64/AmazonSSMAgentSetup.exe `
    -OutFile $env:USERPROFILE\Desktop\SSMAgent_latest.exe
```

32-bit

```
[System.Net.ServicePointManager]::SecurityProtocol = 'TLS12'
$progressPreference = 'silentlyContinue'
Invoke-WebRequest `
    https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/
windows_386/AmazonSSMAgentSetup.exe `
    -OutFile $env:USERPROFILE\Desktop\SSMAgent_latest.exe
```

```
Start-Process `
    -FilePath $env:USERPROFILE\Desktop\SSMAgent_latest.exe `
    -ArgumentList "/S" `
    -Wait
```

```
rm -Force $env:USERPROFILE\Desktop\SSMAgent_latest.exe
```

直接ダウンロード

次のリンクを使用して、最新バージョンの SSM Agent をインスタンスにダウンロードします。必要に応じて、この URL を AWS リージョン 固有の URL で更新します。

https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/windows_amd64/AmazonSSMAgentSetup.exe

ダウンロードした `AmazonSSMAgentSetup.exe` ファイルを実行して、SSM Agent をインストールします。

3. PowerShell で次のコマンドを送信して SSM Agent を起動または再起動します。

```
Restart-Service AmazonSSMAgent
```

> **Note**
>
> Windows Server インスタンスから SSM Agent をアンインストールするには、[コントロールパネル]、[プログラム] を開きます。[Uninstall a program] (プログラムをアンインストール) オプションを選択します。Amazon SSM Agent のコンテキスト (右クリック) メニューを開き、[Uninstall] (アンインストール) を選択します。

SSM Agent が Windows Server インスタンス用にプロキシを使用するように設定する

このトピックの情報は、2016 年 11 月以降に作成された、Nano インストールオプションを使用しない Windows Server インスタンスに該当します。Session Manager を使用する予定の場合は、HTTPS プロキシサーバーはサポートされていないことに注意してください。

> **Note**
>
> 2020 年 1 月 14 日以降、Windows Server 2008 は Microsoft の機能更新プログラムまたはセキュリティ更新プログラムでサポートされなくなりました。Windows Server 2008 および 2008 R2 のレガシー Amazon Machine Images (AMIs) には、依然としてバージョン 2 の SSM Agent がプリインストールされていますが、Systems Manager は 2008 バージョンを正式にサポートしなくなり、これらのバージョンの Windows Server のエージェントを更新しなくなりました。さらに、SSM Agent のバージョン 3 は、Windows Server 2008 および 2008 R2 のいずれのオペレーションとも互換性がない場合があります。Windows Server 2008 バージョンで正式にサポートされている最後の SSM Agent のバージョンは 2.3.1644.0 です。

[開始する前に]

SSM Agent がプロキシを使用するように設定する前に、以下の重要な情報に注意してください。

次の手順ではコマンドを実行し、SSM Agent がプロキシを使用するように設定します。コマンドには、IP アドレスを含む `no_proxy` 設定が含まれています。この IP アドレスは、Systems Manager のインスタンスメタデータサービス (IMDS) エンドポイントです。`no_proxy` を指定しない場合、Systems Manager への呼び出しによってプロキシサービスからアイデンティティを引き受けるか (IMDSv1 フォールバックが有効の場合)、Systems Manager への呼び出しが失敗します (IMDSv2 が強制されている場合)。

- IPv4 の場合は、no_proxy=169.254.169.254 を指定します。
- IPv6 の場合は、no_proxy=[fd00:ec2::254] を指定します。インスタンスメタデータサービスの IPv6 アドレスは、IMDSv2 コマンドと互換性があります。IPv6 アドレスは、AWS Nitro System 上に構築されたインスタンスでのみアクセス可能です。詳細については、「Amazon EC2 ユーザーガイド」の「インスタンスメタデータサービスバージョン 2 の仕組み」を参照してください。

SSM Agent がプロキシを使用するように設定するには

1. リモートデスクトップまたは Windows PowerShell を使用して、プロキシを使用するように設定するインスタンスに接続します。
2. PowerShell で次のコマンドブロックを実行します。*hostname* と *port* を、プロキシの情報に置き換えます。

```
$serviceKey = "HKLM:\SYSTEM\CurrentControlSet\Services\AmazonSSMAgent"
$keyInfo = (Get-Item -Path $serviceKey).GetValue("Environment")
$proxyVariables = @("http_proxy=hostname:port", "https_proxy=hostname:port",
 "no_proxy=IP address for instance metadata services (IMDS)")

if ($keyInfo -eq $null) {
    New-ItemProperty -Path $serviceKey -Name Environment -Value $proxyVariables -
PropertyType MultiString -Force
} else {
    Set-ItemProperty -Path $serviceKey -Name Environment -Value $proxyVariables
}

Restart-Service AmazonSSMAgent
```

上記のコマンドを実行した後、SSM Agent ログを確認すると、プロキシ設定が適用されたことを確認できます。ログのエントリは次のようになります。SSM Agent ログの詳細については、「SSM Agent ログの表示」を参照してください。

```
2020-02-24 15:31:54 INFO Getting IE proxy configuration for current user: The operation
 completed successfully.
2020-02-24 15:31:54 INFO Getting WinHTTP proxy default configuration: The operation
 completed successfully.
2020-02-24 15:31:54 INFO Proxy environment variables:
2020-02-24 15:31:54 INFO http_proxy: hostname:port
2020-02-24 15:31:54 INFO https_proxy: hostname:port
```

```
2020-02-24 15:31:54 INFO no_proxy: IP address for instance metadata services (IMDS)
2020-02-24 15:31:54 INFO Starting Agent: amazon-ssm-agent - v2.3.871.0
2020-02-24 15:31:54 INFO OS: windows, Arch: amd64
```

SSM Agent のプロキシ設定をリセットするには

1. リモートデスクトップまたは Windows PowerShell を使用して、設定先のインスタンスに接続します。
2. リモートデスクトップを使用して接続した場合は、管理者として PowerShell を起動します。
3. PowerShell で次のコマンドブロックを実行します。

```
Remove-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Services\AmazonSSMAgent -
Name Environment
Restart-Service AmazonSSMAgent
```

SSM Agent プロキシ設定の優先順位

Windows Server インスタンスで SSM Agent のプロキシ設定を構成する場合、SSM Agent の起動時にこれらの設定が評価され、エージェント構成に適用されることを理解することが重要です。Windows Server インスタンスのプロキシ設定を構成する方法によって、他の設定が目的の設定よりも優先されるかどうかを決定できます。エージェントは、エージェントが見つけた最初のプロキシ設定を使用します。

> **Important**
>
> SSM Agent は、HTTPS プロトコルを使用して通信します。このため、次の設定オプションのいずれかを使用して `HTTPS proxy` パラメータを設定する必要があります。

SSM Agent プロキシ設定は、次の順序で評価されます。

1. `AmazonSSMAgent` のレジストリ設定 (`HKLM:\SYSTEM\CurrentControlSet\Services\AmazonSSMAgent`)
2. `System` 環境変数 (`http_proxy`、`https_proxy`、`no_proxy`)
3. `LocalSystem` ユーザーアカウントの環境変数 (`http_proxy`、`https_proxy`、`no_proxy`)
4. ブラウザ設定 (`HTTP`、`secure`、`exceptions`)
5. `WinHTTP` のプロキシ設定 (`http=`、`https=`、`bypass-list=`)

SSM Agent プロキシ設定とSystems Manager サービス

プロキシを使用するように SSM Agent を設定し、Windows Server インスタンスでの実行時に PowerShell や Windows Update クライアントを使用する AWS Systems Manager のツール (Run Command や Patch Manager など) を使う場合は、追加のプロキシ設定を行います。そうしないと、プロキシ設定が PowerShell や Windows Update クライアントによって使用され、SSM Agent プロキシ設定から継承されないため、オペレーションが失敗する可能性があります。

Run Command の場合は、Windows Server インスタンスで `WinINet` プロキシ設定を行います。指定される `[System.Net.WebRequest]` コマンドはセッション単位です。これらの設定を Run Command で実行する後続のネットワークコマンドに適用する場合、同じ `aws:runPowershellScript` プラグイン入力内の他の Powershell コマンドの前にこれらのコマンドを指定する必要があります。

次の PowerShell コマンドでは、現在の `WinINet` プロキシ設定を返し、プロキシ設定を `WinINet` に適用します。

```
[System.Net.WebRequest]::DefaultWebProxy

$proxyServer = "http://hostname:port"
$proxyBypass = "169.254.169.254"
$WebProxy = New-Object System.Net.WebProxy($proxyServer,$true,$proxyBypass)

[System.Net.WebRequest]::DefaultWebProxy = $WebProxy
```

Patch Manager の場合は、Windows Update クライアントが更新をスキャンしてダウンロードできるように、システム全体のプロキシ設定を行います。次のコマンドは SYSTEM アカウントで実行され、設定がシステム全体に適用されるため、Run Command を使用して実行することをお勧めします。次の `netsh` コマンドでは、現在のプロキシ設定を返し、プロキシ設定をローカルシステムに適用します。

```
netsh winhttp show proxy

netsh winhttp set proxy proxy-server="hostname:port" bypass-list="169.254.169.254"
```

Run Command の使用の詳細については、「AWS Systems Manager Run Command」を参照してください。

SSM Agent ステータスの確認とエージェントの起動

このトピックでは、サポートされている各オペレーティングシステムで AWS Systems Manager Agent (SSM Agent) が実行されているかどうかを確認するコマンドの一覧を示します。また、エージェントが実行中でない場合にエージェントを起動するためのコマンドも用意されています。

オペレーティングシステム	SSM Agent ステータスを確認するコマンド	SSM Agent を起動するコマンド
Amazon Linux 1	`sudo status amazon-ssm-agent`	`sudo start amazon-ssm-agent`
Amazon Linux 2、Amazon Linux 2022、Amazon Linux 2023	`sudo systemctl status amazon-ssm-agent`	`sudo systemctl enable amazon-ssm-agent` `sudo systemctl start amazon-ssm-agent`
CentOS 6.x	`sudo status amazon-ssm-agent`	`sudo start amazon-ssm-agent`
CentOS 7.x および CentOS 8.x	`sudo systemctl status amazon-ssm-agent`	`sudo systemctl enable amazon-ssm-agent` `sudo systemctl start amazon-ssm-agent`
Debian Server 8、9、10	`sudo systemctl status amazon-ssm-agent`	`sudo systemctl enable amazon-ssm-agent` `sudo systemctl start amazon-ssm-agent`
macOS	`/var/log/amazon/ssm/amazon-ssm-agent.log` で、エージェントのログファイルを確認します。	`sudo launchctl load -w /Library/LaunchDaemons/com.amazon.aws.ssm.plist`

オペレーティングシステム	SSM Agent ステータスを確認するコマンド	SSM Agent を起動するコマンド
		`sudo launchctl start com.amazon.aws.ssm`
Oracle Linux	`sudo systemctl status amazon-ssm-agent`	`sudo systemctl enable amazon-ssm-agent` `sudo systemctl start amazon-ssm-agent`
Red Hat Enterprise Linux (RHEL) 6.x	`sudo status amazon-ssm-agent`	`sudo start amazon-ssm-agent`
Red Hat Enterprise Linux (RHEL) 7.x、8.x、および 9.x	`sudo systemctl status amazon-ssm-agent`	`sudo systemctl enable amazon-ssm-agent` `sudo systemctl start amazon-ssm-agent`
SUSE Linux Enterprise Server (SLES)	`sudo systemctl status amazon-ssm-agent`	`sudo systemctl enable amazon-ssm-agent` `sudo systemctl start amazon-ssm-agent`
Ubuntu Server 14.04 (すべて) および 16.04 (32 ビット)	`sudo status amazon-ssm-agent`	`sudo start amazon-ssm-agent`
Ubuntu Server 16.04 64 ビットインスタンス (deb パッケージのインストール)	`sudo systemctl status amazon-ssm-agent`	`sudo systemctl enable amazon-ssm-agent` `sudo systemctl start amazon-ssm-agent`

オペレーティングシステム	SSM Agent ステータスを確認するコマンド	SSM Agent を起動するコマンド
Ubuntu Server 16.04、18.04、20.04 LTS および 20.10 STR 64 ビット、22.04 LTS (Snap パッケージインストール)、および23.04	`sudo systemctl status snap.amazon-ssm-agent.amazon-ssm-agent.service`	`sudo snap start amazon-ssm-agent`
Windows Server	PowerShell で実行する: `Get-Service AmazonSSMAgent`	PowerShell 管理者モードで実行します。 `Start-Service AmazonSSMAgent`

詳細情報

- Linux 用 EC2 インスタンスで SSM Agent を使用する
- Windows Server 用 EC2 インスタンスで SSM Agent を使用する
- SSM Agent バージョン番号の確認

SSM Agent バージョン番号の確認

AWS Systems Manager の特定の機能には、マネージドノードにインストールする Systems Manager Agent (SSM Agent) の最小バージョンなどの前提条件があります。現在インストールされている SSM Agent バージョンはSystems Manager コンソールを使用してマネージドノードに取得、またはマネージドノードにログインします。

> **Note**
>
> 以前のバージョンの詳細については、GitHub の SSM Agent のリリースノートを参照してください。

以下の手順は、マネージドノードに現在インストールされている SSM Agent バージョンを取得する方法について説明します。

マネージドノードにインストールされている SSM Agent のバージョン番号を確認する方法

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。
3. [SSM Agent バージョン] 列に [エージェントバージョン] 番号を入力します。

オペレーティングシステム内から、現在インストールされている SSM Agent バージョンを取得するには

次のタブから選択して、オペレーティングシステム内から現在インストールされている SSM Agent のバージョンを取得します。

Amazon Linux 1, Amazon Linux 2, and Amazon Linux 2023

> **Note**
>
> このコマンドは、オペレーティングシステムのパッケージマネージャーによって異なります。

1. マネージドノードにログインします。
2. 以下のコマンドを実行してください。

```
yum info amazon-ssm-agent
```

このコマンドは、次のような出力を返します。

```
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
Installed Packages
Name        : amazon-ssm-agent
Arch        : x86_64
Version     : 3.0.655.0
```

CentOS

1. マネージドノードにログインします。

2. CentOS 6 および 7 の場合は、以下のコマンドを実行します。

```
yum info amazon-ssm-agent
```

このコマンドは、次のような出力を返します。

```
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
Installed Packages
Name        : amazon-ssm-agent
Arch        : x86_64
Version     : 3.0.655.0
```

Debian サーバー

1. マネージドノードにログインします。
2. 以下のコマンドを実行してください。

```
apt list amazon-ssm-agent
```

このコマンドは、次のような出力を返します。

```
apt list amazon-ssm-agent
Listing... Done
amazon-ssm-agent/now 3.0.655.0-1 amd64 [installed,local]

3.0.655.0 is the version of SSM agent
```

macOS

1. マネージドノードにログインします。
2. 以下のコマンドを実行してください。

```
pkgutil --pkg-info com.amazon.aws.ssm
```

RHEL

1. マネージドノードにログインします。

2. RHEL 6、7、8 および 9 の場合は、以下のコマンドを実行します。

```
yum info amazon-ssm-agent
```

このコマンドは、次のような出力を返します。

```
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
Installed Packages
Name        : amazon-ssm-agent
Arch        : x86_64
Version     : 3.0.655.0
```

DNF パッケージユーティリティの場合は、次のコマンドを実行します。

```
dnf info amazon-ssm-agent
```

SLES

1. マネージドノードにログインします。
2. SLES 12 および 15 の場合は、以下のコマンドを実行します。

```
zypper info amazon-ssm-agent
```

このコマンドは、次のような出力を返します。

```
Loading repository data...
Reading installed packages...
Information for package amazon-ssm-agent:
----------------------------------------
Repository : @System
Name : amazon-ssm-agent
Version : 3.0.655.0-1
```

Ubuntu Server

> **Note**
>
> Ubuntu Server 16.04 インスタンスが deb パッケージまたは Snap パッケージを使用しているかどうかを確認するには、「Ubuntu Server インスタンスに SSM Agent を手動でインストールする」を参照してください。

1. マネージドノードにログインします。
2. Ubuntu Server 16.04 および 14.04 64 ビット (deb インストーラーパッケージを使用) については、次のコマンドを実行します。

```
apt list amazon-ssm-agent
```

このコマンドは、次のような出力を返します。

```
apt list amazon-ssm-agent
Listing... Done
amazon-ssm-agent/now 3.0.655.0-1 amd64 [installed,local]

3.0.655.0 is the version of SSM agent
```

Ubuntu Server 22.04 LTS、20.10 STR および 20.04、18.04、および 16.04 LTS 64 ビットインスタンス (Snap パッケージ付き) については、次のコマンドを実行します。

```
sudo snap list amazon-ssm-agent
```

このコマンドは、次のような出力を返します。

```
snap list amazon-ssm-agent
Name Version Rev Tracking Publisher Notes
amazon-ssm-agent 3.0.529.0 3552 latest/stable/… aws# classic-

3.0.529.0 is the version of SSM agent
```

Windows

1. マネージドノードにログインします。
2. 次の PowerShell コマンドを実行します。

```
& "C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe" -version
```

このコマンドは、次のような出力を返します。

```
SSM Agent version: 3.1.804.0
```

新機能または更新された機能を利用できるように、SSM Agent の最新バージョンを使用することをお勧めします。マネージドインスタンスで常に SSM Agent の最新バージョンが実行されるように、SSM Agent の更新プロセスを自動化できます。詳細については、「SSM Agent への更新の自動化」を参照してください。

SSM Agent ログの表示

AWS Systems Manager エージェント (SSM Agent) は実行、コマンド、スケジュールされたアクション、エラー、ヘルスステータスに関する情報を各マネージドノードのログファイルに書き込みます。マネージドノードに手動で接続してログファイルを確認、または自動的にログを Amazon CloudWatch Logs に送信できます。CloudWatch Logs へのログの送信の詳細については、「AWS Systems Manager でのログ記録とモニタリング」を参照してください。

マネージドノードの SSM Agent ログは以下の場所で確認できます。

Linux and macOS

```
/var/log/amazon/ssm/
```

Windows

```
%PROGRAMDATA%\Amazon\SSM\Logs\
```

Linux マネージドノードの場合、SSM Agent、`stderr`、`stdout` のファイルは以下のディレクトリに書き込まれます: `/var/lib/amazon/ssm/`。

Windows マネージドノードの場合、SSM Agent、`stderr`、`stdout` のファイルは、`%PROGRAMDATA%\Amazon\SSM\InstanceData\` ディレクトリに書き込まれます。

SSM Agent のデバッグログの許可の詳細については、「SSM Agentデバッグログの有効化」を参照してください。

cihub/seelog 設定の詳細については、GitHub の「Seelog Wiki」を参照してください。cihub/seelog 設定の例については、GitHub の「cihub/seelog の例」リポジトリを参照してください。

SSM Agentデバッグログの有効化

マネージドノードで SSM Agent のデバッグログを許可する場合、以下の手順を使用します。

Linux and macOS

SSM Agent デバッグログを Linux と macOS マネージドノードに許可する方法

1. AWS Systems Manager のツールである Session Manager を使用してデバッグログを許可するマネージドノードに接続するか、またはマネージドノードにログオンします。詳細については、「Session Manager の使用」を参照してください。
2. seelog.xml.template ファイルを探します。

   Linux:

   ほとんどの Linux マネージドノードタイプでは、ファイルはディレクトリ /etc/amazon/ssm/seelog.xml.template にあります。

   Ubuntu Server 20.10 STR および 20.04、18.04、16.04 LTS では、ファイルはディレクトリ /snap/amazon-ssm-agent/current/seelog.xml.template にあります。変更を加える前に、このファイルを /snap/amazon-ssm-agent/current/ ディレクトリから /etc/amazon/ssm/ ディレクトリにコピーします。

   macOS:

   macOS インスタンスタイプでは、ファイルはディレクトリ /opt/aws/ssm/seelog.xml.template にあります。
3. ファイル名を seelog.xml.template から seelog.xml に変更します。

   > **Note**
   >
   > Ubuntu Server 20.10 STR & 20.04、18.04、および 16.04 LTS では、seelog.xml ファイルは /etc/amazon/ssm/ ディレクトリに作成する必要があります。次の 3 つのコマンドを実行して、このディレクトリとファイルを作成できます。

```
sudo mkdir -p /etc/amazon/ssm
```

```
sudo cp -p /snap/amazon-ssm-agent/current/seelog.xml.template /etc/
amazon/ssm/seelog.xml
```

4. seelog.xml ファイルを編集して、デフォルトのログ記録の動作を変更します。次の例に示すように、[minlevel] の値を [info] から [debug] に変更します。

   ```
   <seelog type="adaptive" mininterval="2000000" maxinterval="100000000"
   critmsgcount="500" minlevel="debug">
   ```

5. (オプション) 以下のコマンドを使用して SSM Agent を再起動します。

   Linux:

   ```
   sudo service amazon-ssm-agent restart
   ```

   macOS:

   ```
   sudo /opt/aws/ssm/bin/amazon-ssm-agent restart
   ```

Windows

SSM Agent デバッグログを Windows Server マネージドノードに許可する方法

1. Session Manager を使用してデバッグログを許可するマネージドノードに接続するか、またはマネージドノードにログオンします。詳細については、「Session Manager の使用」を参照してください。
2. seelog.xml.template ファイルのコピーを作成します。seelog.xml へのコピーの名前を変更します。このファイルは次のディレクトリにあります。

   ```
   %PROGRAMFILES%\Amazon\SSM\seelog.xml.template
   ```

3. seelog.xml ファイルを編集して、デフォルトのログ記録の動作を変更します。次の例に示すように、[minlevel] の値を [info] から [debug] に変更します。

   ```
   <seelog type="adaptive" mininterval="2000000" maxinterval="100000000"
   critmsgcount="500" minlevel="debug">
   ```

4. 以下のキーを見つけます。

   ```
   filename="{{LOCALAPPDATA}}\Amazon\SSM\Logs\{{EXECUTABLENAME}}.log"
   ```

   次のパスを使用するようにこのエントリを変更します。

   ```
   filename="C:\ProgramData\Amazon\SSM\Logs\{{EXECUTABLENAME}}.log"
   ```

5. 以下のキーを見つけます。

   ```
   filename="{{LOCALAPPDATA}}\Amazon\SSM\Logs\errors.log"
   ```

   次のパスを使用するようにこのエントリを変更します。

   ```
   filename="C:\ProgramData\Amazon\SSM\Logs\errors.log"
   ```

6. 管理者モードで次の PowerShell コマンドを使用して SSM Agent を再起動します。

   ```
   Restart-Service AmazonSSMAgent
   ```

SSM Agent を介してルートレベルコマンドへのアクセスを制限する

AWS Systems Manager エージェント (SSM Agent) は、ハイブリッドクラウドとマルチクラウド環境の Amazon Elastic Compute Cloud (Amazon EC2) インスタンスおよびその他のマシンタイプで、ルート権限 (Linux) または SYSTEM 権限 (Windows Server) を使用して実行します。最高レベルのシステムアクセス許可が存在するため、SSM Agent にコマンドを送信する許可が付与されている信頼されたエンティティにはルートまたは SYSTEM アクセス許可があります (AWS において、AWS 内でアクションを実行してリソースにアクセスできる信頼されたエンティティはプリンシパルと呼ばれます。プリンシパルは AWS アカウントのルートユーザー、ユーザー、ロールのいずれかになります)。

このレベルのアクセスは、プリンシパルが承認済みの Systems Manager コマンドを SSM Agent に送信するために必要です。ただし、これによりプリンシパルが SSM Agent の潜在的な脆弱性を悪用して、悪意のあるコードを実行できるようになります。

特に、SendCommand および StartSession コマンドを実行する権限を慎重に制限する必要があります。適切な最初のステップは、組織内の選ばれたプリンシパルのみに各コマンドに対するアクセス権限を付与することです。ただし、プリンシパルがこれらのコマンドを実行できる対象マネージドノードを制限して、セキュリティ体制をさらに強化することをお勧めします。これは、プリンシパルに割

り当てられた IAM ポリシーで実行できます。IAM ポリシーに特定のタグまたはタグの組み合わせが付けられたマネージドノードのみでコマンドを実行できるようにユーザーを制限する条件を含めることができます。

例えば、テスト用と本番稼働用の 2 つのサーバーフリートがあるとします。ジュニア (短経歴) エンジニアに指定された IAM ポリシーでは、そのユーザーが `ssm:resourceTag/testServer` でタグ付けされたインスタンスでのみコマンドを実行できるように指定します。ただし、すべてのインスタンスへのアクセスが必要な、主任エンジニアの小さなグループでは、`ssm:resourceTag/testServer` と `ssm:resourceTag/productionServer` の両方でタグ付けされたインスタンスへのアクセス権を付与します。

この方法を使用すると、ジュニアエンジニアが本番稼働用インスタンスでコマンドを実行しようとした場合、アクセスを拒否されます。割り当てられている IAM ポリシーに `ssm:resourceTag/productionServer` でタグ付けされたインスタンスへの明示的なアクセスが許可されていないからです。

詳細情報および例については、次のトピックを参照してください。

- タグによる Run Command アクセスを制限
- Restrict session access based on instance tags (インスタンスタグに基づくセッションのアクセスの制限)

SSM Agent への更新の自動化

AWS は、Systems Manager のツールを追加または更新して、AWS Systems Manager Agent (SSM Agent) の新しいバージョンをリリースします。マネージドノードが古いバージョンのエージェントを使用している場合、新しいツールの使用または更新されたツールを利用することができません。そのため、以下のいずれかの方法でマネージドノード上で SSM Agent を更新するプロセスを自動化することをお勧めします。

Bottlerocket オペレーティングシステム上のエージェントアップデート

Bottlerocket オペレーティングシステムの SSM Agent では、Systems Manager コマンドドキュメント `AWS-UpdateSSMAgent` を使用して更新することはできません。アップデートは Bottlerocket コントロールコンテナ内で管理されます。詳細については、GitHub で「Bottlerocket Control Container」と「Bottlerocket 更新オペレーター」を参照してください。

macOS バージョン要件

インスタンスが macOS バージョン 11.0 (Big Sur) 以降を実行している場合、AWS-UpdateSSMAgent ドキュメントを実行するにはインスタンスの SSM Agent バージョン 3.1.941.0 以上が必要です。インスタンスが 3.1.941.0 より前にリリースされた SSM Agent バージョンを実行している場合は、`brew update` および `brew upgrade amazon-ssm-agent` コマンドを AWS-UpdateSSMAgent を実行するように SSM Agent を更新します。

[メソッド]	詳細
すべてのマネージドノードにワンクリックで自動更新(推奨)	AWS アカウント のすべてのマネージドノードが SSM Agent の新バージョンを自動的に調べてダウンロードするように設定できます。これを実行するには、このトピックで後述するように、Fleet Manager の [設定] タブで [SSM Agent を自動更新] を選択します。
グローバルまたは選択的な更新	AWS Systems Manager のツールである State Manager を使用してマネージドノードに SSM Agent を自動的にダウンロードしてインストールする関連付けを作成できます。ワークロードの中断を制限する場合は、Systems Manager のメンテナンスウィンドウを作成して、指定した期間にインストールを実行できます。どちらの方法ともすべてのマネージドノードにグローバル更新の設定をするか、または更新するインスタンスを選択することを可能にします。State Manager の関連付けの作成については、「チュートリアル: AWS CLI で SSM Agent を自動的に更新する」を参照してください。メンテナンスウィンドウ の作成の詳細については、「チュートリアル: コンソールを使用してパッチ用メンテナンスウィンドウを作成する」を参照してください。
新しい環境のグローバルまたは選択的な更新	Systems Manager の使用を開始する場合、AWS Systems Manager のツールである Quick Setup のSystems Manager (SSM) Agent を 2 週間ごとに更新オプションを使用するこ

[メソッド]	詳細
	とをお勧めします。Quick Setup はすべてのマネージドノードにグローバル更新の設定をするか、または更新するインスタンスを選択することを可能にします。詳細については、「Quick Setup を使用して Amazon EC2 ホスト管理を設定する」を参照してください。

マネージドノードの SSM Agent を手動で更新する場合、エージェントの新しいバージョンがリリースされた際に AWS が発行する通知をサブスクライブできます。詳細については、SSM Agent 通知にサブスクライブする を参照してください。通知をサブスクライブした後、Run Command で 1 つ以上のマネージドノードを最新バージョンに手動で更新できます。詳細については、「Run Command を使用して SSM Agent を更新する」を参照してください。

SSM Agent の自動更新

AWS アカウント 内にあるすべての Linux と Windows のマネージドノードに SSM Agent を自動的に更新するようにSystems Manager を設定できます。このオプションをオンにすると、Systems Manager は 2 週間ごとにエージェントの新しいバージョンを自動的に確認します。新しいバージョンがある場合、Systems Manager は SSM ドキュメント `AWS-UpdateSSMAgent` を使って、エージェントを最新のリリースバージョンに自動更新します。マネージドノードに常に最新バージョンの SSM Agent が実行されるように、このオプションを選択することをお勧めします。

> **Note**
>
> SSM ドキュメント `yum` を使用してエージェントがインストールまたは更新された後、マネージドノードで SSM Agent コマンドを使用して `AWS-UpdateSSMAgent` を更新する場合、「警告: RPMDB が yum 外で変更されました」というメッセージが表示されることがあります。このメッセージは正常であり、無視してもかまいません。

自動的に SSM Agent を更新するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Fleet Manager] を選択します。

3. [Settings] (設定) タブを選択します。
4. [エージェントの自動更新] エリアで、[SSM Agent を自動更新] を選択します。

フリートが更新する SSM Agent のバージョンを変更する場合、[Settings] (設定) タブの [Agent auto update] (エージェントオートアップデート) の下にある [Edit] (編集) を選択します。次に、[パラメータ] の [バージョン] に、更新したい SSM Agent のバージョンを入力します。これを指定しなければ、エージェントは最新バージョンに更新されます。

アカウント内のすべてのマネージドノードに SSM Agent の更新バージョンの自動展開を停止する場合、[Settings] (設定) タブの [Agent auto update] (エージェントオートアップデート) の下にある [Delete] (削除) を選択します。このアクションはマネージドノードの SSM Agent を自動的に更新する State Manager の関連付けを削除されます。

SSM Agent 通知にサブスクライブする

Amazon Simple Notification Service (Amazon SNS) で、AWS Systems Manager Agent (SSM Agent) の新しいバージョンがリリースされたときに通知を受け取れます。このような通知をサブスクライブするには、以下の手順を使用します。

> **Tip**
>
> また、GitHub の「SSM Agent リリースノート」ページを見て、通知をサブスクライブすることもできます。

SSM Agent の通知をサブスクライブするには

1. Amazon SNS コンソール (https://console.aws.amazon.com/sns/v3/home) を開きます。
2. ナビゲーションバーのリージョンセレクタから、リージョンを [米国東部 (バージニア北部)] を選択します (まだ選択されていない場合)。サブスクライブする SSM Agent 用の Amazon SNS 通知はこの からのみ生成されているため、この AWS リージョン を選択する必要があります。
3. ナビゲーションペインで [Subscriptions] を選択します。
4. [Create subscription] を選択します。
5. [サブスクリプションの作成] で、次の操作を行います。

   a. トピックの ARN では、以下の Amazon リソースネーム (ARN) を使用します。

```
arn:aws:sns:us-east-1:720620558202:SSM-Agent-Update
```

b. [プロトコル] で `Email` または `SMS` を選択します。

c. 前のステップで `Email` または `SMS` のどちらを選択したかに応じて、[Endpoint] (エンドポイント) に、通知を受信する電子メールアドレスまたは市外局番と電話番号を入力します。

d. [Create subscription] を選択します。

6. `Email` を選択した場合は、サブスクリプションの確認を求める E メールが届きます。メッセージを開き、指示に従ってサブスクリプションを完了します。

サブスクライバには、SSM Agentの新しいバージョンがリリースされるたびに、通知が送信されます。通知が不要になった場合は、次の手順で受信登録を解除します。

SSM Agent の通知の受信登録を解除するには

1. Amazon SNS コンソールを開きます。
2. ナビゲーションペインで [Subscriptions] を選択します。
3. [Subscription] (サブスクリプション) を選択し、[Delete] (削除) をクリックします。確認を求めるメッセージが表示されたら、[削除] を選択します。

SSM Agent のトラブルシューティング

マネージドノードでオペレーションの実行に問題が発生した場合、AWS Systems Manager エージェント (SSM Agent) に問題がある可能性があります。以下の情報を利用して SSM Agent ログファイルを表示し、エージェントをトラブルシューティングしてください。

トピック

- SSM Agent が最新ではない
- SSM Agent ログファイルを使用して問題をトラブルシューティングする
- エージェントログファイルがローテーションしない (Windows)
- SSM エンドポイントに接続できない
- VPC 設定を検証する
- VPC DNS 関連の属性を検証する
- エンドポイントセキュリティグループでイングレスルールを検証する
- ssm-cli を使用してマネージドノードの可用性をトラブルシューティングする

SSM Agent が最新ではない

新しいツールが Systems Manager に追加されるか、既存のツールが更新されると必ず、更新されたバージョンの SSM Agent がリリースされます。最新バージョンのエージェントを使用しないと、マネージドノードが Systems Manager の各種ツールや機能を使用できなくなる可能性があります。このため、マシン上で SSM Agent を最新状態に維持するプロセスを自動化することをお勧めします。詳細については、SSM Agent への更新の自動化 を参照してください。GitHub の「SSM Agent リリースノート」ページをサブスクライブすると、SSM Agent の更新に関する通知を受け取ることができます。

SSM Agent ログファイルを使用して問題をトラブルシューティングする

SSM Agent は、以下のファイルに情報をログとして記録します。これらのファイルの情報は、問題をトラブルシューティングするのにも役立ちます。デバッグログをオンにする方法など、SSM Agent のログファイルの詳細については、「SSM Agent ログの表示」を参照してください。

> **Note**
>
> Windows ファイルエクスプローラーを使用してこれらのログを表示することを選択した場合は、Folder Options で隠しファイルとシステムファイルの表示を必ず許可してください。

Windows の場合

- `%PROGRAMDATA%\Amazon\SSM\Logs\amazon-ssm-agent.log`
- `%PROGRAMDATA%\Amazon\SSM\Logs\errors.log`

Linux および macOS

- `/var/log/amazon/ssm/amazon-ssm-agent.log`
- `/var/log/amazon/ssm/errors.log`

Linux マネージドノードの場合、以下のディレクトリに書き込まれた `messages` ファイルに詳しい情報があります: `/var/log`。

エージェントログを使用したトラブルシューティングの詳細については、「AWS re:Post ナレッジセンター」の「マネージドインスタンスの SSM Agent の問題をトラブルシューティングするために SSM Agent ログを使用するにはどうすればよいですか」を参照してください。

エージェントログファイルがローテーションしない (Windows)

seelog.xml ファイル (Windows Server マネージドノード内) に日付ベースのログファイルのローテーションを指定してログがローテーションしない場合、`fullname=true` パラメータを指定します。次に、`fullname=true` パラメータが指定された seelog.xml 設定ファイルの例を示します。

```
<seelog type="adaptive" mininterval="2000000" maxinterval="100000000"
 critmsgcount="500" minlevel="debug">
   <exceptions>
      <exception filepattern="test*" minlevel="error" />
   </exceptions>
   <outputs formatid="fmtinfo">
      <console formatid="fmtinfo" />
      <rollingfile type="date" datepattern="200601021504" maxrolls="4" filename="C:
\ProgramData\Amazon\SSM\Logs\amazon-ssm-agent.log" fullname=true />
      <filter levels="error,critical" formatid="fmterror">
         <rollingfile type="date" datepattern="200601021504" maxrolls="4" filename="C:
\ProgramData\Amazon\SSM\Logs\errors.log" fullname=true />
      </filter>
   </outputs>
   <formats>
      <format id="fmterror" format="%Date %Time %LEVEL [%FuncShort @ %File.%Line] %Msg
%n" />
      <format id="fmtdebug" format="%Date %Time %LEVEL [%FuncShort @ %File.%Line] %Msg
%n" />
      <format id="fmtinfo" format="%Date %Time %LEVEL %Msg%n" />
   </formats>
</seelog>
```

SSM エンドポイントに接続できない

SSM Agent は以下のエンドポイントへの HTTPS (ポート 443) アウトバウンドトラフィックを許可する必要があります。

- `ssm.region.amazonaws.com`
- `ssmmessages.region.amazonaws.com`

region は、米国東部 (オハイオ) リージョンの `us-east-2` のように、AWS Systems Manager でサポートされている AWS リージョン の識別子を表します。サポートされている *region* 値の一覧に

ついては、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」にある Region 列を参照してください。

> **Note**
>
> 2024 年以前は ec2messages.*region*.amazonaws.com も必要でした。2024 年より前にローンチされた AWS リージョン の場合、ssmmessages.*region*.amazonaws.com へのトラフィックの許可は引き続き必要となりますが、ec2messages.*region*.amazonaws.com の場合はオプションになります。2024 年以降にローンチされたリージョンでは、ssmmessages.*region*.amazonaws.com へのトラフィックを許可する必要がありますが、これらのリージョンでは ec2messages.*region*.amazonaws.com エンドポイントはサポートされていません。

説明されているように、SSM Agent は、上記のエンドポイントと通信できない場合、Amazon Linux 2 や Amazon Linux 2023 など AWS が提供する Amazon Machine Images (AMIs) を使用しても動作しません。ネットワーク設定には、オープンなインターネットアクセスが必要です。または、カスタム仮想プライベートクラウド (VPC) エンドポイントが設定されている必要があります。カスタム VPC エンドポイントを作成する予定がない場合は、インターネットゲートウェイまたは NAT ゲートウェイを確認してください。VPC エンドポイントを管理する方法の詳細については、「Systems Manager のために VPC エンドポイントを使用して EC2 インスタンスのセキュリティを強化する」を参照してください。

VPC 設定を検証する

Systems Manager で EC2 インスタンスを管理するには、VPC エンドポイントを、ssm.*region*.amazonaws.com、ssmmessages.*region*.amazonaws.com、および (SSM エンドポイントに接続できない のこのトピックの前半で説明したいくつかの場合は) ec2messages.*region*.amazonaws.com のために適切に設定する必要があります。ネットワーク設定には、オープンなインターネットアクセスが必要です。または、これらの仮想プライベートクラウド (VPC) エンドポイントが設定されている必要があります。

VPC エンドポイントに関する問題をトラブルシューティングするには、次を実行します:

- VPC エンドポイントが VPC レベルに含まれているようにします。特定のサービス名を持つ VPC エンドポイントが VPC で見つからない場合は、まず DNS サポートが VPC レベルで有効になっていることを検証します。次に、新しい VPC エンドポイントを作成し、各アベイラビリティーゾーンの 1 つのサブネットに関連付けます。

- VPC エンドポイントレベルでプライベート DNS 名が有効になっているようにします。プライベート DNS 名はデフォルトで有効になっていますが、ある時点で手動で無効にされている可能性があります。
- 既存の VPC エンドポイントが適切なサブネットに関連付けられているようにします。さらに、VPCE がそのアベイラビリティーゾーンのサブネットに既に関連付けられているようにします。

詳細については、以下の各トピックを参照してください。

- 「AWS PrivateLink ガイド」の「インターフェイス VPC エンドポイントを使用して AWS のサービス にアクセスする」
- 「AWS PrivateLink ガイド」の「プライベート DNS 名を関連付ける」
- Systems Manager のために VPC エンドポイントを使用して EC2 インスタンスのセキュリティを強化する

VPC DNS 関連の属性を検証する

VPC 設定の検証の一環として、属性 `enableDnsSupport` と `enableDnsHostnames` が有効になっているようにします。

Amazon EC2 ModifyVPCAttribute API アクションまたは AWS CLI コマンド modify-vpc-attribute を使用して、これらの属性を有効にできます。

Amazon VPC コンソールでこれらの属性を有効にする方法については、「Amazon VPC ユーザーガイド」の「VPC の DNS 属性を表示および更新する」を参照してください。

エンドポイントセキュリティグループでイングレスルールを検証する

ポート 443 でトラフィックの着信を許可するために、設定した VPC エンドポイント (`ssm`、`ssmmessages`、`ec2messages`) に、セキュリティグループでイングレスルールが含まれているようにします。必要に応じて、1 つのイングレスルールを使用して VPC に新しいセキュリティグループを作成し、VPC の Classless Inter-Domain Routing (CIDR) ブロックのためにポート 443 でのトラフィックを許可できます。セキュリティグループを作成したら、それを各 VPC エンドポイントにアタッチします。

詳細については、以下の各トピックを参照してください。

- AWS re:Post の「インターネットにアクセスしなくても、VPC エンドポイントを作成して、Systems Manager でプライベート EC2 インスタンスを管理するにはどうすればよいですか?」
- 「Amazon VPC ユーザーガイド」の「VPC CIDR ブロック」

ssm-cli を使用してマネージドノードの可用性をトラブルシューティングする

SSM Agent バージョン 3.1.501.0 以降では、ssm-cli を使用して、Systems Manager によって管理されたり、Fleet Manager のマネージドノードのリストに表示されたりするための主な要件をマネージドノードが満たしているかどうかを判断できるようになりました。ssm-cli は SSM Agent のインストールに含まれるスタンドアロンのコマンドラインツールです。実行中であることを確認した Amazon EC2 インスタンスまたは EC2 以外のマシンが Systems Manager のマネージドノードのリストに含まれていない理由を診断するために必要な情報を収集する、事前設定済みのコマンドが含まれています。get-diagnostics オプションを指定したときにこれらのコマンドが実行されます。

詳細については、「ssm-cli を使用したマネージドノードの可用性のトラブルシューティング」を参照してください。

「AWS Systems Manager」 のセキュリティ

クラウドセキュリティはアマゾン ウェブ サービスの最優先事項です。AWS のお客様は、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャから利点を得られます。

セキュリティはAWS とお客様の間の共有責任です。責任共有モデルでは、これをクラウド の セキュリティおよびクラウド内 の セキュリティと説明しています。

- クラウドのセキュリティ — AWS は、AWS クラウド で AWS のサービス を実行するインフラストラクチャを保護する責任を負います。また AWS は、お客様が使用するサービスを安全に提供します。AWS コンプライアンスプログラムの一環として、サードパーティーの監査が定期的にセキュリティの有効性をテストおよび検証しています。AWS Systems Manager に適用されるコンプライアンスプログラムの詳細については、「コンプライアンスプログラムによる対象範囲内の AWS のサービス」を参照してください。
- クラウド内のセキュリティ — お客様の責任は、使用する AWS のサービス に応じて異なります。また、お客様は、お客様のデータの機密性、企業の要件、および適用可能な法律および規制などの他の要因についても責任を担います。

このドキュメントは、AWS Systems Manager を使用する際に責任共有モデルを適用する方法を理解するのに役立ちます。以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成するために Systems Manager を設定する方法を示します。また、Systems Manager リソースのモニタリングや保護に役立つ、他の AWS のサービスの使用方法についても説明します。

トピック

- AWS Systems Manager でのデータ保護
- AWS Systems Manager のためのアイデンティティおよびアクセス管理
- Systems Manager のサービスにリンクされたロールの使用
- AWS Systems Manager でのログ記録とモニタリング
- AWS Systems Manager のコンプライアンス検証
- AWS Systems Manager での耐障害性
- AWS Systems Manager 内のインフラストラクチャセキュリティ
- AWS Systems Manager での構成と脆弱性の分析
- Systems Manager のセキュリティに関するベストプラクティス

AWS Systems Manager でのデータ保護

データ保護には、転送中 (Systems Manager 間でデータを送受信するとき) のデータを保護するものと、保管時 (AWS データセンター内のディスクに格納されているとき) のデータを保護するものがあります。

AWS責任共有モデル は、AWS Systems Manager でのデータ保護に適用されます。このモデルで説明されているように、AWS は、AWS クラウド のすべてを実行するグローバルインフラストラクチャを保護するがあります。ユーザーは、このインフラストラクチャでホストされるコンテンツに対する管理を維持する責任があります。また、使用する「AWS のサービス」のセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、データプライバシーに関するよくある質問を参照してください。欧州でのデータ保護の詳細については、AWS セキュリティブログに投稿された AWS 責任共有モデルおよび GDPR のブログ記事を参照してください。

データを保護するため、「AWS アカウント」 認証情報を保護し、「AWS IAM Identity Center」 または 「AWS Identity and Access Management」 (IAM) を使用して個々のユーザーをセットアップすることをお勧めします。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して 「AWS」 リソースと通信します。TLS 1.2 が必須で、TLS 1.3 をお勧めします。
- AWS CloudTrail で API とユーザーアクティビティロギングを設定します。CloudTrail 証跡を使用して AWS アクティビティをキャプチャする方法については、「AWS CloudTrail ユーザーガイド」の「CloudTrail 証跡の使用」を参照してください。
- AWS のサービス 内のすべてのデフォルトセキュリティコントロールに加え、AWS 暗号化ソリューションを使用します。
- Amazon Macie などの高度な管理されたセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API を使用して 「AWS」 にアクセスする際に FIPS 140-3 検証済みの暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-3」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報を、タグ、または [名前] フィールドなどの自由形式のテキストフィールドに含めないことを強くお勧めします。これは、コンソール、API、AWS

CLI、または AWS SDK で Systems Manager または他の AWS のサービス を使用する場合も同様です。タグ、または名前に使用される自由形式のテキストフィールドに入力されるデータは、請求または診断ログに使用される場合があります。外部サーバーに URL を提供する場合、そのサーバーへのリクエストを検証できるように、認証情報を URL に含めないことを強くお勧めします。

データ暗号化

保管中の暗号化

Parameter Store パラメータ

AWS Systems Manager のツールである Parameter Store で作成できるパラメータのタイプには、`String`、`StringList`、`SecureString` があります。

すべてのパラメータは、タイプに関係なく、転送中および保管時の両方で暗号化されます。転送中、パラメータは Transport Layer Security (TLS) を使用して暗号化され、API リクエストの安全な HTTPS 接続が作成されます。保管時には、AWS Key Management Service (AWS KMS) の AWS 所有のキー で暗号化されます。AWS 所有のキー 暗号化の詳細については、「AWS Key Management Service デベロッパーガイド」の「AWS 所有のキー」を参照してください。

`SecureString` タイプには追加の暗号化オプションが用意されており、すべての機密データに推奨されます。次のタイプの AWS KMS キーから選択して、`SecureString` パラメータの値を暗号化および復号できます。

- アカウントの AWS マネージドキー
- アカウントで作成したカスタマーマネージドキー (CMK)
- 共有されている別の AWS アカウント の CMK

AWS KMS 暗号化の詳細については、「AWS Key Management Service デベロッパーガイド」を参照してください。

S3 バケット内のコンテンツ

Systems Manager オペレーションの一環として、1 つまたは複数の Amazon Simple Storage Service (Amazon S3) バケットにデータをアップロードまたは保存できます。

S3 バケット暗号化の詳細については、Amazon Simple Storage Service ユーザーガイドの「暗号化を使用したデータの保護」および「Amazon S3 におけるデータ保護」を参照してください。

Systems Manager アクティビティの一環として S3 バケットにアップロードまたは保存できるデータのタイプは次の通りです。

- AWS Systems Manager のツールである Run Command のコマンドの出力
- AWS Systems Manager のツールである Distributor のパッケージ
- AWS Systems Manager のツールである Patch Manager のパッチ適用オペレーションログ
- Patch Managerのパッチ上書きリスト
- Automation のランブックワークフローで実行するスクリプトまたは Ansible プレイブック (AWS Systems Manager のツール)
- Compliance (AWS Systems Manager のツール) のスキャンで使用する Chef InSpec プロファイル
- AWS CloudTrail ログ
- AWS Systems Manager のツールである Session Manager のセッション履歴ログ
- AWS Systems Manager のツールである Explorer からのレポート
- AWS Systems Manager のツールである OpsCenter からの OpsData
- Automation ワークフローで使用する AWS CloudFormation テンプレート
- リソースデータ同期スキャンからのコンプライアンスデータ
- マネージドノードの State Manager (AWS Systems Manager のツール) の関連付けを作成または編集するリクエストの出力
- AWS 管理対象の SSM ドキュメント `AWS-RunDocument` を使用して実行できる Systems Manager のカスタムドキュメント (SSM ドキュメント)

CloudWatch Logs ロググループ

Systems Manager オペレーションの一環として、1 つ以上の Amazon CloudWatch Logs ロググループにデータをストリーミングできます。

CloudWatch Logs ロググループの暗号化の詳細については、Amazon CloudWatch Logs ユーザーガイドの「AWS Key Management Service を使用した CloudWatch Logs でのログデータの暗号化」を参照してください。

アクティビティの一環として CloudWatch Logs ロググループにSystems Managerストリーミングした可能性のあるデータのタイプは次の通りです。

- Run Command コマンドの出力

- オートメーション runbook 内の `aws:executeScript` アクションを使用して実行されるスクリプトの出力
- Session Manager セッションの履歴ログ
- マネージド型ノードの SSM Agent のログ

転送中の暗号化

Transport Layer Security (TLS) のような暗号化プロトコルを使用してクライアントとユーザーノードの間で送受信される機密データを暗号化することをお勧めします。

Systems Manager では、転送中のデータの暗号化について、次のサポートが提供されます。

Systems Manager API エンドポイントへの接続

Systems Manager API エンドポイントでは、HTTPS 経由の安全な接続のみがサポートされます。Systems Manager リソースを AWS Management Console、AWS SDK、または Systems Manager API を使用して管理する場合、すべての通信は Transport Layer Security (TLS) で暗号化されます。API エンドポイントの完全なリストについては、「Amazon Web Services 全般のリファレンス」の「AWS のサービス エンドポイント」を参照してください。

マネージドインスタンス

AWS は、Amazon Elastic Compute Cloud (Amazon EC2) インスタンス間のセキュアでプライベートな接続を提供します。また、同じ Virtual Private Cloud (VPC) 内やピア接続された VPC 内のサポートされているインスタンス間で転送中のトラフィックを自動的に暗号化します。これには、256 ビット暗号化の AEAD アルゴリズムを使用します。この暗号化機能は、基盤となるハードウェアのオフロード機能を使用し、ネットワークパフォーマンスには影響を及ぼしません。サポートされているインスタンスは、C5n、G4、I3en、M5dn、M5n、P3dn、R5dn、R5n です。

Session Manager セッション

デフォルトでは、Session Manager は、TLS 1.3 を使用して、アカウント内のユーザーのローカルマシンと EC2 インスタンス間で送信されるセッションのデータを暗号化します。AWS KMS で作成された AWS KMS key を使用して、転送中のデータをさらに暗号化することもできます。AWS KMS 暗号化は、`Standard_Stream`、`InteractiveCommands`、および `NonInteractiveCommands` セッションタイプで使用できます。

Run Command アクセス

デフォルトで、Run Command を使用してノードへのリモートアクセスは、TLS 1.3 を使用して暗号化され、接続確立のリクエストは SigV4 を使用して署名されます。

インターネットトラフィックのプライバシー

Amazon Virtual Private Cloud (Amazon VPC) を使用して、マネージドノード内のリソース間に境界を作成し、それらの間のトラフィック、オンプレミス ネットワーク、インターネットを制御できます。詳細については、「Systems Manager のために VPC エンドポイントを使用して EC2 インスタンスのセキュリティを強化する」を参照してください。

Amazon Virtual Private Cloud セキュリティの詳細については、Amazon VPC ユーザーガイドの「Amazon VPC でのインターネットワークトラフィックのプライバシー」を参照してください。

AWS Systems Manager のためのアイデンティティおよびアクセス管理

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御するために役立つ AWS のサービスです。IAM 管理者は、誰を認証 (サインイン) し、誰に Systems Manager リソースの使用を許可する (権限を持たせる) かを制御します。IAM は、無料で使用できる AWS のサービスです。

トピック

- 対象者
- アイデンティティを使用した認証
- ポリシーを使用したアクセス権の管理
- AWS Systems Manager と IAM の連携方法
- AWS Systems Manager アイデンティティベースポリシーの例
- AWS の AWS Systems Manager マネージドポリシー
- AWS Systems Manager ID とアクセスのトラブルシューティング

対象者

AWS Identity and Access Management (IAM) の用途は、Systems Manager で行う作業によって異なります。

サービスユーザー - Systems Manager サービスを使用してジョブを実行する場合は、必要な権限と認証情報を管理者が用意します。作業を実行するためにさらに多くの Systems Manager 機能を使用するとき、追加の権限が必要になる場合があります。アクセスの管理方法を理解すると、管理者か

ら適切な権限をリクエストするのに役に立ちます。Systems Manager 機能にアクセスできない場合は、「AWS Systems Manager ID とアクセスのトラブルシューティング」を参照してください。

サービス管理者 - 社内の Systems Manager リソースを担当している場合は、通常、Systems Manager への完全なアクセスがあります。サービスのユーザーがどの Systems Manager 機能やリソースにアクセスするかを決めるのは管理者の仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を確認して、IAM の基本概念を理解してください。お客様の会社で Systems Manager で IAM を利用する方法の詳細については、「AWS Systems Manager と IAM の連携方法」を参照してください。

IAM 管理者 - 管理者は、Systems Manager へのアクセスを管理するポリシーの書き込み方法の詳細について確認する場合があります。IAM で使用できる Systems Manager アイデンティティベースのポリシーの例を表示するには、「AWS Systems Manager アイデンティティベースポリシーの例」を参照してください。

アイデンティティを使用した認証

認証とは、アイデンティティ認証情報を使用して AWSにサインインする方法です。ユーザーは、AWS アカウントのルートユーザー、IAM ユーザーとして、または IAM ロールを引き受けることによって、認証される (AWSにサインインする) 必要があります。

ID ソースから提供された認証情報を使用して、フェデレーティッドアイデンティティとして AWS にサインインできます。AWS IAM Identity Centerフェデレーティッドアイデンティティの例としては、(IAM アイデンティティセンター) ユーザー、貴社のシングルサインオン認証、Google または Facebook の認証情報などがあります。フェデレーティッド ID としてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。フェデレーションを使用して AWSにアクセスする場合、間接的にロールを引き受けることになります。

ユーザーのタイプに応じて、AWS Management Consoleまたは AWS アクセスポータルにサインインできます。AWS へのサインインの詳細については、AWS サインインユーザーガイドの「AWS アカウントにサインインする方法」を参照してください。

プログラムを使用して AWS にアクセスする場合、AWSは Software Development Kit (SDK) とコマンドラインインターフェイス (CLI) を提供し、認証情報を使用してリクエストに暗号で署名します。AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。リクエストに自分で署名する推奨方法の使用については、「IAM ユーザーガイド」の「API リクエストに対する AWS Signature Version 4」を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。例えば、AWS は、アカウントのセキュリティを強化するために多要素認証 (MFA) を使用することをお勧

めします。詳細については、「AWS IAM Identity Center ユーザーガイド」の「多要素認証」および「IAM ユーザーガイド」の「IAM の AWS 多要素認証」を参照してください。

AWS アカウント のルートユーザー

AWS アカウント を作成する場合は、このアカウントのすべての AWS のサービス とリソースに対して完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。このアイデンティティは AWS アカウント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることによってアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、IAM ユーザーガイドの「ルートユーザー認証情報が必要なタスク」を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、1 人のユーザーまたは 1 つのアプリケーションに対して特定の許可を持つ AWS アカウント 内のアイデンティティです。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、一時的な認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、「IAM ユーザーガイド」の「長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする」を参照してください。

IAM グループは、IAM ユーザーの集団を指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。例えば、IAMAdmins という名前のグループを設定して、そのグループに IAM リソースを管理する許可を与えることができます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時認証情報が提供されます。詳細については、「IAM ユーザーガイド」の「IAM ユーザーに関するユースケース」を参照してください。

IAM ロール

IAM ロールは、特定の許可を持つ、AWS アカウント内のアイデンティティです。これは IAM ユーザーに似ていますが、特定のユーザーには関連付けられていません。AWS Management Console で

IAM ロールを一時的に引き受けるには、ユーザーから IAM ロール に切り替える (コンソール) ことができます。ロールを引き受けるには、AWS CLI または AWS API オペレーションを呼び出すか、カスタム URL を使用します。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「ロールを引き受けるための各種方法」を参照してください。

IAM ロールと一時的な認証情報は、次の状況で役立ちます:

- フェデレーションユーザーアクセス – フェデレーティッド ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーティッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションのロールについては、「IAM ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) 用のロールを作成する」を参照してください。IAM Identity Center を使用する場合は、許可セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。アクセス許可セットの詳細については、「AWS IAM Identity Center User Guide」の「Permission sets」を参照してください。
- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の AWS のサービス では、(ロールをプロキシとして使用する代わりに) リソースにポリシーを直接アタッチできます。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。
- クロスサービスアクセス権 - 一部の AWS のサービス では、他の AWS のサービス の機能を使用します。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用して AWS でアクションを実行するユーザーは、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、AWS のサービスを呼び出すプリンシパルの権限を、AWS のサービスのリクエストと合わせて使用し、ダウンストリームのサービスに対してリクエストを行います。FAS リクエストは、サービスが、完了するために他の AWS のサービス またはリソースとのやりとりを必要とするリクエストを受け取ったときにのみ行われます。この場合、両方のアクションを実行するた

めのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

- サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除することができます。詳細については、「IAM ユーザーガイド」の「AWS のサービス に許可を委任するロールを作成する」を参照してください。
- サービスにリンクされたロール - サービスにリンクされたロールは、AWS のサービス にリンクされたサービスロールの一種です。サービスがロールを引き受け、ユーザーに代わってアクションを実行できるようになります。サービスにリンクされたロールは、AWS アカウント に表示され、サービスによって所有されます。IAM 管理者は、サービスリンクロールのアクセス許可を表示できますが、編集することはできません。

- Amazon EC2 で実行されているアプリケーション - EC2 インスタンスで実行され、AWS CLI または AWS API リクエストを行っているアプリケーションの一時的な認証情報を管理するには、IAM ロールを使用できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。AWS ロールを EC2 インスタンスに割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスに添付されたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、「IAM ユーザーガイド」の「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して許可を付与する」を参照してください。

ポリシーを使用したアクセス権の管理

AWS でアクセスを制御するには、ポリシーを作成して AWS ID またはリソースにアタッチします。ポリシーは AWS のオブジェクトであり、アイデンティティやリソースに関連付けて、これらのアクセス許可を定義します。AWS は、プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うと、これらのポリシーを評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。大半のポリシーは JSON ドキュメントとして AWS に保存されます。JSON ポリシードキュメントの構造と内容の詳細については、IAM ユーザーガイドの JSON ポリシー概要を参照してください。

管理者は AWS JSON ポリシーを使用して、だれが何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

デフォルトでは、ユーザーやロールに権限はありません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き受けることができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションの許可を定義します。例えば、`iam:GetRole` アクションを許可するポリシーがあるとします。このポリシーがあるユーザーは、AWS Management Console、AWS CLI、または AWS API からロール情報を取得できます。

アイデンティティベースのポリシー

アイデンティティベースポリシーは、IAM ユーザーグループ、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」を参照してください。

アイデンティティベースのポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれます。マネージドポリシーは、AWS アカウント内の複数のユーザー、グループ、およびロールにアタッチできるスタンドアロンポリシーです。マネージドポリシーには、AWS マネージドポリシーとカスタマーマネージドポリシーがあります。マネージドポリシーまたはインラインポリシーのいずれかを選択する方法については、「IAM ユーザーガイド」の「管理ポリシーとインラインポリシーのいずれかを選択する」を参照してください。

AWS マネージドポリシーの詳細については、をSystems Manager参照AWS Systems Manager マネージドポリシーしてください。

リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーションユーザー、または AWS のサービス を含めることができます。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシーでは IAM の AWSマネージドポリシーは使用できません。

ポリシー条件キー

ユーザーとロールが実行できるアクションと、それらのアクションを実行できるリソースは、特定の条件によってさらに制限を加えることが可能です。

JSON ポリシードキュメントでは、Condition 要素 (または Condition ブロック) を使用して、特定のステートメントが有効な条件を指定できます。Condition 要素はオプションです。StringEquals や StringNotLike といった条件演算子を使用して条件式を作成し、ポリシーの条件とリクエスト内の値とを一致させることができます。

1 つのステートメントに複数の Condition 要素を指定する場合、または 1 つの Condition 要素に複数のキーを指定する場合、AWS では AND 論理演算子を使用してそれらを評価します。単一の条件キーに複数の値を指定する場合、AWS では OR 論理演算子を使用して条件を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細については、「IAM ユーザーガイド」の「IAM ポリシーの要素: 変数およびタグ」を参照してください。

AWS はグローバル条件キーとサービス固有の条件キーをサポートしています。条件キーの詳細については、IAM ユーザーガイド の「AWS グローバル条件コンテキストキー」 を参照してください。

> **Important**
>
> Systems Manager Automation を使用する場合は、ポリシーで aws:SourceIp 条件キーを使用しないようにしてください。この条件キーの動作は、オートメーションランブック実行の IAM ロールが指定されているかどうかや、ランブックで使用されるオートメーションアクションの内容など、複数の要因によって異なります。その結果、条件キーによって予期しない動作が発生する可能性があります。このため、使用しないことをお勧めします。

Systems Manager は、独自の条件キーを多数サポートしています。詳細については、「Service Authorization Reference」の「Condition keys for AWS Systems Manager」を参照してください。Systems Manager に固有の条件キーを使用できるアクションとリソースは、「Service Authorization Reference」の「Resource types defined by AWS Systems Manager」に記載しています。

Systems Manager サービスが所有するサービスプリンシパル名に、ポリシーを依存させる必要がある場合は、aws:PrincipalServiceName 条件キーではな

く、aws:PrincipalServiceNamesList 複数値の条件キーを使用してその有無を確認することが推奨されます。aws:PrincipalServiceName 条件キーには、サービスプリンシパル名のリストの 1 つのエントリのみが含まれ、また、想定されるサービスプリンシパル名ではない場合もあります。次の Condition ブロックでは、ssm.amazonaws.com の有無をチェックしています。

```
{
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:PrincipalServiceNamesList": "ssm.amazonaws.com"
        }
    }
}
```

Systems Manager でのアイデンティティベースのポリシーの例は、「AWS Systems Manager アイデンティティベースポリシーの例」でご確認ください。

アクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Amazon S3、AWS WAF、および Amazon VPC は、ACL をサポートするサービスの例です。ACL の詳細については、「Amazon Simple Storage Service デベロッパーガイド」の「アクセスコントロールリスト (ACL) の概要」を参照してください。

その他のポリシータイプ

AWS では、他の一般的ではないポリシータイプをサポートしています。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 - アクセス許可の境界は、アイデンティティベースポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。Principal フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可の境界」を参照してください。

- サービスコントロールポリシー (SCP) - SCP は、AWS Organizations で組織や組織単位 (OU) の最大許可を指定する JSON ポリシーです。AWS Organizations は、お客様が所有する複数の AWS アカウントをグループ化し、一元的に管理するサービスです。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCP) を一部またはすべてのアカウントに適用できます。SCP はメンバーアカウントのエンティティに対する権限を制限します (各 AWS アカウントのルートユーザー など)。Organizations と SCP の詳細については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシー (SCP)」を参照してください。
- リソースコントロールポリシー (RCP) – RCP は、所有する各リソースにアタッチされた IAM ポリシーを更新することなく、アカウント内のリソースに利用可能な最大数のアクセス許可を設定するために使用できる JSON ポリシーです。RCP は、メンバーアカウントのリソースの許可を制限し、組織に属するかどうかにかかわらず、AWS アカウントのルートユーザー を含む ID のための有効な許可に影響を及ぼす可能性があります。RCP をサポートする AWS のサービス のリストを含む Organizations と RCP の詳細については、「AWS Organizations ユーザーガイド」の「リソースコントロールポリシー (RCP)」を参照してください。
- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。複数のポリシータイプが関連するとき、リクエストを許可するかどうかを AWS が決定する方法の詳細については、IAM ユーザーガイドのポリシーの評価ロジックを参照してください。

AWS Systems Manager と IAM の連携方法

AWS Identity and Access Management (IAM) を使用して、AWS Systems Manager へのアクセスを管理するには、Systems Manager で使用できる IAM の機能を理解しておく必要があります。Systems Manager およびその他の AWS のサービス のサービスが IAM と連携する方法の概要については、IAM ユーザーガイドの「IAM と連携する AWS のサービス」を参照してください。

トピック

- Systems Manager アイデンティティベースのポリシー

- Systems Manager リソースベースのポリシー
- Systems Manager タグに基づく認可
- Systems Manager IAM ロール

Systems Manager アイデンティティベースのポリシー

IAM アイデンティティベースのポリシーでは、許可または拒否されたアクションとリソースを指定でき、さらにアクションが許可または拒否された条件を指定できます。Systems Manager は、特定のアクション、リソース、および条件キーをサポートします。JSON ポリシーで使用するすべての要素については「IAM ユーザーガイド」の「IAM JSON ポリシーエレメントのリファレンス」を参照してください。

アクション

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対して、どのような条件下でアクションを実行できるかということです。

JSON ポリシーの `Action` 要素にはポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。ポリシーアクションの名前は通常、関連する AWS API オペレーションと同じです。一致する API オペレーションのない許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは依存アクションと呼ばれます。

このアクションは、関連付けられたオペレーションを実行するためのアクセス許可を付与するポリシーで使用されます。

Systems Manager のポリシーアクションは、アクションの前に次のプレフィックスを使用します: `ssm:`。たとえば、Systems Manager `PutParameter` API オペレーションを使用して Systems Manager パラメータ (SSM パラメータ) を作成するアクセス許可を付与するには、ポリシーに `ssm:PutParameter` アクションを含めます。ポリシーステートメントには、`Action` 要素または `NotAction` 要素のいずれかを含める必要があります。 Systems Manager は、このサービスで実行できるタスクを説明する独自の一連のアクションを定義します。

単一のステートメントに複数のアクションを指定するには、次のようにカンマで区切ります。

```
"Action": [
      "ssm:action1",
      "ssm:action2"
```

```
]
```

> **Note**
>
> AWS Systems Manager の以下のツールは、アクションの前に異なるプレフィックスを使用します。
>
> - AWS AppConfig は、アクションの前にプレフィックス `appconfig:` を使用します。
> - インシデントマネージャーは、アクションの前にプレフィックス `ssm-incidents:` または `ssm-contacts:` を使用します。
> - Systems Manager GUI Connect は、アクションの前にプレフィックス `ssm-guiconnect:` を使用します。
> - Quick Setup は、アクションの前にプレフィックス `ssm-quicksetup:` を使用します。

ワイルドカード (*) を使用して複数アクションを指定できます。例えば、`Describe` という単語で始まるすべてのアクションを指定するには次のアクションを含めます。

```
"Action": "ssm:Describe*"
```

Systems Manager アクションのリストを確認するには、サービス認可リファレンスの「AWS Systems Manager で定義されるアクション」を参照してください。

リソース

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

`Resource` JSON ポリシー要素はアクションが適用されるオブジェクトを指定します。ステートメントには`Resource` または `NotResource` 要素を含める必要があります。ベストプラクティスとして、アマゾン リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの許可と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの権限をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

```
"Resource": "*"
```

たとえば、Systems Manager メンテナンスウィンドウリソースには次の ARN 形式があります。

```
arn:aws:ssm:region:account-id:maintenancewindow/window-id
```

米国東部 (オハイオ) リージョンにおいて、ステートメントで mw-0c50858d01EXAMPLE メンテナンスウィンドウを指定するには、次のような ARN を使用します。

```
"Resource": "arn:aws:ssm:us-east-2:123456789012:maintenancewindow/mw-0c50858d01EXAMPLE"
```

特定のアカウントに属するすべてのメンテナンスウィンドウを指定するには、ワイルドカード (*) を使用します。

```
"Resource": "arn:aws:ssm:region:123456789012:maintenancewindow/*"
```

Parameter Store API オペレーションで、階層の 1 レベルのすべてのパラメータに対するアクセスを許可または制限するには、次のように階層名と AWS Identity and Access Management (IAM) ポリシーを使用できます。

```
"Resource": "arn:aws:ssm:region:123456789012:parameter/Dev/ERP/Oracle/*"
```

リソースの作成など、一部の Systems Manager アクションは、特定のリソースで実行できません。このような場合は、ワイルドカード (*) を使用する必要があります。

```
"Resource": "*"
```

一部の Systems Manager API オペレーションは、複数のリソースを受け入れます。1 つのステートメントで複数のリソースを指定するには、次のように ARN をカンマで区切ります。

```
"Resource": [
      "resource1",
      "resource2"
```

> **Note**
>
> ほとんどの AWS のサービスでは、ARN 内のコロン (:) またはスラッシュ (/) は同じ文字として扱われます。ただし、Systems Manager では、リソースパターンおよびルールで完全一致

が必要です。イベントパターンの作成時に、リソースの ARN と一致する正しい ARN 文字を使用します。

以下の表は、Systems Manager でサポートされているリソースタイプの ARN 形式を示しています。

Note

ARN 形式には以下の例外があることに注意してください。

- AWS Systems Manager の以下のツールは、アクションの前に異なるプレフィックスを使用します。
  - AWS AppConfig は、アクションの前にプレフィックス `appconfig:` を使用します。
  - インシデントマネージャーは、アクションの前にプレフィックス `ssm-incidents:` または `ssm-contacts:` を使用します。
  - Systems Manager GUI Connect は、アクションの前にプレフィックス `ssm-guiconnect` を使用します。
- Amazon が所有するドキュメントやオートメーション定義リソース、および Amazon とサードパーティの両方のソースから提供されるパブリックパラメータには、ARN 形式のアカウント ID は含まれていません。例 :
  - SSM ドキュメント `AWS-RunPatchBaseline`:

    ```
    arn:aws:ssm:us-east-2::document/AWS-RunPatchBaseline
    ```
  - オートメーションランブック `AWS-ConfigureMaintenanceWindows`:

    ```
    arn:aws:ssm:us-east-2::automation-definition/AWS-ConfigureMaintenanceWindows
    ```
  - パブリックパラメータ `/aws/service/bottlerocket/aws-ecs-1-nvidia/x86_64/1.13.4/image_version`:

    ```
    arn:aws:ssm:us-east-2::parameter/aws/service/bottlerocket/aws-ecs-1-nvidia/x86_64/1.13.4/image_version
    ```

  これらの 3 種類のリソースタイプの詳細については、次のトピックを参照してください。
  - ドキュメントでの作業
  - Systems Manager Automation を使用した自動オペレーションを実行する
  - Parameter Store でのパブリックパラメータの使用

- Quick Setup は、アクションの前にプレフィックス `ssm-quicksetup:` を使用します。

リソースタイプ	ARN 形式
アプリケーション (AWS AppConfig)	arn:aws:appconfig:*region*:*account-id* :application/*application-id*
関連付け	arn:aws:ssm:*region*:*account-id* :association/*association-id*
自動化の実行	arn:aws:ssm:*region*:*account-id* :automation-execution/*automation-execution-id*
自動化定義 (およびバージョンサブリソース)	arn:aws:ssm:*region*:*account-id* :automation-definition/*automation-definition-id* :*version-id* [1]
設定プロファイル (AWS AppConfig)	arn:aws:appconfig:*region*:*account-id* :application/*application-id* /configurationprofile/*configurationprofile-id*
連絡先 (Incident Manager)	arn:aws:ssm-contacts:*region*:*account-id* :contact/*contact-alias*
デプロイ戦略 (AWS AppConfig)	arn:aws:appconfig:*region*:*account-id* :deploymentstrategy/*deploymentstrategy-id*
ドキュメント	arn:aws:ssm:*region*:*account-id* :document/*document-name*
環境 (AWS AppConfig)	arn:aws:appconfig:*region*:*account-id* :application/*application-id* /environment/*environment-id*
インシデント	arn:aws:ssm-incidents:*region*:*account-id* :incident-record/*response-plan-name* /*incident-id*
メンテナンスウィンドウ	arn:aws:ssm:*region*:*account-id* :maintenancewindow/*window-id*
マネージドノード	arn:aws:ssm:*region*:*account-id* :managed-instance/*managed-node-id*

リソースタイプ	ARN 形式
マネージドノードインベントリ	arn:aws:ssm:*region*:*account-id* :managed-instance-inventory /*managed-node-id*
OpsItem	arn:aws:ssm:*region*:*account-id* :opsitem/*OpsItem-id*
パラメータ	1 レベルのパラメータ: • arn:aws:ssm:*region*:*account-id* :parameter/*parameter-name*/ 階層構造を反映したパラメータ名: • arn:aws:ssm:*region*:*account-id* :parameter/*parameter-name-root* /*level-2*/*level-3*/*level-4*/*level-5* [2]
パッチベースライン	arn:aws:ssm:*region*:*account-id* :patchbaseline/*patch-baseline-id*
対応計画	arn:aws:ssm-incidents:*region*:*account-id* :response-plan/*response-plan-name*
セッション	arn:aws:ssm:*region*:*account-id* :session/*session-id* [3]
すべての Systems Manager リソース	arn:aws:ssm:*
特定の AWS リージョンの特定の AWS アカウント が所有するすべての Systems Manager リソース	arn:aws:ssm:*region*:*account-id* :*

[1]
オートメーションの定義について、Systems Manager は第 2 レベルのリソース、バージョン ID をサ

ポートしています。AWS では、これらの第 2 レベルのリソースはサブリソースと呼ばれます。オートメーション定義リソースのバージョンサブリソースを指定することで、特定バージョンの自動化定義にアクセスできます。たとえば、ノード管理においてオートメーション定義の最新バージョンのみが使用される場合があります。

2

パラメータを編成して管理するには、階層構造を反映したパラメータ名を作成できます。階層構造では、パラメータ名のパスの定義にスラッシュを使用できます。パラメータリソース名には、最大 15 レベルを反映できます。作成する階層には、環境の既存の階層構造を反映するようお勧めします。詳細については、「」を参照してくださいSystems Manager での Parameter Store パラメータの作成

3

ほとんどの場合、セッション ID は、セッションを開始したアカウントユーザーの ID に英数字のサフィックスを付けたものを使用して作成されます。以下に例を示します。

```
arn:aws:us-east-2:111122223333:session/JohnDoe-1a2b3c4sEXAMPLE
```

ただし、ユーザー ID が使用できない場合、ARN は次の方法で構築されます。

```
arn:aws:us-east-2:111122223333:session/session-1a2b3c4sEXAMPLE
```

ARN の形式の詳細については、「Amazon Web Services 全般のリファレンス」の「Amazon リソースネーム (ARN)」を参照してください。

Systems Manager リソースのタイプとその ARN のリストを確認するには、サービス認可リファレンスの「AWS Systems Manager で定義されるリソース」を参照してください。どのアクションで各リソースの ARN を指定できるかについては、「AWS Systems Manager で定義されるアクション」を参照してください。

Systems Manager の条件キー

管理者は AWS JSON ポリシーを使用して、だれが何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

Condition 要素 (または Condition ブロック) を使用すると、ステートメントが有効な条件を指定できます。Condition 要素はオプションです。イコールや未満などの 条件演算子 を使用して条件式を作成して、ポリシーの条件とリクエスト内の値を一致させることができます。

1 つのステートメントに複数の Condition 要素を指定する場合、または 1 つの Condition 要素に複数のキーを指定する場合、AWS では AND 論理演算子を使用してそれらを評価します。単一の条件

キーに複数の値を指定する場合、AWS では OR 論理演算子を使用して条件を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細については、「IAM ユーザーガイド」の「IAM ポリシーの要素: 変数およびタグ」を参照してください。

AWS はグローバル条件キーとサービス固有の条件キーをサポートしています。すべての AWS グローバル条件キーを確認するには、IAM ユーザーガイドのAWS グローバル条件コンテキストキーを参照してください。

Systems Manager の条件キーのリストを確認するには、サービス認可リファレンスのAWS Systems Manager の条件キーを参照してください。どのアクションおよびリソースと条件キーを使用できるかについては、AWS Systems Manager で定義されるアクションを参照してください。

`ssm:resourceTag/*` 条件キーの使用については、以下のトピックを参照してください。

- SSM Agent を介してルートレベルコマンドへのアクセスを制限する
- タグによる Run Command アクセスを制限
- Restrict session access based on instance tags (インスタンスタグに基づくセッションのアクセスの制限)

`ssm:Recursive`、`ssm:Policies`、および `ssm:Overwrite` 条件キーの使用については、「Parameter Store API オペレーションへのアクセスの防止」を参照してください。

例

Systems Manager アイデンティティベースのポリシーの例を表示するには、AWS Systems Manager アイデンティティベースポリシーの例を参照してください。

Systems Manager リソースベースのポリシー

Amazon Simple Storage Service (Amazon S3) などの他の AWS のサービスでは、リソースベースのアクセス権限ポリシーがサポートされています。例えば、ポリシーを S3 バケットにアタッチして、そのバケットに対するアクセス許可を管理できます。

Systems Manager では、リソースベースのポリシーはサポートされていません。

Systems Manager タグに基づく認可

タグを Systems Manager リソースにアタッチすることも、Systems Manager へのリクエストでタグを渡すこともできます。タグに基づいてアクセスを制御するには、`ssm:resourceTag/key-name`、`aws:ResourceTag/key-name`、`aws:RequestTag/key-name`、または `aws:TagKeys` 条件キーを使用して、ポリシーの条件要素でタグ情報を提供します。タグを作成または更新するときに、次のリソースタイプにタグを追加できます。

- ドキュメント
- マネージドノード
- メンテナンスウィンドウ
- Parameter
- パッチベースライン
- OpsItem

リソースのタグに基づいてリソースへのアクセスを制限するためのアイデンティティベースのポリシーの例を表示するには、「タグに基づく Systems Manager ドキュメントの表示」を参照してください。

Systems Manager IAM ロール

IAM ロール は、特定のアクセス許可を持つ、AWS アカウント 内のエンティティです。

Systems Manager での一時的な認証情報の使用

テンポラリ認証情報を使用して、フェデレーションでサインイン、IAM ロールを引き受ける、またはクロスアカウントロールを引き受けることができます。テンポラリセキュリティ認証情報を取得するには、AssumeRole または GetFederationToken などの AWS Security Token Service AWS STSAPI オペレーションを呼び出します。

Systems Manager では、一時認証情報の使用をサポートしています。

サービスリンクロール

サービスにリンクされたロールは、AWS のサービスが他のサービスのリソースにアクセスして自動的にアクションを完了することを許可します。サービスリンクロールは、IAM アカウント内に表示され、サービスによって所有されます。 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。

Systems Manager はサービスにリンクされたロールをサポートします。Systems Manager サービスにリンクされたロールの作成または管理の詳細については、「Systems Manager のサービスにリンクされたロールの使用」を参照してください。

サービス役割

この機能により、ユーザーに代わってサービスがサービス役割を引き受けることが許可されます。このロールにより、サービスはユーザーに代わって他のサービスのリソースにアクセスし、アクションを完了できます。サービスロールは、IAM アカウントに表示され、アカウントによって所有されます。つまり、 管理者は、このロールのアクセス許可を変更できます。ただし、それにより、サービスの機能が損なわれる場合があります。

Systems Manager はサービスロールをサポートします。

Systems Manager で IAM ロールを選択

Systems Manager がマネージドノードとやり取りするには、ユーザーに代わって Systems Manager がノードにアクセスできるようにロールを選択する必要があります。サービスロールあるいはサービスにリンクされたロールを以前に作成している場合、Systems Manager は選択できるロールのリストを示します。マネージドノードの起動と停止を許可するロールを選択することが重要です。

EC2 インスタンスにアクセスするには、インスタンスのアクセス許可を設定する必要があります。詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」を参照してください。

ハイブリッドおよびマルチクラウドの非 EC2 ノードにアクセスするには、AWS アカウント に IAM サービスロールが必要です。詳細については、「ハイブリッドおよびマルチクラウド環境で Systems Manager に必要な IAM サービスロールを作成する」を参照してください。

Automation ワークフローは、サービスロール (または継承ロール) のコンテキストで開始できます。これにより、サービスがユーザーに代わってアクションを実行できるようになります。継承ロールを指定しない場合、オートメーションは、実行を呼び出したユーザーのコンテキストを使用します。ただし、特定の条件では、Automation のサービスロールを指定する必要があります。詳細については、「オートメーションのサービスロール (ロールを引き受ける) アクセスの設定」を参照してください。

AWS Systems Manager マネージドポリシー

AWS は、 によって作成され管理されるスタンドアロンの IAM ポリシーを提供することで、多くの一般的ユースケースに対応します。AWSこれらの AWS 管理ポリシーでは、一般的ユースケースに

必要なアクセス権限を付与されるため、どのアクセス権限が必要であるかを調べる必要がありません。(独自のカスタム IAM ポリシーを作成して、Systems Manager アクションとリソースのための権限を許可することもできます。)

Systems Manager のマネージドポリシーの詳細については、「AWS の AWS Systems Manager マネージドポリシー」を参照してください。

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

AWS Systems Manager アイデンティティベースポリシーの例

デフォルトでは、AWS Identity and Access Management (IAM) エンティティ (ユーザーやロール) には、AWS Systems Manager リソースを作成または変更するアクセス許可は付与されていません。また、Systems Manager コンソール、AWS Command Line Interface (AWS CLI)、または AWS API を使用してタスクを実行しません。IAM 管理者は、指定されたリソースで特定の API 操作を実行するための許可をユーザーとロールに付与する IAM ポリシーを作成する必要があります。続いて、管理者はそれらのアクセス許可が必要なユーザーまたはグループにそのポリシーをアタッチします。

次の許可ポリシーの例では、米国東部 (オハイオ) (us-east-2) AWS リージョン で **MyDocument-** で始まる名前のドキュメントを削除することをユーザーに許可します。

```
{
  "Version": "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:DeleteDocument"
      ],
      "Resource" : [
        "arn:aws:ssm:us-east-2:111122223333:document/MyDocument-*"
      ]
    }
  ]
}
```

JSON ポリシードキュメントのこれらの例を使用して、IAM アイデンティティベースのポリシーを作成する方法については、IAM ユーザーガイドの「IAM ポリシーの作成」を参照してください。

トピック

- ポリシーに関するベストプラクティス
- Systems Manager コンソールを使用する
- 自分の権限の表示をユーザーに許可する
- サービス間の混乱した代理の防止
- カスタマーマネージドポリシーの例
- タグに基づく Systems Manager ドキュメントの表示

ポリシーに関するベストプラクティス

ID ベースのポリシーは、ユーザーのアカウントで誰かが Systems Manager リソースを作成、アクセス、または削除できるどうかを決定します。これらのアクションを実行すると、AWS アカウント に料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS マネージドポリシーを使用して開始し、最小特権の許可に移行する – ユーザーとワークロードへの許可の付与を開始するには、多くの一般的なユースケースのために許可を付与する AWS マネージドポリシーを使用します。これらは AWS アカウントで使用できます。ユースケース別に AWS カスタマーマネージドポリシーを定義して、マネージドポリシーを絞り込むことをお勧めします。詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」または「ジョブ機能の AWS マネージドポリシー」を参照してください。
- 最小特権を適用する – IAM ポリシーで許可を設定する場合は、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、「IAM ユーザーガイド」の「IAM でのポリシーとアクセス許可」を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。また、AWS CloudFormation などの特定の AWS のサービス を介して使用する場合、条件を使用してサービスアクションへのアクセスを許可することもできます。詳細については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素:条件」を参照してください。
- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサ

ポートします。詳細については、「IAM ユーザーガイド」の「IAM Access Analyzer でポリシーを検証する」を参照してください。

- 多要素認証 (MFA) を要求する – AWS アカウントで IAM ユーザーまたはルートユーザーを要求するシナリオがある場合は、セキュリティを強化するために MFA をオンにします。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、「IAM ユーザーガイド」の「MFA を使用した安全な API アクセス」を参照してください。

IAM でのベストプラクティスの詳細については、「IAM ユーザーガイド」の「IAM でのセキュリティのベストプラクティス」を参照してください。

Systems Manager コンソールを使用する

Systems Manager コンソールにアクセスするには、一連の最小限のアクセス許可が必要です。これらのアクセス許可により、AWS アカウント の Systems Manager リソースおよび他のリソースの詳細をリストおよび表示できます。

最小限必要なアクセス許可よりも厳しく制限されたアイデンティティベースのポリシーを作成すると、そのポリシーを持つ IAM エンティティ (ユーザーやロール) に対してコンソールが意図したとおりに機能しなくなります。

AWS CLI または AWS API のみを呼び出すユーザーには、最小限のコンソール許可を付与する必要はありません。代わりに、実行しようとしている API オペレーションに一致するアクションのみへのアクセスが許可されます。

ユーザーおよびロールが引き続き Systems Manager コンソールを使用できるようにするには、エンティティに AmazonSSMFullAccess または AmazonSSMReadOnlyAccess AWS マネージドポリシーもアタッチしてください。詳細については、「IAM ユーザーガイド」の「ユーザーへのアクセス許可の追加」を参照してください。

自分の権限の表示をユーザーに許可する

この例では、ユーザーアイデンティティにアタッチされたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーの作成方法を示します。このポリシーには、コンソールで、または AWS CLI か AWS API を使用してプログラム的に、このアクションを完了するアクセス許可が含まれています。

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

```
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

サービス間の混乱した代理の防止

混乱した代理問題は、アクションを実行する許可を持たないエンティティが、より特権のあるエンティティにアクションを実行するように強制できるセキュリティの問題です。AWS では、サービス間でのなりすましによって、混乱した代理問題が発生する場合があります。サービス間でのなりすましは、1 つのサービス (呼び出し元サービス) が、別のサービス (呼び出し対象サービス) を呼び出すときに発生する可能性があります。呼び出し元サービスは、本来ならアクセスすることが許可されるべきではない方法でその許可を使用して、別のお客様のリソースに対する処理を実行するように操作される場合があります。これを防ぐため、AWS では、アカウント内のリソースへのアクセス権が付与されたサービスプリンシパルですべてのサービスのデータを保護するために役立つツールを提供しています。

リソースポリシーで aws:SourceArn および aws:SourceAccount のグローバル条件コンテキストキーを使用して、AWS Systems Manager が別のサービスに付与する許可をそのリソースに制限することをお勧めします。aws:SourceArn 値に、S3 バケットの Amazon リソースネーム (ARN) などのアカウント ID が含まれていない場合は、アクセス許可を制限するために、両方のグローバル条件コンテキストキーを使用する必要があります。同じポリシーステートメントでこれらのグローバル条件コンテキストキーの両方を使用し、アカウント ID にaws:SourceArn の値が含まれていない場合、aws:SourceAccount 値と aws:SourceArn 値の中のアカウントには、同じアカウント ID を使用する必要があります。クロスサービスのアクセスにリソースを 1 つだけ関連付けたい場合は、aws:SourceArn を使用します。そのアカウント内のリソースをクロスサービスの使用に関連付けることを許可する場合は、aws:SourceAccount を使用します。

以下のセクションは AWS Systems Manager ツールにおけるポリシーの例を示します。

ハイブリッドアクティベーション ポリシーの例

ハイブリッドアクティベーションで使用されるサービスロールの場合、aws:SourceArn の値は AWS アカウント の ARN である必要があります。ハイブリッドアクティベーションを作成したときの ARN の AWS リージョン を必ず指定してください。リソースの ARN 全体が不明または複数のリソースを指定する場合、ARN の未知部分にワイルドカード (*) が付いた aws:SourceArn グローバルコンテキスト条件キー を使用します。例えば、arn:aws:ssm:*:*region*:*123456789012*:* と指定します。

次の例は、オートメーションの aws:SourceArn および aws:SourceAccount グローバル条件コンテキストキーを使用して、米国東部 (オハイオ) リージョン (us-east-2) での混乱した使節の問題を防止する方法を示しています。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"",
         "Effect":"Allow",
         "Principal":{
            "Service":"ssm.amazonaws.com"
         },
         "Action":"sts:AssumeRole",
         "Condition":{
            "StringEquals":{
               "aws:SourceAccount":"123456789012"
            },
            "ArnEquals":{
```

```
                "aws:SourceArn":"arn:aws:ssm:us-east-2:123456789012:*"
            }
         }
      }
   ]
}
```

リソースデータ同期ポリシーの例

Systems Manager Inventory、Explorer、コンプライアンスはリソースデータ同期の作成を実現して、オペレーションデータ (OpsData) のストレージを中央の Amazon Simple Storage Service バケットに一元化できます。AWS Key Management Service (AWS KMS) を使用してリソースデータの同期を暗号化する場合、次のポリシーを含む新しいキーを作成するか、既存のキーを更新してこのポリシーを追加する必要があります。このポリシー内の aws:SourceArn と aws:SourceAccount の条件キーは「混乱した使節の問題」を防止します。次の通り、ポリシーの例を示します。

```
{
    "Version": "2012-10-17",
    "Id": "ssm-access-policy",
    "Statement": [
        {
            "Sid": "ssm-access-policy-statement",
            "Action": [
                "kms:GenerateDataKey"
            ],
            "Effect": "Allow",
            "Principal": {
                "Service": "ssm.amazonaws.com"
            },
            "Resource": "arn:aws:kms:us-east-2:123456789012:key/KMS_key_id",
            "Condition": {
                "StringLike": {
                    "aws:SourceAccount": "123456789012"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:ssm:*:123456789012:role/aws-service-role/
ssm.amazonaws.com/AWSServiceRoleForAmazonSSM"
                }
            }
        }
    ]
}
```

> **Note**
>
> ポリシー例の ARN は、システムに対して AWS Security Hub を除くすべてのソースにおける OpsData の暗号化を実現します。Security Hub データを暗号化する必要がある場合、たとえば Explorer でSecurity Hub データを収集した場合、次の ARN を指定する追加ポリシーをアタッチする必要があります:
> `"aws:SourceArn": "arn:aws:ssm:*:account-id:role/aws-service-role/opsdatasync.ssm.amazonaws.com/AWSServiceRoleForSystemsManagerOpsDataSync"`

カスタマーマネージドポリシーの例

スタンドアロンポリシーを作成して独自の AWS アカウント で管理できます。このようなポリシーは、カスタマー管理ポリシーと呼ばれます。これらのポリシーは、AWS アカウント の複数のプリンシパルエンティティにアタッチできます。ポリシーをプリンシパルエンティティにアタッチすると、ポリシーで定義されたアクセス権限がエンティティに付与されます。詳細については、IAM ユーザーガイドの「お客様が管理するポリシーの例」を参照してください。

以下のユーザーポリシーの例では、さまざまな Systems Manager アクションのアクセス許可を付与します。これらを使用して、IAM エンティティ (ユーザーやロール) の Systems Manager アクセス許可を制限します。これらのポリシーは、Systems Manager API、AWS SDK、または AWS CLI でアクションを実行するときに機能します。コンソールを使用するユーザーに対しては、コンソールに固有の追加のアクセス権限を付与する必要があります。詳細については、「」を参照してくださいSystems Manager コンソールを使用する

> **Note**
>
> すべての例で、米国西部 (オレゴン) リージョン (us-west-2) を使用し、架空のアカウント ID を使用しています。AWS パブリックドキュメント (`AWS-*` で始まるドキュメント) については、Amazon リソースネーム (ARN) にアカウント ID を指定しないでください。

例

- 例 1: ユーザーに単一リージョンで Systems Manager オペレーションを実行することを許可する
- 例 2: 単一リージョンのドキュメントの一覧表示をユーザーに許可する

例 1: ユーザーに単一リージョンで Systems Manager オペレーションを実行することを許可する

次の例では、米国東部 (オハイオ) リージョン (us-east-2) でのみ Systems Manager オペレーションを実行するための許可を付与します。

```
{
  "Version": "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:*"
      ],
      "Resource" : [
        "arn:aws:ssm:us-east-2:aws-account-ID:*"
      ]
    }
  ]
}
```

例 2: 単一リージョンのドキュメントの一覧表示をユーザーに許可する

次の例で付与する許可では、米国東部 (オハイオ) リージョン (us-east-2) の **Update** で始まるすべてのドキュメント名を一覧表示できます。

```
{
  "Version": "2012-10-17",
  "Statement" : [
    {
      "Effect" : "Allow",
      "Action" : [
        "ssm:ListDocuments"
      ],
      "Resource" : [
        "arn:aws:ssm:us-east-2:aws-account-ID:document/Update*"
      ]
    }
  ]
}
```

例3: ユーザーが特定 SSM ドキュメントを使用して特定ノードでコマンドを実行することを許可します。

次の IAM ポリシーの例は、ユーザーが米国東部 (オハイオ) リージョン (us-east-2) で次の操作を実行することを許可します。

- Systems Manager のドキュメント (SSM ドキュメント) とドキュメントバージョンを一覧表示します。
- ドキュメントに関する詳細の表示。
- ポリシーに指定されたドキュメントを使用してコマンドを送信します。ドキュメント名は次のエントリによって決定します。

```
arn:aws:ssm:us-east-2:aws-account-ID:document/Systems-Manager-document-name
```

- コマンドを 3 つのノードに送信します。ノードは 2 番目の Resource セクションにある以下のエントリによって決定されます。

```
"arn:aws:ec2:us-east-2:aws-account-ID:instance/i-02573cafcfEXAMPLE",
"arn:aws:ec2:us-east-2:aws-account-ID:instance/i-0471e04240EXAMPLE",
"arn:aws:ec2:us-east-2:aws-account-ID:instance/i-07782c72faEXAMPLE"
```

- 送信後のコマンドの詳細を表示。
- AWS Systems Manager のツールである Automation でワークフローを開始および停止します。
- 自動化ワークフローに関する情報を取得します。

ユーザーがアクセスできる任意のノードで同ユーザーがこのドキュメントを使用してコマンドを送信する許可を付与する場合、Resource セクションで次のようなエントリを指定してその他のノードエントリを削除します。次の例では、米国東部 (オハイオ) リージョン (us-east-2) を使用しています。

```
"arn:aws:ec2:us-east-2:*:instance/*"
```

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ssm:ListDocuments",
                "ssm:ListDocumentVersions",
```

```
                "ssm:DescribeDocument",
                "ssm:GetDocument",
                "ssm:DescribeInstanceInformation",
                "ssm:DescribeDocumentParameters",
                "ssm:DescribeInstanceProperties"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": "ssm:SendCommand",
            "Effect": "Allow",
            "Resource": [
                "arn:aws:ec2:us-east-2:aws-account-ID:instance/i-02573cafcfEXAMPLE",
                "arn:aws:ec2:us-east-2:aws-account-ID:instance/i-0471e04240EXAMPLE",
                "arn:aws:ec2:us-east-2:aws-account-ID:instance/i-07782c72faEXAMPLE",

                "arn:aws:ssm:us-east-2:aws-account-ID:document/Systems-Manager-
document-name"
            ]
        },
        {
            "Action": [
                "ssm:CancelCommand",
                "ssm:ListCommands",
                "ssm:ListCommandInvocations"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": "ec2:DescribeInstanceStatus",
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": "ssm:StartAutomationExecution",
            "Effect": "Allow",
            "Resource": [
                "arn:aws:ssm:us-east-2:aws-account-ID:automation-definition/*"
            ]
        },
        {
            "Action": "ssm:DescribeAutomationExecutions",
```

```
            "Effect": "Allow",
            "Resource": [
                "*"
            ]
        },
        {
            "Action": [
                "ssm:StopAutomationExecution",
                "ssm:GetAutomationExecution"
            ],
            "Effect": "Allow",
            "Resource": [
                "*"
            ]
        }
    ]
}
```

タグに基づく Systems Manager ドキュメントの表示

アイデンティティベースのポリシーの条件を使用して、タグに基づいて Systems Manager リソースへのアクセスをコントロールできます。この例では、SSM ドキュメントを表示できるポリシーを作成する方法を示します。ただし、ドキュメントタグ Owner にそのユーザーのユーザー名の値がある場合のみ、アクセス許可は付与されます。このポリシーでは、このアクションをコンソールで実行するために必要なアクセス許可も付与します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ListDocumentsInConsole",
            "Effect": "Allow",
            "Action": "ssm:ListDocuments",
            "Resource": "*"
        },
        {
            "Sid": "ViewDocumentIfOwner",
            "Effect": "Allow",
            "Action": "ssm:GetDocument",
            "Resource": "arn:aws:ssm:*:*:document/*",
            "Condition": {
                "StringEquals": {"ssm:ResourceTag/Owner": "${aws:username}"}
            }
```

```
        }
    ]
}
```

このポリシーをアカウントの ユーザーにアタッチできます。richard-roe という名前のユーザーが Systems Manager ドキュメントを表示しようとする場合、ドキュメントに Owner=richard-roe または owner=richard-roe というタグが付いている必要があります。タグが付いていない場合は、アクセスが拒否されます。条件キー名では大文字と小文字は区別されないため、条件タグキー Owner は Owner と owner に一致します。詳細については、IAM ユーザーガイド」の「IAM JSON ポリシー要素: 条件」を参照してください。

AWS の AWS Systems Manager マネージドポリシー

AWS マネージドポリシーは、AWS が作成および管理するスタンドアロンポリシーです。AWS マネージドポリシーは、多くの一般的なユースケースでアクセス許可を提供できるように設計されているため、ユーザー、グループ、ロールへのアクセス許可の割り当てを開始できます。

AWS マネージドポリシーは、ご利用の特定のユースケースに対して最小特権のアクセス許可を付与しない場合があることにご注意ください。これは、すべての AWS ユーザーが使用できるようになるのを避けるためです。ユースケースに固有のカスタマー管理ポリシーを定義して、アクセス許可を絞り込むことをお勧めします。

AWS マネージドポリシーで定義されたアクセス許可は変更できません。AWS が AWS マネージドポリシーに定義されている権限を更新すると、更新はポリシーがアタッチされているすべてのプリンシパルアイデンティティ (ユーザー、グループ、ロール) に影響します。新しい AWS のサービス を起動するか、既存のサービスで新しい API オペレーションが使用可能になると、AWS が AWS マネージドポリシーを更新する可能性が最も高くなります。

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

AWS 管理ポリシー: AmazonSSMServiceRolePolicy

このポリシーを使用すると、AWS Systems Manager によって管理されているか、Systems Manager オペレーションで使用されている数多くの AWS リソースにアクセスできます。

AWS Identity and Access Management (IAM) エンティティに AmazonSSMServiceRolePolicy をアタッチすることはできません。このポリシーは、ユーザーに代わって AWS Systems Manager が

アクションを実行することを許可する、サービスにリンクされたロールにアタッチされます。詳細については、「ロールを使用してインベントリの収集と OpsData の表示を行う」を参照してください。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- ssm – プリンシパルが Run Command と Automation の両方を開始およびステップ実行すること、Run Command と Automation オペレーションに関する情報を取得すること、Parameter Store パラメータである Change Calendar カレンダーに関する情報を取得すること、OpsCenter リソースの Systems Manager サービス設定に関する情報を更新および取得すること、リソースに適用されたタグに関する情報を読み込むことを許可します。
- cloudformation – プリンシパルがスタックセットオペレーションとスタックセットインスタンスに関する情報を取得すること、リソース arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-SSM*:* 上のスタックセットを削除することを許可します。プリンシパルが次のリソースに関連付けられているスタックインスタンスを削除することを許可します。

```
arn:aws:cloudformation:*:*:stackset/AWS-QuickSetup-SSM*:*
arn:aws:cloudformation:*:*:stackset-target/AWS-QuickSetup-SSM*:*
arn:aws:cloudformation:*:*:type/resource/*
```

- cloudwatch – プリンシパルが Amazon CloudWatch アラームに関する情報を取得することを許可します。
- compute-optimizer – プリンシパルが AWS Compute Optimizer サービスに対するアカウントの登録 (オプトイン) ステータスを取得すること、特定の規定要件セットを満たす Amazon EC2 インスタンスの推奨事項を取得することを許可します。
- config – プリンシパルが AWS Config で情報修正設定と設定レコーダーを取得すること、指定された AWS Config ルールと AWS リソースに準拠するかどうかを決定することを許可します。
- events – プリンシパルが EventBridge ルールに関する情報を取得すること、Systems Manager サービス (ssm.amazonaws.com) 専用の EventBridge ルールとターゲットを作成すること、リソース arn:aws:events:*:*:rule/SSMExplorerManagedRule のルールとターゲットを削除することを許可します。
- ec2 – プリンシパルが Amazon EC2 インスタンスに関する情報を取得することを許可します。
- iam – プリンシパルが Systems Manager サービス (ssm.amazonaws.com) のロールのアクセス許可を渡すことを許可します。

- `lambda` – プリンシパルが特に Systems Manager で使用するために設定された Lambda 関数を呼び出すことを許可します。
- `resource-explorer-2` – プリンシパルが EC2 インスタンスに関するデータを取得して、各インスタンスが現在 Systems Manager によって管理されているかどうかを確認することを許可します。

  アクション `resource-explorer-2:CreateManagedView` は、`arn:aws:resource-explorer-2:*:*:managed-view/AWSManagedViewForSSM*` リソースに対して許可されます。
- `resource-groups` – プリンシパルがリソースグループに属する AWS Resource Groups リソースからリソースグループとそのメンバーのリストを取得することを許可します。
- `securityhub` – プリンシパルが現在のアカウントの AWS Security Hub ハブリソースに関する情報を取得することを許可します。
- `states` – プリンシパルが特に Systems Manager で使用するために設定された AWS Step Functions を開始してその情報を取得することを許可します。
- `support` – プリンシパルが AWS Trusted Advisor のチェックとケースに関する情報を取得することを許可します。
- `tag` – プリンシパルがアカウントの指定された AWS リージョンにあるすべてのタグ付けされたリソースまたは以前にタグ付けされていたリソースに関する情報を取得することを許可します。

JSON ポリシードキュメントの最新バージョンなど、ポリシーについてさらに詳しく確認するには、「AWS マネージドポリシーリファレンスガイド」の「AmazonSSMServiceRolePolicy」を参照してください。

AWS マネージドポリシー: AmazonSSMReadOnlyAccess

`AmazonSSMReadOnlyAccess` ポリシーを IAM アイデンティティにアタッチできます。このポリシーは、`Describe*`、`Get*`、`List*` など、AWS Systems Manager API オペレーションへの読み取り専用アクセスを許可します。

JSON ポリシードキュメントの最新バージョンなど、ポリシーについてさらに詳しく確認するには、「AWS マネージドポリシーリファレンスガイド」の「AmazonSSMReadOnlyAccess」を参照してください。

AWS マネージドポリシー: AWSSystemsManagerOpsDataSyncServiceRolePolicy

IAM エンティティに AWSSystemsManagerOpsDataSyncServiceRolePolicy をアタッチすることはできません。このポリシーは、ユーザーに代わって Systems Manager がアクションを実行することを許可する、サービスにリンクされたロールにアタッチされます。詳細については、「ロールを使用して、Explorer の OpsData および OpsItems を作成」を参照してください。

AWSSystemsManagerOpsDataSyncServiceRolePolicy では、AWSServiceRoleForSystemsManagerOpsDataSync サービスリンクロールは AWS Security Hub の結果から OpsItems と OpsData を作成して更新できます。

ポリシーでは、Systems Manager がすべての関連リソース ("Resource": "*") に対して、以下のアクションを実行できます。ただし、後述しているような例外があります。

- ssm:GetOpsItem [1]
- ssm:UpdateOpsItem [1]
- ssm:CreateOpsItem
- ssm:AddTagsToResource [2]
- ssm:UpdateServiceSetting [3]
- ssm:GetServiceSetting [3]
- securityhub:GetFindings
- securityhub:GetFindings
- securityhub:BatchUpdateFindings [4]

[1] ssm:GetOpsItem および ssm:UpdateOpsItem のアクションは以下の条件でのみ Systems Manager のサービスに許可されます。

```
"Condition": {
    "StringEquals": {
        "aws:ResourceTag/ExplorerSecurityHubOpsItem": "true"
    }
}
```

[2] ssm:AddTagsToResource アクションは以下のリソースにのみ許可されます。

```
arn:aws:ssm:*:*:opsitem/*
```

[3] ssm:UpdateServiceSetting および ssm:GetServiceSetting アクションは以下のリソースにのみ許可されます。

```
arn:aws:ssm:*:*:servicesetting/ssm/opsitem/*
arn:aws:ssm:*:*:servicesetting/ssm/opsdata/*
```

[4] securityhub:BatchUpdateFindings は以下の条件でのみ、Systems Manager のサービスへのアクセス許可が拒否されます。

```
{
   "Effect": "Deny",
   "Action": "securityhub:BatchUpdateFindings",
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "securityhub:ASFFSyntaxPath/Workflow.Status": "SUPPRESSED"
    }
   }
  },
  {
   "Effect": "Deny",
   "Action": "securityhub:BatchUpdateFindings",
   "Resource": "*",
   "Condition": {
    "Null": {
     "securityhub:ASFFSyntaxPath/Confidence": false
    }
   }
  },
  {
   "Effect": "Deny",
   "Action": "securityhub:BatchUpdateFindings",
   "Resource": "*",
   "Condition": {
    "Null": {
     "securityhub:ASFFSyntaxPath/Criticality": false
    }
   }
  },
  {
   "Effect": "Deny",
   "Action": "securityhub:BatchUpdateFindings",
   "Resource": "*",
```

```
    "Condition": {
     "Null": {
      "securityhub:ASFFSyntaxPath/Note.Text": false
     }
    }
   },
   {
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
     "Null": {
      "securityhub:ASFFSyntaxPath/Note.UpdatedBy": false
     }
    }
   },
   {
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
     "Null": {
      "securityhub:ASFFSyntaxPath/RelatedFindings": false
     }
    }
   },
   {
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
     "Null": {
      "securityhub:ASFFSyntaxPath/Types": false
     }
    }
   },
   {
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
     "Null": {
      "securityhub:ASFFSyntaxPath/UserDefinedFields.key": false
     }
```

```
    }
   },
   {
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
     "Null": {
      "securityhub:ASFFSyntaxPath/UserDefinedFields.value": false
     }
    }
   },
   {
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
     "Null": {
      "securityhub:ASFFSyntaxPath/VerificationState": false
     }
    }
```

JSON ポリシードキュメントの最新バージョンを確認するには、「AWS マネージドポリシーリファレンスガイド」の「AWSSystemsManagerOpsDataSyncServiceRolePolicy」を参照してください。

AWS マネージドポリシー: AmazonSSMManagedEC2InstanceDefaultPolicy

Systems Manager 機能を使用するアクセス許可が必要な Amazon EC2 インスタンスの IAM ロールにのみ AmazonSSMManagedEC2InstanceDefaultPolicy をアタッチする必要があります。このロールは、IAM ユーザーや IAM グループなど、他の IAM エンティティや、他の目的を果たす IAM ロールにはアタッチしないでください。詳細については、「Default Host Management Configuration を使用した EC2 インスタンスの自動管理」を参照してください。

このポリシーは、さまざまなタスクを実行するために、Amazon EC2 インスタンス上の SSM Agent がクラウド内の Systems Manager サービスと通信することを可能にする許可を付与します。また、認可トークンを提供する 2 つのサービスの許可を付与して、オペレーションが正しいインスタンスで実行されることも確実にします。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- ssm – ドキュメントの取得、Run Command を使用したコマンドの実行、Session Manager を使用したセッションの確立、インスタンスのインベントリの収集、および Patch Manager を使用したパッチとパッチコンプライアンスのスキャンを実行することをプリンシパルに許可します。
- ssmmessages – 各インスタンスで、Amazon Message Gateway Service が作成したパーソナライズ済み認可トークンにアクセスすることをプリンシパルに許可します。Systems Manager は、API オペレーションで提供されたインスタンスの Amazon リソースネーム (ARN) に照らしてパーソナライズされた認可トークンを検証します。このアクセスは、SSM Agent が正しいインスタンスで API オペレーションを実行することを確実にするために必要です。
- ec2messages – 各インスタンスで、Amazon Message Delivery Service が作成したパーソナライズ済み認可トークンにアクセスすることをプリンシパルに許可します。Systems Manager は、API オペレーションで提供されたインスタンスの Amazon リソースネーム (ARN) に照らしてパーソナライズされた認可トークンを検証します。このアクセスは、SSM Agent が正しいインスタンスで API オペレーションを実行することを確実にするために必要です。

ssmmessages および ec2messages エンドポイントに関連する情報 (2 つのエンドポイント間の違いなど) については、「エージェント関連の API オペレーション (ssmmessages および ec2messages エンドポイント)」を参照してください。

JSON ポリシードキュメントの最新バージョンなど、ポリシーについてさらに詳しく確認するには、「AWS マネージドポリシーリファレンスガイド」の「AmazonSSMManagedEC2InstanceDefaultPolicy」を参照してください。

AWS マネージドポリシー: SSMQuickSetupRolePolicy

SSMQuickSetupRolePolicy を IAM エンティティにアタッチすることはできません。このポリシーは、ユーザーに代わって Systems Manager がアクションを実行することを許可する、サービスにリンクされたロールにアタッチされます。詳細については、「ロールを使用して Quick Setup によってプロビジョニングされたリソースの正常性と一貫性を維持する」を参照してください。

このポリシーは、Systems Manager が設定の正常性をチェックし、パラメータとプロビジョニングされたリソースが確実に一貫して使用されるようにするとともに、ドリフトが検出された場合にリソースを修復することを許可する読み取り専用許可を付与します。また、サービスリンクロールを作成するための管理アクセス許可も付与します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `ssm` – プリンシパルが委任管理者アカウントなど Systems Manager でリソースデータ同期と SSM ドキュメントの情報を読み取ることを許可します。これは、設定されたリソースについて意図されている状態を Quick Setup が判別するために必要です。
- `organizations` – プリンシパルが、AWS Organizations で設定されている組織に属するメンバーアカウントに関する情報を読み取るのを許可します。これは、Quick Setup がリソースのヘルスチェックを実行する組織内のすべてのアカウントを識別するために必要です。
- `cloudformation` – プリンシパルが AWS CloudFormation から情報を読み取るのを許可します。これは、Quick Setup がリソースの状態と CloudFormation スタックセットオペレーションを管理するために使用される AWS CloudFormation スタックに関するデータを収集するために必要です。

JSON ポリシードキュメントの最新バージョンなど、ポリシーについてさらに詳しく確認するには、「AWS マネージドポリシーリファレンスガイド」の「SSMQuickSetupRolePolicy」を参照してください。

AWS マネージドポリシー: AWSQuickSetupDeploymentRolePolicy

マネージドポリシー `AWSQuickSetupDeploymentRolePolicy` は複数の Quick Setup 設定タイプをサポートします。これらの設定タイプは、推奨されるベストプラクティスを使用して、頻繁に使用される Amazon Web Services のサービスと機能を設定する IAM ロールとオートメーションを作成します。

IAM エンティティに `AWSQuickSetupDeploymentRolePolicy` をアタッチできます。

このポリシーは、次の Quick Setup 設定に関連付けられたリソースを作成するために必要な管理許可を付与します。

- Quick Setup を使用して Amazon EC2 ホスト管理を設定する
- Quick Setup を使用して AWS Config 設定レコーダーを作成する
- Quick Setup を使用して AWS Config 適合パックをデプロイする
- Quick Setup を使用して DevOps Guru をセットアップする
- Quick Setup を使用して Distributor パッケージをデプロイする
- Quick Setup を使用してスケジュールに従って EC2 インスタンスを自動的に停止および起動する

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- iam – プリンシパルがオートメーション設定タスクに必要な IAM ロールを管理および削除し、オートメーションロールポリシーを管理するのを許可します。
- cloudformation — プリンシパルがスタックセットを作成および管理することを許可します。
- config – プリンシパルが適合パックを作成、管理、削除するのを許可します。
- events – プリンシパルがスケジュールされたアクションのイベントルールを作成、更新、削除するのを許可します。
- resource-groups – プリンシパルが、Quick Setup 設定の対象となるリソースグループに関連付けられているリソースクエリを取得するのを許可します。
- ssm – プリンシパルが Quick Setup 設定を適用するオートメーションランブックと関連付けを作成するのを許可します。

JSON ポリシードキュメントの最新バージョンを確認するには、「AWS マネージドポリシーリファレンスガイド」の「AWSQuickSetupDeploymentRolePolicy」を参照してください。

AWS マネージドポリシー: AWSQuickSetupPatchPolicyDeploymentRolePolicy

マネージドポリシー AWSQuickSetupPatchPolicyDeploymentRolePolicy は Quick Setup パッチポリシーを使用して組織内のインスタンスのためにパッチ適用を設定する Quick Setup タイプをサポートします。この設定タイプは、単一のアカウント内または組織全体でアプリケーションとノードのパッチ適用を自動化するのに役立ちます。

AWSQuickSetupPatchPolicyDeploymentRolePolicy を IAM エンティティにアタッチできます。Systems Manager はまた、Systems Manager がユーザーに代わりアクションを実行することを可能にするサービスロールをこのポリシーにアタッチします。

このポリシーは、Quick Setup がパッチポリシー設定に関連付けられたリソースを作成することを許可する管理許可を付与します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- iam – プリンシパルがオートメーション設定タスクに必要な IAM ロールを管理および削除し、オートメーションロールポリシーを管理するのを許可します。
- cloudformation – プリンシパルが AWS CloudFormation スタック情報を読み取り、AWS CloudFormation スタックセットを使用して Quick Setup によって作成された AWS CloudFormation スタックを制御するのを許可します。

- ssm – プリンシパルが設定タスクに必要なオートメーションランブックを作成、更新、読み取り、削除し、State Manager 関連付けを作成、更新、削除するのを許可します。

- resource-groups – プリンシパルが、Quick Setup 設定の対象となるリソースグループに関連付けられているリソースクエリを取得するのを許可します。

- s3 – プリンシパルが Amazon S3 バケットを一覧表示し、パッチポリシーアクセスログを保存するためのバケットを管理するのを許可します。
- lambda – プリンシパルが設定を正しい状態に維持する AWS Lambda 修復機能を管理するのを許可します。
- logs – プリンシパルが Lambda 設定リソースのロググループを記述および管理するのを許可します。

JSON ポリシードキュメントの最新バージョンを確認するには、「AWS マネージドポリシーリファレンスガイド」の「AWSQuickSetupPatchPolicyDeploymentRolePolicy」を参照してください。

AWS マネージドポリシー: AWSQuickSetupPatchPolicyBaselineAccess

マネージドポリシー AWSQuickSetupPatchPolicyBaselineAccess は Quick Setup パッチポリシーを使用して組織内のインスタンスのためにパッチ適用を設定する Quick Setup タイプをサポートします。この設定タイプは、単一のアカウント内または組織全体でアプリケーションとノードのパッチ適用を自動化するのに役立ちます。

AWSQuickSetupPatchPolicyBaselineAccess を IAM エンティティにアタッチできます。Systems Manager はまた、Systems Manager がユーザーに代わりアクションを実行することを可能にするサービスロールをこのポリシーにアタッチします。

このポリシーは、現在の AWS アカウント または組織内の管理者が Quick Setup を使用して設定したパッチベースラインにアクセスするための読み取り専用許可を付与します。パッチベースラインは Amazon S3 バケットに保存され、単一のアカウントまたは組織全体のインスタンスへのパッチ適用に使用できます。

アクセス許可の詳細

このポリシーには、次の許可が含まれています。

- s3 – プリンシパルが Amazon S3 バケットに保存されているパッチベースラインオーバーライドを読み取るのを許可します。

JSON ポリシードキュメントの最新バージョンを確認するには、「AWS マネージドポリシーリファレンスガイド」の「AWSQuickSetupPatchPolicyBaselineAccess」を参照してください。

AWS マネージドポリシー: AWSSystemsManagerEnableExplorerExecutionPolicy

マネージドポリシー AWSSystemsManagerEnableExplorerExecutionPolicy は AWS Systems Manager のツールである Explorer の有効化をサポートします。

AWSSystemsManagerEnableExplorerExecutionPolicy を IAM エンティティにアタッチできます。Systems Manager はまた、Systems Manager がユーザーに代わりアクションを実行することを可能にするサービスロールをこのポリシーにアタッチします。

このポリシーは、Explorer を有効にするための管理許可を付与します。これには、関連する Systems Manager サービス設定を更新し、Systems Manager のためにサービスにリンクされたロールを作成する許可が含まれます。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- config – 設定レコーダーの詳細への読み取り専用アクセスを提供することで、プリンシパルが Explorer の有効化をサポートするのを許可します。
- iam – プリンシパルが Explorer の有効化をサポートするのを許可します。
- ssm – プリンシパルが Explorer を有効にするオートメーションワークフローを開始するのを許可します。

JSON ポリシードキュメントの最新バージョンを確認するには、「AWS マネージドポリシーリファレンスガイド」の「AWSSystemsManagerEnableExplorerExecutionPolicy」を参照してください。

AWS マネージドポリシー: AWSSystemsManagerEnableConfigRecordingExecutionPolicy

マネージドポリシー AWSSystemsManagerEnableConfigRecordingExecutionPolicy は Quick Setup を使用して AWS Config 設定レコーダーを作成する Quick Setup 設定タイプをサポートします。この設定タイプを使用すると、AWS Config のために選択した AWS リソースタイプに対する変更を追跡および記録するよう Quick Setup を有効にできます。また、記録されたデータの配信および通知オプションを設定するよう Quick Setup を有効にすることもできます。

AWSSystemsManagerEnableConfigRecordingExecutionPolicy を IAM エンティティにアタッチできます。Systems Manager はまた、Systems Manager がユーザーに代わりアクションを実行することを可能にするサービスロールをこのポリシーにアタッチします。

このポリシーは、Quick Setup が AWS Config 設定記録を有効にして設定することを許可する管理許可を付与します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- s3 – プリンシパルが設定記録の配信用に Amazon S3 バケットを作成および設定するのを許可します。
- sns – プリンシパルが Amazon SNS トピックを一覧表示および作成するのを許可します。
- config – プリンシパルが設定レコーダーを設定して起動し、Explorer の有効化をサポートするのを許可します。
- iam – プリンシパルが AWS Config のためにサービスにリンクされたロールを作成、取得、渡して、Systems Manager のためにサービスにリンクされたロールを作成し、Explorer の有効化をサポートするのを許可します。
- ssm – プリンシパルが Explorer を有効にするオートメーションワークフローを開始するのを許可します。
- compute-optimizer – リソースが AWS Compute Optimizer に登録されているかどうかを判断するための読み取り専用アクセスを提供することで、プリンシパルが Explorer の有効化をサポートするのを許可します。
- support – リソースが AWS Compute Optimizer に登録されているかどうかを判断するための読み取り専用アクセスを提供することで、プリンシパルが Explorer の有効化をサポートするのを許可します。

JSON ポリシードキュメントの最新バージョンを確認するには、「AWS マネージドポリシーリファレンスガイド」の「AWSSystemsManagerEnableConfigRecordingExecutionPolicy」を参照してください。

AWS マネージドポリシー: AWSQuickSetupDevOpsGuruPermissionsBoundary

> **Note**
>
> このポリシーはアクセス許可の境界です。アクセス許可の境界は、アイデンティティベースのポリシーで IAM エンティティに付与することのできる許可の上限を設定します。Quick Setup アクセス許可の境界ポリシーを独自に使用したり、アタッチしたりしないでください。Quick Setup アクセス許可の境界ポリシーは、Quick Setup マネージドロールにのみアタッチする必要があります。アクセス許可の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可の境界」を参照してください。

マネージドポリシー `AWSQuickSetupDevOpsGuruPermissionsBoundary` は Quick Setup を使用して DevOps Guru をセットアップする タイプをサポートします。この設定タイプにより、機械学習を活用した Amazon DevOps Guru が有効になります。DevOps Guru サービスは、アプリケーションの運用パフォーマンスと可用性の向上に役立ちます。

Quick Setup を使用して `AWSQuickSetupDevOpsGuruPermissionsBoundary` 設定を作成すると、システムはこのアクセス許可の境界を、設定のデプロイ時に作成される IAM ロールに適用します。アクセス許可の境界により、Quick Setup が作成するロールの範囲が制限されます。

このポリシーは、Quick Setup が Amazon DevOps Guru を有効にして設定するのを許可する管理許可を付与します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `iam` – プリンシパルが DevOps Guru および Systems Manager のためにサービスにリンクされたロールを作成し、Explorer を有効にするのに役立つロールを一覧表示するのを許可します。
- `cloudformation` — プリンシパルが AWS CloudFormation スタックを一覧表示および記述することを許可します。
- `sns` – プリンシパルが Amazon SNS トピックを一覧表示および作成するのを許可します。
- `devops-guru` – プリンシパルが DevOps Guru を設定し、通知チャネルを追加するのを許可します。
- `config` – – 設定レコーダーの詳細への読み取り専用アクセスを提供することで、プリンシパルが Explorer の有効化をサポートするのを許可します。

- ssm – プリンシパルが Explorer を有効にするオートメーションワークフローを開始すること、および Explorer サービス設定を読み取ったり、更新したりすることを許可します。
- compute-optimizer – リソースが AWS Compute Optimizer に登録されているかどうかを判断するための読み取り専用アクセスを提供することで、プリンシパルが Explorer の有効化をサポートするのを許可します。
- support – リソースが AWS Compute Optimizer に登録されているかどうかを判断するための読み取り専用アクセスを提供することで、プリンシパルが Explorer の有効化をサポートするのを許可します。

JSON ポリシードキュメントの最新バージョンを確認するには、「AWS マネージドポリシーリファレンスガイド」の「AWSQuickSetupDevOpsGuruPermissionsBoundary」を参照してください。

AWS マネージドポリシー: AWSQuickSetupDistributorPermissionsBoundary

> **Note**
>
> このポリシーはアクセス許可の境界です。アクセス許可の境界は、アイデンティティベースのポリシーで IAM エンティティに付与することのできる許可の上限を設定します。Quick Setup アクセス許可の境界ポリシーを独自に使用したり、アタッチしたりしないでください。Quick Setup アクセス許可の境界ポリシーは、Quick Setup マネージドロールにのみアタッチする必要があります。アクセス許可の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可の境界」を参照してください。

マネージドポリシー AWSQuickSetupDistributorPermissionsBoundary は Quick Setup を使用して Distributor パッケージをデプロイする Quick Setup 設定タイプをサポートします。この設定タイプは、AWS Systems Manager のツールである Distributor を使用して、エージェントなどのソフトウェアパッケージの Amazon Elastic Compute Cloud (Amazon EC2) インスタンスへの配布の有効化をサポートします。

Quick Setup を使用して AWSQuickSetupDistributorPermissionsBoundary 設定を作成すると、システムはこのアクセス許可の境界を、設定のデプロイ時に作成される IAM ロールに適用します。アクセス許可の境界により、Quick Setup が作成するロールの範囲が制限されます。

このポリシーは、ディストリビューターを使用した、エージェントなどのソフトウェアパッケージの Amazon EC2 インスタンスへの配布を Quick Setup が有効にすることを許可する管理許可を付与します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- iam – プリンシパルがディストリビューターオートメーションロールを取得して渡すこと、デフォルトのインスタンスロールを作成、読み取り、更新、削除すること、デフォルトのインスタンスロールを Amazon EC2 および Systems Manager に渡すこと、インスタンスマネージドポリシーをインスタンスロールにアタッチすること、Systems Manager のためにサービスにリンクされたロールを作成すること、デフォルトのインスタンスロールをインスタンスプロファイルに追加すること、IAM ロールとインスタンスプロファイルに関する情報を読み取ること、およびデフォルトのインスタンスプロファイルを作成することを許可します。
- ec2 – プリンシパルがデフォルトのインスタンスプロファイルを EC2 インスタンスに関連付け、Explorer の有効化をサポートするのを許可します。
- ssm – プリンシパルがインスタンスを設定してパッケージをインストールするオートメーションワークフローを開始すること、Explorer を有効にするオートメーションワークフローの開始をサポートすること、Explorer サービス設定を読み取ったり、更新したりすることを許可します。
- config – 設定レコーダーの詳細への読み取り専用アクセスを提供することで、プリンシパルが Explorer の有効化をサポートするのを許可します。
- compute-optimizer – リソースが AWS Compute Optimizer に登録されているかどうかを判断するための読み取り専用アクセスを提供することで、プリンシパルが Explorer の有効化をサポートするのを許可します。
- support – リソースが AWS Compute Optimizer に登録されているかどうかを判断するための読み取り専用アクセスを提供することで、プリンシパルが Explorer の有効化をサポートするのを許可します。

JSON ポリシードキュメントの最新バージョンを確認するには、「AWS マネージドポリシーリファレンスガイド」の「AWSQuickSetupDistributorPermissionsBoundary」を参照してください。

AWS マネージドポリシー: AWSQuickSetupSSMHostMgmtPermissionsBoundary

> **Note**
>
> このポリシーはアクセス許可の境界です。アクセス許可の境界は、アイデンティティベースのポリシーで IAM エンティティに付与することのできる許可の上限を設定します。Quick Setup アクセス許可の境界ポリシーを独自に使用したり、アタッチしたりしないでください。Quick Setup アクセス許可の境界ポリシーは、Quick Setup マネージドロールにのみア

タッチする必要があります。アクセス許可の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可の境界」を参照してください。

マネージドポリシー AWSQuickSetupSSMHostMgmtPermissionsBoundary は Quick Setup を使用して Amazon EC2 ホスト管理を設定する Quick Setup 設定タイプをサポートします。この設定タイプは、IAM ロールを設定し、一般的に使用される Systems Manager のツールを有効にして、Amazon EC2 インスタンスを安全に管理します。

Quick Setup を使用して AWSQuickSetupSSMHostMgmtPermissionsBoundary 設定を作成すると、システムはこのアクセス許可の境界を、設定のデプロイ時に作成される IAM ロールに適用します。アクセス許可の境界により、Quick Setup が作成するロールの範囲が制限されます。

このポリシーは、Quick Setup が EC2 インスタンスを安全に管理するために必要な Systems Manager のツールを有効にして設定することを許可する管理許可を付与します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- iam – プリンシパルがサービスロールを取得してオートメーションに渡すのを許可します。プリンシパルがデフォルトのインスタンスロールを作成、読み取り、更新、削除すること、デフォルトのインスタンスロールを Amazon EC2 および Systems Manager に渡すこと、インスタンスマネージドポリシーをインスタンスロールにアタッチすること、Systems Manager のためにサービスにリンクされたロールを作成すること、デフォルトのインスタンスロールをインスタンスプロファイルに追加すること、IAM ロールとインスタンスプロファイルに関する情報を読み取ること、およびデフォルトのインスタンスプロファイルを作成することを許可します。
- ec2 – プリンシパルがデフォルトのインスタンスプロファイルを EC2 インスタンスに関連付けたり、関連付けを解除したりするのを許可します
- ssm – プリンシパルが Explorer を有効にするオートメーションワークフローを開始すること、Explorer サービス設定を読み取ったり、更新したりすること、インスタンスを設定すること、インスタンスで Systems Manager のツールを有効にすることを許可します。
- compute-optimizer – リソースが AWS Compute Optimizer に登録されているかどうかを判断するための読み取り専用アクセスを提供することで、プリンシパルが Explorer の有効化をサポートするのを許可します。
- support – リソースが AWS Compute Optimizer に登録されているかどうかを判断するための読み取り専用アクセスを提供することで、プリンシパルが Explorer の有効化をサポートするのを許可します。

JSON ポリシードキュメントの最新バージョンを確認するには、「AWS マネージドポリシーリファレンスガイド」の「AWSQuickSetupSSMHostMgmtPermissionsBoundary」を参照してください。

AWS マネージドポリシー: AWSQuickSetupPatchPolicyPermissionsBoundary

> **Note**
>
> このポリシーはアクセス許可の境界です。アクセス許可の境界は、アイデンティティベースのポリシーで IAM エンティティに付与することのできる許可の上限を設定します。Quick Setup アクセス許可の境界ポリシーを独自に使用したり、アタッチしたりしないでください。Quick Setup アクセス許可の境界ポリシーは、Quick Setup マネージドロールにのみアタッチする必要があります。アクセス許可の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可の境界」を参照してください。

マネージドポリシー `AWSQuickSetupPatchPolicyPermissionsBoundary` は Quick Setup パッチポリシーを使用して組織内のインスタンスのためにパッチ適用を設定する Quick Setup タイプをサポートします。この設定タイプは、単一のアカウント内または組織全体でアプリケーションとノードのパッチ適用を自動化するのに役立ちます。

Quick Setup を使用して `AWSQuickSetupPatchPolicyPermissionsBoundary` 設定を作成すると、システムはこのアクセス許可の境界を、設定のデプロイ時に作成される IAM ロールに適用します。アクセス許可の境界により、Quick Setup が作成するロールの範囲が制限されます。

このポリシーは、Quick Setup が AWS Systems Manager のツールである Patch Manager でパッチポリシーを有効にして設定することを許可する管理許可を付与します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `iam` – プリンシパルが Patch Manager オートメーションロールを取得すること、オートメーションロールを Patch Manager パッチ適用オペレーションに渡すこと、デフォルトのインスタンスロール `AmazonSSMRoleForInstancesQuickSetup` を作成すること、デフォルトのインスタンスロールを Amazon EC2 および Systems Manager に渡すこと、選択した AWS マネージドポリシーをインスタンスロールにアタッチすること、Systems Manager のためにサービスにリンクされたロールを作成すること、デフォルトのインスタンスロールをインスタンスプロファイルに追加すること、インスタンスプロファイルとロールに関する情報を読み取ること、デフォルトのインスタンスプロファイルを作成すること、パッチベースラインオーバーライドを読み取るための許可を持つロールにタグ付けすることを許可します。

- ssm – プリンシパルが Systems Manager によって管理されるインスタンスロールを更新すること、Quick Setup で作成された Patch Manager パッチポリシーによって作成された関連付けを管理すること、パッチポリシー設定の対象となるインスタンスにタグ付けすること、インスタンスとパッチ適用ステータスに関する情報を読み取ること、インスタンスパッチを設定、有効化、修復するオートメーションワークフローを開始すること、Explorer を有効にするオートメーションワークフローを開始すること、Explorer の有効化をサポートすること、Explorer サービス設定を読み取ったり、更新したりすることを許可します。
- ec2 – プリンシパルが、デフォルトのインスタンスプロファイルの EC2 インスタンスへの関連付けおよび関連付け解除、パッチポリシー設定の対象となるインスタンスへのタグ付け、Explorer の有効化のサポートを実行するのを許可します。
- s3 – プリンシパルがパッチベースラインオーバーライドを保存するために S3 バケットを作成および設定するのを許可します。
- lambda – プリンシパルがパッチ適用を設定する AWS Lambda 関数を呼び出し、Quick Setup パッチポリシー設定が削除された後にクリーンアップオペレーションを実行するのを許可します。
- logs – プリンシパルが Patch Manager Quick Setup AWS Lambda 関数についてのログ記録を設定するのを許可します。
- config – 設定レコーダーの詳細への読み取り専用アクセスを提供することで、プリンシパルが Explorer の有効化をサポートするのを許可します。
- compute-optimizer – リソースが AWS Compute Optimizer に登録されているかどうかを判断するための読み取り専用アクセスを提供することで、プリンシパルが Explorer の有効化をサポートするのを許可します。
- support – リソースが AWS Compute Optimizer に登録されているかどうかを判断するための読み取り専用アクセスを提供することで、プリンシパルが Explorer の有効化をサポートするのを許可します。

JSON ポリシードキュメントの最新バージョンを確認するには、「AWS マネージドポリシーリファレンスガイド」の「AWSQuickSetupPatchPolicyPermissionsBoundary」を参照してください。

AWS マネージドポリシー: AWSQuickSetupSchedulerPermissionsBoundary

> **Note**
>
> このポリシーはアクセス許可の境界です。アクセス許可の境界は、アイデンティティベースのポリシーで IAM エンティティに付与することのできる許可の上限を設定します。Quick Setup アクセス許可の境界ポリシーを独自に使用したり、アタッチしたりしないでくださ

い。Quick Setup アクセス許可の境界ポリシーは、Quick Setup マネージドロールにのみアタッチする必要があります。アクセス許可の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可の境界」を参照してください。

マネージドポリシー AWSQuickSetupSchedulerPermissionsBoundary は Quick Setup を使用してスケジュールに従って EC2 インスタンスを自動的に停止および起動する Quick Setup 設定タイプをサポートします。この設定タイプを使用すると、指定した時刻に EC2 インスタンスや他のリソースを停止および起動できます。

Quick Setup を使用して AWSQuickSetupSchedulerPermissionsBoundary 設定を作成すると、システムはこのアクセス許可の境界を、設定のデプロイ時に作成される IAM ロールに適用します。アクセス許可の境界により、Quick Setup が作成するロールの範囲が制限されます。

このポリシーは、Quick Setup が EC2 インスタンスや他のリソースでスケジュールされたオペレーションを有効にして設定することを許可する管理許可を付与します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- iam – プリンシパルがインスタンス管理オートメーションアクション用のロールを取得して渡すこと、EC2 インスタンス管理用のデフォルトのインスタンスロールを管理およびアタッチしたり、渡したりすること、デフォルトのインスタンスプロファイルを作成すること、インスタンスプロファイルにデフォルトのインスタンスロールを追加すること、Systems Manager のためにサービスにリンクされたロールを作成すること、IAM ロールとインスタンスプロファイルに関する情報を読み取ること、デフォルトのインスタンスプロファイルを EC2 インスタンスに関連付けること、ならびにオートメーションワークフローを開始してインスタンスを設定し、それらで Systems Manager ツールを有効にすることを許可します。
- ssm – プリンシパルが Explorer を有効にするオートメーションワークフローを開始し、Explorer サービス設定を読み取ったり、更新したりするのを許可します。
- ec2 – プリンシパルがターゲットインスタンスを見つけて、スケジュールに従ってそれらのインスタンスを起動および停止するのを許可します。
- config – 設定レコーダーの詳細への読み取り専用アクセスを提供することで、プリンシパルが Explorer の有効化をサポートするのを許可します。
- compute-optimizer – リソースが AWS Compute Optimizer に登録されているかどうかを判断するための読み取り専用アクセスを提供することで、プリンシパルが Explorer の有効化をサポートするのを許可します。

- support – プリンシパルがアカウントの AWS Trusted Advisor チェックへの読み取り専用アクセスを提供することで、Explorer の有効化をサポートするのを許可します。

JSON ポリシードキュメントの最新バージョンを確認するには、「AWS マネージドポリシーリファレンスガイド」の「AWSQuickSetupSchedulerPermissionsBoundary」を参照してください。

AWS マネージドポリシー: AWSQuickSetupCFGCPacksPermissionsBoundary

> **Note**
>
> このポリシーはアクセス許可の境界です。アクセス許可の境界は、アイデンティティベースのポリシーで IAM エンティティに付与することのできる許可の上限を設定します。Quick Setup アクセス許可の境界ポリシーを独自に使用したり、アタッチしたりしないでください。Quick Setup アクセス許可の境界ポリシーは、Quick Setup マネージドロールにのみアタッチする必要があります。アクセス許可の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可の境界」を参照してください。

マネージドポリシー AWSQuickSetupCFGCPacksPermissionsBoundary は Quick Setup を使用して AWS Config 適合パックをデプロイする Quick Setup 設定タイプをサポートします。この設定タイプは、AWS Config 適合パックをデプロイします。適合パックは、単一のエンティティとしてデプロイできる AWS Config ルールと修復アクションをまとめたものです。

Quick Setup を使用して AWSQuickSetupCFGCPacksPermissionsBoundary 設定を作成すると、システムはこのアクセス許可の境界を、設定のデプロイ時に作成される IAM ロールに適用します。アクセス許可の境界により、Quick Setup が作成するロールの範囲が制限されます。

このポリシーは、Quick Setup が AWS Config 適合パックをデプロイすることを許可する管理許可を付与します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- iam – プリンシパルが AWS Config のためにサービスにリンクされたロールを作成、取得、渡すのを許可します。
- sns – プリンシパルが Amazon SNS でプラットフォームアプリケーションを一覧表示するのを許可します。

- config – プリンシパルが AWS Config 適合パックをデプロイすること、適合パックのステータスを取得すること、設定レコーダーに関する情報を取得することを許可します。
- ssm – プリンシパルが SSM ドキュメントとオートメーションワークフローに関する情報を取得すること、リソースタグに関する情報を取得すること、サービス設定に関する情報を取得し、サービス設定を更新することを許可します。
- compute-optimizer – プリンシパルがアカウントのオプトインステータスを取得するのを許可します。
- support – プリンシパルが AWS Trusted Advisor チェックに関する情報を取得するのを許可します。

JSON ポリシードキュメントの最新バージョンを確認するには、「AWS マネージドポリシーリファレンスガイド」の「AWSQuickSetupCFGCPacksPermissionsBoundary」を参照してください。

AWS マネージドポリシー: AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy

ポリシー AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy では、ノードが管理されているアカウントとリージョンで Automation ワークフローを開始することで、Systems Manager サービスとやり取りするノードの問題を診断するためのアクセス許可を付与できます。

AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy を IAM エンティティにアタッチできます。Systems Manager はまた、Systems Manager がユーザーに代わって診断アクションを実行することを許可するサービスロールをこのポリシーにアタッチします。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- ssm – プリンシパルがノードの問題を診断する Automation ランブックを実行し、ワークフローの実行ステータスにアクセスすることを許可します。
- kms – プリンシパルが S3 バケット内のオブジェクトの暗号化に使用されるお客様指定の AWS Key Management Service キーを使用して、バケット内のオブジェクトのコンテンツを復号化してアクセスすることを許可します。
- sts – プリンシパルが診断実行ロールを引き受けて同じアカウントで Automation ランブックを実行することを許可します。
- iam – プリンシパルが診断管理ロール (例えば、self) を Systems Manager に渡して Automation ランブックを実行することを許可します。

- s3 – プリンシパルがオブジェクトにアクセスして S3 バケットに書き込むことを許可します。

JSON ポリシードキュメントの最新バージョンを確認するには、「AWS マネージドポリシーリファレンスガイド」の「AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy」を参照してください。

AWS マネージドポリシー: AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy

マネージドポリシー AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy では、ターゲットの AWS アカウントとリージョンで Automation ランブックを実行して、Systems Manager サービスとやり取りするマネージドノードの問題を診断するための管理アクセス許可を付与できます。

AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy を IAM エンティティにアタッチできます。Systems Manager はまた、Systems Manager がユーザーに代わりアクションを実行することを可能にするサービスロールをこのポリシーにアタッチします。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- ssm – プリンシパルが診断固有の Automation ランブックを実行し、Automation ワークフローのステータスと実行メタデータにアクセスすることを許可します。
- ec2 – プリンシパルが Amazon EC2 および Amazon VPC のリソースとその設定を記述して、Systems Manager サービスに関する問題を診断することを許可します。
- kms – プリンシパルが S3 バケット内のオブジェクトの暗号化に使用されるお客様指定の AWS Key Management Service キーを使用して、バケット内のオブジェクトのコンテンツを復号化してアクセスすることを許可します。
- iam – プリンシパルが診断実行ロール (例えば、self) を Systems Manager に渡して Automation ドキュメントを実行することを許可します。

JSON ポリシードキュメントの最新バージョンを確認するには、「AWS マネージドポリシーリファレンスガイド」の「AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy」を参照してください。

AWS マネージドポリシー: AWS-SSM-RemediationAutomation-AdministrationRolePolicy

マネージドポリシー AWS-SSM-RemediationAutomation-AdministrationRolePolicy では、ノードを管理しているアカウントとリージョンで Automation ワークフローを開始することによ

り、Systems Manager サービスとやり取りするマネージドノードの問題を修復するためのアクセス許可を付与できます。

このポリシーを IAM エンティティにアタッチできます。Systems Manager は、Systems Manager がユーザーに代わって修復アクションを実行することを許可するサービスロールにも、このポリシーをアタッチします。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `ssm` – プリンシパルが特定の Automation ランブックを実行し、Automation ワークフローのステータスと実行ステータスにアクセスすることを許可します。
- `kms` – プリンシパルが S3 バケット内のオブジェクトの暗号化に使用されるお客様指定の AWS Key Management Service キーを使用して、バケット内のオブジェクトのコンテンツを復号化してアクセスすることを許可します。
- `sts` – プリンシパルが修復実行ロールを引き受けて同じアカウントで SSM Automation ドキュメントを実行することを許可します。
- `iam` – プリンシパルが修復管理者ロール (例えば、self) を Systems Manager に渡して Automation ドキュメントを実行することを許可します。
- `s3` – プリンシパルがオブジェクトにアクセスして S3 バケットに書き込むことを許可します。

JSON ポリシードキュメントの最新バージョンを確認するには、「AWS マネージドポリシーリファレンスガイド」の「AWS-SSM-RemediationAutomation-AdministrationRolePolicy」を参照してください。

AWS マネージドポリシー: AWS-SSM-RemediationAutomation-ExecutionRolePolicy

マネージドポリシー `AWS-SSM-RemediationAutomation-ExecutionRolePolicy` では、特定のターゲットアカウントとリージョンで Automation ランブックを実行して、Systems Manager サービスとやり取りするマネージドノードの問題を修復するためのアクセス許可を付与できます。

このポリシーを IAM エンティティにアタッチできます。Systems Manager は、Systems Manager がユーザーに代わって修復アクションを実行することを許可するサービスロールにも、このポリシーをアタッチします。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- ssm – プリンシパルが特定の Automation ランブックを実行し、実行メタデータと実行ステータスにアクセスすることを許可します。
- ec2 – プリンシパルが Systems Manager サービスとその関連するリソース (セキュリティグループなど) の問題を修復するために Amazon EC2 リソースおよび Amazon VPC リソースとその設定を作成、アクセス、変更し、リソースにタグをアタッチすることを許可します。
- kms – プリンシパルが S3 バケット内のオブジェクトの暗号化に使用されるお客様指定の AWS Key Management Service キーを使用して、バケット内のオブジェクトのコンテンツを復号化してアクセスすることを許可します。
- iam – プリンシパルが修復実行ロール (例えば、self) を SSM サービスに渡して Automation ドキュメントを実行することを許可します。

JSON ポリシードキュメントの最新バージョンを確認するには、「AWS マネージドポリシーリファレンスガイド」の「AWS-SSM-RemediationAutomation-ExecutionRolePolicy」を参照してください。

AWS マネージドポリシー: AWSQuickSetupSSMManageResourcesExecutionPolicy

このポリシーは、Quick Setup が AWSQuickSetupType-SSM-SetupResources Automation ランブックを実行することを許可するアクセス許可を付与します。このランブックは Quick Setup 関連付けの IAM ロールを作成し、関連付けは AWSQuickSetupType-SSM のデプロイによって作成されます。また、Quick Setup 削除オペレーション時に関連する Amazon S3 バケットをクリーンアップするためのアクセス許可も付与します。

このポリシーを IAM エンティティにアタッチできます。Systems Manager はまた、Systems Manager がユーザーに代わってアクションを実行することを許可するサービスロールをこのポリシーにアタッチします。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- iam – プリンシパルが Quick Setup Systems Manager Explorer オペレーションで使用する IAM ロールをリストおよび管理すること、Quick Setup および Systems Manager Explorer で使用する IAM ポリシーを表示、アタッチ、デタッチすることを許可します。これらのアクセス許可は、Quick Setup で一部の設定オペレーションに必要なロールを作成するために必要です。
- s3 – プリンシパルがプリンシパルアカウントの Amazon S3 バケットにあるオブジェクトのうち、特に Quick Setup 設定オペレーションに使用されるオブジェクトの情報を取得すること、そのオブ

ジェクトを Amazon S3 バケットから削除することを許可します。これは、設定後に不要になった S3 オブジェクトを削除するために必要です。

JSON ポリシードキュメントの最新バージョンを確認するには、「AWS マネージドポリシーリファレンスガイド」の「AWSQuickSetupSSMManageResourcesExecutionPolicy」を参照してください。

AWS マネージドポリシー: AWSQuickSetupSSMLifecycleManagementExecutionPolicy

`AWSQuickSetupSSMLifecycleManagementExecutionPolicy` ポリシーは、Systems Manager に Quick Setup をデプロイする際にライフサイクルイベントに対して AWS CloudFormation カスタムリソースを実行することを Quick Setup に許可する管理アクセス許可を付与します。

このポリシーを IAM エンティティにアタッチできます。Systems Manager は、Systems Manager がユーザーに代わってアクションを実行することを許可するサービスロールにも、このポリシーをアタッチします。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `ssm` – プリンシパルがオートメーションの実行に関する情報を取得し、特定の Quick Setup オペレーションをセットアップするためのオートメーションの実行を開始することを許可します。
- `iam` – プリンシパルが特定の Quick Setup リソースをセットアップするためのロールを IAM から渡すことを許可します。

JSON ポリシードキュメントの最新バージョンを確認するには、「AWS マネージドポリシーリファレンスガイド」の「AWSQuickSetupSSMLifecycleManagementExecutionPolicy」を参照してください。

AWS マネージドポリシー: AWSQuickSetupSSMDeploymentRolePolicy

マネージドポリシー `AWSQuickSetupSSMDeploymentRolePolicy` は、Systems Manager のオンボーディングプロセス時に使用されるリソースの作成を Quick Setup に許可する管理アクセス許可を付与します。

このポリシーを IAM エンティティに手動でアタッチすることもできますがお勧めしません。Quick Setup は、ユーザーに代わってアクションを実行することを Systems Manager に許可するサービスロールにこのポリシーをアタッチするエンティティを作成します。

このポリシーは、SSMQuickSetupRolePolicy ポリシーとは関係ありません。これは、AWSServiceRoleForSSMQuickSetup サービスリンクロールにアクセス許可を付与するために使用するポリシーです。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- ssm – プリンシパルが AWS CloudFormation テンプレートと特定の SSM ドキュメントセットを使用して作成された特定のリソースの関連付けを管理すること、AWS CloudFormation テンプレートを使用してマネージドノードを診断して修復するためのロールとロールポリシーを管理すること、Quick Setup ライフサイクルイベントのポリシーをアタッチおよび削除することを許可します。
- iam – プリンシパルが Systems Manager サービスと Lambda サービスのロールにタグ付けすることとロールのアクセス許可を渡すこと、診断オペレーションのロールのアクセス許可を渡すことを許可します。
- lambda – プリンシパルが AWS CloudFormation テンプレートを使用してプリンシパルアカウントの Quick Setup ライフサイクルの関数をタグ付けおよび管理することを許可します。
- cloudformation – プリンシパルが AWS CloudFormation から情報を読み取るのを許可します。これは、Quick Setup がリソースの状態と CloudFormation スタックセットオペレーションを管理するために使用される AWS CloudFormation スタックに関するデータを収集するために必要です。

JSON ポリシードキュメントの最新バージョンを確認するには、「AWS マネージドポリシーリファレンスガイド」の「AWSQuickSetupSSMDeploymentRolePolicy」を参照してください。

AWS マネージドポリシー: AWSQuickSetupSSMDeploymentS3BucketRolePolicy

AWSQuickSetupSSMDeploymentS3BucketRolePolicy ポリシーは、アカウント内のすべての S3 バケットをリストするためのアクセス許可と、プリンシパルアカウントで AWS CloudFormation テンプレートを使用して管理される特定のバケットに関する情報を管理および取得するためのアクセス許可を付与します。

AWSQuickSetupSSMDeploymentS3BucketRolePolicy を IAM エンティティにアタッチできます。Systems Manager はまた、Systems Manager がユーザーに代わりアクションを実行することを可能にするサービスロールをこのポリシーにアタッチします。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- s3 – プリンシパルがアカウント内のすべての S3 バケットをリストすること、プリンシパルアカウントで AWS CloudFormation テンプレートを使用して管理される特定のバケットに関する情報を管理および取得することを許可します。

JSON ポリシードキュメントの最新バージョンを確認するには、「AWS マネージドポリシーリファレンスガイド」の「AWSQuickSetupSSMDeploymentS3BucketRolePolicy」を参照してください。

AWS マネージドポリシー: AWSQuickSetupEnableDHMCExecutionPolicy

このポリシーは、プリンシパルが AWSQuickSetupType-EnableDHMC Automation ランブックを実行してデフォルトのホスト管理設定を有効にすることを許可する管理アクセス許可を付与します。デフォルトのホスト管理設定では、Systems Manager が Amazon EC2 インスタンスをマネージドインスタンスとして自動的に管理できます。マネージドインスタンスとは、Systems Manager で使用するために設定された EC2 インスタンスです。このポリシーは、Systems Manager サービス設定に SSM Agent のデフォルトのロールとして指定されている IAM ロールを作成するためのアクセス許可も付与します。

AWSQuickSetupEnableDHMCExecutionPolicy を IAM エンティティにアタッチできます。Systems Manager はまた、Systems Manager がユーザーに代わりアクションを実行することを可能にするサービスロールをこのポリシーにアタッチします。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- ssm – プリンシパルが Systems Manager サービス設定に関する情報を更新および取得することを許可します。
- iam – プリンシパルが Quick Setup オペレーションの IAM ロールに関する情報を作成および取得することを許可します。

JSON ポリシードキュメントの最新バージョンなど、ポリシーについてさらに詳しく確認するには、「AWS マネージドポリシーリファレンスガイド」の「AWSQuickSetupEnableDHMCExecutionPolicy」を参照してください。

AWS マネージドポリシー: AWSQuickSetupEnableAREXExecutionPolicy

このポリシーは、AWSQuickSetupType-EnableAREX Automation ランブックを実行して Systems Manager で AWS Resource Explorer を使用できるようにすることを Systems Manager に許可する管理アクセス許可を付与します。Resource Explorer を使用すると、インターネット検索エンジンと似た検索エクスペリエンスでアカウントのリソースを表示できます。このポリシーは、Resource Explorer のインデックスとビューを管理するためのアクセス許可も付与します。

AWSQuickSetupEnableAREXExecutionPolicy を IAM エンティティにアタッチできます。Systems Manager はまた、Systems Manager がユーザーに代わりアクションを実行することを可能にするサービスロールをこのポリシーにアタッチします。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- iam – プリンシパルが AWS Identity and Access Management (IAM) サービスにサービスリンクロールを作成することを許可します。
- resource-explorer-2 – プリンシパルが Resource Explorer のビューとインデックスに関する情報を取得すること、Resource Explorer のビューとインデックスを作成すること、Quick Setup に表示されているインデックスのインデックスタイプを変更することを許可します。

JSON ポリシードキュメントの最新バージョンなど、ポリシーについてさらに詳しく確認するには、「AWS マネージドポリシーリファレンスガイド」の「AWSQuickSetupEnableAREXExecutionPolicy」を参照してください。

AWS マネージドポリシー: AWSQuickSetupManagedInstanceProfileExecutionPolicy

このポリシーは、Quick Setup ツールのデフォルトの IAM インスタンスプロファイルを作成して、まだインスタンスプロファイルがアタッチされていない Amazon EC2 インスタンスにアタッチすることを Systems Manager に許可する管理アクセス許可を付与します。このポリシーは、既存のインスタンスプロファイルにアクセス許可をアタッチする機能も Systems Manager に付与します。その目的は、Systems Manager が EC2 インスタンス上の SSM Agent と通信するために必要なアクセス許可を確実に付与することです。

AWSQuickSetupManagedInstanceProfileExecutionPolicy を IAM エンティティにアタッチできます。Systems Manager はまた、Systems Manager がユーザーに代わりアクションを実行することを可能にするサービスロールをこのポリシーにアタッチします。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- ssm – プリンシパルが Quick Setup プロセスに関連付けられている Automation ワークフローを開始することを許可します。
- ec2 – プリンシパルが Quick Setup によって管理される EC2 インスタンスに IAM インスタンスプロファイルをアタッチすることを許可します。
- iam – プリンシパルが Quick Setup プロセスに使用されるロールに関する情報を作成、更新、および IAM から取得すること、IAM インスタンスプロファイルを作成すること、IAM インスタンスプロファイルに AmazonSSMManagedInstanceCore マネージドポリシーをアタッチすることを許可します。

JSON ポリシードキュメントの最新バージョンを確認するには、「AWS マネージドポリシーリファレンスガイド」の「AWSQuickSetupManagedInstanceProfileExecutionPolicy」を参照してください。

AWS マネージドポリシー: AWSQuickSetupFullAccess

このポリシーは、AWS Management Consoleおよび AWS SDK 内の AWS Systems Manager Quick Setup API アクションとデータへのフルアクセスと、Quick Setup オペレーションに必要な他の AWS のサービスリソースへの制限付きアクセスを許可する管理アクセス許可を付与します。

AWSQuickSetupFullAccess ポリシーを IAM アイデンティティにアタッチできます。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- ssm – プリンシパルが Explorer を有効にすること、State Manager でリソースデータ同期オペレーションを実行すること、SSM コマンドドキュメントと Automation ランブックを使用してオペレーションを実行することを許可します。

  Explorer、State Manager、Documents、Automation はすべて Systems Manager のツールです。
- cloudformation – プリンシパルが AWS リージョンと AWS アカウント全体にわたってリソースをプロビジョニングするために必要な AWS CloudFormation オペレーションを実行することを許可します。
- ec2 – プリンシパルが AWS Management Consoleで特定の設定に必要なパラメータを選択して検証を実施することを許可します。

- iam – プリンシパルが Quick Setup オペレーションに必要なサービスロールとサービスリンクロールを作成することを許可します。
- organizations – プリンシパルが AWS Organizations 組織内のアカウントのステータスを読み取ること、組織の構造を取得すること、信頼できるアクセスを有効にすること、管理アカウントから委任管理者アカウントを登録することを許可します。
- resource-groups – プリンシパルが AWS Management Consoleで特定の設定に必要なパラメータを選択して検証を実施することを許可します。
- s3 – プリンシパルが AWS Management Consoleで特定の設定に必要なパラメータを選択して検証を実施することを許可します。
- ssm-quicksetup – プリンシパルが Quick Setup で読み取り専用アクションを実行することを許可します。

JSON ポリシードキュメントの最新バージョンを確認するには、「AWS マネージドポリシーリファレンスガイド」の「AWSQuickSetupFullAccess」を参照してください。

AWS マネージドポリシー: AWSQuickSetupReadOnlyAccess

このポリシーは、Quick Setup オペレーションに必要な他の AWS のサービスリソースからの情報など、プリンシパルが AWS Systems Manager Quick Setup データとレポートを表示することを許可する読み取り専用アクセス許可を付与します。

AWSQuickSetupReadOnlyAccess ポリシーを IAM アイデンティティにアタッチできます。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- ssm – プリンシパルが SSM コマンドドキュメントと Automation ランブックを読み取ること、State Manager 関連付け実行のステータスを取得することを許可します。
- cloudformation – プリンシパルが AWS CloudFormation のデプロイのステータスを取得するために必要なオペレーションを開始することを許可します。
- organizations – プリンシパルが AWS Organizations 組織内のアカウントのステータスを読み取ることを許可します。
- ssm-quicksetup – プリンシパルが Quick Setup で読み取り専用アクションを実行することを許可します。

JSON ポリシードキュメントの最新バージョンを確認するには、「AWS マネージドポリシーリファレンスガイド」の「AWSQuickSetupReadOnlyAccess」を参照してください。

AWS マネージドポリシー: AWSQuickSetupManageJITNAResourcesExecutionPolicy

マネージドポリシー `AWSQuickSetupManageJITNAResourcesExecutionPolicy` により、Systems Manager のツールである Quick Setup がジャストインタイムノードアクセスを設定できるようになります。

`AWSQuickSetupManageJITNAResourcesExecutionPolicy` を IAM エンティティにアタッチできます。Systems Manager はまた、Systems Manager がユーザーに代わりアクションを実行することを可能にするサービスロールをこのポリシーにアタッチします。

このポリシーは、Systems Manager がジャストインタイムノードアクセスに関連付けられたリソースを作成することを許可する管理アクセス許可を付与します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `ssm` – プリンシパルがジャストインタイムノードアクセスの ID プロバイダーを指定するサービス設定を取得および更新することを許可します。
- `iam` – プリンシパルがロールを作成、タグ付け、および取得すること、ジャストインタイムノードアクセスマネージドポリシーのロールポリシーをアタッチすること、ジャストインタイムノードアクセスと通知のサービスにリンクされたロールを作成することを許可します。

JSON ポリシードキュメントの最新バージョンを含む、ポリシーの詳細を確認するには、「AWS マネージドポリシーリファレンスガイド」の「AWSQuickSetupManageJITNAResourcesExecutionPolicy」を参照してください。

AWS マネージドポリシー: AWSQuickSetupJITNADeploymentRolePolicy

マネージドポリシー `AWSQuickSetupJITNADeploymentRolePolicy` は、Quick Setup がジャストインタイムノードアクセスの設定に必要な設定タイプをデプロイすることを許可します。

`AWSQuickSetupJITNADeploymentRolePolicy` を IAM エンティティにアタッチできます。Systems Manager はまた、Systems Manager がユーザーに代わりアクションを実行することを可能にするサービスロールをこのポリシーにアタッチします。

このポリシーは、Systems Manager がジャストインタイムノードアクセスに関連付けられたリソースを作成することを許可する管理アクセス許可を付与します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `cloudformation` – プリンシパルが AWS CloudFormation スタックの作成、更新、削除、および読み取りを行うことを許可します。
- `ssm` – プリンシパルが AWS CloudFormation によって呼び出される State Manager の関連付けの作成、削除、更新、および読み取りを行うことを許可します。
- `iam` – プリンシパルが AWS CloudFormation によって呼び出される IAM ロールの作成、削除、読み取り、およびタグ付けを行うことを許可します。

JSON ポリシードキュメントの最新バージョンを含む、ポリシーの詳細を確認するには、「AWS マネージドポリシーリファレンスガイド」の「AWSQuickSetupJITNADeploymentRolePolicy」を参照してください。

AWS マネージドポリシー: AWSSystemsManagerJustInTimeAccessServicePolicy

マネージドポリシー `AWSSystemsManagerJustInTimeAccessServicePolicy` は、Systems Manager のジャストインタイムノードアクセス機能によって管理または使用される AWS リソースへのアクセス許可を提供します。

IAM エンティティに `AWSSystemsManagerJustInTimeAccessServicePolicy` をアタッチすることはできません。このポリシーは、ユーザーに代わって Systems Manager がアクションを実行することを許可する、サービスにリンクされたロールにアタッチされます。詳細については、「ロールを使用してジャストインタイムノードアクセスを有効にする」を参照してください。

このポリシーは、ジャストインタイムノードアクセスに関連付けられたリソースへのアクセスを許可する管理アクセス許可を付与します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `ssm` – プリンシパルが OpsItems を作成、記述、および更新すること、セッションを記述してマネージドノードのタグを一覧表示することを許可します。
- `ssm-guiconnect` – プリンシパルが接続を一覧表示することを許可します。
- `identitystore` – ユーザー ID とグループ ID を取得すること、ユーザーを記述すること、グループメンバーシップを一覧表示することを許可します。

- sso-directory – プリンシパルがユーザーを記述すること、ユーザーがグループのメンバーであるかどうかを判断することを許可します。
- sso – プリンシパルが登録されているリージョンを記述すること、インスタンスとディレクトリの関連付けを一覧表示することを許可します。
- cloudwatch – プリンシパルが AWS/SSM/JustInTimeAccess 名前空間のメトリクスデータを配置することを許可します。
- ec2 – プリンシパルがタグを記述することを許可します。

JSON ポリシードキュメントの最新バージョンを含む、ポリシーの詳細を確認するには、「AWS マネージドポリシーリファレンスガイド」の「AWSSystemsManagerJustInTimeAccessServicePolicy」を参照してください。

AWS マネージドポリシー: AWSSystemsManagerJustInTimeAccessTokenPolicy

マネージドポリシー AWSSystemsManagerJustInTimeAccessTokenPolicy は、Systems Manager がジャストインタイムノードアクセスに使用されるアクセストークンを生成することを許可します。

IAM エンティティに AWSSystemsManagerJustInTimeAccessTokenPolicy をアタッチできます。

このポリシーは、Systems Manager がセッションを開始し、ジャストインタイムノードアクセス用のアクセストークンを生成することを許可する管理アクセス許可を付与します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- ssm – プリンシパルがコマンドを送信すること、コマンド呼び出しを一覧表示すること、Session Manager セッションを開始、再開、および終了することを許可します。
- ssm-guiconnect – プリンシパルが Systems Manager GUI Connect RDP 接続を開始、記述、および終了することを許可します。
- kms – プリンシパルが権限を作成すること、キーデータを生成することを許可します。
- sso – プリンシパルがディレクトリの関連付けを一覧表示することを許可します。
- identitystore – プリンシパルがユーザーを記述することを許可します。

JSON ポリシードキュメントの最新バージョンを含む、ポリシーの詳細を確認するには、「AWS マネージドポリシーリファレンスガイド」の「AWSSystemsManagerJustInTimeAccessTokenPolicy」を参照してください。

AWS マネージドポリシー: AWSSystemsManagerJustInTimeAccessTokenSessionPolicy

マネージドポリシー `AWSSystemsManagerJustInTimeAccessTokenSessionPolicy` は、Systems Manager がスコープダウンされたアクセス許可をジャストインタイムノードアクセストークンに適用することを許可します。

IAM エンティティに `AWSSystemsManagerJustInTimeAccessTokenSessionPolicy` をアタッチできます。

このポリシーは、Systems Manager がジャストインタイムノードアクセストークンのアクセス許可をスコープダウンすることを許可する管理アクセス許可を付与します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `ssm` – プリンシパルが `SSM-SessionManagerRunShell` ドキュメントを使用して Session Manager セッションを開始することを許可します。また、`ssm-guiconnect` によって最初に呼び出されたときに、`AWS-StartPortForwardingSession` ドキュメントを使用してセッションを開始し、コマンド呼び出しを一覧表示し、`AWSSSO-CreateSSOUser` ドキュメントを使用してコマンドを送信します。
- `ssm-guiconnect` – プリンシパルがすべてのリソースで接続をキャンセル、取得、および開始することを許可します。
- `kms` – AWS サービスを介して `ssm-guiconnect` によって呼び出されたときに `SystemsManagerJustInTimeNodeAccessManaged` でタグ付けされたキーについて、プリンシパルが権限を作成すること、データキーを生成することを許可します。
- `sso` – `ssm-guiconnect` によって呼び出されたときに、プリンシパルがディレクトリの関連付けを一覧表示することを許可します。
- `identitystore` – `ssm-guiconnect` によって呼び出されたときに、プリンシパルがユーザーを記述することを許可します。

JSON ポリシードキュメントの最新バージョンを含む、ポリシーの詳細を確認するには、「AWS マネージドポリシーリファレンスガイド」の「AWSSystemsManagerJustInTimeAccessTokenSessionPolicy」を参照してください。

AWS マネージドポリシー: AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy

マネージドポリシー `AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy` は、Systems Manager が委任管理者アカウントからメンバーアカウントにアクセス拒否ポリシーを共有すること、ポリシーを複数の AWS リージョンにレプリケートすることを許可します。

IAM エンティティに `AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy` をアタッチできます。

このポリシーは、Systems Manager がアクセス拒否ポリシーを共有および作成するために必要な管理アクセス許可を提供します。これにより、ジャストインタイムノードアクセス用に設定された AWS Organizations の組織とリージョン内のすべてのアカウントにアクセス拒否ポリシーが適用されます。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `ssm` – プリンシパルが SSM ドキュメントとリソースポリシーを管理することを許可します。
- `ssm-quicksetup` – プリンシパルが Quick Setup 設定マネージャーを読み取ることを許可します。
- `organizations` – プリンシパルが AWS Organizations の組織と委任管理者に関する詳細を一覧表示することを許可します。
- `ram` – プリンシパルがリソース共有を作成、タグ付け、および記述することを許可します。
- `iam` – プリンシパルがサービスロールを記述することを許可します。

JSON ポリシードキュメントの最新バージョンを含む、ポリシーの詳細を確認するには、「AWS マネージドポリシーリファレンスガイド」の「AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy」を参照してください。

AWS マネージドポリシー: AWSSystemsManagerNotificationsServicePolicy

マネージドポリシー AWSSystemsManagerNotificationsServicePolicy は、Systems Manager がジャストインタイムノードアクセスリクエストの E メール通知を送信して、リクエスト承認者にアクセスすることを許可します。

IAM エンティティに AWSSystemsManagerJustInTimeAccessServicePolicy をアタッチすることはできません。このポリシーは、ユーザーに代わって Systems Manager がアクションを実行することを許可する、サービスにリンクされたロールにアタッチされます。詳細については、「ロールを使用してジャストインタイムノードアクセスリクエスト通知を送信する」を参照してください。

このポリシーは、Systems Manager がアクセスリクエスト承認者にジャストインタイムノードアクセスリクエストの E メール通知を送信することを許可する管理アクセス許可を付与します。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- identitystore – プリンシパルがユーザーとグループのメンバーシップを一覧表示および記述することを許可します。
- sso – プリンシパルがインスタンスとディレクトリを一覧表示すること、登録されたリージョンを記述することを許可します。
- sso-directory – プリンシパルがユーザーを記述すること、グループのメンバーを一覧表示することを許可します。
- iam – プリンシパルがロールに関する情報を取得することを許可します。

JSON ポリシードキュメントの最新バージョンを含む、ポリシーの詳細を確認するには、「AWS マネージドポリシーリファレンスガイド」の「AWSSystemsManagerNotificationsServicePolicy」を参照してください。

AWS マネージドポリシー: AWS-SSM-Automation-DiagnosisBucketPolicy

マネージドポリシー AWS-SSM-Automation-DiagnosisBucketPolicy では、問題の診断と修復に使用される S3 バケットにアクセスして、AWS Systems Manager サービスとやり取りするノードの問題を診断するためのアクセス許可を付与できます。

AWS-SSM-Automation-DiagnosisBucketPolicy ポリシーを IAM アイデンティティにアタッチできます。Systems Manager は、ユーザーに代わって診断アクションを実行することを許可する IAM ロールにもこのポリシーをアタッチします。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- s3 – プリンシパルがオブジェクトにアクセスして Amazon S3 バケットに書き込むことを許可します。

JSON ポリシードキュメントの最新バージョンを確認するには、「AWS マネージドポリシーリファレンスガイド」の「AWS-SSM-Automation-DiagnosisBucketPolicy」を参照してください。

AWS マネージドポリシー: AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy

マネージドポリシー AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy では、組織固有のアクセス許可を提供することで、ノードの問題を診断するためのアクセス許可を運用アカウントに付与できます。

AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy を IAM ID にアタッチできます。Systems Manager は、ユーザーに代わって診断アクションを実行することを許可する IAM ロールにもこのポリシーをアタッチします。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- organizations – プリンシパルが組織のルートをリストし、メンバーアカウントを取得してターゲットアカウントを決定することを許可します。
- sts – プリンシパルが修復実行ロールを引き受けて同じ組織内のアカウントとリージョン全体にわたって SSM Automation ドキュメントを実行することを許可します。

JSON ポリシードキュメントの最新バージョンを確認するには、「AWS マネージドポリシーリファレンスガイド」の「AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy」を参照してください。

AWS マネージドポリシー: AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy

マネージドポリシー `AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy` では、組織固有のアクセス許可を提供することで、ノードの問題を診断するためのアクセス許可を運用アカウントに付与できます。

`AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy` ポリシーを IAM アイデンティティにアタッチできます。Systems Manager は、ユーザーに代わって診断アクションを実行することを許可する IAM ロールにもこのポリシーをアタッチします。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `organizations` – プリンシパルが組織のルートをリストし、メンバーアカウントを取得してターゲットアカウントを決定することを許可します。
- `sts` – プリンシパルが診断実行ロールを引き受けて同じ組織内のアカウントとリージョン全体にわたって SSM Automation ドキュメントを実行することを許可します。

JSON ポリシードキュメントの最新バージョンを確認するには、「AWS マネージドポリシーリファレンスガイド」の「AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy」を参照してください。

AWS マネージドポリシーの Systems Manager 更新

以下の表には、このサービスによりこれらの変更の追跡が開始された 2021 年 3 月 12 日以降に行われた Systems Manager 用 AWS マネージドポリシーに対する更新の詳しい説明が記載されています。Systems Manager サービスの他のマネージドポリシーについては、このトピックの後半の「Systems Manager 用の追加のマネージドポリシー」を参照してください。このページの変更に関する自動通知については、[Systems Manager ドキュメント履歴] ページの RSS フィードを購読してください。

変更	説明	日付
AWSQuickSetupDeploymentRolePolicy – ポリシーへの更新	Systems Manager は、Amazon 所有のランブック AWSQuickSetupType-ManageInstanceProfile にアクセスするためのアクセス許可をマネージドポリシー AWSQuickSetupDeploymentRolePolicy に追加しました。このアクセス許可により、Quick Setup はインラインポリシーではなく管理ポリシーを使用して関連付けを作成できます。	2025 年 6 月 10 日
AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy – ポリシーの更新	ジャストインタイムノードアクセスのために AWS Resource Access Manager により共有されているリソースに、Systems Manager がタグを付けることを許可するアクセス許可が Systems Manager に追加されました。	2025 年 4 月 30 日
AWSQuickSetupManageJITNAResourcesExecutionPolicy – ポリシーへの更新	ジャストインタイムノードアクセスのために作成された IAM ロールにタグを付けることを Systems Manager に許可するアクセス許可が Systems Manager に追加されました。	2025 年 4 月 30 日
AWSSystemsManagerJustInTimeAccessTokenSessionPolicy – 新しいポリシー	ジャストインタイムノードアクセストークンにスコープダウンされたアクセス許可を適用することを Systems Manager に許可する新しいポ	2025 年 4 月 30 日

変更	説明	日付
	リシーが Systems Manager に追加されました。	
AWSSystemsManagerNotificationsServicePolicy – 新しいポリシー	ジャストインタイムノードアクセスリクエストの E メール通知をアクセスリクエスト承認者に送信することを Systems Manager に許可する新しいポリシーが Systems Manager に追加されました。	2025 年 4 月 30 日
AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy – 新しいポリシー	承認ポリシーを異なるリージョンにレプリケートすることを Systems Manager に許可する新しいポリシーが Systems Manager に追加されました。	2025 年 4 月 30 日
AWSSystemsManagerJustInTimeAccessTokenPolicy – 新しいポリシー	ジャストインタイムノードアクセスのために使用されるアクセストークンを生成することを Systems Manager に許可する新しいポリシーが Systems Manager に追加されました。	2025 年 4 月 30 日
AWSSystemsManagerJustInTimeAccessServicePolicy – 新しいポリシー	Systems Manager のジャストインタイムノードアクセス機能によって管理または使用される AWS リソースへのアクセス許可を提供する新しいポリシーが Systems Manager に追加されました。	2025 年 4 月 30 日

変更	説明	日付
AWSQuickSetupManageJITNAResourcesExecutionPolicy – 新しいポリシー	ジャストインタイムノードアクセスのために必要なIAM ロールを作成することを、Systems Manager のツールである Quick Setup に許可する新しいポリシーが Systems Manager に追加されました。	2025 年 4 月 30 日
AWSQuickSetupJITNADeploymentRolePolicy – 新しいポリシー	ジャストインタイムノードアクセスを設定するために必要な設定タイプをデプロイすることを Quick Setup に許可するアクセス許可を提供する新しいポリシーが Systems Manager に追加されました。	2025 年 4 月 30 日
AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy – ポリシーの更新	ジャストインタイムノードアクセスのために AWS Resource Access Manager により共有されているリソースに、Systems Manager がタグを付けることを許可するアクセス許可が Systems Manager に追加されました。	2025 年 4 月 30 日
AWSQuickSetupManageJITNAResourcesExecutionPolicy – ポリシーの更新	ジャストインタイムノードアクセスのために作成されたIAM ロールにタグを付けることを Systems Manager に許可するアクセス許可が Systems Manager に追加されました。	2025 年 4 月 30 日

変更	説明	日付
AWSSystemsManagerJustInTimeAccessTokenSessionPolicy – 新しいポリシー	ジャストインタイムノードアクセストークンにスコープダウンされたアクセス許可を適用することを Systems Manager に許可する新しいポリシーが Systems Manager に追加されました。	2025 年 4 月 30 日
AWSSystemsManagerNotificationsServicePolicy – 新しいポリシー	ジャストインタイムノードアクセスリクエストの E メール通知をアクセスリクエスト承認者に送信することを Systems Manager に許可する新しいポリシーが Systems Manager に追加されました。	2025 年 4 月 30 日
AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy – 新しいポリシー	承認ポリシーを異なるリージョンにレプリケートすることを Systems Manager に許可する新しいポリシーが Systems Manager に追加されました。	2025 年 4 月 30 日
AWSSystemsManagerJustInTimeAccessTokenPolicy – 新しいポリシー	ジャストインタイムノードアクセスのために使用されるアクセストークンを生成することを Systems Manager に許可する新しいポリシーが Systems Manager に追加されました。	2025 年 4 月 30 日

変更	説明	日付
AWSSystemsManagerJustInTimeAccessServicePolicy – 新しいポリシー	Systems Manager のジャストインタイムノードアクセス機能によって管理または使用される AWS リソースへのアクセス許可を提供する新しいポリシーが Systems Manager に追加されました。	2025 年 4 月 30 日
AWSQuickSetupManageJITNAResourcesExecutionPolicy – 新しいポリシー	ジャストインタイムノードアクセスのために必要な IAM ロールを作成することを、Systems Manager のツールである Quick Setup に許可する新しいポリシーが Systems Manager に追加されました。	2025 年 4 月 30 日
AWSQuickSetupJITNADeploymentRolePolicy – 新しいポリシー	ジャストインタイムノードアクセスを設定するために必要な設定タイプをデプロイすることを Quick Setup に許可するアクセス許可を提供する新しいポリシーが Systems Manager に追加されました。	2025 年 4 月 30 日
AWS-SSM-DiagnosisAutomation-OperationalAccountAdministrationRolePolicy - 新しいポリシー	組織固有のアクセス許可を提供することで、ノードの問題を診断するためのアクセス許可を運用アカウントに付与できる新しいポリシーが Systems Manager に追加されました。	2024 年 11 月 21 日

変更	説明	日付
AWS-SSM-RemediationAutomation-OperationalAccountAdministrationRolePolicy - 新しいポリシー	組織固有のアクセス許可を提供することで、ノードの問題を診断するためのアクセス許可を運用アカウントに付与できる新しいポリシーが Systems Manager に追加されました。	2024 年 11 月 21 日
AWS-SSM-Automation-DiagnosisBucketPolicy - 新しいポリシー	ターゲットのアカウントとリージョン内のマネージドノードに関する問題を診断する Automation ワークフローを開始できるように、新しいポリシーが Systems Manager に追加されました。	2024 年 11 月 21 日
AmazonSSMServiceRolePolicy – 既存ポリシーへの更新	AWS Resource Explorer に Amazon EC2 インスタンスに関する詳細を収集し、結果を新しい Systems Manager ダッシュボードのウィジェットに表示することを許可する新しいアクセス許可が Systems Manager に追加されました。	2024 年 11 月 21 日
SSMQuickSetupRolePolicy – 既存ポリシーへの更新	Systems Manager のマネージドポリシー SSMQuickSetupRolePolicy が更新されました。この更新により、関連付けられたサービスリンクロール AWSServiceRoleForSSMQuickSetup でリソースデータの同期を管理できるようになります。	2024 年 11 月 21 日

変更	説明	日付
AWS-SSM-DiagnosisAutomation-AdministrationRolePolicy - 新しいポリシー	ターゲットのアカウントとリージョン内のマネージドノードに関する問題を診断する Automation ワークフローを開始できるように、新しいポリシーが Systems Manager に追加されました。	2024 年 11 月 21 日
AWS-SSM-DiagnosisAutomation-ExecutionRolePolicy - 新しいポリシー	ターゲットのアカウントとリージョン内のマネージドノードに関する問題を診断する Automation ワークフローを開始できるように、新しいポリシーが Systems Manager に追加されました。	2024 年 11 月 21 日
AWS-SSM-RemediationAutomation-AdministrationRolePolicy - 新しいポリシー	ターゲットのアカウントとリージョン内のマネージドノードに関する問題を修復する Automation ワークフローを開始できるように、新しいポリシーが Systems Manager に追加されました。	2024 年 11 月 21 日
AWS-SSM-RemediationAutomation-ExecutionRolePolicy - 新しいポリシー	ターゲットのアカウントとリージョン内のマネージドノードに関する問題を修復する Automation ワークフローを開始できるように、新しいポリシーが Systems Manager に追加されました。	2024 年 11 月 21 日

変更	説明	日付
AWSQuickSetupSSMDeploymentRolePolicy – ポリシーの更新	統合コンソール用に作成された IAM ロールと Lambda にタグを付けることを Systems Manager に許可するアクセス許可が Systems Manager に追加されました。	2025 年 5 月 7 日
AWSQuickSetupSSMManageResourcesExecutionPolicy - 新しいポリシー	Quick Setup で Quick Setup 関連付けの IAM ロールを作成するオペレーションを実行できるように、新しいポリシーが Systems Manager に追加されました。関連付けは AWSQuickSetupType-SSM のデプロイによって作成されます。	2024 年 11 月 21 日
AWSQuickSetupSSMLifecycleManagementExecutionPolicy - 新しいポリシー	Quick Setup のデプロイ時に Quick Setup がライフサイクルイベントで AWS CloudFormation カスタムリソースを実行できるように、新しいポリシーが Systems Manager に追加されました。	2024 年 11 月 21 日
AWSQuickSetupSSMDeploymentRolePolicy - 新しいポリシー	Systems Manager のオンボーディングプロセス時に使用されるリソースの作成を Quick Setup に許可する管理アクセス許可を付与できるように、新しいポリシーが Systems Manager に追加されました。	2024 年 11 月 21 日

変更	説明	日付
AWSQuickSetupSSMDeploymentS3BucketRolePolicy - 新しいポリシー	AWS CloudFormation テンプレートを使用して管理されるプリンシパルアカウントの特定のバケットに関する情報を管理および取得できるように、新しいポリシーが Systems Manager に追加されました。	2024 年 11 月 21 日
AWSQuickSetupEnableDHMCExecutionPolicy - 新しいポリシー	自ら既存の AmazonSSMManagedEC2InstanceDefaultPolicy を使用する IAM ロールを作成することを Quick Setup に許可する新しいポリシーが Systems Manager に導入されます。このポリシーには、SSM Agent が Systems Manager サービスと通信するために必要なアクセス許可がすべて含まれています。この新しいポリシーでは、Systems Manager サービス設定に変更を加えることもできます。	2024 年 11 月 21 日
AWSQuickSetupEnableAREXExecutionPolicy - 新しいポリシー	Quick Setup が AWS Resource Explorer のサービスリンクロールを作成して Resource Explorer のビューとアグリゲーターインデックスにアクセスできるように、新しいポリシーが Systems Manager に追加されました。	2024 年 11 月 21 日

変更	説明	日付
AWSQuickSetupManagedInstanceProfileExecutionPolicy - 新しいポリシー	Quick Setup がデフォルトの Quick Setup インスタンスプロファイルを作成して、関連付けられたインスタンスプロファイルがない任意の Amazon EC2 インスタンスにアタッチできるように、新しいポリシーが Systems Manager に追加されました。この新しいポリシーにより、Quick Setup は既存のプロファイルにアクセス許可をアタッチして、必要なすべての Systems Manager アクセス許可を確実に付与できるようになります。	2024 年 11 月 21 日
AWSQuickSetupFullAccess - 新しいポリシー	エンティティに AWS Management Consoleおよび AWS SDK 内の AWS Systems Manager Quick Setup API アクションとデータへのフルアクセスと、Quick Setup オペレーションに必要な他の AWS のサービスリソースへの制限付きアクセスを付与できるように、新しいポリシーが Systems Manager に追加されました。	2024 年 11 月 21 日

変更	説明	日付
AWSQuickSetupReadOnlyAccess - 新しいポリシー	Quick Setup オペレーションに必要な他の AWS のサービスリソースからの情報など、プリンシパルが AWS Systems Manager Quick Setup データとレポートを表示することを許可する読み取り専用アクセス許可を付与できるように、新しいポリシーが Systems Manager に追加されました。	2024 年 11 月 21 日
SSMQuickSetupRolePolicy – 既存ポリシーへの更新	Quick Setup で作成した追加の AWS CloudFormation スタックセットの健全性をチェックできるよう、Systems Manager で新しいアクセス許可を追加しました。	2024 年 8 月 13 日
AmazonSSMManagedEC2InstanceDefaultPolicy – 既存ポリシーへの更新	Systems Manager が、AmazonSSMManagedEC2InstanceDefaultPolicy の JSON ポリシーにステートメント ID (Sid) を追加しました。これらの Sid は、各ポリシーステートメントの目的のインライン記述を提供します。	2024 年 7 月 18 日
SSMQuickSetupRolePolicy - 新しいポリシー	Systems Manager は、デプロイされたリソースの正常性をチェックし、元の設定からドリフトしたインスタンスを修復することを Quick Setup に許可する新しいポリシーを追加しました。	2024 年 7 月 3 日

変更	説明	日付
AWSQuickSetupDeploymentRolePolicy - 新しいポリシー	Systems Manager は、IAM ロールとオートメーションを作成する (これは、推奨されるベストプラクティスを使用して頻繁に使用される Amazon Web Services サービスと機能を設定します) 複数の Quick Setup 設定タイプをサポートする新しいポリシーを追加しました。	2024 年 7 月 3 日
AWSQuickSetupPatchPolicyDeploymentRolePolicy – 新しいポリシー	Systems Manager は、Patch Manager パッチポリシー Quick Setup 設定に関連付けられたリソースを作成することを Quick Setup に許可する新しいポリシーを追加しました。	2024 年 7 月 3 日
AWSQuickSetupPatchPolicyBaselineAccess – 新しいポリシー	Systems Manager は、読み取り専用許可で Patch Manager のパッチベースラインにアクセスすることを Quick Setup に許可する新しいポリシーを追加しました。	2024 年 7 月 3 日
AWSSystemsManagerEnableExplorerExecutionPolicy – 新しいポリシー	Systems Manager は、Explorer を有効にするための管理許可を付与することを Quick Setup に許可する新しいポリシーを追加しました。	2024 年 7 月 3 日

変更	説明	日付
AWSSystemsManagerEnableConfigRecordingExecutionPolicy – 新しいポリシー	Systems Manager は、AWS Config 設定記録を有効にして設定することを Quick Setup に許可する新しいポリシーを追加しました。	2024 年 7 月 3 日
AWSQuickSetupDevOpsGuruPermissionsBoundary – 新しいポリシー	Systems Manager は、Amazon DevOps Guru を有効にして設定することを Quick Setup に許可する新しいポリシーを追加しました。	2024 年 7 月 3 日
AWSQuickSetupDistributorPermissionsBoundary – 新しいポリシー	Systems Manager は、AWS Systems Manager のツールである Distributor を有効にして設定することを Quick Setup に許可する新しいポリシーを追加しました。	2024 年 7 月 3 日
AWSQuickSetupSSMHostMgmtPermissionsBoundary – 新しいポリシー	Systems Manager は、Amazon EC2 インスタンスを安全に管理するための Systems Manager のツールを有効にして設定することを Quick Setup に許可する新しいポリシーを追加しました。	2024 年 7 月 3 日
AWSQuickSetupPatchPolicyPermissionsBoundary – 新しいポリシー	Systems Manager は、AWS Systems Manager のツールである Patch Manager でパッチポリシーを有効にして設定することを Quick Setup に許可する新しいポリシーを追加しました。	2024 年 7 月 3 日

変更	説明	日付
AWSQuickSetupSchedulerPermissionsBoundary – 新しいポリシー	Systems Manager は、Amazon EC2 インスタンスや他のリソースでスケジュールされたオペレーションを有効にして設定することを Quick Setup に許可する新しいポリシーを追加しました。	2024 年 7 月 3 日
AWSQuickSetupCFGCPacksPermissionsBoundary – 新しいポリシー	Systems Manager は、AWS Config 適合パックをデプロイすることを Quick Setup に許可する新しいポリシーを追加しました。	2024 年 7 月 3 日
AWSSystemsManagerOpsDataSyncServiceRolePolicy – 既存ポリシーへの更新	OpsCenter は、OpsData 関連のオペレーションを管理するための Explorer のサービスにリンクされたロール内のサービスコードのセキュリティを強化することを目的として、ポリシーを更新しました。	2023 年 7 月 3 日
AmazonSSMManagedEC2InstanceDefaultPolicy - 新しいポリシー	Systems Manager は、IAM インスタンスプロファイルを使用せずに、Amazon EC2 インスタンスで Systems Manager 機能を許可する新しいポリシーを追加しました。	2022 年 8 月 18 日

変更	説明	日付
AmazonSSMServiceRolePolicy – 既存のポリシーを更新します	Systems Manager では、Explorer または OpsCenter からSecurity Hub を有効にしたときに、Explorer が管理ルールを作成できるようにする新しいアクセス許可が追加されました。OpsData を許可する前に、その設定と Compute Optimizer コンピュートオプティマイザが、必要な要件を満たしていることを確認するための新しいアクセス許可が追加されました。	2021 年 4 月 27 日
AWSSystemsManagerOpsDataSyncServiceRolePolicy - 新しいポリシー	Systems Manager は、Explorer と OpsCenter のSecurity Hub 結果から OpsItems と OpsData を作成および更新する新しいポリシーを追加しました。	2021 年 4 月 27 日
AmazonSSMServiceRolePolicy – 既存ポリシーへの更新	Systems Manager では、Explorer の複数のアカウントと AWS リージョン からの集計 OpsData と OpsItems の詳細を表示できるようにする新しいアクセス許可が追加されました。	2021 年 3 月 24 日
Systems Manager は変更の追跡を開始しました	Systems Manager が AWS マネージドポリシーの変更の追跡を開始しました。	2021 年 3 月 12 日

Systems Manager 用の追加のマネージドポリシー

Systems Manager では、このトピックで前述したマネージドポリシーに加えて、次のポリシーもサポートされています。

- AmazonSSMAutomationApproverAccess – オートメーションの実行を表示するアクセスと、承認待ちのオートメーションへの承認決定を送信するアクセスを許可する AWS マネージドポリシー。
- AmazonSSMAutomationRole – Systems Manager オートメーションサービスにオートメーションランブックで定義されているアクティビティを実行するためのアクセス許可を付与する AWS マネージドポリシー。このポリシーは、管理者および信頼されたパワーユーザーに割り当てます。
- AmazonSSMDirectoryServiceAccess – マネージドノードによるドメインの参加リクエストに対して、SSM Agent による AWS Directory Service へのアクセスをユーザーに代わって許可する AWS マネージドポリシー。
- AmazonSSMFullAccess – Systems Manager API およびドキュメントに対するフルアクセス権を付与する AWS マネージドポリシー。
- AmazonSSMMaintenanceWindowRole – Systems Manager API へのアクセス許可をメンテナンスウィンドウに付与する AWS マネージドポリシー。
- AmazonSSMManagedInstanceCore – ノードに Systems Manager サービスコア機能の使用を許可する AWS マネージドポリシー。
- AmazonSSMPatchAssociation – パッチ関連付け操作用の子インスタンスへのアクセス権を付与する AWS マネージドポリシー。
- AmazonSSMReadOnlyAccess – Systems Manager の読み取り専用 API オペレーション (`Get*` や `List*` など) へのアクセス権を付与する AWS マネージドポリシー。
- AWSSSMOpsInsightsServiceRolePolicy – Systems Manager での運用上のインサイト OpsItems を作成および更新するアクセス許可を付与する AWS マネージドポリシー。サービスにリンクされたロール AWSServiceRoleForAmazonSSM_OpsInsights を通じてアクセス許可を付与するために使用されます。
- AWSSystemsManagerAccountDiscoveryServicePolicy – Systems Manager に AWS アカウント 情報を検出するアクセス許可を付与する AWS マネージドポリシー。
- AWSSystemsManagerChangeManagementServicePolicy – Systems Manager 変更管理フレームワークによって管理または使用され、サービスにリンクされたロール `AWSServiceRoleForSystemsManagerChangeManagement` によって使用される AWS リソースへのアクセス権を付与する AWS マネージドポリシー。

- AmazonEC2RoleforSSM – このポリシーはサポートされなくなったため、使用しないでください。代わりに、AmazonSSMManagedInstanceCore ポリシーを使用して、EC2 インスタンスで Systems Manager サービスコア機能を有効にします。詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」を参照してください。

AWS Systems Manager ID とアクセスのトラブルシューティング

次の情報は、AWS Systems Manager と AWS Identity and Access Management (IAM) の使用に伴って発生する可能性がある一般的な問題の診断や修復に役立ちます。

トピック

- Systems Manager でアクションを実行する権限がない
- iam:PassRole を実行する権限がない
- 自分の AWS アカウント 以外のユーザーに Systems Manager リソースへのアクセスを許可したい

Systems Manager でアクションを実行する権限がない

AWS Management Console から、アクションを実行する権限がないと通知された場合は、管理者に問い合わせてサポートを依頼する必要があります。管理者とは、サインイン認証情報を提供した担当者です。

以下の例のエラーは、mateojackson ユーザーがコンソールを使用して、ドキュメントの詳細を表示しようとしているが、ssm:GetDocument アクセス許可がない場合に発生します。

```
User: arn:aws:ssm::123456789012:user/mateojackson isn't authorized to perform:
 ssm:GetDocument on resource: MyExampleDocument
```

この場合、Mateo は、ssm:GetDocument アクションを使用して MyExampleDocument リソースにアクセスできるように、管理者にポリシーの更新を依頼します。

iam:PassRole を実行する権限がない

iam:PassRole アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新して Systems Manager にロールを渡すことができるようにする必要があります。

一部の AWS のサービスでは、新しいサービスロールやサービスリンクロールを作成せずに、既存のロールをサービスに渡すことができます。そのためには、サービスにロールを渡す権限が必要です。

以下の例のエラーは、marymajor という IAM ユーザーがコンソールを使用して Systems Manager でアクションを実行しようする場合に発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与された権限が必要です。メアリーには、ロールをサービスに渡す許可がありません。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

この場合、Mary のポリシーを更新してメアリーに iam:PassRole アクションの実行を許可する必要があります。

サポートが必要な場合は、AWS 管理者に問い合わせてください。サインイン認証情報を提供した担当者が管理者です。

自分の AWS アカウント 以外のユーザーに Systems Manager リソースへのアクセスを許可したい

他のアカウントのユーザーや組織外のユーザーが、リソースへのアクセスに使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセスコントロールリスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください。

- Systems Manager がこれらの機能をサポートしているかどうかを確認するには、「AWS Systems Manager と IAM の連携方法」をご参照ください。
- 所有している AWS アカウント 全体のリソースへのアクセス権を提供する方法については、IAM ユーザーガイドの所有している別の AWS アカウント アカウントへのアクセス権を IAM ユーザーに提供を参照してください。
- サードパーティーの AWS アカウント にリソースへのアクセス権を提供する方法については、「IAM ユーザーガイド」の「サードパーティが所有する AWS アカウント へのアクセス権を付与する」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、IAM ユーザーガイドの外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可を参照してください。
- クロスアカウントアクセスにおけるロールとリソースベースのポリシーの使用方法の違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。

Systems Manager のサービスにリンクされたロールの使用

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

> **Note**
>
> 「サービスロール」のロールはサービスにリンクされたロールとは異なります。サービスロールは、サービスが AWS のリソースにアクセスできるように、AWS のサービス にアクセス許可を付与する AWS Identity and Access Management (IAM) ロールのタイプです。サービスロールを必要とする Systems Manager のシナリオはごくわずかです。Systems Manager のサービスロールを作成する場合は、他の AWS リソースにアクセスまたは通信するために付与するアクセス許可を選択します。

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

サービスリンクロールを削除するには、最初に関連リソースを削除する必要があります。これにより、リソースへの意図しないアクセスによる権限の削除が防止され、Systems Manager リソースは保護されます。

> **Note**
>
> ハイブリッドおよびマルチクラウド環境内の非 EC2 ノードの場合、それらのマシンが Systems Manager サービスと通信できるようにする追加の IAM ロールが必要です。これは、Systems Manager の IAM サービスロールです。このロールは、Systems Manager サービスに対して AWS Security Token Service (AWS STS) AssumeRole 信頼を付与します。`AssumeRole` アクションは、一時的なセキュリティ認証情報 (アクセスキー ID、シークレットアクセスキー、セキュリティトークンで構成) を返します。これらの一時的な認証情報を使用して、通常はアクセスできない AWS リソースにアクセスします。詳細については、「ハイブリッドおよびマルチクラウド環境で Systems Manager に必要な IAM

サービスロールを作成する」および「AWS Security Token Service API リファレンス」の「AssumeRole」を参照してください。

サービスにリンクされたロールをサポートする他のサービスについては、「IAM と連携する AWS のサービス」を参照し、「サービスにリンクされたロール」の列内で「はい」と表記されたサービスを確認してください。サービスリンクロールに関するドキュメントをサービスで表示するには、リンクで [はい] を選択します。

トピック

- ロールを使用してインベントリの収集と OpsData の表示を行う
- ロールを使用した OpsCenter および Explorer の AWS アカウント 情報の収集
- ロールを使用して、Explorer の OpsData および OpsItems を作成
- ロールを使用して Systems Manager OpsCenter で運用上のインサイト OpsItems を作成する
- ロールを使用して Quick Setup によってプロビジョニングされたリソースの正常性と一貫性を維持する
- ロールを使用した Explorer OpsData のエクスポート
- ロールを使用してジャストインタイムノードアクセスを有効にする
- ロールを使用してジャストインタイムノードアクセスリクエスト通知を送信する

ロールを使用してインベントリの収集と OpsData の表示を行う

Systems Manager は、**AWSServiceRoleForAmazonSSM** と呼ばれるサービスにリンクされたロールを使用します。AWS Systems Manager は、このIAM サービスロールを使用して、ユーザーに代わって AWS リソースを管理します。

インベントリ、OpsData、OpsItems のサービスにリンクされたロールアクセス権限

AWSServiceRoleForAmazonSSM サービスにリンクされたロールは、このロールを引き受ける上で ssm.amazonaws.com のみを信頼します。

Systems Manager のサービスリンクロールの AWSServiceRoleForAmazonSSM は、次の目的で使用することができます。

- Systems Manager Inventory ツールは、サービスリンクロールの AWSServiceRoleForAmazonSSM を使用して、インベントリのメタデータをタグおよびリソースグループから収集します。

- Explorer ツールは、サービスリンクロールの AWSServiceRoleForAmazonSSM を使用して、複数のアカウントから OpsData および OpsItems を表示できるようにします。また、このサービスにリンクされたロールでは、Explorer または OpsCenter からデータソースとして Security Hub を有効にすると、Explorer がマネージドルールを作成できます。

> **Important**
>
> 以前は、Systems Manager コンソールが、AWS マネージド IAM サービスリンクロール AWSServiceRoleForAmazonSSM を選択して、タスクのメンテナンスロールとして使用する機能を提供していました。メンテナンスウィンドウのタスクにおける、このロールとそれに関連するポリシーである AmazonSSMServiceRolePolicy の使用は推奨されなくなりました。このロールをメンテナンスウィンドウのタスクに使用している場合は、使用を中止することをお勧めします。代わりに、メンテナンスウィンドウのタスクが実行されたときに、Systems Manager と他の AWS のサービス間の通信を可能にする独自の IAM ロールを作成します。
>
> 詳細については、「Maintenance Windows を設定する」を参照してください。

AWSServiceRoleForAmazonSSM ロールのアクセス許可を提供するために使用される管理ポリシーは、AmazonSSMServiceRolePolicy です。付与されるアクセス許可の詳細については、「AWS 管理ポリシー: AmazonSSMServiceRolePolicy」を参照してください。

Systems Manager の **AWSServiceRoleForAmazonSSM** のサービスにリンクされたロールの作成

EC2 ユースケースでサービスにリンクされたロールを作成するには、IAM コンソールを使用できます。IAM のコマンドを AWS Command Line Interface (AWS CLI) で使用するか、IAM API を使用して、ssm.amazonaws.com サービス名でサービスにリンクされたロールを作成します。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの作成」を参照してください。

このサービスリンク役割を削除した後で再度作成する必要が生じた場合は同じ方法でアカウントに役割を再作成できます。

Systems Manager の **AWSServiceRoleForAmazonSSM** のサービスにリンクされたロールの編集

Systems Manager では、AWSServiceRoleForAmazonSSM のサービスにリンクされたロールを編集することはできません。サービスにリンクされたロールを作成すると、多くのエンティティによっ

てロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用したロール記述の編集はできます。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの編集」を参照してください。

Systems Manager の **AWSServiceRoleForAmazonSSM** サービスにリンクされたロールの削除

サービスにリンクされたロールが必要な機能またはサービスが不要になった場合は、そのロールを削除することをお勧めします。そうすることで、使用していないエンティティがアクティブにモニタリングまたはメンテナンスされることがなくなります。サービスにリンクされたロールは、IAM コンソール、AWS CLI、または IAM API を使用して手動で削除することができます。そのためにはまず、サービスにリンクされたロールのリソースをクリーンアップする必要があります。その後で、そのロールを手動で削除できます。

AWSServiceRoleForAmazonSSM のサービスにリンクされたロールは複数のツールで使用されていることがあるため、削除する前に、そのロールが使用されていないことを確認してください。

- Inventory: インベントリツールで使用される、サービスにリンクされたロールを削除すると、タグとリソースグループのインベントリデータは同期されなくなります。手動で削除する前に、サービスにリンクされたロールのリソースをクリーンアップする必要があります。
- Explorer: Explorer ツールで使用されるサービスにリンクされたロールを削除すると、クロスアカウント、クロスリージョン OpsData および OpsItems は表示できなくなります。

> **Note**
>
> タグまたはリソースグループを削除する際に、Systems Manager サービスでロールが使用されている場合、削除は失敗することがあります。失敗した場合は数分待ってから操作を再試行してください。

AWSServiceRoleForAmazonSSM で使用されている Systems Manager リソースを削除するには

1. タグを削除するには、「個々のリソースでのタグの追加と削除」を参照してください。
2. リソースグループを削除するには、「AWS Resource Groups からのグループの削除」を参照してください。

IAM を使用して **AWSServiceRoleForAmazonSSM** サービスリンクロールを手動で削除するには

AWSServiceRoleForAmazonSSM サービスにリンクされたロールを削除するには、IAM コンソール、AWS CLI、または IAM API を使用します。詳細については、 IAM ユーザーガイド の「サービスにリンクされたロールの削除」を参照してください。

Systems Manager**AWSServiceRoleForAmazonSSM** サービスにリンクされたロールをサポートするリージョン

Systems Manager では、このサービスが利用可能なすべての AWS リージョンで、AWSServiceRoleForAmazonSSM サービスにリンクされたロールの使用をサポートしています。詳細については、「AWS Systems Manager endpoints and quotas」を参照してください。

ロールを使用した OpsCenter および Explorer の AWS アカウント 情報の収集

Systems Manager は、**AWSServiceRoleForAmazonSSM_AccountDiscovery** と呼ばれるサービスにリンクされたロールを使用します。AWS Systems Manager は、この IAM サービスロールを使用して、AWS アカウント 情報を検出するために他の AWS のサービスを呼び出します。

Systems Manager アカウント検出のためのサービスにリンクされたロールの許可

AWSServiceRoleForAmazonSSM_AccountDiscovery サービスリンク役割は役割の引き受けについて以下のサービスを信頼します。

- accountdiscovery.ssm.amazonaws.com

ロールのアクセス許可ポリシーは、指定したリソースに対して以下のアクションを実行することを Systems Manager に許可します。

- organizations:DescribeAccount
- organizations:DescribeOrganizationalUnit
- organizations:DescribeOrganization
- organizations:ListAccounts
- organizations:ListAWSServiceAccessForOrganization
- organizations:ListChildren
- organizations:ListParents
- organizations:ListDelegatedServicesForAccount
- organizations:ListDelegatedAdministrators

- `organizations:ListRoots`

サービスリンク役割の作成、編集、削除を IAM エンティティ (ユーザー、グループ、役割など) に許可するにはアクセス許可を設定する必要があります。詳細については、「IAM User Guide」(IAM ユーザーガイド) の「Service-linked role permissions」(サービスにリンクされたロールのアクセス権限) を参照してください。

Systems Manager の **AWSServiceRoleForAmazonSSM_AccountDiscovery** のサービスにリンクされたロールの作成

Systems Manager のツールである Explorer および OpsCenter を複数の AWS アカウントで使用する場合は、サービスにリンクされたロールを作成する必要があります。OpsCenter では、サービスにリンクされたロールを手作業で作成する必要があります。詳細については、「(オプション) OpsCenter の手動設定により、複数のアカウント間で OpsItems を一元管理する」を参照してください。

Explorer では、AWS Management Console で Systems Manager を使用してリソースデータ同期を作成する場合、[Create role] (ロールの作成) ボタンを選択して、サービスにリンクされたロールを作成できます。リソースデータの同期をプログラムで作成する場合は、リソースデータの同期を作成する前に、ロールを作成する必要があります。CreateServiceLinkedRole API オペレーションを使用してロールを作成できます。

Systems Manager の **AWSServiceRoleForAmazonSSM_AccountDiscovery** のサービスにリンクされたロールの編集

Systems Manager では、`AWSServiceRoleForAmazonSSM_AccountDiscovery` のサービスにリンクされたロールを編集することはできません。サービスにリンクされたロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用したロール記述の編集はできます。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの編集」を参照してください。

Systems Manager の **AWSServiceRoleForAmazonSSM_AccountDiscovery** サービスにリンクされたロールの削除

サービスリンク役割が必要な機能またはサービスが不要になった場合にはその役割を削除することをお勧めします。そうすることで、使用していないエンティティがアクティブにモニタリングまたはメンテナンスされることがなくなります。ただし、手動で削除する前に、サービスリンクロールをクリーンアップする必要があります。

AWSServiceRoleForAmazonSSM_AccountDiscovery サービスにリンクされたロールのクリーンアップ

IAM を使用して AWSServiceRoleForAmazonSSM_AccountDiscovery サービスにリンクされたロールを削除するには、最初に、Explorer リソースデータ同期をすべて削除する必要があります。

> **Note**
>
> リソースを削除する際に、Systems Manager のサービスでロールが使用されている場合、削除は失敗することがあります。失敗した場合は数分待ってから操作を再試行してください。

AWSServiceRoleForAmazonSSM_AccountDiscovery サービスにリンクされたロールを手動で削除する

IAM コンソール、AWS CLI、または AWS API を使用して、AWSServiceRoleForAmazonSSM_AccountDiscovery サービスにリンクされたロールを削除します。詳細については、 IAM ユーザーガイド の「サービスにリンクされたロールの削除」を参照してください。

Systems Manager**AWSServiceRoleForAmazonSSM_AccountDiscovery** サービスにリンクされたロールをサポートするリージョン

Systems Manager は、サービスを利用できるすべてのリージョンで、サービスにリンクされたロールの使用をサポートします。詳細については、「AWS Systems Manager エンドポイントとクォータ」を参照してください。

AWSServiceRoleForAmazonSSM_AccountDiscovery のサービスにリンクされたロールへの更新

このサービスがこれらの変更の追跡を開始して以降行われた、AWSServiceRoleForAmazonSSM_AccountDiscovery のサービスにリンクされたロールの更新に関する詳細を表示します。このページの変更に関する自動通知については、[Systems Manager ドキュメント履歴] ページの RSS フィードを購読してください。

変更	説明	日付
新しいアクセス許可の追加	このサービスにリンクされたロールに、organizat	2022 年 10 月 17 日

変更	説明	日付
	ions:DescribeOrganizationalUnit および organizations:ListRoots のアクセス許可が含まれるようになりました。これらのアクセス許可により、AWS Organizations の管理アカウントまたは Systems Manager の委任された管理者アカウントが複数のアカウントで OpsItems を使用できるようになります。詳細については、「(オプション) OpsCenter の手動設定により、複数のアカウント間で OpsItems を一元管理する」を参照してください。	

ロールを使用して、Explorer の OpsData および OpsItems を作成

Systems Manager は、**AWSServiceRoleForSystemsManagerOpsDataSync** と呼ばれるサービスにリンクされたロールを使用します。AWS Systems Manager は、この Explorer の IAM サービスロールを使用して OpsData と OpsItems を作成します。

Systems Manager OpsData 同期のためのサービスにリンクされたロールの許可

AWSServiceRoleForSystemsManagerOpsDataSync サービスにリンクされたロールは、ロールの引き受けについて以下のサービスを信頼します。

- opsdatasync.ssm.amazonaws.com

ロールのアクセス許可ポリシーは、指定したリソースに対して以下のアクションを実行することを Systems Manager に許可します。

- Systems Manager Explorer には、OpsItem が更新された際のセキュリティに関する検出結果の更新、OpsItem の作成および更新、SSM マネージドルールが削除された場合の Security Hub データソースの無効化のための許可が、サービスにリンクされたロールから付与される必要があります。

`AWSServiceRoleForSystemsManagerOpsDataSync` ロールのアクセス許可を提供するために使用される管理ポリシーは、`AWSSystemsManagerOpsDataSyncServiceRolePolicy` です。付与されるアクセス許可の詳細については、「AWS マネージドポリシー: AWSSystemsManagerOpsDataSyncServiceRolePolicy」を参照してください。

サービスにリンクされたロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するには、アクセス許可を設定する必要があります。詳細については、「IAM User Guide」(IAM ユーザーガイド) の「Service-linked role permissions」(サービスにリンクされたロールのアクセス権限) を参照してください。

Systems Manager の **AWSServiceRoleForSystemsManagerOpsDataSync** のサービスにリンクされたロールの作成

サービスリンクロールを手動で作成する必要はありません。AWS Management Console で Explorer を有効にすると、Systems Manager によって、サービスにリンクされたロールが作成されます。

> **Important**
>
> このサービスにリンクされたロールがアカウントに表示されるのは、このロールでサポートされている機能を使用する別のサービスでアクションが完了した場合です。また、サービスにリンクされたロールのサポートが開始された 2017 年 1 月 1 日よりも前に Systems Manager サービスを使用していた場合は、Systems Manager によって `AWSServiceRoleForSystemsManagerOpsDataSync` ロールがアカウントに作成されています。詳細については、「IAM アカウントに新しいロールが表示される」を参照してください。

このサービスリンクロールを削除した後で再度作成する必要が生じた場合は、同じ手順でアカウントにロールを再作成できます。AWS Management Console で Explorer を有効にすると、Systems Manager によって、サービスにリンクされたロールが再度作成されます。

AWS のサービスロール (Explorer による OpsData とOpsItems ユースケースの作成を許可) を指定してサービスにリンクされたロールを作成する場合にも、IAM コンソールを使用できます。AWS CLI または AWS API では、`opsdatasync.ssm.amazonaws.com` サービス名を使用してサービスにリ

ンクされたロールを作成します。詳細については、IAM ユーザーガイドの「サービスリンクロールの作成」を参照してください。このサービスリンクロールを削除しても、同じ方法でロールを再作成できます。

Systems Manager の **AWSServiceRoleForSystemsManagerOpsDataSync** のサービスにリンクされたロールの編集

Systems Manager では、AWSServiceRoleForSystemsManagerOpsDataSync のサービスにリンクされたロールを編集することはできません。サービスにリンクされたロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用したロール記述の編集はできます。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの編集」を参照してください。

Systems Manager の **AWSServiceRoleForSystemsManagerOpsDataSync** サービスにリンクされたロールの削除

サービスリンクロールが必要な機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。そうすることで、使用していないエンティティがアクティブにモニタリングまたはメンテナンスされることがなくなります。ただし、手動で削除する前に、サービスリンクロールのリソースをクリーンアップする必要があります。

> **Note**
>
> リソースを削除する際に、Systems Manager のサービスでロールが使用されている場合、削除は失敗することがあります。失敗した場合は、数分待ってから操作を再試行してください。

AWSServiceRoleForSystemsManagerOpsDataSync ロールによる Systems Manager のリソースを削除する手順は、Security Hub と統合できるように Explorer または OpsCenter を構成しているかどうかによって異なります。

AWSServiceRoleForSystemsManagerOpsDataSync ロールで使用されている Systems Manager リソースを削除するには

- Explorer がSecurity Hub 結果に対して新しい OpsItems を作成しないようにするには、「検出結果の受け取りを停止する方法」を参照してください。
- OpsCenter が Security Hub 結果に対して新しい OpsItems を作成しないようにするには、以下を参照してください。

IAM を使用して **AWSServiceRoleForSystemsManagerOpsDataSync** サービスリンクロールを手動で削除するには

IAM コンソール、AWS CLI、または AWS API を使用して、AWSServiceRoleForSystemsManagerOpsDataSync サービスリンクロールを削除します。詳細については、 IAM ユーザーガイド の「サービスにリンクされたロールの削除」を参照してください。

Systems Manager**AWSServiceRoleForSystemsManagerOpsDataSync** サービスにリンクされたロールをサポートするリージョン

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

Systems Manager は、このサービスを利用できるすべてのリージョンで、サービスにリンクされたロールの使用をサポートしているわけではありません。以下のリージョンでは、AWSServiceRoleForSystemsManagerOpsDataSync ロールを使用できます。

AWS リージョン 名	リージョン識別子	Systems Manager でのサポート
米国東部 (バージニア北部)	us-east-1	はい
米国東部 (オハイオ)	us-east-2	はい
米国西部 (北カリフォルニア)	us-west-1	はい
米国西部 (オレゴン)	us-west-2	はい
アジアパシフィック (ムンバイ)	ap-south-1	はい
アジアパシフィック (大阪)	ap-northeast-3	はい
アジアパシフィック (ソウル)	ap-northeast-2	はい
アジアパシフィック (シンガポール)	ap-southeast-1	はい
アジアパシフィック (シドニー)	ap-southeast-2	はい
アジアパシフィック (東京)	ap-northeast-1	はい

AWS リージョン 名	リージョン識別子	Systems Manager でのサポート
カナダ (中部)	ca-central-1	はい
欧州 (フランクフルト)	eu-central-1	はい
欧州 (アイルランド)	eu-west-1	はい
欧州 (ロンドン)	eu-west-2	はい
欧州 (パリ)	eu-west-3	はい
欧州 (ストックホルム)	eu-north-1	はい
南米 (サンパウロ)	sa-east-1	はい
AWS GovCloud (US)	us-gov-west-1	いいえ

ロールを使用して Systems Manager OpsCenter で運用上のインサイト OpsItems を作成する

Systems Manager では、**AWSServiceRoleForAmazonSSM_OpsInsights** と呼ばれるサービスにリンクされたロールを使用します。AWS Systems Manager は、この IAM サービスロールを使用して、Systems Manager OpsCenter でオペレーションインサイト OpsItems を作成および更新します。

Systems Manager 運用上のインサイト OpsItems のための **AWSServiceRoleForAmazonSSM_OpsInsights** サービスにリンクされたロールの許可

AWSServiceRoleForAmazonSSM_OpsInsights サービスにリンクされたロールは、ロールの引き受けについて以下のサービスを信頼します。

- opsinsights.ssm.amazonaws.com

ロールのアクセス許可ポリシーは、指定したリソースに対して以下のアクションを実行することを Systems Manager に許可します。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AllowCreateOpsItem",
   "Effect": "Allow",
   "Action": [
    "ssm:CreateOpsItem",
    "ssm:AddTagsToResource"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowAccessOpsItem",
   "Effect": "Allow",
   "Action": [
    "ssm:UpdateOpsItem",
    "ssm:GetOpsItem"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceTag/SsmOperationalInsight": "true"
    }
   }
  }
 ]
}
```

サービスリンクロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するには、アクセス許可を設定する必要があります。詳細については、「IAM User Guide」(IAM ユーザーガイド) の「Service-linked role permissions」(サービスにリンクされたロールのアクセス権限) を参照してください。

Systems Manager の **AWSServiceRoleForAmazonSSM_OpsInsights** のサービスにリンクされたロールの作成

サービスリンクされたロールを作成する必要があります。AWS Management Console で Systems Manager を使用してオペレーションインサイトを有効にした場合、[Enable (有効化)] ボタンを選択すると、サービスにリンクされたロールを作成できます。

Systems Manager の **AWSServiceRoleForAmazonSSM_OpsInsights** のサービスにリンクされたロールの編集

Systems Manager では、AWSServiceRoleForAmazonSSM_OpsInsights のサービスにリンクされたロールを編集することはできません。サービスリンクロールを作成した後は、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用したロールの説明の編集はできます。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの編集」を参照してください。

Systems Manager の **AWSServiceRoleForAmazonSSM_OpsInsights** サービスにリンクされたロールの削除

サービスリンクロールが必要な機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。そうすることで、モニタリングや保守が積極的に行われていない未使用のエンティティを排除できます。ただし、手動で削除する前に、サービスリンクロールをクリーンアップする必要があります。

AWSServiceRoleForAmazonSSM_OpsInsights サービスにリンクされたロールのクリーンアップ

IAM を使用して AWSServiceRoleForAmazonSSM_OpsInsights サービスにリンクされたロールを削除するには、最初に Systems Manager OpsCenter でオペレーションのインサイトを無効化する必要があります。詳細については、「OpsItems を減らすために運用上のインサイトを分析する」を参照してください。

AWSServiceRoleForAmazonSSM_OpsInsights サービスにリンクされたロールを手動で削除する

IAM コンソール、AWS CLI、または AWS API を使用して、AWSServiceRoleForAmazonSSM_OpsInsights サービスにリンクされたロールを削除します。詳細については、 IAM ユーザーガイド の「サービスにリンクされたロールの削除」を参照してください。

Systems Manager**AWSServiceRoleForAmazonSSM_OpsInsights** サービスにリンクされたロールをサポートするリージョン

Systems Manager は、サービスを利用できるすべてのリージョンで、サービスにリンクされたロールの使用をサポートしているわけではありません。AWSServiceRoleForAmazonSSM_OpsInsights ロールは、以下の各リージョンで使用できます。

リージョン名	リージョン識別子	Systems Manager でのサポート
米国東部 (バージニア北部)	us-east-1	はい
米国東部 (オハイオ)	us-east-2	はい
米国西部 (北カリフォルニア)	us-west-1	はい
米国西部 (オレゴン)	us-west-2	はい
アジアパシフィック (ムンバイ)	ap-south-1	可能
アジアパシフィック (東京)	ap-northeast-1	可能
アジアパシフィック (ソウル)	ap-northeast-2	はい
アジアパシフィック (シンガポール)	ap-southeast-1	はい
アジアパシフィック (シドニー)	ap-southeast-2	可能
アジアパシフィック (香港)	ap-east-1	可能
カナダ (中部)	ca-central-1	はい
欧州 (フランクフルト)	eu-central-1	はい
欧州 (アイルランド)	eu-west-1	はい
欧州 (ロンドン)	eu-west-2	はい
欧州 (パリ)	eu-west-3	はい
欧州 (ストックホルム)	eu-north-1	可能
欧州 (ミラノ)	eu-south-1	可能
南米 (サンパウロ)	sa-east-1	可能
中東 (バーレーン)	me-south-1	可能
アフリカ (ケープタウン)	af-south-1	可能

リージョン名	リージョン識別子	Systems Manager でのサポート
AWS GovCloud (US)	us-gov-west-1	可能
AWS GovCloud (US)	us-gov-east-1	可能

ロールを使用して Quick Setup によってプロビジョニングされたリソースの正常性と一貫性を維持する

Systems Manager では、**AWSServiceRoleForSSMQuickSetup** という名前のサービスにリンクされたロールを使用します。

Systems Manager の **AWSServiceRoleForSSMQuickSetup** サービスにリンクされたロールの許可

AWSServiceRoleForSSMQuickSetup サービスリンク役割は役割の引き受けについて以下のサービスを信頼します。

- ssm-quicksetup.amazonaws.com

AWS Systems Manager は、この IAM サービスロールを使用して、設定の正常性をチェックし、パラメータとプロビジョニングされたリソースが確実に一貫して使用されるようにするとともに、ドリフトが検出されたときにリソースを修復します。

ロールのアクセス許可ポリシーは、指定したリソースに対して以下のアクションを実行することを Systems Manager に許可します。

- ssm (Systems Manager) – 委任管理者アカウントなど、設定されたリソースの意図される状態に関する情報を読み取ります。
- iam (AWS Identity and Access Management) – これは、AWS Organizations の組織全体にわたってリソースデータの同期にアクセスするために必要です。
- organizations (AWS Organizations) – Organizations で設定された組織に属するメンバーアカウントに関する情報を読み取ります。
- cloudformation (AWS CloudFormation) – リソースの状態と CloudFormation スタックセットオペレーションを管理するために使用される CloudFormation スタックに関する情報を読み取ります。

AWSServiceRoleForSSMQuickSetup ロールのアクセス許可を提供するために使用される管理ポリシーは、SSMQuickSetupRolePolicy です。付与されるアクセス許可の詳細については、「AWS マネージドポリシー: SSMQuickSetupRolePolicy」を参照してください。

サービスにリンクされたロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するには、アクセス許可を設定する必要があります。詳細については、「IAM User Guide」(IAM ユーザーガイド) の「Service-linked role permissions」(サービスにリンクされたロールのアクセス権限) を参照してください。

Systems Manager の **AWSServiceRoleForSSMQuickSetup** のサービスにリンクされたロールの作成

AWSServiceRoleForSSMQuickSetup サービスにリンクされたロールを手動で作成する必要はありません。AWS Management Console で Quick Setup 設定を作成すると、Systems Manager は、サービスにリンクされたロールを自動的に作成します。

Systems Manager の **AWSServiceRoleForSSMQuickSetup** のサービスにリンクされたロールの編集

Systems Manager では、AWSServiceRoleForSSMQuickSetup のサービスにリンクされたロールを編集することはできません。サービスにリンクされた役割を作成すると、多くのエンティティによって役割が参照される可能性があるため、役割名を変更することはできません。ただし、IAM を使用した役割の説明の編集はできます。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの編集」を参照してください。

Systems Manager の **AWSServiceRoleForSSMQuickSetup** サービスにリンクされたロールの削除

サービスリンク役割が必要な機能またはサービスが不要になった場合にはその役割を削除することをお勧めします。そうすることで、モニタリングや保守が積極的に行われていない未使用のエンティティを排除できます。ただし、手動で削除する前に、サービスリンクロールをクリーンアップする必要があります。

AWSServiceRoleForSSMQuickSetup サービスにリンクされたロールのクリーンアップ

IAM を使用して AWSServiceRoleForSSMQuickSetup サービスにリンクされたロールを削除する前に、まずそのロールを使用している Quick Setup 設定を削除する必要があります。詳細については、「設定の編集と削除」を参照してください。

AWSServiceRoleForSSMQuickSetup サービスにリンクされたロールを手動で削除する

IAM コンソール、AWS CLI、または AWS API を使用して、AWSServiceRoleForSSMQuickSetup サービスにリンクされたロールを削除します。詳細については、以下の各トピックを参照してください。

- 「IAM ユーザーガイド」の「サービスにリンクされたロールの削除」
- 「AWS CLI リファレンス」内の Quick Setup セクションの「delete-configuration-manager」
- 「DeleteConfigurationManager API リファレンス」の「Quick Setup」

Systems Manager**AWSServiceRoleForSSMQuickSetup** サービスにリンクされたロールをサポートするリージョン

Systems Manager は、サービスを利用できるすべてのリージョンで、サービスにリンクされたロールの使用をサポートしているわけではありません。AWSServiceRoleForSSMQuickSetup ロールは、以下のリージョンで使用できます。

- 米国東部(オハイオ)
- 米国東部 (バージニア北部)
- 米国西部 (北カリフォルニア)
- 米国西部 (オレゴン)
- アジアパシフィック (ムンバイ)
- アジアパシフィック (ソウル)
- アジアパシフィック (シンガポール)
- アジアパシフィック (シドニー)
- アジアパシフィック (東京)
- カナダ (中部)
- 欧州 (フランクフルト)
- 欧州 (ストックホルム)
- 欧州 (アイルランド)
- 欧州 (ロンドン)
- 欧州 (パリ)
- 南米 (サンパウロ)

ロールを使用した Explorer OpsData のエクスポート

AWS Systems Manager Explorer は、AmazonSSMExplorerExportRole サービスロールを使用して、AWS-ExportOpsDataToS3 オートメーションランブックを使用して運用データ (OpsData) をエクスポートします。

Explorer のサービスリンクロールのアクセス許可

AmazonSSMExplorerExportRole サービスにリンクされたロールは、このロールを引き受ける上で ssm.amazonaws.com のみを信頼します。

AmazonSSMExplorerExportRole サービスにリンクされたロールと AWS-ExportOpsDataToS3 オートメーションランブックを使用してオペレーションデータ (OpsData) をエクスポートできます。カンマ区切り (.csv) ファイルとして、Explorer から 5,000 個の OpsData の項目を Amazon Simple Storage Service (Amazon S3) バケットにエクスポートできます。

ロールのアクセス許可ポリシーは、指定したリソースに対して以下のアクションを実行することを Systems Manager に許可します。

- s3:PutObject
- s3:GetBucketAcl
- s3:GetBucketLocation
- sns:Publish
- logs:DescribeLogGroups
- logs:DescribeLogStreams
- logs:CreateLogGroup
- logs:PutLogEvents
- logs:CreateLogStream
- ssm:GetOpsSummary

サービスリンクロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するには、アクセス許可を設定する必要があります。詳細については、「IAM User Guide」(IAM ユーザーガイド) の「Service-linked role permissions」(サービスにリンクされたロールのアクセス権限) を参照してください。

Systems Manager の **AmazonSSMExplorerExportRole** のサービスにリンクされたロールの作成

ユーザーが Systems Manager コンソールで Explorer を使用して OpsData をエクスポートする際に、Systems Manager は `AmazonSSMExplorerExportRole` サービスにリンクされたロールを作成します。詳細については、「Systems Manager Explorer から OpsData をエクスポートする」を参照してください。

このサービスリンクロールを削除した後で再度作成する必要が生じた場合は、同じ方法でアカウントにロールを再作成できます。

Systems Manager の **AmazonSSMExplorerExportRole** のサービスにリンクされたロールの編集

Systems Manager では、`AmazonSSMExplorerExportRole` のサービスにリンクされたロールを編集することはできません。サービスにリンクされたロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用したロール記述の編集はできます。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの編集」を参照してください。

Systems Manager の **AmazonSSMExplorerExportRole** サービスにリンクされたロールの削除

サービスにリンクされたロールが必要な機能またはサービスが不要になった場合は、そのロールを削除することをお勧めします。そうすることで、使用していないエンティティがアクティブにモニタリングまたはメンテナンスされることがなくなります。サービスにリンクされたロールは、IAM コンソール、AWS CLI、または IAM API を使用して手動で削除することができます。そのためにはまず、サービスにリンクされたロールのリソースをクリーンアップする必要があります。その後で、そのロールを手動で削除できます。

> **Note**
>
> タグまたはリソースグループを削除する際に、Systems Manager サービスでロールが使用されている場合、削除は失敗することがあります。失敗した場合は、数分待ってから操作を再試行してください。

AmazonSSMExplorerExportRole で使用されている Systems Manager リソースを削除するには

1. タグを削除するには、「個々のリソースでのタグの追加と削除」を参照してください。
2. リソースグループを削除するには、「AWS Resource Groups からのグループの削除」を参照してください。

IAM を使用して **AmazonSSMExplorerExportRole** サービスリンクロールを手動で削除するには

AmazonSSMExplorerExportRole サービスにリンクされたロールを削除するには、IAM コンソール、AWS CLI、または IAM API を使用します。詳細については、 IAM ユーザーガイド の「サービスにリンクされたロールの削除」を参照してください。

Systems Manager**AmazonSSMExplorerExportRole** サービスにリンクされたロールをサポートするリージョン

Systems Manager では、このサービスが利用可能なすべての AWS リージョンで、AmazonSSMExplorerExportRole サービスにリンクされたロールの使用をサポートしています。詳細については、「AWS Systems Manager エンドポイントとクォータ」を参照してください。

ロールを使用してジャストインタイムノードアクセスを有効にする

Systems Manager は、**AWSServiceRoleForSystemsManagerJustInTimeAccess** という名前のサービスリンクロールを使用します。AWS Systems Manager は、この IAM サービスロールを使用してジャストインタイムノードアクセスを有効にします。

Systems Manager ジャストインタイムノードアクセス用のサービスリンクロールアクセス許可

AWSServiceRoleForSystemsManagerJustInTimeAccess サービスリンクロールは、以下のサービスを信頼してロールを引き受けます。

- ssm.amazonaws.com

ロールのアクセス許可ポリシーは、指定したリソースに対して以下のアクションを実行することを Systems Manager に許可します。

- ssm:CreateOpsItem
- ssm:GetOpsItem

- ssm:UpdateOpsItem
- ssm:DescribeOpsItems
- ssm:DescribeSessions
- ssm:ListTagsForResource
- ssm-guiconnect:ListConnections
- identitystore:ListGroupMembershipsForMember
- identitystore:DescribeUser
- identitystore:GetGroupId
- identitystore:GetUserId
- sso-directory:DescribeUsers
- sso-directory:IsMemberInGroup
- sso:ListInstances
- sso:DescribeRegisteredRegions
- sso:ListDirectoryAssociations
- ec2:DescribeTags

AWSServiceRoleForSystemsManagerJustInTimeAccess ロールのアクセス許可を提供するために使用される管理ポリシーは、AWSSystemsManagerEnableJustInTimeAccessPolicy です。付与されるアクセス許可の詳細については、「AWS マネージドポリシー: AWSSystemsManagerJustInTimeAccessServicePolicy」を参照してください。

サービスにリンクされたロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するには、アクセス許可を設定する必要があります。詳細についてはIAM ユーザーガイド の「サービスにリンクされた役割のアクセス許可」を参照してください。

Systems Manager の **AWSServiceRoleForSystemsManagerJustInTimeAccess** のサービスにリンクされたロールの作成

サービスリンクロールを手動で作成する必要はありません。AWS Management Consoleでジャストインタイムノードアクセスを有効にすると、Systems Manager が自動的にサービスリンクロールを作成します。

> **Important**
>
> このサービスにリンクされたロールがアカウントに表示されるのは、このロールでサポートされている機能を使用する別のサービスでアクションが完了した場合です。また、サービスリンクロールのサポートが開始された 2024 年 11 月 19 日より前に Systems Manager サービスを使用していた場合、Systems Manager がアカウント内に `AWSServiceRoleForSystemsManagerJustInTimeAccess` ロールを既に作成しています。詳細については、「IAM アカウントに新しいロールが表示される」を参照してください。

このサービスリンクロールを削除した後で再度作成する必要が生じた場合は、同じ手順でアカウントにロールを再作成できます。AWS Management Consoleでジャストインタイムノードアクセスを有効にすると、Systems Manager が再度自動的にサービスリンクロールを作成します。

また、Systems Manager でジャストインタイムノードアクセスを有効にできるようにする AWS サービスロールというユースケースでも、IAM コンソールを使用してサービスリンクロールを作成できます。AWS CLI または AWS API では、`ssm.amazonaws.com` サービス名を使用してサービスにリンクされたロールを作成します。詳細については、IAM ユーザーガイドの「サービスリンクロールの作成」を参照してください。このサービスリンクロールを削除しても、同じ方法でロールを再作成できます。

Systems Manager の **AWSServiceRoleForSystemsManagerJustInTimeAccess** のサービスにリンクされたロールの編集

Systems Manager では、`AWSServiceRoleForSystemsManagerJustInTimeAccess` のサービスにリンクされたロールを編集することはできません。サービスにリンクされたロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用したロール記述の編集はできます。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの編集」を参照してください。

Systems Manager の **AWSServiceRoleForSystemsManagerJustInTimeAccess** サービスにリンクされたロールの削除

サービスリンクロールを必要とする機能やサービスが不要になった場合は、ロールを削除することをお勧めします。そうすることで、使用していないエンティティがアクティブにモニタリングまたはメンテナンスされることがなくなります。ただし、手動で削除する前に、サービスリンクロールのリソースをクリーンアップする必要があります。

> **Note**
>
> リソースを削除する際に、Systems Manager のサービスでロールが使用されている場合、削除は失敗することがあります。その場合は、数分待ってからオペレーションを再試行してください。

IAM を使用して **AWSServiceRoleForSystemsManagerJustInTimeAccess** サービスリンクロールを手動で削除するには

IAM コンソール、AWS CLI、または AWS API を使用して、AWSServiceRoleForSystemsManagerJustInTimeAccess サービスリンクロールを削除します。詳細については、IAM ユーザーガイド の「サービスにリンクされたロールの削除」を参照してください。

Systems Manager**AWSServiceRoleForSystemsManagerJustInTimeAccess** サービスにリンクされたロールをサポートするリージョン

AWS リージョン 名	リージョン識別子	Systems Manager でのサポート
米国東部 (バージニア北部)	us-east-1	はい
米国東部 (オハイオ)	us-east-2	はい
米国西部 (北カリフォルニア)	us-west-1	はい
米国西部 (オレゴン)	us-west-2	はい
アジアパシフィック (ムンバイ)	ap-south-1	はい
アジアパシフィック (大阪)	ap-northeast-3	はい
アジアパシフィック (ソウル)	ap-northeast-2	はい
アジアパシフィック (シンガポール)	ap-southeast-1	はい
アジアパシフィック (シドニー)	ap-southeast-2	はい
アジアパシフィック (東京)	ap-northeast-1	はい

AWS リージョン 名	リージョン識別子	Systems Manager でのサポート
カナダ (中部)	ca-central-1	はい
欧州 (フランクフルト)	eu-central-1	はい
欧州 (アイルランド)	eu-west-1	はい
欧州 (ロンドン)	eu-west-2	はい
欧州 (パリ)	eu-west-3	はい
欧州 (ストックホルム)	eu-north-1	はい
南米 (サンパウロ)	sa-east-1	はい
AWS GovCloud (US)	us-gov-west-1	いいえ

ロールを使用してジャストインタイムノードアクセスリクエスト通知を送信する

Systems Manager は、**AWSServiceRoleForSystemsManagerNotifications** という名前のサービスリンクロールを使用します。AWS Systems Manager は、この IAM サービスロールを使用してアクセスリクエスト承認者に通知を送信します。

Systems Manager ジャストインタイムノードアクセス通知用のサービスリンクロールアクセス許可

AWSServiceRoleForSystemsManagerNotifications サービスリンクロールは、以下のサービスを信頼してロールを引き受けます。

- ssm.amazonaws.com

ロールのアクセス許可ポリシーは、指定したリソースに対して以下のアクションを実行することを Systems Manager に許可します。

- identitystore:ListGroupMembershipsForMember

- identitystore:ListGroupMemberships
- identitystore:DescribeUser
- sso:ListInstances
- sso:DescribeRegisteredRegions
- sso:ListDirectoryAssociations
- sso-directory:DescribeUser
- sso-directory:ListMembersInGroup
- iam:GetRole

AWSServiceRoleForSystemsManagerNotifications ロールのアクセス許可を提供するために使用される管理ポリシーは、AWSSystemsManagerNotificationsServicePolicy です。付与されるアクセス許可の詳細については、「AWS マネージドポリシー: AWSSystemsManagerNotificationsServicePolicy」を参照してください。

サービスにリンクされたロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するには、アクセス許可を設定する必要があります。詳細についてはIAM ユーザーガイド の「サービスにリンクされた役割のアクセス許可」を参照してください。

Systems Manager の **AWSServiceRoleForSystemsManagerNotifications** のサービスにリンクされたロールの作成

サービスリンクロールを手動で作成する必要はありません。AWS Management Consoleでジャストインタイムノードアクセスを有効にすると、Systems Manager が自動的にサービスリンクロールを作成します。

> **Important**
>
> このサービスにリンクされたロールがアカウントに表示されるのは、このロールでサポートされている機能を使用する別のサービスでアクションが完了した場合です。また、サービスリンクロールのサポートが開始された 2024 年 11 月 19 日より前に Systems Manager サービスを使用していた場合、Systems Manager がアカウント内に AWSServiceRoleForSystemsManagerNotifications ロールを既に作成しています。詳細については、「IAM アカウントに新しいロールが表示される」を参照してください。

このサービスリンクロールを削除した後で再度作成する必要が生じた場合は、同じ手順でアカウントにロールを再作成できます。AWS Management Consoleでジャストインタイムノードアクセスを有効にすると、Systems Manager が再度自動的にサービスリンクロールを作成します。

また、Systems Manager でアクセスリクエスト承認者に通知を送信できるようにする AWS サービスロールというユースケースでも、IAM コンソールを使用してサービスリンクロールを作成できます。AWS CLI または AWS API では、`ssm.amazonaws.com` サービス名を使用してサービスにリンクされたロールを作成します。詳細については、IAM ユーザーガイドの「サービスリンクロールの作成」を参照してください。このサービスリンクロールを削除しても、同じ方法でロールを再作成できます。

Systems Manager の **AWSServiceRoleForSystemsManagerNotifications** のサービスにリンクされたロールの編集

Systems Manager では、`AWSServiceRoleForSystemsManagerNotifications` のサービスにリンクされたロールを編集することはできません。サービスにリンクされたロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用したロール記述の編集はできます。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの編集」を参照してください。

Systems Manager の **AWSServiceRoleForSystemsManagerNotifications** サービスにリンクされたロールの削除

サービスリンクロールを必要とする機能やサービスが不要になった場合は、ロールを削除することをお勧めします。そうすることで、使用していないエンティティがアクティブにモニタリングまたはメンテナンスされることがなくなります。ただし、手動で削除する前に、サービスリンクロールのリソースをクリーンアップする必要があります。

> **Note**
>
> リソースを削除する際に、Systems Manager のサービスでロールが使用されている場合、削除は失敗することがあります。その場合は、数分待ってからオペレーションを再試行してください。

IAM を使用して **AWSServiceRoleForSystemsManagerNotifications** サービスリンクロールを手動で削除するには

IAM コンソール、AWS CLI、または AWS API を使用して、`AWSServiceRoleForSystemsManagerNotifications` サービスリンクロールを削除します。詳細については、IAM ユーザーガイド の「サービスにリンクされたロールの削除」を参照してください。

Systems Manager**AWSServiceRoleForSystemsManagerNotifications** サービスにリンクされたロールをサポートするリージョン

AWS リージョン 名	リージョン識別子	Systems Manager でのサポート
米国東部 (バージニア北部)	us-east-1	はい
米国東部 (オハイオ)	us-east-2	はい
米国西部 (北カリフォルニア)	us-west-1	はい
米国西部 (オレゴン)	us-west-2	はい
アジアパシフィック (ムンバイ)	ap-south-1	はい
アジアパシフィック (大阪)	ap-northeast-3	はい
アジアパシフィック (ソウル)	ap-northeast-2	はい
アジアパシフィック (シンガポール)	ap-southeast-1	はい
アジアパシフィック (シドニー)	ap-southeast-2	はい
アジアパシフィック (東京)	ap-northeast-1	はい
カナダ (中部)	ca-central-1	はい
欧州 (フランクフルト)	eu-central-1	はい
欧州 (アイルランド)	eu-west-1	はい
欧州 (ロンドン)	eu-west-2	はい
欧州 (パリ)	eu-west-3	はい

AWS リージョン 名	リージョン識別子	Systems Manager でのサポート
欧州 (ストックホルム)	eu-north-1	はい
南米 (サンパウロ)	sa-east-1	はい
AWS GovCloud (US)	us-gov-west-1	いいえ

AWS Systems Manager でのログ記録とモニタリング

モニタリングは、AWS Systems Manager と AWSソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。マルチポイント障害が発生した場合は、その障害をデバッグできるように、AWS ソリューションのすべての部分からモニタリングデータを収集する必要があります。AWS には、Systems Manager およびその他のリソースをモニタリングし、潜在的なインシデントに対応するための複数のツールが用意されています。

AWS CloudTrail ログ

CloudTrail は、Systems Manager のユーザー、ロール、または AWS のサービスによって実行されたアクションの記録を提供します。CloudTrail で収集した情報を使用して、Systems Manager に対して行ったリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。詳細については、「AWS Systems Manager による AWS CloudTrail API コールのログ記録」を参照してください。

Amazon CloudWatch アラーム

Amazon CloudWatch アラームを使用して、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスやその他のリソースに対して指定した期間にわたって 1 つのメトリクスを監視します。メトリクスが特定のしきい値を超えると、Amazon Simple Notification Service (Amazon SNS) のトピックまたは AWS Auto Scaling のポリシーに通知が送信されます。CloudWatch アラームは、特定の状態にあるという理由でアクションを呼び出すことはしません。状態が変わり、それが指定した期間だけ維持される必要があります。詳細については、『Amazon CloudWatch ユーザーガイド』の「Amazon CloudWatch アラームの使用」を参照してください。

Amazon CloudWatch ダッシュボード

CloudWatch ダッシュボードは、CloudWatch コンソールにあるカスタマイズ可能なホームページであり、異なる AWS リージョン にまたがっているリソースでも、1 つのビューでモニタリングできます。CloudWatch ダッシュボードを使用して、AWS のリソースのメトリクスおよびア

ラームのカスタマイズされたビューを作成できます。詳細については、「」を参照してくださいSystems Manager がホストする Amazon CloudWatch ダッシュボードの使用

Amazon EventBridge

Amazon EventBridge を使用すると、Systems Manager リソースの変更を警告するようにルールを設定し、EventBridge がそれらのイベントの内容に基づいてアクションを実行するように指示できます。EventBridge は、さまざまな Systems Manager ツールによって発行される多数のイベントをサポートします。詳細については、「Amazon EventBridge を使用して Systems Manager イベントをモニタリングする」を参照してください。

Amazon CloudWatch Logs とSSM Agent ログ

SSM Agent は実行、スケジュールされたアクション、エラー、ヘルスステータスに関連した情報をまとめて各ノードのログファイルに書き込みます。ノードに手動で接続してログファイルを閲覧できます。分析のために、エージェントログデータを CloudWatch Logs のロググループに自動的に送信することをお勧めします。詳細については、統合された CloudWatch Logs へのノードログの送信 (CloudWatch エージェント)およびSSM Agent ログの表示を参照してください。

AWS Systems Manager Compliance

AWS Systems Manager のツールである Compliance を使ってマネージドノードのフリートをスキャンし、パッチコンプライアンスと設定の不整合を調べるために使用できます。複数の AWS アカウント と AWS リージョン からデータを収集して集計し、それに準拠していない特定のリソースにドリルダウンすることができます。デフォルトで、Compliance は、AWS Systems Manager のツールである Patch Manager でのパッチ適用、および AWS Systems Manager のツールである State Manager での関連付けに関する現在のコンプライアンスデータを表示します。詳細については、「AWS Systems Manager のコンプライアンス」を参照してください。

AWS Systems Manager Explorer

AWS Systems Manager のツールである Explorer は、AWS リソースに関する情報を報告するカスタマイズ可能なオペレーションダッシュボードです。Explorer には、AWS アカウントおよび AWS リージョン全体のオペレーションデータ (OpsData) の集約ビューが表示されます。Explorer では、OpsData に EC2 インスタンス、パッチコンプライアンスの詳細、および運用作業項目 (OpsItems) に関するメタデータが含まれています。Explorer では、OpsItems が事業部門またはアプリケーション全体にどのように分散されているか、それらが時間の経過とともにどのような傾向を示すか、およびカテゴリによってどのように異なるかに関するコンテキストが提供されます。Explorer で情報をグループ化およびフィルタリングすると、自身に関連する項目や、アクションが必要な項目に注目することができます。詳細については、「AWS Systems Manager Explorer」を参照してください。

AWS Systems Manager OpsCenter

AWS Systems Manager のツールである OpsCenter は、オペレーションエンジニアと IT プロフェッショナルが AWS リソースに関連するオペレーション作業項目 (OpsItems) を一元的に表示、調査、および解決できる場所を提供します。OpsCenter は、各 OpsItem、関連する OpsItems、および関連リソースに関するコンテキスト調査データを提供しながら、複数のサービスの OpsItems を集約および標準化します。OpsCenter は、問題をすばやく解決するために使用できる Automation (AWS Systems Manager のツール) でランブックも提供します。OpsCenter は Amazon EventBridge と統合されています。つまり、Eventbridge にイベントを発行するすべての AWS のサービスに対して自動的に OpsItems を作成する Eventbridge ルールを作成できます。詳細については、「AWS Systems Manager OpsCenter」を参照してください。

Amazon Simple Notification Service

Amazon Simple Notification Service (Amazon SNS) を設定して、AWS Systems Manager のツールである Run Command または Maintenance Windows を使用して送信したコマンドのステータスに関する通知を送信できます。Amazon SNS は、Amazon SNS トピックをサブスクライブしているクライアントまたはエンドポイントへの通知の送信および配信を管理します。コマンドが新しい状態に変更されるたび、または `Failed` や `Timed Out` などの特定の状態に変更されるたびに通知を受け取ることができます。複数のノードにコマンドを送信する場合、特定ノードに送信されたコマンドの各コピーに対して通知を受けることができます。詳細については、「Amazon SNS 通知を使用した Systems Manager のステータス変更のモニタリング」を参照してください。

AWS Trusted Advisor および AWS Health Dashboard

Trusted Advisor は、AWS の数十万のお客様にサービスを提供することにより得られた、運用実績から学んだベストプラクティスを活用しています。Trusted Advisor はお客様の AWS 環境を検査し、システムの可用性とパフォーマンスを向上させたりセキュリティギャップを埋めたりする機会がある場合には、推奨事項を作成します。すべての AWS のお客様は、Trusted Advisor の 5 つのチェックにアクセスできます。AWS サポート のビジネスまたはエンタープライズプランをご利用のお客様は、すべての Trusted Advisor チェックを表示できます。詳細については、「AWS サポート ユーザーガイド」および「AWS Health ユーザーガイド」の「AWS Trusted Advisor」を参照してください。

詳細情報

- AWS Systems Manager でのログ記録とモニタリング

AWS Systems Manager のコンプライアンス検証

このトピックでは、サードパーティーの保証プログラムへの AWS Systems Manager のコンプライアンスについて説明します。マネージドノードのコンプライアンス データの閲覧に関する情報については、 AWS Systems Manager のコンプライアンス をご参照ください 。

サードパーティーの監査者は、さまざまな AWS コンプライアンスプログラムの一環として Systems Manager のセキュリティとコンプライアンスを評価します。これらのプログラムには、SOC、PCI、FedRAMP、HIPAA などがあります。

特定のコンプライアンスプログラムの対象となる AWS のサービスのリストについては、「コンプライアンスプログラムによる対象範囲内の AWS のサービス」を参照してください。一般的な情報については、「AWSコンプライアンスプログラム」「」「」を参照してください。

AWS Artifact を使用して、サードパーティーの監査レポートをダウンロードできます。詳細については、のAWS Artifact におけるレポートのダウンロードレポートを参照してください。

Systems Manager を使用する際のユーザーのコンプライアンス責任は、ユーザーのデータの機密性や貴社のコンプライアンス目的、適用される法律および規制によって決まります。AWS では、コンプライアンスに役立つ次のリソースを提供しています。

- セキュリティ & コンプライアンス クイックリファレンスガイド – これらのデプロイガイドには、アーキテクチャ上の考慮事項の説明と、AWS でセキュリティとコンプライアンスに重点を置いたベースライン環境をデプロイするためのステップが記載されています。
- HIPAA のセキュリティとコンプライアンスに関するホワイトペーパーを作成する – このホワイトペーパーでは、企業が AWS を使用して HIPAA 準拠のアプリケーションを作成する方法について説明します。
- AWS コンプライアンスのリソース - このワークブックおよびガイドのコレクションは、ユーザーの業界や地域で使用できるかもしれません。
- 「AWS Config デベロッパーガイド」の「ルールでのリソースの評価」 — AWS Config のサービスでは、自社のプラクティス、業界ガイドライン、および規制に対するリソースの設定の準拠状態を評価します。
- AWS Security Hub — この AWS のサービス では、AWS 内のセキュリティ状態が包括的に示されており、セキュリティ業界の標準およびベストプラクティスへの準拠の確認に役立ちます。

AWS Systems Manager での耐障害性

AWS グローバルインフラストラクチャは AWS リージョン およびアベイラビリティーゾーンを中心に構築されています。AWS リージョン は、低レイテンシー、高スループット、そして高度な冗長ネットワークで接続される物理的に独立、隔離された複数のアベイラビリティーゾーンを提供します。アベイラビリティーゾーンを使用すると、中断することなくゾーン間で自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用できます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性が高く、フォールトトレラントで、スケーラブルです。

AWS リージョン とアベイラビリティーゾーンの詳細については、「AWS グローバルインフラストラクチャ」を参照してください。

AWS Systems Manager 内のインフラストラクチャセキュリティ

マネージドサービスである AWS Systems Manager は、AWS グローバルネットワークセキュリティで保護されています。AWSセキュリティサービスと AWS がインフラストラクチャを保護する方法については、「AWSクラウドセキュリティ」を参照してください。インフラストラクチャセキュリティのベストプラクティスを使用して AWS 環境を設計するには、セキュリティの柱 - AWS Well-Architected Frameworkのインフラストラクチャ保護を参照してください。

AWS の発行済み API コールを使用して、ネットワーク経由で Systems Manager にアクセスします。クライアントは以下をサポートする必要があります:

- Transport Layer Security (TLS)。TLS 1.2 は必須で TLS 1.3 がお勧めです。
- DHE (楕円ディフィー・ヘルマン鍵共有) や ECDHE (楕円曲線ディフィー・ヘルマン鍵共有) などの完全前方秘匿性 (PFS) による暗号スイート。これらのモードは、Java 7 以降など、ほとんどの最新システムでサポートされています。

また、リクエストには、アクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。または、AWS Security Token ServiceAWS STS を使用して、一時的なセキュリティ認証情報を生成し、リクエストに署名することもできます。

AWS Systems Manager での構成と脆弱性の分析

AWS は、ファイアウォールの設定やディザスタリカバリなどの基本的なセキュリティタスクを処理します。これらの手順は適切な第三者によって確認され、証明されています。詳細については、以下のリソース を参照してください。

- AWS Systems Manager のコンプライアンス検証
- 責任共有モデル
- セキュリティ、アイデンティティ、コンプライアンスのベストプラクティス

Systems Manager のセキュリティに関するベストプラクティス

AWS Systems Manager には、独自のセキュリティポリシーを開発および実装する際に考慮する必要のあるいくつかのセキュリティ機能が用意されています。以下のベストプラクティスは一般的なガイドラインであり、完全なセキュリティソリューションに相当するものではありません。これらのベストプラクティスはお客様の環境に適切ではないか、十分ではない場合があるため、これらは指示ではなく、有用な考慮事項と見なしてください。

トピック

- Systems Manager の予防的セキュリティのベストプラクティス
- Systems Manager のモニタリングと監査のベストプラクティス

Systems Manager の予防的セキュリティのベストプラクティス

Systems Manager の以下のベストプラクティスはセキュリティ問題を防ぐのに役立ちます。

最小特権アクセスの実装

アクセス許可を付与する場合、どのユーザーにどの Systems Manager リソースに対するアクセス許可を付与するかは、お客様が決定します。つまり、該当リソースに対して許可する特定のアクションを許可するということです。このため、タスクの実行に必要なアクセス許可のみを付与する必要があります。最小限の特権アクセスの実装は、セキュリティリスクはもちろん、エラーや悪意ある行動によってもたらされる可能性のある影響を減らす上での基本となります。

以下のツールは、最小限の特権アクセスを実装するために使用できます。

- IAM ユーザーポリシーと IAM エンティティのアクセス許可の境界
- サービスコントロールポリシー

プロキシを使用する設定になっている場合は、SSM Agent の推奨設定を使用します。

プロキシを使用するように SSM Agent を設定する場合は、Systems Manager インスタンスメタデータサービスの IP アドレスを持つ no_proxy 変数を使用し、Systems Manager への呼び出しがプロキシサービスのアイデンティティを引き受けないようにします。

詳細については、Linux ノードでプロキシを使用するための SSM Agent の設定およびSSM Agent が Windows Server インスタンス用にプロキシを使用するように設定するを参照してください。

SecureString パラメータを使用して機密データを暗号化および保護する

AWS Systems Manager のツールである Parameter Store にある SecureString パラメータは、セキュアな方法で保存および参照する必要のある機密データです。パスワードやライセンスキーなどプレーンテキストで、ユーザーに変更または参照させたくないデータがある場合は、SecureString データ型を使用してこれらのパラメータを作成します。Parameter Store は AWS Key Management Service (AWS KMS) で AWS KMS key を使用してパラメータ値を暗号化します。AWS KMS は、パラメータ値を暗号化する際、カスタマーマネージドキーまたは AWS マネージドキー のいずれかを使用します。セキュリティを最大限に高めるため、独自の KMS キーを使用することをお勧めします。AWS マネージドキー を使用する場合、アカウントで GetParameter アクションと GetParameters アクションを実行する権限のあるユーザーは、すべての SecureString パラメータのコンテンツを表示または取得できます。カスタマーマネージドキーを使用してセキュアな SecureString 値を暗号化する場合、IAM ポリシーとキーポリシーを使用して、パラメータの暗号化と復号化のアクセス許可を管理できます。

AWS マネージドキー を使用する場合、これらのオペレーションのためにアクセスコントロールポリシーを確立することはより困難です。例えば、AWS マネージドキー を使用して SecureString パラメータを暗号化し、ユーザーが SecureString パラメータを操作しないようにする場合は、ユーザーの IAM ポリシーでデフォルトキーへのアクセスを明示的に拒否する必要があります。

詳細については、AWS Key Management Service デベロッパーガイドの「IAM ポリシーを使用して Parameter Store パラメータへのアクセスを制限する」と「AWS Systems ManagerParameter Store が AWS KMS を使用する方法」を参照してください。

ドキュメントパラメータの allowedValues および allowedPattern を定義する

allowedValues および allowedPattern を定義することで、Systems Manager ドキュメント (SSM ドキュメント) のパラメータのユーザー入力を検証できます。allowedValues では、パラメータに使用できる値の配列を定義します。使用できない値をユーザーが入力すると、実行の開始に失敗します。allowedPattern では、ユーザー入力がパラメータに対して定義されたパターンと一致するかどうかを検証する正規表現を定義します。ユーザー入力が使用できるパターンと一致しない場合、実行は開始されません。

allowedValues と allowedPattern の詳細については、「データ要素とパラメータ」を参照してください。

ドキュメントのパブリック共有をブロックする

ユースケースでパブリック共有を有効にする必要がある場合を除き、Systems Manager ドキュメントコンソールの [Preferences] (詳細設定) セクションで、SSM ドキュメントのパブリック共有のブロックの設定をオンにすることをお勧めします。

Amazon Virtual Private Cloud (Amazon VPC) および VPC エンドポイントを使用する

Amazon VPC を使用して、定義した仮想ネットワーク内で AWS リソースを起動できます。仮想ネットワークは、お客様自身のデータセンターで運用されていた従来のネットワークによく似ていますが、 のスケーラブルなインフラストラクチャを使用できるというメリットがあります AWS

VPC エンドポイントを実装することにより、インターネットゲートウェイ、NAT デバイス、VPN 接続、または AWS Direct Connect 接続の必要なく、AWS PrivateLink でサポートされる AWS のサービスおよび VPC エンドポイントサービスに VPC を非公開で接続できます。VPC のインスタンスでは、サービスのリソースと通信するためにパブリック IP アドレスを必要としません。VPC と他のサービス間のトラフィックは、Amazon ネットワークを離れることはありません。

Amazon VPC セキュリティの詳細については、「Amazon VPC ユーザーガイド」の「Systems Manager のために VPC エンドポイントを使用して EC2 インスタンスのセキュリティを強化する」および「Amazon VPC のインターネットワークトラフィックのプライバシー」を参照してください。

Session Manager ユーザーを、対話型コマンドと特定の SSM セッションドキュメントを使用しているセッションに限定する

AWS Systems Manager のツールである Session Manager はマネージドノードにセッションを開始する複数の方法を提供します。最も安全な接続を実現するため、対話型コマンド方式を使用して接続するようにユーザーに要求し、ユーザーの操作を特定のコマンドまたはコマンドシーケンスに制限できます。これにより、ユーザーが実行できる対話型アクションを管理できます。詳細については、「セッションの開始 (対話形式と非対話形式のコマンド)」を参照してください。

セキュリティを強化するために、特定の Amazon EC2 Session Manager インスタンスと特定の Session Manager セッションドキュメントへのアクセスを制限できます。この方法で、AWS Identity and Access Management (IAM) Session Manager ポリシーを使用してアクセスを許可または取り消すことができます。詳細については、「ステップ 3: マネージドノードへのセッションアクセスを制御」を参照してください。

オートメーション ワークフローに対して一時的なノード許可を付与します

AWS Systems Manager のツールである Automation のワークフロー中に、その実行のためにのみ、ノードが許可を必要とする場合がありますが、他の Systems Manager オペレーションには不要です。例えばオートメーション ワークフローでは、特定の API オペレーションを呼び出すためのノードに加え、特にワークフロー中では AWS リソースへのアクセスなどが必要となる場合があります。このような呼び出しまたはリソースへのアクセスを制限する場合、IAM インスタンスプロファイルにアクセス許可を追加する代わりに、オートメーション ランブック自体の中にあるノードに対して一時的かつ付随するアクセス許可を付与できます。Automation のワークフローが終了すると、一時的なアクセス許可は削除されます。詳細については、 AWS Management and Governance Blog の「Providing temporary instance permissions with AWS Systems Manager Automations」を参照してください。

AWS と Systems Manager ツールを最新の状態に維持する

AWS は、AWS および Systems Manager オペレーションで使用できるツールおよびプラグインの更新バージョンを定期的にリリースします。これらのリソースを最新の状態に維持することで、アカウント内のユーザーとノードがこれらツールの最新の機能性やセキュリティ機能にアクセスできるようにします。

- SSM Agent – AWS Systems Manager エージェント (SSM Agent) は、Amazon Elastic Compute Cloud (Amazon EC2) インスタンス、オンプレミスサーバー、仮想マシン (VM) にインストールして設定することができる Amazon のソフトウェアです。SSM Agent により、Systems Manager がこれらのリソースを更新、管理、設定できるようなります。少なくとも 2 週間ごとに新しいバージョンをチェックするか、エージェントの更新を自動化することをお勧めします。詳細については、SSM Agent への更新の自動化 を参照してください。また、更新プロセスの一環として SSM Agent の署名を確認することをお勧めします。詳細については、SSM Agent の署名の確認 を参照してください。
- AWS CLI – AWS Command Line Interface (AWS CLI) は、コマンドラインシェルでコマンドを使用して AWS のサービスとやり取りするためのオープンソースツールです。AWS CLI を更新するには、AWS CLI のインストールに使用したコマンドと同じコマンドを実行します。オペレーティングシステムに適したコマンドを実行するために、少なくとも 2 週間に 1 回ローカルマシンでスケジュールされたタスクを作成することをお勧めします。インストールコマンドの詳細については、AWS Command Line Interface ユーザーガイドの「AWS CLI バージョン 2 のインストール」を参照してください。
- AWS Tools for Windows PowerShell – Tools for Windows PowerShell は、AWS SDK for .NET によって公開されている機能を基盤として構築された PowerShell モジュールです。AWS Tools for Windows PowerShell を使用することにより、PowerShell コマンドラインから AWS リソースに対する操作をスクリプト処理できます。または Tools for Windows PowerShell の

アップデートバージョンが定期的にリリースされているため、ローカルで実行しているバージョンを更新する必要があります。詳細については、IAM ポリシーシミュレーターユーザーガイドの「Updating the AWS Tools for Windows PowerShell on Windows」または「Updating the AWS Tools for Windows PowerShell on Linux or macOS」 を参照してください。

- Session Manager プラグイン – Session Manager を使用する許可を持つ組織内のユーザーが AWS CLI を使用してノードに接続を希望する場合、まずユーザーのローカルマシンに Session Manager のプラグインをインストールする必要があります。プラグインを更新するには、プラグインのインストールに使用したのと同じコマンドを実行します。オペレーティングシステムに適したコマンドを実行するために、少なくとも 2 週間に 1 回ローカルマシンでスケジュールされたタスクを作成することをお勧めします。詳細については、AWS CLI 用の Session Manager プラグインをインストールする を参照してください。
- CloudWatch エージェント – CloudWatch エージェントを設定および使用すると、EC2 インスタンス、オンプレミスインスタンス、仮想マシン (VM) からメトリクスとログを収集できます。これらのログは、モニタリングおよび分析のために Amazon CloudWatch Logs に送信できます。少なくとも 2 週間ごとに新しいバージョンをチェックするか、エージェントの更新を自動化することをお勧めします。最も簡単な更新を行うには、AWS Systems Manager Quick Setup を使用します。詳細については、「AWS Systems Manager Quick Setup」を参照してください。

Systems Manager のモニタリングと監査のベストプラクティス

以下の Systems Manager のベストプラクティスは、潜在的なセキュリティ上の弱点とインシデントを検出するのに役立ちます。

Systems Manager のすべてのリソースの特定と監査

IT アセットの特定はガバナンスとセキュリティの重要な側面です。セキュリティの状態を評価し、潜在的な弱点に対処するには、すべての Systems Manager リソースを特定する必要があります。

タグエディターを使用してセキュリティまたは監査で注意を要するリソースを識別してから、それらのタグを、リソースを検索する必要があるときに使用します。詳細については、AWS Resource Groups ユーザーガイドの「タグ付けするリソースの検索」を参照してください。

Systems Manager リソースのリソースグループを作成します。詳細については、 リソースグループとはを参照してください。

Amazon CloudWatch モニタリングツールを使用したモニタリングの実装

モニタリングは、Systems Manager および AWS ソリューションの信頼性、セキュリティ、可用性、パフォーマンスを維持する上で重要です。Amazon CloudWatch には、Systems Manager と他の AWS のサービスのモニタリングに役立つツールとサービスが含まれています。詳細については、統合された CloudWatch Logs へのノードログの送信 (CloudWatch エージェント)およびAmazon EventBridge を使用して Systems Manager イベントをモニタリングするを参照してください。

CloudTrail の使用

AWS CloudTrail は、Systems Manager のユーザー、ロール、または AWS のサービスによって実行されたアクションのレコードを提供します。CloudTrail で収集した情報を使用して、Systems Manager に対して行ったリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。詳細については、「AWS Systems Manager による AWS CloudTrail API コールのログ記録」を参照してください。

AWS Config をオンにする

AWS Config を使用すると、AWS リソースの設定を評価して監査することができます。AWS Config はリソースの設定を監視し、必要となるセキュアな設定に照らし合わせて、記録された設定を評価できます。AWS Config を使用すると、AWS リソース間の設定や関連性の変更を確認し、詳細なリソース設定履歴を調べ、社内ガイドラインで指定された設定に対して、全体的なコンプライアンスを確認できます。これにより、コンプライアンス監査、セキュリティ分析、変更管理、運用上のトラブルシューティングを簡素化できます。詳細については、AWS Config デベロッパーガイドのコンソールを使用した AWS Config の設定 を参照してください。記録するリソースタイプを指定するときは、必ず Systems Manager リソースを含めてください。

AWS セキュリティアドバイザリを監視する

AWS アカウント について Trusted Advisor に投稿されたセキュリティ勧告を定期的に確認してください。これは、describe-trusted-advisor-checks を使用してプログラムにより行うことができます。

さらに、各 AWS アカウント に登録されているメインの E メールアドレスを注意してモニタリングしてください。AWS は、この E メールアドレスを使用して、お客様に影響を与える可能性のあるセキュリティ問題が新たに発生した場合に連絡します。

広範な影響を与える AWS の運用上の問題は AWS Service Health Dashboard に投稿されます。運用上の問題は Personal Health ダッシュボードを介して個々のアカウントにも投稿されます。詳細については、AWS Health のドキュメントを参照してください。

詳細情報

- セキュリティ、アイデンティティ、コンプライアンスのベストプラクティス
- 開始する: AWS リソースの設定時にセキュリティのベストプラクティスに従う (AWS セキュリティブログ)
- IAM でのセキュリティのベストプラクティス
- AWS CloudTrail でのセキュリティのベストプラクティス
- Amazon S3 のセキュリティのベストプラクティス
- AWS Key Management Service のセキュリティのベストプラクティス

AWS SDK を使用した Systems Manager のコード例

以下は、AWS Software Development Kit (SDK) で Systems Manager を使用する方法を説明するコード例です。

基本は、重要なオペレーションをサービス内で実行する方法を示すコード例です。

アクションはより大きなプログラムからのコードの抜粋であり、コンテキスト内で実行する必要があります。アクションは個々のサービス機能を呼び出す方法を示していますが、コンテキスト内のアクションは、関連するシナリオで確認できます。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

開始方法

こんにちは、Systems Manager

次のコード例は、Systems Manager の使用を開始する方法を示しています。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.ssm.SsmClient;
import software.amazon.awssdk.services.ssm.model.DocumentFilter;
import software.amazon.awssdk.services.ssm.model.ListDocumentsRequest;
import software.amazon.awssdk.services.ssm.model.ListDocumentsResponse;

public class HelloSSM {

    public static void main(String[] args) {
        final String usage = """
```

```
                Usage:
                    <awsAccount>

                Where:
                    awsAccount - Your AWS Account number.
                """;

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }

        String awsAccount = args[0] ;
        Region region = Region.US_EAST_1;
        SsmClient ssmClient = SsmClient.builder()
            .region(region)
            .build();

        listDocuments(ssmClient, awsAccount);
    }

    /*
    This code automatically fetches the next set of results using the `nextToken`
and
    stops once the desired maxResults (20 in this case) have been reached.
    */
    public static void listDocuments(SsmClient ssmClient, String awsAccount) {
        String nextToken = null;
        int totalDocumentsReturned = 0;
        int maxResults = 20;
        do {
            ListDocumentsRequest request = ListDocumentsRequest.builder()
                .documentFilterList(
                    DocumentFilter.builder()
                        .key("Owner")
                        .value(awsAccount)
                        .build()
                    )
                .maxResults(maxResults)
                .nextToken(nextToken)
                .build();

            ListDocumentsResponse response = ssmClient.listDocuments(request);
```

```
            response.documentIdentifiers().forEach(identifier ->
 System.out.println("Document Name: " + identifier.name()));
            nextToken = response.nextToken();
            totalDocumentsReturned += response.documentIdentifiers().size();
        } while (nextToken != null && totalDocumentsReturned < maxResults);
    }
}
```

- API の詳細については、「AWS SDK for Java 2.x API リファレンス」の「ListDocuments」を参照してください。

JavaScript

SDK for JavaScript (v3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
import { paginateListDocuments, SSMClient } from "@aws-sdk/client-ssm";

// Call ListDocuments and display the result.
export const main = async () => {
  const client = new SSMClient();
  const listDocumentsPaginated = [];
  console.log(
    "Hello, AWS Systems Manager! Let's list some of your documents:\n",
  );
  try {
    // The paginate function is a wrapper around the base command.
    const paginator = paginateListDocuments({ client }, { MaxResults: 5 });
    for await (const page of paginator) {
      listDocumentsPaginated.push(...page.DocumentIdentifiers);
    }
  } catch (caught) {
    console.error(`There was a problem saying hello: ${caught.message}`);
    throw caught;
  }
```

```
  for (const { Name, DocumentFormat, CreatedDate } of listDocumentsPaginated) {
    console.log(`${Name} - ${DocumentFormat} - ${CreatedDate}`);
  }
};

// Call function if run directly.
import { fileURLToPath } from "node:url";
if (process.argv[1] === fileURLToPath(import.meta.url)) {
  main();
}
```

- API の詳細については、「AWS SDK for JavaScript API リファレンス」の「ListDocuments」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
import boto3
from botocore.exceptions import ClientError


def hello_systems_manager(ssm_client):
    """
    Use the AWS SDK for Python (Boto3) to create an AWS Systems Manager
    client and list the first 5 documents in your account.
    This example uses the default settings specified in your shared credentials
    and config files.

    :param ssm_client: A Boto3 AWS Systems Manager Client object. This object
 wraps
                           the low-level AWS Systems Manager service API.
    """
```

```
    print("Hello, AWS Systems Manager! Let's list some of your documents:\n")

    paginator = ssm_client.get_paginator("list_documents")
    page_iterator = paginator.paginate(PaginationConfig={"MaxItems": 5})
    for page in page_iterator:
        for document in page["DocumentIdentifiers"]:
            print(f"  {document['Name']}")


if __name__ == "__main__":
    try:
        hello_systems_manager(boto3.client("ssm"))
    except ClientError as err:
        print("Hello systems manager had an error.")
        print(err.response["Error"]["Code"])
        print(err.response["Error"]["Message"])
```

- API の詳細については、「AWSSDK for Python (Boto3) API リファレンス」の「ListDocuments」を参照してください。

コードの例

- AWS SDK を使用した Systems Manager の基本例
  - こんにちは、Systems Manager
  - AWS SDK を使用した Systems Manager の基本について説明します。
  - AWS SDK を使用する Secrets Manager のアクション
    - CLI で AddTagsToResource を使用する
    - CLI で CancelCommand を使用する
    - CLI で CreateActivation を使用する
    - CLI で CreateAssociation を使用する
    - CLI で CreateAssociationBatch を使用する
    - AWS SDK または CLI で CreateDocument を使用する
    - AWS SDK または CLI で CreateMaintenanceWindow を使用する
    - AWS SDK または CLI で CreateOpsItem を使用する
    - CLI で CreatePatchBaseline を使用する
    - CLI で DeleteActivation を使用する

- CLI で DeleteAssociation を使用する
- AWS SDK または CLI で DeleteDocument を使用する
- AWS SDK または CLI で DeleteMaintenanceWindow を使用する
- AWS SDK で DeleteOpsItem を使用する
- CLI で DeleteParameter を使用する
- CLI で DeletePatchBaseline を使用する
- CLI で DeregisterManagedInstance を使用する
- CLI で DeregisterPatchBaselineForPatchGroup を使用する
- CLI で DeregisterTargetFromMaintenanceWindow を使用する
- CLI で DeregisterTaskFromMaintenanceWindow を使用する
- CLI で DescribeActivations を使用する
- CLI で DescribeAssociation を使用する
- CLI で DescribeAssociationExecutionTargets を使用する
- CLI で DescribeAssociationExecutions を使用する
- CLI で DescribeAutomationExecutions を使用する
- CLI で DescribeAutomationStepExecutions を使用する
- CLI で DescribeAvailablePatches を使用する
- CLI で DescribeDocument を使用する
- CLI で DescribeDocumentPermission を使用する
- CLI で DescribeEffectiveInstanceAssociations を使用する
- CLI で DescribeEffectivePatchesForPatchBaseline を使用する
- CLI で DescribeInstanceAssociationsStatus を使用する
- CLI で DescribeInstanceInformation を使用する
- CLI で DescribeInstancePatchStates を使用する
- CLI で DescribeInstancePatchStatesForPatchGroup を使用する
- CLI で DescribeInstancePatches を使用する
- CLI で DescribeMaintenanceWindowExecutionTaskInvocations を使用する
- CLI で DescribeMaintenanceWindowExecutionTasks を使用する
- CLI で DescribeMaintenanceWindowExecutions を使用する
- CLI で DescribeMaintenanceWindowTargets を使用する

- CLI で DescribeMaintenanceWindowTasks を使用する
- CLI で DescribeMaintenanceWindows を使用する
- AWS SDK または CLI で DescribeOpsItems を使用する
- AWS SDK または CLI で DescribeParameters を使用する
- CLI で DescribePatchBaselines を使用する
- CLI で DescribePatchGroupState を使用する
- CLI で DescribePatchGroups を使用する
- CLI で GetAutomationExecution を使用する
- CLI で GetCommandInvocation を使用する
- CLI で GetConnectionStatus を使用する
- CLI で GetDefaultPatchBaseline を使用する
- CLI で GetDeployablePatchSnapshotForInstance を使用する
- CLI で GetDocument を使用する
- CLI で GetInventory を使用する
- CLI で GetInventorySchema を使用する
- CLI で GetMaintenanceWindow を使用する
- CLI で GetMaintenanceWindowExecution を使用する
- CLI で GetMaintenanceWindowExecutionTask を使用する
- AWS SDK または CLI で GetParameter を使用する
- CLI で GetParameterHistory を使用する
- CLI で GetParameters を使用する
- CLI で GetPatchBaseline を使用する
- CLI で GetPatchBaselineForPatchGroup を使用する
- CLI で ListAssociationVersions を使用する
- CLI で ListAssociations を使用する
- AWS SDK または CLI で ListCommandInvocations を使用する
- CLI で ListCommands を使用する
- CLI で ListComplianceItems を使用する
- CLI で ListComplianceSummaries を使用する
- CLI で ListDocumentVersions を使用する

- CLI で ListDocuments を使用する
- CLI で ListInventoryEntries を使用する
- CLI で ListResourceComplianceSummaries を使用する
- CLI で ListTagsForResource を使用する
- CLI で ModifyDocumentPermission を使用する
- CLI で PutComplianceItems を使用する
- CLI で PutInventory を使用する
- AWS SDK または CLI で PutParameter を使用する
- CLI で RegisterDefaultPatchBaseline を使用する
- CLI で RegisterPatchBaselineForPatchGroup を使用する
- CLI で RegisterTargetWithMaintenanceWindow を使用する
- CLI で RegisterTaskWithMaintenanceWindow を使用する
- CLI で RemoveTagsFromResource を使用する
- AWS SDK または CLI で SendCommand を使用する
- CLI で StartAutomationExecution を使用する
- CLI で StartSession を使用する
- CLI で StopAutomationExecution を使用する
- CLI で UpdateAssociation を使用する
- CLI で UpdateAssociationStatus を使用する
- CLI で UpdateDocument を使用する
- CLI で UpdateDocumentDefaultVersion を使用する
- AWS SDK または CLI で UpdateMaintenanceWindow を使用する
- CLI で UpdateManagedInstanceRole を使用する
- AWS SDK または CLI で UpdateOpsItem を使用する
- CLI で UpdatePatchBaseline を使用する

AWS SDK を使用した Systems Manager の基本例

次のコード例は、AWS SDK で AWS Systems Manager の基本的な使用方法を示しています。

- こんにちは、Systems Manager
- AWS SDK を使用した Systems Manager の基本について説明します。
- AWS SDK を使用する Secrets Manager のアクション
  - CLI で AddTagsToResource を使用する
  - CLI で CancelCommand を使用する
  - CLI で CreateActivation を使用する
  - CLI で CreateAssociation を使用する
  - CLI で CreateAssociationBatch を使用する
  - AWS SDK または CLI で CreateDocument を使用する
  - AWS SDK または CLI で CreateMaintenanceWindow を使用する
  - AWS SDK または CLI で CreateOpsItem を使用する
  - CLI で CreatePatchBaseline を使用する
  - CLI で DeleteActivation を使用する
  - CLI で DeleteAssociation を使用する
  - AWS SDK または CLI で DeleteDocument を使用する
  - AWS SDK または CLI で DeleteMaintenanceWindow を使用する
  - AWS SDK で DeleteOpsItem を使用する
  - CLI で DeleteParameter を使用する
  - CLI で DeletePatchBaseline を使用する
  - CLI で DeregisterManagedInstance を使用する
  - CLI で DeregisterPatchBaselineForPatchGroup を使用する
  - CLI で DeregisterTargetFromMaintenanceWindow を使用する
  - CLI で DeregisterTaskFromMaintenanceWindow を使用する
  - CLI で DescribeActivations を使用する
  - CLI で DescribeAssociation を使用する
  - CLI で DescribeAssociationExecutionTargets を使用する
  - CLI で DescribeAssociationExecutions を使用する
  - CLI で DescribeAutomationExecutions を使用する
  - CLI で DescribeAutomationStepExecutions を使用する
  - CLI で DescribeAvailablePatches を使用する

- CLI で DescribeDocument を使用する
- CLI で DescribeDocumentPermission を使用する
- CLI で DescribeEffectiveInstanceAssociations を使用する
- CLI で DescribeEffectivePatchesForPatchBaseline を使用する
- CLI で DescribeInstanceAssociationsStatus を使用する
- CLI で DescribeInstanceInformation を使用する
- CLI で DescribeInstancePatchStates を使用する
- CLI で DescribeInstancePatchStatesForPatchGroup を使用する
- CLI で DescribeInstancePatches を使用する
- CLI で DescribeMaintenanceWindowExecutionTaskInvocations を使用する
- CLI で DescribeMaintenanceWindowExecutionTasks を使用する
- CLI で DescribeMaintenanceWindowExecutions を使用する
- CLI で DescribeMaintenanceWindowTargets を使用する
- CLI で DescribeMaintenanceWindowTasks を使用する
- CLI で DescribeMaintenanceWindows を使用する
- AWS SDK または CLI で DescribeOpsItems を使用する
- AWS SDK または CLI で DescribeParameters を使用する
- CLI で DescribePatchBaselines を使用する
- CLI で DescribePatchGroupState を使用する
- CLI で DescribePatchGroups を使用する
- CLI で GetAutomationExecution を使用する
- CLI で GetCommandInvocation を使用する
- CLI で GetConnectionStatus を使用する
- CLI で GetDefaultPatchBaseline を使用する
- CLI で GetDeployablePatchSnapshotForInstance を使用する
- CLI で GetDocument を使用する
- CLI で GetInventory を使用する
- CLI で GetInventorySchema を使用する
- CLI で GetMaintenanceWindow を使用する
- CLI で GetMaintenanceWindowExecution を使用する

- CLI で GetMaintenanceWindowExecutionTask を使用する
- AWS SDK または CLI で GetParameter を使用する
- CLI で GetParameterHistory を使用する
- CLI で GetParameters を使用する
- CLI で GetPatchBaseline を使用する
- CLI で GetPatchBaselineForPatchGroup を使用する
- CLI で ListAssociationVersions を使用する
- CLI で ListAssociations を使用する
- AWS SDK または CLI で ListCommandInvocations を使用する
- CLI で ListCommands を使用する
- CLI で ListComplianceItems を使用する
- CLI で ListComplianceSummaries を使用する
- CLI で ListDocumentVersions を使用する
- CLI で ListDocuments を使用する
- CLI で ListInventoryEntries を使用する
- CLI で ListResourceComplianceSummaries を使用する
- CLI で ListTagsForResource を使用する
- CLI で ModifyDocumentPermission を使用する
- CLI で PutComplianceItems を使用する
- CLI で PutInventory を使用する
- AWS SDK または CLI で PutParameter を使用する
- CLI で RegisterDefaultPatchBaseline を使用する
- CLI で RegisterPatchBaselineForPatchGroup を使用する
- CLI で RegisterTargetWithMaintenanceWindow を使用する
- CLI で RegisterTaskWithMaintenanceWindow を使用する
- CLI で RemoveTagsFromResource を使用する
- AWS SDK または CLI で SendCommand を使用する
- CLI で StartAutomationExecution を使用する
- CLI で StartSession を使用する
- CLI で StopAutomationExecution を使用する

- CLI で UpdateAssociation を使用する
- CLI で UpdateAssociationStatus を使用する
- CLI で UpdateDocument を使用する
- CLI で UpdateDocumentDefaultVersion を使用する
- AWS SDK または CLI で UpdateMaintenanceWindow を使用する
- CLI で UpdateManagedInstanceRole を使用する
- AWS SDK または CLI で UpdateOpsItem を使用する
- CLI で UpdatePatchBaseline を使用する

こんにちは、Systems Manager

次のコード例は、Systems Manager の使用を開始する方法を示しています。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.ssm.SsmClient;
import software.amazon.awssdk.services.ssm.model.DocumentFilter;
import software.amazon.awssdk.services.ssm.model.ListDocumentsRequest;
import software.amazon.awssdk.services.ssm.model.ListDocumentsResponse;

public class HelloSSM {

    public static void main(String[] args) {
        final String usage = """

                Usage:
                    <awsAccount>

                Where:
```

```
                    awsAccount - Your AWS Account number.
                """;

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }

        String awsAccount = args[0] ;
        Region region = Region.US_EAST_1;
        SsmClient ssmClient = SsmClient.builder()
            .region(region)
            .build();

        listDocuments(ssmClient, awsAccount);
    }

    /*
    This code automatically fetches the next set of results using the `nextToken`
and
    stops once the desired maxResults (20 in this case) have been reached.
    */
    public static void listDocuments(SsmClient ssmClient, String awsAccount) {
        String nextToken = null;
        int totalDocumentsReturned = 0;
        int maxResults = 20;
        do {
            ListDocumentsRequest request = ListDocumentsRequest.builder()
                .documentFilterList(
                    DocumentFilter.builder()
                        .key("Owner")
                        .value(awsAccount)
                        .build()
                    )
                .maxResults(maxResults)
                .nextToken(nextToken)
                .build();

            ListDocumentsResponse response = ssmClient.listDocuments(request);
            response.documentIdentifiers().forEach(identifier ->
System.out.println("Document Name: " + identifier.name()));
            nextToken = response.nextToken();
            totalDocumentsReturned += response.documentIdentifiers().size();
        } while (nextToken != null && totalDocumentsReturned < maxResults);
```

```
    }
}
```

- API の詳細については、「AWS SDK for Java 2.x API リファレンス」の「ListDocuments」を参照してください。

JavaScript

SDK for JavaScript (v3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
import { paginateListDocuments, SSMClient } from "@aws-sdk/client-ssm";

// Call ListDocuments and display the result.
export const main = async () => {
  const client = new SSMClient();
  const listDocumentsPaginated = [];
  console.log(
    "Hello, AWS Systems Manager! Let's list some of your documents:\n",
  );
  try {
    // The paginate function is a wrapper around the base command.
    const paginator = paginateListDocuments({ client }, { MaxResults: 5 });
    for await (const page of paginator) {
      listDocumentsPaginated.push(...page.DocumentIdentifiers);
    }
  } catch (caught) {
    console.error(`There was a problem saying hello: ${caught.message}`);
    throw caught;
  }

  for (const { Name, DocumentFormat, CreatedDate } of listDocumentsPaginated) {
    console.log(`${Name} - ${DocumentFormat} - ${CreatedDate}`);
  }
};
```

```
// Call function if run directly.
import { fileURLToPath } from "node:url";
if (process.argv[1] === fileURLToPath(import.meta.url)) {
  main();
}
```

- API の詳細については、「AWS SDK for JavaScript API リファレンス」の「ListDocuments」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
import boto3
from botocore.exceptions import ClientError


def hello_systems_manager(ssm_client):
    """
    Use the AWS SDK for Python (Boto3) to create an AWS Systems Manager
    client and list the first 5 documents in your account.
    This example uses the default settings specified in your shared credentials
    and config files.

    :param ssm_client: A Boto3 AWS Systems Manager Client object. This object
 wraps
                           the low-level AWS Systems Manager service API.
    """
    print("Hello, AWS Systems Manager! Let's list some of your documents:\n")

    paginator = ssm_client.get_paginator("list_documents")
    page_iterator = paginator.paginate(PaginationConfig={"MaxItems": 5})
    for page in page_iterator:
```

```
        for document in page["DocumentIdentifiers"]:
            print(f"  {document['Name']}")


if __name__ == "__main__":
    try:
        hello_systems_manager(boto3.client("ssm"))
    except ClientError as err:
        print("Hello systems manager had an error.")
        print(err.response["Error"]["Code"])
        print(err.response["Error"]["Message"])
```

- API の詳細については、「AWSSDK for Python (Boto3) API リファレンス」の「ListDocuments」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK を使用した Systems Manager の基本について説明します。

次のコード例は、以下を実行する方法を示しています。

- メンテナンスウィンドウを作成します。
- メンテナンスウィンドウのスケジュールを変更します。
- ドキュメントを作成します。
- 指定された EC2 インスタンスにコマンドを送信します。
- 新しい OpsItem を作成します。
- OpsItem を更新して解決します。
- メンテナンスウィンドウ、OpsItem、およびドキュメントを削除します。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
import software.amazon.awssdk.services.ssm.model.DocumentAlreadyExistsException;
import software.amazon.awssdk.services.ssm.model.SsmException;

import java.util.Scanner;
public class SSMScenario {
    public static final String DASHES = new String(new char[80]).replace("\0",
 "-");

    public static void main(String[] args) {
        String usage = """
            Usage:
              <instanceId> <title> <source> <category> <severity>

            Where:
                instanceId - The Amazon EC2 Linux/UNIX instance Id that AWS
 Systems Manager uses (ie, i-0149338494ed95f06).
                title - The title of the parameter (default is Disk Space Alert).
                source - The source of the parameter (default is EC2).
                category - The category of the parameter. Valid values are
 'Availability', 'Cost', 'Performance', 'Recovery', 'Security' (default is
 Performance).
                severity - The severity of the parameter. Severity should be a
 number from 1 to 4 (default is 2).
        """;

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }

        Scanner scanner = new Scanner(System.in);
        SSMActions actions = new SSMActions();
```

```
        String documentName;
        String windowName;
        String instanceId = args[0];
        String title = "Disk Space Alert" ;
        String source = "EC2" ;
        String category = "Availability" ;
        String severity = "2" ;

        System.out.println(DASHES);
        System.out.println("""
                Welcome to the AWS Systems Manager SDK Basics scenario.
                This Java program demonstrates how to interact with AWS Systems
Manager using the AWS SDK for Java (v2).
                AWS Systems Manager is the operations hub for your AWS
applications and resources and a secure end-to-end management solution.
                The program's primary functionalities include creating a
maintenance window, creating a document, sending a command to a document,
                listing documents, listing commands, creating an OpsItem,
modifying an OpsItem, and deleting AWS SSM resources.
                Upon completion of the program, all AWS resources are cleaned up.
                Let's get started...

                """);
        waitForInputToContinue(scanner);
        System.out.println(DASHES);

        System.out.println("1. Create an SSM maintenance window.");
        System.out.println("Please enter the maintenance window name (default is
ssm-maintenance-window):");
        String win = scanner.nextLine();
        windowName = win.isEmpty() ? "ssm-maintenance-window" : win;
        String winId = null;
        try {
            winId = actions.createMaintenanceWindow(windowName);
            waitForInputToContinue(scanner);
            System.out.println("The maintenance window ID is: " + winId);
        } catch (DocumentAlreadyExistsException e) {
            System.err.println("The SSM maintenance window already exists.
Retrieving existing window ID...");
            String existingWinId = actions.createMaintenanceWindow(windowName);
            System.out.println("Existing window ID: " + existingWinId);
        } catch (SsmException e) {
            System.err.println("SSM error: " + e.getMessage());
            return;
```

```
        } catch (RuntimeException e) {
            System.err.println("Unexpected error: " + e.getMessage());
            return;
        }
        waitForInputToContinue(scanner);
        System.out.println(DASHES);

        System.out.println("2. Modify the maintenance window by changing the
schedule");
        waitForInputToContinue(scanner);
        try {
            actions.updateSSMMaintenanceWindow(winId, windowName);
            waitForInputToContinue(scanner);
            System.out.println("The SSM maintenance window was successfully
updated");
        } catch (SsmException e) {
            System.err.println("SSM error: " + e.getMessage());
            return;
        } catch (RuntimeException e) {
            System.err.println("Unexpected error: " + e.getMessage());
            return;
        }
        waitForInputToContinue(scanner);
        System.out.println(DASHES);

        System.out.println("3. Create an SSM document that defines the actions
that Systems Manager performs on your managed nodes.");
        System.out.println("Please enter the document name (default is
ssmdocument):");
        String doc = scanner.nextLine();
        documentName = doc.isEmpty() ? "ssmdocument" : doc;
        try {
            actions.createSSMDoc(documentName);
            waitForInputToContinue(scanner);
            System.out.println("The SSM document was successfully created");
        } catch (DocumentAlreadyExistsException e) {
            System.err.println("The SSM document already exists. Moving on");
        } catch (SsmException e) {
            System.err.println("SSM error: " + e.getMessage());
            return;
        } catch (RuntimeException e) {
            System.err.println("Unexpected error: " + e.getMessage());
        }
        waitForInputToContinue(scanner);
```

```
        System.out.println(DASHES);

        System.out.println("4. Now we are going to run a command on an EC2
instance");
        waitForInputToContinue(scanner);
        String commandId="";
        try {
            commandId = actions.sendSSMCommand(documentName, instanceId);
            waitForInputToContinue(scanner);
            System.out.println("The command was successfully sent. Command ID: "
+ commandId);
        } catch (SsmException e) {
            System.err.println("SSM error: " + e.getMessage());
        } catch (InterruptedException e) {
            System.err.println("Thread was interrupted: " + e.getMessage());
        } catch (RuntimeException e) {
            System.err.println("Unexpected error: " + e.getMessage());
        }
        waitForInputToContinue(scanner);
        System.out.println(DASHES);

        System.out.println("5. Lets get the time when the specific command was
sent to the specific managed node");
        waitForInputToContinue(scanner);
        try {
            actions.displayCommands(commandId);
            System.out.println("The command invocations were successfully
displayed.");
        } catch (SsmException e) {
            System.err.println("SSM error: " + e.getMessage());
            return;
        } catch (RuntimeException e) {
            System.err.println("Unexpected error: " + e.getMessage());
            return;
        }
        waitForInputToContinue(scanner);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("""
             6. Now we will create an SSM OpsItem.
             A SSM OpsItem is a feature provided by Amazon's Systems Manager
(SSM) service.
```

```
            It is a type of operational data item that allows you to manage and
track various operational issues,
            events, or tasks within your AWS environment.

            You can create OpsItems to track and manage operational issues as
they arise.
            For example, you could create an OpsItem whenever your application
detects a critical error
            or an anomaly in your infrastructure.
           """);

       waitForInputToContinue(scanner);
       String opsItemId;
       try {
           opsItemId = actions.createSSMOpsItem(title, source, category,
severity);
           System.out.println(opsItemId + " was created");
       } catch (SsmException e) {
           System.err.println("SSM error: " + e.getMessage());
           return;
       } catch (RuntimeException e) {
           System.err.println("Unexpected error: " + e.getMessage());
           return;
       }
       waitForInputToContinue(scanner);
       System.out.println(DASHES);

       System.out.println(DASHES);
       System.out.println("7. Now we will update the SSM OpsItem "+opsItemId);
       waitForInputToContinue(scanner);
       String description = "An update to "+opsItemId ;
       try {
           actions.updateOpsItem(opsItemId, title, description);
       } catch (SsmException e) {
           System.err.println("SSM error: " + e.getMessage());
           return;
       } catch (RuntimeException e) {
           System.err.println("Unexpected error: " + e.getMessage());
           return;
       }

       System.out.println(DASHES);
       System.out.println("8. Now we will get the status of the SSM OpsItem
"+opsItemId);
```

```
        waitForInputToContinue(scanner);
        try {
            actions.describeOpsItems(opsItemId);
        } catch (SsmException e) {
            System.err.println("SSM error: " + e.getMessage());
            return;
        } catch (RuntimeException e) {
            System.err.println("Unexpected error: " + e.getMessage());
            return;
        }

        System.out.println(DASHES);
        System.out.println("9. Now we will resolve the SSM OpsItem "+opsItemId);
        waitForInputToContinue(scanner);
        try {
            actions.resolveOpsItem(opsItemId);
        } catch (SsmException e) {
            System.err.println("SSM error: " + e.getMessage());
            return;
        } catch (RuntimeException e) {
            System.err.println("Unexpected error: " + e.getMessage());
            return;
        }

        System.out.println(DASHES);
        System.out.println("10. Would you like to delete the AWS Systems Manager
resources? (y/n)");
        String delAns = scanner.nextLine().trim();
        if (delAns.equalsIgnoreCase("y")) {
            System.out.println("You selected to delete the resources.");
            waitForInputToContinue(scanner);
            try {
                actions.deleteMaintenanceWindow(winId);
                actions.deleteDoc(documentName);
            } catch (SsmException e) {
                System.err.println("SSM error: " + e.getMessage());
                return;
            } catch (RuntimeException e) {
                System.err.println("Unexpected error: " + e.getMessage());
                return;
            }
        } else {
            System.out.println("The AWS Systems Manager resources will not be
deleted");
```

```
        }
        System.out.println(DASHES);

        System.out.println("This concludes the AWS Systems Manager SDK Basics
 scenario.");
        System.out.println(DASHES);
    }

    private static void waitForInputToContinue(Scanner scanner) {
        while (true) {
            System.out.println("");
            System.out.println("Enter 'c' followed by <ENTER> to continue:");
            String input = scanner.nextLine();

            if (input.trim().equalsIgnoreCase("c")) {
                System.out.println("Continuing with the program...");
                System.out.println("");
                break;
            } else {
                // Handle invalid input.
                System.out.println("Invalid input. Please try again.");
            }
        }
    }
}
```

Systems Manager SDK メソッドのラッパークラス。

```
public class SSMActions {

    private static SsmAsyncClient ssmAsyncClient;

    private static SsmAsyncClient getAsyncClient() {
        if (ssmAsyncClient == null) {
            SdkAsyncHttpClient httpClient = NettyNioAsyncHttpClient.builder()
                    .maxConcurrency(100)
                    .connectionTimeout(Duration.ofSeconds(60))
                    .readTimeout(Duration.ofSeconds(60))
                    .writeTimeout(Duration.ofSeconds(60))
                    .build();
```

```
            ClientOverrideConfiguration overrideConfig =
ClientOverrideConfiguration.builder()
                    .apiCallTimeout(Duration.ofMinutes(2))
                    .apiCallAttemptTimeout(Duration.ofSeconds(90))
                    .retryPolicy(RetryPolicy.builder()
                            .numRetries(3)
                            .build())
                    .build();

            ssmAsyncClient = SsmAsyncClient.builder()
                    .region(Region.US_EAST_1)
                    .httpClient(httpClient)
                    .overrideConfiguration(overrideConfig)
                    .build();
        }
        return ssmAsyncClient;
    }

    /**
     * Deletes an AWS SSM document asynchronously.
     *
     * @param documentName The name of the document to delete.
     * <p>
     * This method initiates an asynchronous request to delete an SSM document.
     * If an exception occurs, it handles the error appropriately.
     */
    public void deleteDoc(String documentName) {
        DeleteDocumentRequest documentRequest = DeleteDocumentRequest.builder()
                .name(documentName)
                .build();

        CompletableFuture<Void> future = CompletableFuture.runAsync(() -> {
            getAsyncClient().deleteDocument(documentRequest)
                    .thenAccept(response -> {
                        System.out.println("The SSM document was successfully
deleted.");
                    })
                    .exceptionally(ex -> {
                        throw new CompletionException(ex);
                    }).join();
        }).exceptionally(ex -> {
            Throwable cause = (ex instanceof CompletionException) ?
ex.getCause() : ex;
            if (cause instanceof SsmException) {
```

```
                throw new RuntimeException("SSM error: " + cause.getMessage(),
cause);
            } else {
                throw new RuntimeException("Unexpected error: " +
cause.getMessage(), cause);
            }
        });

        try {
            future.join();
        } catch (CompletionException ex) {
            throw ex.getCause() instanceof RuntimeException ? (RuntimeException)
ex.getCause() : ex;
        }
    }

    /**
     * Deletes an AWS SSM Maintenance Window asynchronously.
     *
     * @param winId The ID of the Maintenance Window to delete.
     * <p>
     * This method initiates an asynchronous request to delete an SSM Maintenance
Window.
     * If an exception occurs, it handles the error appropriately.
     */
    public void deleteMaintenanceWindow(String winId) {
        DeleteMaintenanceWindowRequest windowRequest =
DeleteMaintenanceWindowRequest.builder()
                .windowId(winId)
                .build();

        CompletableFuture<Void> future = CompletableFuture.runAsync(() -> {
            getAsyncClient().deleteMaintenanceWindow(windowRequest)
                    .thenAccept(response -> {
                        System.out.println("The maintenance window was
successfully deleted.");
                    })
                    .exceptionally(ex -> {
                        throw new CompletionException(ex);
                    }).join();
        }).exceptionally(ex -> {
            Throwable cause = (ex instanceof CompletionException) ?
ex.getCause() : ex;
            if (cause instanceof SsmException) {
```

```
                throw new RuntimeException("SSM error: " + cause.getMessage(),
cause);
            } else {
                throw new RuntimeException("Unexpected error: " +
cause.getMessage(), cause);
            }
        });

        try {
            future.join();
        } catch (CompletionException ex) {
            throw ex.getCause() instanceof RuntimeException ? (RuntimeException)
ex.getCause() : ex;
        }
    }

    /**
     * Resolves an AWS SSM OpsItem asynchronously.
     *
     * @param opsID The ID of the OpsItem to resolve.
     * <p>
     * This method initiates an asynchronous request to resolve an SSM OpsItem.
     * If an exception occurs, it handles the error appropriately.
     */
    public void resolveOpsItem(String opsID) {
        UpdateOpsItemRequest opsItemRequest = UpdateOpsItemRequest.builder()
                .opsItemId(opsID)
                .status(OpsItemStatus.RESOLVED)
                .build();

        CompletableFuture<Void> future = CompletableFuture.runAsync(() -> {
            getAsyncClient().updateOpsItem(opsItemRequest)
                    .thenAccept(response -> {
                        System.out.println("OpsItem resolved successfully.");
                    })
                    .exceptionally(ex -> {
                        throw new CompletionException(ex);
                    }).join();
        }).exceptionally(ex -> {
            Throwable cause = (ex instanceof CompletionException) ?
ex.getCause() : ex;
            if (cause instanceof SsmException) {
                throw new RuntimeException("SSM error: " + cause.getMessage(),
cause);
```

```
            } else {
                throw new RuntimeException("Unexpected error: " +
cause.getMessage(), cause);
            }
        });

        try {
            future.join();
        } catch (CompletionException ex) {
            throw ex.getCause() instanceof RuntimeException ? (RuntimeException)
ex.getCause() : ex;
        }
    }

    /**
     * Describes AWS SSM OpsItems asynchronously.
     *
     * @param key The key to filter OpsItems by (e.g., OPS_ITEM_ID).
     *
     * This method initiates an asynchronous request to describe SSM OpsItems.
     * If the request is successful, it prints the title and status of each
OpsItem.
     * If an exception occurs, it handles the error appropriately.
     */
    public void describeOpsItems(String key) {
        OpsItemFilter filter = OpsItemFilter.builder()
                .key(OpsItemFilterKey.OPS_ITEM_ID)
                .values(key)
                .operator(OpsItemFilterOperator.EQUAL)
                .build();

        DescribeOpsItemsRequest itemsRequest = DescribeOpsItemsRequest.builder()
                .maxResults(10)
                .opsItemFilters(filter)
                .build();

        CompletableFuture<Void> future = CompletableFuture.runAsync(() -> {
            getAsyncClient().describeOpsItems(itemsRequest)
                    .thenAccept(itemsResponse -> {
                        List<OpsItemSummary> items =
itemsResponse.opsItemSummaries();
                        for (OpsItemSummary item : items) {
                            System.out.println("The item title is " +
item.title() + " and the status is " + item.status().toString());
```

```
                        }
                    })
                    .exceptionally(ex -> {
                        throw new CompletionException(ex);
                    }).join();
        }).exceptionally(ex -> {
            Throwable cause = (ex instanceof CompletionException) ?
ex.getCause() : ex;
            if (cause instanceof SsmException) {
                throw new RuntimeException("SSM error: " + cause.getMessage(),
cause);
            } else {
                throw new RuntimeException("Unexpected error: " +
cause.getMessage(), cause);
            }
        });

        try {
            future.join();
        } catch (CompletionException ex) {
            throw ex.getCause() instanceof RuntimeException ? (RuntimeException)
ex.getCause() : ex;
        }
    }

    /**
     * Updates the AWS SSM OpsItem asynchronously.
     *
     * @param opsItemId The ID of the OpsItem to update.
     * @param title The new title of the OpsItem.
     * @param description The new description of the OpsItem.
     * <p>
     * This method initiates an asynchronous request to update an SSM OpsItem.
     * If the request is successful, it completes without returning a value.
     * If an exception occurs, it handles the error appropriately.
     */
    public void updateOpsItem(String opsItemId, String title, String description)
{
        Map<String, OpsItemDataValue> operationalData = new HashMap<>();
        operationalData.put("key1",
OpsItemDataValue.builder().value("value1").build());
        operationalData.put("key2",
OpsItemDataValue.builder().value("value2").build());
```

```
        CompletableFuture<Void> future =
getOpsItem(opsItemId).thenCompose(opsItem -> {
            UpdateOpsItemRequest request = UpdateOpsItemRequest.builder()
                    .opsItemId(opsItemId)
                    .title(title)
                    .operationalData(operationalData)
                    .status(opsItem.statusAsString())
                    .description(description)
                    .build();

            return getAsyncClient().updateOpsItem(request).thenAccept(response ->
{
                System.out.println(opsItemId + " updated successfully.");
            }).exceptionally(ex -> {
                throw new CompletionException(ex);
            });
        }).exceptionally(ex -> {
            Throwable cause = (ex instanceof CompletionException) ?
ex.getCause() : ex;
            if (cause instanceof SsmException) {
                throw new RuntimeException("SSM error: " + cause.getMessage(),
cause);
            } else {
                throw new RuntimeException("Unexpected error: " +
cause.getMessage(), cause);
            }
        });

        try {
            future.join();
        } catch (CompletionException ex) {
            throw ex.getCause() instanceof RuntimeException ? (RuntimeException)
ex.getCause() : ex;
        }
    }


    private static CompletableFuture<OpsItem> getOpsItem(String opsItemId) {
        GetOpsItemRequest request =
GetOpsItemRequest.builder().opsItemId(opsItemId).build();
        return
getAsyncClient().getOpsItem(request).thenApply(GetOpsItemResponse::opsItem);
    }
```

```
    /**
     * Creates an SSM OpsItem asynchronously.
     *
     * @param title The title of the OpsItem.
     * @param source The source of the OpsItem.
     * @param category The category of the OpsItem.
     * @param severity The severity of the OpsItem.
     * @return The ID of the created OpsItem.
     * <p>
     * This method initiates an asynchronous request to create an SSM OpsItem.
     * If the request is successful, it returns the OpsItem ID.
     * If an exception occurs, it handles the error appropriately.
     */
    public String createSSMOpsItem(String title, String source, String category,
String severity) {
        CreateOpsItemRequest opsItemRequest = CreateOpsItemRequest.builder()
                .description("Created by the SSM Java API")
                .title(title)
                .source(source)
                .category(category)
                .severity(severity)
                .build();

        CompletableFuture<CreateOpsItemResponse> future =
getAsyncClient().createOpsItem(opsItemRequest);

        try {
            CreateOpsItemResponse response = future.join();
            return response.opsItemId();
        } catch (CompletionException e) {
            Throwable cause = e.getCause();
            if (cause instanceof SsmException) {
                throw (SsmException) cause;
            } else {
                throw new RuntimeException(cause);
            }
        }
    }

    /**
     * Displays the date and time when the specific command was invoked.
     *
     * @param commandId The ID of the command to describe.
     * <p>
```

```
    * This method initiates an asynchronous request to list command invocations
and prints the date and time of each command invocation.
    * If an exception occurs, it handles the error appropriately.
    */
   public void displayCommands(String commandId) {
       ListCommandInvocationsRequest commandInvocationsRequest =
ListCommandInvocationsRequest.builder()
               .commandId(commandId)
               .build();

       CompletableFuture<ListCommandInvocationsResponse> future =
getAsyncClient().listCommandInvocations(commandInvocationsRequest);
       future.thenAccept(response -> {
           List<CommandInvocation> commandList = response.commandInvocations();
           DateTimeFormatter formatter = DateTimeFormatter.ofPattern("yyyy-MM-dd
HH:mm:ss").withZone(ZoneId.systemDefault());
           for (CommandInvocation invocation : commandList) {
               System.out.println("The time of the command invocation is " +
formatter.format(invocation.requestedDateTime()));
           }
       }).exceptionally(ex -> {
           Throwable cause = (ex instanceof CompletionException) ?
ex.getCause() : ex;
           if (cause instanceof SsmException) {
               throw (SsmException) cause;
           } else {
               throw new RuntimeException(cause);
           }
       }).join();
   }

   /**
    * Sends a SSM command to a managed node asynchronously.
    *
    * @param documentName The name of the document to use.
    * @param instanceId The ID of the instance to send the command to.
    * @return The command ID.
    * <p>
    * This method initiates asynchronous requests to send a SSM command to a
managed node.
    * It waits until the document is active, sends the command, and checks the
command execution status.
    */
```

```
   public String sendSSMCommand(String documentName, String instanceId) throws
InterruptedException, SsmException {
       // Before we use Document to send a command - make sure it is active.
       CompletableFuture<Void> documentActiveFuture =
CompletableFuture.runAsync(() -> {
           boolean isDocumentActive = false;
           DescribeDocumentRequest request = DescribeDocumentRequest.builder()
                   .name(documentName)
                   .build();

           while (!isDocumentActive) {
               CompletableFuture<DescribeDocumentResponse> response =
getAsyncClient().describeDocument(request);
               String documentStatus =
response.join().document().statusAsString();
               if (documentStatus.equals("Active")) {
                   System.out.println("The SSM document is active and ready to
use.");
                   isDocumentActive = true;
               } else {
                   System.out.println("The SSM document is not active. Status: "
+ documentStatus);
                   try {
                       Thread.sleep(5000);
                   } catch (InterruptedException e) {
                       throw new RuntimeException(e);
                   }
               }
           }
       });

       documentActiveFuture.join();

       // Create the SendCommandRequest.
       SendCommandRequest commandRequest = SendCommandRequest.builder()
               .documentName(documentName)
               .instanceIds(instanceId)
               .build();

       // Send the command.
       CompletableFuture<SendCommandResponse> commandFuture =
getAsyncClient().sendCommand(commandRequest);
       final String[] commandId = {null};
```

```
        commandFuture.whenComplete((commandResponse, ex) -> {
            if (commandResponse != null) {
                commandId[0] = commandResponse.command().commandId();
                System.out.println("Command ID: " + commandId[0]);

                // Wait for the command execution to complete.
                GetCommandInvocationRequest invocationRequest =
GetCommandInvocationRequest.builder()
                        .commandId(commandId[0])
                        .instanceId(instanceId)
                        .build();

                try {
                    System.out.println("Wait 5 secs");
                    TimeUnit.SECONDS.sleep(5);

                    // Retrieve the command execution details.
                    CompletableFuture<GetCommandInvocationResponse>
invocationFuture = getAsyncClient().getCommandInvocation(invocationRequest);
                    invocationFuture.whenComplete((commandInvocationResponse,
invocationEx) -> {
                        if (commandInvocationResponse != null) {
                            // Check the status of the command execution.
                            CommandInvocationStatus status =
commandInvocationResponse.status();
                            if (status == CommandInvocationStatus.SUCCESS) {
                                System.out.println("Command execution
successful");
                            } else {
                                System.out.println("Command execution failed.
Status: " + status);
                            }
                        } else {
                            Throwable invocationCause = (invocationEx instanceof
CompletionException) ? invocationEx.getCause() : invocationEx;
                            throw new CompletionException(invocationCause);
                        }
                    }).join();
                } catch (InterruptedException e) {
                    throw new RuntimeException(e);
                }
            } else {
                Throwable cause = (ex instanceof CompletionException) ?
ex.getCause() : ex;
```

```
                if (cause instanceof SsmException) {
                    throw (SsmException) cause;
                } else {
                    throw new RuntimeException(cause);
                }
            }
        }).join();

        return commandId[0];
    }

    /**
     * Creates an AWS SSM document asynchronously.
     *
     * @param docName The name of the document to create.
     * <p>
     * This method initiates an asynchronous request to create an SSM document.
     * If the request is successful, it prints the document status.
     * If an exception occurs, it handles the error appropriately.
     */
    public void createSSMDoc(String docName) throws SsmException {
        String jsonData = """
        {
        "schemaVersion": "2.2",
        "description": "Run a simple shell command",
        "mainSteps": [
            {
                "action": "aws:runShellScript",
                "name": "runEchoCommand",
                "inputs": {
                  "runCommand": [
                    "echo 'Hello, world!'"
                  ]
                }
              }
            ]
        }
        """;

        CreateDocumentRequest request = CreateDocumentRequest.builder()
                .content(jsonData)
                .name(docName)
                .documentType(DocumentType.COMMAND)
                .build();
```

```
        CompletableFuture<CreateDocumentResponse> future =
getAsyncClient().createDocument(request);
        future.thenAccept(response -> {
            System.out.println("The status of the SSM document is " +
response.documentDescription().status());
        }).exceptionally(ex -> {
            Throwable cause = (ex instanceof CompletionException) ?
ex.getCause() : ex;
            if (cause instanceof DocumentAlreadyExistsException) {
                throw new CompletionException(cause);
            } else if (cause instanceof SsmException) {
                throw new CompletionException(cause);
            } else {
                throw new RuntimeException(cause);
            }
        }).join();
    }

    /**
     * Updates an SSM maintenance window asynchronously.
     *
     * @param id The ID of the maintenance window to update.
     * @param name The new name for the maintenance window.
     * <p>
     * This method initiates an asynchronous request to update an SSM maintenance
window.
     * If the request is successful, it prints a success message.
     * If an exception occurs, it handles the error appropriately.
     */
    public void updateSSMMaintenanceWindow(String id, String name) throws
SsmException {
        UpdateMaintenanceWindowRequest updateRequest =
UpdateMaintenanceWindowRequest.builder()
                .windowId(id)
                .allowUnassociatedTargets(true)
                .duration(24)
                .enabled(true)
                .name(name)
                .schedule("cron(0 0 ? * MON *)")
                .build();

        CompletableFuture<UpdateMaintenanceWindowResponse> future =
getAsyncClient().updateMaintenanceWindow(updateRequest);
```

```
        future.whenComplete((response, ex) -> {
            if (response != null) {
                System.out.println("The SSM maintenance window was successfully
updated");
            } else {
                Throwable cause = (ex instanceof CompletionException) ?
ex.getCause() : ex;
                if (cause instanceof SsmException) {
                    throw new CompletionException(cause);
                } else {
                    throw new RuntimeException(cause);
                }
            }
        }).join();
    }

    /**
     * Creates an SSM maintenance window asynchronously.
     *
     * @param winName The name of the maintenance window.
     * @return The ID of the created or existing maintenance window.
     * <p>
     * This method initiates an asynchronous request to create an SSM maintenance
window.
     * If the request is successful, it prints the maintenance window ID.
     * If an exception occurs, it handles the error appropriately.
     */
    public String createMaintenanceWindow(String winName) throws SsmException,
DocumentAlreadyExistsException {
        CreateMaintenanceWindowRequest request =
CreateMaintenanceWindowRequest.builder()
                .name(winName)
                .description("This is my maintenance window")
                .allowUnassociatedTargets(true)
                .duration(2)
                .cutoff(1)
                .schedule("cron(0 10 ? * MON-FRI *)")
                .build();

        CompletableFuture<CreateMaintenanceWindowResponse> future =
getAsyncClient().createMaintenanceWindow(request);
        final String[] windowId = {null};
        future.whenComplete((response, ex) -> {
            if (response != null) {
```

```
                String maintenanceWindowId = response.windowId();
                System.out.println("The maintenance window id is " +
maintenanceWindowId);
                windowId[0] = maintenanceWindowId;
            } else {
                Throwable cause = (ex instanceof CompletionException) ?
ex.getCause() : ex;
                if (cause instanceof DocumentAlreadyExistsException) {
                    throw new CompletionException(cause);
                } else if (cause instanceof SsmException) {
                    throw new CompletionException(cause);
                } else {
                    throw new RuntimeException(cause);
                }
            }
        }).join();

        if (windowId[0] == null) {
            MaintenanceWindowFilter filter = MaintenanceWindowFilter.builder()
                    .key("name")
                    .values(winName)
                    .build();

            DescribeMaintenanceWindowsRequest winRequest =
DescribeMaintenanceWindowsRequest.builder()
                    .filters(filter)
                    .build();

            CompletableFuture<DescribeMaintenanceWindowsResponse> describeFuture
= getAsyncClient().describeMaintenanceWindows(winRequest);
            describeFuture.whenComplete((describeResponse, describeEx) -> {
                if (describeResponse != null) {
                    List<MaintenanceWindowIdentity> windows =
describeResponse.windowIdentities();
                    if (!windows.isEmpty()) {
                        windowId[0] = windows.get(0).windowId();
                        System.out.println("Window ID: " + windowId[0]);
                    } else {
                        System.out.println("Window not found.");
                        windowId[0] = "";
                    }
                } else {
                    Throwable describeCause = (describeEx instanceof
CompletionException) ? describeEx.getCause() : describeEx;
```

```
                    throw new RuntimeException("Error describing maintenance
 windows: " + describeCause.getMessage(), describeCause);
                }
            }).join();
        }

        return windowId[0];
    }
}
```

- API の詳細については、『AWS SDK for Java 2.x API リファレンス』の以下のトピックを参照してください。
  - CreateDocument
  - CreateMaintenanceWindow
  - CreateOpsItem
  - DeleteMaintenanceWindow
  - ListCommandInvocations
  - SendCommand
  - UpdateOpsItem

JavaScript

SDK for JavaScript (v3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
import {
  Scenario,
  ScenarioAction,
  ScenarioInput,
  ScenarioOutput,
} from "@aws-doc-sdk-examples/lib/scenario/index.js";
import { fileURLToPath } from "node:url";
```

```
import {
  CreateDocumentCommand,
  CreateMaintenanceWindowCommand,
  CreateOpsItemCommand,
  DeleteDocumentCommand,
  DeleteMaintenanceWindowCommand,
  DeleteOpsItemCommand,
  DescribeOpsItemsCommand,
  DocumentAlreadyExists,
  OpsItemStatus,
  waitUntilCommandExecuted,
  CancelCommandCommand,
  paginateListCommandInvocations,
  SendCommandCommand,
  UpdateMaintenanceWindowCommand,
  UpdateOpsItemCommand,
  SSMClient,
} from "@aws-sdk/client-ssm";
import { parseArgs } from "node:util";

/**
 * @typedef {{
 *   ssmClient: import('@aws-sdk/client-ssm').SSMClient,
 *   documentName?: string
 *   maintenanceWindow?: string
 *   winId?: int
 *   ec2InstanceId?: string
 *   requestedDateTime?: Date
 *   opsItemId?: string
 *   askToDeleteResources?: boolean
 * }} State
 */

const defaultMaintenanceWindow = "ssm-maintenance-window";
const defaultDocumentName = "ssmdocument";
// The timeout duration is highly dependent on the specific setup and environment
 necessary. This example handles only the most common error cases, and uses a
 much shorter duration than most productions systems would use.
const COMMAND_TIMEOUT_DURATION_SECONDS = 30; // 30 seconds

const pressEnter = new ScenarioInput("continue", "Press Enter to continue", {
  type: "confirm",
});
```

```
const greet = new ScenarioOutput(
  "greet",
  `Welcome to the AWS Systems Manager SDK Getting Started scenario.
    This program demonstrates how to interact with Systems Manager using the AWS
 SDK for JavaScript V3.
    Systems Manager is the operations hub for your AWS applications and resources
 and a secure end-to-end management solution.
    The program's primary functions include creating a maintenance window,
 creating a document, sending a command to a document,
    listing documents, listing commands, creating an OpsItem, modifying an
 OpsItem, and deleting Systems Manager resources.
    Upon completion of the program, all AWS resources are cleaned up.
    Let's get started...`,
  { header: true },
);

const createMaintenanceWindow = new ScenarioOutput(
  "createMaintenanceWindow",
  "Step 1: Create a Systems Manager maintenance window.",
);

const getMaintenanceWindow = new ScenarioInput(
  "maintenanceWindow",
  "Please enter the maintenance window name:",
  { type: "input", default: defaultMaintenanceWindow },
);

export const sdkCreateMaintenanceWindow = new ScenarioAction(
  "sdkCreateMaintenanceWindow",
  async (/** @type {State} */ state) => {
    try {
      const response = await state.ssmClient.send(
        new CreateMaintenanceWindowCommand({
          Name: state.maintenanceWindow,
          Schedule: "cron(0 10 ? * MON-FRI *)", //The schedule of the maintenance
 window in the form of a cron or rate expression.
          Duration: 2, //The duration of the maintenance window in hours.
          Cutoff: 1, //The number of hours before the end of the maintenance
 window that Amazon Web Services Systems Manager stops scheduling new tasks for
 execution.
          AllowUnassociatedTargets: true, //Allow the maintenance window to run
 on managed nodes, even if you haven't registered those nodes as targets.
        }),
      );
```

```
      state.winId = response.WindowId;
    } catch (caught) {
      console.error(caught.message);
      console.log(
        `An error occurred while creating the maintenance window. Please fix the
 error and try again. Error message: ${caught.message}`,
      );
      throw caught;
    }
  },
);

const modifyMaintenanceWindow = new ScenarioOutput(
  "modifyMaintenanceWindow",
  "Modify the maintenance window by changing the schedule.",
);

const sdkModifyMaintenanceWindow = new ScenarioAction(
  "sdkModifyMaintenanceWindow",
  async (/** @type {State} */ state) => {
    try {
      await state.ssmClient.send(
        new UpdateMaintenanceWindowCommand({
          WindowId: state.winId,
          Schedule: "cron(0 0 ? * MON *)",
        }),
      );
    } catch (caught) {
      console.error(caught.message);
      console.log(
        `An error occurred while modifying the maintenance window. Please fix the
 error and try again. Error message: ${caught.message}`,
      );
      throw caught;
    }
  },
);

const createSystemsManagerActions = new ScenarioOutput(
  "createSystemsManagerActions",
  "Create a document that defines the actions that Systems Manager performs on
 your EC2 instance.",
);
```

```
const getDocumentName = new ScenarioInput(
  "documentName",
  "Please enter the document: ",
  { type: "input", default: defaultDocumentName },
);

const sdkCreateSSMDoc = new ScenarioAction(
  "sdkCreateSSMDoc",
  async (/** @type {State} */ state) => {
    const contentData = `{
                "schemaVersion": "2.2",
                "description": "Run a simple shell command",
                "mainSteps": [
                    {
                        "action": "aws:runShellScript",
                        "name": "runEchoCommand",
                        "inputs": {
                          "runCommand": [
                            "echo 'Hello, world!'"
                          ]
                        }
                    }
                ]
            }`;
    try {
      await state.ssmClient.send(
        new CreateDocumentCommand({
          Content: contentData,
          Name: state.documentName,
          DocumentType: "Command",
        }),
      );
    } catch (caught) {
      console.log(`Exception type: (${typeof caught})`);
      if (caught instanceof DocumentAlreadyExists) {
        console.log("Document already exists. Continuing...\n");
      } else {
        console.error(caught.message);
        console.log(
          `An error occurred while creating the document. Please fix the error
 and try again. Error message: ${caught.message}`,
        );
        throw caught;
      }
```

```
    }
  },
);

const ec2HelloWorld = new ScenarioOutput(
  "ec2HelloWorld",
  `Now you have the option of running a command on an EC2 instance that echoes
 'Hello, world!'. In order to run this command, you must provide the instance ID
 of a Linux EC2 instance. If you do not already have a running Linux EC2 instance
 in your account, you can create one using the AWS console. For information
 about creating an EC2 instance, see https://docs.aws.amazon.com/AWSEC2/latest/
UserGuide/ec2-launch-instance-wizard.html.`,
);

const enterIdOrSkipEC2HelloWorld = new ScenarioInput(
  "enterIdOrSkipEC2HelloWorld",
  "Enter your EC2 InstanceId or press enter to skip this step: ",
  { type: "input", default: "" },
);

const sdkEC2HelloWorld = new ScenarioAction(
  "sdkEC2HelloWorld",
  async (/** @type {State} */ state) => {
    try {
      const response = await state.ssmClient.send(
        new SendCommandCommand({
          DocumentName: state.documentName,
          InstanceIds: [state.ec2InstanceId],
          TimeoutSeconds: COMMAND_TIMEOUT_DURATION_SECONDS,
        }),
      );
      state.CommandId = response.Command.CommandId;
    } catch (caught) {
      console.error(caught.message);
      console.log(
        `An error occurred while sending the command. Please fix the error and
 try again. Error message: ${caught.message}`,
      );
      throw caught;
    }
  },
  {
    skipWhen: (/** @type {State} */ state) =>
      state.enterIdOrSkipEC2HelloWorld === "",
```

```
  },
);

const sdkGetCommandTime = new ScenarioAction(
  "sdkGetCommandTime",
  async (/** @type {State} */ state) => {
    const listInvocationsPaginated = [];
    console.log(
      "Let's get the time when the specific command was sent to the specific
 managed node.",
    );

    console.log(
      `First, we'll wait for the command to finish executing. This may take up to
 ${COMMAND_TIMEOUT_DURATION_SECONDS} seconds.`,
    );
    const commandExecutedResult = waitUntilCommandExecuted(
      { client: state.ssmClient },
      {
        CommandId: state.CommandId,
        InstanceId: state.ec2InstanceId,
      },
    );
    // This is necessary because the TimeoutSeconds of SendCommandCommand is only
 for the delivery, not execution.
    try {
      await new Promise((_, reject) =>
        setTimeout(
          reject,
          COMMAND_TIMEOUT_DURATION_SECONDS * 1000,
          new Error("Command Timed Out"),
        ),
      );
    } catch (caught) {
      if (caught.message === "Command Timed Out") {
        commandExecutedResult.state = "TIMED_OUT";
      } else {
        throw caught;
      }
    }

    if (commandExecutedResult.state !== "SUCCESS") {
      console.log(
```

```
        `The command with id: ${state.CommandId} did not execute in the allotted
 time. Canceling command.`,
      );
      state.ssmClient.send(
        new CancelCommandCommand({
          CommandId: state.CommandId,
        }),
      );
      state.enterIdOrSkipEC2HelloWorld === "";
      return;
    }

    for await (const page of paginateListCommandInvocations(
      { client: state.ssmClient },
      { CommandId: state.CommandId },
    )) {
      listInvocationsPaginated.push(...page.CommandInvocations);
    }
    /**
     * @type {import('@aws-sdk/client-ssm').CommandInvocation}
     */
    const commandInvocation = listInvocationsPaginated.shift(); // Because the
 call was made with CommandId, there's only one result, so shift it off.
    state.requestedDateTime = commandInvocation.RequestedDateTime;

    console.log(
      `The command invocation happened at: ${state.requestedDateTime}.`,
    );
  },
  {
    skipWhen: (/** @type {State} */ state) =>
      state.enterIdOrSkipEC2HelloWorld === "",
  },
);

const createSSMOpsItem = new ScenarioOutput(
  "createSSMOpsItem",
  `Now we will create a Systems Manager OpsItem. An OpsItem is a feature provided
 by the Systems Manager service. It is a type of operational data item that
 allows you to manage and track various operational issues, events, or tasks
 within your AWS environment.
You can create OpsItems to track and manage operational issues as they arise.
 For example, you could create an OpsItem whenever your application detects a
 critical error or an anomaly in your infrastructure.`,
```

```
);

const sdkCreateSSMOpsItem = new ScenarioAction(
  "sdkCreateSSMOpsItem",
  async (/** @type {State} */ state) => {
    try {
      const response = await state.ssmClient.send(
        new CreateOpsItemCommand({
          Description: "Created by the System Manager Javascript API",
          Title: "Disk Space Alert",
          Source: "EC2",
          Category: "Performance",
          Severity: "2",
        }),
      );
      state.opsItemId = response.OpsItemId;
    } catch (caught) {
      console.error(caught.message);
      console.log(
        `An error occurred while creating the ops item. Please fix the error and
 try again. Error message: ${caught.message}`,
      );
      throw caught;
    }
  },
);

const updateOpsItem = new ScenarioOutput(
  "updateOpsItem",
  (/** @type {State} */ state) =>
    `Now we will update the OpsItem: ${state.opsItemId}`,
);

const sdkUpdateOpsItem = new ScenarioAction(
  "sdkUpdateOpsItem",
  async (/** @type {State} */ state) => {
    try {
      const _response = await state.ssmClient.send(
        new UpdateOpsItemCommand({
          OpsItemId: state.opsItemId,
          Description: `An update to ${state.opsItemId}`,
        }),
      );
    } catch (caught) {
```

```
      console.error(caught.message);
      console.log(
        `An error occurred while updating the ops item. Please fix the error and
 try again. Error message: ${caught.message}`,
      );
      throw caught;
    }
  },
);

const getOpsItemStatus = new ScenarioOutput(
  "getOpsItemStatus",
  (/** @type {State} */ state) =>
    `Now we will get the status of the OpsItem: ${state.opsItemId}`,
);

const sdkOpsItemStatus = new ScenarioAction(
  "sdkGetOpsItemStatus",
  async (/** @type {State} */ state) => {
    try {
      const response = await state.ssmClient.send(
        new DescribeOpsItemsCommand({
          OpsItemId: state.opsItemId,
        }),
      );
      state.opsItemStatus = response.OpsItemStatus;
    } catch (caught) {
      console.error(caught.message);
      console.log(
        `An error occurred while describing the ops item. Please fix the error
 and try again. Error message: ${caught.message}`,
      );
      throw caught;
    }
  },
);

const resolveOpsItem = new ScenarioOutput(
  "resolveOpsItem",
  (/** @type {State} */ state) =>
    `Now we will resolve the OpsItem: ${state.opsItemId}`,
);

const sdkResolveOpsItem = new ScenarioAction(
```

```
  "sdkResolveOpsItem",
  async (/** @type {State} */ state) => {
    try {
      const _response = await state.ssmClient.send(
        new UpdateOpsItemCommand({
          OpsItemId: state.opsItemId,
          Status: OpsItemStatus.RESOLVED,
        }),
      );
    } catch (caught) {
      console.error(caught.message);
      console.log(
        `An error occurred while updating the ops item. Please fix the error and
 try again. Error message: ${caught.message}`,
      );
      throw caught;
    }
  },
);

const askToDeleteResources = new ScenarioInput(
  "askToDeleteResources",
  "Would you like to delete the Systems Manager resources created during this
 example run?",
  { type: "confirm" },
);

const confirmDeleteChoice = new ScenarioOutput(
  "confirmDeleteChoice",
  (/** @type {State} */ state) => {
    if (state.askToDeleteResources) {
      return "You chose to delete the resources.";
    }
    return "The Systems Manager resources will not be deleted. Please delete them
 manually to avoid charges.";
  },
);

export const sdkDeleteResources = new ScenarioAction(
  "sdkDeleteResources",
  async (/** @type {State} */ state) => {
    try {
      await state.ssmClient.send(
        new DeleteOpsItemCommand({
```

```
          OpsItemId: state.opsItemId,
        }),
      );
      console.log(`The ops item: ${state.opsItemId} was successfully deleted.`);
    } catch (caught) {
      console.log(
        `There was a problem deleting the ops item: ${state.opsItemId}. Please
delete it manually. Error: ${caught.message}`,
      );
    }

    try {
      await state.ssmClient.send(
        new DeleteMaintenanceWindowCommand({
          Name: state.maintenanceWindow,
          WindowId: state.winId,
        }),
      );
      console.log(
        `The maintenance window: ${state.maintenanceWindow} was successfully
deleted.`,
      );
    } catch (caught) {
      console.log(
        `There was a problem deleting the maintenance window: ${state.opsItemId}.
Please delete it manually. Error: ${caught.message}`,
      );
    }

    try {
      await state.ssmClient.send(
        new DeleteDocumentCommand({
          Name: state.documentName,
        }),
      );
      console.log(
        `The document: ${state.documentName} was successfully deleted.`,
      );
    } catch (caught) {
      console.log(
        `There was a problem deleting the document: ${state.documentName}. Please
delete it manually. Error: ${caught.message}`,
      );
    }
```

```
  },
  { skipWhen: (/** @type {{}} */ state) => !state.askToDeleteResources },
);

const goodbye = new ScenarioOutput(
  "goodbye",
  "This concludes the Systems Manager Basics scenario for the AWS Javascript SDK
 v3. Thank you!",
);

const myScenario = new Scenario(
  "SSM Basics",
  [
    greet,
    pressEnter,
    createMaintenanceWindow,
    getMaintenanceWindow,
    sdkCreateMaintenanceWindow,
    modifyMaintenanceWindow,
    pressEnter,
    sdkModifyMaintenanceWindow,
    createSystemsManagerActions,
    getDocumentName,
    sdkCreateSSMDoc,
    ec2HelloWorld,
    enterIdOrSkipEC2HelloWorld,
    sdkEC2HelloWorld,
    sdkGetCommandTime,
    pressEnter,
    createSSMOpsItem,
    pressEnter,
    sdkCreateSSMOpsItem,
    updateOpsItem,
    pressEnter,
    sdkUpdateOpsItem,
    getOpsItemStatus,
    pressEnter,
    sdkOpsItemStatus,
    resolveOpsItem,
    pressEnter,
    sdkResolveOpsItem,
    askToDeleteResources,
    confirmDeleteChoice,
    sdkDeleteResources,
```

```
    goodbye,
  ],
  { ssmClient: new SSMClient({}) },
);

/** @type {{ stepHandlerOptions: StepHandlerOptions }} */
export const main = async (stepHandlerOptions) => {
  await myScenario.run(stepHandlerOptions);
};

// Invoke main function if this file was run directly.
if (process.argv[1] === fileURLToPath(import.meta.url)) {
  const { values } = parseArgs({
    options: {
      yes: {
        type: "boolean",
        short: "y",
      },
    },
  });
  main({ confirmAll: values.yes });
}
```

- API の詳細については、『AWS SDK for JavaScript API リファレンス』の以下のトピックを参照してください。
  - CreateDocument
  - CreateMaintenanceWindow
  - CreateOpsItem
  - DeleteMaintenanceWindow
  - ListCommandInvocations
  - SendCommand
  - UpdateOpsItem

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

コマンドプロンプトからインタラクティブのシナリオを実行します。

```
class SystemsManagerScenario:
    """Runs an interactive scenario that shows how to get started using Amazon
 Systems Manager."""

    def __init__(self, document_wrapper, maintenance_window_wrapper,
 ops_item_wrapper):
        """
        :param document_wrapper: An object that wraps Systems Manager document
 functions.
        :param maintenance_window_wrapper: An object that wraps Systems Manager
 maintenance window functions.
        :param ops_item_wrapper: An object that wraps Systems Manager OpsItem
 functions.
        """
        self.document_wrapper = document_wrapper
        self.maintenance_window_wrapper = maintenance_window_wrapper
        self.ops_item_wrapper = ops_item_wrapper

    def run(self):
        """Demonstrates how to use the AWS SDK for Python (Boto3) to get started
 with Systems Manager."""
        try:
            print("-" * 88)
            print(
                """
Welcome to the AWS Systems Manager SDK Getting Started scenario.
This program demonstrates how to interact with Systems Manager using the AWS SDK
 for Python (Boto3).
Systems Manager is the operations hub for your AWS applications and resources and
 a secure end-to-end management
```

```
solution. The program's primary functions include creating a maintenance window,
 creating a document, sending a
command to a document, listing documents, listing commands, creating an OpsItem,
 modifying an OpsItem, and deleting
Systems Manager resources. Upon completion of the program, all AWS resources are
 cleaned up.
Let's get started..."""
            )
            q.ask("Please hit Enter")

            print("-" * 88)
            print("Create a Systems Manager maintenance window.")
            maintenance_window_name = q.ask(
                "Please enter the maintenance window name (default is ssm-
maintenance-window):",
            )
            if not maintenance_window_name:
                maintenance_window_name = "ssm-maintenance-window"

            self.maintenance_window_wrapper.create(
                name=maintenance_window_name,
                schedule="cron(0 10 ? * MON-FRI *)",
                duration=2,
                cutoff=1,
                allow_unassociated_targets=True,
            )

            print("-" * 88)
            print("Modify the maintenance window by changing the schedule")
            q.ask("Please hit Enter")

            self.maintenance_window_wrapper.update(
                name=maintenance_window_name,
                schedule="cron(0 0 ? * MON *)",
                duration=24,
                cutoff=1,
                allow_unassociated_targets=True,
                enabled=True,
            )

            print("-" * 88)
            print(
                "Create a document that defines the actions that Systems Manager
 performs on your EC2 instance."
```

```
            )
            document_name = q.ask(
                "Please enter the document name (default is ssmdocument):"
            )

            if not document_name:
                document_name = "ssmdocument"

            self.document_wrapper.create(
                name=document_name,
                content="""
{
    "schemaVersion": "2.2",
    "description": "Run a simple shell command",
    "mainSteps": [
        {
            "action": "aws:runShellScript",
            "name": "runEchoCommand",
            "inputs": {
              "runCommand": [
                "echo 'Hello, world!'"
              ]
            }
        }
    ]
}
            """,
            )

            self.document_wrapper.wait_until_active()

            print(
                """
Now you have the option of running a command on an EC2 instance that echoes
 'Hello, world!'.
In order to run this command, you must provide the instance ID of a Linux EC2
 instance. If you do
not already have a running Linux EC2 instance in your account, you can create one
 using the AWS console.
For information about creating an EC2 instance, see
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-launch-instance-
wizard.html.
            """
            )
```

```
            if q.ask(
                "Would you like to run a command on an EC2 instance? (y/n)",
                q.is_yesno,
            ):
                instance_id = q.ask(
                    "Please enter the instance ID of the EC2 instance:",
 q.non_empty
                )
                command_id = self.document_wrapper.send_command(
                    instance_ids=[instance_id]
                )

                self.document_wrapper.wait_command_executed(
                    command_id=command_id, instance_id=instance_id
                )

                print("-" * 88)
                print(
                    "Lets get the time when the specific command was sent to the
 specific managed node"
                )
                q.ask("Please hit Enter")


 self.document_wrapper.list_command_invocations(instance_id=instance_id)

            print("-" * 88)
            print("-" * 88)
            print(
                """
Now we will create a  Systems Manager OpsItem.
An OpsItem is a feature provided by the Systems Manager service.
It is a type of operational data item that allows you to manage and track various
 operational issues,
events, or tasks within your AWS environment.

You can create OpsItems to track and manage operational issues as they arise.
For example, you could create an OpsItem whenever your application detects a
 critical error
or an anomaly in your infrastructure.
            """
            )
            q.ask("Please hit Enter")
```

```
            self.ops_item_wrapper.create(
                title="Disk Space Alert",
                description="Created by the Systems Manager Python (Boto3) API",
                source="EC2",
                category="Performance",
                severity="2",
            )

            print("-" * 88)
            print("-" * 88)
            print(f"Now we will update  the OpsItem {self.ops_item_wrapper.id}")
            q.ask("Please hit Enter")

            self.ops_item_wrapper.update(
                title="Disk Space Alert",
                description=f"An update to {self.ops_item_wrapper.id}",
            )

            print(
                f"Now we will get the status of the OpsItem
{self.ops_item_wrapper.id}"
            )
            q.ask("Please hit Enter")

            # It may take a second for the ops item to be available
            counter = 0
            while not self.ops_item_wrapper.describe() and counter < 5:
                counter += 1
                time.sleep(1)

            print(f"Now we will resolve the OpsItem {self.ops_item_wrapper.id}")
            q.ask("Please hit Enter")

            self.ops_item_wrapper.update(status="Resolved")

            print("-" * 88)
            print("-" * 88)
            if q.ask(
                "Would you like to delete the Systems Manager resources? (y/n)",
                q.is_yesno,
            ):
                print("You selected to delete the resources.")
                self.cleanup()
```

```
            else:
                print("The Systems Manager resources will not be deleted")

            print("-" * 88)
            print("This concludes the Systems Manager SDK Getting Started
 scenario.")
            print("-" * 88)

        except Exception:
            self.cleanup()
            raise

    def cleanup(self):
        self.maintenance_window_wrapper.delete()
        self.ops_item_wrapper.delete()
        self.document_wrapper.delete()


if __name__ == "__main__":
    try:
        scenario = SystemsManagerScenario(
            DocumentWrapper.from_client(),
            MaintenanceWindowWrapper.from_client(),
            OpsItemWrapper.from_client(),
        )
        scenario.run()
    except Exception:
        logging.exception("Something went wrong with the demo.")
```

ドキュメントとコマンドのアクションをラップするクラスを定義します。

```
class DocumentWrapper:
    """Encapsulates AWS Systems Manager Document actions."""

    def __init__(self, ssm_client):
        """
        :param ssm_client: A Boto3 Systems Manager client.
        """
        self.ssm_client = ssm_client
        self.name = None

    @classmethod
```

```
    def from_client(cls):
        ssm_client = boto3.client("ssm")
        return cls(ssm_client)


    def create(self, content, name):
        """
        Creates a document.

        :param content: The content of the document.
        :param name: The name of the document.
        """
        try:
            self.ssm_client.create_document(
                Name=name, Content=content, DocumentType="Command"
            )
            self.name = name
        except self.ssm_client.exceptions.DocumentAlreadyExists:
            print(f"Document {name} already exists.")
            self.name = name
        except ClientError as err:
            logger.error(
                "Couldn't create %s. Here's why: %s: %s",
                name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise


    def delete(self):
        """
        Deletes an AWS Systems Manager document.
        """
        if self.name is None:
            return

        try:
            self.ssm_client.delete_document(Name=self.name)
            print(f"Deleted document {self.name}.")
            self.name = None
        except ClientError as err:
            logger.error(
                "Couldn't delete %s. Here's why: %s: %s",
```

```
                self.name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise


    def send_command(self, instance_ids):
        """
        Sends a command to one or more instances.

        :param instance_ids: The IDs of the instances to send the command to.
        :return: The ID of the command.
        """
        try:
            response = self.ssm_client.send_command(
                InstanceIds=instance_ids, DocumentName=self.name,
TimeoutSeconds=3600
            )
            return response["Command"]["CommandId"]
        except ClientError as err:
            logger.error(
                "Couldn't send command to %s. Here's why: %s: %s",
                self.name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise


    def describe(self):
        """
        Describes the document.

        :return: Document status.
        """
        try:
            response = self.ssm_client.describe_document(Name=self.name)
            return response["Document"]["Status"]
        except ClientError as err:
            logger.error(
                "Couldn't get %s. Here's why: %s: %s",
                self.name,
                err.response["Error"]["Code"],
```

```
                err.response["Error"]["Message"],
            )
            raise


    def wait_until_active(self, max_attempts=20, delay=5):
        """
        Waits until the document is active.

        :param max_attempts: The maximum number of attempts for checking the
status.
        :param delay: The delay in seconds between each check.
        """
        attempt = 0
        status = ""
        while attempt <= max_attempts:
            status = self.describe()
            if status == "Active":
                break
            attempt += 1
            time.sleep(delay)

        if status != "Active":
            logger.error("Document is not active.")
        else:
            logger.info("Document is active.")

    def wait_command_executed(self, command_id, instance_id):
        """
        Waits until the command is executed on the instance.

        :param command_id: The ID of the command.
        :param instance_id: The ID of the instance.
        """

        waiter = self.ssm_client.get_waiter("command_executed")
        waiter.wait(CommandId=command_id, InstanceId=instance_id)

    def list_command_invocations(self, instance_id):
        """
        Lists the commands for an instance.

        :param instance_id: The ID of the instance.
        :return: The list of commands.
```

```
        """
        try:
            paginator = self.ssm_client.get_paginator("list_command_invocations")
            command_invocations = []
            for page in paginator.paginate(InstanceId=instance_id):
                command_invocations.extend(page["CommandInvocations"])
            num_of_commands = len(command_invocations)
            print(
                f"{num_of_commands} command invocation(s) found for instance
{instance_id}."
            )

            if num_of_commands > 10:
                print("Displaying the first 10 commands:")
                num_of_commands = 10
            date_format = "%A, %d %B %Y %I:%M%p"
            for command in command_invocations[:num_of_commands]:
                print(
                    f"   The time of command invocation is
{command['RequestedDateTime'].strftime(date_format)}"
                )
        except ClientError as err:
            logger.error(
                "Couldn't list commands for %s. Here's why: %s: %s",
                instance_id,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
```

Ops 項目のアクションをラップするクラスを定義します。

```
class OpsItemWrapper:
    """Encapsulates AWS Systems Manager OpsItem actions."""

    def __init__(self, ssm_client):
        """
        :param ssm_client: A Boto3 Systems Manager client.
        """
```

```
        self.ssm_client = ssm_client
        self.id = None

    @classmethod
    def from_client(cls):
        """
        :return: A OpsItemWrapper instance.
        """
        ssm_client = boto3.client("ssm")
        return cls(ssm_client)


    def create(self, title, source, category, severity, description):
        """
        Create an OpsItem

        :param title: The OpsItem title.
        :param source: The OpsItem source.
        :param category: The OpsItem category.
        :param severity: The OpsItem severity.
        :param description: The OpsItem description.

        """
        try:
            response = self.ssm_client.create_ops_item(
                Title=title,
                Source=source,
                Category=category,
                Severity=severity,
                Description=description,
            )
            self.id = response["OpsItemId"]
        except self.ssm_client.exceptions.OpsItemLimitExceededException as err:
            logger.error(
                "Couldn't create ops item because you have exceeded your open
OpsItem limit. "
                "Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        except ClientError as err:
            logger.error(
                "Couldn't create ops item %s. Here's why: %s: %s",
```

```
                title,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise

    def delete(self):
        """
        Delete the OpsItem.
        """
        if self.id is None:
            return
        try:
            self.ssm_client.delete_ops_item(OpsItemId=self.id)
            print(f"Deleted ops item with id {self.id}")
            self.id = None
        except ClientError as err:
            logger.error(
                "Couldn't delete ops item %s. Here's why: %s: %s",
                self.id,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise


    def describe(self):
        """
        Describe an OpsItem.
        """
        try:
            paginator = self.ssm_client.get_paginator("describe_ops_items")
            ops_items = []
            for page in paginator.paginate(
                OpsItemFilters=[
                    {"Key": "OpsItemId", "Values": [self.id], "Operator":
"Equal"}
                ]
            ):
                ops_items.extend(page["OpsItemSummaries"])

            for item in ops_items:
                print(
```

```
                    f"The item title is {item['Title']} and the status is
{item['Status']}"
                )
            return len(ops_items) > 0
        except ClientError as err:
            logger.error(
                "Couldn't describe ops item %s. Here's why: %s: %s",
                self.id,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise


    def update(self, title=None, description=None, status=None):
        """
        Update an OpsItem.

        :param title: The new OpsItem title.
        :param description: The new OpsItem description.
        :param status: The new OpsItem status.
        :return:
        """
        args = dict(OpsItemId=self.id)
        if title is not None:
            args["Title"] = title
        if description is not None:
            args["Description"] = description
        if status is not None:
            args["Status"] = status
        try:
            self.ssm_client.update_ops_item(**args)
        except ClientError as err:
            logger.error(
                "Couldn't update ops item %s. Here's why: %s: %s",
                self.id,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
```

メンテナンスウィンドウのアクションをラップするクラスを定義します。

```
class MaintenanceWindowWrapper:
    """Encapsulates AWS Systems Manager maintenance window actions."""

    def __init__(self, ssm_client):
        """
        :param ssm_client: A Boto3 Systems Manager client.
        """
        self.ssm_client = ssm_client
        self.window_id = None
        self.name = None

    @classmethod
    def from_client(cls):
        ssm_client = boto3.client("ssm")
        return cls(ssm_client)


    def create(self, name, schedule, duration, cutoff,
 allow_unassociated_targets):
        """
        Create an AWS Systems Manager maintenance window.

        :param name: The name of the maintenance window.
        :param schedule: The schedule of the maintenance window.
        :param duration: The duration of the maintenance window.
        :param cutoff: The cutoff time of the maintenance window.
        :param allow_unassociated_targets: Allow the maintenance window to run on
 managed nodes, even
                                           if you haven't registered those nodes
 as targets.
        """
        try:
            response = self.ssm_client.create_maintenance_window(
                Name=name,
                Schedule=schedule,
                Duration=duration,
                Cutoff=cutoff,
                AllowUnassociatedTargets=allow_unassociated_targets,
            )
```

```
            self.window_id = response["WindowId"]
            self.name = name
            logger.info("Created maintenance window %s.", self.window_id)
        except ParamValidationError as error:
            logger.error(
                "Parameter validation error when trying to create maintenance
window %s. Here's why: %s",
                self.window_id,
                error,
            )
            raise
        except ClientError as err:
            logger.error(
                "Couldn't create maintenance window %s. Here's why: %s: %s",
                name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise


    def delete(self):
        """
        Delete the associated AWS Systems Manager maintenance window.
        """
        if self.window_id is None:
            return

        try:
            self.ssm_client.delete_maintenance_window(WindowId=self.window_id)
            logger.info("Deleted maintenance window %s.", self.window_id)
            print(f"Deleted maintenance window {self.name}")
            self.window_id = None
        except ClientError as err:
            logger.error(
                "Couldn't delete maintenance window %s. Here's why: %s: %s",
                self.window_id,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise


    def update(
```

```
        self, name, enabled, schedule, duration, cutoff,
allow_unassociated_targets
    ):
        """
        Update an AWS Systems Manager maintenance window.

        :param name: The name of the maintenance window.
        :param enabled: Whether the maintenance window is enabled to run on
managed nodes.
        :param schedule: The schedule of the maintenance window.
        :param duration: The duration of the maintenance window.
        :param cutoff: The cutoff time of the maintenance window.
        :param allow_unassociated_targets: Allow the maintenance window to run on
managed nodes, even
                                           if you haven't registered those nodes
as targets.
        """
        try:
            self.ssm_client.update_maintenance_window(
                WindowId=self.window_id,
                Name=name,
                Enabled=enabled,
                Schedule=schedule,
                Duration=duration,
                Cutoff=cutoff,
                AllowUnassociatedTargets=allow_unassociated_targets,
            )
            self.name = name
            logger.info("Updated maintenance window %s.", self.window_id)
        except ParamValidationError as error:
            logger.error(
                "Parameter validation error when trying to update maintenance
window %s. Here's why: %s",
                self.window_id,
                error,
            )
            raise
        except ClientError as err:
            logger.error(
                "Couldn't update maintenance window %s. Here's why: %s: %s",
                self.name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
```

```
            raise
```

- API の詳細については、『AWS SDK for Python (Boto3) API リファレンス』の以下のトピックを参照してください。
  - CreateDocument
  - CreateMaintenanceWindow
  - CreateOpsItem
  - DeleteMaintenanceWindow
  - ListCommandInvocations
  - SendCommand
  - UpdateOpsItem

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK を使用する Secrets Manager のアクション

次のコード例は、AWS SDK で個々の Systems Manager アクションを実行する方法を示しています。それぞれの例には、GitHub へのリンクがあり、そこにはコードの設定と実行に関する説明が記載されています。

以下の例には、最も一般的に使用されるアクションのみ含まれています。詳細な一覧については、「AWS Systems Manager API リファレンス」を参照してください。

例

- CLI で AddTagsToResource を使用する
- CLI で CancelCommand を使用する
- CLI で CreateActivation を使用する
- CLI で CreateAssociation を使用する
- CLI で CreateAssociationBatch を使用する
- AWS SDK または CLI で CreateDocument を使用する
- AWS SDK または CLI で CreateMaintenanceWindow を使用する

- AWS SDK または CLI で CreateOpsItem を使用する
- CLI で CreatePatchBaseline を使用する
- CLI で DeleteActivation を使用する
- CLI で DeleteAssociation を使用する
- AWS SDK または CLI で DeleteDocument を使用する
- AWS SDK または CLI で DeleteMaintenanceWindow を使用する
- AWS SDK で DeleteOpsItem を使用する
- CLI で DeleteParameter を使用する
- CLI で DeletePatchBaseline を使用する
- CLI で DeregisterManagedInstance を使用する
- CLI で DeregisterPatchBaselineForPatchGroup を使用する
- CLI で DeregisterTargetFromMaintenanceWindow を使用する
- CLI で DeregisterTaskFromMaintenanceWindow を使用する
- CLI で DescribeActivations を使用する
- CLI で DescribeAssociation を使用する
- CLI で DescribeAssociationExecutionTargets を使用する
- CLI で DescribeAssociationExecutions を使用する
- CLI で DescribeAutomationExecutions を使用する
- CLI で DescribeAutomationStepExecutions を使用する
- CLI で DescribeAvailablePatches を使用する
- CLI で DescribeDocument を使用する
- CLI で DescribeDocumentPermission を使用する
- CLI で DescribeEffectiveInstanceAssociations を使用する
- CLI で DescribeEffectivePatchesForPatchBaseline を使用する
- CLI で DescribeInstanceAssociationsStatus を使用する
- CLI で DescribeInstanceInformation を使用する
- CLI で DescribeInstancePatchStates を使用する
- CLI で DescribeInstancePatchStatesForPatchGroup を使用する
- CLI で DescribeInstancePatches を使用する

- CLI で DescribeMaintenanceWindowExecutionTaskInvocations を使用する
- CLI で DescribeMaintenanceWindowExecutionTasks を使用する
- CLI で DescribeMaintenanceWindowExecutions を使用する
- CLI で DescribeMaintenanceWindowTargets を使用する
- CLI で DescribeMaintenanceWindowTasks を使用する
- CLI で DescribeMaintenanceWindows を使用する
- AWS SDK または CLI で DescribeOpsItems を使用する
- AWS SDK または CLI で DescribeParameters を使用する
- CLI で DescribePatchBaselines を使用する
- CLI で DescribePatchGroupState を使用する
- CLI で DescribePatchGroups を使用する
- CLI で GetAutomationExecution を使用する
- CLI で GetCommandInvocation を使用する
- CLI で GetConnectionStatus を使用する
- CLI で GetDefaultPatchBaseline を使用する
- CLI で GetDeployablePatchSnapshotForInstance を使用する
- CLI で GetDocument を使用する
- CLI で GetInventory を使用する
- CLI で GetInventorySchema を使用する
- CLI で GetMaintenanceWindow を使用する
- CLI で GetMaintenanceWindowExecution を使用する
- CLI で GetMaintenanceWindowExecutionTask を使用する
- AWS SDK または CLI で GetParameter を使用する
- CLI で GetParameterHistory を使用する
- CLI で GetParameters を使用する
- CLI で GetPatchBaseline を使用する
- CLI で GetPatchBaselineForPatchGroup を使用する
- CLI で ListAssociationVersions を使用する
- CLI で ListAssociations を使用する

- AWS SDK または CLI で ListCommandInvocations を使用する
- CLI で ListCommands を使用する
- CLI で ListComplianceItems を使用する
- CLI で ListComplianceSummaries を使用する
- CLI で ListDocumentVersions を使用する
- CLI で ListDocuments を使用する
- CLI で ListInventoryEntries を使用する
- CLI で ListResourceComplianceSummaries を使用する
- CLI で ListTagsForResource を使用する
- CLI で ModifyDocumentPermission を使用する
- CLI で PutComplianceItems を使用する
- CLI で PutInventory を使用する
- AWS SDK または CLI で PutParameter を使用する
- CLI で RegisterDefaultPatchBaseline を使用する
- CLI で RegisterPatchBaselineForPatchGroup を使用する
- CLI で RegisterTargetWithMaintenanceWindow を使用する
- CLI で RegisterTaskWithMaintenanceWindow を使用する
- CLI で RemoveTagsFromResource を使用する
- AWS SDK または CLI で SendCommand を使用する
- CLI で StartAutomationExecution を使用する
- CLI で StartSession を使用する
- CLI で StopAutomationExecution を使用する
- CLI で UpdateAssociation を使用する
- CLI で UpdateAssociationStatus を使用する
- CLI で UpdateDocument を使用する
- CLI で UpdateDocumentDefaultVersion を使用する
- AWS SDK または CLI で UpdateMaintenanceWindow を使用する
- CLI で UpdateManagedInstanceRole を使用する
- AWS SDK または CLI で UpdateOpsItem を使用する
- CLI で UpdatePatchBaseline を使用する

CLI で **AddTagsToResource** を使用する

次のサンプルコードは、AddTagsToResource を使用する方法を説明しています。

CLI

AWS CLI

例 1: メンテナンスウィンドウにタグを追加するには

次の add-tags-to-resource の例では、指定されたメンテナンスウィンドウにタグを追加します。

```
aws ssm add-tags-to-resource \
    --resource-type "MaintenanceWindow" \
    --resource-id "mw-03eb9db428EXAMPLE" \
    --tags "Key=Stack,Value=Production"
```

このコマンドでは何も出力されません。

例 2: パラメータにタグを追加するには

次の add-tags-to-resource の例では、指定されたパラメータに 2 つのタグを追加します。

```
aws ssm add-tags-to-resource \
    --resource-type "Parameter" \
    --resource-id "My-Parameter" \
    --tags '[{"Key":"Region","Value":"East"},{"Key":"Environment",
 "Value":"Production"}]'
```

このコマンドでは何も出力されません。

例 3: SSM ドキュメントにタグを追加するには

次の add-tags-to-resource の例では、指定されたドキュメントにタグを追加します。

```
aws ssm add-tags-to-resource \
    --resource-type "Document" \
    --resource-id "My-Document" \
    --tags "Key=Quarter,Value=Q322"
```

このコマンドでは何も出力されません。

詳細については、「AWS Systems Manager ユーザーガイド」の「Systems Manager リソースにタグを付ける」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「AddTagsToResource」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、新しいタグを使用してメンテナンスウィンドウを更新します。コマンドが成功した場合、出力はありません。この例で使用される構文には、PowerShell バージョン 3 以降が必要です。

```
$option1 = @{Key="Stack";Value=@("Production")}
Add-SSMResourceTag -ResourceId "mw-03eb9db42890fb82d" -ResourceType
 "MaintenanceWindow" -Tag $option1
```

例 2: PowerShell バージョン 2 では、New-Object を使用して各タグを作成する必要があります。コマンドが成功した場合、出力はありません。

```
$tag1 = New-Object Amazon.SimpleSystemsManagement.Model.Tag
$tag1.Key = "Stack"
$tag1.Value = "Production"

Add-SSMResourceTag -ResourceId "mw-03eb9db42890fb82d" -ResourceType
 "MaintenanceWindow" -Tag $tag1
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「AddTagsToResource」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **CancelCommand** を使用する

次のサンプルコードは、CancelCommand を使用する方法を説明しています。

CLI

AWS CLI

例 1: すべてのインスタンスのコマンドをキャンセルするには

次の cancel-command の例では、すべてのインスタンスで既に実行されている、指定されたコマンドのキャンセルを試みます。

```
aws ssm cancel-command \
    --command-id "662add3d-5831-4a10-b64a-f2ff3EXAMPLE"
```

このコマンドでは何も出力されません。

例 2: 特定のインスタンスのコマンドをキャンセルするには

次の cancel-command の例では、指定されたインスタンスに対してのみ実行するコマンドのキャンセルを試みます。

```
aws ssm cancel-command \
    --command-id "662add3d-5831-4a10-b64a-f2ff3EXAMPLE"
    --instance-ids "i-02573cafcfEXAMPLE"
```

このコマンドでは何も出力されません。

詳細については、「AWS Systems Manager ユーザーガイド」の「Systems Manager パラメータにタグをつける」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「CancelCommand」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、コマンドのキャンセルを試みます。オペレーションが成功した場合、出力はありません。

```
Stop-SSMCommand -CommandId "9ded293e-e792-4440-8e3e-7b8ec5feaa38"
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「CancelCommand」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **CreateActivation** を使用する

次のサンプルコードは、CreateActivation を使用する方法を説明しています。

CLI

AWS CLI

マネージドインスタンスのアクティベーションを作成するには

次の create-activation の例では、マネージドインスタンスのアクティベーションを作成します。

```
aws ssm create-activation \
    --default-instance-name "HybridWebServers" \
    --iam-role "HybridWebServersRole" \
    --registration-limit 5
```

出力:

```
{
    "ActivationId": "5743558d-563b-4457-8682-d16c3EXAMPLE",
    "ActivationCode": "dRmgnYaFv567vEXAMPLE"
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「Step 4: Create a Managed-Instance Activation for a Hybrid Environment」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「CreateActivation」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、マネージドインスタンスを作成します。

```
New-SSMActivation -DefaultInstanceName "MyWebServers" -IamRole
 "SSMAutomationRole" -RegistrationLimit 10
```

出力:

```
ActivationCode       ActivationId
--------------       ------------
KWChhOxBTiwDcKE9BlKC 08e51e79-1e36-446c-8e63-9458569c1363
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「CreateActivation」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **CreateAssociation** を使用する

次のサンプルコードは、CreateAssociation を使用する方法を説明しています。

CLI

AWS CLI

例 1: インスタンス ID を使用してドキュメントを関連付けるには

この例では、インスタンス ID を使用して、設定ドキュメントをインスタンスに関連付けます。

```
aws ssm create-association \
    --instance-id "i-0cb2b964d3e14fd9f" \
    --name "AWS-UpdateSSMAgent"
```

出力:

```
{
    "AssociationDescription": {
        "Status": {
            "Date": 1487875500.33,
            "Message": "Associated with AWS-UpdateSSMAgent",
            "Name": "Associated"
```

```
        },
        "Name": "AWS-UpdateSSMAgent",
        "InstanceId": "i-0cb2b964d3e14fd9f",
        "Overview": {
            "Status": "Pending",
            "DetailedStatus": "Creating"
        },
        "AssociationId": "b7c3266e-a544-44db-877e-b20d3a108189",
        "DocumentVersion": "$DEFAULT",
        "LastUpdateAssociationDate": 1487875500.33,
        "Date": 1487875500.33,
        "Targets": [
            {
                "Values": [
                    "i-0cb2b964d3e14fd9f"
                ],
                "Key": "InstanceIds"
            }
        ]
    }
}
```

詳細については、「AWS Systems Manager API リファレンス」の「CreateAssociation」を参照してください。

例 2: ターゲットを使用してドキュメントを関連付けるには

この例では、ターゲットを使用して、設定ドキュメントをインスタンスに関連付けます。

```
aws ssm create-association \
    --name "AWS-UpdateSSMAgent" \
    --targets "Key=instanceids,Values=i-0cb2b964d3e14fd9f"
```

出力:

```
{
    "AssociationDescription": {
        "Status": {
            "Date": 1487875500.33,
            "Message": "Associated with AWS-UpdateSSMAgent",
            "Name": "Associated"
        },
        "Name": "AWS-UpdateSSMAgent",
```

```
        "InstanceId": "i-0cb2b964d3e14fd9f",
        "Overview": {
            "Status": "Pending",
            "DetailedStatus": "Creating"
        },
        "AssociationId": "b7c3266e-a544-44db-877e-b20d3a108189",
        "DocumentVersion": "$DEFAULT",
        "LastUpdateAssociationDate": 1487875500.33,
        "Date": 1487875500.33,
        "Targets": [
            {
                "Values": [
                    "i-0cb2b964d3e14fd9f"
                ],
                "Key": "InstanceIds"
            }
        ]
    }
}
```

詳細については、「AWS Systems Manager API リファレンス」の「CreateAssociation」を参照してください。

例 3: 1 回だけ実行される関連付けを作成するには

この例では、指定された日付および時刻に 1 回だけ実行される新しい関連付けを作成します。過去または現在の日付で作成された関連付け (処理されるまで日付は過去のものです) は、ただちに実行されます。

```
aws ssm create-association \
    --name "AWS-UpdateSSMAgent" \
    --targets "Key=instanceids,Values=i-0cb2b964d3e14fd9f" \
    --schedule-expression "at(2020-05-14T15:55:00)"  \
    --apply-only-at-cron-interval
```

出力:

```
{
    "AssociationDescription": {
        "Status": {
            "Date": 1487875500.33,
            "Message": "Associated with AWS-UpdateSSMAgent",
```

```
            "Name": "Associated"
        },
        "Name": "AWS-UpdateSSMAgent",
        "InstanceId": "i-0cb2b964d3e14fd9f",
        "Overview": {
            "Status": "Pending",
            "DetailedStatus": "Creating"
        },
        "AssociationId": "b7c3266e-a544-44db-877e-b20d3a108189",
        "DocumentVersion": "$DEFAULT",
        "LastUpdateAssociationDate": 1487875500.33,
        "Date": 1487875500.33,
        "Targets": [
            {
                "Values": [
                    "i-0cb2b964d3e14fd9f"
                ],
                "Key": "InstanceIds"
            }
        ]
    }
}
```

詳細については、「AWS Systems Manager API リファレンス」の「CreateAssociation」、または「AWS Systems Manager ユーザーガイド」の「リファレンス: Systems Manager の Cron 式および rate 式」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「CreateAssociation」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、インスタンス ID を使用して、設定ドキュメントをインスタンスに関連付けます。

```
New-SSMAssociation -InstanceId "i-0cb2b964d3e14fd9f" -Name "AWS-UpdateSSMAgent"
```

出力:

```
Name                  : AWS-UpdateSSMAgent
```

```
InstanceId            : i-0000293ffd8c57862
Date                  : 2/23/2017 6:55:22 PM
Status.Name           : Associated
Status.Date           : 2/20/2015 8:31:11 AM
Status.Message        : Associated with AWS-UpdateSSMAgent
Status.AdditionalInfo :
```

例 2: この例では、ターゲットを使用して、設定ドキュメントをインスタンスに関連付けます。

```
$target = @{Key="instanceids";Values=@("i-0cb2b964d3e14fd9f")}
New-SSMAssociation -Name "AWS-UpdateSSMAgent" -Target $target
```

出力:

```
Name                  : AWS-UpdateSSMAgent
InstanceId            :
Date                  : 3/1/2017 6:22:21 PM
Status.Name           :
Status.Date           :
Status.Message        :
Status.AdditionalInfo :
```

例 3: この例では、ターゲットとパラメータを使用して、設定ドキュメントをインスタンスに関連付けます。

```
$target = @{Key="instanceids";Values=@("i-0cb2b964d3e14fd9f")}
$params = @{
  "action"="configure"
  "mode"="ec2"
  "optionalConfigurationSource"="ssm"
  "optionalConfigurationLocation"=""
  "optionalRestart"="yes"
}
New-SSMAssociation -Name "Configure-CloudWatch" -AssociationName
 "CWConfiguration" -Target $target -Parameter $params
```

出力:

```
Name                  : Configure-CloudWatch
InstanceId            :
```

```
Date                   : 5/17/2018 3:17:44 PM
Status.Name            :
Status.Date            :
Status.Message         :
Status.AdditionalInfo :
```

例 4: この例では、**AWS-GatherSoftwareInventory** を使用して、リージョン内におけるすべてのインスタンスとの関連付けを作成します。また、収集するパラメータにカスタムファイルとレジストリの場所を指定します。

```
$params =
 [Collections.Generic.Dictionary[String,Collections.Generic.List[String]]]::new()
$params["windowsRegistry"] ='[{"Path":"HKEY_LOCAL_MACHINE\SOFTWARE\Amazon
\MachineImage","Recursive":false,"ValueNames":["AMIName"]}]'
$params["files"] = '[{"Path":"C:\Program Files","Pattern":
["*.exe"],"Recursive":true}, {"Path":"C:\ProgramData","Pattern":
["*.log"],"Recursive":true}]'
New-SSMAssociation -AssociationName new-in-mum -Name AWS-GatherSoftwareInventory
 -Target @{Key="instanceids";Values="*"} -Parameter $params -region ap-south-1 -
ScheduleExpression "rate(720 minutes)"
```

出力:

```
Name                   : AWS-GatherSoftwareInventory
InstanceId             :
Date                   : 6/9/2019 8:57:56 AM
Status.Name            :
Status.Date            :
Status.Message         :
Status.AdditionalInfo :
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「CreateAssociation」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **CreateAssociationBatch** を使用する

次のサンプルコードは、CreateAssociationBatch を使用する方法を説明しています。

CLI

AWS CLI

複数の関連付けを削除するには

この例では、設定ドキュメントを複数のインスタンスに関連付けます。出力では、成功したオペレーションと失敗したオペレーションのリストが返されます (該当する場合)。

コマンド:

```
aws ssm create-association-batch --entries "Name=AWS-
UpdateSSMAgent,InstanceId=i-1234567890abcdef0" "Name=AWS-
UpdateSSMAgent,InstanceId=i-9876543210abcdef0"
```

出力:

```
{
  "Successful": [
      {
          "Name": "AWS-UpdateSSMAgent",
          "InstanceId": "i-1234567890abcdef0",
          "AssociationVersion": "1",
          "Date": 1550504725.007,
          "LastUpdateAssociationDate": 1550504725.007,
          "Status": {
              "Date": 1550504725.007,
              "Name": "Associated",
              "Message": "Associated with AWS-UpdateSSMAgent"
          },
          "Overview": {
              "Status": "Pending",
              "DetailedStatus": "Creating"
          },
          "DocumentVersion": "$DEFAULT",
          "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
          "Targets": [
              {
                  "Key": "InstanceIds",
                  "Values": [
                      "i-1234567890abcdef0"
                  ]
              }
```

```
            ]
        },
        {
            "Name": "AWS-UpdateSSMAgent",
            "InstanceId": "i-9876543210abcdef0",
            "AssociationVersion": "1",
            "Date": 1550504725.057,
            "LastUpdateAssociationDate": 1550504725.057,
            "Status": {
                "Date": 1550504725.057,
                "Name": "Associated",
                "Message": "Associated with AWS-UpdateSSMAgent"
            },
            "Overview": {
                "Status": "Pending",
                "DetailedStatus": "Creating"
            },
            "DocumentVersion": "$DEFAULT",
            "AssociationId": "9c9f7f20-5154-4fed-a83e-0123456789ab",
            "Targets": [
                {
                    "Key": "InstanceIds",
                    "Values": [
                        "i-9876543210abcdef0"
                    ]
                }
            ]
        }
    ],
    "Failed": []
}
```

- API の詳細については、「AWS CLI Command Reference」の「CreateAssociationBatch」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、設定ドキュメントを複数のインスタンスに関連付けます。出力では、成功したオペレーションと失敗したオペレーションのリストが返されます (該当する場合)。

```
$option1 = @{InstanceId="i-0cb2b964d3e14fd9f";Name=@("AWS-UpdateSSMAgent")}
$option2 = @{InstanceId="i-0000293ffd8c57862";Name=@("AWS-UpdateSSMAgent")}
New-SSMAssociationFromBatch -Entry $option1,$option2
```

出力:

```
Failed  Successful
------  ----------
{}      {Amazon.SimpleSystemsManagement.Model.FailedCreateAssociation,
 Amazon.SimpleSystemsManagement.Model.FailedCreateAsso...
```

例 2: この例では、成功したオペレーションの詳細を表示します。

```
$option1 = @{InstanceId="i-0cb2b964d3e14fd9f";Name=@("AWS-UpdateSSMAgent")}
$option2 = @{InstanceId="i-0000293ffd8c57862";Name=@("AWS-UpdateSSMAgent")}
(New-SSMAssociationFromBatch -Entry $option1,$option2).Successful
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「CreateAssociationBatch」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI で **CreateDocument** を使用する

次のサンプルコードは、CreateDocument を使用する方法を説明しています。

アクション例は、より大きなプログラムからのコードの抜粋であり、コンテキスト内で実行する必要があります。次のコード例で、このアクションのコンテキストを確認できます。

- 基本を学ぶ

CLI

AWS CLI

ドキュメントを作成するには

次の create-document の例では、新しい Systems Manager ドキュメントを作成します。

```
aws ssm create-document \
    --content file://exampleDocument.yml \
    --name "Example" \
    --document-type "Automation" \
    --document-format YAML
```

出力:

```
{
    "DocumentDescription": {
        "Hash":
 "fc2410281f40779e694a8b95975d0f9f316da8a153daa94e3d9921102EXAMPLE",
        "HashType": "Sha256",
        "Name": "Example",
        "Owner": "29884EXAMPLE",
        "CreatedDate": 1583256349.452,
        "Status": "Creating",
        "DocumentVersion": "1",
        "Description": "Document Example",
        "Parameters": [
            {
                "Name": "AutomationAssumeRole",
                "Type": "String",
                "Description": "(Required) The ARN of the role that allows
 Automation to perform the actions on your behalf. If no role is specified,
 Systems Manager Automation uses your IAM permissions to execute this document.",
                "DefaultValue": ""
            },
            {
                "Name": "InstanceId",
                "Type": "String",
                "Description": "(Required) The ID of the Amazon EC2 instance.",
                "DefaultValue": ""
            }
        ],
        "PlatformTypes": [
            "Windows",
            "Linux"
        ],
        "DocumentType": "Automation",
        "SchemaVersion": "0.3",
```

```
        "LatestVersion": "1",
        "DefaultVersion": "1",
        "DocumentFormat": "YAML",
        "Tags": []
    }
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「SSM ドキュメントコンテンツを作成する」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「CreateDocument」を参照してください。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
    /**
     * Creates an AWS SSM document asynchronously.
     *
     * @param docName The name of the document to create.
     * <p>
     * This method initiates an asynchronous request to create an SSM document.
     * If the request is successful, it prints the document status.
     * If an exception occurs, it handles the error appropriately.
     */
    public void createSSMDoc(String docName) throws SsmException {
        String jsonData = """
        {
        "schemaVersion": "2.2",
        "description": "Run a simple shell command",
        "mainSteps": [
            {
                "action": "aws:runShellScript",
                "name": "runEchoCommand",
```

```
                "inputs": {
                  "runCommand": [
                    "echo 'Hello, world!'"
                  ]
                }
              }
            ]
        }
        """;

        CreateDocumentRequest request = CreateDocumentRequest.builder()
                .content(jsonData)
                .name(docName)
                .documentType(DocumentType.COMMAND)
                .build();

        CompletableFuture<CreateDocumentResponse> future =
getAsyncClient().createDocument(request);
        future.thenAccept(response -> {
            System.out.println("The status of the SSM document is " +
response.documentDescription().status());
        }).exceptionally(ex -> {
            Throwable cause = (ex instanceof CompletionException) ?
ex.getCause() : ex;
            if (cause instanceof DocumentAlreadyExistsException) {
                throw new CompletionException(cause);
            } else if (cause instanceof SsmException) {
                throw new CompletionException(cause);
            } else {
                throw new RuntimeException(cause);
            }
        }).join();
    }
```

- API の詳細については、「AWS SDK for Java 2.x API Reference」の「CreateDocument」を参照してください。

JavaScript

SDK for JavaScript (v3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
import { CreateDocumentCommand, SSMClient } from "@aws-sdk/client-ssm";
import { parseArgs } from "node:util";

/**
 * Create an SSM document.
 * @param {{ content: string, name: string, documentType?: DocumentType }}
 */
export const main = async ({ content, name, documentType }) => {
  const client = new SSMClient({});
  try {
    const { documentDescription } = await client.send(
      new CreateDocumentCommand({
        Content: content, // The content for the new SSM document. The content
 must not exceed 64KB.
        Name: name,
        DocumentType: documentType, // Document format type can be JSON, YAML, or
 TEXT. The default format is JSON.
      }),
    );
    console.log("Document created successfully.");
    return { DocumentDescription: documentDescription };
  } catch (caught) {
    if (caught instanceof Error && caught.name === "DocumentAlreadyExists") {
      console.warn(`${caught.message}. Did you provide a new document name?`);
    } else {
      throw caught;
    }
  }
};
```

- API の詳細については、「AWS SDK for JavaScript API Reference」の「CreateDocument」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、アカウントにドキュメントを作成します。ドキュメントは JSON 形式である必要があります。設定ドキュメントの記述については、「SSM API Reference」の「Configuration Document」を参照してください。

```
New-SSMDocument -Content (Get-Content -Raw "c:\temp\RunShellScript.json") -Name
 "RunShellScript" -DocumentType "Command"
```

出力:

```
CreatedDate     : 3/1/2017 1:21:33 AM
DefaultVersion  : 1
Description     : Run an updated script
DocumentType    : Command
DocumentVersion : 1
Hash            :
 1d5ce820e999ff051eb4841ed887593daf77120fd76cae0d18a53cc42e4e22c1
HashType        : Sha256
LatestVersion   : 1
Name            : RunShellScript
Owner           : 809632081692
Parameters      : {commands}
PlatformTypes   : {Linux}
SchemaVersion   : 2.0
Sha1            :
Status          : Creating
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「CreateDocument」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
class DocumentWrapper:
    """Encapsulates AWS Systems Manager Document actions."""

    def __init__(self, ssm_client):
        """
        :param ssm_client: A Boto3 Systems Manager client.
        """
        self.ssm_client = ssm_client
        self.name = None

    @classmethod
    def from_client(cls):
        ssm_client = boto3.client("ssm")
        return cls(ssm_client)


    def create(self, content, name):
        """
        Creates a document.

        :param content: The content of the document.
        :param name: The name of the document.
        """
        try:
            self.ssm_client.create_document(
                Name=name, Content=content, DocumentType="Command"
            )
            self.name = name
        except self.ssm_client.exceptions.DocumentAlreadyExists:
            print(f"Document {name} already exists.")
            self.name = name
        except ClientError as err:
```

```
            logger.error(
                "Couldn't create %s. Here's why: %s: %s",
                name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
```

- API の詳細については、「AWS SDK for Python (Boto3) API リファレンス」の「CreateDocument」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI で **CreateMaintenanceWindow** を使用する

次のサンプルコードは、CreateMaintenanceWindow を使用する方法を説明しています。

アクション例は、より大きなプログラムからのコードの抜粋であり、コンテキスト内で実行する必要があります。次のコード例で、このアクションのコンテキストを確認できます。

- 基本を学ぶ

CLI

AWS CLI

例 1: メンテナンスウィンドウを作成するには

次の create-maintenance-window の例では、5 分ごとに最大 2 時間 (必要に応じて) の新しいメンテナンスウィンドウを作成し、メンテナンスウィンドウの実行終了から 1 時間以内に新しいタスクが開始されないようにします。また、関連付けられていないターゲット (メンテナンスウィンドウに登録されていないインスタンス) を許可し、カスタムタグを使用することで、その作成者がチュートリアルで使用する意図があることを示します。

```
aws ssm create-maintenance-window \
    --name "My-Tutorial-Maintenance-Window" \
```

```
    --schedule "rate(5 minutes)" \
    --duration 2 --cutoff 1 \
    --allow-unassociated-targets \
    --tags "Key=Purpose,Value=Tutorial"
```

出力:

```
{
    "WindowId": "mw-0c50858d01EXAMPLE"
}
```

例 2: 1 回だけ実行されるメンテナンスウィンドウを作成するには

次の create-maintenance-window の例では、指定した日付および時刻に 1 回だけ実行される新しいメンテナンスウィンドウを作成します。

```
aws ssm create-maintenance-window \
    --name My-One-Time-Maintenance-Window \
    --schedule "at(2020-05-14T15:55:00)" \
    --duration 5 \
    --cutoff 2 \
    --allow-unassociated-targets \
    --tags "Key=Environment,Value=Production"
```

出力:

```
{
    "WindowId": "mw-01234567890abcdef"
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「Maintenance Windows」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「CreateMaintenanceWindow」を参照してください。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
   /**
    * Creates an SSM maintenance window asynchronously.
    *
    * @param winName The name of the maintenance window.
    * @return The ID of the created or existing maintenance window.
    * <p>
    * This method initiates an asynchronous request to create an SSM maintenance
window.
    * If the request is successful, it prints the maintenance window ID.
    * If an exception occurs, it handles the error appropriately.
    */
   public String createMaintenanceWindow(String winName) throws SsmException,
DocumentAlreadyExistsException {
       CreateMaintenanceWindowRequest request =
CreateMaintenanceWindowRequest.builder()
               .name(winName)
               .description("This is my maintenance window")
               .allowUnassociatedTargets(true)
               .duration(2)
               .cutoff(1)
               .schedule("cron(0 10 ? * MON-FRI *)")
               .build();

       CompletableFuture<CreateMaintenanceWindowResponse> future =
getAsyncClient().createMaintenanceWindow(request);
       final String[] windowId = {null};
       future.whenComplete((response, ex) -> {
           if (response != null) {
               String maintenanceWindowId = response.windowId();
               System.out.println("The maintenance window id is " +
maintenanceWindowId);
               windowId[0] = maintenanceWindowId;
```

```
            } else {
                Throwable cause = (ex instanceof CompletionException) ?
ex.getCause() : ex;
                if (cause instanceof DocumentAlreadyExistsException) {
                    throw new CompletionException(cause);
                } else if (cause instanceof SsmException) {
                    throw new CompletionException(cause);
                } else {
                    throw new RuntimeException(cause);
                }
            }
        }).join();

        if (windowId[0] == null) {
            MaintenanceWindowFilter filter = MaintenanceWindowFilter.builder()
                    .key("name")
                    .values(winName)
                    .build();

            DescribeMaintenanceWindowsRequest winRequest =
DescribeMaintenanceWindowsRequest.builder()
                    .filters(filter)
                    .build();

            CompletableFuture<DescribeMaintenanceWindowsResponse> describeFuture
= getAsyncClient().describeMaintenanceWindows(winRequest);
            describeFuture.whenComplete((describeResponse, describeEx) -> {
                if (describeResponse != null) {
                    List<MaintenanceWindowIdentity> windows =
describeResponse.windowIdentities();
                    if (!windows.isEmpty()) {
                        windowId[0] = windows.get(0).windowId();
                        System.out.println("Window ID: " + windowId[0]);
                    } else {
                        System.out.println("Window not found.");
                        windowId[0] = "";
                    }
                } else {
                    Throwable describeCause = (describeEx instanceof
CompletionException) ? describeEx.getCause() : describeEx;
                    throw new RuntimeException("Error describing maintenance
windows: " + describeCause.getMessage(), describeCause);
                }
            }).join();
```

```
        }

        return windowId[0];
    }
```

- API の詳細については、「AWS SDK for Java 2.x API Reference」の「CreateMaintenanceWindow」を参照してください。

JavaScript

SDK for JavaScript (v3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
import { CreateMaintenanceWindowCommand, SSMClient } from "@aws-sdk/client-ssm";
import { parseArgs } from "node:util";

/**
 * Create an SSM maintenance window.
 * @param {{ name: string, allowUnassociatedTargets: boolean, duration: number,
 cutoff: number, schedule: string, description?: string }}
 */
export const main = async ({
  name,
  allowUnassociatedTargets, // Allow the maintenance window to run on managed
 nodes, even if you haven't registered those nodes as targets.
  duration, // The duration of the maintenance window in hours.
  cutoff, // The number of hours before the end of the maintenance window that
 Amazon Web Services Systems Manager stops scheduling new tasks for execution.
  schedule, // The schedule of the maintenance window in the form of a cron or
 rate expression.
  description = undefined,
}) => {
  const client = new SSMClient({});

  try {
```

```
    const { windowId } = await client.send(
      new CreateMaintenanceWindowCommand({
        Name: name,
        Description: description,
        AllowUnassociatedTargets: allowUnassociatedTargets, // Allow the
 maintenance window to run on managed nodes, even if you haven't registered those
 nodes as targets.
        Duration: duration, // The duration of the maintenance window in hours.
        Cutoff: cutoff, // The number of hours before the end of the maintenance
 window that Amazon Web Services Systems Manager stops scheduling new tasks for
 execution.
        Schedule: schedule, // The schedule of the maintenance window in the form
 of a cron or rate expression.
      }),
    );
    console.log(`Maintenance window created with Id: ${windowId}`);
    return { WindowId: windowId };
  } catch (caught) {
    if (caught instanceof Error && caught.name === "MissingParameter") {
      console.warn(`${caught.message}. Did you provide these values?`);
    } else {
      throw caught;
    }
  }
};
```

- API の詳細については、「AWS SDK for JavaScript API Reference」の「CreateMaintenanceWindow」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、そのウィンドウは、毎週火曜日の午後 4 時に 4 時間実行され (カットオフは 1 時間)、関連付けられていないターゲットを許可する、指定された名前の新しいメンテナンスウィンドウを作成します。

```
New-SSMMaintenanceWindow -Name "MyMaintenanceWindow" -Duration 4 -Cutoff 1 -
AllowUnassociatedTarget $true -Schedule "cron(0 16 ? * TUE *)"
```

出力:

```
mw-03eb53e1ea7383998
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「CreateMaintenanceWindow」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
class MaintenanceWindowWrapper:
    """Encapsulates AWS Systems Manager maintenance window actions."""

    def __init__(self, ssm_client):
        """
        :param ssm_client: A Boto3 Systems Manager client.
        """
        self.ssm_client = ssm_client
        self.window_id = None
        self.name = None

    @classmethod
    def from_client(cls):
        ssm_client = boto3.client("ssm")
        return cls(ssm_client)


    def create(self, name, schedule, duration, cutoff,
 allow_unassociated_targets):
        """
        Create an AWS Systems Manager maintenance window.

        :param name: The name of the maintenance window.
        :param schedule: The schedule of the maintenance window.
        :param duration: The duration of the maintenance window.
        :param cutoff: The cutoff time of the maintenance window.
```

```
        :param allow_unassociated_targets: Allow the maintenance window to run on
managed nodes, even
                                           if you haven't registered those nodes
as targets.
        """
        try:
            response = self.ssm_client.create_maintenance_window(
                Name=name,
                Schedule=schedule,
                Duration=duration,
                Cutoff=cutoff,
                AllowUnassociatedTargets=allow_unassociated_targets,
            )
            self.window_id = response["WindowId"]
            self.name = name
            logger.info("Created maintenance window %s.", self.window_id)
        except ParamValidationError as error:
            logger.error(
                "Parameter validation error when trying to create maintenance
window %s. Here's why: %s",
                self.window_id,
                error,
            )
            raise
        except ClientError as err:
            logger.error(
                "Couldn't create maintenance window %s. Here's why: %s: %s",
                name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
```

- API の詳細については、「AWS SDK for Python (Boto3) API リファレンス」の「CreateMaintenanceWindow」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI で **CreateOpsItem** を使用する

次のサンプルコードは、CreateOpsItem を使用する方法を説明しています。

アクション例は、より大きなプログラムからのコードの抜粋であり、コンテキスト内で実行する必要があります。次のコード例で、このアクションのコンテキストを確認できます。

- 基本を学ぶ

CLI

AWS CLI

OpsItems を作成するには

次の create-ops-item の例は、OperationalData の /aws/resources キーを使用して、Amazon DynamoDB 関連リソースで OpsItem を作成します。

```
aws ssm create-ops-item \
    --title "EC2 instance disk full" \
    --description "Log clean up may have failed which caused the disk to be full"
 \
    --priority 2 \
    --source ec2 \
    --operational-data '{"/aws/resources":{"Value":"[{\"arn
\": \"arn:aws:dynamodb:us-west-2:12345678:table/OpsItems
\"}]","Type":"SearchableString"}}' \
    --notifications Arn="arn:aws:sns:us-west-2:12345678:TestUser"
```

出力:

```
{
    "OpsItemId": "oi-1a2b3c4d5e6f"
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「OpsItems の作成」を参照してください。

- API の詳細については、AWS CLI コマンドリファレンスの「CreateOpsItem」を参照してください。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
   /**
    * Creates an SSM OpsItem asynchronously.
    *
    * @param title The title of the OpsItem.
    * @param source The source of the OpsItem.
    * @param category The category of the OpsItem.
    * @param severity The severity of the OpsItem.
    * @return The ID of the created OpsItem.
    * <p>
    * This method initiates an asynchronous request to create an SSM OpsItem.
    * If the request is successful, it returns the OpsItem ID.
    * If an exception occurs, it handles the error appropriately.
    */
   public String createSSMOpsItem(String title, String source, String category,
String severity) {
       CreateOpsItemRequest opsItemRequest = CreateOpsItemRequest.builder()
               .description("Created by the SSM Java API")
               .title(title)
               .source(source)
               .category(category)
               .severity(severity)
               .build();

       CompletableFuture<CreateOpsItemResponse> future =
getAsyncClient().createOpsItem(opsItemRequest);

       try {
           CreateOpsItemResponse response = future.join();
           return response.opsItemId();
       } catch (CompletionException e) {
           Throwable cause = e.getCause();
           if (cause instanceof SsmException) {
```

```
                throw (SsmException) cause;
            } else {
                throw new RuntimeException(cause);
            }
        }
    }
```

- API の詳細については、「AWS SDK for Java 2.x API リファレンス」の「CreateOpsItem」を参照してください。

JavaScript

SDK for JavaScript (v3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
import { CreateOpsItemCommand, SSMClient } from "@aws-sdk/client-ssm";
import { parseArgs } from "node:util";

/**
 * Create an SSM OpsItem.
 * @param {{ title: string, source: string, category?: string, severity?:
 string }}
 */
export const main = async ({
  title,
  source,
  category = undefined,
  severity = undefined,
}) => {
  const client = new SSMClient({});
  try {
    const { opsItemArn, opsItemId } = await client.send(
      new CreateOpsItemCommand({
        Title: title,
```

```
        Source: source, // The origin of the OpsItem, such as Amazon EC2 or
 Systems Manager.
        Category: category,
        Severity: severity,
      }),
    );
    console.log(`Ops item created with id: ${opsItemId}`);
    return { OpsItemArn: opsItemArn, OpsItemId: opsItemId };
  } catch (caught) {
    if (caught instanceof Error && caught.name === "MissingParameter") {
      console.warn(`${caught.message}. Did you provide these values?`);
    } else {
      throw caught;
    }
  }
};
```

- API の詳細については、「AWS SDK for JavaScript API リファレンス」の「CreateOpsItem」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
class OpsItemWrapper:
    """Encapsulates AWS Systems Manager OpsItem actions."""

    def __init__(self, ssm_client):
        """
        :param ssm_client: A Boto3 Systems Manager client.
        """
        self.ssm_client = ssm_client
        self.id = None
```

```
    @classmethod
    def from_client(cls):
        """
        :return: A OpsItemWrapper instance.
        """
        ssm_client = boto3.client("ssm")
        return cls(ssm_client)


    def create(self, title, source, category, severity, description):
        """
        Create an OpsItem

        :param title: The OpsItem title.
        :param source: The OpsItem source.
        :param category: The OpsItem category.
        :param severity: The OpsItem severity.
        :param description: The OpsItem description.

        """
        try:
            response = self.ssm_client.create_ops_item(
                Title=title,
                Source=source,
                Category=category,
                Severity=severity,
                Description=description,
            )
            self.id = response["OpsItemId"]
        except self.ssm_client.exceptions.OpsItemLimitExceededException as err:
            logger.error(
                "Couldn't create ops item because you have exceeded your open
OpsItem limit. "
                "Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        except ClientError as err:
            logger.error(
                "Couldn't create ops item %s. Here's why: %s: %s",
                title,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
```

```
            )
            raise
```

- API の詳細については、「AWS SDK for Python (Boto3) API リファレンス」の「CreateOpsItem」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **CreatePatchBaseline** を使用する

次のサンプルコードは、CreatePatchBaseline を使用する方法を説明しています。

CLI

AWS CLI

例 1: 自動承認を設定したパッチベースラインを作成するには

次の create-patch-baseline の例では、Microsoft からリリースされてから 7 日後に本番環境のパッチを承認する Windows Server のパッチベースラインを作成します。

```
aws ssm create-patch-baseline \
    --name "Windows-Production-Baseline-AutoApproval" \
    --operating-system "WINDOWS" \
    --approval-
rules "PatchRules=[{PatchFilterGroup={PatchFilters=[{Key=MSRC_SEVERITY,Values=[Critical,1
{Key=CLASSIFICATION,Values=[SecurityUpdates,Updates,UpdateRollups,CriticalUpdates]}]},App
 \
    --description "Baseline containing all updates approved for Windows Server
 production systems"
```

出力:

```
{
    "BaselineId": "pb-045f10b4f3EXAMPLE"
}
```

例 2: 承認のカットオフ日を設定したパッチベースラインを作成するには

次の create-patch-baseline の例では、2020 年 7 月 7 日より前にリリースされた本番環境のすべてのパッチを承認する Windows Server のパッチベースラインを作成します。

```
aws ssm create-patch-baseline \
    --name "Windows-Production-Baseline-AutoApproval" \
    --operating-system "WINDOWS" \
    --approval-
rules "PatchRules=[{PatchFilterGroup={PatchFilters=[{Key=MSRC_SEVERITY,Values=[Critical,1
{Key=CLASSIFICATION,Values=[SecurityUpdates,Updates,UpdateRollups,CriticalUpdates]}]},App
 \
    --description "Baseline containing all updates approved for Windows Server
 production systems"
```

出力:

```
{
    "BaselineId": "pb-045f10b4f3EXAMPLE"
}
```

例 3: 承認ルールを JSON ファイルに保存してパッチベースラインを作成するには

次の create-patch-baseline の例では、Amazon Linux 2017.09 のパッチベースラインを作成し、リリースされてから 7 日後に本番環境のパッチを承認し、パッチベースラインの承認ルールを指定し、パッチのカスタムリポジトリを指定します。

```
aws ssm create-patch-baseline \
    --cli-input-json file://my-amazon-linux-approval-rules-and-repo.json
```

my-amazon-linux-approval-rules-and-repo.json の内容:

```
{
    "Name": "Amazon-Linux-2017.09-Production-Baseline",
    "Description": "My approval rules patch baseline for Amazon Linux 2017.09
 instances",
    "OperatingSystem": "AMAZON_LINUX",
    "Tags": [
        {
            "Key": "Environment",
            "Value": "Production"
        }
    ],
    "ApprovalRules": {
```

```
        "PatchRules": [
            {
                "ApproveAfterDays": 7,
                "EnableNonSecurity": true,
                "PatchFilterGroup": {
                    "PatchFilters": [
                        {
                            "Key": "SEVERITY",
                            "Values": [
                                "Important",
                                "Critical"
                            ]
                        },
                        {
                            "Key": "CLASSIFICATION",
                            "Values": [
                                "Security",
                                "Bugfix"
                            ]
                        },
                        {
                            "Key": "PRODUCT",
                            "Values": [
                                "AmazonLinux2017.09"
                            ]
                        }
                    ]
                }
            }
        ]
    },
    "Sources": [
        {
            "Name": "My-AL2017.09",
            "Products": [
                "AmazonLinux2017.09"
            ],
            "Configuration": "[amzn-main] \nname=amzn-main-Base
\nmirrorlist=http://repo./$awsregion./$awsdomain//$releasever/main/
mirror.list //nmirrorlist_expire=300//nmetadata_expire=300 \npriority=10
 \nfailovermethod=priority \nfastestmirror_enabled=0 \ngpgcheck=1
 \ngpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-amazon-ga \nenabled=1 \nretries=3
 \ntimeout=5\nreport_instanceid=yes"
        }
```

```
    ]
}
```

例 4: 承認するパッチと拒否するパッチを指定したパッチベースラインを作成するには

次の create-patch-baseline の例では、デフォルトの承認ルールの例外として、承認するパッチと拒否するパッチを明示的に指定します。

```
aws ssm create-patch-baseline \
    --name "Amazon-Linux-2017.09-Alpha-Baseline" \
    --description "My custom approve/reject patch baseline for Amazon Linux
 2017.09 instances" \
    --operating-system "AMAZON_LINUX" \
    --approved-patches "CVE-2018-1234567,example-pkg-EE-2018*.amzn1.noarch" \
    --approved-patches-compliance-level "HIGH" \
    --approved-patches-enable-non-security \
    --tags "Key=Environment,Value=Alpha"
```

詳細については、「AWS Systems Manager ユーザーガイド」の「Create a Custom Patch Baseline」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「CreatePatchBaseline」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、本番環境で Windows Server 2019 を実行しているマネージドインスタンスに対して、Microsoft からリリースされてから 7 日後にパッチを承認するパッチベースラインを作成します。

```
$rule = New-Object Amazon.SimpleSystemsManagement.Model.PatchRule
$rule.ApproveAfterDays = 7

$ruleFilters = New-Object Amazon.SimpleSystemsManagement.Model.PatchFilterGroup

$patchFilter = New-Object Amazon.SimpleSystemsManagement.Model.PatchFilter
$patchFilter.Key="PRODUCT"
$patchFilter.Values="WindowsServer2019"

$severityFilter = New-Object Amazon.SimpleSystemsManagement.Model.PatchFilter
```

```
$severityFilter.Key="MSRC_SEVERITY"
$severityFilter.Values.Add("Critical")
$severityFilter.Values.Add("Important")
$severityFilter.Values.Add("Moderate")

$classificationFilter = New-Object
 Amazon.SimpleSystemsManagement.Model.PatchFilter
$classificationFilter.Key = "CLASSIFICATION"
$classificationFilter.Values.Add( "SecurityUpdates" )
$classificationFilter.Values.Add( "Updates" )
$classificationFilter.Values.Add( "UpdateRollups" )
$classificationFilter.Values.Add( "CriticalUpdates" )

$ruleFilters.PatchFilters.Add($severityFilter)
$ruleFilters.PatchFilters.Add($classificationFilter)
$ruleFilters.PatchFilters.Add($patchFilter)
$rule.PatchFilterGroup = $ruleFilters

New-SSMPatchBaseline -Name "Production-Baseline-Windows2019" -Description
 "Baseline containing all updates approved for production systems" -
ApprovalRules_PatchRule $rule
```

出力:

```
pb-0z4z6221c4296b23z
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「CreatePatchBaseline」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DeleteActivation** を使用する

次のサンプルコードは、DeleteActivation を使用する方法を説明しています。

CLI

AWS CLI

マネージドインスタンスのアクティベーションを削除するには

次の delete-activation の例では、マネージドインスタンスのアクティベーションを削除します。

```
aws ssm delete-activation \
    --activation-id "aa673477-d926-42c1-8757-1358cEXAMPLE"
```

このコマンドでは何も出力されません。

詳細については、「AWS Systems Manager ユーザーガイド」の「ハイブリッドおよびマルチクラウド環境に AWS Systems Manager をセットアップする」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「DeleteActivation」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、アクティベーションを削除します。コマンドが成功した場合、出力はありません。

```
Remove-SSMActivation -ActivationId "08e51e79-1e36-446c-8e63-9458569c1363"
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「DeleteActivation」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DeleteAssociation** を使用する

次のサンプルコードは、DeleteAssociation を使用する方法を説明しています。

CLI

AWS CLI

例 1: 関連付け ID を使用して関連付けを削除するには

次の delete-association の例では、指定された関連付け ID の関連付けを削除します。コマンドが成功した場合、出力はありません。

```
aws ssm delete-association \
    --association-id "8dfe3659-4309-493a-8755-0123456789ab"
```

このコマンドでは何も出力されません。

詳細については、「AWS Systems Manager ユーザーガイド」の「関連付けの編集と新しいバージョンの作成」を参照してください。

例 2: 関連付けを削除するには

次の delete-association の例では、インスタンスとドキュメント間の関連付けを削除します。コマンドが成功した場合、出力はありません。

```
aws ssm delete-association \
    --instance-id "i-1234567890abcdef0" \
    --name "AWS-UpdateSSMAgent"
```

このコマンドでは何も出力されません。

詳細については、「AWS Systems Manager ユーザーガイド」の「Systems Manager の関連付けの使用」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「DeleteAssociation」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、インスタンスとドキュメント間の関連付けを削除します。コマンドが成功した場合、出力はありません。

```
Remove-SSMAssociation -InstanceId "i-0cb2b964d3e14fd9f" -Name "AWS-
UpdateSSMAgent"
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「DeleteAssociation」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI で **DeleteDocument** を使用する

次のサンプルコードは、DeleteDocument を使用する方法を説明しています。

CLI

AWS CLI

ドキュメントを削除するには

次の delete-document の例では、Systems Manager ドキュメントを削除します。

```
aws ssm delete-document \
    --name "Example"
```

このコマンドでは何も出力されません。

詳細については、「AWS Systems Manager ユーザーガイド」の「SSM ドキュメントコンテンツを作成する」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「DeleteDocument」を参照してください。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
/**
 * Deletes an AWS SSM document asynchronously.
```

```
     *
     * @param documentName The name of the document to delete.
     * <p>
     * This method initiates an asynchronous request to delete an SSM document.
     * If an exception occurs, it handles the error appropriately.
     */
    public void deleteDoc(String documentName) {
        DeleteDocumentRequest documentRequest = DeleteDocumentRequest.builder()
                .name(documentName)
                .build();

        CompletableFuture<Void> future = CompletableFuture.runAsync(() -> {
            getAsyncClient().deleteDocument(documentRequest)
                    .thenAccept(response -> {
                        System.out.println("The SSM document was successfully
deleted.");
                    })
                    .exceptionally(ex -> {
                        throw new CompletionException(ex);
                    }).join();
        }).exceptionally(ex -> {
            Throwable cause = (ex instanceof CompletionException) ?
ex.getCause() : ex;
            if (cause instanceof SsmException) {
                throw new RuntimeException("SSM error: " + cause.getMessage(),
cause);
            } else {
                throw new RuntimeException("Unexpected error: " +
cause.getMessage(), cause);
            }
        });

        try {
            future.join();
        } catch (CompletionException ex) {
            throw ex.getCause() instanceof RuntimeException ? (RuntimeException)
ex.getCause() : ex;
        }
    }
```

- API の詳細については、「AWS SDK for Java 2.x API Reference」の「DeleteDocument」を参照してください。

JavaScript

SDK for JavaScript (v3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
import { DeleteDocumentCommand, SSMClient } from "@aws-sdk/client-ssm";
import { parseArgs } from "node:util";

/**
 * Delete an SSM document.
 * @param {{ documentName: string }}
 */
export const main = async ({ documentName }) => {
  const client = new SSMClient({});
  try {
    await client.send(new DeleteDocumentCommand({ Name: documentName }));
    console.log(`Document '${documentName}' deleted.`);
    return { Deleted: true };
  } catch (caught) {
    if (caught instanceof Error && caught.name === "MissingParameter") {
      console.warn(`${caught.message}. Did you provide this value?`);
    } else {
      throw caught;
    }
  }
};
```

- API の詳細については、「AWS SDK for JavaScript API Reference」の「DeleteDocument」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、ドキュメントを削除します。コマンドが成功した場合、出力はありません。

```
Remove-SSMDocument -Name "RunShellScript"
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「DeleteDocument」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
class DocumentWrapper:
    """Encapsulates AWS Systems Manager Document actions."""

    def __init__(self, ssm_client):
        """
        :param ssm_client: A Boto3 Systems Manager client.
        """
        self.ssm_client = ssm_client
        self.name = None

    @classmethod
    def from_client(cls):
        ssm_client = boto3.client("ssm")
        return cls(ssm_client)


    def delete(self):
        """
        Deletes an AWS Systems Manager document.
```

```
        """
        if self.name is None:
            return

        try:
            self.ssm_client.delete_document(Name=self.name)
            print(f"Deleted document {self.name}.")
            self.name = None
        except ClientError as err:
            logger.error(
                "Couldn't delete %s. Here's why: %s: %s",
                self.name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
```

- API の詳細については、「AWS SDK for Python (Boto3) API リファレンス」の「DeleteDocument」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI で **DeleteMaintenanceWindow** を使用する

次のサンプルコードは、DeleteMaintenanceWindow を使用する方法を説明しています。

アクション例は、より大きなプログラムからのコードの抜粋であり、コンテキスト内で実行する必要があります。次のコード例で、このアクションのコンテキストを確認できます。

- 基本を学ぶ

CLI

AWS CLI

メンテナンスウィンドウを削除するには

この delete-maintenance-window の例では、指定されたメンテナンスウィンドウを削除します。

```
aws ssm delete-maintenance-window \
    --window-id "mw-1a2b3c4d5e6f7g8h9"
```

出力:

```
{
    "WindowId":"mw-1a2b3c4d5e6f7g8h9"
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「メンテナンスウィンドウの削除 (AWS CLI)」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「DeleteMaintenanceWindow」を参照してください。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
    /**
     * Deletes an AWS SSM Maintenance Window asynchronously.
     *
     * @param winId The ID of the Maintenance Window to delete.
     * <p>
     * This method initiates an asynchronous request to delete an SSM Maintenance
Window.
     * If an exception occurs, it handles the error appropriately.
     */
    public void deleteMaintenanceWindow(String winId) {
        DeleteMaintenanceWindowRequest windowRequest =
DeleteMaintenanceWindowRequest.builder()
```

```
                .windowId(winId)
                .build();

        CompletableFuture<Void> future = CompletableFuture.runAsync(() -> {
            getAsyncClient().deleteMaintenanceWindow(windowRequest)
                    .thenAccept(response -> {
                        System.out.println("The maintenance window was
successfully deleted.");
                    })
                    .exceptionally(ex -> {
                        throw new CompletionException(ex);
                    }).join();
        }).exceptionally(ex -> {
            Throwable cause = (ex instanceof CompletionException) ?
ex.getCause() : ex;
            if (cause instanceof SsmException) {
                throw new RuntimeException("SSM error: " + cause.getMessage(),
cause);
            } else {
                throw new RuntimeException("Unexpected error: " +
cause.getMessage(), cause);
            }
        });

        try {
            future.join();
        } catch (CompletionException ex) {
            throw ex.getCause() instanceof RuntimeException ? (RuntimeException)
ex.getCause() : ex;
        }
    }
```

- API の詳細については、「AWS SDK for Java 2.x API Reference」の「DeleteMaintenanceWindow」を参照してください。

JavaScript

SDK for JavaScript (v3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
import { DeleteMaintenanceWindowCommand, SSMClient } from "@aws-sdk/client-ssm";
import { parseArgs } from "node:util";

/**
 * Delete an SSM maintenance window.
 * @param {{ windowId: string }}
 */
export const main = async ({ windowId }) => {
  const client = new SSMClient({});
  try {
    await client.send(
      new DeleteMaintenanceWindowCommand({ WindowId: windowId }),
    );
    console.log(`Maintenance window '${windowId}' deleted.`);
    return { Deleted: true };
  } catch (caught) {
    if (caught instanceof Error && caught.name === "MissingParameter") {
      console.warn(`${caught.message}. Did you provide this value?`);
    } else {
      throw caught;
    }
  }
};
```

- API の詳細については、「AWS SDK for JavaScript API Reference」の「DeleteMaintenanceWindow」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、メンテナンスウィンドウを削除します。

```
Remove-SSMMaintenanceWindow -WindowId "mw-06d59c1a07c022145"
```

出力:

```
mw-06d59c1a07c022145
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「DeleteMaintenanceWindow」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
class MaintenanceWindowWrapper:
    """Encapsulates AWS Systems Manager maintenance window actions."""

    def __init__(self, ssm_client):
        """
        :param ssm_client: A Boto3 Systems Manager client.
        """
        self.ssm_client = ssm_client
        self.window_id = None
        self.name = None

    @classmethod
    def from_client(cls):
        ssm_client = boto3.client("ssm")
        return cls(ssm_client)
```

```
    def delete(self):
        """
        Delete the associated AWS Systems Manager maintenance window.
        """
        if self.window_id is None:
            return

        try:
            self.ssm_client.delete_maintenance_window(WindowId=self.window_id)
            logger.info("Deleted maintenance window %s.", self.window_id)
            print(f"Deleted maintenance window {self.name}")
            self.window_id = None
        except ClientError as err:
            logger.error(
                "Couldn't delete maintenance window %s. Here's why: %s: %s",
                self.window_id,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
```

- API の詳細については、「AWS SDK for Python (Boto3) API リファレンス」の「DeleteMaintenanceWindow」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK で **DeleteOpsItem** を使用する

次の例は、DeleteOpsItem を使用する方法を説明しています。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
class OpsItemWrapper:
    """Encapsulates AWS Systems Manager OpsItem actions."""

    def __init__(self, ssm_client):
        """
        :param ssm_client: A Boto3 Systems Manager client.
        """
        self.ssm_client = ssm_client
        self.id = None

    @classmethod
    def from_client(cls):
        """
        :return: A OpsItemWrapper instance.
        """
        ssm_client = boto3.client("ssm")
        return cls(ssm_client)


    def delete(self):
        """
        Delete the OpsItem.
        """
        if self.id is None:
            return
        try:
            self.ssm_client.delete_ops_item(OpsItemId=self.id)
            print(f"Deleted ops item with id {self.id}")
            self.id = None
        except ClientError as err:
            logger.error(
                "Couldn't delete ops item %s. Here's why: %s: %s",
```

```
                self.id,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
```

- API の詳細については、「AWS SDK for Python (Boto3) API リファレンス」の「DeleteOpsItem」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DeleteParameter** を使用する

次のサンプルコードは、DeleteParameter を使用する方法を説明しています。

CLI

AWS CLI

パラメータを削除をするには

次の delete-parameter の例では、指定された単一のパラメータを削除します。

```
aws ssm delete-parameter \
    --name "MyParameter"
```

このコマンドでは何も出力されません。

詳細については、「AWS Systems Manager ユーザーガイド」の「Parameter Store の使用」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「DeleteParameter」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例ではパラメータを削除します。コマンドが成功した場合、出力はありません。

```
Remove-SSMParameter -Name "helloWorld"
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「DeleteParameter」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DeletePatchBaseline** を使用する

次のサンプルコードは、DeletePatchBaseline を使用する方法を説明しています。

CLI

AWS CLI

パッチベースラインを削除するには

次の delete-patch-baseline の例では、指定されたパッチベースラインを削除します。

```
aws ssm delete-patch-baseline \
    --baseline-id "pb-045f10b4f382baeda"
```

出力:

```
{
    "BaselineId": "pb-045f10b4f382baeda"
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「Update or Delete a Patch Baseline (Console)」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「DeletePatchBaseline」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、パッチベースラインを削除します。

```
Remove-SSMPatchBaseline -BaselineId "pb-045f10b4f382baeda"
```

出力:

```
pb-045f10b4f382baeda
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「DeletePatchBaseline」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DeregisterManagedInstance** を使用する

次のサンプルコードは、DeregisterManagedInstance を使用する方法を説明しています。

CLI

AWS CLI

マネージドインスタンスを登録解除するには

次の deregister-managed-instance の例では、指定されたマネージドインスタンスを登録解除します。

```
aws ssm deregister-managed-instance \
    --instance-id 'mi-08ab247cdfEXAMPLE'
```

このコマンドでは何も出力されません。

詳細については、「AWS Systems Manager ユーザーガイド」の「ハイブリッドおよびマルチクラウド環境でのマネージドノードの登録解除」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「DeregisterManagedInstance」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、マネージドインスタンスを登録解除します。コマンドが成功した場合、出力はありません。

```
Unregister-SSMManagedInstance -InstanceId "mi-08ab247cdf1046573"
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「DeregisterManagedInstance」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DeregisterPatchBaselineForPatchGroup** を使用する

次のサンプルコードは、DeregisterPatchBaselineForPatchGroup を使用する方法を説明しています。

CLI

AWS CLI

パッチグループをパッチベースラインから登録解除するには

次の deregister-patch-baseline-for-patch-group の例では、指定されたパッチグループを指定されたパッチベースラインから登録解除します。

```
aws ssm deregister-patch-baseline-for-patch-group \
    --patch-group "Production" \
    --baseline-id "pb-0ca44a362fEXAMPLE"
```

出力:

```
{
  "PatchGroup":"Production",
  "BaselineId":"pb-0ca44a362fEXAMPLE"
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「パッチベースラインにパッチグループを追加します」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「DeregisterPatchBaselineForPatchGroup」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、パッチグループをパッチベースラインから登録解除します。

```
Unregister-SSMPatchBaselineForPatchGroup -BaselineId "pb-045f10b4f382baeda" -
PatchGroup "Production"
```

出力:

```
BaselineId           PatchGroup
----------           ----------
pb-045f10b4f382baeda Production
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「DeregisterPatchBaselineForPatchGroup」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DeregisterTargetFromMaintenanceWindow** を使用する

次のサンプルコードは、DeregisterTargetFromMaintenanceWindow を使用する方法を説明しています。

CLI

AWS CLI

メンテナンスウィンドウからターゲットを削除するには

次のderegister-target-from-maintenance-window の例では、指定されたターゲットを指定されたメンテナンスウィンドウから削除します。

```
aws ssm deregister-target-from-maintenance-window \
    --window-id "mw-ab12cd34ef56gh78" \
    --window-target-id "1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4d-1a2"
```

出力:

```
{
    "WindowId":"mw-ab12cd34ef56gh78",
    "WindowTargetId":"1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4d-1a2"
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「メンテナンスウィンドウの更新 (AWS CLI)」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「DeregisterTargetFromMaintenanceWindow」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、メンテナンスウィンドウからターゲットを削除します。

```
Unregister-SSMTargetFromMaintenanceWindow -WindowTargetId
 "6ab5c208-9fc4-4697-84b7-b02a6cc25f7d" -WindowId "mw-06cf17cbefcb4bf4f"
```

出力:

```
WindowId             WindowTargetId
--------             --------------
mw-06cf17cbefcb4bf4f 6ab5c208-9fc4-4697-84b7-b02a6cc25f7d
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「DeregisterTargetFromMaintenanceWindow」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DeregisterTaskFromMaintenanceWindow** を使用する

次のサンプルコードは、DeregisterTaskFromMaintenanceWindow を使用する方法を説明しています。

CLI

AWS CLI

メンテナンスウィンドウからタスクを削除するには

次の deregister-task-from-maintenance-window 例では、指定されたタスクを指定されたメンテナンスウィンドウから削除します。

```
aws ssm deregister-task-from-maintenance-window \
    --window-id "mw-ab12cd34ef56gh78" \
    --window-task-id "1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4d5e6c"
```

出力:

```
{
    "WindowTaskId":"1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4d5e6c",
    "WindowId":"mw-ab12cd34ef56gh78"
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「Systems Manager Maintenance Windows のチュートリアル (AWS CLI)」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「DeregisterTaskFromMaintenanceWindow」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、メンテナンスウィンドウからタスクを削除します。

```
Unregister-SSMTaskFromMaintenanceWindow -WindowTaskId "f34a2c47-ddfd-4c85-
a88d-72366b69af1b" -WindowId "mw-03a342e62c96d31b0"
```

出力:

```
WindowId             WindowTaskId
--------             ------------
mw-03a342e62c96d31b0 f34a2c47-ddfd-4c85-a88d-72366b69af1b
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「DeregisterTaskFromMaintenanceWindow」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DescribeActivations** を使用する

次のサンプルコードは、DescribeActivations を使用する方法を説明しています。

CLI

AWS CLI

アクティベーションについて表示するには

次の describe-activations の例では、AWS アカウントのアクティベーションに関する詳細情報を一覧表示します。

```
aws ssm describe-activations
```

出力:

```
{
    "ActivationList": [
        {
            "ActivationId": "5743558d-563b-4457-8682-d16c3EXAMPLE",
            "Description": "Example1",
            "IamRole": "HybridWebServersRole,
            "RegistrationLimit": 5,
            "RegistrationsCount": 5,
            "ExpirationDate": 1584316800.0,
            "Expired": false,
            "CreatedDate": 1581954699.792
        },
```

```
        {
            "ActivationId": "3ee0322b-f62d-40eb-b672-13ebfEXAMPLE",
            "Description": "Example2",
            "IamRole": "HybridDatabaseServersRole",
            "RegistrationLimit": 5,
            "RegistrationsCount": 5,
            "ExpirationDate": 1580515200.0,
            "Expired": true,
            "CreatedDate": 1578064132.002
        },
    ]
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「Step 4: Create a Managed-Instance Activation for a Hybrid Environment」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「DescribeActivations」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、アカウントのアクティベーションに関する詳細情報を示します。

```
Get-SSMActivation
```

出力:

```
ActivationId        : 08e51e79-1e36-446c-8e63-9458569c1363
CreatedDate         : 3/1/2017 12:01:51 AM
DefaultInstanceName : MyWebServers
Description         :
ExpirationDate      : 3/2/2017 12:01:51 AM
Expired             : False
IamRole             : AutomationRole
RegistrationLimit   : 10
RegistrationsCount  : 0
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「DescribeActivations」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DescribeAssociation** を使用する

次のサンプルコードは、DescribeAssociation を使用する方法を説明しています。

CLI

AWS CLI

例 1: 関連付けの詳細情報を取得するには

次の describe-association の例では、指定された関連付け ID の関連付けを記述します。

```
aws ssm describe-association \
    --association-id "8dfe3659-4309-493a-8755-0123456789ab"
```

出力:

```
{
    "AssociationDescription": {
        "Name": "AWS-GatherSoftwareInventory",
        "AssociationVersion": "1",
        "Date": 1534864780.995,
        "LastUpdateAssociationDate": 1543235759.81,
        "Overview": {
            "Status": "Success",
            "AssociationStatusAggregatedCount": {
                "Success": 2
            }
        },
        "DocumentVersion": "$DEFAULT",
        "Parameters": {
            "applications": [
                "Enabled"
            ],
            "awsComponents": [
                "Enabled"
            ],
```

```
            "customInventory": [
                "Enabled"
            ],
            "files": [
                ""
            ],
            "instanceDetailedInformation": [
                "Enabled"
            ],
            "networkConfig": [
                "Enabled"
            ],
            "services": [
                "Enabled"
            ],
            "windowsRegistry": [
                ""
            ],
            "windowsRoles": [
                "Enabled"
            ],
            "windowsUpdates": [
                "Enabled"
            ]
        },
        "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
        "Targets": [
            {
                "Key": "InstanceIds",
                "Values": [
                    "*"
                ]
            }
        ],
        "ScheduleExpression": "rate(24 hours)",
        "LastExecutionDate": 1550501886.0,
        "LastSuccessfulExecutionDate": 1550501886.0,
        "AssociationName": "Inventory-Association"
    }
}
```


詳細については、「AWS Systems Manager ユーザーガイド」の「関連付けの編集と新しいバージョンの作成」を参照してください。

例 2: 特定のインスタンスとドキュメントの関連付けの詳細情報を取得するには

次の describe-association の例では、インスタンスとドキュメントの関連付けを記述します。

```
aws ssm describe-association \
    --instance-id "i-1234567890abcdef0" \
    --name "AWS-UpdateSSMAgent"
```

出力:

```
{
    "AssociationDescription": {
        "Status": {
            "Date": 1487876122.564,
            "Message": "Associated with AWS-UpdateSSMAgent",
            "Name": "Associated"
        },
        "Name": "AWS-UpdateSSMAgent",
        "InstanceId": "i-1234567890abcdef0",
        "Overview": {
            "Status": "Pending",
            "DetailedStatus": "Associated",
            "AssociationStatusAggregatedCount": {
                "Pending": 1
            }
        },
        "AssociationId": "d8617c07-2079-4c18-9847-1234567890ab",
        "DocumentVersion": "$DEFAULT",
        "LastUpdateAssociationDate": 1487876122.564,
        "Date": 1487876122.564,
        "Targets": [
            {
                "Values": [
                    "i-1234567890abcdef0"
                ],
                "Key": "InstanceIds"
            }
        ]
    }
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「関連付けの編集と新しいバージョンの作成」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「DescribeAssociation」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、インスタンスとドキュメントの関連付けを記述します。

```
Get-SSMAssociation -InstanceId "i-0000293ffd8c57862" -Name "AWS-UpdateSSMAgent"
```

出力:

```
Name                  : AWS-UpdateSSMAgent
InstanceId            : i-0000293ffd8c57862
Date                  : 2/23/2017 6:55:22 PM
Status.Name           : Pending
Status.Date           : 2/20/2015 8:31:11 AM
Status.Message        : temp_status_change
Status.AdditionalInfo : Additional-Config-Needed
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「DescribeAssociation」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DescribeAssociationExecutionTargets** を使用する

次のサンプルコードは、DescribeAssociationExecutionTargets を使用する方法を説明しています。

CLI

AWS CLI

関連付けの実行の詳細情報を取得するには

次の describe-association-execution-targets の例では、指定された関連付けの実行を記述します。

```
aws ssm describe-association-execution-targets \
    --association-id "8dfe3659-4309-493a-8755-0123456789ab" \
    --execution-id "7abb6378-a4a5-4f10-8312-0123456789ab"
```

出力:

```
{
    "AssociationExecutionTargets": [
        {
            "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
            "AssociationVersion": "1",
            "ExecutionId": "7abb6378-a4a5-4f10-8312-0123456789ab",
            "ResourceId": "i-1234567890abcdef0",
            "ResourceType": "ManagedInstance",
            "Status": "Success",
            "DetailedStatus": "Success",
            "LastExecutionDate": 1550505538.497,
            "OutputSource": {
                "OutputSourceId": "97fff367-fc5a-4299-aed8-0123456789ab",
                "OutputSourceType": "RunCommand"
            }
        }
    ]
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「関連付けの履歴の表示」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「DescribeAssociationExecutionTargets」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、関連付けの実行ターゲットの一部であるリソース ID とその実行ステータスを表示します。

```
Get-SSMAssociationExecutionTarget -AssociationId 123a45a0-
c678-9012-3456-78901234db5e -ExecutionId 123a45a0-c678-9012-3456-78901234db5e |
 Select-Object ResourceId, Status
```

出力:

```
ResourceId           Status
----------           ------
i-0b1b2a3456f7a890b  Success
i-01c12a45d6fc7a89f  Success
i-0a1caf234f56d7dc8  Success
i-012a3fd45af6dbcfe  Failed
i-0ddc1df23c4a5fb67  Success
```

例 2: このコマンドは、コマンドドキュメントが関連付けられている昨日以降の特定のオートメーションにおける、特定の実行をチェックします。さらに、関連付けの実行が失敗したかどうかを確認し、失敗した場合は、実行のコマンド呼び出しの詳細情報とインスタンス ID が表示されます。

```
$AssociationExecution= Get-SSMAssociationExecutionTarget -
AssociationId 1c234567-890f-1aca-a234-5a678d901cb0 -ExecutionId
 12345ca12-3456-2345-2b45-23456789012 |
    Where-Object {$_.LastExecutionDate -gt (Get-Date -Hour 00 -Minute
 00).AddDays(-1)}

foreach ($execution in $AssociationExecution) {
    if($execution.Status -ne 'Success'){
        Write-Output "There was an issue executing the association
 $($execution.AssociationId) on $($execution.ResourceId)"
        Get-SSMCommandInvocation -CommandId
 $execution.OutputSource.OutputSourceId -Detail:$true | Select-Object -
ExpandProperty CommandPlugins
    }
}
```

出力:

```
There was an issue executing the association 1c234567-890f-1aca-a234-5a678d901cb0
 on i-0a1caf234f56d7dc8
```

```
Name                    : aws:runPowerShellScript
Output                  :
                          ----------ERROR-------
                          failed to run commands: exit status 1
OutputS3BucketName      :
OutputS3KeyPrefix       :
OutputS3Region          : eu-west-1
ResponseCode            : 1
ResponseFinishDateTime  : 5/29/2019 11:04:49 AM
ResponseStartDateTime   : 5/29/2019 11:04:49 AM
StandardErrorUrl        :
StandardOutputUrl       :
Status                  : Failed
StatusDetails           : Failed
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「DescribeAssociationExecutionTargets」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DescribeAssociationExecutions** を使用する

次のサンプルコードは、DescribeAssociationExecutions を使用する方法を説明しています。

CLI

AWS CLI

例 1: 関連付けのすべての実行に関する詳細情報を取得するには

次の describe-association-executions の例では、指定された関連付けのすべての実行を記述します。

```
aws ssm describe-association-executions \
    --association-id "8dfe3659-4309-493a-8755-0123456789ab"
```

出力:

```
{
```

```
    "AssociationExecutions": [
        {
            "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
            "AssociationVersion": "1",
            "ExecutionId": "474925ef-1249-45a2-b93d-0123456789ab",
            "Status": "Success",
            "DetailedStatus": "Success",
            "CreatedTime": 1550505827.119,
            "ResourceCountByStatus": "{Success=1}"
        },
        {
            "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
            "AssociationVersion": "1",
            "ExecutionId": "7abb6378-a4a5-4f10-8312-0123456789ab",
            "Status": "Success",
            "DetailedStatus": "Success",
            "CreatedTime": 1550505536.843,
            "ResourceCountByStatus": "{Success=1}"
        },
        ...
    ]
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「関連付けの履歴の表示」を参照してください。

例 2: 特定の日付および時刻より後における、関連付けのすべての実行の詳細情報を取得するには

次の describe-association-executions の例では、指定した日付および時刻より後における関連付けのすべての実行を記述します。

```
aws ssm describe-association-executions \
    --association-id "8dfe3659-4309-493a-8755-0123456789ab" \
    --filters "Key=CreatedTime,Value=2019-02-18T16:00:00Z,Type=GREATER_THAN"
```

出力:

```
{
    "AssociationExecutions": [
        {
            "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
```

```
            "AssociationVersion": "1",
            "ExecutionId": "474925ef-1249-45a2-b93d-0123456789ab",
            "Status": "Success",
            "DetailedStatus": "Success",
            "CreatedTime": 1550505827.119,
            "ResourceCountByStatus": "{Success=1}"
        },
        {
            "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
            "AssociationVersion": "1",
            "ExecutionId": "7abb6378-a4a5-4f10-8312-0123456789ab",
            "Status": "Success",
            "DetailedStatus": "Success",
            "CreatedTime": 1550505536.843,
            "ResourceCountByStatus": "{Success=1}"
        },
        ...
    ]
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「関連付けの履歴の表示」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「DescribeAssociationExecutions」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、指定された関連付け ID の実行を返します。

```
Get-SSMAssociationExecution -AssociationId 123a45a0-c678-9012-3456-78901234db5e
```

出力:

```
AssociationId         : 123a45a0-c678-9012-3456-78901234db5e
AssociationVersion    : 2
CreatedTime           : 3/2/2019 8:53:29 AM
DetailedStatus        :
ExecutionId           : 123a45a0-c678-9012-3456-78901234db5e
LastExecutionDate     : 1/1/0001 12:00:00 AM
```

```
ResourceCountByStatus : {Success=4}
Status                : Success
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「DescribeAssociationExecutions」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DescribeAutomationExecutions** を使用する

次のサンプルコードは、DescribeAutomationExecutions を使用する方法を説明しています。

CLI

AWS CLI

オートメーションの実行を記述するには

次の describe-automation-executions の例では、オートメーションの実行の詳細情報を表示します。

```
aws ssm describe-automation-executions \
    --filters Key=ExecutionId,Values=73c8eef8-f4ee-4a05-820c-e354fEXAMPLE
```

出力:

```
{
    "AutomationExecutionMetadataList": [
        {
            "AutomationExecutionId": "73c8eef8-f4ee-4a05-820c-e354fEXAMPLE",
            "DocumentName": "AWS-StartEC2Instance",
            "DocumentVersion": "1",
            "AutomationExecutionStatus": "Success",
            "ExecutionStartTime": 1583737233.748,
            "ExecutionEndTime": 1583737234.719,
            "ExecutedBy": "arn:aws:sts::29884EXAMPLE:assumed-role/
mw_service_role/OrchestrationService",
            "LogFile": "",
            "Outputs": {},
```

```
            "Mode": "Auto",
            "Targets": [],
            "ResolvedTargets": {
                "ParameterValues": [],
                "Truncated": false
            },
            "AutomationType": "Local"
        }
    ]
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「シンプルなオートメーションを実行する」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「DescribeAutomationExecutions」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、アカウントに関連付けられているすべてのアクティブなオートメーションの実行と、終了したオートメーションの実行を記述します。

```
Get-SSMAutomationExecutionList
```

出力:

```
AutomationExecutionId     : 4105a4fc-f944-11e6-9d32-8fb2db27a909
AutomationExecutionStatus : Failed
DocumentName              : AWS-UpdateLinuxAmi
DocumentVersion           : 1
ExecutedBy                : admin
ExecutionEndTime          : 2/22/2017 9:17:08 PM
ExecutionStartTime        : 2/22/2017 9:17:02 PM
LogFile                   :
Outputs                   : {[createImage.ImageId,
 Amazon.Runtime.Internal.Util.AlwaysSendList`1[System.String]]}
```

例 2: この例では、AutomationExecutionStatus の「Success」以外の実行について、ExecutionID、ドキュメント、実行開始/終了タイムスタンプを表示します。

```
Get-SSMAutomationExecutionList | Where-Object AutomationExecutionStatus
 -ne "Success" | Select-Object AutomationExecutionId, DocumentName,
 AutomationExecutionStatus, ExecutionStartTime, ExecutionEndTime | Format-Table -
AutoSize
```

出力:

```
AutomationExecutionId                DocumentName
 AutomationExecutionStatus ExecutionStartTime   ExecutionEndTime
--------------------                 ------------
 ------------------------ ------------------   ----------------
e1d2bad3-4567-8901-ae23-456c7c8901be AWS-UpdateWindowsAmi
 Cancelled                 4/16/2019 5:37:04 AM 4/16/2019 5:47:29 AM
61234567-a7f8-90e1-2b34-567b8bf9012c Fixed-UpdateAmi
 Cancelled                 4/16/2019 5:33:04 AM 4/16/2019 5:40:15 AM
91234d56-7e89-0ac1-2aee-34ea5d6a7c89 AWS-UpdateWindowsAmi
 Failed                    4/16/2019 5:22:46 AM 4/16/2019 5:27:29 AM
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「DescribeAutomationExecutions」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DescribeAutomationStepExecutions** を使用する

次のサンプルコードは、DescribeAutomationStepExecutions を使用する方法を説明しています。

CLI

AWS CLI

例 1: オートメーションの実行におけるすべてのステップを表示するには

次の describe-automation-step-executions の例では、オートメーションの実行におけるステップの詳細情報を表示します。

```
aws ssm describe-automation-step-executions \
```

```
    --automation-execution-id 73c8eef8-f4ee-4a05-820c-e354fEXAMPLE
```

出力:

```
{
    "StepExecutions": [
        {
            "StepName": "startInstances",
            "Action": "aws:changeInstanceState",
            "ExecutionStartTime": 1583737234.134,
            "ExecutionEndTime": 1583737234.672,
            "StepStatus": "Success",
            "Inputs": {
                "DesiredState": "\"running\"",
                "InstanceIds": "[\"i-0cb99161f6EXAMPLE\"]"
            },
            "Outputs": {
                "InstanceStates": [
                    "running"
                ]
            },
            "StepExecutionId": "95e70479-cf20-4d80-8018-7e4e2EXAMPLE",
            "OverriddenParameters": {}
        }
    ]
}
```

例 2: オートメーションの実行における特定のステップを表示するには

次の describe-automation-step-executions の例では、オートメーションの実行における特定のステップの詳細情報を表示します。

```
aws ssm describe-automation-step-executions \
    --automation-execution-id 73c8eef8-f4ee-4a05-820c-e354fEXAMPLE \
    --filters Key=StepExecutionId,Values=95e70479-cf20-4d80-8018-7e4e2EXAMPLE
```

詳細については、「AWS Systems Manager ユーザーガイド」の「オートメーションをステップごとに実行する (コマンドライン)」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「DescribeAutomationStepExecutions」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、オートメーションワークフローにおけるすべてのアクティブなステップの実行と、終了したステップの実行に関する情報を表示します。

```
Get-SSMAutomationStepExecution -AutomationExecutionId e1d2bad3-4567-8901-
ae23-456c7c8901be | Select-Object StepName, Action, StepStatus
```

出力:

```
StepName                  Action                   StepStatus
--------                  ------                   ----------
LaunchInstance            aws:runInstances         Success
OSCompatibilityCheck      aws:runCommand           Success
RunPreUpdateScript        aws:runCommand           Success
UpdateEC2Config           aws:runCommand           Cancelled
UpdateSSMAgent            aws:runCommand           Pending
UpdateAWSPVDriver         aws:runCommand           Pending
UpdateAWSEnaNetworkDriver aws:runCommand           Pending
UpdateAWSNVMe             aws:runCommand           Pending
InstallWindowsUpdates     aws:runCommand           Pending
RunPostUpdateScript       aws:runCommand           Pending
RunSysprepGeneralize      aws:runCommand           Pending
StopInstance              aws:changeInstanceState Pending
CreateImage               aws:createImage          Pending
TerminateInstance         aws:changeInstanceState Pending
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「DescribeAutomationStepExecutions」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DescribeAvailablePatches** を使用する

次のサンプルコードは、DescribeAvailablePatches を使用する方法を説明しています。

CLI

AWS CLI

利用可能なパッチを取得するには

次のdescribe-available-patches の例では、Windows Server 2019 で利用でき、MSRC 重要度が「緊急」のすべてのパッチに関する詳細情報を取得します。

```
aws ssm describe-available-patches \
    --
filters "Key=PRODUCT,Values=WindowsServer2019" "Key=MSRC_SEVERITY,Values=Critical"
```

出力:

```
{
    "Patches": [
        {
            "Id": "fe6bd8c2-3752-4c8b-ab3e-1a7ed08767ba",
            "ReleaseDate": 1544047205.0,
            "Title": "2018-11 Update for Windows Server 2019 for x64-based
 Systems (KB4470788)",
            "Description": "Install this update to resolve issues in Windows.
 For a complete listing of the issues that are included in this update, see the
 associated Microsoft Knowledge Base article for more information. After you
 install this item, you may have to restart your computer.",
            "ContentUrl": "https://support.microsoft.com/en-us/kb/4470788",
            "Vendor": "Microsoft",
            "ProductFamily": "Windows",
            "Product": "WindowsServer2019",
            "Classification": "SecurityUpdates",
            "MsrcSeverity": "Critical",
            "KbNumber": "KB4470788",
            "MsrcNumber": "",
            "Language": "All"
        },
        {
            "Id": "c96115e1-5587-4115-b851-22baa46a3f11",
            "ReleaseDate": 1549994410.0,
            "Title": "2019-02 Security Update for Adobe Flash Player for Windows
 Server 2019 for x64-based Systems (KB4487038)",
            "Description": "A security issue has been identified in a Microsoft
 software product that could affect your system. You can help protect your system
```

```
 by installing this update from Microsoft. For a complete listing of the issues
 that are included in this update, see the associated Microsoft Knowledge Base
 article. After you install this update, you may have to restart your system.",
            "ContentUrl": "https://support.microsoft.com/en-us/kb/4487038",
            "Vendor": "Microsoft",
            "ProductFamily": "Windows",
            "Product": "WindowsServer2019",
            "Classification": "SecurityUpdates",
            "MsrcSeverity": "Critical",
            "KbNumber": "KB4487038",
            "MsrcNumber": "",
            "Language": "All"
        },
        ...
    ]
}
```

特定のパッチの詳細情報を取得するには

次の describe-available-patches の例では、指定されたパッチの詳細情報を取得します。

```
aws ssm describe-available-patches \
    --filters "Key=PATCH_ID,Values=KB4480979"
```

出力:

```
{
    "Patches": [
        {
            "Id": "680861e3-fb75-432e-818e-d72e5f2be719",
            "ReleaseDate": 1546970408.0,
            "Title": "2019-01 Security Update for Adobe Flash Player for Windows
 Server 2016 for x64-based Systems (KB4480979)",
            "Description": "A security issue has been identified in a Microsoft
 software product that could affect your system. You can help protect your system
 by installing this update from Microsoft. For a complete listing of the issues
 that are included in this update, see the associated Microsoft Knowledge Base
 article. After you install this update, you may have to restart your system.",
            "ContentUrl": "https://support.microsoft.com/en-us/kb/4480979",
            "Vendor": "Microsoft",
            "ProductFamily": "Windows",
            "Product": "WindowsServer2016",
```

```
            "Classification": "SecurityUpdates",
            "MsrcSeverity": "Critical",
            "KbNumber": "KB4480979",
            "MsrcNumber": "",
            "Language": "All"
        }
    ]
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「Patch Manager の動作の仕組み」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「DescribeAvailablePatches」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、Windows Server 2012 で利用でき、MSRC 重要度が「緊急」のすべてのパッチを取得します。この例で使用される構文には、PowerShell バージョン 3 以降が必要です。

```
$filter1 = @{Key="PRODUCT";Values=@("WindowsServer2012")}
$filter2 = @{Key="MSRC_SEVERITY";Values=@("Critical")}

Get-SSMAvailablePatch -Filter $filter1,$filter2
```

出力:

```
Classification : SecurityUpdates
ContentUrl     : https://support.microsoft.com/en-us/kb/2727528
Description    : A security issue has been identified that could allow an
 unauthenticated remote attacker to compromise your system and gain control
                  over it. You can help protect your system by installing this
 update from Microsoft. After you install this update, you may have to
                  restart your system.
Id             : 1eb507be-2040-4eeb-803d-abc55700b715
KbNumber       : KB2727528
Language       : All
MsrcNumber     : MS12-072
MsrcSeverity   : Critical
```

```
Product        : WindowsServer2012
ProductFamily  : Windows
ReleaseDate    : 11/13/2012 6:00:00 PM
Title          : Security Update for Windows Server 2012 (KB2727528)
Vendor         : Microsoft
...
```

例 2: PowerShell バージョン 2 では、New-Object を使用して各フィルターを作成する必要があります。

```
$filter1 = New-Object
 Amazon.SimpleSystemsManagement.Model.PatchOrchestratorFilter
$filter1.Key = "PRODUCT"
$filter1.Values = "WindowsServer2012"
$filter2 = New-Object
 Amazon.SimpleSystemsManagement.Model.PatchOrchestratorFilter
$filter2.Key = "MSRC_SEVERITY"
$filter2.Values = "Critical"

Get-SSMAvailablePatch -Filter $filter1,$filter2
```

例 3: この例では、過去 20 日間にリリースされた、Windows Server 2019 に一致する製品に適用されるすべてのパッチの更新情報を取得します。

```
Get-SSMAvailablePatch | Where-Object ReleaseDate -ge (Get-Date).AddDays(-20)
 | Where-Object Product -eq "WindowsServer2019" | Select-Object ReleaseDate,
 Product, Title
```

出力:

```
ReleaseDate         Product           Title
-----------         -------           -----
4/9/2019 5:00:12 PM WindowsServer2019 2019-04 Security Update for Adobe Flash
 Player for Windows Server 2019 for x64-based Systems (KB4493478)
4/9/2019 5:00:06 PM WindowsServer2019 2019-04 Cumulative Update for Windows
 Server 2019 for x64-based Systems (KB4493509)
4/2/2019 5:00:06 PM WindowsServer2019 2019-03 Servicing Stack Update for Windows
 Server 2019 for x64-based Systems (KB4493510)
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「DescribeAvailablePatches」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DescribeDocument** を使用する

次のサンプルコードは、DescribeDocument を使用する方法を説明しています。

CLI

AWS CLI

ドキュメントの詳細情報を表示するには

次のdescribe-document の例では、AWS アカウントの Systems Manager ドキュメントに関する詳細情報を表示します。

```
aws ssm describe-document \
    --name "Example"
```

出力:

```
{
    "Document": {
        "Hash":
 "fc2410281f40779e694a8b95975d0f9f316da8a153daa94e3d9921102EXAMPLE",
        "HashType": "Sha256",
        "Name": "Example",
        "Owner": "29884EXAMPLE",
        "CreatedDate": 1583257938.266,
        "Status": "Active",
        "DocumentVersion": "1",
        "Description": "Document Example",
        "Parameters": [
            {
                "Name": "AutomationAssumeRole",
                "Type": "String",
                "Description": "(Required) The ARN of the role that allows
 Automation to perform the actions on your behalf. If no role is specified,
 Systems Manager Automation uses your IAM permissions to execute this document.",
                "DefaultValue": ""
            },
            {
```

```
                "Name": "InstanceId",
                "Type": "String",
                "Description": "(Required) The ID of the Amazon EC2 instance.",
                "DefaultValue": ""
            }
        ],
        "PlatformTypes": [
            "Windows",
            "Linux"
        ],
        "DocumentType": "Automation",
        "SchemaVersion": "0.3",
        "LatestVersion": "1",
        "DefaultVersion": "1",
        "DocumentFormat": "YAML",
        "Tags": []
    }
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「SSM ドキュメントコンテンツを作成する」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「DescribeDocument」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、ドキュメントに関する情報を返します。

```
Get-SSMDocumentDescription -Name "RunShellScript"
```

出力:

```
CreatedDate     : 2/24/2017 5:25:13 AM
DefaultVersion  : 1
Description     : Run an updated script
DocumentType    : Command
DocumentVersion : 1
Hash            :
 f775e5df4904c6fa46686c4722fae9de1950dace25cd9608ff8d622046b68d9b
```

```
HashType         : Sha256
LatestVersion    : 1
Name             : RunShellScript
Owner            : 123456789012
Parameters       : {commands}
PlatformTypes    : {Linux}
SchemaVersion    : 2.0
Sha1             :
Status           : Active
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「DescribeDocument」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DescribeDocumentPermission** を使用する

次のサンプルコードは、DescribeDocumentPermission を使用する方法を説明しています。

CLI

AWS CLI

ドキュメントのアクセス許可を表示するには

次の describe-document-permission の例では、パブリックに共有されている Systems Manager ドキュメントに関するアクセス許可の詳細情報を表示します。

```
aws ssm describe-document-permission \
    --name "Example" \
    --permission-type "Share"
```

出力:

```
{
    "AccountIds": [
        "all"
    ],
```

```
    "AccountSharingInfoList": [
        {
            "AccountId": "all",
            "SharedDocumentVersion": "$DEFAULT"
        }
    ]
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「Share a Systems Manager Document」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「DescribeDocumentPermission」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、ドキュメントのすべてのバージョンを一覧表示します。

```
Get-SSMDocumentVersionList -Name "RunShellScript"
```

出力:

```
CreatedDate          DocumentVersion IsDefaultVersion Name
-----------          --------------- ---------------- ----
2/24/2017 5:25:13 AM 1               True             RunShellScript
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「DescribeDocumentPermission」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DescribeEffectiveInstanceAssociations** を使用する

次のサンプルコードは、DescribeEffectiveInstanceAssociations を使用する方法を説明しています。

CLI

AWS CLI

インスタンスの有効な関連付けの詳細情報を取得するには

次の describe-effective-instance-associations の例では、インスタンスの有効な関連付けに関する詳細情報を取得します。

コマンド:

```
aws ssm describe-effective-instance-associations --instance-
id "i-1234567890abcdef0"
```

出力:

```
{
    "Associations": [
        {
            "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
            "InstanceId": "i-1234567890abcdef0",
            "Content": "{\n    \"schemaVersion\": \"1.2\",\n    \"description\":
 \"Update the Amazon SSM Agent to the latest version or specified version.\",\n
  \"parameters\": {\n        \"version\": {\n            \"default\": \"\",\n
       \"description\": \"(Optional) A specific version of the Amazon SSM Agent
 to install. If not specified, the agent will be updated to the latest version.
\",\n            \"type\": \"String\"\n        },\n        \"allowDowngrade
\": {\n            \"default\": \"false\",\n            \"description\":
 \"(Optional) Allow the Amazon SSM Agent service to be downgraded to an earlier
 version. If set to false, the service can be upgraded to newer versions only
 (default). If set to true, specify the earlier version.\",\n            \"type
\": \"String\",\n            \"allowedValues\": [\n                \"true\",\n
               \"false\"\n            ]\n        }\n    },\n    \"runtimeConfig
\": {\n        \"aws:updateSsmAgent\": {\n            \"properties\": [\n
         {\n                \"agentName\": \"amazon-ssm-agent\",\n
  \"source\": \"https://s3.{Region}.amazonaws.com/amazon-ssm-{Region}/ssm-agent-
manifest.json\",\n                \"allowDowngrade\": \"{{ allowDowngrade }}\",\n
                \"targetVersion\": \"{{ version }}\"\n                }\n
    ]\n        }\n    }\n}\n",
            "AssociationVersion": "1"
        }
    ]
}
```

- API の詳細については、「AWS CLI Command Reference」の「DescribeEffectiveInstanceAssociations」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、インスタンスの有効な関連付けを記述します。

```
Get-SSMEffectiveInstanceAssociationList -InstanceId "i-0000293ffd8c57862" -
MaxResult 5
```

出力:

```
AssociationId                        Content
-------------                        -------
d8617c07-2079-4c18-9847-1655fc2698b0 {...
```

例 2: この例では、インスタンスの有効な関連付けの内容を記述します。

```
(Get-SSMEffectiveInstanceAssociationList -InstanceId "i-0000293ffd8c57862" -
MaxResult 5).Content
```

出力:

```
{
    "schemaVersion": "1.2",
    "description": "Update the Amazon SSM Agent to the latest version or
 specified version.",
    "parameters": {
        "version": {
            "default": "",
            "description": "(Optional) A specific version of the Amazon SSM Agent
 to install. If not specified, the agen
t will be updated to the latest version.",
            "type": "String"
        },
        "allowDowngrade": {
            "default": "false",
            "description": "(Optional) Allow the Amazon SSM Agent service to be
 downgraded to an earlier version. If set
```

```
 to false, the service can be upgraded to newer versions only (default). If set
 to true, specify the earlier version.",
            "type": "String",
            "allowedValues": [
                "true",
                "false"
            ]
        }
    },
    "runtimeConfig": {
        "aws:updateSsmAgent": {
            "properties": [
                {
                "agentName": "amazon-ssm-agent",
                "source": "https://s3.{Region}.amazonaws.com/amazon-ssm-{Region}/
ssm-agent-manifest.json",
                "allowDowngrade": "{{ allowDowngrade }}",
                "targetVersion": "{{ version }}"
                }
            ]
        }
    }
}
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「DescribeEffectiveInstanceAssociations」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DescribeEffectivePatchesForPatchBaseline** を使用する

次のサンプルコードは、DescribeEffectivePatchesForPatchBaseline を使用する方法を説明しています。

CLI

AWS CLI

例 1: カスタムパッチベースラインで定義されている、すべてのパッチを取得するには

次の describe-effective-patches-for-patch-baseline の例では、現在の AWS アカウントのカスタムパッチベースラインで定義されているパッチを返します。カスタムベースラインの場合、--baseline-id には ID のみが必要であることに注意してください。

```
aws ssm describe-effective-patches-for-patch-baseline \
    --baseline-id "pb-08b654cf9b9681f04"
```

出力:

```
{
    "EffectivePatches": [
        {
            "Patch": {
                "Id": "fe6bd8c2-3752-4c8b-ab3e-1a7ed08767ba",
                "ReleaseDate": 1544047205.0,
                "Title": "2018-11 Update for Windows Server 2019 for x64-based
 Systems (KB4470788)",
                "Description": "Install this update to resolve issues in Windows.
 For a complete listing of the issues that are included in this update, see the
 associated Microsoft Knowledge Base article for more information. After you
 install this item, you may have to restart your computer.",
                "ContentUrl": "https://support.microsoft.com/en-us/kb/4470788",
                "Vendor": "Microsoft",
                "ProductFamily": "Windows",
                "Product": "WindowsServer2019",
                "Classification": "SecurityUpdates",
                "MsrcSeverity": "Critical",
                "KbNumber": "KB4470788",
                "MsrcNumber": "",
                "Language": "All"
            },
            "PatchStatus": {
                "DeploymentStatus": "APPROVED",
                "ComplianceLevel": "CRITICAL",
                "ApprovalDate": 1544047205.0
            }
        },
        {
            "Patch": {
                "Id": "915a6b1a-f556-4d83-8f50-b2e75a9a7e58",
                "ReleaseDate": 1549994400.0,
                "Title": "2019-02 Cumulative Update for .NET Framework 3.5 and
 4.7.2 for Windows Server 2019 for x64 (KB4483452)",
```

```
                "Description": "A security issue has been identified in a
 Microsoft software product that could affect your system. You can help protect
 your system by installing this update from Microsoft. For a complete listing
 of the issues that are included in this update, see the associated Microsoft
 Knowledge Base article. After you install this update, you may have to restart
 your system.",
                "ContentUrl": "https://support.microsoft.com/en-us/kb/4483452",
                "Vendor": "Microsoft",
                "ProductFamily": "Windows",
                "Product": "WindowsServer2019",
                "Classification": "SecurityUpdates",
                "MsrcSeverity": "Important",
                "KbNumber": "KB4483452",
                "MsrcNumber": "",
                "Language": "All"
            },
            "PatchStatus": {
                "DeploymentStatus": "APPROVED",
                "ComplianceLevel": "CRITICAL",
                "ApprovalDate": 1549994400.0
            }
        },
        ...
    ],
    "NextToken": "--token string truncated--"
}
```

例 2: AWS マネージドパッチベースラインで定義されている、すべてのパッチを取得するには

次の describe-effective-patches-for-patch-baseline の例では、AWS マネージドパッチベースラインで定義されているパッチを返します。AWS マネージドベースラインの場合、--baseline-id には完全なベースライン ARN が必要であることに注意してください。

```
aws ssm describe-effective-patches-for-patch-baseline \
    --baseline-id "arn:aws:ssm:us-east-2:733109147000:patchbaseline/
pb-020d361a05defe4ed"
```

出力例については、例 1 を参照してください。

詳細については、「AWS Systems Manager ユーザーガイド」の「セキュリティに関連するパッチの選択方法」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「DescribeEffectivePatchesForPatchBaseline」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、すべてのパッチベースラインを一覧表示します。結果の最大表示件数は 1 です。

```
Get-SSMEffectivePatchesForPatchBaseline -BaselineId "pb-0a2f1059b670ebd31" -
MaxResult 1
```

出力:

```
Patch                                          PatchStatus
-----                                          -----------
Amazon.SimpleSystemsManagement.Model.Patch
 Amazon.SimpleSystemsManagement.Model.PatchStatus
```

例 2: この例では、すべてのパッチベースラインのパッチステータスを表示します。結果の最大表示件数は 1 です。

```
(Get-SSMEffectivePatchesForPatchBaseline -BaselineId "pb-0a2f1059b670ebd31" -
MaxResult 1).PatchStatus
```

出力:

```
ApprovalDate          DeploymentStatus
------------          ----------------
12/21/2010 6:00:00 PM APPROVED
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「DescribeEffectivePatchesForPatchBaseline」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DescribeInstanceAssociationsStatus** を使用する

次のサンプルコードは、DescribeInstanceAssociationsStatus を使用する方法を説明しています。

CLI

AWS CLI

インスタンスの関連付けのステータスを表示するには

この例では、インスタンスの関連付けの詳細情報を表示します。

コマンド:

```
aws ssm describe-instance-associations-status --instance-id "i-1234567890abcdef0"
```

出力:

```
{
  "InstanceAssociationStatusInfos": [
      {
          "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
          "Name": "AWS-GatherSoftwareInventory",
          "DocumentVersion": "1",
          "AssociationVersion": "1",
          "InstanceId": "i-1234567890abcdef0",
          "ExecutionDate": 1550501886.0,
          "Status": "Success",
          "ExecutionSummary": "1 out of 1 plugin processed, 1 success, 0 failed,
 0 timedout, 0 skipped. ",
          "AssociationName": "Inventory-Association"
      },
      {
          "AssociationId": "5c5a31f6-6dae-46f9-944c-0123456789ab",
          "Name": "AWS-UpdateSSMAgent",
          "DocumentVersion": "1",
          "AssociationVersion": "1",
          "InstanceId": "i-1234567890abcdef0",
          "ExecutionDate": 1550505828.548,
          "Status": "Success",
          "DetailedStatus": "Success",
          "AssociationName": "UpdateSSMAgent"
```

```
        }
    ]
}
```

- API の詳細については、「AWS CLI Command リファレンス」の「DescribeInstanceAssociationsStatus」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、インスタンスの関連付けの詳細情報を表示します。

```
Get-SSMInstanceAssociationsStatus -InstanceId "i-0000293ffd8c57862"
```

出力:

```
AssociationId    : d8617c07-2079-4c18-9847-1655fc2698b0
DetailedStatus   : Pending
DocumentVersion  : 1
ErrorCode        :
ExecutionDate    : 2/20/2015 8:31:11 AM
ExecutionSummary : temp_status_change
InstanceId       : i-0000293ffd8c57862
Name             : AWS-UpdateSSMAgent
OutputUrl        :
Status           : Pending
```

例 2: この例では、指定されたインスタンス ID におけるインスタンスの関連付けのステータスを確認し、それらの関連付けの実行ステータスを表示します。

```
Get-SSMInstanceAssociationsStatus -InstanceId i-012e3cb4df567e8aa | ForEach-
Object {Get-SSMAssociationExecution -AssociationId .AssociationId}
```

出力:

```
AssociationId         : 512a34a5-c678-1234-1234-12345678db9e
AssociationVersion    : 2
CreatedTime           : 3/2/2019 8:53:29 AM
DetailedStatus        :
ExecutionId           : 512a34a5-c678-1234-1234-12345678db9e
```

```
LastExecutionDate     : 1/1/0001 12:00:00 AM
ResourceCountByStatus : {Success=9}
Status                : Success
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「DescribeInstanceAssociationsStatus」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DescribeInstanceInformation** を使用する

次のサンプルコードは、DescribeInstanceInformation を使用する方法を説明しています。

CLI

AWS CLI

例 1: マネージドインスタンスの情報を表示するには

次の describe-instance-information の例では、各マネージドインスタンスの詳細情報を取得します。

```
aws ssm describe-instance-information
```

例 2: 特定のマネージドインスタンスに関する情報を表示するには

次の describe-instance-information の例では、マネージドインスタンス i-028ea792daEXAMPLE の詳細情報を表示します。

```
aws ssm describe-instance-information \
    --filters "Key=InstanceIds,Values=i-028ea792daEXAMPLE"
```

例 3: 特定のタグキーを持つマネージドインスタンスに関する情報を表示するには

次の describe-instance-information の例では、タグキー DEV を持つマネージドインスタンスの詳細情報を表示します。

```
aws ssm describe-instance-information \
    --filters "Key=tag-key,Values=DEV"
```

出力:

```
{
    "InstanceInformationList": [
        {
            "InstanceId": "i-028ea792daEXAMPLE",
            "PingStatus": "Online",
            "LastPingDateTime": 1582221233.421,
            "AgentVersion": "2.3.842.0",
            "IsLatestVersion": true,
            "PlatformType": "Linux",
            "PlatformName": "SLES",
            "PlatformVersion": "15.1",
            "ResourceType": "EC2Instance",
            "IPAddress": "192.0.2.0",
            "ComputerName": "ip-198.51.100.0.us-east-2.compute.internal",
            "AssociationStatus": "Success",
            "LastAssociationExecutionDate": 1582220806.0,
            "LastSuccessfulAssociationExecutionDate": 1582220806.0,
            "AssociationOverview": {
                "DetailedStatus": "Success",
                "InstanceAssociationStatusAggregatedCount": {
                    "Success": 2
                }
            }
        }
    ]
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「Managed Instances」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「DescribeInstanceInformation」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、各インスタンスの詳細情報を表示します。

```
Get-SSMInstanceInformation
```

出力:

```
ActivationId                          :
AgentVersion                          : 2.0.672.0
AssociationOverview                   :
 Amazon.SimpleSystemsManagement.Model.InstanceAggregatedAssociationOverview
AssociationStatus                     : Success
ComputerName                          : ip-172-31-44-222.us-
west-2.compute.internal
IamRole                               :
InstanceId                            : i-0cb2b964d3e14fd9f
IPAddress                             : 172.31.44.222
IsLatestVersion                       : True
LastAssociationExecutionDate          : 2/24/2017 3:18:09 AM
LastPingDateTime                      : 2/24/2017 3:35:03 AM
LastSuccessfulAssociationExecutionDate : 2/24/2017 3:18:09 AM
Name                                  :
PingStatus                            : ConnectionLost
PlatformName                          : Amazon Linux AMI
PlatformType                          : Linux
PlatformVersion                       : 2016.09
RegistrationDate                      : 1/1/0001 12:00:00 AM
ResourceType                          : EC2Instance
```

例 2: この例では、 -Filter パラメータを使用して、**AgentVersion** が **2.2.800.0** の **us-east-1** リージョンにある AWS Systems Manager インスタンスのみに結果をフィルタリングする方法を示しています。有効な -Filter キー値のリストは、InstanceInformation の API リファレンストピック (https://docs.aws.amazon.com/systems-manager/latest/APIReference/API_InstanceInformation.html#systemsmanager-Type-InstanceInformation-ActivationId) で確認できます。

```
$Filters = @{
    Key="AgentVersion"
    Values="2.2.800.0"
}
Get-SSMInstanceInformation -Region us-east-1 -Filter $Filters
```

出力:

```
ActivationId                          :
AgentVersion                          : 2.2.800.0
```

```
AssociationOverview                     :
 Amazon.SimpleSystemsManagement.Model.InstanceAggregatedAssociationOverview
AssociationStatus                       : Success
ComputerName                            : EXAMPLE-EXAMPLE.WORKGROUP
IamRole                                 :
InstanceId                              : i-EXAMPLEb0792d98ce
IPAddress                               : 10.0.0.01
IsLatestVersion                         : False
LastAssociationExecutionDate            : 8/16/2018 12:02:50 AM
LastPingDateTime                        : 8/16/2018 7:40:27 PM
LastSuccessfulAssociationExecutionDate : 8/16/2018 12:02:50 AM
Name                                    :
PingStatus                              : Online
PlatformName                            : Microsoft Windows Server 2016 Datacenter
PlatformType                            : Windows
PlatformVersion                         : 10.0.14393
RegistrationDate                        : 1/1/0001 12:00:00 AM
ResourceType                            : EC2Instance

ActivationId                            :
AgentVersion                            : 2.2.800.0
AssociationOverview                     :
 Amazon.SimpleSystemsManagement.Model.InstanceAggregatedAssociationOverview
AssociationStatus                       : Success
ComputerName                            : EXAMPLE-EXAMPLE.WORKGROUP
IamRole                                 :
InstanceId                              : i-EXAMPLEac7501d023
IPAddress                               : 10.0.0.02
IsLatestVersion                         : False
LastAssociationExecutionDate            : 8/16/2018 12:00:20 AM
LastPingDateTime                        : 8/16/2018 7:40:35 PM
LastSuccessfulAssociationExecutionDate : 8/16/2018 12:00:20 AM
Name                                    :
PingStatus                              : Online
PlatformName                            : Microsoft Windows Server 2016 Datacenter
PlatformType                            : Windows
PlatformVersion                         : 10.0.14393
RegistrationDate                        : 1/1/0001 12:00:00 AM
ResourceType                            : EC2Instance
```

例 3: この例は、-InstanceInformationFilterList パラメータを使用して、**Windows** または **Linux** の **PlatformTypes** を持つ **us-east-1** リージョンにある AWS Systems Manager インスタンスのみに結果をフィルタリングする方法を示しています。有効な -

InstanceInformationFilterList キー値のリストは、InstanceInformationFilter の API リファレンストピック (https://docs.aws.amazon.com/systems-manager/latest/APIReference/API_InstanceInformationFilter.html) で確認できます。

```
$Filters = @{
   Key="PlatformTypes"
   ValueSet=("Windows","Linux")
}
Get-SSMInstanceInformation -Region us-east-1 -InstanceInformationFilterList
 $Filters
```

出力:

```
ActivationId                          :
AgentVersion                          : 2.2.800.0
AssociationOverview                   :
 Amazon.SimpleSystemsManagement.Model.InstanceAggregatedAssociationOverview
AssociationStatus                     : Success
ComputerName                          : EXAMPLE-EXAMPLE.WORKGROUP
IamRole                               :
InstanceId                            : i-EXAMPLEb0792d98ce
IPAddress                             : 10.0.0.27
IsLatestVersion                       : False
LastAssociationExecutionDate          : 8/16/2018 12:02:50 AM
LastPingDateTime                      : 8/16/2018 7:40:27 PM
LastSuccessfulAssociationExecutionDate : 8/16/2018 12:02:50 AM
Name                                  :
PingStatus                            : Online
PlatformName                          : Ubuntu Server 18.04 LTS
PlatformType                          : Linux
PlatformVersion                       : 18.04
RegistrationDate                      : 1/1/0001 12:00:00 AM
ResourceType                          : EC2Instance

ActivationId                          :
AgentVersion                          : 2.2.800.0
AssociationOverview                   :
 Amazon.SimpleSystemsManagement.Model.InstanceAggregatedAssociationOverview
AssociationStatus                     : Success
ComputerName                          : EXAMPLE-EXAMPLE.WORKGROUP
IamRole                               :
InstanceId                            : i-EXAMPLEac7501d023
IPAddress                             : 10.0.0.100
```

```
IsLatestVersion                          : False
LastAssociationExecutionDate             : 8/16/2018 12:00:20 AM
LastPingDateTime                         : 8/16/2018 7:40:35 PM
LastSuccessfulAssociationExecutionDate : 8/16/2018 12:00:20 AM
Name                                     :
PingStatus                               : Online
PlatformName                             : Microsoft Windows Server 2016 Datacenter
PlatformType                             : Windows
PlatformVersion                          : 10.0.14393
RegistrationDate                         : 1/1/0001 12:00:00 AM
ResourceType                             : EC2Instance
```

例 4: この例では、ssm マネージドインスタンスを一覧表示し、InstanceId、PingStatus、LastPingDateTime、PlatformName を csv ファイルにエクスポートします。

```
Get-SSMInstanceInformation | Select-Object InstanceId, PingStatus,
 LastPingDateTime, PlatformName | Export-Csv Instance-details.csv -
NoTypeInformation
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「DescribeInstanceInformation」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DescribeInstancePatchStates** を使用する

次のサンプルコードは、DescribeInstancePatchStates を使用する方法を説明しています。

CLI

AWS CLI

インスタンスのパッチの概要状態を取得するには

この describe-instance-patch-states の例では、インスタンスのパッチの概要状態を取得します。

```
aws ssm describe-instance-patch-states \
```

```
    --instance-ids "i-1234567890abcdef0"
```

出力:

```
{
    "InstancePatchStates": [
        {
            "InstanceId": "i-1234567890abcdef0",
            "PatchGroup": "my-patch-group",
            "BaselineId": "pb-0713accee01234567",
            "SnapshotId": "521c3536-930c-4aa9-950e-01234567abcd",
            "CriticalNonCompliantCount": 2,
            "SecurityNonCompliantCount": 2,
            "OtherNonCompliantCount": 1,
            "InstalledCount": 123,
            "InstalledOtherCount": 334,
            "InstalledPendingRebootCount": 0,
            "InstalledRejectedCount": 0,
            "MissingCount": 1,
            "FailedCount": 2,
            "UnreportedNotApplicableCount": 11,
            "NotApplicableCount": 2063,
            "OperationStartTime": "2021-05-03T11:00:56-07:00",
            "OperationEndTime": "2021-05-03T11:01:09-07:00",
            "Operation": "Scan",
            "LastNoRebootInstallOperationTime": "2020-06-14T12:17:41-07:00",
            "RebootOption": "RebootIfNeeded"
        }
    ]
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「About Patch Compliance」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「DescribeInstancePatchStates」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、インスタンスのパッチの概要状態を取得します。

```
Get-SSMInstancePatchState -InstanceId "i-08ee91c0b17045407"
```

例 2: この例では、2 つのインスタンスにおけるパッチの概要状態を取得します。

```
Get-SSMInstancePatchState -InstanceId "i-08ee91c0b17045407","i-09a618aec652973a9"
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「DescribeInstancePatchStates」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DescribeInstancePatchStatesForPatchGroup** を使用する

次のサンプルコードは、DescribeInstancePatchStatesForPatchGroup を使用する方法を説明しています。

CLI

AWS CLI

例 1: パッチグループのインスタンスの状態を取得するには

次のdescribe-instance-patch-states-for-patch-group の例では、指定されたパッチグループにおけるインスタンスごとのパッチの概要状態に関する詳細情報を取得します。

```
aws ssm describe-instance-patch-states-for-patch-group \
    --patch-group "Production"
```

出力:

```
{
    "InstancePatchStates": [
        {
            "InstanceId": "i-02573cafcfEXAMPLE",
            "PatchGroup": "Production",
            "BaselineId": "pb-0c10e65780EXAMPLE",
            "SnapshotId": "a3f5ff34-9bc4-4d2c-a665-4d1c1EXAMPLE",
            "OwnerInformation": "",
```

```
            "InstalledCount": 32,
            "InstalledOtherCount": 1,
            "InstalledPendingRebootCount": 0,
            "InstalledRejectedCount": 0,
            "MissingCount": 2,
            "FailedCount": 0,
            "UnreportedNotApplicableCount": 2671,
            "NotApplicableCount": 400,
            "OperationStartTime": "2021-08-04T11:03:50.590000-07:00",
            "OperationEndTime": "2021-08-04T11:04:21.555000-07:00",
            "Operation": "Scan",
            "RebootOption": "NoReboot",
            "CriticalNonCompliantCount": 0,
            "SecurityNonCompliantCount": 1,
            "OtherNonCompliantCount": 0
        },
        {
            "InstanceId": "i-0471e04240EXAMPLE",
            "PatchGroup": "Production",
            "BaselineId": "pb-09ca3fb51fEXAMPLE",
            "SnapshotId": "05d8ffb0-1bbe-4812-ba2d-d9b7bEXAMPLE",
            "OwnerInformation": "",
            "InstalledCount": 32,
            "InstalledOtherCount": 1,
            "InstalledPendingRebootCount": 0,
            "InstalledRejectedCount": 0,
            "MissingCount": 2,
            "FailedCount": 0,
            "UnreportedNotApplicableCount": 2671,
            "NotApplicableCount": 400,
            "OperationStartTime": "2021-08-04T22:06:20.340000-07:00",
            "OperationEndTime": "2021-08-04T22:07:11.220000-07:00",
            "Operation": "Scan",
            "RebootOption": "NoReboot",
            "CriticalNonCompliantCount": 0,
            "SecurityNonCompliantCount": 1,
            "OtherNonCompliantCount": 0
        }
    ]
}
```

例 2: パッチグループの欠落しているパッチが 5 個以上あるインスタンスの状態を取得するには

次の describe-instance-patch-states-for-patch-group の例では、指定されたパッチグループにおいて、欠落しているパッチが 5 個以上あるインスタンスのパッチの概要状態に関する詳細情報を取得します。

```
aws ssm describe-instance-patch-states-for-patch-group \
    --filters Key=MissingCount,Type=GreaterThan,Values=5 \
    --patch-group "Production"
```

出力:

```
{
    "InstancePatchStates": [
        {
            "InstanceId": "i-02573cafcfEXAMPLE",
            "PatchGroup": "Production",
            "BaselineId": "pb-0c10e65780EXAMPLE",
            "SnapshotId": "a3f5ff34-9bc4-4d2c-a665-4d1c1EXAMPLE",
            "OwnerInformation": "",
            "InstalledCount": 46,
            "InstalledOtherCount": 4,
            "InstalledPendingRebootCount": 1,
            "InstalledRejectedCount": 1,
            "MissingCount": 7,
            "FailedCount": 0,
            "UnreportedNotApplicableCount": 232,
            "NotApplicableCount": 654,
            "OperationStartTime": "2021-08-04T11:03:50.590000-07:00",
            "OperationEndTime": "2021-08-04T11:04:21.555000-07:00",
            "Operation": "Scan",
            "RebootOption": "NoReboot",
            "CriticalNonCompliantCount": 0,
            "SecurityNonCompliantCount": 1,
            "OtherNonCompliantCount": 1
        }
    ]
}
```

例 3: パッチグループにおいて、再起動が必要なインスタンスが 10 個未満のインスタンスの状態を取得するには

次のdescribe-instance-patch-states-for-patch-group の例では、指定されたパッチグループにおいて、再起動が必要なインスタンスが 10 個未満であるインスタンスのパッチの概要状態に関する詳細情報を取得します。

```
aws ssm describe-instance-patch-states-for-patch-group \
    --filters Key=InstalledPendingRebootCount,Type=LessThan,Values=10 \
    --patch-group "Production"
```

出力:

```
{
    "InstancePatchStates": [
        {
            "InstanceId": "i-02573cafcfEXAMPLE",
            "BaselineId": "pb-0c10e65780EXAMPLE",
            "SnapshotId": "a3f5ff34-9bc4-4d2c-a665-4d1c1EXAMPLE",
            "PatchGroup": "Production",
            "OwnerInformation": "",
            "InstalledCount": 32,
            "InstalledOtherCount": 1,
            "InstalledPendingRebootCount": 4,
            "InstalledRejectedCount": 0,
            "MissingCount": 2,
            "FailedCount": 0,
            "UnreportedNotApplicableCount": 846,
            "NotApplicableCount": 212,
            "OperationStartTime": "2021-08-046T11:03:50.590000-07:00",
            "OperationEndTime": "2021-08-06T11:04:21.555000-07:00",
            "Operation": "Scan",
            "RebootOption": "NoReboot",
            "CriticalNonCompliantCount": 0,
            "SecurityNonCompliantCount": 1,
            "OtherNonCompliantCount": 0
        }
    ]
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「パッチコンプライアンス状態の値について」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「DescribeInstancePatchStatesForPatchGroup」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、パッチグループにおけるインスタンスごとのパッチの概要状態を取得します。

```
Get-SSMInstancePatchStatesForPatchGroup -PatchGroup "Production"
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「DescribeInstancePatchStatesForPatchGroup」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DescribeInstancePatches** を使用する

次のサンプルコードは、DescribeInstancePatches を使用する方法を説明しています。

CLI

AWS CLI

例 1: インスタンスのパッチ状態の詳細を取得するには

次の describe-instance-patches の例では、指定されたインスタンスのパッチに関する詳細情報を取得します。

```
aws ssm describe-instance-patches \
    --instance-id "i-1234567890abcdef0"
```

出力:

```
{
    "Patches": [
        {
            "Title": "2019-01 Security Update for Adobe Flash Player for Windows
 Server 2016 for x64-based Systems (KB4480979)",
            "KBId": "KB4480979",
            "Classification": "SecurityUpdates",
            "Severity": "Critical",
```

```
            "State": "Installed",
            "InstalledTime": "2019-01-09T00:00:00+00:00"
        },
        {
            "Title": "",
            "KBId": "KB4481031",
            "Classification": "",
            "Severity": "",
            "State": "InstalledOther",
            "InstalledTime": "2019-02-08T00:00:00+00:00"
        },
        ...
    ],
    "NextToken": "--token string truncated--"
}
```

例 2: インスタンスで欠落しているパッチのリストを取得するには

次のdescribe-instance-patches の例では、指定されたインスタンスで欠落しているパッチに関する情報を取得します。

```
aws ssm describe-instance-patches \
    --instance-id "i-1234567890abcdef0" \
    --filters Key=State,Values=Missing
```

出力:

```
{
    "Patches": [
        {
            "Title": "Windows Malicious Software Removal Tool x64 - February 2019
 (KB890830)",
            "KBId": "KB890830",
            "Classification": "UpdateRollups",
            "Severity": "Unspecified",
            "State": "Missing",
            "InstalledTime": "1970-01-01T00:00:00+00:00"
        },
        ...
    ],
    "NextToken": "--token string truncated--"
}
```

詳細については、「AWS Systems Manager」の「パッチコンプライアンス状態の値について」を参照してください。

例 3: インスタンスに対して、指定された InstalledTime よりも後にインストールされたパッチのリストを取得するには

次のdescribe-instance-patches の例では、--filters と --query を組み合わせて、指定されたインスタンスに対して、指定された時刻よりも後にインストールされたパッチに関する情報を取得します。

```
aws ssm describe-instance-patches \
    --instance-id "i-1234567890abcdef0" \
    --filters Key=State,Values=Installed \
    --query "Patches[?InstalledTime >= `2023-01-01T16:00:00`]"
```

出力:

```
{
    "Patches": [
        {
            "Title": "2023-03 Cumulative Update for Windows Server 2019 (1809)
 for x64-based Systems (KB5023702)",
            "KBId": "KB5023702",
            "Classification": "SecurityUpdates",
            "Severity": "Critical",
            "State": "Installed",
            "InstalledTime": "2023-03-16T11:00:00+00:00"
        },
        ...
    ],
    "NextToken": "--token string truncated--"
}
```

- API の詳細については、「AWS CLI Command Reference」の「DescribeInstancePatches」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、インスタンスのパッチコンプライアンスの詳細を取得します。

```
Get-SSMInstancePatch -InstanceId "i-08ee91c0b17045407"
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「DescribeInstancePatches」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DescribeMaintenanceWindowExecutionTaskInvocations** を使用する

次のサンプルコードは、DescribeMaintenanceWindowExecutionTaskInvocations を使用する方法を説明しています。

CLI

AWS CLI

メンテナンスウィンドウのタスク実行で実行される、特定のタスク呼び出しを取得するには

次の describe-maintenance-window-execution-task-invocations の例では、指定されたメンテナンスウィンドウの実行の一部として実行される、指定したタスクの呼び出しを一覧表示します。

```
aws ssm describe-maintenance-window-execution-task-invocations \
    --window-execution-id "518d5565-5969-4cca-8f0e-da3b2a638355" \
    --task-id "ac0c6ae1-daa3-4a89-832e-d384503b6586"
```

出力:

```
{
    "WindowExecutionTaskInvocationIdentities": [
        {
            "Status": "SUCCESS",
            "Parameters": "{\"documentName\":\"AWS-RunShellScript\",
\"instanceIds\":[\"i-0000293ffd8c57862\"],\"parameters\":{\"commands\":[\"df\"]},
\"maxConcurrency\":\"1\",\"maxErrors\":\"1\"}",
            "InvocationId": "e274b6e1-fe56-4e32-bd2a-8073c6381d8b",
            "StartTime": 1487692834.723,
            "EndTime": 1487692834.871,
```

```
            "WindowExecutionId": "518d5565-5969-4cca-8f0e-da3b2a638355",
            "TaskExecutionId": "ac0c6ae1-daa3-4a89-832e-d384503b6586"
        }
    ]
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「タスクとタスクの実行に関する情報の表示 (AWS CLI)」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「DescribeMaintenanceWindowExecutionTaskInvocations」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、メンテナンスウィンドウの実行の一部として実行される、タスクの呼び出しを一覧表示します。

```
Get-SSMMaintenanceWindowExecutionTaskInvocationList -TaskId "ac0c6ae1-
daa3-4a89-832e-d384503b6586" -WindowExecutionId "518d5565-5969-4cca-8f0e-
da3b2a638355"
```

出力:

```
EndTime           : 2/21/2017 4:00:34 PM
ExecutionId       :
InvocationId      : e274b6e1-fe56-4e32-bd2a-8073c6381d8b
OwnerInformation  :
Parameters        : {"documentName":"AWS-RunShellScript","instanceIds":
["i-0000293ffd8c57862"],"parameters":{"commands":["df"]},"maxConcurrency":"1",
                    "maxErrors":"1"}
StartTime         : 2/21/2017 4:00:34 PM
Status            : FAILED
StatusDetails     : The instance IDs list contains an invalid entry.
TaskExecutionId   : ac0c6ae1-daa3-4a89-832e-d384503b6586
WindowExecutionId : 518d5565-5969-4cca-8f0e-da3b2a638355
WindowTargetId    :
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「DescribeMaintenanceWindowExecutionTaskInvocations」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DescribeMaintenanceWindowExecutionTasks** を使用する

次のサンプルコードは、DescribeMaintenanceWindowExecutionTasks を使用する方法を説明しています。

CLI

AWS CLI

メンテナンスウィンドウの実行に関連するすべてのタスクを一覧表示するには

次の ssm describe-maintenance-window-execution-tasks の例では、指定されたメンテナンスウィンドウの実行に関連するタスクを一覧表示します。

```
aws ssm describe-maintenance-window-execution-tasks \
    --window-execution-id "518d5565-5969-4cca-8f0e-da3b2EXAMPLE"
```

出力:

```
{
    "WindowExecutionTaskIdentities": [
        {
            "Status": "SUCCESS",
            "TaskArn": "AWS-RunShellScript",
            "StartTime": 1487692834.684,
            "TaskType": "RUN_COMMAND",
            "EndTime": 1487692835.005,
            "WindowExecutionId": "518d5565-5969-4cca-8f0e-da3b2EXAMPLE",
            "TaskExecutionId": "ac0c6ae1-daa3-4a89-832e-d3845EXAMPLE"
        }
    ]
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「タスクとタスクの実行に関する情報の表示 (AWS CLI)」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「DescribeMaintenanceWindowExecutionTasks」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、メンテナンスウィンドウの実行に関連するタスクを一覧表示します。

```
Get-SSMMaintenanceWindowExecutionTaskList -WindowExecutionId
 "518d5565-5969-4cca-8f0e-da3b2a638355"
```

出力:

```
EndTime           : 2/21/2017 4:00:35 PM
StartTime         : 2/21/2017 4:00:34 PM
Status            : SUCCESS
TaskArn           : AWS-RunShellScript
TaskExecutionId   : ac0c6ae1-daa3-4a89-832e-d384503b6586
TaskType          : RUN_COMMAND
WindowExecutionId : 518d5565-5969-4cca-8f0e-da3b2a638355
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「DescribeMaintenanceWindowExecutionTasks」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DescribeMaintenanceWindowExecutions** を使用する

次のサンプルコードは、DescribeMaintenanceWindowExecutions を使用する方法を説明しています。

CLI

AWS CLI

例 1: メンテナンスウィンドウにおけるすべての実行を一覧表示するには

次の describe-maintenance-window-executions の例では、指定されたメンテナンスウィンドウにおけるすべての実行を一覧表示します。

```
aws ssm describe-maintenance-window-executions \
```

```
    --window-id "mw-ab12cd34eEXAMPLE"
```

出力:

```
{
    "WindowExecutions": [
        {
            "WindowId": "mw-ab12cd34eEXAMPLE",
            "WindowExecutionId": "6027b513-64fe-4cf0-be7d-1191aEXAMPLE",
            "Status": "IN_PROGRESS",
            "StartTime": "2021-08-04T11:00:00.000000-07:00"

        },
        {
            "WindowId": "mw-ab12cd34eEXAMPLE",
            "WindowExecutionId": "ff75b750-4834-4377-8f61-b3cadEXAMPLE",
            "Status": "SUCCESS",
            "StartTime": "2021-08-03T11:00:00.000000-07:00",
            "EndTime": "2021-08-03T11:37:21.450000-07:00"
        },
        {
            "WindowId": "mw-ab12cd34eEXAMPLE",
            "WindowExecutionId": "9fac7dd9-ff21-42a5-96ad-bbc4bEXAMPLE",
            "Status": "FAILED",
            "StatusDetails": "One or more tasks in the orchestration failed.",
            "StartTime": "2021-08-02T11:00:00.000000-07:00",
            "EndTime": "2021-08-02T11:22:36.190000-07:00"
        }
    ]
}
```

例 2: メンテナンスウィンドウにおける指定された日付より前のすべての実行を一覧表示するには

次の describe-maintenance-window-executions の例では、指定されたメンテナンスウィンドウにおける指定された日付より前のすべての実行を一覧表示します。

```
aws ssm describe-maintenance-window-executions \
    --window-id "mw-ab12cd34eEXAMPLE" \
    --filters "Key=ExecutedBefore,Values=2021-08-03T00:00:00Z"
```

出力:

```
{
    "WindowExecutions": [
        {
        "WindowId": "mw-ab12cd34eEXAMPLE",
        "WindowExecutionId": "9fac7dd9-ff21-42a5-96ad-bbc4bEXAMPLE",
        "Status": "FAILED",
        "StatusDetails": "One or more tasks in the orchestration failed.",
        "StartTime": "2021-08-02T11:00:00.000000-07:00",
        "EndTime": "2021-08-02T11:22:36.190000-07:00"
    }
    ]
}
```

例 3: メンテナンスウィンドウにおける指定された日付より後のすべての実行を一覧表示するには

次の describe-maintenance-window-executions の例では、メンテナンスウィンドウにおける指定された日付より後のすべての実行を一覧表示します。

```
aws ssm describe-maintenance-window-executions \
    --window-id "mw-ab12cd34eEXAMPLE" \
    --filters "Key=ExecutedAfter,Values=2021-08-04T00:00:00Z"
```

出力:

```
{
    "WindowExecutions": [
        {
        "WindowId": "mw-ab12cd34eEXAMPLE",
        "WindowExecutionId": "6027b513-64fe-4cf0-be7d-1191aEXAMPLE",
        "Status": "IN_PROGRESS",
        "StartTime": "2021-08-04T11:00:00.000000-07:00"
        }
    ]
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「タスクとタスクの実行に関する情報の表示 (AWS CLI)」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「DescribeMaintenanceWindowExecutions」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、メンテナンスウィンドウにおけるすべての実行を一覧表示します。

```
Get-SSMMaintenanceWindowExecutionList -WindowId "mw-03eb9db42890fb82d"
```

出力:

```
EndTime           : 2/20/2017 6:30:17 PM
StartTime         : 2/20/2017 6:30:16 PM
Status            : FAILED
StatusDetails     : One or more tasks in the orchestration failed.
WindowExecutionId : 6f3215cf-4101-4fa0-9b7b-9523269599c7
WindowId          : mw-03eb9db42890fb82d
```

例 2: この例では、指定されたメンテナンスウィンドウにおける指定された日付より前のすべての実行を一覧表示します。

```
$option1 = @{Key="ExecutedBefore";Values=@("2016-11-04T05:00:00Z")}
Get-SSMMaintenanceWindowExecutionList -WindowId "mw-03eb9db42890fb82d" -Filter
 $option1
```

例 3: この例では、指定されたメンテナンスウィンドウにおける指定された日付より後のすべての実行を一覧表示します。

```
$option1 = @{Key="ExecutedAfter";Values=@("2016-11-04T05:00:00Z")}
Get-SSMMaintenanceWindowExecutionList -WindowId "mw-03eb9db42890fb82d" -Filter
 $option1
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「DescribeMaintenanceWindowExecutions」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DescribeMaintenanceWindowTargets** を使用する

次のサンプルコードは、DescribeMaintenanceWindowTargets を使用する方法を説明しています。

CLI

AWS CLI

例 1: メンテナンスウィンドウのすべてのターゲットを一覧表示するには

次の describe-maintenance-window-targets の例では、メンテナンスウィンドウのすべてのターゲットを一覧表示します。

```
aws ssm describe-maintenance-window-targets \
    --window-id "mw-06cf17cbefEXAMPLE"
```

出力:

```
{
    "Targets": [
        {
            "ResourceType": "INSTANCE",
            "OwnerInformation": "Single instance",
            "WindowId": "mw-06cf17cbefEXAMPLE",
            "Targets": [
                {
                    "Values": [
                        "i-0000293ffdEXAMPLE"
                    ],
                    "Key": "InstanceIds"
                }
            ],
            "WindowTargetId": "350d44e6-28cc-44e2-951f-4b2c9EXAMPLE"
        },
        {
            "ResourceType": "INSTANCE",
            "OwnerInformation": "Two instances in a list",
            "WindowId": "mw-06cf17cbefEXAMPLE",
            "Targets": [
                {
                    "Values": [
```

```
                        "i-0000293ffdEXAMPLE",
                        "i-0cb2b964d3EXAMPLE"
                    ],
                    "Key": "InstanceIds"
                }
            ],
            "WindowTargetId": "e078a987-2866-47be-bedd-d9cf4EXAMPLE"
        }
    ]
}
```

例 2: 特定の所有者情報の値に一致するメンテナンスウィンドウのターゲットを一覧表示するには

この describe-maintenance-window-targets の例では、特定の値を持つメンテナンスウィンドウにおける、すべてのターゲットを一覧表示します。

```
aws ssm describe-maintenance-window-targets \
    --window-id "mw-0ecb1226ddEXAMPLE" \
    --filters "Key=OwnerInformation,Values=CostCenter1"
```

出力:

```
{
    "Targets": [
        {
            "WindowId": "mw-0ecb1226ddEXAMPLE",
            "WindowTargetId": "da89dcc3-7f9c-481d-ba2b-edcb7d0057f9",
            "ResourceType": "INSTANCE",
            "Targets": [
                {
                    "Key": "tag:Environment",
                    "Values": [
                        "Prod"
                    ]
                }
            ],
            "OwnerInformation": "CostCenter1",
            "Name": "ProdTarget1"
        }
    ]
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「メンテナンスウィンドウに関する情報の表示 (AWS CLI)」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「DescribeMaintenanceWindowTargets」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、メンテナンスウィンドウのすべてのターゲットを一覧表示します。

```
Get-SSMMaintenanceWindowTarget -WindowId "mw-06cf17cbefcb4bf4f"
```

出力:

```
OwnerInformation : Single instance
ResourceType     : INSTANCE
Targets          : {InstanceIds}
WindowId         : mw-06cf17cbefcb4bf4f
WindowTargetId   : 350d44e6-28cc-44e2-951f-4b2c985838f6

OwnerInformation : Two instances in a list
ResourceType     : INSTANCE
Targets          : {InstanceIds}
WindowId         : mw-06cf17cbefcb4bf4f
WindowTargetId   : e078a987-2866-47be-bedd-d9cf49177d3a
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「DescribeMaintenanceWindowTargets」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DescribeMaintenanceWindowTasks** を使用する

次のサンプルコードは、DescribeMaintenanceWindowTasks を使用する方法を説明しています。

CLI

AWS CLI

例 1: メンテナンスウィンドウのすべてのタスクを一覧表示するには

次の describe-maintenance-window-tasks の例では、指定されたメンテナンスウィンドウのすべてのタスクを一覧表示します。

```
aws ssm describe-maintenance-window-tasks \
    --window-id "mw-06cf17cbefEXAMPLE"
```

出力:

```
{
    "Tasks": [
        {
            "WindowId": "mw-06cf17cbefEXAMPLE",
            "WindowTaskId": "018b31c3-2d77-4b9e-bd48-c91edEXAMPLE",
            "TaskArn": "AWS-RestartEC2Instance",
            "TaskParameters": {},
            "Type": "AUTOMATION",
            "Description": "Restarting EC2 Instance for maintenance",
            "MaxConcurrency": "1",
            "MaxErrors": "1",
            "Name": "My-Automation-Example-Task",
            "Priority": 0,
            "ServiceRoleArn": "arn:aws:iam::111222333444:role/aws-service-role/
ssm.amazonaws.com/AWSServiceRoleForAmazonSSM",
            "Targets": [
                {
                    "Key": "WindowTargetIds",
                    "Values": [
                        "da89dcc3-7f9c-481d-ba2b-edcb7EXAMPLE"
                    ]
                }
            ]
        },
        {
            "WindowId": "mw-06cf17cbefEXAMPLE",
            "WindowTaskId": "1943dee0-0a17-4978-9bf4-3cc2fEXAMPLE",
            "TaskArn": "AWS-DisableS3BucketPublicReadWrite",
            "TaskParameters": {},
```

```
            "Type": "AUTOMATION",
            "Description": "Automation task to disable read/write access on
 public S3 buckets",
            "MaxConcurrency": "10",
            "MaxErrors": "5",
            "Name": "My-Disable-S3-Public-Read-Write-Access-Automation-Task",
            "Priority": 0,
            "ServiceRoleArn": "arn:aws:iam::111222333444:role/aws-service-role/
ssm.amazonaws.com/AWSServiceRoleForAmazonSSM",
            "Targets": [
                {
                    "Key": "WindowTargetIds",
                    "Values": [
                        "da89dcc3-7f9c-481d-ba2b-edcb7EXAMPLE"
                    ]
                }
            ]
        }
    ]
}
```

例 2: AWS-RunPowerShellScript コマンドドキュメントを呼び出すメンテナンスウィンドウのすべてのタスクを一覧表示するには

次の describe-maintenance-window-tasks の例では、AWS-RunPowerShellScript コマンドドキュメントを呼び出す、指定されたメンテナンスウィンドウのタスクを一覧表示します。

```
aws ssm describe-maintenance-window-tasks \
    --window-id "mw-ab12cd34eEXAMPLE" \
    --filters "Key=TaskArn,Values=AWS-RunPowerShellScript"
```

出力:

```
{
    "Tasks": [
        {
            "WindowId": "mw-ab12cd34eEXAMPLE",
            "WindowTaskId": "0d36e6b4-3a4f-411e-adcb-3558eEXAMPLE",
            "TaskArn": "AWS-RunPowerShellScript",
            "Type": "RUN_COMMAND",
            "Targets": [
```

```
                {
                    "Key": "WindowTargetIds",
                    "Values": [
                        "da89dcc3-7f9c-481d-ba2b-edcb7EXAMPLE"
                    ]
                }
            ],
            "TaskParameters": {},
            "Priority": 1,
            "ServiceRoleArn": "arn:aws:iam::111222333444:role/aws-service-role/
ssm.amazonaws.com/AWSServiceRoleForAmazonSSM",
            "MaxConcurrency": "1",
            "MaxErrors": "1",
            "Name": "MyTask"
        }
    ]
}
```

例 3: メンテナンスウィンドウのタスクのうち、Priority が 3 のすべてのタスクを一覧表示するには

次の describe-maintenance-window-tasks の例では、指定されたメンテナンスウィンドウのタスクのうち、Priority が 3 であるすべてのタスクを一覧表示します。

```
aws ssm describe-maintenance-window-tasks \
    --window-id "mw-ab12cd34eEXAMPLE" \
    --filters "Key=Priority,Values=3"
```

出力:

```
{
    "Tasks": [
        {
            "WindowId": "mw-ab12cd34eEXAMPLE",
            "WindowTaskId": "0d36e6b4-3a4f-411e-adcb-3558eEXAMPLE",
            "TaskArn": "AWS-RunPowerShellScript",
            "Type": "RUN_COMMAND",
            "Targets": [
                {
                    "Key": "WindowTargetIds",
                    "Values": [
                        "da89dcc3-7f9c-481d-ba2b-edcb7EXAMPLE"
                    ]
```

```
                }
            ],
            "TaskParameters": {},
            "Priority": 3,
            "ServiceRoleArn": "arn:aws:iam::111222333444:role/aws-service-role/
ssm.amazonaws.com/AWSServiceRoleForAmazonSSM",
            "MaxConcurrency": "1",
            "MaxErrors": "1",
            "Name": "MyRunCommandTask"
        },
        {
            "WindowId": "mw-ab12cd34eEXAMPLE",
            "WindowTaskId": "ee45feff-ad65-4a6c-b478-5cab8EXAMPLE",
            "TaskArn": "AWS-RestartEC2Instance",
            "Type": "AUTOMATION",
            "Targets": [
                {
                    "Key": "WindowTargetIds",
                    "Values": [
                        "da89dcc3-7f9c-481d-ba2b-edcb7EXAMPLE"
                    ]
                }
            ],
            "TaskParameters": {},
            "Priority": 3,
            "ServiceRoleArn": "arn:aws:iam::111222333444:role/aws-service-role/
ssm.amazonaws.com/AWSServiceRoleForAmazonSSM",
            "MaxConcurrency": "10",
            "MaxErrors": "5",
            "Name": "My-Automation-Task",
            "Description": "A description for my Automation task"
        }
    ]
}
```

例 4: メンテナンスウィンドウのタスクのうち、Priority が 1 で Run Command を使用するすべてのタスクを一覧表示するには

この describe-maintenance-window-tasks の例では、指定されたメンテナンスウィンドウのタスクのうち、Priority が 1 で Run Command を使用するすべてのタスクを一覧表示します。

```
aws ssm describe-maintenance-window-tasks \
```

```
    --window-id "mw-ab12cd34eEXAMPLE" \
    --filters "Key=Priority,Values=1" "Key=TaskType,Values=RUN_COMMAND"
```

出力:

```
{
    "Tasks": [
        {
            "WindowId": "mw-ab12cd34eEXAMPLE",
            "WindowTaskId": "0d36e6b4-3a4f-411e-adcb-3558eEXAMPLE",
            "TaskArn": "AWS-RunPowerShellScript",
            "Type": "RUN_COMMAND",
            "Targets": [
                {
                    "Key": "WindowTargetIds",
                    "Values": [
                        "da89dcc3-7f9c-481d-ba2b-edcb7EXAMPLE"
                    ]
                }
            ],
            "TaskParameters": {},
            "Priority": 1,
            "ServiceRoleArn": "arn:aws:iam::111222333444:role/aws-service-role/
ssm.amazonaws.com/AWSServiceRoleForAmazonSSM",
            "MaxConcurrency": "1",
            "MaxErrors": "1",
            "Name": "MyRunCommandTask"
        }
    ]
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「メンテナンスウィンドウに関する情報の表示 (AWS CLI)」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「DescribeMaintenanceWindowTasks」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、メンテナンスウィンドウのすべてのタスクを一覧表示します。

```
Get-SSMMaintenanceWindowTaskList -WindowId "mw-06cf17cbefcb4bf4f"
```

出力:

```
LoggingInfo    :
MaxConcurrency : 1
MaxErrors      : 1
Priority       : 10
ServiceRoleArn : arn:aws:iam::123456789012:role/MaintenanceWindowsRole
Targets        : {InstanceIds}
TaskArn        : AWS-RunShellScript
TaskParameters : {[commands,
 Amazon.SimpleSystemsManagement.Model.MaintenanceWindowTaskParameterValueExpression]}
Type           : RUN_COMMAND
WindowId       : mw-06cf17cbefcb4bf4f
WindowTaskId   : a23e338d-ff30-4398-8aa3-09cd052ebf17
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「DescribeMaintenanceWindowTasks」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DescribeMaintenanceWindows** を使用する

次のサンプルコードは、DescribeMaintenanceWindows を使用する方法を説明しています。

CLI

AWS CLI

例 1: すべてのメンテナンスウィンドウを一覧表示するには

次の describe-maintenance-windows の例では、現在のリージョンにおける、AWS アカウントのすべてのメンテナンスウィンドウを一覧表示します。

```
aws ssm describe-maintenance-windows
```

出力:

```
{
    "WindowIdentities": [
        {
            "WindowId": "mw-0ecb1226ddEXAMPLE",
            "Name": "MyMaintenanceWindow-1",
            "Enabled": true,
            "Duration": 2,
            "Cutoff": 1,
            "Schedule": "rate(180 minutes)",
            "NextExecutionTime": "2020-02-12T23:19:20.596Z"
        },
        {
            "WindowId": "mw-03eb9db428EXAMPLE",
            "Name": "MyMaintenanceWindow-2",
            "Enabled": true,
            "Duration": 3,
            "Cutoff": 1,
            "Schedule": "rate(7 days)",
            "NextExecutionTime": "2020-02-17T23:22:00.956Z"
        },
    ]
}
```

例 2: すべての有効なメンテナンスウィンドウを一覧表示するには

次の describe-maintenance-windows の例では、すべての有効なメンテナンスウィンドウを一覧表示します。

```
aws ssm describe-maintenance-windows \
    --filters "Key=Enabled,Values=true"
```

例 3: 特定の名前に一致するメンテナンスウィンドウを一覧表示するには

この describe-maintenance-windows の例では、指定された名前を持つすべてのメンテナンスウィンドウを一覧表示します。

```
aws ssm describe-maintenance-windows \
    --filters "Key=Name,Values=MyMaintenanceWindow"
```

詳細については、「AWS Systems Manager ユーザーガイド」の「メンテナンスウィンドウに関する情報の表示 (AWS CLI)」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「DescribeMaintenanceWindows」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、アカウントにおけるすべてのメンテナンスウィンドウを一覧表示します。

```
Get-SSMMaintenanceWindowList
```

出力:

```
Cutoff   : 1
Duration : 4
Enabled  : True
Name     : My-First-Maintenance-Window
WindowId : mw-06d59c1a07c022145
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「DescribeMaintenanceWindows」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI で **DescribeOpsItems** を使用する

次のサンプルコードは、DescribeOpsItems を使用する方法を説明しています。

CLI

AWS CLI

OpsItems のセットを一覧表示するには

次の describe-ops-items の例は、AWS　アカウントで開いているすべての OpsItems のリストを表示します。

```
aws ssm describe-ops-items \
```

```
    --ops-item-filters "Key=Status,Values=Open,Operator=Equal"
```

出力:

```
{
    "OpsItemSummaries": [
        {
            "CreatedBy": "arn:aws:sts::111222333444:assumed-role/OpsItem-CWE-
Role/fbf77cbe264a33509569f23e4EXAMPLE",
            "CreatedTime": "2020-03-14T17:02:46.375000-07:00",
            "LastModifiedBy": "arn:aws:sts::111222333444:assumed-role/OpsItem-
CWE-Role/fbf77cbe264a33509569f23e4EXAMPLE",
            "LastModifiedTime": "2020-03-14T17:02:46.375000-07:00",
            "Source": "SSM",
            "Status": "Open",
            "OpsItemId": "oi-7cfc5EXAMPLE",
            "Title": "SSM Maintenance Window execution failed",
            "OperationalData": {
                "/aws/dedup": {
                    "Value": "{\"dedupString\":\"SSMOpsItems-SSM-maintenance-
window-execution-failed\"}",
                    "Type": "SearchableString"
                },
                "/aws/resources": {
                    "Value": "[{\"arn\":\"arn:aws:ssm:us-
east-2:111222333444:maintenancewindow/mw-034093d322EXAMPLE\"}]",
                    "Type": "SearchableString"
                }
            },
            "Category": "Availability",
            "Severity": "3"
        },
        {
            "CreatedBy": "arn:aws:sts::1112223233444:assumed-role/OpsItem-CWE-
Role/fbf77cbe264a33509569f23e4EXAMPLE",
            "CreatedTime": "2020-02-26T11:43:15.426000-08:00",
            "LastModifiedBy": "arn:aws:sts::111222333444:assumed-role/OpsItem-
CWE-Role/fbf77cbe264a33509569f23e4EXAMPLE",
            "LastModifiedTime": "2020-02-26T11:43:15.426000-08:00",
            "Source": "EC2",
            "Status": "Open",
            "OpsItemId": "oi-6f966EXAMPLE",
            "Title": "EC2 instance stopped",
```

```
            "OperationalData": {
                "/aws/automations": {
                    "Value": "[ { \"automationType\": \"AWS:SSM:Automation\",
 \"automationId\": \"AWS-RestartEC2Instance\" } ]",
                    "Type": "SearchableString"
                },
                "/aws/dedup": {
                    "Value": "{\"dedupString\":\"SSMOpsItems-EC2-instance-stopped
\"}",
                    "Type": "SearchableString"
                },
                "/aws/resources": {
                    "Value": "[{\"arn\":\"arn:aws:ec2:us-
east-2:111222333444:instance/i-0beccfbc02EXAMPLE\"}]",
                    "Type": "SearchableString"
                }
            },
            "Category": "Availability",
            "Severity": "3"
        }
    ]
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「OpsItems を管理する」を参照してください。

- API の詳細については、AWS CLI コマンドリファレンスの「DescribeOpsItems」を参照してください。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
    /**
     * Describes AWS SSM OpsItems asynchronously.
     *
```

```
    * @param key The key to filter OpsItems by (e.g., OPS_ITEM_ID).
    *
    * This method initiates an asynchronous request to describe SSM OpsItems.
    * If the request is successful, it prints the title and status of each
OpsItem.
    * If an exception occurs, it handles the error appropriately.
    */
   public void describeOpsItems(String key) {
       OpsItemFilter filter = OpsItemFilter.builder()
               .key(OpsItemFilterKey.OPS_ITEM_ID)
               .values(key)
               .operator(OpsItemFilterOperator.EQUAL)
               .build();

       DescribeOpsItemsRequest itemsRequest = DescribeOpsItemsRequest.builder()
               .maxResults(10)
               .opsItemFilters(filter)
               .build();

       CompletableFuture<Void> future = CompletableFuture.runAsync(() -> {
           getAsyncClient().describeOpsItems(itemsRequest)
                   .thenAccept(itemsResponse -> {
                       List<OpsItemSummary> items =
itemsResponse.opsItemSummaries();
                       for (OpsItemSummary item : items) {
                           System.out.println("The item title is " +
item.title() + " and the status is " + item.status().toString());
                       }
                   })
                   .exceptionally(ex -> {
                       throw new CompletionException(ex);
                   }).join();
       }).exceptionally(ex -> {
           Throwable cause = (ex instanceof CompletionException) ?
ex.getCause() : ex;
           if (cause instanceof SsmException) {
               throw new RuntimeException("SSM error: " + cause.getMessage(),
cause);
           } else {
               throw new RuntimeException("Unexpected error: " +
cause.getMessage(), cause);
           }
       });
```

```
        try {
            future.join();
        } catch (CompletionException ex) {
            throw ex.getCause() instanceof RuntimeException ? (RuntimeException)
 ex.getCause() : ex;
        }
    }
```

- API の詳細については、「AWS SDK for Java 2.x API リファレンス」の「DescribeOpsItems」を参照してください。

JavaScript

SDK for JavaScript (v3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
import {
  OpsItemFilterOperator,
  OpsItemFilterKey,
  paginateDescribeOpsItems,
  SSMClient,
} from "@aws-sdk/client-ssm";
import { parseArgs } from "node:util";

/**
 * Describe SSM OpsItems.
 * @param {{ opsItemId: string }}
 */
export const main = async ({ opsItemId }) => {
  const client = new SSMClient({});
  try {
    const describeOpsItemsPaginated = [];
    for await (const page of paginateDescribeOpsItems(
      { client },
      {
```

```
        OpsItemFilters: {
          Key: OpsItemFilterKey.OPSITEM_ID,
          Operator: OpsItemFilterOperator.EQUAL,
          Values: opsItemId,
        },
      },
    )) {
      describeOpsItemsPaginated.push(...page.OpsItemSummaries);
    }
    console.log("Here are the ops items:");
    console.log(describeOpsItemsPaginated);
    return { OpsItemSummaries: describeOpsItemsPaginated };
  } catch (caught) {
    if (caught instanceof Error && caught.name === "MissingParameter") {
      console.warn(`${caught.message}. Did you provide this value?`);
    }
    throw caught;
  }
};
```

- API の詳細については、「AWS SDK for JavaScript API リファレンス」の「DescribeOpsItems」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
class OpsItemWrapper:
    """Encapsulates AWS Systems Manager OpsItem actions."""

    def __init__(self, ssm_client):
        """
        :param ssm_client: A Boto3 Systems Manager client.
        """
```

```
        self.ssm_client = ssm_client
        self.id = None

    @classmethod
    def from_client(cls):
        """
        :return: A OpsItemWrapper instance.
        """
        ssm_client = boto3.client("ssm")
        return cls(ssm_client)


    def describe(self):
        """
        Describe an OpsItem.
        """
        try:
            paginator = self.ssm_client.get_paginator("describe_ops_items")
            ops_items = []
            for page in paginator.paginate(
                OpsItemFilters=[
                    {"Key": "OpsItemId", "Values": [self.id], "Operator":
"Equal"}
                ]
            ):
                ops_items.extend(page["OpsItemSummaries"])

            for item in ops_items:
                print(
                    f"The item title is {item['Title']} and the status is
{item['Status']}"
                )
            return len(ops_items) > 0
        except ClientError as err:
            logger.error(
                "Couldn't describe ops item %s. Here's why: %s: %s",
                self.id,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
```

- API の詳細については、「AWS SDK for Python (Boto3) API リファレンス」の「DescribeOpsItems」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI で **DescribeParameters** を使用する

次のサンプルコードは、DescribeParameters を使用する方法を説明しています。

CLI

AWS CLI

例 1: すべてのパラメータを一覧表示するには

次の describe-parameters の例は、現在の AWS アカウントとリージョンのすべてのパラメータを一覧表示します。

```
aws ssm describe-parameters
```

出力:

```
{
    "Parameters": [
        {
            "Name": "MySecureStringParameter",
            "Type": "SecureString",
            "KeyId": "alias/aws/ssm",
            "LastModifiedDate": 1582155479.205,
            "LastModifiedUser": "arn:aws:sts::111222333444:assumed-role/Admin/
Richard-Roe-Managed",
            "Description": "This is a SecureString parameter",
            "Version": 2,
            "Tier": "Advanced",
            "Policies": [
                {
                    "PolicyText": "{\"Type\":\"Expiration\",\"Version\":\"1.0\",
\"Attributes\":{\"Timestamp\":\"2020-07-07T22:30:00Z\"}}",
                    "PolicyType": "Expiration",
                    "PolicyStatus": "Pending"
```

```
                },
                {
                    "PolicyText": "{\"Type\":\"ExpirationNotification\",\"Version
\":\"1.0\",\"Attributes\":{\"Before\":\"12\",\"Unit\":\"Hours\"}}",
                    "PolicyType": "ExpirationNotification",
                    "PolicyStatus": "Pending"
                }
            ]
        },
        {
            "Name": "MyStringListParameter",
            "Type": "StringList",
            "LastModifiedDate": 1582154764.222,
            "LastModifiedUser": "arn:aws:iam::111222333444:user/Mary-Major",
            "Description": "This is a StringList parameter",
            "Version": 1,
            "Tier": "Standard",
            "Policies": []
        },
        {
            "Name": "MyStringParameter",
            "Type": "String",
            "LastModifiedDate": 1582154711.976,
            "LastModifiedUser": "arn:aws:iam::111222333444:user/Alejandro-
Rosalez",
            "Description": "This is a String parameter",
            "Version": 1,
            "Tier": "Standard",
            "Policies": []
        },
        {
            "Name": "latestAmi",
            "Type": "String",
            "LastModifiedDate": 1580862415.521,
            "LastModifiedUser": "arn:aws:sts::111222333444:assumed-role/lambda-
ssm-role/Automation-UpdateSSM-Param",
            "Version": 3,
            "Tier": "Standard",
            "Policies": []
        }
    ]
}
```

例 2: 特定のメタデータに一致するすべてのパラメータを一覧表示するには

この `describe-parameters` の例は、フィルターに一致するすべてのパラメータを一覧表示します。

aws ssm describe-parameters --filters "Key=Type,Values=StringList"

出力:

```
{
    "Parameters": [
        {
            "Name": "MyStringListParameter",
            "Type": "StringList",
            "LastModifiedDate": 1582154764.222,
            "LastModifiedUser": "arn:aws:iam::111222333444:user/Mary-Major",
            "Description": "This is a StringList parameter",
            "Version": 1,
            "Tier": "Standard",
            "Policies": []
        }
    ]
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「Systems Manager のパラメータを検索する」を参照してください。

- API の詳細については、AWS CLI コマンドリファレンスの「DescribeParameters」を参照してください。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.ssm.SsmClient;
```

```
import software.amazon.awssdk.services.ssm.model.GetParameterRequest;
import software.amazon.awssdk.services.ssm.model.GetParameterResponse;
import software.amazon.awssdk.services.ssm.model.SsmException;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */
public class GetParameter {
    public static void main(String[] args) {
        final String usage = """

                Usage:
                    <paraName>

                Where:
                    paraName - The name of the parameter.
                """;

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }

        String paraName = args[0];
        Region region = Region.US_EAST_1;
        SsmClient ssmClient = SsmClient.builder()
                .region(region)
                .build();

        getParaValue(ssmClient, paraName);
        ssmClient.close();
    }

    public static void getParaValue(SsmClient ssmClient, String paraName) {
        try {
            GetParameterRequest parameterRequest = GetParameterRequest.builder()
                    .name(paraName)
                    .build();
```

```
            GetParameterResponse parameterResponse =
 ssmClient.getParameter(parameterRequest);
            System.out.println("The parameter value is " +
 parameterResponse.parameter().value());

        } catch (SsmException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
}
```

- API の詳細については、「AWS SDK for Java 2.x API リファレンス」の「DescribeParameters」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、すべてのパラメータを一覧表示します。

```
Get-SSMParameterList
```

出力:

```
Description      :
KeyId            :
LastModifiedDate : 3/3/2017 6:58:23 PM
LastModifiedUser : arn:aws:iam::123456789012:user/admin
Name             : Welcome
Type             : String
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「DescribeParameters」を参照してください。

Rust

SDK for Rust

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
async fn show_parameters(client: &Client) -> Result<(), Error> {
    let resp = client.describe_parameters().send().await?;

    for param in resp.parameters() {
        println!("  {}", param.name().unwrap_or_default());
    }

    Ok(())
}
```

- API の詳細については、AWS SDK for Rust API リファレンスの「DescribeParameters」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DescribePatchBaselines** を使用する

次のサンプルコードは、DescribePatchBaselines を使用する方法を説明しています。

CLI

AWS CLI

例 1: すべてのパッチベースラインを一覧表示するには

次の describe-patch-baselines の例では、現在のリージョンにおけるアカウントのすべてのパッチベースラインに関する詳細情報を取得します。

```
aws ssm describe-patch-baselines
```

出力:

```
{
    "BaselineIdentities": [
        {
            "BaselineName": "AWS-SuseDefaultPatchBaseline",
            "DefaultBaseline": true,
            "BaselineDescription": "Default Patch Baseline for Suse Provided by
 AWS.",
            "BaselineId": "arn:aws:ssm:us-east-2:733109147000:patchbaseline/
pb-0123fdb36e334a3b2",
            "OperatingSystem": "SUSE"
        },
        {
            "BaselineName": "AWS-DefaultPatchBaseline",
            "DefaultBaseline": false,
            "BaselineDescription": "Default Patch Baseline Provided by AWS.",
            "BaselineId": "arn:aws:ssm:us-east-2:733109147000:patchbaseline/
pb-020d361a05defe4ed",
            "OperatingSystem": "WINDOWS"
        },
        ...
        {
            "BaselineName": "MyWindowsPatchBaseline",
            "DefaultBaseline": true,
            "BaselineDescription": "My patch baseline for EC2 instances for
 Windows Server",
            "BaselineId": "pb-0ad00e0dd7EXAMPLE",
            "OperatingSystem": "WINDOWS"
        }
    ]
}
```

例 2: AWS によって提供されるすべてのパッチベースラインを一覧表示するには

次の describe-patch-baselines の例では、AWS によって提供されるすべてのパッチベースラインを一覧表示します。

```
aws ssm describe-patch-baselines \
    --filters "Key=OWNER,Values=[AWS]"
```

例 3: 所有しているすべてのパッチベースラインを一覧表示するには

次の describe-patch-baselines の例では、現在のリージョンにおけるアカウントで作成されたすべてのカスタムパッチベースラインを一覧表示します。

```
aws ssm describe-patch-baselines \
    --filters "Key=OWNER,Values=[Self]"
```

詳細については、「AWS Systems Manager ユーザーガイド」の「事前定義されたパッチベースラインについて」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「DescribePatchBaselines」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、すべてのパッチベースラインを一覧表示します。

```
Get-SSMPatchBaseline
```

出力:

```
BaselineDescription                                                BaselineId
                                                  BaselineName
------------------                                                ----------
                                                  ------------
Default Patch Baseline Provided by AWS.                           arn:aws:ssm:us-
west-2:123456789012:patchbaseline/pb-04fb4ae6142167966 AWS-DefaultP...
Baseline containing all updates approved for production systems
 pb-045f10b4f382baeda
 Production-B...
Baseline containing all updates approved for production systems
 pb-0a2f1059b670ebd31
 Production-B...
```

例 2: この例では、AWS によって提供されるすべてのパッチベースラインを一覧表示します。この例で使用される構文には、PowerShell バージョン 3 以降が必要です。

```
$filter1 = @{Key="OWNER";Values=@("AWS")}
```

出力:

```
Get-SSMPatchBaseline -Filter $filter1
```

例 3: この例では、所有者しているすべてのパッチベースラインを一覧表示します。この例で使用される構文には、PowerShell バージョン 3 以降が必要です。

```
$filter1 = @{Key="OWNER";Values=@("Self")}
```

出力:

```
Get-SSMPatchBaseline -Filter $filter1
```

例 4: PowerShell バージョン 2 では、New-Object を使用して各タグを作成する必要があります。

```
$filter1 = New-Object
 Amazon.SimpleSystemsManagement.Model.PatchOrchestratorFilter
$filter1.Key = "OWNER"
$filter1.Values = "AWS"

Get-SSMPatchBaseline -Filter $filter1
```

出力:

```
BaselineDescription                     BaselineId
                            BaselineName            DefaultBaselin


                                                    e
------------------                      ----------
                            ------------            --------------
Default Patch Baseline Provided by AWS. arn:aws:ssm:us-
west-2:123456789012:patchbaseline/pb-04fb4ae6142167966 AWS-DefaultPatchBaseline
 True
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「DescribePatchBaselines」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DescribePatchGroupState** を使用する

次のサンプルコードは、DescribePatchGroupState を使用する方法を説明しています。

CLI

AWS CLI

パッチグループの状態を取得するには

次の describe-patch-group-state の例では、パッチグループのパッチコンプライアンスの概要を取得します。

```
aws ssm describe-patch-group-state \
    --patch-group "Production"
```

出力:

```
{
    "Instances": 21,
    "InstancesWithCriticalNonCompliantPatches": 1,
    "InstancesWithFailedPatches": 2,
    "InstancesWithInstalledOtherPatches": 3,
    "InstancesWithInstalledPatches": 21,
    "InstancesWithInstalledPendingRebootPatches": 2,
    "InstancesWithInstalledRejectedPatches": 1,
    "InstancesWithMissingPatches": 3,
    "InstancesWithNotApplicablePatches": 4,
    "InstancesWithOtherNonCompliantPatches": 1,
    "InstancesWithSecurityNonCompliantPatches": 1,
    "InstancesWithUnreportedNotApplicablePatches": 2
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「パッチグループについて」<https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-patch-patchgroups.html> および「パッチコンプライアンス状態の値について」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「DescribePatchGroupState」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、パッチグループのパッチコンプライアンスの概要を取得します。

```
Get-SSMPatchGroupState -PatchGroup "Production"
```

出力:

```
Instances                          : 4
InstancesWithFailedPatches         : 1
InstancesWithInstalledOtherPatches : 4
InstancesWithInstalledPatches      : 3
InstancesWithMissingPatches        : 0
InstancesWithNotApplicablePatches  : 0
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「DescribePatchGroupState」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **DescribePatchGroups** を使用する

次のサンプルコードは、DescribePatchGroups を使用する方法を説明しています。

CLI

AWS CLI

パッチグループの登録を表示するには

次の describe-patch-groups の例では、パッチグループの登録を一覧表示します。

```
aws ssm describe-patch-groups
```

出力:

```
{
    "Mappings": [
        {
            "PatchGroup": "Production",
            "BaselineIdentity": {
                "BaselineId": "pb-0123456789abcdef0",
                "BaselineName": "ProdPatching",
                "OperatingSystem": "WINDOWS",
                "BaselineDescription": "Patches for Production",
                "DefaultBaseline": false
            }
        },
        {
            "PatchGroup": "Development",
            "BaselineIdentity": {
                "BaselineId": "pb-0713accee01234567",
                "BaselineName": "DevPatching",
                "OperatingSystem": "WINDOWS",
                "BaselineDescription": "Patches for Development",
                "DefaultBaseline": true
            }
        },
        ...
    ]
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「Create a Patch Group」<https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-patch-group-tagging.html>__ および「パッチベースラインにパッチグループを追加します」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「DescribePatchGroups」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、パッチグループの登録を一覧表示します。

```
Get-SSMPatchGroup
```

出力:

```
BaselineIdentity                                                PatchGroup
----------------                                                ----------
Amazon.SimpleSystemsManagement.Model.PatchBaselineIdentity Production
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「DescribePatchGroups」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **GetAutomationExecution** を使用する

次のサンプルコードは、GetAutomationExecution を使用する方法を説明しています。

CLI

AWS CLI

オートメーションの実行に関する詳細情報を表示するには

次の get-automation-execution の例では、オートメーションの実行に関する詳細情報を表示します。

```
aws ssm get-automation-execution \
    --automation-execution-id 73c8eef8-f4ee-4a05-820c-e354fEXAMPLE
```

出力:

```
{
    "AutomationExecution": {
        "AutomationExecutionId": "73c8eef8-f4ee-4a05-820c-e354fEXAMPLE",
        "DocumentName": "AWS-StartEC2Instance",
        "DocumentVersion": "1",
        "ExecutionStartTime": 1583737233.748,
        "ExecutionEndTime": 1583737234.719,
        "AutomationExecutionStatus": "Success",
```

```
        "StepExecutions": [
            {
                "StepName": "startInstances",
                "Action": "aws:changeInstanceState",
                "ExecutionStartTime": 1583737234.134,
                "ExecutionEndTime": 1583737234.672,
                "StepStatus": "Success",
                "Inputs": {
                    "DesiredState": "\"running\"",
                    "InstanceIds": "[\"i-0cb99161f6EXAMPLE\"]"
                },
                "Outputs": {
                    "InstanceStates": [
                        "running"
                    ]
                },
                "StepExecutionId": "95e70479-cf20-4d80-8018-7e4e2EXAMPLE",
                "OverriddenParameters": {}
            }
        ],
        "StepExecutionsTruncated": false,
        "Parameters": {
            "AutomationAssumeRole": [
                ""
            ],
            "InstanceId": [
                "i-0cb99161f6EXAMPLE"
            ]
        },
        "Outputs": {},
        "Mode": "Auto",
        "ExecutedBy": "arn:aws:sts::29884EXAMPLE:assumed-role/mw_service_role/
OrchestrationService",
        "Targets": [],
        "ResolvedTargets": {
            "ParameterValues": [],
            "Truncated": false
        }
    }
}
```


詳細については、「AWS Systems Manager ユーザーガイド」の「Walkthrough: Patch a Linux AMI (AWS CLI)」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「GetAutomationExecution」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、オートメーションの実行に関する詳細を表示します。

```
Get-SSMAutomationExecution -AutomationExecutionId "4105a4fc-
f944-11e6-9d32-8fb2db27a909"
```

出力:

```
AutomationExecutionId     : 4105a4fc-f944-11e6-9d32-8fb2db27a909
AutomationExecutionStatus : Failed
DocumentName              : AWS-UpdateLinuxAmi
DocumentVersion           : 1
ExecutionEndTime          : 2/22/2017 9:17:08 PM
ExecutionStartTime        : 2/22/2017 9:17:02 PM
FailureMessage            : Step launchInstance failed maximum allowed times. You
 are not authorized to perform this operation. Encoded
                            authorization failure message:
 B_V2QyyN7NhSZQYpmVzpEc4oSnj2GLTNYnXUHsTbqJkNMoDgubmbtthLmZyaiUYekORIrA42-
fv1x-04q5Fjff6glh
                            Yb6TI5b0GQeeNrpwNvpDzmO-
PSR1swlAbg9fdM9BcNjyrznspUkWpuKu9EC1Ou6v3OXU1KC9nZ7mPlWMFZNkSioQqpwWEvMw-
GZktsQzm67qOhUhBNOLWYhbS
                            pkfiqzY-5nw3S0obx30fhd3EJa5O_-
GjV_a0nFXQJa70ik40bFOrEh3MtCSbrQT6--DvFy_FQ8TKvkIXadyVskeJI84XOF5WmA60f1pi5GI08i-
nRfZS6oDeU

 gELBjjoFKD8s3L2aI0B6umWVxnQOjqhQRxwJ53b54sZJ2PW3v_mtg9-q0CK0ezS3xfh_y0ilaUGOAZG-
xjQFuvU_JZedWpla3xi-MZsmblAifBI
                            (Service: AmazonEC2; Status Code: 403; Error Code:
 UnauthorizedOperation; Request ID:
                            6a002f94-ba37-43fd-99e6-39517715fce5)
Outputs                   : {[createImage.ImageId,
 Amazon.Runtime.Internal.Util.AlwaysSendList`1[System.String]]}
Parameters                : {[AutomationAssumeRole,
 Amazon.Runtime.Internal.Util.AlwaysSendList`1[System.String]], [InstanceIamRole,
```

```
 Amazon.Runtime.Internal.Util.AlwaysSendList`1[System.String]], [SourceAmiId,

 Amazon.Runtime.Internal.Util.AlwaysSendList`1[System.String]]}
StepExecutions            : {launchInstance, updateOSSoftware, stopInstance,
 createImage...}
```

例 2: この例では、指定されたオートメーションの実行 ID におけるステップの詳細情報を一覧表示します。

```
Get-SSMAutomationExecution -AutomationExecutionId e1d2bad3-4567-8901-
ae23-456c7c8901be | Select-Object -ExpandProperty StepExecutions | Select-Object
 StepName, Action, StepStatus, ValidNextSteps
```

出力:

```
StepName                  Action                  StepStatus ValidNextSteps
--------                  ------                  ---------- --------------
LaunchInstance            aws:runInstances        Success
 {OSCompatibilityCheck}
OSCompatibilityCheck      aws:runCommand          Success    {RunPreUpdateScript}
RunPreUpdateScript        aws:runCommand          Success    {UpdateEC2Config}
UpdateEC2Config           aws:runCommand          Cancelled  {}
UpdateSSMAgent            aws:runCommand          Pending    {}
UpdateAWSPVDriver         aws:runCommand          Pending    {}
UpdateAWSEnaNetworkDriver aws:runCommand          Pending    {}
UpdateAWSNVMe             aws:runCommand          Pending    {}
InstallWindowsUpdates     aws:runCommand          Pending    {}
RunPostUpdateScript       aws:runCommand          Pending    {}
RunSysprepGeneralize      aws:runCommand          Pending    {}
StopInstance              aws:changeInstanceState Pending    {}
CreateImage               aws:createImage         Pending    {}
TerminateInstance         aws:changeInstanceState Pending    {}
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「GetAutomationExecution」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **GetCommandInvocation** を使用する

次のサンプルコードは、GetCommandInvocation を使用する方法を説明しています。

CLI

AWS CLI

コマンド呼び出しの詳細情報を表示するには

次の get-command-invocation の例では、指定されたインスタンスにおける指定されたコマンドのすべての呼び出しを一覧表示します。

```
aws ssm get-command-invocation \
    --command-id "ef7fdfd8-9b57-4151-a15c-db9a12345678" \
    --instance-id "i-1234567890abcdef0"
```

出力:

```
{
    "CommandId": "ef7fdfd8-9b57-4151-a15c-db9a12345678",
    "InstanceId": "i-1234567890abcdef0",
    "Comment": "b48291dd-ba76-43e0-b9df-13e11ddaac26:6960febb-2907-4b59-8e1a-
d6ce8EXAMPLE",
    "DocumentName": "AWS-UpdateSSMAgent",
    "DocumentVersion": "",
    "PluginName": "aws:updateSsmAgent",
    "ResponseCode": 0,
    "ExecutionStartDateTime": "2020-02-19T18:18:03.419Z",
    "ExecutionElapsedTime": "PT0.091S",
    "ExecutionEndDateTime": "2020-02-19T18:18:03.419Z",
    "Status": "Success",
    "StatusDetails": "Success",
    "StandardOutputContent": "Updating amazon-ssm-agent from 2.3.842.0 to latest
\nSuccessfully downloaded https://s3.us-east-2.amazonaws.com/amazon-ssm-us-
east-2/ssm-agent-manifest.json\namazon-ssm-agent 2.3.842.0 has already been
 installed, update skipped\n",
    "StandardOutputUrl": "",
    "StandardErrorContent": "",
    "StandardErrorUrl": "",
    "CloudWatchOutputConfig": {
        "CloudWatchLogGroupName": "",
```

```
        "CloudWatchOutputEnabled": false
    }
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「コマンドのステータスについて」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「GetCommandInvocation」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、インスタンスで実行されたコマンドの詳細情報を表示します。

```
Get-SSMCommandInvocationDetail -InstanceId "i-0cb2b964d3e14fd9f" -CommandId
 "b8eac879-0541-439d-94ec-47a80d554f44"
```

出力:

```
CommandId              : b8eac879-0541-439d-94ec-47a80d554f44
Comment                : IP config
DocumentName           : AWS-RunShellScript
ExecutionElapsedTime   : PT0.004S
ExecutionEndDateTime   : 2017-02-22T20:13:16.651Z
ExecutionStartDateTime : 2017-02-22T20:13:16.651Z
InstanceId             : i-0cb2b964d3e14fd9f
PluginName             : aws:runShellScript
ResponseCode           : 0
StandardErrorContent   :
StandardErrorUrl       :
StandardOutputContent  :
StandardOutputUrl      :
Status                 : Success
StatusDetails          : Success
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「GetCommandInvocation」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **GetConnectionStatus** を使用する

次のサンプルコードは、GetConnectionStatus を使用する方法を説明しています。

CLI

AWS CLI

マネージドインスタンスの接続ステータスを表示するには

この get-connection-status の例では、指定されたマネージドインスタンスの接続ステータスを返します。

```
aws ssm get-connection-status \
    --target i-1234567890abcdef0
```

出力:

```
{
    "Target": "i-1234567890abcdef0",
    "Status": "connected"
}
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「GetConnectionStatus」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、インスタンスが接続され、Session Manager 接続を受信する準備ができているかどうかを判断するため、インスタンスの Session Manager 接続ステータスを取得します。

```
Get-SSMConnectionStatus -Target i-0a1caf234f12d3dc4
```

出力:

```
Status    Target
------    ------
Connected i-0a1caf234f12d3dc4
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「GetConnectionStatus」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **GetDefaultPatchBaseline** を使用する

次のサンプルコードは、GetDefaultPatchBaseline を使用する方法を説明しています。

CLI

AWS CLI

例 1: デフォルトの Windows パッチベースラインを表示するには

次の get-default-patch-baseline の例では、Windows Server のデフォルトのパッチベースラインの詳細を取得します。

```
aws ssm get-default-patch-baseline
```

出力:

```
{
  "BaselineId": "pb-0713accee01612345",
  "OperatingSystem": "WINDOWS"
}
```

例 2: デフォルトの Amazon Linux パッチベースラインを表示するには

次の get-default-patch-baseline の例では、Amazon Linux のデフォルトのパッチベースラインの詳細を取得します。

```
aws ssm get-default-patch-baseline \
    --operating-system AMAZON_LINUX
```

出力:

```
{
    "BaselineId": "pb-047c6eb9c8fc12345",
    "OperatingSystem": "AMAZON_LINUX"
}
```

詳細については、「事前定義されたパッチベースラインおよびカスタムパッチベースラインについて」<https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-patch-baselines.html> および「AWS Systems Manager ユーザーガイド」の「既存のパッチベースラインをデフォルトとして設定する」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「GetDefaultPatchBaseline」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、デフォルトのパッチベースラインを表示します。

```
Get-SSMDefaultPatchBaseline
```

出力:

```
arn:aws:ssm:us-west-2:123456789012:patchbaseline/pb-04fb4ae6142167966
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「GetDefaultPatchBaseline」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **GetDeployablePatchSnapshotForInstance** を使用する

次のサンプルコードは、GetDeployablePatchSnapshotForInstance を使用する方法を説明しています。

CLI

AWS CLI

インスタンスが使用するパッチベースラインの現在のスナップショットを取得するには

次の get-deployable-patch-snapshot-for-instance の例では、インスタンスが使用する指定されたパッチベースラインの現在のスナップショットの詳細を取得します。このコマンドは、インスタンス認証情報を使用してインスタンスから実行する必要があります。インスタンス認証情報が使用されるようにするため、aws configure を実行し、インスタンスのリージョンのみを指定します。Access Key および Secret Key フィールドは空のままにします。

ヒント: uuidgen を使用して snapshot-id を生成します。

```
aws ssm get-deployable-patch-snapshot-for-instance \
    --instance-id "i-1234567890abcdef0" \
    --snapshot-id "521c3536-930c-4aa9-950e-01234567abcd"
```

出力:

```
{
    "InstanceId": "i-1234567890abcdef0",
    "SnapshotId": "521c3536-930c-4aa9-950e-01234567abcd",
    "Product": "AmazonLinux2018.03",
    "SnapshotDownloadUrl": "https://patch-baseline-snapshot-us-
east-1.s3.amazonaws.com/
ed85194ef27214f5984f28b4d664d14f7313568fea7d4b6ac6c10ad1f729d7e7-773304212436/
AMAZON_LINUX-521c3536-930c-4aa9-950e-01234567abcd?X-Amz-
Algorithm=AWS4-HMAC-SHA256&X-Amz-Date=20190215T164031Z&X-Amz-
SignedHeaders=host&X-Amz-Expires=86400&X-Amz-Credential=AKIAJ5C56P35AEBRX2QQ
%2F20190215%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-
Signature=efaaaf6e3878e77f48a6697e015efdbda9c426b09c5822055075c062f6ad2149"
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「Parameter name: Snapshot ID」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「GetDeployablePatchSnapshotForInstance」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、インスタンスで使用されるパッチベースラインの現在のスナップショットを表示します。このコマンドは、インスタンス認証情報を使用してインスタンスから実行する必要があります。この例では、インスタンス認証情報が使用されるようにするため、Credentials パラメータに **Amazon.Runtime.InstanceProfileAWSCredentials** オブジェクトを渡します。

```
$credentials = [Amazon.Runtime.InstanceProfileAWSCredentials]::new()
Get-SSMDeployablePatchSnapshotForInstance -SnapshotId "4681775b-098f-4435-
a956-0ef33373ac11" -InstanceId "i-0cb2b964d3e14fd9f" -Credentials $credentials
```

出力:

```
InstanceId          SnapshotDownloadUrl
----------          -------------------
i-0cb2b964d3e14fd9f https://patch-baseline-snapshot-us-west-2.s3-us-
west-2.amazonaws.com/853d0d3db0f0cafe...1692/4681775b-098f-4435...
```

例 2: この例は、完全な SnapshotDownloadUrl を取得する方法を示しています。このコマンドは、インスタンス認証情報を使用してインスタンスから実行する必要があります。この例では、インスタンス認証情報が使用されるようにするため PowerShell セッションが **Amazon.Runtime.InstanceProfileAWSCredentials** オブジェクトを使用するように設定しています。

```
Set-AWSCredential -Credential
 ([Amazon.Runtime.InstanceProfileAWSCredentials]::new())
(Get-SSMDeployablePatchSnapshotForInstance -SnapshotId "4681775b-098f-4435-
a956-0ef33373ac11" -InstanceId "i-0cb2b964d3e14fd9f").SnapshotDownloadUrl
```

出力:

```
https://patch-baseline-snapshot-us-west-2.s3-us-
west-2.amazonaws.com/853d0d3db0f0cafe...
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「GetDeployablePatchSnapshotForInstance」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **GetDocument** を使用する

次のサンプルコードは、GetDocument を使用する方法を説明しています。

CLI

AWS CLI

ドキュメントコンテンツを取得するには

次の get-document の例では、Systems Manager ドキュメントのコンテンツを表示します。

```
aws ssm get-document \
    --name "AWS-RunShellScript"
```

出力:

```
{
    "Name": "AWS-RunShellScript",
    "DocumentVersion": "1",
    "Status": "Active",
    "Content": "{\n    \"schemaVersion\":\"1.2\",\n    \"description\":\"Run
 a shell script or specify the commands to run.\",\n    \"parameters\":{\n
        \"commands\":{\n            \"type\":\"StringList\",\n
 \"description\":\"(Required) Specify a shell script or a command to run.\",
\n            \"minItems\":1,\n            \"displayType\":\"textarea\"\n
      },\n        \"workingDirectory\":{\n            \"type\":\"String\",\n
            \"default\":\"\",\n            \"description\":\"(Optional) The
 path to the working directory on your instance.\",\n            \"maxChars
\":4096\n        },\n        \"executionTimeout\":{\n            \"type\":
\"String\",\n            \"default\":\"3600\",\n            \"description
\":\"(Optional) The time in seconds for a command to complete before it is
 considered to have failed. Default is 3600 (1 hour). Maximum is 172800 (48
 hours).\",\n            \"allowedPattern\":\"([1-9][0-9]{0,4})|(1[0-6][0-9]
{4})|(17[0-1][0-9]{3})|(172[0-7][0-9]{2})|(172800)\"\n        }\n    },\n
 \"runtimeConfig\":{\n        \"aws:runShellScript\":{\n            \"properties
\":[\n                {\n                    \"id\":\"0.aws:runShellScript
```

```
\",\n                    \"runCommand\":\"{{ commands }}\",\n
      \"workingDirectory\":\"{{ workingDirectory }}\",\n
 \"timeoutSeconds\":\"{{ executionTimeout }}\"\n                }\n
  ]\n        }\n    }\n}\n",
    "DocumentType": "Command",
    "DocumentFormat": "JSON"
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「AWS Systems Manager ドキュメント」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「GetDocument」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、ドキュメントのコンテンツを返します。

```
Get-SSMDocument -Name "RunShellScript"
```

出力:

```
Content
-------
{...
```

例 2: この例では、ドキュメントの完全なコンテンツを表示します。

```
(Get-SSMDocument -Name "RunShellScript").Content
{
   "schemaVersion":"2.0",
   "description":"Run an updated script",
   "parameters":{
      "commands":{
         "type":"StringList",
         "description":"(Required) Specify a shell script or a command to run.",
         "minItems":1,
         "displayType":"textarea"
      }
   },
```

```
   "mainSteps":[
      {
         "action":"aws:runShellScript",
         "name":"runShellScript",
         "inputs":{
            "commands":"{{ commands }}"
         }
      },
      {
         "action":"aws:runPowerShellScript",
         "name":"runPowerShellScript",
         "inputs":{
            "commands":"{{ commands }}"
         }
      }
   ]
}
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「GetDocument」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **GetInventory** を使用する

次のサンプルコードは、GetInventory を使用する方法を説明しています。

CLI

AWS CLI

インベントリを表示するには

この例では、インベントリのカスタムメタデータを取得します。

コマンド:

```
aws ssm get-inventory
```

出力:

```
{
  "Entities": [
      {
          "Data": {
              "AWS:InstanceInformation": {
                  "Content": [
                      {
                          "ComputerName": "ip-172-31-44-222.us-
west-2.compute.internal",
                          "InstanceId": "i-0cb2b964d3e14fd9f",
                          "IpAddress": "172.31.44.222",
                          "AgentType": "amazon-ssm-agent",
                          "ResourceType": "EC2Instance",
                          "AgentVersion": "2.0.672.0",
                          "PlatformVersion": "2016.09",
                          "PlatformName": "Amazon Linux AMI",
                          "PlatformType": "Linux"
                      }
                  ],
                  "TypeName": "AWS:InstanceInformation",
                  "SchemaVersion": "1.0",
                  "CaptureTime": "2017-02-20T18:03:58Z"
              }
          },
          "Id": "i-0cb2b964d3e14fd9f"
      }
  ]
}
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「GetInventory」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、インベントリのカスタムメタデータを取得します。

```
Get-SSMInventory
```

出力:

```
Data
     Id
----
     --
{[AWS:InstanceInformation,
 Amazon.SimpleSystemsManagement.Model.InventoryResultItem]} i-0cb2b964d3e14fd9f
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「GetInventory」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **GetInventorySchema** を使用する

次のサンプルコードは、GetInventorySchema を使用する方法を説明しています。

CLI

AWS CLI

インベントリスキーマを表示するには

この例では、アカウントのインベントリタイプ名のリストを返します。

コマンド:

```
aws ssm get-inventory-schema
```

出力:

```
{
  "Schemas": [
      {
          "TypeName": "AWS:AWSComponent",
          "Version": "1.0",
          "Attributes": [
              {
                  "Name": "Name",
                  "DataType": "STRING"
```

```
            },
            {
                "Name": "ApplicationType",
                "DataType": "STRING"
            },
            {
                "Name": "Publisher",
                "DataType": "STRING"
            },
            {
                "Name": "Version",
                "DataType": "STRING"
            },
            {
                "Name": "InstalledTime",
                "DataType": "STRING"
            },
            {
                "Name": "Architecture",
                "DataType": "STRING"
            },
            {
                "Name": "URL",
                "DataType": "STRING"
            }
        ]
    },
    ...
  ],
  "NextToken": "--token string truncated--"
}
```

特定のインベントリタイプのインベントリスキーマを表示するには

この例では、AWS：AWS コンポーネントインベントリタイプのインベントリスキーマを返します。

コマンド:

```
aws ssm get-inventory-schema --type-name "AWS:AWSComponent"
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「GetInventorySchema」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、アカウントのインベントリタイプ名のリストを返します。

```
Get-SSMInventorySchema
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「GetInventorySchema」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **GetMaintenanceWindow** を使用する

次のサンプルコードは、GetMaintenanceWindow を使用する方法を説明しています。

CLI

AWS CLI

メンテナンスウィンドウに関する情報を取得するには

次の get-maintenance-window の例では、指定されたメンテナンスウィンドウの詳細情報を取得します。

```
aws ssm get-maintenance-window \
    --window-id "mw-03eb9db428EXAMPLE"
```

出力:

```
{
    "AllowUnassociatedTargets": true,
    "CreatedDate": 1515006912.957,
    "Cutoff": 1,
    "Duration": 6,
    "Enabled": true,
    "ModifiedDate": 2020-01-01T10:04:04.099Z,
    "Name": "My-Maintenance-Window",
```

```
    "Schedule": "rate(3 days)",
    "WindowId": "mw-03eb9db428EXAMPLE",
    "NextExecutionTime": "2020-02-25T00:08:15.099Z"
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「メンテナンスウィンドウに関する情報の表示 (AWS CLI)」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「GetMaintenanceWindow」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、メンテナンスウィンドウの詳細を取得します。

```
Get-SSMMaintenanceWindow -WindowId "mw-03eb9db42890fb82d"
```

出力:

```
AllowUnassociatedTargets : False
CreatedDate              : 2/20/2017 6:14:05 PM
Cutoff                   : 1
Duration                 : 2
Enabled                  : True
ModifiedDate             : 2/20/2017 6:14:05 PM
Name                     : TestMaintWin
Schedule                 : cron(0 */30 * * * ? *)
WindowId                 : mw-03eb9db42890fb82d
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「GetMaintenanceWindow」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **GetMaintenanceWindowExecution** を使用する

次のサンプルコードは、GetMaintenanceWindowExecution を使用する方法を説明しています。

CLI

AWS CLI

メンテナンスウィンドウのタスクの実行に関する情報を取得するには

次の get-maintenance-window-execution の例では、指定されたメンテナンスウィンドウの一部として実行されるタスクに関する情報を一覧表示します。

```
aws ssm get-maintenance-window-execution \
    --window-execution-id "518d5565-5969-4cca-8f0e-da3b2EXAMPLE"
```

出力:

```
{
    "Status": "SUCCESS",
    "TaskIds": [
        "ac0c6ae1-daa3-4a89-832e-d3845EXAMPLE"
    ],
    "StartTime": 1487692834.595,
    "EndTime": 1487692835.051,
    "WindowExecutionId": "518d5565-5969-4cca-8f0e-da3b2EXAMPLE",
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「タスクとタスクの実行に関する情報の表示 (AWS CLI)」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「GetMaintenanceWindowExecution」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、メンテナンスウィンドウの実行の一部として実行されるタスクに関する情報を一覧表示します。

```
Get-SSMMaintenanceWindowExecution -WindowExecutionId "518d5565-5969-4cca-8f0e-
da3b2a638355"
```

出力:

```
EndTime           : 2/21/2017 4:00:35 PM
StartTime         : 2/21/2017 4:00:34 PM
Status            : FAILED
StatusDetails     : One or more tasks in the orchestration failed.
TaskIds           : {ac0c6ae1-daa3-4a89-832e-d384503b6586}
WindowExecutionId : 518d5565-5969-4cca-8f0e-da3b2a638355
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「GetMaintenanceWindowExecution」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **GetMaintenanceWindowExecutionTask** を使用する

次のサンプルコードは、GetMaintenanceWindowExecutionTask を使用する方法を説明しています。

CLI

AWS CLI

メンテナンスウィンドウのタスクの実行に関する情報を取得するには

次の get-maintenance-window-execution-task の例では、指定されたメンテナンスウィンドウの実行の一部であるタスクに関する情報を一覧表示します。

```
aws ssm get-maintenance-window-execution-task \
    --window-execution-id "518d5565-5969-4cca-8f0e-da3b2EXAMPLE" \
    --task-id "ac0c6ae1-daa3-4a89-832e-d3845EXAMPLE"
```

出力:

```
{
    "WindowExecutionId": "518d5565-5969-4cca-8f0e-da3b2EXAMPLE",
    "TaskExecutionId": "ac0c6ae1-daa3-4a89-832e-d3845EXAMPLE",
    "TaskArn": "AWS-RunPatchBaseline",
    "ServiceRole": "arn:aws:iam::111222333444:role/aws-service-role/
ssm.amazonaws.com/AWSServiceRoleForAmazonSSM",
    "Type": "RUN_COMMAND",
```

```
    "TaskParameters": [
        {
            "BaselineOverride": {
                "Values": [
                    ""
                ]
            },
            "InstallOverrideList": {
                "Values": [
                    ""
                ]
            },
            "Operation": {
                "Values": [
                    "Scan"
                ]
            },
            "RebootOption": {
                "Values": [
                    "RebootIfNeeded"
                ]
            },
            "SnapshotId": {
                "Values": [
                    "{{ aws:ORCHESTRATION_ID }}"
                ]
            },
            "aws:InstanceId": {
                "Values": [
                    "i-02573cafcfEXAMPLE",
                    "i-0471e04240EXAMPLE",
                    "i-07782c72faEXAMPLE"
                ]
            }
        }
    ],
    "Priority": 1,
    "MaxConcurrency": "1",
    "MaxErrors": "3",
    "Status": "SUCCESS",
    "StartTime": "2021-08-04T11:45:35.088000-07:00",
    "EndTime": "2021-08-04T11:53:09.079000-07:00"
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「タスクとタスクの実行に関する情報の表示 (AWS CLI)」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「GetMaintenanceWindowExecutionTask」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、メンテナンスウィンドウの実行の一部であったタスクに関する情報を一覧表示します。

```
Get-SSMMaintenanceWindowExecutionTask -TaskId "ac0c6ae1-daa3-4a89-832e-
d384503b6586" -WindowExecutionId "518d5565-5969-4cca-8f0e-da3b2a638355"
```

出力:

```
EndTime           : 2/21/2017 4:00:35 PM
MaxConcurrency    : 1
MaxErrors         : 1
Priority          : 10
ServiceRole       : arn:aws:iam::123456789012:role/MaintenanceWindowsRole
StartTime         : 2/21/2017 4:00:34 PM
Status            : FAILED
StatusDetails     : The maximum error count was exceeded.
TaskArn           : AWS-RunShellScript
TaskExecutionId   : ac0c6ae1-daa3-4a89-832e-d384503b6586
TaskParameters    :
 {Amazon.Runtime.Internal.Util.AlwaysSendDictionary`2[System.String,Amazon.SimpleSystemsM
                     meterValueExpression]}
Type              : RUN_COMMAND
WindowExecutionId : 518d5565-5969-4cca-8f0e-da3b2a638355
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「GetMaintenanceWindowExecutionTask」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI で **GetParameter** を使用する

次のサンプルコードは、GetParameter を使用する方法を説明しています。

CLI

AWS CLI

例 1: パラメータの値を表示する

次の get-parameter 例は、指定された単一のパラメータの値を一覧表示します。

```
aws ssm get-parameter \
    --name "MyStringParameter"
```

出力:

```
{
    "Parameter": {
        "Name": "MyStringParameter",
        "Type": "String",
        "Value": "Veni",
        "Version": 1,
        "LastModifiedDate": 1530018761.888,
        "ARN": "arn:aws:ssm:us-east-2:111222333444:parameter/MyStringParameter"
        "DataType": "text"
    }
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「Parameter Store の使用」を参照してください。

例 2: SecureString パラメータの値を復号化する

次の get-parameter 例は、指定された SecureString パラメータの値を複合化します。

```
aws ssm get-parameter \
    --name "MySecureStringParameter" \
    --with-decryption
```

出力:

```
{
    "Parameter": {
        "Name": "MySecureStringParameter",
        "Type": "SecureString",
        "Value": "16679b88-310b-4895-a943-e0764EXAMPLE",
        "Version": 2,
        "LastModifiedDate": 1582155479.205,
        "ARN": "arn:aws:ssm:us-east-2:111222333444:parameter/
MySecureStringParameter"
        "DataType": "text"
    }
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「Parameter Store の使用」を参照してください。

例 3: ラベルを使用してパラメータの値を表示する

次の get-parameter 例は、特定のラベルを使用して、指定された単一のパラメータの値を一覧表示します。

```
aws ssm get-parameter \
    --name "MyParameter:label"
```

出力:

```
{
    "Parameter": {
        "Name": "MyParameter",
        "Type": "String",
        "Value": "parameter version 2",
        "Version": 2,
        "Selector": ":label",
        "LastModifiedDate": "2021-07-12T09:49:15.865000-07:00",
        "ARN": "arn:aws:ssm:us-west-2:786973925828:parameter/MyParameter",
        "DataType": "text"
    }
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「パラメータラベルの操作」を参照してください。

例 4: バージョンを使用してパラメータの値を表示する

次の get-parameter 例は、指定された単一のパラメータバージョンの値を一覧表示します。

```
aws ssm get-parameter \
    --name "MyParameter:2"
```

出力:

```
{
    "Parameter": {
        "Name": "MyParameter",
        "Type": "String",
        "Value": "parameter version 2",
        "Version": 2,
        "Selector": ":2",
        "LastModifiedDate": "2021-07-12T09:49:15.865000-07:00",
        "ARN": "arn:aws:ssm:us-west-2:786973925828:parameter/MyParameter",
        "DataType": "text"
    }
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「パラメータラベルの操作」を参照してください。

- API の詳細については、「AWS CLI Command Reference」の「GetParameter」を参照してください。

Rust

SDK for Rust

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
    pub async fn list_path(&self, path: &str) -> Result<Vec<Parameter>, EC2Error>
{
```

```
        let maybe_params: Vec<Result<Parameter, _>> = TryFlatMap::new(
            self.inner
                .get_parameters_by_path()
                .path(path)
                .into_paginator()
                .send(),
        )
        .flat_map(|item| item.parameters.unwrap_or_default())
        .collect()
        .await;
        // Fail on the first error
        let params = maybe_params
            .into_iter()
            .collect::<Result<Vec<Parameter>, _>>()?;
        Ok(params)
    }
```

- API の詳細については、「AWS SDK for Rust API reference」の「GetParameter」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **GetParameterHistory** を使用する

次のサンプルコードは、GetParameterHistory を使用する方法を説明しています。

CLI

AWS CLI

パラメータの値の履歴を取得するには

次の get-parameter-history の例では、指定されたパラメータの変更履歴を、値を含めて一覧表示します。

```
aws ssm get-parameter-history \
    --name "MyStringParameter"
```

出力:

```
{
    "Parameters": [
        {
            "Name": "MyStringParameter",
            "Type": "String",
            "LastModifiedDate": 1582154711.976,
            "LastModifiedUser": "arn:aws:iam::111222333444:user/Mary-Major",
            "Description": "This is the first version of my String parameter",
            "Value": "Veni",
            "Version": 1,
            "Labels": [],
            "Tier": "Standard",
            "Policies": []
        },
        {
            "Name": "MyStringParameter",
            "Type": "String",
            "LastModifiedDate": 1582156093.471,
            "LastModifiedUser": "arn:aws:iam::111222333444:user/Mary-Major",
            "Description": "This is the second version of my String parameter",
            "Value": "Vidi",
            "Version": 2,
            "Labels": [],
            "Tier": "Standard",
            "Policies": []
        },
        {
            "Name": "MyStringParameter",
            "Type": "String",
            "LastModifiedDate": 1582156117.545,
            "LastModifiedUser": "arn:aws:iam::111222333444:user/Mary-Major",
            "Description": "This is the third version of my String parameter",
            "Value": "Vici",
            "Version": 3,
            "Labels": [],
            "Tier": "Standard",
            "Policies": []
        }
    ]
}
```


詳細については、「AWS Systems Manager ユーザーガイド」の「パラメータバージョンの使用」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「GetParameterHistory」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、パラメータの値の履歴を一覧表示します。

```
Get-SSMParameterHistory -Name "Welcome"
```

出力:

```
Description      :
KeyId            :
LastModifiedDate : 3/3/2017 6:55:25 PM
LastModifiedUser : arn:aws:iam::123456789012:user/admin
Name             : Welcome
Type             : String
Value            : helloWorld
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「GetParameterHistory」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **GetParameters** を使用する

次のサンプルコードは、GetParameters を使用する方法を説明しています。

CLI

AWS CLI

例 1: パラメータの値を一覧表示するには

次の get-parameters の例では、指定した 3 つのパラメータの値を一覧表示します。

```
aws ssm get-parameters \
    --names "MyStringParameter" "MyStringListParameter" "MyInvalidParameterName"
```

出力:

```
{
    "Parameters": [
        {
            "Name": "MyStringListParameter",
            "Type": "StringList",
            "Value": "alpha,beta,gamma",
            "Version": 1,
            "LastModifiedDate": 1582154764.222,
            "ARN": "arn:aws:ssm:us-east-2:111222333444:parameter/
MyStringListParameter"
            "DataType": "text"
        },
        {
            "Name": "MyStringParameter",
            "Type": "String",
            "Value": "Vici",
            "Version": 3,
            "LastModifiedDate": 1582156117.545,
            "ARN": "arn:aws:ssm:us-east-2:111222333444:parameter/
MyStringParameter"
            "DataType": "text"
        }
    ],
    "InvalidParameters": [
        "MyInvalidParameterName"
    ]
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「Parameter Store の使用」を参照してください。

例 2: ``--query`` オプションを使用して複数のパラメータの名前と値を一覧表示するには

次の get-parameters の例では、指定したパラメータの名前と値を一覧表示します。

```
aws ssm get-parameters \
    --names MyStringParameter MyStringListParameter \
```

```
    --query "Parameters[*].{Name:Name,Value:Value}"
```

出力:

```
[
    {
        "Name": "MyStringListParameter",
        "Value": "alpha,beta,gamma"
    },
    {
        "Name": "MyStringParameter",
        "Value": "Vidi"
    }
]
```

詳細については、「AWS Systems Manager ユーザーガイド」の「Parameter Store の使用」を参照してください。

例 3: ラベルを使用してパラメータの値を表示する

次の get-parameter 例は、特定のラベルを使用して、指定された単一のパラメータの値を一覧表示します。

```
aws ssm get-parameter \
    --name "MyParameter:label"
```

出力:

```
{
    "Parameters": [
        {
            "Name": "MyLabelParameter",
            "Type": "String",
            "Value": "parameter by label",
            "Version": 1,
            "Selector": ":label",
            "LastModifiedDate": "2021-07-12T09:49:15.865000-07:00",
            "ARN": "arn:aws:ssm:us-west-2:786973925828:parameter/MyParameter",
            "DataType": "text"
        },
        {
            "Name": "MyVersionParameter",
```

```
            "Type": "String",
            "Value": "parameter by version",
            "Version": 2,
            "Selector": ":2",
            "LastModifiedDate": "2021-03-24T16:20:28.236000-07:00",
            "ARN": "arn:aws:ssm:us-west-2:786973925828:parameter/unlabel-param",
            "DataType": "text"
        }
    ],
    "InvalidParameters": []
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「パラメータラベルの操作」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「GetParameters」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、パラメータの値を一覧表示します。

```
Get-SSMParameterValue -Name "Welcome"
```

出力:

```
InvalidParameters Parameters
----------------- ----------
{}                {Welcome}
```

例 2: この例では、値の詳細を一覧表示します。

```
(Get-SSMParameterValue -Name "Welcome").Parameters
```

出力:

```
Name    Type   Value
----    ----   -----
```

```
Welcome String Good day, Sunshine!
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「GetParameters」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **GetPatchBaseline** を使用する

次のサンプルコードは、GetPatchBaseline を使用する方法を説明しています。

CLI

AWS CLI

パッチベースラインを表示するには

次の get-patch-baseline の例では、指定されたパッチベースラインの詳細を取得します。

```
aws ssm get-patch-baseline \
    --baseline-id "pb-0123456789abcdef0"
```

出力:

```
{
    "BaselineId": "pb-0123456789abcdef0",
    "Name": "WindowsPatching",
    "OperatingSystem": "WINDOWS",
    "GlobalFilters": {
        "PatchFilters": []
    },
    "ApprovalRules": {
        "PatchRules": [
            {
                "PatchFilterGroup": {
                    "PatchFilters": [
                        {
                            "Key": "PRODUCT",
```

```
                            "Values": [
                                "WindowsServer2016"
                            ]
                        }
                    ]
                },
                "ComplianceLevel": "CRITICAL",
                "ApproveAfterDays": 0,
                "EnableNonSecurity": false
            }
        ]
    },
    "ApprovedPatches": [],
    "ApprovedPatchesComplianceLevel": "UNSPECIFIED",
    "ApprovedPatchesEnableNonSecurity": false,
    "RejectedPatches": [],
    "RejectedPatchesAction": "ALLOW_AS_DEPENDENCY",
    "PatchGroups": [
        "QA",
        "DEV"
    ],
    "CreatedDate": 1550244180.465,
    "ModifiedDate": 1550244180.465,
    "Description": "Patches for Windows Servers",
    "Sources": []
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「パッチベースラインについて」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「GetPatchBaseline」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、パッチベースラインの詳細を表示します。

```
Get-SSMPatchBaselineDetail -BaselineId "pb-03da896ca3b68b639"
```

出力:

```
ApprovalRules   : Amazon.SimpleSystemsManagement.Model.PatchRuleGroup
ApprovedPatches : {}
BaselineId      : pb-03da896ca3b68b639
CreatedDate     : 3/3/2017 5:02:19 PM
Description     : Baseline containing all updates approved for production systems
GlobalFilters   : Amazon.SimpleSystemsManagement.Model.PatchFilterGroup
ModifiedDate    : 3/3/2017 5:02:19 PM
Name            : Production-Baseline
PatchGroups     : {}
RejectedPatches : {}
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「GetPatchBaseline」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **GetPatchBaselineForPatchGroup** を使用する

次のサンプルコードは、GetPatchBaselineForPatchGroup を使用する方法を説明しています。

CLI

AWS CLI

パッチグループのパッチベースラインを表示するには

次の get-patch-baseline-for-patch-group の例では、指定されたパッチグループのパッチベースラインに関する詳細を取得します。

```
aws ssm get-patch-baseline-for-patch-group \
    --patch-group "DEV"
```

出力:

```
{
    "PatchGroup": "DEV",
    "BaselineId": "pb-0123456789abcdef0",
    "OperatingSystem": "WINDOWS"
```

```
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「Create a Patch Group」<https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-patch-group-tagging.html>__ および「パッチベースラインにパッチグループを追加します」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「GetPatchBaselineForPatchGroup」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、パッチグループのパッチベースラインを表示します。

```
Get-SSMPatchBaselineForPatchGroup -PatchGroup "Production"
```

出力:

```
BaselineId           PatchGroup
----------           ----------
pb-045f10b4f382baeda Production
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「GetPatchBaselineForPatchGroup」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **ListAssociationVersions** を使用する

次のサンプルコードは、ListAssociationVersions を使用する方法を説明しています。

CLI

AWS CLI

特定の関連付け ID のすべてのバージョンの関連付けを取得するには

次の list-association-versions の例では、指定された関連付けのすべてのバージョンを一覧表示します。

```
aws ssm list-association-versions \
    --association-id "8dfe3659-4309-493a-8755-0123456789ab"
```

出力:

```
{
"AssociationVersions": [
        {
            "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
            "AssociationVersion": "1",
            "CreatedDate": 1550505536.726,
            "Name": "AWS-UpdateSSMAgent",
            "Parameters": {
                "allowDowngrade": [
                    "false"
                ],
                "version": [
                    ""
                ]
            },
            "Targets": [
                {
                    "Key": "InstanceIds",
                    "Values": [
                        "i-1234567890abcdef0"
                    ]
                }
            ],
            "ScheduleExpression": "cron(0 00 12 ? * SUN *)",
            "AssociationName": "UpdateSSMAgent"
        }
    ]
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「Systems Manager の関連付けの使用」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「ListAssociationVersions」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、指定された関連付けのすべてのバージョンを取得します。

```
Get-SSMAssociationVersionList -AssociationId 123a45a0-c678-9012-3456-78901234db5e
```

出力:

```
AssociationId      : 123a45a0-c678-9012-3456-78901234db5e
AssociationName    :
AssociationVersion : 2
ComplianceSeverity :
CreatedDate        : 3/12/2019 9:21:01 AM
DocumentVersion    :
MaxConcurrency     :
MaxErrors          :
Name               : AWS-GatherSoftwareInventory
OutputLocation     :
Parameters         : {}
ScheduleExpression :
Targets            : {InstanceIds}

AssociationId      : 123a45a0-c678-9012-3456-78901234db5e
AssociationName    : test-case-1234567890
AssociationVersion : 1
ComplianceSeverity :
CreatedDate        : 3/2/2019 8:53:29 AM
DocumentVersion    :
MaxConcurrency     :
MaxErrors          :
Name               : AWS-GatherSoftwareInventory
OutputLocation     :
Parameters         : {}
ScheduleExpression : rate(30minutes)
Targets            : {InstanceIds}
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「ListAssociationVersions」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **ListAssociations** を使用する

次のサンプルコードは、ListAssociations を使用する方法を説明しています。

CLI

AWS CLI

例 1: 特定のインスタンスの関連付けを一覧表示するには

次の list-associations の例では、AssociationName、UpdateSSMAgent とのすべての関連付けを一覧表示します。

```
aws ssm list-associations /
    --association-filter-list "key=AssociationName,value=UpdateSSMAgent"
```

出力:

```
{
    "Associations": [
        {
            "Name": "AWS-UpdateSSMAgent",
            "InstanceId": "i-1234567890abcdef0",
            "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
            "AssociationVersion": "1",
            "Targets": [
                {
                    "Key": "InstanceIds",
                    "Values": [
                        "i-016648b75dd622dab"
                    ]
                }
            ],
            "Overview": {
                "Status": "Pending",
                "DetailedStatus": "Associated",
                "AssociationStatusAggregatedCount": {
                    "Pending": 1
                }
```

```
            },
            "ScheduleExpression": "cron(0 00 12 ? * SUN *)",
            "AssociationName": "UpdateSSMAgent"
        }
    ]
}
```

詳細については、「Systems Manager ユーザーガイド」の「Systems Manager の関連付けの使用」を参照してください。

例 2: 特定のドキュメントの関連付けを一覧表示するには

次の list-associations の例では、指定したドキュメントのすべての関連付けを一覧表示します。

```
aws ssm list-associations /
    --association-filter-list "key=Name,value=AWS-UpdateSSMAgent"
```

出力:

```
{
    "Associations": [
        {
            "Name": "AWS-UpdateSSMAgent",
            "InstanceId": "i-1234567890abcdef0",
            "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
            "AssociationVersion": "1",
            "Targets": [
                {
                    "Key": "InstanceIds",
                    "Values": [
                        "i-1234567890abcdef0"
                    ]
                }
            ],
            "LastExecutionDate": 1550505828.548,
            "Overview": {
                "Status": "Success",
                "DetailedStatus": "Success",
                "AssociationStatusAggregatedCount": {
                    "Success": 1
                }
            },
```

```
            "ScheduleExpression": "cron(0 00 12 ? * SUN *)",
            "AssociationName": "UpdateSSMAgent"
        },
    {
            "Name": "AWS-UpdateSSMAgent",
            "InstanceId": "i-9876543210abcdef0",
            "AssociationId": "fbc07ef7-b985-4684-b82b-0123456789ab",
            "AssociationVersion": "1",
            "Targets": [
                {
                    "Key": "InstanceIds",
                    "Values": [
                        "i-9876543210abcdef0"
                    ]
                }
            ],
            "LastExecutionDate": 1550507531.0,
            "Overview": {
                "Status": "Success",
                "AssociationStatusAggregatedCount": {
                    "Success": 1
                }
            }
        }
    ]
}
```

詳細については、「Systems Manager ユーザーガイド」の「Systems Manager の関連付けの使用」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「ListAssociations」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、インスタンスのすべての関連付けを一覧表示します。この例で使用される構文には、PowerShell バージョン 3 以降が必要です。

```
$filter1 = @{Key="InstanceId";Value=@("i-0000293ffd8c57862")}
Get-SSMAssociationList -AssociationFilterList $filter1
```

出力:

```
AssociationId      : d8617c07-2079-4c18-9847-1655fc2698b0
DocumentVersion    :
InstanceId         : i-0000293ffd8c57862
LastExecutionDate  : 2/20/2015 8:31:11 AM
Name               : AWS-UpdateSSMAgent
Overview           : Amazon.SimpleSystemsManagement.Model.AssociationOverview
ScheduleExpression :
Targets            : {InstanceIds}
```

例 2: この例では、設定ドキュメントのすべての関連付けを一覧表示します。この例で使用される構文には、PowerShell バージョン 3 以降が必要です。

```
$filter2 = @{Key="Name";Value=@("AWS-UpdateSSMAgent")}
Get-SSMAssociationList -AssociationFilterList $filter2
```

出力:

```
AssociationId      : d8617c07-2079-4c18-9847-1655fc2698b0
DocumentVersion    :
InstanceId         : i-0000293ffd8c57862
LastExecutionDate  : 2/20/2015 8:31:11 AM
Name               : AWS-UpdateSSMAgent
Overview           : Amazon.SimpleSystemsManagement.Model.AssociationOverview
ScheduleExpression :
Targets            : {InstanceIds}
```

例 3: PowerShell バージョン 2 では、New-Object を使用して各フィルターを作成する必要があります。

```
$filter1 = New-Object Amazon.SimpleSystemsManagement.Model.AssociationFilter
$filter1.Key = "InstanceId"
$filter1.Value = "i-0000293ffd8c57862"

Get-SSMAssociationList -AssociationFilterList $filter1
```

出力:

```
AssociationId      : d8617c07-2079-4c18-9847-1655fc2698b0
DocumentVersion    :
```

```
InstanceId          : i-0000293ffd8c57862
LastExecutionDate   : 2/20/2015 8:31:11 AM
Name                : AWS-UpdateSSMAgent
Overview            : Amazon.SimpleSystemsManagement.Model.AssociationOverview
ScheduleExpression  :
Targets             : {InstanceIds}
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「ListAssociations」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI で **ListCommandInvocations** を使用する

次のサンプルコードは、ListCommandInvocations を使用する方法を説明しています。

アクション例は、より大きなプログラムからのコードの抜粋であり、コンテキスト内で実行する必要があります。次のコード例で、このアクションのコンテキストを確認できます。

- 基本を学ぶ

CLI

AWS CLI

特定のコマンドの呼び出しを一覧表示するには

次の list-command-invocations の例では、コマンドのすべての呼び出しを一覧表示します。

```
aws ssm list-command-invocations \
    --command-id "ef7fdfd8-9b57-4151-a15c-db9a12345678" \
    --details
```

出力:

```
{
    "CommandInvocations": [
        {
```

```
            "CommandId": "ef7fdfd8-9b57-4151-a15c-db9a12345678",
            "InstanceId": "i-02573cafcfEXAMPLE",
            "InstanceName": "",
            "Comment": "b48291dd-ba76-43e0-
b9df-13e11ddaac26:6960febb-2907-4b59-8e1a-d6ce8EXAMPLE",
            "DocumentName": "AWS-UpdateSSMAgent",
            "DocumentVersion": "",
            "RequestedDateTime": 1582136283.089,
            "Status": "Success",
            "StatusDetails": "Success",
            "StandardOutputUrl": "",
            "StandardErrorUrl": "",
            "CommandPlugins": [
                {
                    "Name": "aws:updateSsmAgent",
                    "Status": "Success",
                    "StatusDetails": "Success",
                    "ResponseCode": 0,
                    "ResponseStartDateTime": 1582136283.419,
                    "ResponseFinishDateTime": 1582136283.51,
                    "Output": "Updating amazon-ssm-agent from 2.3.842.0 to latest
\nSuccessfully downloaded https://s3.us-east-2.amazonaws.com/amazon-ssm-us-
east-2/ssm-agent-manifest.json\namazon-ssm-agent 2.3.842.0 has already been
 installed, update skipped\n",
                    "StandardOutputUrl": "",
                    "StandardErrorUrl": "",
                    "OutputS3Region": "us-east-2",
                    "OutputS3BucketName": "",
                    "OutputS3KeyPrefix": ""
                }
            ],
            "ServiceRole": "",
            "NotificationConfig": {
                "NotificationArn": "",
                "NotificationEvents": [],
                "NotificationType": ""
            },
            "CloudWatchOutputConfig": {
                "CloudWatchLogGroupName": "",
                "CloudWatchOutputEnabled": false
            }
        },
        {
            "CommandId": "ef7fdfd8-9b57-4151-a15c-db9a12345678",
```

```
            "InstanceId": "i-0471e04240EXAMPLE",
            "InstanceName": "",
            "Comment": "b48291dd-ba76-43e0-
b9df-13e11ddaac26:6960febb-2907-4b59-8e1a-d6ce8EXAMPLE",
            "DocumentName": "AWS-UpdateSSMAgent",
            "DocumentVersion": "",
            "RequestedDateTime": 1582136283.02,
            "Status": "Success",
            "StatusDetails": "Success",
            "StandardOutputUrl": "",
            "StandardErrorUrl": "",
            "CommandPlugins": [
                {
                    "Name": "aws:updateSsmAgent",
                    "Status": "Success",
                    "StatusDetails": "Success",
                    "ResponseCode": 0,
                    "ResponseStartDateTime": 1582136283.812,
                    "ResponseFinishDateTime": 1582136295.031,
                    "Output": "Updating amazon-ssm-agent from 2.3.672.0 to
 latest\nSuccessfully downloaded https://s3.us-east-2.amazonaws.com/amazon-
ssm-us-east-2/ssm-agent-manifest.json\nSuccessfully downloaded https://s3.us-
east-2.amazonaws.com/amazon-ssm-us-east-2/amazon-ssm-agent-updater/2.3.842.0/
amazon-ssm-agent-updater-snap-amd64.tar.gz\nSuccessfully downloaded https://
s3.us-east-2.amazonaws.com/amazon-ssm-us-east-2/amazon-ssm-agent/2.3.672.0/
amazon-ssm-agent-snap-amd64.tar.gz\nSuccessfully downloaded https://s3.us-
east-2.amazonaws.com/amazon-ssm-us-east-2/amazon-ssm-agent/2.3.842.0/amazon-ssm-
agent-snap-amd64.tar.gz\nInitiating amazon-ssm-agent update to 2.3.842.0\namazon-
ssm-agent updated successfully to 2.3.842.0",
                    "StandardOutputUrl": "",
                    "StandardErrorUrl": "",
                    "OutputS3Region": "us-east-2",
                    "OutputS3BucketName": "",
                    "OutputS3KeyPrefix": "8bee3135-398c-4d31-99b6-e42d2EXAMPLE/
i-0471e04240EXAMPLE/awsupdateSsmAgent"
                }
            ],
            "ServiceRole": "",
            "NotificationConfig": {
                "NotificationArn": "",
                "NotificationEvents": [],
                "NotificationType": ""
            },
            "CloudWatchOutputConfig": {
```

```
                "CloudWatchLogGroupName": "",
                "CloudWatchOutputEnabled": false
            }
        }
    ]
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「コマンドのステータスについて」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「ListCommandInvocations」を参照してください。

JavaScript

SDK for JavaScript (v3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
import { paginateListCommandInvocations, SSMClient } from "@aws-sdk/client-ssm";
import { parseArgs } from "node:util";

/**
 * List SSM command invocations on an instance.
 * @param {{ instanceId: string }}
 */
export const main = async ({ instanceId }) => {
  const client = new SSMClient({});
  try {
    const listCommandInvocationsPaginated = [];
    // The paginate function is a wrapper around the base command.
    const paginator = paginateListCommandInvocations(
      { client },
      {
        InstanceId: instanceId,
      },
    );
    for await (const page of paginator) {
```

```
      listCommandInvocationsPaginated.push(...page.CommandInvocations);
    }
    console.log("Here is the list of command invocations:");
    console.log(listCommandInvocationsPaginated);
    return { CommandInvocations: listCommandInvocationsPaginated };
  } catch (caught) {
    if (caught instanceof Error && caught.name === "ValidationError") {
      console.warn(`${caught.message}. Did you provide a valid instance ID?`);
    }
    throw caught;
  }
};
```

- API の詳細については、「AWS SDK for JavaScript API リファレンス」の「ListCommandInvocations」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、コマンドのすべての呼び出しを一覧表示します。

```
Get-SSMCommandInvocation -CommandId "b8eac879-0541-439d-94ec-47a80d554f44" -
Detail $true
```

出力:

```
CommandId          : b8eac879-0541-439d-94ec-47a80d554f44
CommandPlugins     : {aws:runShellScript}
Comment            : IP config
DocumentName       : AWS-RunShellScript
InstanceId         : i-0cb2b964d3e14fd9f
InstanceName       :
NotificationConfig : Amazon.SimpleSystemsManagement.Model.NotificationConfig
RequestedDateTime  : 2/22/2017 8:13:16 PM
ServiceRole        :
StandardErrorUrl   :
StandardOutputUrl  :
Status             : Success
StatusDetails      : Success
TraceOutput        :
```

例 2: この例では、コマンド ID e1eb2e3c-ed4c-5123-45c1-234f5612345f の呼び出し用の CommandPlugins を一覧表示します。

```
Get-SSMCommandInvocation -CommandId e1eb2e3c-ed4c-5123-45c1-234f5612345f -Detail:
$true | Select-Object -ExpandProperty CommandPlugins
```

出力:

```
Name                   : aws:runPowerShellScript
Output                 : Completed 17.7 KiB/17.7 KiB (40.1 KiB/s) with 1 file(s)
 remainingdownload: s3://dd-aess-r-ctmer/KUMO.png to ..\..\programdata\KUMO.png
                        kumo available

OutputS3BucketName     :
OutputS3KeyPrefix      :
OutputS3Region         : eu-west-1
ResponseCode           : 0
ResponseFinishDateTime : 4/3/2019 11:53:23 AM
ResponseStartDateTime  : 4/3/2019 11:53:21 AM
StandardErrorUrl       :
StandardOutputUrl      :
Status                 : Success
StatusDetails          : Success
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「ListCommandInvocations」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
class DocumentWrapper:
    """Encapsulates AWS Systems Manager Document actions."""
```

```
    def __init__(self, ssm_client):
        """
        :param ssm_client: A Boto3 Systems Manager client.
        """
        self.ssm_client = ssm_client
        self.name = None

    @classmethod
    def from_client(cls):
        ssm_client = boto3.client("ssm")
        return cls(ssm_client)


    def list_command_invocations(self, instance_id):
        """
        Lists the commands for an instance.

        :param instance_id: The ID of the instance.
        :return: The list of commands.
        """
        try:
            paginator = self.ssm_client.get_paginator("list_command_invocations")
            command_invocations = []
            for page in paginator.paginate(InstanceId=instance_id):
                command_invocations.extend(page["CommandInvocations"])
            num_of_commands = len(command_invocations)
            print(
                f"{num_of_commands} command invocation(s) found for instance
{instance_id}."
            )

            if num_of_commands > 10:
                print("Displaying the first 10 commands:")
                num_of_commands = 10
            date_format = "%A, %d %B %Y %I:%M%p"
            for command in command_invocations[:num_of_commands]:
                print(
                    f"   The time of command invocation is
{command['RequestedDateTime'].strftime(date_format)}"
                )
        except ClientError as err:
            logger.error(
                "Couldn't list commands for %s. Here's why: %s: %s",
                instance_id,
```

```
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
```

- API の詳細については、「AWS SDK for Python (Boto3) API リファレンス」の「ListCommandInvocations」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **ListCommands** を使用する

次のサンプルコードは、ListCommands を使用する方法を説明しています。

CLI

AWS CLI

例 1: 特定のコマンドのステータスを取得するには

次の list-commands の例では、指定されたコマンドのステータスを取得して表示します。

```
aws ssm list-commands \
    --command-id "0831e1a8-a1ac-4257-a1fd-c831bEXAMPLE"
```

例 2: 特定の日付より後にリクエストされたコマンドのステータスを取得するには

次の list-commands の例では、指定した日付より後にリクエストされたコマンドの詳細を取得します。

```
aws ssm list-commands \
    --filter "key=InvokedAfter,value=2020-02-01T00:00:00Z"
```

例 3: AWS アカウントでリクエストされたすべてのコマンドを一覧表示するには

次の list-commands の例では、現在の AWS アカウントとリージョンでユーザーがリクエストしたすべてのコマンドを一覧表示します。

```
aws ssm list-commands
```

出力:

```
{
    "Commands": [
        {
            "CommandId": "8bee3135-398c-4d31-99b6-e42d2EXAMPLE",
            "DocumentName": "AWS-UpdateSSMAgent",
            "DocumentVersion": "",
            "Comment": "b48291dd-ba76-43e0-
b9df-13e11ddaac26:6960febb-2907-4b59-8e1a-d6ce8EXAMPLE",
            "ExpiresAfter": "2020-02-19T11:28:02.500000-08:00",
            "Parameters": {},
            "InstanceIds": [
                "i-028ea792daEXAMPLE",
                "i-02feef8c46EXAMPLE",
                "i-038613f3f0EXAMPLE",
                "i-03a530a2d4EXAMPLE",
                "i-083b678d37EXAMPLE",
                "i-0dee81debaEXAMPLE"
            ],
            "Targets": [],
            "RequestedDateTime": "2020-02-19T10:18:02.500000-08:00",
            "Status": "Success",
            "StatusDetails": "Success",
            "OutputS3BucketName": "",
            "OutputS3KeyPrefix": "",
            "MaxConcurrency": "50",
            "MaxErrors": "100%",
            "TargetCount": 6,
            "CompletedCount": 6,
            "ErrorCount": 0,
            "DeliveryTimedOutCount": 0,
            "ServiceRole": "",
            "NotificationConfig": {
                "NotificationArn": "",
                "NotificationEvents": [],
                "NotificationType": ""
            },
            "CloudWatchOutputConfig": {
                "CloudWatchLogGroupName": "",
                "CloudWatchOutputEnabled": false
```

```
            }
        }
        {
            "CommandId": "e9ade581-c03d-476b-9b07-26667EXAMPLE",
            "DocumentName": "AWS-FindWindowsUpdates",
            "DocumentVersion": "1",
            "Comment": "",
            "ExpiresAfter": "2020-01-24T12:37:31.874000-08:00",
            "Parameters": {
                "KbArticleIds": [
                    ""
                ],
                "UpdateLevel": [
                    "All"
                ]
            },
            "InstanceIds": [],
            "Targets": [
                {
                    "Key": "InstanceIds",
                    "Values": [
                        "i-00ec29b21eEXAMPLE",
                        "i-09911ddd90EXAMPLE"
                    ]
                }
            ],
            "RequestedDateTime": "2020-01-24T11:27:31.874000-08:00",
            "Status": "Success",
            "StatusDetails": "Success",
            "OutputS3BucketName": "my-us-east-2-bucket",
            "OutputS3KeyPrefix": "my-rc-output",
            "MaxConcurrency": "50",
            "MaxErrors": "0",
            "TargetCount": 2,
            "CompletedCount": 2,
            "ErrorCount": 0,
            "DeliveryTimedOutCount": 0,
            "ServiceRole": "arn:aws:iam::111222333444:role/aws-service-role/
ssm.amazonaws.com/AWSServiceRoleForAmazonSSM",
            "NotificationConfig": {
                "NotificationArn": "arn:aws:sns:us-east-2:111222333444:my-us-
east-2-notification-arn",
                "NotificationEvents": [
                    "All"
```

```
                ],
                "NotificationType": "Invocation"
            },
            "CloudWatchOutputConfig": {
                "CloudWatchLogGroupName": "",
                "CloudWatchOutputEnabled": false
            }
        }
        {
            "CommandId": "d539b6c3-70e8-4853-80e5-0ce4fEXAMPLE",
            "DocumentName": "AWS-RunPatchBaseline",
            "DocumentVersion": "1",
            "Comment": "",
            "ExpiresAfter": "2020-01-24T12:21:04.350000-08:00",
            "Parameters": {
                "InstallOverrideList": [
                    ""
                ],
                "Operation": [
                    "Install"
                ],
                "RebootOption": [
                    "RebootIfNeeded"
                ],
                "SnapshotId": [
                    ""
                ]
            },
            "InstanceIds": [],
            "Targets": [
                {
                    "Key": "InstanceIds",
                    "Values": [
                        "i-00ec29b21eEXAMPLE",
                        "i-09911ddd90EXAMPLE"
                    ]
                }
            ],
            "RequestedDateTime": "2020-01-24T11:11:04.350000-08:00",
            "Status": "Success",
            "StatusDetails": "Success",
            "OutputS3BucketName": "my-us-east-2-bucket",
            "OutputS3KeyPrefix": "my-rc-output",
            "MaxConcurrency": "50",
```

```
            "MaxErrors": "0",
            "TargetCount": 2,
            "CompletedCount": 2,
            "ErrorCount": 0,
            "DeliveryTimedOutCount": 0,
            "ServiceRole": "arn:aws:iam::111222333444:role/aws-service-role/
ssm.amazonaws.com/AWSServiceRoleForAmazonSSM",
            "NotificationConfig": {
                "NotificationArn": "arn:aws:sns:us-east-2:111222333444:my-us-
east-2-notification-arn",
                "NotificationEvents": [
                    "All"
                ],
                "NotificationType": "Invocation"
            },
            "CloudWatchOutputConfig": {
                "CloudWatchLogGroupName": "",
                "CloudWatchOutputEnabled": false
            }
        }
    ]
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「Running Commands Using Systems Manager Run Command」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「ListCommands」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、リクエストされたすべてのコマンドを一覧表示します。

```
Get-SSMCommand
```

出力:

```
CommandId          : 4b75a163-d39a-4d97-87c9-98ae52c6be35
Comment            : Apply association with id at update time: 4cc73e42-
d5ae-4879-84f8-57e09c0efcd0
```

```
CompletedCount     : 1
DocumentName       : AWS-RefreshAssociation
ErrorCount         : 0
ExpiresAfter       : 2/24/2017 3:19:08 AM
InstanceIds        : {i-0cb2b964d3e14fd9f}
MaxConcurrency     : 50
MaxErrors          : 0
NotificationConfig : Amazon.SimpleSystemsManagement.Model.NotificationConfig
OutputS3BucketName :
OutputS3KeyPrefix  :
OutputS3Region     :
Parameters         : {[associationIds,
 Amazon.Runtime.Internal.Util.AlwaysSendList`1[System.String]]}
RequestedDateTime  : 2/24/2017 3:18:08 AM
ServiceRole        :
Status             : Success
StatusDetails      : Success
TargetCount        : 1
Targets            : {}
```

例 2: この例では、特定のコマンドのステータスを取得します。

```
Get-SSMCommand -CommandId "4b75a163-d39a-4d97-87c9-98ae52c6be35"
```

例 3: この例では、2019-04-01T00:00:00Z より後に呼び出されたすべての SSM コマンドを取得します。

```
Get-SSMCommand -Filter @{Key="InvokedAfter";Value="2019-04-01T00:00:00Z"} |
 Select-Object CommandId, DocumentName, Status, RequestedDateTime | Sort-Object -
Property RequestedDateTime -Descending
```

出力:

```
CommandId                            DocumentName               Status
 RequestedDateTime
---------                            ------------               ------
 -----------------
edb1b23e-456a-7adb-aef8-90e-012ac34f AWS-RunPowerShellScript    Cancelled
 4/16/2019 5:45:23 AM
1a2dc3fb-4567-890d-a1ad-234b5d6bc7d9 AWS-ConfigureAWSPackage    Success
 4/6/2019 9:19:42 AM
```

```
12c3456c-7e90-4f12-1232-1234f5b67893 KT-Retrieve-Cloud-Type-Win Failed
 4/2/2019 4:13:07 AM
fe123b45-240c-4123-a2b3-234bdd567ecf AWS-RunInspecChecks        Failed
 4/1/2019 2:27:31 PM
1eb23aa4-567d-4123-12a3-4c1c2ab34561 AWS-RunPowerShellScript    Success
 4/1/2019 1:05:55 PM
1c2f3bb4-ee12-4bc1-1a23-12345eea123e AWS-RunInspecChecks        Failed
 4/1/2019 11:13:09 AM
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「ListCommands」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **ListComplianceItems** を使用する

次のサンプルコードは、ListComplianceItems を使用する方法を説明しています。

CLI

AWS CLI

特定のインスタンスのコンプライアンス項目を一覧表示するには

この例では、指定したインスタンスのすべてのコンプライアンス項目を一覧表示します。

コマンド:

```
aws ssm list-compliance-items --resource-ids "i-1234567890abcdef0" --resource-
types "ManagedInstance"
```

出力:

```
{
  "ComplianceItems": [
      {
          "ComplianceType": "Association",
          "ResourceType": "ManagedInstance",
```

```
            "ResourceId": "i-1234567890abcdef0",
            "Id": "8dfe3659-4309-493a-8755-0123456789ab",
            "Title": "",
            "Status": "COMPLIANT",
            "Severity": "UNSPECIFIED",
            "ExecutionSummary": {
                "ExecutionTime": 1550408470.0
            },
            "Details": {
                "DocumentName": "AWS-GatherSoftwareInventory",
                "DocumentVersion": "1"
            }
        },
        {
            "ComplianceType": "Association",
            "ResourceType": "ManagedInstance",
            "ResourceId": "i-1234567890abcdef0",
            "Id": "e4c2ed6d-516f-41aa-aa2a-0123456789ab",
            "Title": "",
            "Status": "COMPLIANT",
            "Severity": "UNSPECIFIED",
            "ExecutionSummary": {
                "ExecutionTime": 1550508475.0
            },
            "Details": {
                "DocumentName": "AWS-UpdateSSMAgent",
                "DocumentVersion": "1"
            }
        },
                ...
    ],
    "NextToken": "--token string truncated--"
}
```

特定のインスタンスと関連付け ID のコンプライアンス項目を一覧表示するには

この例では、指定したインスタンスと関連付け ID のすべてのコンプライアンス項目を一覧表示します。

コマンド:

```
aws ssm list-compliance-items --resource-ids "i-1234567890abcdef0" --resource-
types "ManagedInstance" --
```

```
filters "Key=ComplianceType,Values=Association,Type=EQUAL" "Key=Id,Values=e4c2ed6d-516f-4
aa2a-0123456789ab,Type=EQUAL"
```

特定の日時より後のインスタンスのコンプライアンス項目を一覧表示するには

この例では、指定した日時より後のインスタンスのすべてのコンプライアンス項目を一覧表示します。

コマンド:

```
aws ssm list-compliance-items --resource-ids "i-1234567890abcdef0" --resource-
types "ManagedInstance" --
filters "Key=ExecutionTime,Values=2019-02-18T16:00:00Z,Type=GREATER_THAN"
```

- API の詳細については、AWS CLI コマンドリファレンスの「ListComplianceItems」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、任意のリソース ID とタイプのコンプライアンス項目リストを一覧表示し、コンプライアンスタイプを「関連付け」でフィルタリングします。

```
Get-SSMComplianceItemList -ResourceId i-1a2caf345f67d0dc2 -ResourceType
 ManagedInstance -Filter @{Key="ComplianceType";Values="Association"}
```

出力:

```
ComplianceType   : Association
Details          : {[DocumentName, AWS-GatherSoftwareInventory],
 [DocumentVersion, 1]}
ExecutionSummary :
 Amazon.SimpleSystemsManagement.Model.ComplianceExecutionSummary
Id               : 123a45a1-c234-1234-1245-67891236db4e
ResourceId       : i-1a2caf345f67d0dc2
ResourceType     : ManagedInstance
Severity         : UNSPECIFIED
Status           : COMPLIANT
Title            :
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「ListComplianceItems」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **ListComplianceSummaries** を使用する

次のサンプルコードは、ListComplianceSummaries を使用する方法を説明しています。

CLI

AWS CLI

すべてのコンプライアンスタイプのコンプライアンス概要を一覧表示するには

この例では、アカウント内のすべてのコンプライアンスタイプのコンプライアンス概要を一覧表示します。

コマンド:

```
aws ssm list-compliance-summaries
```

出力:

```
{
  "ComplianceSummaryItems": [
      {
          "ComplianceType": "Association",
          "CompliantSummary": {
              "CompliantCount": 2,
              "SeveritySummary": {
                  "CriticalCount": 0,
                  "HighCount": 0,
                  "MediumCount": 0,
                  "LowCount": 0,
                  "InformationalCount": 0,
                  "UnspecifiedCount": 2
              }
          },
          "NonCompliantSummary": {
```

```
                "NonCompliantCount": 0,
                "SeveritySummary": {
                    "CriticalCount": 0,
                    "HighCount": 0,
                    "MediumCount": 0,
                    "LowCount": 0,
                    "InformationalCount": 0,
                    "UnspecifiedCount": 0
                }
            }
        },
        {
            "ComplianceType": "Patch",
            "CompliantSummary": {
                "CompliantCount": 1,
                "SeveritySummary": {
                    "CriticalCount": 0,
                    "HighCount": 0,
                    "MediumCount": 0,
                    "LowCount": 0,
                    "InformationalCount": 0,
                    "UnspecifiedCount": 1
                }
            },
            "NonCompliantSummary": {
                "NonCompliantCount": 1,
                "SeveritySummary": {
                    "CriticalCount": 1,
                    "HighCount": 0,
                    "MediumCount": 0,
                    "LowCount": 0,
                    "InformationalCount": 0,
                    "UnspecifiedCount": 0
                }
            }
        },
                ...
    ],
    "NextToken": "eyJOZXh0VG9rZW4iOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAyfQ=="
}
```

特定のコンプライアンスタイプのコンプライアンス概要を一覧表示するには

この例では、パッチコンプライアンスタイプのコンプライアンス概要を一覧表示します。

コマンド:

```
aws ssm list-compliance-summaries --
filters "Key=ComplianceType,Values=Patch,Type=EQUAL"
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「ListComplianceSummaries」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、すべてのコンプライアンスタイプの準拠リソースと非準拠リソースの集計カウントを返します。

```
Get-SSMComplianceSummaryList
```

出力:

```
ComplianceType CompliantSummary
 NonCompliantSummary
-------------- ---------------
 -------------------
FleetTotal     Amazon.SimpleSystemsManagement.Model.CompliantSummary
 Amazon.SimpleSystemsManagement.Model.NonCompliantSummary
Association    Amazon.SimpleSystemsManagement.Model.CompliantSummary
 Amazon.SimpleSystemsManagement.Model.NonCompliantSummary
Custom:InSpec  Amazon.SimpleSystemsManagement.Model.CompliantSummary
 Amazon.SimpleSystemsManagement.Model.NonCompliantSummary
Patch          Amazon.SimpleSystemsManagement.Model.CompliantSummary
 Amazon.SimpleSystemsManagement.Model.NonCompliantSummary
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「ListComplianceSummaries」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **ListDocumentVersions** を使用する

次のサンプルコードは、ListDocumentVersions を使用する方法を説明しています。

CLI

AWS CLI

ドキュメントバージョンを一覧表示するには

次の list-document-versions の例では、Systems Manager ドキュメントのすべてのバージョンを一覧表示します。

```
aws ssm list-document-versions \
    --name "Example"
```

出力:

```
{
    "DocumentVersions": [
        {
            "Name": "Example",
            "DocumentVersion": "1",
            "CreatedDate": 1583257938.266,
            "IsDefaultVersion": true,
            "DocumentFormat": "YAML",
            "Status": "Active"
        }
    ]
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「Sending Commands that Use the Document Version Parameter」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス.」の「ListDocumentVersions」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、ドキュメントのすべてのバージョンを一覧表示します。

```
Get-SSMDocumentVersionList -Name "AWS-UpdateSSMAgent"
```

出力:

```
CreatedDate       : 6/1/2021 5:19:10 PM
DocumentFormat    : JSON
DocumentVersion   : 1
IsDefaultVersion  : True
Name              : AWS-UpdateSSMAgent
Status            : Active
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「ListDocumentVersions」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **ListDocuments** を使用する

次のサンプルコードは、ListDocuments を使用する方法を説明しています。

CLI

AWS CLI

例 1: ドキュメントを一覧表示するには

次の list-documents の例では、カスタムタグでタグ付けされたリクエスト元のアカウントが所有するドキュメントを一覧表示します。

```
aws ssm list-documents \
    --filters Key=Owner,Values=Self Key=tag:DocUse,Values=Testing
```

出力:

```
{
    "DocumentIdentifiers": [
        {
            "Name": "Example",
```

```
            "Owner": "29884EXAMPLE",
            "PlatformTypes": [
                "Windows",
                "Linux"
            ],
            "DocumentVersion": "1",
            "DocumentType": "Automation",
            "SchemaVersion": "0.3",
            "DocumentFormat": "YAML",
            "Tags": [
                {
                    "Key": "DocUse",
                    "Value": "Testing"
                }
            ]
        }
    ]
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「AWS Systems Manager ドキュメント」を参照してください。

例 2: 共有ドキュメントを一覧表示するには

次の `list-documents` の例では、AWS が所有していないプライベート共有ドキュメントを含む共有ドキュメントを一覧表示します。

```
aws ssm list-documents \
    --filters Key=Name,Values=sharedDocNamePrefix  Key=Owner,Values=Private
```

出力:

```
{
    "DocumentIdentifiers": [
        {
            "Name": "Example",
            "Owner": "12345EXAMPLE",
            "PlatformTypes": [
                "Windows",
                "Linux"
            ],
            "DocumentVersion": "1",
            "DocumentType": "Command",
```

```
            "SchemaVersion": "0.3",
            "DocumentFormat": "YAML",
            "Tags": []
        }
    ]
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「AWS Systems Manager ドキュメント」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「ListDocuments」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: アカウント内のすべての設定ドキュメントを一覧表示します。

```
Get-SSMDocumentList
```

出力:

```
DocumentType    : Command
DocumentVersion : 1
Name            : AWS-ApplyPatchBaseline
Owner           : Amazon
PlatformTypes   : {Windows}
SchemaVersion   : 1.2

DocumentType    : Command
DocumentVersion : 1
Name            : AWS-ConfigureAWSPackage
Owner           : Amazon
PlatformTypes   : {Windows, Linux}
SchemaVersion   : 2.0

DocumentType    : Command
DocumentVersion : 1
Name            : AWS-ConfigureCloudWatch
Owner           : Amazon
PlatformTypes   : {Windows}
```

```
SchemaVersion   : 1.2
...
```

例 2: この例では、名前が「プラットフォーム」と一致するすべてのオートメーションドキュメントを取得します。

```
Get-SSMDocumentList -DocumentFilterList @{Key="DocumentType";Value="Automation"}
 | Where-Object Name -Match "Platform"
```

出力:

```
DocumentFormat  : JSON
DocumentType    : Automation
DocumentVersion : 7
Name            : KT-Get-Platform
Owner           : 987654123456
PlatformTypes   : {Windows, Linux}
SchemaVersion   : 0.3
Tags            : {}
TargetType      :
VersionName     :
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「ListDocuments」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **ListInventoryEntries** を使用する

次のサンプルコードは、ListInventoryEntries を使用する方法を説明しています。

CLI

AWS CLI

例 1: インスタンスの特定のインベントリタイプのエントリを表示するには

次の list-inventory-entries の例では、特定のインスタンスの AWS:Application インベントリタイプのインベントリエントリを一覧表示します。

```
aws ssm list-inventory-entries \
    --instance-id "i-1234567890abcdef0" \
    --type-name "AWS:Application"
```

出力:

```
{
  "TypeName": "AWS:Application",
  "InstanceId": "i-1234567890abcdef0",
  "SchemaVersion": "1.1",
  "CaptureTime": "2019-02-15T12:17:55Z",
  "Entries": [
    {
      "Architecture": "i386",
      "Name": "Amazon SSM Agent",
      "PackageId": "{88a60be2-89a1-4df8-812a-80863c2a2b68}",
      "Publisher": "Amazon Web Services",
      "Version": "2.3.274.0"
    },
    {
      "Architecture": "x86_64",
      "InstalledTime": "2018-05-03T13:42:34Z",
      "Name": "AmazonCloudWatchAgent",
      "Publisher": "",
      "Version": "1.200442.0"
    }
  ]
}
```

例 2: インスタンスに割り当てられたカスタムインベントリエントリを表示するには

次の `list-inventory-entries` の例では、インスタンスに割り当てられたカスタムインベントリエントリを一覧表示します。

```
aws ssm list-inventory-entries \
    --instance-id "i-1234567890abcdef0" \
    --type-name "Custom:RackInfo"
```

出力:

```
{
  "TypeName": "Custom:RackInfo",
```

```
  "InstanceId": "i-1234567890abcdef0",
  "SchemaVersion": "1.0",
  "CaptureTime": "2021-05-22T10:01:01Z",
  "Entries": [
    {
      "RackLocation": "Bay B/Row C/Rack D/Shelf E"
    }
  ]
}
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「ListInventoryEntries」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、インスタンスのすべてのカスタムインベントリエントリを一覧表示します。

```
Get-SSMInventoryEntriesList -InstanceId "i-0cb2b964d3e14fd9f" -TypeName
 "Custom:RackInfo"
```

出力:

```
CaptureTime   : 2016-08-22T10:01:01Z
Entries       :
 {Amazon.Runtime.Internal.Util.AlwaysSendDictionary`2[System.String,System.String]}
InstanceId    : i-0cb2b964d3e14fd9f
NextToken     :
SchemaVersion : 1.0
TypeName      : Custom:RackInfo
```

例 2: この例では詳細を一覧表示します。

```
(Get-SSMInventoryEntriesList -InstanceId "i-0cb2b964d3e14fd9f" -TypeName
 "Custom:RackInfo").Entries
```

出力:

```
Key          Value
```

```
---          -----
RackLocation Bay B/Row C/Rack D/Shelf E
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「ListInventoryEntries」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **ListResourceComplianceSummaries** を使用する

次のサンプルコードは、ListResourceComplianceSummaries を使用する方法を説明しています。

CLI

AWS CLI

リソースレベルのコンプライアンス概要数を一覧表示するには

この例では、リソースレベルのコンプライアンス概要数を一覧表示します。

コマンド:

```
aws ssm list-resource-compliance-summaries
```

出力:

```
{
  "ResourceComplianceSummaryItems": [
      {
          "ComplianceType": "Association",
          "ResourceType": "ManagedInstance",
          "ResourceId": "i-1234567890abcdef0",
          "Status": "COMPLIANT",
          "OverallSeverity": "UNSPECIFIED",
          "ExecutionSummary": {
              "ExecutionTime": 1550509273.0
          },
          "CompliantSummary": {
              "CompliantCount": 2,
```

```
            "SeveritySummary": {
                "CriticalCount": 0,
                "HighCount": 0,
                "MediumCount": 0,
                "LowCount": 0,
                "InformationalCount": 0,
                "UnspecifiedCount": 2
            }
        },
        "NonCompliantSummary": {
            "NonCompliantCount": 0,
            "SeveritySummary": {
                "CriticalCount": 0,
                "HighCount": 0,
                "MediumCount": 0,
                "LowCount": 0,
                "InformationalCount": 0,
                "UnspecifiedCount": 0
            }
        }
    },
    {
        "ComplianceType": "Patch",
        "ResourceType": "ManagedInstance",
        "ResourceId": "i-9876543210abcdef0",
        "Status": "COMPLIANT",
        "OverallSeverity": "UNSPECIFIED",
        "ExecutionSummary": {
            "ExecutionTime": 1550248550.0,
            "ExecutionId": "7abb6378-a4a5-4f10-8312-0123456789ab",
            "ExecutionType": "Command"
        },
        "CompliantSummary": {
            "CompliantCount": 397,
            "SeveritySummary": {
                "CriticalCount": 0,
                "HighCount": 0,
                "MediumCount": 0,
                "LowCount": 0,
                "InformationalCount": 0,
                "UnspecifiedCount": 397
            }
        },
        "NonCompliantSummary": {
```

```
                "NonCompliantCount": 0,
                "SeveritySummary": {
                    "CriticalCount": 0,
                    "HighCount": 0,
                    "MediumCount": 0,
                    "LowCount": 0,
                    "InformationalCount": 0,
                    "UnspecifiedCount": 0
                }
            }
        }
    ],
    "NextToken": "--token string truncated--"
}
```

特定のコンプライアンスタイプのリソースレベルのコンプライアンス概要を一覧表示するには

この例では、パッチコンプライアンスタイプのリソースレベルのコンプライアンス概要を一覧表示します。

コマンド:

```
aws ssm list-resource-compliance-summaries --
filters "Key=ComplianceType,Values=Patch,Type=EQUAL"
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「ListResourceComplianceSummaries」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、リソースレベルの概要数を取得します。概要には、「Windows10」に一致する製品の準拠ステータスと非準拠ステータス、および詳細なコンプライアンス項目の重要度数に関する情報が含まれます。MaxResult のデフォルトは、パラメータが指定されていない場合は 100 であり、この値は有効ではないため、MaxResult パラメータが追加され、値は 50 に設定されます。

```
$FilterValues = @{
  "Key"="Product"
        "Type"="EQUAL"
```

```
        "Values"="Windows10"
}
        Get-SSMResourceComplianceSummaryList -Filter $FilterValues -MaxResult 50
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「ListResourceComplianceSummaries」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **ListTagsForResource** を使用する

次のサンプルコードは、ListTagsForResource を使用する方法を説明しています。

CLI

AWS CLI

パッチベースラインに適用されたタグを一覧表示するには

次の list-tags-for-resource の例では、パッチベースラインのタグを一覧表示します。

```
aws ssm list-tags-for-resource \
    --resource-type "PatchBaseline" \
    --resource-id "pb-0123456789abcdef0"
```

出力:

```
{
    "TagList": [
        {
            "Key": "Environment",
            "Value": "Production"
        },
        {
            "Key": "Region",
            "Value": "EMEA"
        }
    ]
}
```

詳細については、「AWS 全般リファレンス」の「AWS リソースのタグ付け」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「ListTagsForResource」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、メンテナンスウィンドウのタグを一覧表示します。

```
Get-SSMResourceTag -ResourceId "mw-03eb9db42890fb82d" -ResourceType
 "MaintenanceWindow"
```

出力:

```
Key   Value
---   -----
Stack Production
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「ListTagsForResource」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **ModifyDocumentPermission** を使用する

次のサンプルコードは、ModifyDocumentPermission を使用する方法を説明しています。

CLI

AWS CLI

ドキュメントのアクセス許可を変更するには

次の modify-document-permission の例では、Systems Manager ドキュメントをパブリックで共有します。

```
aws ssm modify-document-permission \
    --name "Example" \
    --permission-type "Share" \
    --account-ids-to-add "All"
```

このコマンドでは何も出力されません。

詳細については、「AWS Systems Manager ユーザーガイド」の「Share a Systems Manager Document」を参照してください。

- API の詳細については、AWS CLI コマンドリファレンスの「ModifyDocumentPermission」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、ドキュメントのすべてのアカウントに「共有」アクセス許可を追加します。コマンドが成功した場合、出力はありません。

```
Edit-SSMDocumentPermission -Name "RunShellScript" -PermissionType "Share" -
AccountIdsToAdd all
```

例 2: この例では、ドキュメントの特定のアカウントに「共有」アクセス許可を追加します。コマンドが成功した場合、出力はありません。

```
Edit-SSMDocumentPermission -Name "RunShellScriptNew" -PermissionType "Share" -
AccountIdsToAdd "123456789012"
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「ModifyDocumentPermission」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **PutComplianceItems** を使用する

次のサンプルコードは、PutComplianceItems を使用する方法を説明しています。

CLI

AWS CLI

コンプライアンスタイプおよびコンプライアンスの詳細を指定されたインスタンスに登録するには

この例では、指定されたマネージドインスタンスにコンプライアンスタイプ Custom:AVCheck を登録します。コマンドが成功した場合、出力はありません。

コマンド:

```
aws ssm put-compliance-items --resource-id "i-1234567890abcdef0" --
resource-type "ManagedInstance" --compliance-type "Custom:AVCheck"
 --execution-summary "ExecutionTime=2019-02-18T16:00:00Z" --
items "Id=Version2.0,Title=ScanHost,Severity=CRITICAL,Status=COMPLIANT"
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「PutComplianceItems」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、任意のマネージドインスタンスのカスタムコンプライアンス項目を書き込みます。

```
$item = [Amazon.SimpleSystemsManagement.Model.ComplianceItemEntry]::new()
$item.Id = "07Jun2019-3"
$item.Severity="LOW"
$item.Status="COMPLIANT"
$item.Title="Fin-test-1 - custom"
Write-SSMComplianceItem -ResourceId mi-012dcb3ecea45b678 -ComplianceType
 Custom:VSSCompliant2 -ResourceType ManagedInstance -Item $item -
ExecutionSummary_ExecutionTime "07-Jun-2019"
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「PutComplianceItems」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **PutInventory** を使用する

次のサンプルコードは、PutInventory を使用する方法を説明しています。

CLI

AWS CLI

顧客のメタデータをインスタンスに割り当てるには

この例では、ラックの場所情報をインスタンスに割り当てます。コマンドが成功した場合、出力はありません。

コマンド (Linux):

```
aws ssm put-inventory --instance-id "i-016648b75dd622dab" --items
 '[{"TypeName": "Custom:RackInfo","SchemaVersion": "1.0","CaptureTime":
 "2019-01-22T10:01:01Z","Content":[{"RackLocation": "Bay B/Row C/Rack D/Shelf
 E"}]}]'
```

コマンド (Windows):

```
aws ssm put-inventory --instance-id "i-016648b75dd622dab" --
items "TypeName=Custom:RackInfo,SchemaVersion=1.0,CaptureTime=2019-01-22T10:01:01Z,Conten
 B/Row C/Rack D/Shelf F'}]"
```

- API の詳細については、AWS CLI コマンドリファレンスの「PutInventory」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、ラックの場所情報をインスタンスに割り当てます。コマンドが成功した場合、出力はありません。

```
$data = New-Object
 "System.Collections.Generic.Dictionary[System.String,System.String]"
```

```
$data.Add("RackLocation", "Bay B/Row C/Rack D/Shelf F")

$items = New-Object
 "System.Collections.Generic.List[System.Collections.Generic.Dictionary[System.String,
 System.String]]"
$items.Add($data)

$customInventoryItem = New-Object
 Amazon.SimpleSystemsManagement.Model.InventoryItem
$customInventoryItem.CaptureTime = "2016-08-22T10:01:01Z"
$customInventoryItem.Content = $items
$customInventoryItem.TypeName = "Custom:TestRackInfo2"
$customInventoryItem.SchemaVersion = "1.0"

$inventoryItems = @($customInventoryItem)

Write-SSMInventory -InstanceId "i-0cb2b964d3e14fd9f" -Item $inventoryItems
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「PutInventory」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI で **PutParameter** を使用する

次のサンプルコードは、PutParameter を使用する方法を説明しています。

CLI

AWS CLI

例 1: パラメータ値を変更するには

次の put-parameter の例は、指定されたパラメータの値を変更します。

```
aws ssm put-parameter \
    --name "MyStringParameter" \
    --type "String" \
    --value "Vici" \
    --overwrite
```

出力:

```
{
    "Version": 2,
    "Tier": "Standard"
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「Create a Systems Manager parameter (AWS CLI)」、「パラメータ層の管理」、「Working with parameter policies」を参照してください。

例 2: アドバンストパラメータを作成するには

次の put-parameter の例は、アドバンストパラメータを作成します。

```
aws ssm put-parameter \
    --name "MyAdvancedParameter" \
    --description "This is an advanced parameter" \
    --value "Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do
 eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim
 veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo
 consequat [truncated]" \
    --type "String" \
    --tier Advanced
```

出力:

```
{
    "Version": 1,
    "Tier": "Advanced"
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「Create a Systems Manager parameter (AWS CLI)」、「パラメータ層の管理」、「Working with parameter policies」を参照してください。

例 3: スタンダードパラメータをアドバンストパラメータに変換するには

次の put-parameter の例は、既存のスタンダードパラメータをアドバンストパラメータに変換します。

```
aws ssm put-parameter \
    --name "MyConvertedParameter" \
    --value "abc123" \
    --type "String" \
    --tier Advanced \
    --overwrite
```

出力:

```
{
    "Version": 2,
    "Tier": "Advanced"
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「Create a Systems Manager parameter (AWS CLI)」、「パラメータ層の管理」、「Working with parameter policies」を参照してください。

例 4: ポリシーがアタッチされたパラメータを作成するには

次の put-parameter の例は、パラメータポリシーがアタッチされたアドバンストパラメータを作成します。

```
aws ssm put-parameter \
    --name "/Finance/Payroll/q2accesskey" \
    --value "P@sSwW)rd" \
    --type "SecureString" \
    --tier Advanced \
    --policies "[{\"Type\":\"Expiration\",\"Version\":\"1.0\",\"Attributes\":
{\"Timestamp\":\"2020-06-30T00:00:00.000Z\"}},{\"Type\":\"ExpirationNotification
\",\"Version\":\"1.0\",\"Attributes\":{\"Before\":\"5\",\"Unit\":\"Days\"}},
{\"Type\":\"NoChangeNotification\",\"Version\":\"1.0\",\"Attributes\":{\"After\":
\"60\",\"Unit\":\"Days\"}}]"
```

出力:

```
{
    "Version": 1,
    "Tier": "Advanced"
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「Create a Systems Manager parameter (AWS CLI)」、「パラメータ層の管理」、「Working with parameter policies」を参照してください。

例 5: 既存のパラメータにポリシーを追加するには

次の put-parameter の例は、ポリシーを既存のアドバンストパラメータにアタッチします。

```
aws ssm put-parameter \
    --name "/Finance/Payroll/q2accesskey" \
    --value "N3wP@sSwW)rd" \
    --type "SecureString" \
    --tier Advanced \
    --policies "[{\"Type\":\"Expiration\",\"Version\":\"1.0\",\"Attributes\":
{\"Timestamp\":\"2020-06-30T00:00:00.000Z\"}},{\"Type\":\"ExpirationNotification
\",\"Version\":\"1.0\",\"Attributes\":{\"Before\":\"5\",\"Unit\":\"Days\"}},
{\"Type\":\"NoChangeNotification\",\"Version\":\"1.0\",\"Attributes\":{\"After\":
\"60\",\"Unit\":\"Days\"}}]"
    --overwrite
```

出力:

```
{
    "Version": 2,
    "Tier": "Advanced"
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「Create a Systems Manager parameter (AWS CLI)」、「パラメータ層の管理」、「Working with parameter policies」を参照してください。

- API の詳細については、AWS CLI コマンドリファレンスの「PutParameter」を参照してください。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.ssm.SsmClient;
import software.amazon.awssdk.services.ssm.model.ParameterType;
import software.amazon.awssdk.services.ssm.model.PutParameterRequest;
import software.amazon.awssdk.services.ssm.model.SsmException;

public class PutParameter {

    public static void main(String[] args) {
        final String usage = """

                Usage:
                    <paraName>

                Where:
                    paraName - The name of the parameter.
                    paraValue - The value of the parameter.
                """;

        if (args.length != 2) {
            System.out.println(usage);
            System.exit(1);
        }

        String paraName = args[0];
        String paraValue = args[1];
        Region region = Region.US_EAST_1;
        SsmClient ssmClient = SsmClient.builder()
                .region(region)
                .build();

        putParaValue(ssmClient, paraName, paraValue);
```

```
        ssmClient.close();
    }

    public static void putParaValue(SsmClient ssmClient, String paraName, String
 value) {
        try {
            PutParameterRequest parameterRequest = PutParameterRequest.builder()
                    .name(paraName)
                    .type(ParameterType.STRING)
                    .value(value)
                    .build();

            ssmClient.putParameter(parameterRequest);
            System.out.println("The parameter was successfully added.");

        } catch (SsmException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
}
```

- API の詳細については、「AWS SDK for Java 2.x API リファレンス」の「PutParameter」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例ではパラメータを作成します。コマンドが成功した場合、出力はありません。

```
Write-SSMParameter -Name "Welcome" -Type "String" -Value "helloWorld"
```

例 2: この例ではパラメータを変更します。コマンドが成功した場合、出力はありません。

```
Write-SSMParameter -Name "Welcome" -Type "String" -Value "Good day, Sunshine!" -
Overwrite $true
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「PutParameter」を参照してください。

Rust

SDK for Rust

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
async fn make_parameter(
    client: &Client,
    name: &str,
    value: &str,
    description: &str,
) -> Result<(), Error> {
    let resp = client
        .put_parameter()
        .overwrite(true)
        .r#type(ParameterType::String)
        .name(name)
        .value(value)
        .description(description)
        .send()
        .await?;

    println!("Success! Parameter now has version: {}", resp.version());

    Ok(())
}
```

- API の詳細については、AWS SDK for Rust API リファレンスの「PutParameter」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **RegisterDefaultPatchBaseline** を使用する

次のサンプルコードは、RegisterDefaultPatchBaseline を使用する方法を説明しています。

CLI

AWS CLI

デフォルトパッチベースラインを設定するには

次の register-default-patch-baseline の例では、指定したカスタムパッチベースラインを、サポートするオペレーティングシステムタイプのデフォルトのパッチベースラインとして登録します。

```
aws ssm register-default-patch-baseline \
    --baseline-id "pb-abc123cf9bEXAMPLE"
```

出力:

```
{
    "BaselineId":"pb-abc123cf9bEXAMPLE"
}
```

次の register-default-patch-baseline の例では、AWS for CentOS が提供するデフォルトのパッチベースラインをデフォルトのパッチベースラインとして登録します。

```
aws ssm register-default-patch-baseline \
    --baseline-id "arn:aws:ssm:us-east-2:733109147000:patchbaseline/
pb-0574b43a65ea646ed"
```

出力:

```
{
    "BaselineId":"pb-abc123cf9bEXAMPLE"
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「事前定義されたパッチベースラインについて」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」のRegisterDefaultPatchBaseline」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、パッチベースラインをデフォルトのパッチベースラインとして登録します。

```
Register-SSMDefaultPatchBaseline -BaselineId "pb-03da896ca3b68b639"
```

出力:

```
pb-03da896ca3b68b639
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「RegisterDefaultPatchBaseline」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **RegisterPatchBaselineForPatchGroup** を使用する

次のサンプルコードは、RegisterPatchBaselineForPatchGroup を使用する方法を説明しています。

CLI

AWS CLI

パッチグループのパッチベースラインを登録するには

次の register-patch-baseline-for-patch-group の例では、パッチグループのパッチベースラインを登録します。

```
aws ssm register-patch-baseline-for-patch-group \
    --baseline-id "pb-045f10b4f382baeda" \
    --patch-group "Production"
```

出力:

```
{
    "BaselineId": "pb-045f10b4f382baeda",
    "PatchGroup": "Production"
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「パッチグループの使用 <https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-patch-group-tagging.html>__」および「パッチベースラインにパッチグループを追加します」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」のRegisterPatchBaselineForPatchGroup」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、パッチグループのパッチベースラインを登録します。

```
Register-SSMPatchBaselineForPatchGroup -BaselineId "pb-03da896ca3b68b639" -
PatchGroup "Production"
```

出力:

```
BaselineId           PatchGroup
----------           ----------
pb-03da896ca3b68b639 Production
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「RegisterPatchBaselineForPatchGroup」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **RegisterTargetWithMaintenanceWindow** を使用する

次のサンプルコードは、RegisterTargetWithMaintenanceWindow を使用する方法を説明しています。

CLI

AWS CLI

例 1: メンテナンスウィンドウに単一のターゲットを登録するには

次の register-target-with-maintenance-window の例では、インスタンスをメンテナンスウィンドウに登録します。

```
aws ssm register-target-with-maintenance-window \
    --window-id "mw-ab12cd34ef56gh78" \
    --target "Key=InstanceIds,Values=i-0000293ffd8c57862" \
    --owner-information "Single instance" \
    --resource-type "INSTANCE"
```

出力:

```
{
    "WindowTargetId":"1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4d-1a2"
}
```

例 2: インスタンス ID を使用して、メンテナンスウィンドウに複数のターゲットを登録するには

次の register-target-with-maintenance-window の例では、インスタンス ID を指定して、2 つのインスタンスをメンテナンスウィンドウに登録します。

```
aws ssm register-target-with-maintenance-window \
    --window-id "mw-ab12cd34ef56gh78" \
    --target "Key=InstanceIds,Values=i-0000293ffd8c57862,i-0cb2b964d3e14fd9f" \
    --owner-information "Two instances in a list" \
    --resource-type "INSTANCE"
```

出力:

```
{
    "WindowTargetId":"1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4d-1a2"
}
```

例 3: リソースタグを使用してメンテナンスウィンドウにターゲットを登録するには

次の register-target-with-maintenance-window の例では、インスタンスに適用されたリソースタグを指定して、インスタンスをメンテナンスウィンドウに登録します。

```
aws ssm register-target-with-maintenance-window \
    --window-id "mw-06cf17cbefcb4bf4f" \
    --targets "Key=tag:Environment,Values=Prod" "Key=Role,Values=Web" \
    --owner-information "Production Web Servers" \
    --resource-type "INSTANCE"
```

出力:

```
{
    "WindowTargetId":"1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4d-1a2"
}
```

例 4: タグキーのグループを使用してターゲットを登録するには

次の register-target-with-maintenance-window の例では、キー値に関係なく、1 つまたは複数のタグキーが割り当てられているインスタンスをすべて登録します。

```
aws ssm register-target-with-maintenance-window \
    --window-id "mw-0c50858d01EXAMPLE" \
    --resource-type "INSTANCE" \
    --target "Key=tag-key,Values=Name,Instance-Type,CostCenter"
```

出力:

```
{
    "WindowTargetId":"1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4d-1a2"
}
```

例 5: リソースグループ名を使用してターゲットを登録するには

次の register-target-with-maintenance-window の例では、含まれるリソースタイプに関係なく、指定されたリソースグループを登録します。

```
aws ssm register-target-with-maintenance-window \
    --window-id "mw-0c50858d01EXAMPLE" \
    --resource-type "RESOURCE_GROUP" \
    --target "Key=resource-groups:Name,Values=MyResourceGroup"
```

出力:

```
{
    "WindowTargetId":"1a2b3c4d-1a2b-1a2b-1a2b-1a2b3c4d-1a2"
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「Register a Target Instance with the Maintenance Window (AWS CLI)」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「RegisterTargetWithMaintenanceWindow」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、インスタンスをメンテナンスウィンドウに登録します。

```
$option1 = @{Key="InstanceIds";Values=@("i-0000293ffd8c57862")}
Register-SSMTargetWithMaintenanceWindow -WindowId "mw-06cf17cbefcb4bf4f" -Target
 $option1 -OwnerInformation "Single instance" -ResourceType "INSTANCE"
```

出力:

```
d8e47760-23ed-46a5-9f28-927337725398
```

例 2: この例では、複数のインスタンスをメンテナンスウィンドウに登録します。

```
$option1 =
 @{Key="InstanceIds";Values=@("i-0000293ffd8c57862","i-0cb2b964d3e14fd9f")}
Register-SSMTargetWithMaintenanceWindow -WindowId "mw-06cf17cbefcb4bf4f" -Target
 $option1 -OwnerInformation "Single instance" -ResourceType "INSTANCE"
```

出力:

```
6ab5c208-9fc4-4697-84b7-b02a6cc25f7d
```

例 3: この例では、EC2 タグを使用して、インスタンスをメンテナンスウィンドウに登録します。

```
$option1 = @{Key="tag:Environment";Values=@("Production")}
Register-SSMTargetWithMaintenanceWindow -WindowId "mw-06cf17cbefcb4bf4f" -Target
 $option1 -OwnerInformation "Production Web Servers" -ResourceType "INSTANCE"
```

出力:

```
2994977e-aefb-4a71-beac-df620352f184
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「RegisterTargetWithMaintenanceWindow」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **RegisterTaskWithMaintenanceWindow** を使用する

次のサンプルコードは、RegisterTaskWithMaintenanceWindow を使用する方法を説明しています。

CLI

AWS CLI

例 1: メンテナンスウィンドウにオートメーションタスクを登録するには

次の register-task-with-maintenance-window の例では、インスタンスをターゲットとするメンテナンスウィンドウにオートメーションタスクを登録します。

```
aws ssm register-task-with-maintenance-window \
    --window-id "mw-082dcd7649EXAMPLE" \
    --targets Key=InstanceIds,Values=i-1234520122EXAMPLE \
    --task-arn AWS-RestartEC2Instance \
    --service-role-arn arn:aws:iam::111222333444:role/SSM --task-type AUTOMATION
 \
    --task-invocation-parameters "{\"Automation\":{\"DocumentVersion\":\"\$LATEST
\",\"Parameters\":{\"InstanceId\":[\"{{RESOURCE_ID}}\"]}}}" \
    --priority 0 \
    --max-concurrency 1 \
    --max-errors 1 \
```

```
    --name "AutomationExample" \
    --description "Restarting EC2 Instance for maintenance"
```

出力:

```
{
    "WindowTaskId":"11144444-5555-6666-7777-88888888"
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「Register a Task with the Maintenance Window (AWS CLI)」を参照してください。

例 2: メンテナンスウィンドウに Lambda タスクを登録するには

次の `register-task-with-maintenance-window` の例では、インスタンスをターゲットとするメンテナンスウィンドウに Lambda タスクを登録します。

```
aws ssm register-task-with-maintenance-window \
    --window-id "mw-082dcd7649dee04e4" \
    --targets Key=InstanceIds,Values=i-12344d305eEXAMPLE \
    --task-arn arn:aws:lambda:us-east-1:111222333444:function:SSMTestLAMBDA \
    --service-role-arn arn:aws:iam::111222333444:role/SSM \
    --task-type LAMBDA \
    --task-invocation-parameters '{"Lambda":{"Payload":"{\"InstanceId\":
\"{{RESOURCE_ID}}\",\"targetType\":\"{{TARGET_TYPE}}\"}","Qualifier":"$LATEST"}}'
 \
    --priority 0 \
    --max-concurrency 10 \
    --max-errors 5 \
    --name "Lambda_Example" \
    --description "My Lambda Example"
```

出力:

```
{
    "WindowTaskId":"22244444-5555-6666-7777-88888888"
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「Register a Task with the Maintenance Window (AWS CLI)」を参照してください。

例 3: メンテナンスウィンドウに Run Command タスクを登録するには

次の `register-task-with-maintenance-window` の例では、インスタンスをターゲットとするメンテナンスウィンドウに Run Command タスクを登録します。

```
aws ssm register-task-with-maintenance-window \
    --window-id "mw-082dcd7649dee04e4" \
    --targets "Key=InstanceIds,Values=i-12344d305eEXAMPLE" \
    --service-role-arn "arn:aws:iam::111222333444:role/SSM" \
    --task-type "RUN_COMMAND" \
    --name "SSMInstallPowerShellModule" \
    --task-arn "AWS-InstallPowerShellModule" \
    --task-invocation-parameters "{\"RunCommand\":{\"Comment\":\"\",
\"OutputS3BucketName\":\"runcommandlogs\",\"Parameters\":{\"commands\":[\"Get-
Module -ListAvailable\"],\"executionTimeout\":[\"3600\"],\"source\":[\"https:\/
\/gallery.technet.microsoft.com\/EZOut-33ae0fb7\/file\/110351\/1\/EZOut.zip\"],
\"workingDirectory\":[\"\\\\\"]},\"TimeoutSeconds\":600}}" \
    --max-concurrency 1 \
    --max-errors 1 \
    --priority 10
```

出力:

```
{
    "WindowTaskId":"33344444-5555-6666-7777-88888888"
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「Register a Task with the Maintenance Window (AWS CLI)」を参照してください。

例 4: Step Functions タスクをメンテナンスウィンドウに登録するには

次の `register-task-with-maintenance-window` の例では、インスタンスをターゲットとするメンテナンスウィンドウに Step Functions タスクを登録します。

```
aws ssm register-task-with-maintenance-window \
    --window-id "mw-1234d787d6EXAMPLE" \
    --targets Key=WindowTargetIds,Values=12347414-69c3-49f8-95b8-ed2dcEXAMPLE \
    --task-arn arn:aws:states:us-
east-1:111222333444:stateMachine:SSMTestStateMachine \
    --service-role-arn arn:aws:iam::111222333444:role/MaintenanceWindows \
```

```
    --task-type STEP_FUNCTIONS \
    --task-invocation-parameters '{"StepFunctions":{"Input":"{\"InstanceId\":
\"{{RESOURCE_ID}}\"}"}}' \
    --priority 0 \
    --max-concurrency 10 \
    --max-errors 5 \
    --name "Step_Functions_Example" \
    --description "My Step Functions Example"
```

出力:

```
{
    "WindowTaskId":"44444444-5555-6666-7777-88888888"
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「Register a Task with the Maintenance Window (AWS CLI)」を参照してください。

例 5: メンテナンスウィンドウのターゲット ID を使用してタスクを登録するには

次の register-task-with-maintenance-window の例では、メンテナンスウィンドウのターゲット ID を使用してタスクを登録します。メンテナンスウィンドウのターゲット ID は、aws ssm register-target-with-maintenance-window コマンドの出力に含まれていました。この情報は aws ssm describe-maintenance-window-targets コマンドの出力から取得することもできます。

```
aws ssm register-task-with-maintenance-window \
    --targets "Key=WindowTargetIds,Values=350d44e6-28cc-44e2-951f-4b2c9EXAMPLE" \
    --task-arn "AWS-RunShellScript" \
    --service-role-arn "arn:aws:iam::111222333444:role/MaintenanceWindowsRole" \
    --window-id "mw-ab12cd34eEXAMPLE" \
    --task-type "RUN_COMMAND" \
    --task-parameters  "{\"commands\":{\"Values\":[\"df\"]}}" \
    --max-concurrency 1 \
    --max-errors 1 \
    --priority 10
```

出力:

```
{
    "WindowTaskId":"33344444-5555-6666-7777-88888888"
```

```
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「Register a Task with the Maintenance Window (AWS CLI)」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「RegisterTaskWithMaintenanceWindow」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、インスタンス ID を使用して、タスクをメンテナンスウィンドウに登録します。出力はタスク ID です。

```
$parameters = @{}
$parameterValues = New-Object
 Amazon.SimpleSystemsManagement.Model.MaintenanceWindowTaskParameterValueExpression
$parameterValues.Values = @("Install")
$parameters.Add("Operation", $parameterValues)

Register-SSMTaskWithMaintenanceWindow -WindowId "mw-03a342e62c96d31b0"
 -ServiceRoleArn "arn:aws:iam::123456789012:role/MaintenanceWindowsRole"
 -MaxConcurrency 1 -MaxError 1 -TaskArn "AWS-RunShellScript" -Target
 @{ Key="InstanceIds";Values="i-0000293ffd8c57862" } -TaskType "RUN_COMMAND" -
Priority 10 -TaskParameter $parameters
```

出力:

```
f34a2c47-ddfd-4c85-a88d-72366b69af1b
```

例 2: この例では、ターゲット ID を使用して、タスクをメンテナンスウィンドウに登録します。出力はタスク ID です。

```
$parameters = @{}
$parameterValues = New-Object
 Amazon.SimpleSystemsManagement.Model.MaintenanceWindowTaskParameterValueExpression
$parameterValues.Values = @("Install")
$parameters.Add("Operation", $parameterValues)
```

```
register-ssmtaskwithmaintenancewindow -WindowId "mw-03a342e62c96d31b0"
 -ServiceRoleArn "arn:aws:iam::123456789012:role/MaintenanceWindowsRole"
 -MaxConcurrency 1 -MaxError 1 -TaskArn "AWS-RunShellScript" -Target
 @{ Key="WindowTargetIds";Values="350d44e6-28cc-44e2-951f-4b2c985838f6" } -
TaskType "RUN_COMMAND" -Priority 10 -TaskParameter $parameters
```

出力:

```
f34a2c47-ddfd-4c85-a88d-72366b69af1b
```

例 3: この例では、run コマンドドキュメント **AWS-RunPowerShellScript** のパラメータオブジェクトを作成し、ターゲット ID を使用して任意のメンテナンスウィンドウを持つタスクを作成します。返される出力はタスク ID です。

```
$parameters =
 [Collections.Generic.Dictionary[String,Collections.Generic.List[String]]]::new()
$parameters.Add("commands",@("ipconfig","dir env:\computername"))
$parameters.Add("executionTimeout",@(3600))

$props = @{
    WindowId = "mw-0123e4cce56ff78ae"
    ServiceRoleArn = "arn:aws:iam::123456789012:role/MaintenanceWindowsRole"
    MaxConcurrency = 1
    MaxError = 1
    TaskType = "RUN_COMMAND"
    TaskArn = "AWS-RunPowerShellScript"
    Target =
 @{Key="WindowTargetIds";Values="fe1234ea-56d7-890b-12f3-456b789bee0f"}
    Priority = 1
    RunCommand_Parameter = $parameters
    Name = "set-via-cmdlet"
}

Register-SSMTaskWithMaintenanceWindow @props
```

出力:

```
f1e2ef34-5678-12e3-456a-12334c5c6cbe
```

例 4: この例では、**Create-Snapshots** という名前のドキュメントを使用して AWS Systems Manager Automation タスクを登録します。

```
$automationParameters = @{}
$automationParameters.Add( "instanceId", @("{{ TARGET_ID }}") )
$automationParameters.Add( "AutomationAssumeRole",
 @("{arn:aws:iam::111111111111:role/AutomationRole}") )
$automationParameters.Add( "SnapshotTimeout", @("PT20M") )
Register-SSMTaskWithMaintenanceWindow -WindowId mw-123EXAMPLE456`
    -ServiceRoleArn "arn:aws:iam::123456789012:role/MW-Role"`
    -MaxConcurrency 1 -MaxError 1 -TaskArn "CreateVolumeSnapshots"`
    -Target @{ Key="WindowTargetIds";Values="4b5acdf4-946c-4355-
bd68-4329a43a5fd1" }`
    -TaskType "AUTOMATION"`
    -Priority 4`
    -Automation_DocumentVersion '$DEFAULT' -Automation_Parameter
 $automationParameters -Name "Create-Snapshots"
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「RegisterTaskWithMaintenanceWindow」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **RemoveTagsFromResource** を使用する

次のサンプルコードは、RemoveTagsFromResource を使用する方法を説明しています。

CLI

AWS CLI

パッチベースラインからタグを削除するには

次の remove-tags-from-resource の例では、パッチベースラインからタグが削除されます。

```
aws ssm remove-tags-from-resource \
    --resource-type "PatchBaseline" \
    --resource-id "pb-0123456789abcdef0" \
    --tag-keys "Region"
```

このコマンドでは何も出力されません。

詳細については、「AWS 全般リファレンス」の「AWS リソースのタグ付け」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「RemoveTagsFromResource」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、メンテナンスウィンドウからタグを削除します。コマンドが成功した場合、出力はありません。

```
Remove-SSMResourceTag -ResourceId "mw-03eb9db42890fb82d" -ResourceType
 "MaintenanceWindow" -TagKey "Production"
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「RemoveTagsFromResource」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI で **SendCommand** を使用する

次のサンプルコードは、SendCommand を使用する方法を説明しています。

アクション例は、より大きなプログラムからのコードの抜粋であり、コンテキスト内で実行する必要があります。次のコード例で、このアクションのコンテキストを確認できます。

- 基本を学ぶ

CLI

AWS CLI

例 1: 1 つ以上のリモートインスタンスでコマンドを実行するには

次の send-command の例では、ターゲットインスタンスで echo コマンドを実行します。

```
aws ssm send-command \
    --document-name "AWS-RunShellScript" \
    --parameters 'commands=["echo HelloWorld"]' \
    --targets "Key=instanceids,Values=i-1234567890abcdef0" \
    --comment "echo HelloWorld"
```

出力:

```
{
    "Command": {
        "CommandId": "92853adf-ba41-4cd6-9a88-142d1EXAMPLE",
        "DocumentName": "AWS-RunShellScript",
        "DocumentVersion": "",
        "Comment": "echo HelloWorld",
        "ExpiresAfter": 1550181014.717,
        "Parameters": {
            "commands": [
                "echo HelloWorld"
            ]
        },
        "InstanceIds": [
            "i-0f00f008a2dcbefe2"
        ],
        "Targets": [],
        "RequestedDateTime": 1550173814.717,
        "Status": "Pending",
        "StatusDetails": "Pending",
        "OutputS3BucketName": "",
        "OutputS3KeyPrefix": "",
        "MaxConcurrency": "50",
        "MaxErrors": "0",
        "TargetCount": 1,
        "CompletedCount": 0,
        "ErrorCount": 0,
        "DeliveryTimedOutCount": 0,
        "ServiceRole": "",
        "NotificationConfig": {
            "NotificationArn": "",
            "NotificationEvents": [],
            "NotificationType": ""
        },
        "CloudWatchOutputConfig": {
            "CloudWatchLogGroupName": "",
```

```
            "CloudWatchOutputEnabled": false
        }
    }
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「Running Commands Using Systems Manager Run Command」を参照してください。

例 2: インスタンスの IP 情報を取得するには

次の send-command の例では、インスタンスに関する IP 情報を取得します。

```
aws ssm send-command \
    --instance-ids "i-1234567890abcdef0" \
    --document-name "AWS-RunShellScript" \
    --comment "IP config" \
    --parameters "commands=ifconfig"
```

出力例については、例 1 を参照してください。

詳細については、「AWS Systems Manager ユーザーガイド」の「Running Commands Using Systems Manager Run Command」を参照してください。

例 3: 特定のタグを持つインスタンスでコマンドを実行するには

次の send-command の例では、タグキー「ENV」と値「Dev」を持つインスタンスでコマンドを実行します。

```
aws ssm send-command \
    --targets "Key=tag:ENV,Values=Dev" \
    --document-name "AWS-RunShellScript" \
    --parameters "commands=ifconfig"
```

出力例については、例 1 を参照してください。

詳細については、「AWS Systems Manager ユーザーガイド」の「Running Commands Using Systems Manager Run Command」を参照してください。

例 4: SNS 通知を送信するコマンドを実行するには

次の send-command の例では、すべての通知イベントと Command 通知タイプの SNS 通知を送信するコマンドを実行します。

```
aws ssm send-command \
    --instance-ids "i-1234567890abcdef0" \
    --document-name "AWS-RunShellScript" \
    --comment "IP config" \
    --parameters "commands=ifconfig" \
    --service-role-arn "arn:aws:iam::123456789012:role/SNS_Role" \
    --notification-config "NotificationArn=arn:aws:sns:us-
east-1:123456789012:SNSTopicName,NotificationEvents=All,NotificationType=Command"
```

出力例については、例 1 を参照してください。

詳細については、「AWS Systems Manager ユーザーガイド」の「Running Commands Using Systems Manager Run Command」を参照してください。

例 5: S3 と CloudWatch に出力するコマンドを実行するには

次の send-command の例では、コマンドの詳細を S3 バケットと CloudWatch Logs ロググループに出力するコマンドを実行します。

```
aws ssm send-command \
    --instance-ids "i-1234567890abcdef0" \
    --document-name "AWS-RunShellScript" \
    --comment "IP config" \
    --parameters "commands=ifconfig" \
    --output-s3-bucket-name "s3-bucket-name" \
    --output-s3-key-prefix "runcommand" \
    --cloud-watch-output-
config "CloudWatchOutputEnabled=true,CloudWatchLogGroupName=CWLGroupName"
```

出力例については、例 1 を参照してください。

詳細については、「AWS Systems Manager ユーザーガイド」の「Running Commands Using Systems Manager Run Command」を参照してください。

例 6: タグが異なる複数のインスタンスでコマンドを実行するには

次の send-command の例では、2 つの異なるタグキーと値を持つインスタンスでコマンドを実行します。

```
aws ssm send-command \
```

```
    --document-name "AWS-RunPowerShellScript" \
    --parameters commands=["echo helloWorld"] \
    --targets Key=tag:Env,Values=Dev Key=tag:Role,Values=WebServers
```

出力例については、例 1 を参照してください。

詳細については、「AWS Systems Manager ユーザーガイド」の「Running Commands Using Systems Manager Run Command」を参照してください。

例 7: 同じタグキーを持つ複数のインスタンスをターゲットにするには

次の send-command の例では、タグキーは同じだが異なる値を持つインスタンスにコマンドを実行します。

```
aws ssm send-command \
    --document-name "AWS-RunPowerShellScript" \
    --parameters commands=["echo helloWorld"] \
    --targets Key=tag:Env,Values=Dev,Test
```

出力例については、例 1 を参照してください。

詳細については、「AWS Systems Manager ユーザーガイド」の「Running Commands Using Systems Manager Run Command」を参照してください。

例 8: 共有ドキュメントを使用するコマンドを実行するには

次の send-command の例では、ターゲットインスタンスで共有ドキュメントを実行します。

```
aws ssm send-command \
    --document-name "arn:aws:ssm:us-east-1:123456789012:document/ExampleDocument"
 \
    --targets "Key=instanceids,Values=i-1234567890abcdef0"
```

出力例については、例 1 を参照してください。

詳細については、「AWS Systems Manager ユーザーガイド」の「Using shared SSM documents」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「SendCommand」を参照してください。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
   /**
    * Sends a SSM command to a managed node asynchronously.
    *
    * @param documentName The name of the document to use.
    * @param instanceId The ID of the instance to send the command to.
    * @return The command ID.
    * <p>
    * This method initiates asynchronous requests to send a SSM command to a
managed node.
    * It waits until the document is active, sends the command, and checks the
command execution status.
    */
   public String sendSSMCommand(String documentName, String instanceId) throws
InterruptedException, SsmException {
       // Before we use Document to send a command - make sure it is active.
       CompletableFuture<Void> documentActiveFuture =
CompletableFuture.runAsync(() -> {
           boolean isDocumentActive = false;
           DescribeDocumentRequest request = DescribeDocumentRequest.builder()
                   .name(documentName)
                   .build();

           while (!isDocumentActive) {
               CompletableFuture<DescribeDocumentResponse> response =
getAsyncClient().describeDocument(request);
               String documentStatus =
response.join().document().statusAsString();
               if (documentStatus.equals("Active")) {
                   System.out.println("The SSM document is active and ready to
use.");
                   isDocumentActive = true;
               } else {
```

```
                    System.out.println("The SSM document is not active. Status: "
+ documentStatus);
                    try {
                        Thread.sleep(5000);
                    } catch (InterruptedException e) {
                        throw new RuntimeException(e);
                    }
                }
            }
        });

        documentActiveFuture.join();

        // Create the SendCommandRequest.
        SendCommandRequest commandRequest = SendCommandRequest.builder()
                .documentName(documentName)
                .instanceIds(instanceId)
                .build();

        // Send the command.
        CompletableFuture<SendCommandResponse> commandFuture =
getAsyncClient().sendCommand(commandRequest);
        final String[] commandId = {null};

        commandFuture.whenComplete((commandResponse, ex) -> {
            if (commandResponse != null) {
                commandId[0] = commandResponse.command().commandId();
                System.out.println("Command ID: " + commandId[0]);

                // Wait for the command execution to complete.
                GetCommandInvocationRequest invocationRequest =
GetCommandInvocationRequest.builder()
                        .commandId(commandId[0])
                        .instanceId(instanceId)
                        .build();

                try {
                    System.out.println("Wait 5 secs");
                    TimeUnit.SECONDS.sleep(5);

                    // Retrieve the command execution details.
                    CompletableFuture<GetCommandInvocationResponse>
invocationFuture = getAsyncClient().getCommandInvocation(invocationRequest);
```

```
                    invocationFuture.whenComplete((commandInvocationResponse,
invocationEx) -> {
                        if (commandInvocationResponse != null) {
                            // Check the status of the command execution.
                            CommandInvocationStatus status =
commandInvocationResponse.status();
                            if (status == CommandInvocationStatus.SUCCESS) {
                                System.out.println("Command execution
successful");
                            } else {
                                System.out.println("Command execution failed.
Status: " + status);
                            }
                        } else {
                            Throwable invocationCause = (invocationEx instanceof
CompletionException) ? invocationEx.getCause() : invocationEx;
                            throw new CompletionException(invocationCause);
                        }
                    }).join();
                } catch (InterruptedException e) {
                    throw new RuntimeException(e);
                }
            } else {
                Throwable cause = (ex instanceof CompletionException) ?
ex.getCause() : ex;
                if (cause instanceof SsmException) {
                    throw (SsmException) cause;
                } else {
                    throw new RuntimeException(cause);
                }
            }
        }).join();

        return commandId[0];
    }
```

- API の詳細については、「AWS SDK for Java 2.x API リファレンス」の「SendCommand」を参照してください。

JavaScript

SDK for JavaScript (v3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
import { SendCommandCommand, SSMClient } from "@aws-sdk/client-ssm";
import { parseArgs } from "node:util";

/**
 * Send an SSM command to a managed node.
 * @param {{ documentName: string }}
 */
export const main = async ({ documentName }) => {
  const client = new SSMClient({});
  try {
    await client.send(
      new SendCommandCommand({
        DocumentName: documentName,
      }),
    );
    console.log("Command sent successfully.");
    return { Success: true };
  } catch (caught) {
    if (caught instanceof Error && caught.name === "ValidationError") {
      console.warn(`${caught.message}. Did you provide a valid document name?`);
    } else {
      throw caught;
    }
  }
};
```

- API の詳細については、「AWS SDK for JavaScript API リファレンス」の「SendCommand」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、ターゲットインスタンスで echo コマンドを実行します。

```
Send-SSMCommand -DocumentName "AWS-RunPowerShellScript" -Parameter @{commands =
 "echo helloWorld"} -Target @{Key="instanceids";Values=@("i-0cb2b964d3e14fd9f")}
```

出力:

```
CommandId          : d8d190fc-32c1-4d65-a0df-ff5ff3965524
Comment            :
CompletedCount     : 0
DocumentName       : AWS-RunPowerShellScript
ErrorCount         : 0
ExpiresAfter       : 3/7/2017 10:48:37 PM
InstanceIds        : {}
MaxConcurrency     : 50
MaxErrors          : 0
NotificationConfig : Amazon.SimpleSystemsManagement.Model.NotificationConfig
OutputS3BucketName :
OutputS3KeyPrefix  :
OutputS3Region     :
Parameters         : {[commands,
 Amazon.Runtime.Internal.Util.AlwaysSendList`1[System.String]]}
RequestedDateTime  : 3/7/2017 9:48:37 PM
ServiceRole        :
Status             : Pending
StatusDetails      : Pending
TargetCount        : 0
Targets            : {instanceids}
```

例 2: この例は、ネストされたパラメータを受け入れるコマンドを実行する方法を示しています。

```
Send-SSMCommand -DocumentName "AWS-RunRemoteScript" -Parameter
 @{ sourceType="GitHub";sourceInfo='{"owner": "me","repository": "amazon-
ssm","path": "Examples/Install-Win32OpenSSH"}'; "commandLine"=".\Install-
Win32OpenSSH.ps1"} -InstanceId i-0cb2b964d3e14fd9f
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「SendCommand」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
class DocumentWrapper:
    """Encapsulates AWS Systems Manager Document actions."""

    def __init__(self, ssm_client):
        """
        :param ssm_client: A Boto3 Systems Manager client.
        """
        self.ssm_client = ssm_client
        self.name = None

    @classmethod
    def from_client(cls):
        ssm_client = boto3.client("ssm")
        return cls(ssm_client)


    def send_command(self, instance_ids):
        """
        Sends a command to one or more instances.

        :param instance_ids: The IDs of the instances to send the command to.
        :return: The ID of the command.
        """
        try:
            response = self.ssm_client.send_command(
                InstanceIds=instance_ids, DocumentName=self.name,
 TimeoutSeconds=3600
            )
```

```
            return response["Command"]["CommandId"]
        except ClientError as err:
            logger.error(
                "Couldn't send command to %s. Here's why: %s: %s",
                self.name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
```

- API の詳細については、「AWS SDK for Python (Boto3) API リファレンス」の「SendCommand」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **StartAutomationExecution** を使用する

次のサンプルコードは、StartAutomationExecution を使用する方法を説明しています。

CLI

AWS CLI

例 1: オートメーションドキュメントを実行するには

次の start-automation-execution の例では、オートメーションドキュメントを実行します。

```
aws ssm start-automation-execution \
    --document-name "AWS-UpdateLinuxAmi" \
    --parameters "AutomationAssumeRole=arn:aws:iam::123456789012:role/
SSMAutomationRole,SourceAmiId=ami-EXAMPLE,IamInstanceProfileName=EC2InstanceRole"
```

出力:

```
{
  "AutomationExecutionId": "4105a4fc-f944-11e6-9d32-0a1b2EXAMPLE"
```

```
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「オートメーションを手動で実行する」を参照してください。

例 2: 共有オートメーションドキュメントを実行するには

次の start-automation-execution の例では、共有オートメーションドキュメントを実行します。

```
aws ssm start-automation-execution \
    --document-name "arn:aws:ssm:us-east-1:123456789012:document/ExampleDocument"
```

出力:

```
{
  "AutomationExecutionId": "4105a4fc-f944-11e6-9d32-0a1b2EXAMPLE"
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「Using shared SSM documents」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「StartAutomationExecution」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、オートメーションロール、AMI ソース ID、および Amazon EC2 インスタンスロールを指定するドキュメントを実行します。

```
Start-SSMAutomationExecution -DocumentName AWS-UpdateLinuxAmi -
Parameter @{'AutomationAssumeRole'='arn:aws:iam::123456789012:role/
SSMAutomationRole';'SourceAmiId'='ami-
f173cc91';'InstanceIamRole'='EC2InstanceRole'}
```

出力:

```
3a532a4f-0382-11e7-9df7-6f11185f6dd1
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「StartAutomationExecution」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **StartSession** を使用する

次のサンプルコードは、StartSession を使用する方法を説明しています。

CLI

AWS CLI

例 1: Session Manager のセッションを開始するには

この start-session の例では、Session Manager のセッションのためにインスタンスとの接続を確立します。このインタラクティブなコマンドでは、呼び出しを実行するクライアントマシンに Session Manager プラグインがインストールされている必要があることに留意してください。

```
aws ssm start-session \
    --target "i-1234567890abcdef0"
```

出力:

```
Starting session with SessionId: Jane-Roe-07a16060613c408b5
```

例 2: SSH を使用して Session Manager のセッションを開始するには

この start-session の例では、SSH を使用して Session Manager のセッションのためにインスタンスとの接続を確立します。このインタラクティブなコマンドでは、呼び出しを実行するクライアントマシンに Session Manager プラグインがインストールされている必要があり、コマンドは Linux の EC2 インスタンスの ec2-user など、インスタンスのデフォルトユーザーを使用することに留意してください。

```
ssh -i /path/my-key-pair.pem ec2-user@i-02573cafcfEXAMPLE
```

出力:

```
Starting session with SessionId: ec2-user-07a16060613c408b5
```

詳細については、「AWS Systems Manager ユーザーガイド」の「セッションを開始する」および「AWS CLI 用の Session Manager プラグインをインストールする」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「StartSession」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、Session Manager のセッションのターゲットへの接続を開始し、ポート転送を有効にします。

```
Start-SSMSession -Target 'i-064578e5e7454488f' -DocumentName 'AWS-
StartPortForwardingSession' -Parameter @{ localPortNumber = '8080'; portNumber =
 '80' }
```

出力:

```
SessionId    StreamUrl
----------    ----------
random-id0    wss://ssmmessages.amazonaws.com/v1/data-channel/random-id
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「StartSession」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **StopAutomationExecution** を使用する

次のサンプルコードは、StopAutomationExecution を使用する方法を説明しています。

CLI

AWS CLI

オートメーションの実行を停止するには

次の stop-automation-execution の例では、オートメーションドキュメントを停止します。

```
aws ssm stop-automation-execution
    --automation-execution-id "4105a4fc-f944-11e6-9d32-0a1b2EXAMPLE"
```

このコマンドでは何も出力されません。

詳細については、「AWS Systems Manager ユーザーガイド」の「オートメーションを手動で実行する」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「StopAutomationExecution」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、オートメーションの実行を停止します。コマンドが成功した場合、出力はありません。

```
Stop-SSMAutomationExecution -AutomationExecutionId "4105a4fc-
f944-11e6-9d32-8fb2db27a909"
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「StopAutomationExecution」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **UpdateAssociation** を使用する

次のサンプルコードは、UpdateAssociation を使用する方法を説明しています。

CLI

AWS CLI

例 1: ドキュメントの関連付けを更新するには

次の update-association の例では、新しいドキュメントバージョンとの関連付けを更新します。

```
aws ssm update-association \
    --association-id "8dfe3659-4309-493a-8755-0123456789ab" \
    --document-version "\$LATEST"
```

出力:

```
{
    "AssociationDescription": {
        "Name": "AWS-UpdateSSMAgent",
        "AssociationVersion": "2",
        "Date": 1550508093.293,
        "LastUpdateAssociationDate": 1550508106.596,
        "Overview": {
            "Status": "Pending",
            "DetailedStatus": "Creating"
        },
        "DocumentVersion": "$LATEST",
        "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
        "Targets": [
            {
                "Key": "tag:Name",
                "Values": [
                    "Linux"
                ]
            }
        ],
        "LastExecutionDate": 1550508094.879,
        "LastSuccessfulExecutionDate": 1550508094.879
    }
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「関連付けの編集と新しいバージョンの作成」を参照してください。

例 2: 関連付けのスケジュール式を更新するには

次の update-association の例では、指定された関連付けのスケジュール式を更新します。

```
aws ssm update-association \
    --association-id "8dfe3659-4309-493a-8755-0123456789ab" \
    --schedule-expression "cron(0 0 0/4 1/1 * ? *)"
```

出力:

```
{
    "AssociationDescription": {
        "Name": "AWS-HelloWorld",
        "AssociationVersion": "2",
        "Date": "2021-02-08T13:54:19.203000-08:00",
        "LastUpdateAssociationDate": "2021-06-29T11:51:07.933000-07:00",
        "Overview": {
            "Status": "Pending",
            "DetailedStatus": "Creating"
        },
        "DocumentVersion": "$DEFAULT",
        "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
        "Targets": [
            {
                "Key": "aws:NoOpAutomationTag",
                "Values": [
                    "AWS-NoOpAutomationTarget-Value"
                ]
            }
        ],
        "ScheduleExpression": "cron(0 0 0/4 1/1 * ? *)",
        "LastExecutionDate": "2021-06-26T19:00:48.110000-07:00",
        "ApplyOnlyAtCronInterval": false
    }
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「関連付けの編集と新しいバージョンの作成」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「UpdateAssociation」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、新しいドキュメントバージョンとの関連付けを更新します。

```
Update-SSMAssociation -AssociationId "93285663-92df-44cb-9f26-2292d4ecc439" -
DocumentVersion "1"
```

出力:

```
Name                  : AWS-UpdateSSMAgent
InstanceId            :
Date                  : 3/1/2017 6:22:21 PM
Status.Name           :
Status.Date           :
Status.Message        :
Status.AdditionalInfo :
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「UpdateAssociation」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **UpdateAssociationStatus** を使用する

次のサンプルコードは、UpdateAssociationStatus を使用する方法を説明しています。

CLI

AWS CLI

関連付けステータスを更新するには

次の update-association-status の例では、インスタンスとドキュメント間の関連付けの関連付けステータスを更新します。

```
aws ssm update-association-status \
    --name "AWS-UpdateSSMAgent" \
    --instance-id "i-1234567890abcdef0" \
```

```
    --association-
status "Date=1424421071.939,Name=Pending,Message=temp_status_change,AdditionalInfo=Additi
Config-Needed"
```

出力:

```
{
    "AssociationDescription": {
        "Name": "AWS-UpdateSSMAgent",
        "InstanceId": "i-1234567890abcdef0",
        "AssociationVersion": "1",
        "Date": 1550507529.604,
        "LastUpdateAssociationDate": 1550507806.974,
        "Status": {
            "Date": 1424421071.0,
            "Name": "Pending",
            "Message": "temp_status_change",
            "AdditionalInfo": "Additional-Config-Needed"
        },
        "Overview": {
            "Status": "Success",
            "AssociationStatusAggregatedCount": {
                "Success": 1
            }
        },
        "DocumentVersion": "$DEFAULT",
        "AssociationId": "8dfe3659-4309-493a-8755-0123456789ab",
        "Targets": [
            {
                "Key": "InstanceIds",
                "Values": [
                    "i-1234567890abcdef0"
                ]
            }
        ],
        "LastExecutionDate": 1550507808.0,
        "LastSuccessfulExecutionDate": 1550507808.0
    }
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「Systems Manager の関連付けの使用」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「UpdateAssociationStatus」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、インスタンスと設定ドキュメント間の関連付けのステータスを更新します。

```
Update-SSMAssociationStatus -Name "AWS-UpdateSSMAgent" -InstanceId
 "i-0000293ffd8c57862" -AssociationStatus_Date "2015-02-20T08:31:11Z"
 -AssociationStatus_Name "Pending" -AssociationStatus_Message
 "temporary_status_change" -AssociationStatus_AdditionalInfo "Additional-Config-
Needed"
```

出力:

```
Name                   : AWS-UpdateSSMAgent
InstanceId             : i-0000293ffd8c57862
Date                   : 2/23/2017 6:55:22 PM
Status.Name            : Pending
Status.Date            : 2/20/2015 8:31:11 AM
Status.Message         : temporary_status_change
Status.AdditionalInfo : Additional-Config-Needed
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「UpdateAssociationStatus」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **UpdateDocument** を使用する

次のサンプルコードは、UpdateDocument を使用する方法を説明しています。

CLI

AWS CLI

ドキュメントの新しいバージョンを作成するには

次の update-document の例では、Windows コンピュータでの実行時に、ドキュメントの新しいバージョンを作成します。--document で指定されるドキュメントは JSON 形式である必要があります。file:// に続くコンテンツファイルのパスを参照する必要があることに注意してください。--document-version パラメータの先頭に $ があるため、Windows では値を二重引用符で囲む必要があります。Linux、MacOS、または PowerShell プロンプトでは、値を一重引用符で囲む必要があります。

Windows のバージョン:

```
aws ssm update-document \
    --name "RunShellScript" \
    --content "file://RunShellScript.json" \
    --document-version "$LATEST"
```

Linux/Mac バージョン:

```
aws ssm update-document \
    --name "RunShellScript" \
    --content "file://RunShellScript.json" \
    --document-version '$LATEST'
```

出力:

```
{
  "DocumentDescription": {
      "Status": "Updating",
      "Hash": "f775e5df4904c6fa46686c4722fae9de1950dace25cd9608ff8d622046b68d9b",
      "Name": "RunShellScript",
      "Parameters": [
          {
              "Type": "StringList",
              "Name": "commands",
              "Description": "(Required) Specify a shell script or a command to
 run."
          }
```

```
      ],
      "DocumentType": "Command",
      "PlatformTypes": [
          "Linux"
      ],
      "DocumentVersion": "2",
      "HashType": "Sha256",
      "CreatedDate": 1487899655.152,
      "Owner": "809632081692",
      "SchemaVersion": "2.0",
      "DefaultVersion": "1",
      "LatestVersion": "2",
      "Description": "Run an updated script"
  }
}
```

- API の詳細については、「AWS CLI コマンドリファレンス」の「UpdateDocument」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: これは、指定した JSON ファイルの更新内容を含むドキュメントの新しいバージョンを作成するためのものです。ドキュメントは JSON 形式である必要があります。ドキュメントバージョンは、「Get-SSMDocumentVersionList」コマンドレットで取得できます。

```
Update-SSMDocument -Name RunShellScript -DocumentVersion "1" -Content (Get-
Content -Raw "c:\temp\RunShellScript.json")
```

出力:

```
CreatedDate     : 3/1/2017 2:59:17 AM
DefaultVersion  : 1
Description     : Run an updated script
DocumentType    : Command
DocumentVersion : 2
Hash            :
 1d5ce820e999ff051eb4841ed887593daf77120fd76cae0d18a53cc42e4e22c1
HashType        : Sha256
LatestVersion   : 2
```

```
Name            : RunShellScript
Owner           : 809632081692
Parameters      : {commands}
PlatformTypes   : {Linux}
SchemaVersion   : 2.0
Sha1            :
Status          : Updating
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「UpdateDocument」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **UpdateDocumentDefaultVersion** を使用する

次のサンプルコードは、UpdateDocumentDefaultVersion を使用する方法を説明しています。

CLI

AWS CLI

ドキュメントのデフォルトバージョンを更新するには

次の update-document-default-version の例では、Systems Manager ドキュメントのデフォルトバージョンを更新します。

```
aws ssm update-document-default-version \
    --name "Example" \
    --document-version "2"
```

出力:

```
{
    "Description": {
        "Name": "Example",
        "DefaultVersion": "2"
    }
}
```

詳細については、「AWS Systems Manager ユーザーガイド」の「SSM ドキュメントコンテンツを書き込む」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「UpdateDocumentDefaultVersion」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: ここではドキュメントのデフォルトバージョンを更新します。利用可能なドキュメントバージョンは、「Get-SSMDocumentVersionList」コマンドレットで取得できます。

```
Update-SSMDocumentDefaultVersion -Name "RunShellScript" -DocumentVersion "2"
```

出力:

```
DefaultVersion Name
-------------- ----
2              RunShellScript
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「UpdateDocumentDefaultVersion」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI で **UpdateMaintenanceWindow** を使用する

次のサンプルコードは、UpdateMaintenanceWindow を使用する方法を説明しています。

CLI

AWS CLI

例 1: メンテナンスウィンドウを更新するには

次の update-maintenance-window の例では、メンテナンスウィンドウの名前を更新します。

```
aws ssm update-maintenance-window \
    --window-id "mw-1a2b3c4d5e6f7g8h9" \
    --name "My-Renamed-MW"
```

出力:

```
{
    "Cutoff": 1,
    "Name": "My-Renamed-MW",
    "Schedule": "cron(0 16 ? * TUE *)",
    "Enabled": true,
    "AllowUnassociatedTargets": true,
    "WindowId": "mw-1a2b3c4d5e6f7g8h9",
    "Duration": 4
}
```

例 2: メンテナンスウィンドウを無効にするには

次の update-maintenance-window の例では、メンテナンスウィンドウを無効にします。

```
aws ssm update-maintenance-window \
    --window-id "mw-1a2b3c4d5e6f7g8h9" \
    --no-enabled
```

例 3: メンテナンスウィンドウを有効にするには

次の update-maintenance-window の例では、メンテナンスウィンドウを有効にします。

```
aws ssm update-maintenance-window \
    --window-id "mw-1a2b3c4d5e6f7g8h9" \
    --enabled
```

詳細については、「AWS Systems Manager ユーザーガイド」の「メンテナンスウィンドウの更新 (AWS CLI)」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「UpdateMaintenanceWindow」を参照してください。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
   /**
    * Updates an SSM maintenance window asynchronously.
    *
    * @param id The ID of the maintenance window to update.
    * @param name The new name for the maintenance window.
    * <p>
    * This method initiates an asynchronous request to update an SSM maintenance
window.
    * If the request is successful, it prints a success message.
    * If an exception occurs, it handles the error appropriately.
    */
   public void updateSSMMaintenanceWindow(String id, String name) throws
SsmException {
       UpdateMaintenanceWindowRequest updateRequest =
UpdateMaintenanceWindowRequest.builder()
               .windowId(id)
               .allowUnassociatedTargets(true)
               .duration(24)
               .enabled(true)
               .name(name)
               .schedule("cron(0 0 ? * MON *)")
               .build();

       CompletableFuture<UpdateMaintenanceWindowResponse> future =
getAsyncClient().updateMaintenanceWindow(updateRequest);
       future.whenComplete((response, ex) -> {
           if (response != null) {
               System.out.println("The SSM maintenance window was successfully
updated");
           } else {
               Throwable cause = (ex instanceof CompletionException) ?
ex.getCause() : ex;
```

```
                if (cause instanceof SsmException) {
                    throw new CompletionException(cause);
                } else {
                    throw new RuntimeException(cause);
                }
            }
        }).join();
    }
```

- API の詳細については、「AWS SDK for Java 2.x API リファレンス」の「UpdateMaintenanceWindow」を参照してください。

JavaScript

SDK for JavaScript (v3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
import { UpdateMaintenanceWindowCommand, SSMClient } from "@aws-sdk/client-ssm";
import { parseArgs } from "node:util";

/**
 * Update an SSM maintenance window.
 * @param {{ windowId: string, allowUnassociatedTargets?: boolean, duration?:
 number, enabled?: boolean, name?: string, schedule?: string }}
 */
export const main = async ({
  windowId,
  allowUnassociatedTargets = undefined, //Allow the maintenance window to run on
 managed nodes, even if you haven't registered those nodes as targets.
  duration = undefined, //The duration of the maintenance window in hours.
  enabled = undefined,
  name = undefined,
  schedule = undefined, //The schedule of the maintenance window in the form of a
 cron or rate expression.
}) => {
```

```
  const client = new SSMClient({});
  try {
    const { opsItemArn, opsItemId } = await client.send(
      new UpdateMaintenanceWindowCommand({
        WindowId: windowId,
        AllowUnassociatedTargets: allowUnassociatedTargets,
        Duration: duration,
        Enabled: enabled,
        Name: name,
        Schedule: schedule,
      }),
    );
    console.log("Maintenance window updated.");
    return { OpsItemArn: opsItemArn, OpsItemId: opsItemId };
  } catch (caught) {
    if (caught instanceof Error && caught.name === "ValidationError") {
      console.warn(`${caught.message}. Are these values correct?`);
    } else {
      throw caught;
    }
  }
};
```

- API の詳細については、「AWS SDK for JavaScript API リファレンス」の「UpdateMaintenanceWindow」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、メンテナンスウィンドウの名前を更新します。

```
Update-SSMMaintenanceWindow -WindowId "mw-03eb9db42890fb82d" -Name "My-Renamed-
MW"
```

出力:

```
AllowUnassociatedTargets : False
Cutoff                   : 1
Duration                 : 2
Enabled                  : True
```

```
Name                        : My-Renamed-MW
Schedule                    : cron(0 */30 * * * ? *)
WindowId                    : mw-03eb9db42890fb82d
```

例 2: この例では、メンテナンスウィンドウを有効にします。

```
Update-SSMMaintenanceWindow -WindowId "mw-03eb9db42890fb82d" -Enabled $true
```

出力:

```
AllowUnassociatedTargets : False
Cutoff                   : 1
Duration                 : 2
Enabled                  : True
Name                     : My-Renamed-MW
Schedule                 : cron(0 */30 * * * ? *)
WindowId                 : mw-03eb9db42890fb82d
```

例 3: この例では、メンテナンスウィンドウを無効にします。

```
Update-SSMMaintenanceWindow -WindowId "mw-03eb9db42890fb82d" -Enabled $false
```

出力:

```
AllowUnassociatedTargets : False
Cutoff                   : 1
Duration                 : 2
Enabled                  : False
Name                     : My-Renamed-MW
Schedule                 : cron(0 */30 * * * ? *)
WindowId                 : mw-03eb9db42890fb82d
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「UpdateMaintenanceWindow」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
class MaintenanceWindowWrapper:
    """Encapsulates AWS Systems Manager maintenance window actions."""

    def __init__(self, ssm_client):
        """
        :param ssm_client: A Boto3 Systems Manager client.
        """
        self.ssm_client = ssm_client
        self.window_id = None
        self.name = None

    @classmethod
    def from_client(cls):
        ssm_client = boto3.client("ssm")
        return cls(ssm_client)


    def update(
        self, name, enabled, schedule, duration, cutoff,
 allow_unassociated_targets
    ):
        """
        Update an AWS Systems Manager maintenance window.

        :param name: The name of the maintenance window.
        :param enabled: Whether the maintenance window is enabled to run on
 managed nodes.
        :param schedule: The schedule of the maintenance window.
        :param duration: The duration of the maintenance window.
        :param cutoff: The cutoff time of the maintenance window.
        :param allow_unassociated_targets: Allow the maintenance window to run on
 managed nodes, even
```

```
                                        if you haven't registered those nodes
as targets.
        """
        try:
            self.ssm_client.update_maintenance_window(
                WindowId=self.window_id,
                Name=name,
                Enabled=enabled,
                Schedule=schedule,
                Duration=duration,
                Cutoff=cutoff,
                AllowUnassociatedTargets=allow_unassociated_targets,
            )
            self.name = name
            logger.info("Updated maintenance window %s.", self.window_id)
        except ParamValidationError as error:
            logger.error(
                "Parameter validation error when trying to update maintenance
window %s. Here's why: %s",
                self.window_id,
                error,
            )
            raise
        except ClientError as err:
            logger.error(
                "Couldn't update maintenance window %s. Here's why: %s: %s",
                self.name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
```

- API の詳細については、「AWS SDK for Python (Boto3) API リファレンス」の「UpdateMaintenanceWindow」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **UpdateManagedInstanceRole** を使用する

次のサンプルコードは、UpdateManagedInstanceRole を使用する方法を説明しています。

CLI

AWS CLI

マネージドインスタンスの IAM ロールを更新するには

次の update-managed-instance-role の例では、マネージドインスタンスの IAM インスタンスプロファイルを更新します。

```
aws ssm update-managed-instance-role \
    --instance-id "mi-08ab247cdfEXAMPLE" \
    --iam-role "ExampleRole"
```

このコマンドでは何も出力されません。

詳細については、「AWS Systems Manager ユーザーガイド」の「Step 4: Create an IAM Instance Profile for Systems Manager」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「UpdateManagedInstanceRole」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、マネージドインスタンスのロールを更新します。コマンドが成功した場合、出力はありません。

```
Update-SSMManagedInstanceRole -InstanceId "mi-08ab247cdf1046573" -IamRole
 "AutomationRole"
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「UpdateManagedInstanceRole」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS SDK または CLI で **UpdateOpsItem** を使用する

次のサンプルコードは、UpdateOpsItem を使用する方法を説明しています。

アクション例は、より大きなプログラムからのコードの抜粋であり、コンテキスト内で実行する必要があります。次のコード例で、このアクションのコンテキストを確認できます。

- 基本を学ぶ

CLI

AWS CLI

OpsItem を更新するには

次の update-ops-item の例は、OpsItem の記述、優先度、カテゴリを更新します。さらに、このコマンドは、この OpsItem が編集または変更されたときに通知が送信される SNS トピックを指定します。

```
aws ssm update-ops-item \
    --ops-item-id "oi-287b5EXAMPLE" \
    --description "Primary OpsItem for failover event 2020-01-01-fh398yf" \
    --priority 2 \
    --category "Security" \
    --notifications "Arn=arn:aws:sns:us-east-2:111222333444:my-us-east-2-topic"
```

出力:

```
This command produces no output.
```

詳細については、「AWS Systems Manager ユーザーガイド」の「OpsItems を管理する」を参照してください。

- API の詳細については、AWS CLI コマンドリファレンスの「UpdateOpsItem」を参照してください。

Java

SDK for Java 2.x

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
    /**
     * Resolves an AWS SSM OpsItem asynchronously.
     *
     * @param opsID The ID of the OpsItem to resolve.
     * <p>
     * This method initiates an asynchronous request to resolve an SSM OpsItem.
     * If an exception occurs, it handles the error appropriately.
     */
    public void resolveOpsItem(String opsID) {
        UpdateOpsItemRequest opsItemRequest = UpdateOpsItemRequest.builder()
                .opsItemId(opsID)
                .status(OpsItemStatus.RESOLVED)
                .build();

        CompletableFuture<Void> future = CompletableFuture.runAsync(() -> {
            getAsyncClient().updateOpsItem(opsItemRequest)
                    .thenAccept(response -> {
                        System.out.println("OpsItem resolved successfully.");
                    })
                    .exceptionally(ex -> {
                        throw new CompletionException(ex);
                    }).join();
        }).exceptionally(ex -> {
            Throwable cause = (ex instanceof CompletionException) ?
ex.getCause() : ex;
            if (cause instanceof SsmException) {
                throw new RuntimeException("SSM error: " + cause.getMessage(),
cause);
            } else {
                throw new RuntimeException("Unexpected error: " +
cause.getMessage(), cause);
            }
```

```
        });

        try {
            future.join();
        } catch (CompletionException ex) {
            throw ex.getCause() instanceof RuntimeException ? (RuntimeException)
 ex.getCause() : ex;
        }
    }
```

- API の詳細については、「AWS SDK for Java 2.xAPI リファレンス」の「UpdateOpsItem」を参照してください。

JavaScript

SDK for JavaScript (v3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
import { UpdateOpsItemCommand, SSMClient } from "@aws-sdk/client-ssm";
import { parseArgs } from "node:util";

/**
 * Update an SSM OpsItem.
 * @param {{ opsItemId: string, status?: OpsItemStatus }}
 */
export const main = async ({
  opsItemId,
  status = undefined, // The OpsItem status. Status can be Open, In Progress, or
 Resolved
}) => {
  const client = new SSMClient({});
  try {
    await client.send(
      new UpdateOpsItemCommand({
        OpsItemId: opsItemId,
```

```
        Status: status,
      }),
    );
    console.log("Ops item updated.");
    return { Success: true };
  } catch (caught) {
    if (
      caught instanceof Error &&
      caught.name === "OpsItemLimitExceededException"
    ) {
      console.warn(
        `Couldn't create ops item because you have exceeded your open OpsItem
 limit. ${caught.message}.`,
      );
    } else {
      throw caught;
    }
  }
};
```

- API の詳細については、「AWS SDK for JavaScriptAPI リファレンス」の「UpdateOpsItem」を参照してください。

Python

SDK for Python (Boto3)

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
class OpsItemWrapper:
    """Encapsulates AWS Systems Manager OpsItem actions."""

    def __init__(self, ssm_client):
        """
        :param ssm_client: A Boto3 Systems Manager client.
        """
```

```
        self.ssm_client = ssm_client
        self.id = None

    @classmethod
    def from_client(cls):
        """
        :return: A OpsItemWrapper instance.
        """
        ssm_client = boto3.client("ssm")
        return cls(ssm_client)


    def update(self, title=None, description=None, status=None):
        """
        Update an OpsItem.

        :param title: The new OpsItem title.
        :param description: The new OpsItem description.
        :param status: The new OpsItem status.
        :return:
        """
        args = dict(OpsItemId=self.id)
        if title is not None:
            args["Title"] = title
        if description is not None:
            args["Description"] = description
        if status is not None:
            args["Status"] = status
        try:
            self.ssm_client.update_ops_item(**args)
        except ClientError as err:
            logger.error(
                "Couldn't update ops item %s. Here's why: %s: %s",
                self.id,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
```

- API の詳細については、「AWS SDK for Python (Boto3) API リファレンス」の「UpdateOpsItem」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

CLI で **UpdatePatchBaseline** を使用する

次のサンプルコードは、UpdatePatchBaseline を使用する方法を説明しています。

CLI

AWS CLI

例 1: パッチベースラインを更新するには

次の update-patch-baseline の例では、指定された 2 つのパッチを拒否済み、1 つのパッチを承認済みとして、指定されたパッチベースラインに追加します。

```
aws ssm update-patch-baseline \
        --baseline-id "pb-0123456789abcdef0" \
        --rejected-patches "KB2032276" "MS10-048" \
        --approved-patches "KB2124261"
```

出力:

```
{
    "BaselineId": "pb-0123456789abcdef0",
    "Name": "WindowsPatching",
    "OperatingSystem": "WINDOWS",
    "GlobalFilters": {
        "PatchFilters": []
    },
    "ApprovalRules": {
        "PatchRules": [
            {
                "PatchFilterGroup": {
                    "PatchFilters": [
                        {
                            "Key": "PRODUCT",
                            "Values": [
                                "WindowsServer2016"
                            ]
                        }
```

```
                    ]
                },
                "ComplianceLevel": "CRITICAL",
                "ApproveAfterDays": 0,
                "EnableNonSecurity": false
            }
        ]
    },
    "ApprovedPatches": [
        "KB2124261"
    ],
    "ApprovedPatchesComplianceLevel": "UNSPECIFIED",
    "ApprovedPatchesEnableNonSecurity": false,
    "RejectedPatches": [
        "KB2032276",
        "MS10-048"
    ],
    "RejectedPatchesAction": "ALLOW_AS_DEPENDENCY",
    "CreatedDate": 1550244180.465,
    "ModifiedDate": 1550244180.465,
    "Description": "Patches for Windows Servers",
    "Sources": []
}
```

例 2: パッチベースラインの名前を変更するには

次の update-patch-baseline の例では、指定されたパッチベースラインの名前を変更します。

```
aws ssm update-patch-baseline \
    --baseline-id "pb-0713accee01234567" \
    --name "Windows-Server-2012-R2-Important-and-Critical-Security-Updates"
```

詳細については、「AWS Systems Manager ユーザーガイド」の「カスタムパッチベースラインの更新または削除 <https://docs.aws.amazon.com/systems-manager/latest/userguide/patch-baseline-update-or-delete.html>`__」を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「UpdatePatchBaseline」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: この例では、2 つのパッチを拒否済み、1 つのパッチを承認済みとして既存のパッチベースラインに追加します。

```
Update-SSMPatchBaseline -BaselineId "pb-03da896ca3b68b639" -RejectedPatch
 "KB2032276","MS10-048" -ApprovedPatch "KB2124261"
```

出力:

```
ApprovalRules   : Amazon.SimpleSystemsManagement.Model.PatchRuleGroup
ApprovedPatches : {KB2124261}
BaselineId      : pb-03da896ca3b68b639
CreatedDate     : 3/3/2017 5:02:19 PM
Description     : Baseline containing all updates approved for production systems
GlobalFilters   : Amazon.SimpleSystemsManagement.Model.PatchFilterGroup
ModifiedDate    : 3/3/2017 5:22:10 PM
Name            : Production-Baseline
RejectedPatches : {KB2032276, MS10-048}
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet リファレンス (V4)」の「UpdatePatchBaseline」を参照してください。

AWS SDK デベロッパーガイドとコード例の詳細なリストについては、「このサービスを AWS SDK で使用する」を参照してください。このトピックには、使用開始方法に関する情報と、以前の SDK バージョンの詳細も含まれています。

AWS Systems Manager でのログ記録とモニタリング

モニタリングは、AWS Systems Manager と AWS ソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。マルチポイント障害が発生した場合は、その障害をデバッグできるように、AWS ソリューションのすべての部分からモニタリングデータを収集する必要があります。ただし、Systems Manager のモニタリングを開始する前に、以下の質問に対する回答を反映したモニタリング計画を作成する必要があります。

- どのような目的でモニタリングしますか?
- どのリソースをモニタリングしますか?
- どのくらいの頻度でこれらのリソースをモニタリングしますか?
- 使用するモニタリングツールは?
- 誰がモニタリングタスクを実行しますか?
- 問題が発生したときに誰が通知を受け取りますか?

モニタリングの目的を定義し、モニタリングの計画を作成したら、次のステップとして、お客様の環境内で通常の Systems Manager パフォーマンスのベースラインを確立します。さまざまな時間帯に、さまざまな負荷条件で Systems Manager パフォーマンスを測定します。Systems Manager をモニタリングしながら、収集したモニタリングデータの履歴を保存する必要があります。現在の Systems Manager パフォーマンスをこの履歴データと比較して、通常のパフォーマンスパターンとパフォーマンス異常を識別することで、異常への対処方法を作成することが容易になります。

たとえば、オートメーションワークフロー、パッチベースラインの適用、メンテナンスウィンドウイベント、および設定のコンプライアンスなどのオペレーションの成功または失敗をモニタリングできます。Automation は AWS Systems Manager のツールです。

マネージドノードの CPU 使用率、ディスク I/O、およびネットワーク使用率をモニタリングすることもできます。確立したベースラインからパフォーマンスが外れた場合は、ノードの再設定または最適化を行って CPU 使用率の抑制、ディスク I/O の改善、またはネットワークトラフィックの低減を行うことが必要な場合があります。EC2 インスタンスのモニタリングの詳細については、「Amazon EC2 ユーザーガイド」の「Amazon EC2 のモニタリング」を参照してください。

トピック

- モニタリングツール
- 統合された CloudWatch Logs へのノードログの送信 (CloudWatch エージェント)

- CloudWatch Logs に SSM Agent ログを送信する
- 変更リクエストイベントのモニタリング
- オートメーションのモニタリング
- Amazon CloudWatch を使用した Run Command メトリクスのモニタリング
- AWS Systems Manager による AWS CloudTrail API コールのログ記録
- CloudWatch Logs を使用した自動アクション出力のログ記録
- Run Command の Amazon CloudWatch Logs の設定
- Amazon EventBridge を使用して Systems Manager イベントをモニタリングする
- Amazon SNS 通知を使用した Systems Manager のステータス変更のモニタリング

モニタリングツール

この章のコンテンツでは、Systems Manager と他の AWS リソースのモニタリングに使用できるツールの使用方法について説明します。ツールの詳細なリストについては、「AWS Systems Manager でのログ記録とモニタリング」を参照してください。

統合された CloudWatch Logs へのノードログの送信 (CloudWatch エージェント)

ノードのメトリクスとログを収集するには、AWS Systems Manager エージェント (SSM Agent) を使用する代わりに、Amazon CloudWatch を設定して使用できます。SSM Agent よりも CloudWatch エージェント を使用したほうが、EC2 インスタンスのメトリクスを多く収集できます。また、CloudWatch エージェント を使用すると、オンプレミスのサーバーからもメトリクスを収集できます。

エージェントの構成設定を Systems Manager Parameter Store に保存し、CloudWatch エージェントで使用することもできます。Parameter Store は AWS Systems Manager のツールです。

> **Note**
>
> AWS Systems Manager は SSM Agent から統合された CloudWatch エージェントへの移行をサポートし、64 ビットバージョンの Windows でのみログとメトリクスを収集します。他のオペレーティングシステムで統合された CloudWatch エージェントをセットアップする方法と、CloudWatch エージェントの使用方法の詳細については、「Amazon CloudWatch ユー

ザーガイド」の「CloudWatch エージェントを使用して Amazon EC2 インスタンスとオンプレミスサーバーからメトリクスを収集する」を参照してください。
CloudWatch エージェントは、サポートされている他のオペレーティングシステムでも使用できますが、Systems Manager を使用してツールの移行を実行することはできません。

SSM Agent は実行、スケジュールされたアクション、エラー、ヘルスステータスに関連した情報をまとめて各ノードのログファイルに書き込みます。ノードに手動で接続してログファイルを表示し、SSM Agent を使用してトラブルシューティングを行うと、時間がかかります。ノードを効率的にモニタリングするには、このログデータを Amazon CloudWatch Logs に送信するように SSM Agent 自体または Amazon CloudWatch エージェントを設定できます。

Important

CloudWatch の統合エージェントによって、ログデータを Amazon CloudWatch Logs に送信するためのツールとして SSM Agent が置き換えられました。SSM Agent aws:cloudWatch プラグインはサポートされていません。ログ収集プロセスには、統合された CloudWatch エージェントのみを使用することをお勧めします。詳細については、以下の各トピックを参照してください。

- 統合された CloudWatch Logs へのノードログの送信 (CloudWatch エージェント)
- Windows Server ノードのログ収集を CloudWatch エージェントに移行する
- 「Amazon CloudWatch ユーザーガイド」の「CloudWatch エージェントを使用してメトリクス、ログ、トレースを収集する」。

CloudWatch Logs を使用すると、ログデータのリアルタイムのモニタリング、1 つ以上のメトリクスフィルターを作成してのログデータの検索とフィルター、および必要に応じた履歴データのアーカイブと取得を行うことができます。CloudWatch Logs の詳細については、「Amazon CloudWatch Logs ユーザーガイド」を参照してください。

ログデータを Amazon CloudWatch Logs に送信するようにエージェントを設定すると、以下の利点があります。

- あらゆる SSM Agent ログファイルを集中管理するログファイルストレージ。
- エラーを調査するためのファイルへの迅速なアクセス。
- ログファイルの無制限の保持 (設定可能)。

- ログは、ノードのステータスに関係なく維持し、アクセスできます。
- メトリクスやアラームなど、CloudWatch の他の機能へのアクセス。

Session Manager アクティビティのモニタリングについては、「セッションアクティビティのログ記録」 および セッションロギングの有効化と無効化 を参照してください。

Windows Server ノードのログ収集を CloudWatch エージェントに移行する

サポートされている Windows Server ノードで SSM Agent を使用して SSM Agent ログファイルを Amazon CloudWatch Logs に送信している場合、Systems Manager を使用して SSM Agent から CloudWatch エージェントへログ収集ツールとして移行し、構成設定も移行できます。

CloudWatch エージェントは、32 ビットバージョンの Windows Server ではサポートされていません。

64 ビットの Windows Server の EC2 インスタンスの場合、CloudWatch エージェントへの移行は自動または手動で実行できます。オンプレミスサーバーと仮想マシンの場合、プロセスは手動で実行する必要があります。

> **Note**
>
> 移行プロセス中に、CloudWatch へのデータ送信が中断または重複する場合があります。メトリクスとログデータは、移行の完了後に、再度 CloudWatch に正確に記録されます。

一部のノードで移行をテストしてから、フリート全体を CloudWatch エージェント に移行することをお勧めします。必要に応じて、移行後に再度 SSM Agent に戻してログ収集を行うことができます。

> **Important**
>
> 以下の場合、このトピックで説明している手順を使用して CloudWatch エージェントに移行することはできません。
>
> - SSM Agent の既存の設定で、複数のリージョンを指定している場合。
> - SSM Agent の既存の設定で、複数のアクセス/シークレットキー認証情報のセットを指定している場合。

上記の場合は、SSM Agent でのログ収集を無効にし、移行プロセスを使わずに CloudWatch エージェントをインストールする必要があります。詳細については、「Amazon CloudWatch ユーザーガイド」の次のトピックを参照してください。

- CloudWatch エージェントのインストール
- オンプレミスサーバーへの CloudWatch エージェントのインストール

[開始する前に]

CloudWatch エージェントに移行してログ収集を開始する前に、移行を実行するノードが以下の要件を満たしていることを確認します。

- OS が 64 ビットバージョンの Windows Server である。
- SSM Agent 2.2.93.0 以降がノードにインストールされている。
- ノードでモニタリングするように SSM Agent が設定されている。

トピック

- CloudWatch エージェントへの自動移行
- CloudWatch エージェントへの手動での移行

CloudWatch エージェントへの自動移行

Windows Server の EC2 インスタンスに限り、AWS Systems Manager コンソール、または AWS Command Line Interface (AWS CLI) を使用して、ログ収集ツールとして CloudWatch エージェントに移行します。

> **Note**
>
> AWS Systems Manager は SSM Agent から統合された CloudWatch エージェントへの移行をサポートし、64 ビットバージョンの Windows でのみログとメトリクスを収集します。他のオペレーティングシステムで統合された CloudWatch エージェントをセットアップする方法と、CloudWatch エージェントの使用方法の詳細については、「Amazon CloudWatch ユーザーガイド」の「CloudWatch エージェントを使用して Amazon EC2 インスタンスとオンプレミスサーバーからメトリクスを収集する」を参照してください。

CloudWatch エージェントは、サポートされている他のオペレーティングシステムでも使用できますが、Systems Manager を使用してツールの移行を実行することはできません。

移行が成功したら、CloudWatch で結果をチェックし、必要なメトリクス、ログ、または Windows イベントログが収集されていることを確認します。結果に満足したら、オプションとして CloudWatch エージェントの設定を Parameter Store に保存する することができます。移行が失敗した場合や、結果が不満足なものである場合は、SSM Agent でのログ収集へのロールバック をすることができます。

Note

{hostname} エントリが含まれているソース設定ファイルを移行する場合、移行が完了した後で {hostname} エントリがフィールドの値を変更できることに注意してください。たとえば、次の "LogStream": "{hostname}" エントリが MyLogServer001 という名前のサーバーにマッピングされているとします。

```
{
"Id": "CloudWatchIISLogs",
"FullName":
 "AWS.EC2.Windows.CloudWatch.CloudWatchLogsOutput,AWS.EC2.Windows.CloudWatch",
"Parameters": {
"AccessKey": "",
"SecretKey": "",
"Region": "us-east-1",
"LogGroup": "Production-Windows-IIS",
"LogStream": "{hostname}"
     }
}
```

移行後、このエントリは ip-11-1-1-11.production などのドメインにマップされます。ExampleCompany.com。ローカルホスト名の値を保持するには、{local_hostname} ではなく {hostname} を指定します。

CloudWatch エージェントに自動的に移行するには (コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。

2. ナビゲーションペインで、[Run Command] を選択し、次に [Run command (コマンドの実行)] を選択します。
3. [コマンドのドキュメント] リストで、`AmazonCloudWatch-MigrateCloudWatchAgent[]` を選択します。
4. [Status] で、[Enabled] を選択します。
5. [ターゲット] セクションで、タグの指定、インスタンスやエッジデバイスの手動選択、リソースグループの指定により、このオペレーションを実行するマネージドノードを選択します。

> **Tip**
>
> 表示されるはずのマネージドノードが表示されない場合は、トラブルシューティングのヒントについて「マネージドノードの可用性のトラブルシューティング」を参照してください。

6. [レート制御] の場合:
   - [同時実行数] の場合、コマンドを同時に実行するマネージドノードの数または割合を指定します。

     > **Note**
     >
     > マネージドノードに適用されるタグを指定するか、AWS リソースグループを指定してターゲットを選択し、ターゲットとなるマネージドノードの数が不明な場合は、割合を指定してドキュメントを同時に実行できるターゲットの数を制限します。

   - [エラーのしきい値] で、ノードの数または割合のいずれかで失敗した後、他のマネージドノードでのコマンドの実行をいつ停止するか指定します。例えば、3 つのエラーを指定した場合、4 番目のエラーが受信されると、システムマネージャー はコマンドの送信を停止します。コマンドを処理しているマネージドノードもエラーを送信する可能性があります。
7. (オプション) コマンド出力をファイルに保存する場合は、[出力オプション] の [S3 バケットにコマンド出力を書き込む] ボックスを選択します。ボックスにバケット名とプレフィックス (フォルダ) 名を入力します。

> **Note**
>
> S3 バケットにデータを書き込む機能を許可する S3 許可は、このタスクを実行する IAM ユーザーのものではなく、インスタンスに割り当てられたインスタンスプロファイル

(EC2 インスタンスの場合) または IAM サービスロール (ハイブリッドアクティベーションマシン) のものです。詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」または「ハイブリッド環境に IAM サービスロールを作成する」を参照してください。さらに、指定された S3 バケットが別の AWS アカウント にある場合は、マネージドノードに関連付けられたインスタンスプロファイルまたは IAM サービスロールが、そのバケットへの書き込みに必要なアクセス許可があることを確認してください。

8. [SNS Notifications (SNS 通知)] セクションで、コマンドの実行状態に関する通知を受け取る場合は、[Enable SNS notifications (SNS 通知を有効にする)] チェックボックスをオンにします。

   Run Command 用の Amazon SNS 通知の設定の詳細については、「Amazon SNS 通知を使用した Systems Manager のステータス変更のモニタリング」を参照してください。

9. [Run (実行)] を選択します。

CloudWatch エージェントに自動的に移行するには (AWS CLI)

- 以下のコマンドを実行してください。

```
aws ssm send-command --document-name AmazonCloudWatch-MigrateCloudWatchAgent --
targets Key=instanceids,Values=ID1,ID2,ID3
```

ID1、*ID2*、*ID3* は、更新するノードの ID (i-02573cafcfEXAMPLE など) です。

CloudWatch エージェントへの手動での移行

オンプレミスの Windows Server ノード、または Windows Server の EC2 インスタンスの場合は、以下のステップに従って、ログ収集を Amazon CloudWatch エージェントに手動で移行します。

> **Note**
>
> {hostname} エントリが含まれているソース設定ファイルを移行する場合、移行が完了した後で {hostname} エントリがフィールドの値を変更できることに注意してください。たとえば、次の "LogStream": "{hostname}" エントリが MyLogServer001 という名前のサーバーにマッピングされているとします。

```
{
"Id": "CloudWatchIISLogs",
```

```
"FullName":
 "AWS.EC2.Windows.CloudWatch.CloudWatchLogsOutput,AWS.EC2.Windows.CloudWatch",
"Parameters": {
"AccessKey": "",
"SecretKey": "",
"Region": "us-east-1",
"LogGroup": "Production-Windows-IIS",
"LogStream": "{hostname}"
     }
}
```

移行後、このエントリは ip-11-1-1-11.production.ExampleCompany.com などのドメインにマップされます。ローカルホスト名の値を保持するには、`{local_hostname}` ではなく `{hostname}` を指定します。

ステップ 1: CloudWatch エージェントをインストールするには (コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Run Command] を選択し、次に [Run command (コマンドの実行)] を選択します。
3. [コマンドのドキュメント] リストで、`AWS-ConfigureAWSPackage[]` を選択します。
4. [Action] (アクション) で、`Install` を選択します。
5. [名前] に**`AmazonCloudWatchAgent`**と入力してください。
6. [Version] (バージョン) には **`latest`** を入力します (デフォルトで提供されていない場合)。
7. [ターゲット] セクションで、タグの指定、インスタンスやエッジデバイスの手動選択、リソースグループの指定により、このオペレーションを実行するマネージドノードを選択します。

   > **Tip**
   >
   > 表示されるはずのマネージドノードが表示されない場合は、トラブルシューティングのヒントについて「マネージドノードの可用性のトラブルシューティング」を参照してください。

8. [レート制御] の場合:

- [同時実行数] の場合、コマンドを同時に実行するマネージドノードの数または割合を指定します。

> **Note**
>
> マネージドノードに適用されるタグを指定するか、AWS リソースグループを指定してターゲットを選択し、ターゲットとなるマネージドノードの数が不明な場合は、割合を指定してドキュメントを同時に実行できるターゲットの数を制限します。

- [エラーのしきい値] で、ノードの数または割合のいずれかで失敗した後、他のマネージドノードでのコマンドの実行をいつ停止するか指定します。例えば、3 つのエラーを指定した場合、4 番目のエラーが受信されると、システムマネージャー はコマンドの送信を停止します。コマンドを処理しているマネージドノードもエラーを送信する可能性があります。

9. (オプション) コマンド出力をファイルに保存する場合は、[出力オプション] の [S3 バケットにコマンド出力を書き込む] ボックスを選択します。ボックスにバケット名とプレフィックス (フォルダ) 名を入力します。

> **Note**
>
> S3 バケットにデータを書き込む機能を許可する S3 許可は、このタスクを実行する IAM ユーザーのものではなく、インスタンスに割り当てられたインスタンスプロファイル (EC2 インスタンスの場合) または IAM サービスロール (ハイブリッドアクティベーションマシン) のものです。詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」または「ハイブリッド環境に IAM サービスロールを作成する」を参照してください。さらに、指定された S3 バケットが別の AWS アカウント にある場合は、マネージドノードに関連付けられたインスタンスプロファイルまたは IAM サービスロールが、そのバケットへの書き込みに必要なアクセス許可があることを確認してください。

10. [SNS Notifications (SNS 通知)] セクションで、コマンドの実行状態に関する通知を受け取る場合は、[Enable SNS notifications (SNS 通知を有効にする)] チェックボックスをオンにします。

    Run Command 用の Amazon SNS 通知の設定の詳細については、「Amazon SNS 通知を使用した Systems Manager のステータス変更のモニタリング」を参照してください。

11. [Run (実行)] を選択します。

ステップ 2: 設定データの JSON 形式を更新するには

- CloudWatch エージェントの既存の Config 設定の JSON 形式を更新するには、AWS Systems Manager のツールである Run Command を使用するか、RDP 接続で直接ノードにログインして以下の Windows PowerShell コマンドを 1 回に 1 つずつノードで実行します。

```
cd ${Env:ProgramFiles}\\Amazon\\AmazonCloudWatchAgent
```

```
.\\amazon-cloudwatch-agent-config-wizard.exe --isNonInteractiveWindowsMigration
```

{Env:ProgramFiles} は、ACloudWatch エージェントが含まれている Amazon ディレクトリの場所 (通常は `C:\Program Files`) を表します。

ステップ 3: CloudWatch エージェントを設定して開始するには (コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Run Command] を選択し、次に [Run command (コマンドの実行)] を選択します。
3. [コマンドのドキュメント] リストで、`AWS-RunPowerShellScript[]` を選択します。
4. [Commands] (コマンド) に、以下の 2 つのコマンドを入力します。

```
cd ${Env:ProgramFiles}\Amazon\AmazonCloudWatchAgent
```

```
.\amazon-cloudwatch-agent-ctl.ps1 -a fetch-config -m ec2 -c file:config.json -s
```

{Env:ProgramFiles} は、ACloudWatch エージェントが含まれている Amazon ディレクトリの場所 (通常は `C:\Program Files`) を表します。

5. [ターゲット] セクションで、タグの指定、インスタンスやエッジデバイスの手動選択、リソースグループの指定により、このオペレーションを実行するマネージドノードを選択します。

> **Tip**
>
> 表示されるはずのマネージドノードが表示されない場合は、トラブルシューティングのヒントについて「マネージドノードの可用性のトラブルシューティング」を参照してください。

6. [レート制御] の場合:

   - [同時実行数] の場合、コマンドを同時に実行するマネージドノードの数または割合を指定します。

     > **Note**
     >
     > マネージドノードに適用されるタグを指定するか、AWS リソースグループを指定してターゲットを選択し、ターゲットとなるマネージドノードの数が不明な場合は、割合を指定してドキュメントを同時に実行できるターゲットの数を制限します。

   - [エラーのしきい値] で、ノードの数または割合のいずれかで失敗した後、他のマネージドノードでのコマンドの実行をいつ停止するか指定します。例えば、3 つのエラーを指定した場合、4 番目のエラーが受信されると、システムマネージャー はコマンドの送信を停止します。コマンドを処理しているマネージドノードもエラーを送信する可能性があります。

7. (オプション) コマンド出力をファイルに保存する場合は、[出力オプション] の [S3 バケットにコマンド出力を書き込む] ボックスを選択します。ボックスにバケット名とプレフィックス (フォルダ) 名を入力します。

   > **Note**
   >
   > S3 バケットにデータを書き込む機能を許可する S3 許可は、このタスクを実行する IAM ユーザーのものではなく、インスタンスに割り当てられたインスタンスプロファイル (EC2 インスタンスの場合) または IAM サービスロール (ハイブリッドアクティベーションマシン) のものです。詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」または「ハイブリッド環境に IAM サービスロールを作成する」を参照してください。さらに、指定された S3 バケットが別の AWS アカウント にある場合は、マネージドノードに関連付けられたインスタンスプロファイルまたは IAM サービスロールが、そのバケットへの書き込みに必要なアクセス許可があることを確認してください。

8. [SNS Notifications (SNS 通知)] セクションで、コマンドの実行状態に関する通知を受け取る場合は、[Enable SNS notifications (SNS 通知を有効にする)] チェックボックスをオンにします。

   Run Command 用の Amazon SNS 通知の設定の詳細については、「Amazon SNS 通知を使用した Systems Manager のステータス変更のモニタリング」を参照してください。

9. [Run (実行)] を選択します。

4：SSM Agent でログ収集を無効にするには (コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Run Command] を選択し、次に [Run command (コマンドの実行)] を選択します。
3. [コマンドのドキュメント] リストで、`AWS-ConfigureCloudWatch`[] を選択します。
4. [Status] (ステータス) で、[Disabled] (無効) を選択します。
5. [ターゲット] セクションで、タグの指定、インスタンスやエッジデバイスの手動選択、リソースグループの指定により、このオペレーションを実行するマネージドノードを選択します。

   > **Tip**
   >
   > 表示されるはずのマネージドノードが表示されない場合は、トラブルシューティングのヒントについて「マネージドノードの可用性のトラブルシューティング」を参照してください。

6. [Status] (ステータス) で、`Disabled` を選択します。
7. [レート制御] の場合:

   - [同時実行数] の場合、コマンドを同時に実行するマネージドノードの数または割合を指定します。

     > **Note**
     >
     > マネージドノードに適用されるタグを指定するか、AWS リソースグループを指定してターゲットを選択し、ターゲットとなるマネージドノードの数が不明な場合は、割合を指定してドキュメントを同時に実行できるターゲットの数を制限します。

- [エラーのしきい値] で、ノードの数または割合のいずれかで失敗した後、他のマネージドノードでのコマンドの実行をいつ停止するか指定します。例えば、3 つのエラーを指定した場合、4 番目のエラーが受信されると、システムマネージャー はコマンドの送信を停止します。コマンドを処理しているマネージドノードもエラーを送信する可能性があります。

8. (オプション) コマンド出力をファイルに保存する場合は、[出力オプション] の [S3 バケットにコマンド出力を書き込む] ボックスを選択します。ボックスにバケット名とプレフィックス (フォルダ) 名を入力します。

> **Note**
>
> S3 バケットにデータを書き込む機能を許可する S3 許可は、このタスクを実行する IAM ユーザーのものではなく、インスタンスに割り当てられたインスタンスプロファイル (EC2 インスタンスの場合) または IAM サービスロール (ハイブリッドアクティベーションマシン) のものです。詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」または「ハイブリッド環境に IAM サービスロールを作成する」を参照してください。さらに、指定された S3 バケットが別の AWS アカウント にある場合は、マネージドノードに関連付けられたインスタンスプロファイルまたは IAM サービスロールが、そのバケットへの書き込みに必要なアクセス許可があることを確認してください。

9. [SNS Notifications (SNS 通知)] セクションで、コマンドの実行状態に関する通知を受け取る場合は、[Enable SNS notifications (SNS 通知を有効にする)] チェックボックスをオンにします。

   Run Command 用の Amazon SNS 通知の設定の詳細については、「Amazon SNS 通知を使用した Systems Manager のステータス変更のモニタリング」を参照してください。

10. [Run (実行)] を選択します。

    以上の手順を完了したら、CloudWatch で結果をチェックし、必要なメトリクス、ログ、または Windows イベントログが収集されていることを検証します。結果に満足したら、オプションとして CloudWatch エージェントの設定を Parameter Store に保存する することができます。移行が失敗した場合や、結果が不満足なものである場合は、SSM Agent での口グ収集へのロールバック をすることができます。

CloudWatch エージェントの設定を Parameter Store に保存する

CloudWatch エージェントの設定ファイルの内容は、Parameter Store に保存できます。この設定データをパラメータに保持すると、その構成設定を複数のノードで継承できるため、構成ファイルの

作成や手動の更新をノードで行う必要がなくなります。例えば、Run Command を使用してパラメータの内容を複数のノードの設定ファイルに書き込んだり、AWS Systems Manager のツールである State Manager を使用してノードのフリート全体で CloudWatch エージェントの構成の設定ドリフトを回避したりできます。

CloudWatch エージェント設定ウィザードを実行すると、このウィザードで構成設定を新しいパラメータとして Parameter Store に保存できます。CloudWatch エージェント設定ウィザード実行の詳細については、「Amazon CloudWatch ユーザーガイド」の「ウィザードを使用して CloudWatch エージェント設定ファイルを作成する」を参照してください。

ウィザードを実行しても、設定をパラメータとして保存するオプションを選択しなかった場合や、CloudWatch エージェント設定ファイルを手動で作成した場合は、ノードでデータを取得してパラメータとして次のファイルに保存できます。

```
${Env:ProgramFiles}\Amazon\AmazonCloudWatchAgent\config.json
```

{Env:ProgramFiles} は、ACloudWatch エージェントが含まれている Amazon ディレクトリの場所 (通常は `C:\Program Files`) を表します。

このファイルの JSON のバックアップを作成し、ノード自体とは異なる場所に保持することをお勧めします。

パラメータの作成方法については、「Systems Manager での Parameter Store パラメータの作成」を参照してください。

CloudWatch エージェントの詳細については、Amazon CloudWatch ユーザーガイドの「CloudWatch エージェントを使用した Amazon EC2 インスタンスとオンプレミスサーバーからのメトリクスとログの収集」を参照してください。

SSM Agent でのログ収集へのロールバック

ログ収集に再び SSM Agent を使用する場合は、以下の手順に従います。

ステップ 1: SSM Agent から設定データを取得するには

1. ログ収集に再び SSM Agent を使用するノードで、SSM Agent 設定ファイルの内容を見つけます。通常、この JSON ファイルは次の場所にあります。

   ```
   ${Env:ProgramFiles}\\Amazon\\SSM\\Plugins\\awsCloudWatch\
   \AWS.EC2.Windows.CloudWatch.json
   ```

{Env:ProgramFiles} は、Amazon ディレクトリがある場所 (通常は C:\Program Files) を表します。

2. このデータをテキストファイルにコピーし、後のステップで使用します。

   JSON のバックアップは、ノード自体とは異なる場所に保存することをお勧めします。

2: CloudWatch エージェントをアンインストールするには (コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Run Command] を選択し、次に [Run command (コマンドの実行)] を選択します。
3. [コマンドのドキュメント] リストで、AWS-ConfigureAWSPackage[] を選択します。
4. [Action] (アクション) で、[Uninstall] (アンインストール) を選択します。
5. [名前] に**AmazonCloudWatchAgent**と入力してください。
6. [ターゲット] セクションで、タグの指定、インスタンスやエッジデバイスの手動選択、リソースグループの指定により、このオペレーションを実行するマネージドノードを選択します。

   > **Tip**
   >
   > 表示されるはずのマネージドノードが表示されない場合は、トラブルシューティングのヒントについて「マネージドノードの可用性のトラブルシューティング」を参照してください。

7. [レート制御] の場合:

   - [同時実行数] の場合、コマンドを同時に実行するマネージドノードの数または割合を指定します。

     > **Note**
     >
     > マネージドノードに適用されるタグを指定するか、AWS リソースグループを指定してターゲットを選択し、ターゲットとなるマネージドノードの数が不明な場合は、割合を指定してドキュメントを同時に実行できるターゲットの数を制限します。

- [エラーのしきい値] で、ノードの数または割合のいずれかで失敗した後、他のマネージドノードでのコマンドの実行をいつ停止するか指定します。例えば、3 つのエラーを指定した場合、4 番目のエラーが受信されると、システムマネージャー はコマンドの送信を停止します。コマンドを処理しているマネージドノードもエラーを送信する可能性があります。

8. (オプション) コマンド出力をファイルに保存する場合は、[出力オプション] の [S3 バケットにコマンド出力を書き込む] ボックスを選択します。ボックスにバケット名とプレフィックス (フォルダ) 名を入力します。

> **Note**
>
> S3 バケットにデータを書き込む機能を許可する S3 許可は、このタスクを実行する IAM ユーザーのものではなく、インスタンスに割り当てられたインスタンスプロファイル (EC2 インスタンスの場合) または IAM サービスロール (ハイブリッドアクティベーションマシン) のものです。詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」または「ハイブリッド環境に IAM サービスロールを作成する」を参照してください。さらに、指定された S3 バケットが別の AWS アカウント にある場合は、マネージドノードに関連付けられたインスタンスプロファイルまたは IAM サービスロールが、そのバケットへの書き込みに必要なアクセス許可があることを確認してください。

9. [SNS Notifications (SNS 通知)] セクションで、コマンドの実行状態に関する通知を受け取る場合は、[Enable SNS notifications (SNS 通知を有効にする)] チェックボックスをオンにします。

   Run Command 用の Amazon SNS 通知の設定の詳細については、「Amazon SNS 通知を使用した Systems Manager のステータス変更のモニタリング」を参照してください。

10. [Run (実行)] を選択します。

3：SSM Agent でログ収集を有効に戻すには (コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Run Command] を選択し、次に [Run command (コマンドの実行)] を選択します。
3. [コマンドのドキュメント] リストで、`AWS-ConfigureCloudWatch`[] を選択します。
4. [Status] (ステータス) で、`Enabled` を選択します。

5. [Properties] (プロパティ) に、テキストファイルとして保存してある、古い設定データの内容を貼り付けます。
6. [ターゲット] セクションで、タグの指定、インスタンスやエッジデバイスの手動選択、リソースグループの指定により、このオペレーションを実行するマネージドノードを選択します。

> **Tip**
>
> 表示されるはずのマネージドノードが表示されない場合は、トラブルシューティングのヒントについて「マネージドノードの可用性のトラブルシューティング」を参照してください。

7. [レート制御] の場合:

   - [同時実行数] の場合、コマンドを同時に実行するマネージドノードの数または割合を指定します。

   > **Note**
   >
   > マネージドノードに適用されるタグを指定するか、AWS リソースグループを指定してターゲットを選択し、ターゲットとなるマネージドノードの数が不明な場合は、割合を指定してドキュメントを同時に実行できるターゲットの数を制限します。

   - [エラーのしきい値] で、ノードの数または割合のいずれかで失敗した後、他のマネージドノードでのコマンドの実行をいつ停止するか指定します。例えば、3 つのエラーを指定した場合、4 番目のエラーが受信されると、システムマネージャー はコマンドの送信を停止します。コマンドを処理しているマネージドノードもエラーを送信する可能性があります。
8. (オプション) コマンド出力をファイルに保存する場合は、[出力オプション] の [S3 バケットにコマンド出力を書き込む] ボックスを選択します。ボックスにバケット名とプレフィックス (フォルダ) 名を入力します。

> **Note**
>
> S3 バケットにデータを書き込む機能を許可する S3 許可は、このタスクを実行する IAM ユーザーのものではなく、インスタンスに割り当てられたインスタンスプロファイル (EC2 インスタンスの場合) または IAM サービスロール (ハイブリッドアクティベーションマシン) のものです。詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」または「ハイブリッド環境に IAM サービスロールを作成する」を参照してください。さらに、指定された S3 バケットが別の AWS アカウント に

ある場合は、マネージドノードに関連付けられたインスタンスプロファイルまたは IAM サービスロールが、そのバケットへの書き込みに必要なアクセス許可があることを確認してください。

9. [SNS Notifications (SNS 通知)] セクションで、コマンドの実行状態に関する通知を受け取る場合は、[Enable SNS notifications (SNS 通知を有効にする)] チェックボックスをオンにします。

   Run Command 用の Amazon SNS 通知の設定の詳細については、「Amazon SNS 通知を使用した Systems Manager のステータス変更のモニタリング」を参照してください。

10. [Run (実行)] を選択します。

CloudWatch Logs に SSM Agent ログを送信する

AWS Systems Manager エージェント (SSM Agent) は、Systems Manager 用に設定された EC2 インスタンス、エッジデバイス、オンプレミスサーバー、および仮想マシン (VM) で動作する Amazon ソフトウェアです。SSM Agent は、クラウド内の Systems Manager サービスからのリクエストを処理し、リクエストに指定されているとおりにマシンを設定します。SSM Agent の詳細については、「「SSM Agent」 の使用」を参照してください。

また、以下のステップを使用して、ログデータを Amazon CloudWatch Logs に送信するように SSM Agent を設定できます。

開始する前に

CloudWatch Logs にロググループを作成します。詳細については、「Amazon CloudWatch Logs ユーザーガイド」の「CloudWatch Logs の開始方法」を参照してください。

CloudWatch にログを送信するように SSM Agent を設定するには

1. ノードにログインして、次のファイルを見つけます。

   Linux

   ほとんどの Linux のノードタイプ:`/etc/amazon/ssm/seelog.xml.template`。

   Ubuntu Server 20.10 STR & 20.04、18.04、および 16.04 LTS: `/snap/amazon-ssm-agent/current/seelog.xml.template`

   macOS

```
/opt/aws/ssm/seelog.xml.template
```

Windows

```
%ProgramFiles%\Amazon\SSM\seelog.xml.template
```

2. ファイル名を `seelog.xml.template` から `seelog.xml` に変更します。

> **Note**
>
> Ubuntu Server 20.10 STR & 20.04、18.04、および 16.04 LTS では、`seelog.xml` ファイルは `/etc/amazon/ssm/` ディレクトリに作成する必要があります。次の 3 つのコマンドを実行して、このディレクトリとファイルを作成できます。
>
> ```
> sudo mkdir -p /etc/amazon/ssm
> ```
>
> ```
> sudo cp -pr /snap/amazon-ssm-agent/current/* /etc/amazon/ssm
> ```
>
> ```
> sudo cp -p /etc/amazon/ssm/seelog.xml.template /etc/amazon/ssm/seelog.xml
> ```

3. テキストエディタで `seelog.xml` ファイルを開き、次のセクションを見つけます。

Linux and macOS

```
<outputs formatid="fmtinfo">
   <console formatid="fmtinfo"/>
   <rollingfile type="size" filename="/var/log/amazon/ssm/amazon-ssm-agent.log"
 maxsize="30000000" maxrolls="5"/>
   <filter levels="error,critical" formatid="fmterror">
      <rollingfile type="size" filename="/var/log/amazon/ssm/errors.log"
 maxsize="10000000" maxrolls="5"/>
   </filter>
</outputs>
```

Windows

```
<outputs formatid="fmtinfo">
   <console formatid="fmtinfo"/>
```

```
   <rollingfile type="size" maxrolls="5" maxsize="30000000"
 filename="{{LOCALAPPDATA}}\Amazon\SSM\Logs\amazon-ssm-agent.log"/>
   <filter formatid="fmterror" levels="error,critical">
      <rollingfile type="size" maxrolls="5" maxsize="10000000"
 filename="{{LOCALAPPDATA}}\Amazon\SSM\Logs\errors.log"/>
   </filter>
</outputs>
```

4. ファイルを編集し、closing </filter> タグの後にカスタム名要素を追加します 。次の例では、カスタム名は `cloudwatch_receiver` として指定されています。

   Linux and macOS

```
<outputs formatid="fmtinfo">
   <console formatid="fmtinfo"/>
   <rollingfile type="size" filename="/var/log/amazon/ssm/amazon-ssm-agent.log"
 maxsize="30000000" maxrolls="5"/>
   <filter levels="error,critical" formatid="fmterror">
      <rollingfile type="size" filename="/var/log/amazon/ssm/errors.log"
 maxsize="10000000" maxrolls="5"/>
   </filter>
   <custom name="cloudwatch_receiver" formatid="fmtdebug" data-log-group="your-
CloudWatch-log-group-name"/>
</outputs>
```

   Windows

```
<outputs formatid="fmtinfo">
   <console formatid="fmtinfo"/>
   <rollingfile type="size" maxrolls="5" maxsize="30000000"
 filename="{{LOCALAPPDATA}}\Amazon\SSM\Logs\amazon-ssm-agent.log"/>
   <filter formatid="fmterror" levels="error,critical">
      <rollingfile type="size" maxrolls="5" maxsize="10000000"
 filename="{{LOCALAPPDATA}}\Amazon\SSM\Logs\errors.log"/>
   </filter>
   <custom name="cloudwatch_receiver" formatid="fmtdebug" data-log-group="your-
CloudWatch-log-group-name"/>
</outputs>
```

5. 変更を保存して、SSM Agent またはノードを再起動します。
6. CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) を開きます。
7. ナビゲーションペインで [ロググループ] を選択し、ロググループの名前を選択します。

> **Tip**
>
> SSM Agent のログファイルデータのログストリームは、ノード ID に基づいて編成されています。

変更リクエストイベントのモニタリング

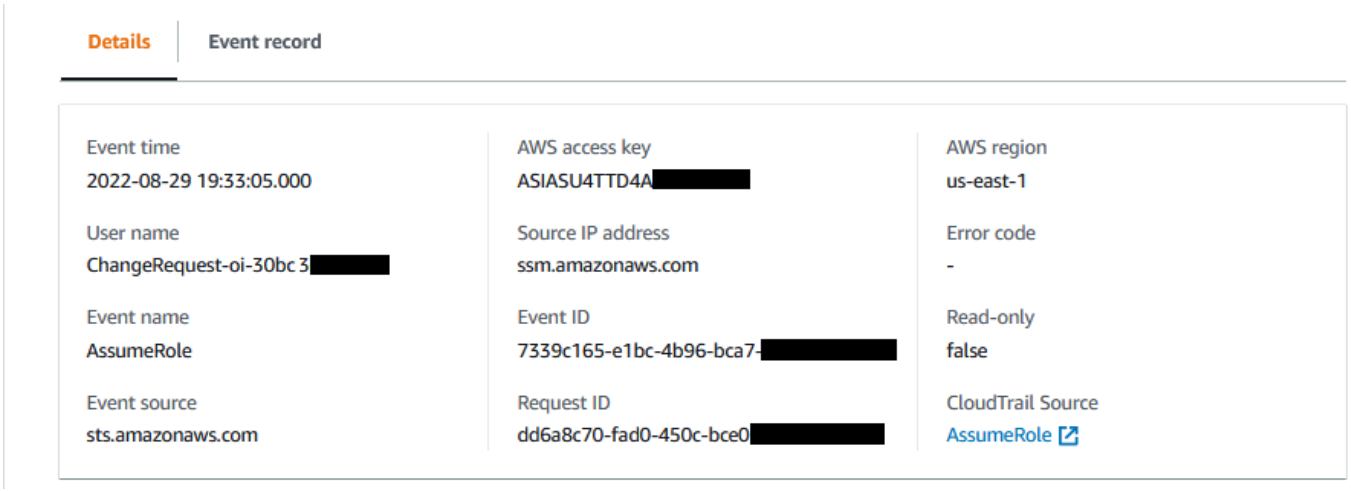
AWS CloudTrail Lake との統合を有効にしてイベントデータストアを作成すると、アカウントまたは組織で実行された変更リクエストに関する (監査可能な) 詳細を表示できます。これには、以下のような詳細情報が含まれます。

- 変更リクエストを開始したユーザーの ID
- 変更が行われた AWS リージョン
- リクエストの送信元 IP アドレス
- リクエストに使用された AWS アクセスキー
- 変更リクエストで実行された API アクション
- このアクションに含まれているリクエストパラメータ
- 処理中に更新されたリソース

以下に、AWS CloudTrail Lake でイベントデータストアを作成した後に表示できる、変更リクエストに対応したイベント詳細の例を示します。

Details

以下の画像は、[Details] (詳細) タブに表示された、変更リクエストに関する概要情報を示しています。これらの詳細情報には、変更リクエストオペレーションの開始時刻、変更リクエストを開始したユーザーの ID、影響を受ける AWS リージョン、および、このリクエストに関連するイベント ID とリクエスト ID などが含まれます。



Event record

次の図は、CloudTrail Lake が変更リクエストイベントのために提供する、JSON コンテンツの構造を示しています。このデータは、変更リクエストの [Event record] (イベントレコード) タブに表示されます。

> **Important**
>
> 組織で Change Manager を使用している場合は、Change Manager の管理アカウントまたは委任管理者アカウントのいずれかでサインインした状態で、以下の手順を完了できます。ただし、委任管理者アカウントを使用してこれらの手順を完了するには、CloudTrail と Change Manager の両方で、同じ委任管理者アカウントを指定しておく必要があります。Change Manager の管理アカウントにサインインすると、CloudTrail の [Settings] (設定) ページから、委任管理者アカウントを追加または変更できます。この処理は、委任管理者アカウントが組織全体で使用するためのイベントデータストアを作成する前に実行しておく必要があります。

Change Manager から CloudTrail Lake のイベントトラッキングを有効にするには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Change Manager] を選択します。
3. [Requests] (リクエスト) タブを選択します。
4. 既存の変更リクエストを選択し、次に [Associated events] (関連付けられたイベント) タブを選択します。
5. [Enable CloudTrail Lake] (CloudTrail Lake を有効にする) を選択します。
6. 「AWS CloudTrail ユーザーガイド」の「CloudTrail イベント用のイベントデータストアの作成」の手順に従います。

   変更リクエストのイベントデータが確実に保存されるようにするには、手順を完了するときに次の選択を行ってください。

   - [イベントタイプ] で、デフォルトの [AWS イベント] と [CloudTrail イベント] が選択されたままにします。
   - 組織で Change Manager を使用している場合、[組織内のすべてのアカウントについて有効化] を選択します。
   - [管理イベント] の [書き込み] チェックボックスは、オンのままにしておきます。

   イベントデータストアを作成する際に選択した他のオプションは、変更リクエストのイベントデータの保存には影響しません。

オートメーションのモニタリング

メトリクスは Amazon CloudWatch での基本的な概念です。メトリクスは、&CW; に発行された時系列のデータポイントのセットを表します。メトリクスはモニタリング対象の変数と考え、データポイントはその変数における時間の経過を表す値と考えます。

Automation は AWS Systems Manager のツールです。Systems Manager は、オートメーションの使用状況に関するメトリクスを CloudWatch にパブリッシュします。これにより、メトリクスに基づいてアラームを設定することを可能にしています。

CloudWatch コンソールでオートメーションメトリクスを表示する

1. CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) を開きます。
2. ナビゲーションペインで [Metrics (メトリクス)] を選択します。
3. [SSM] を選択します。
4. [メトリクス] タブで、[使用状況]、[AWS リソース] の順に選択します。
5. メトリクスのリストの近くにある検索ボックスに、「SSM」と入力します。

AWS CLIを使用してオートメーションメトリクスを表示するには

コマンドプロンプトを開き、次のコマンドを使用します。

```
aws cloudwatch list-metrics \
    --namespace "AWS/Usage"
```

オートメーションメトリクス

Systems Manager は次のオートメーションメトリクスを CloudWatch に送信します。

メトリクス	説明
ConcurrentAutomationUsage	現在の AWS アカウント および AWS リージョン で、同時に実行される自動化処理の数
QueuedAutomationUsage	現在キューに入っているオートメーションのうち、開始されておらず、ステータスが Pending となっているものの数。

CloudWatch メトリクスの使用の詳細については、Amazon CloudWatch ユーザーガイドの以下のトピックを参照してください。

- メトリクス
- Amazon CloudWatch メトリクスを使用する
- Amazon CloudWatch でのアラームの使用

Amazon CloudWatch を使用した Run Command メトリクスのモニタリング

メトリクスは Amazon CloudWatch での基本的な概念です。メトリクスは、&CW; に発行された時系列のデータポイントのセットを表します。メトリクスはモニターリング対象の変数と考え、データポイントは時間の経過と共に変数の値を表します。

AWS Systems Manager は、Run Command コマンドのステータスに関するメトリクスを CloudWatch に公開します。これにより、このようなメトリクスに基づいてアラームを設定できます。Run Command は AWS Systems Manager のツールです。これらの統計は長期間記録されるため、履歴情報にアクセスして、AWS アカウント で実行されるコマンドの成功率をより確実に把握できます。

コマンドの端末ステータス値で、メトリクスを追跡できるものには `Success`、`Failed`、および `Delivery Timed Out` があります。たとえば、SSM コマンドドキュメントが 1 時間ごとに実行されるように設定されている場合、これらの時間に `Success` のステータスがレポートされない場合、それを通知するようアラームを設定できます。コマンドステータス値の詳細については、「コマンドのステータスについて」を参照してください。

CloudWatch コンソールでメトリクスを表示する

1. CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) を開きます。
2. ナビゲーションペインで [Metrics (メトリクス)] を選択します。
3. [AWS のサービスによるアラーム] エリアの [サービス] で、[SSM-Run Command] を選択します。

AWS CLI を使ってメトリクスを表示するには

コマンドプロンプトを開き、次のコマンドを使用します。

```
aws cloudwatch list-metrics --namespace "AWS/SSM-RunCommand"
```

すべての使用可能なメトリクスのリストを表示するには、次のコマンドを使用します。

```
aws cloudwatch list-metrics
```

Systems Manager Run Command のメトリクスとディメンション

Systems Manager は、Run Command コマンドメトリクスを CloudWatch に毎分 1 回送信します。

Systems Manager は次のコマンドメトリクスを CloudWatch に送信します。

> **Note**
>
> これらのメトリクスは単位として `Count` を使用するため、`Sum` と `SampleCount` は最も有用な統計情報です。

メトリクス	説明
`CommandsDeliveryTimedOut`	端末ステータスが `Delivery Timed Out` のコマンドの数。
`CommandsFailed`	端末ステータスが `Failed` のコマンドの数。
`CommandsSucceeded`	端末ステータスが `Success` のコマンドの数。

CloudWatch メトリクスの使用の詳細については、Amazon CloudWatch ユーザーガイドの以下のトピックを参照してください。

- メトリクス
- Amazon CloudWatch メトリクスを使用する
- Amazon CloudWatch でのアラームの使用

AWS Systems Manager による AWS CloudTrail API コールのログ記録

AWS Systems Manager は、ユーザー、ロール、または AWS のサービス によって実行されたアクションの記録を提供するサービスである AWS CloudTrail と統合されています。CloudTrail は、Systems Manager のすべての API コールをイベントとしてキャプチャします。キャプチャされたコールには、Systems Manager コンソールのコールと、Systems Manager API オペレーションへのコードのコールが含まれます。CloudTrail で収集された情報を使用して、Systems Manager に対するリクエスト、リクエスト元の IP アドレス、リクエストの作成日時、その他の詳細を確認できます。

各イベントまたはログエントリには、リクエストの生成者に関する情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます。

- ルートユーザーまたはユーザー認証情報のどちらを使用してリクエストが送信されたか。
- リクエストが IAM Identity Center ユーザーに代わって行われたかどうか。
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが、別の AWS のサービス によって送信されたかどうか。

アカウントを作成すると、AWS アカウント で CloudTrail がアクティブになり、自動的に CloudTrail の[イベント履歴] にアクセスできるようになります。CloudTrail の [イベント履歴] では、AWS リージョン で過去 90 日間に記録された 管理イベントの表示、検索、およびダウンロードが可能で、変更不可能な記録を確認できます。詳細については、「AWS CloudTrail ユーザーガイド」の「CloudTrail イベント履歴の使用」を参照してください。[イベント履歴] の閲覧には CloudTrail の料金はかかりません。

AWS アカウント で過去 90 日間のイベントを継続的に記録するには、証跡または CloudTrail Lake イベントデータストアを作成します。

CloudTrail 証跡

証跡により、CloudTrail はログファイルを Amazon S3 バケットに配信できます。AWS Management Console を使用して作成した証跡はマルチリージョンです。AWS CLI を使用する際は、単一リージョンまたは複数リージョンの証跡を作成できます。アカウント内のすべて AWS リージョン でアクティビティを把握するため、マルチリージョン証跡を作成することをお勧めします。単一リージョンの証跡を作成する場合、証跡の AWS リージョン に記録されたイベントの

みを表示できます。証跡の詳細については、「AWS CloudTrail ユーザーガイド」の「AWS アカウント の証跡の作成」および「組織の証跡の作成」を参照してください。

証跡を作成すると、進行中の管理イベントのコピーを 1 つ無料で CloudTrail から Amazon S3 バケットに配信できますが、Amazon S3 ストレージには料金がかかります。CloudTrail の料金の詳細については、「AWS CloudTrail の料金」を参照してください。Amazon S3 の料金に関する詳細については、「Amazon S3 の料金」を参照してください。

CloudTrail Lake イベントデータストア

[CloudTrail Lake] を使用すると、イベントに対して SQL ベースのクエリを実行できます。CloudTrail Lake は、行ベースの JSON 形式の既存のイベントを Apache ORC 形式に変換します。ORC は、データを高速に取得するために最適化された単票ストレージ形式です。イベントは、イベントデータストアに集約されます。イベントデータストアは、高度なイベントセレクタを適用することによって選択する条件に基づいた、イベントのイミュータブルなコレクションです。どのイベントが存続し、クエリに使用できるかは、イベントデータストアに適用するセレクタが制御します。CloudTrail Lake の詳細については、「AWS CloudTrail ユーザーガイド」の「AWS CloudTrail Lake の使用」を参照してください。

CloudTrail Lake のイベントデータストアとクエリにはコストがかかります。イベントデータストアを作成する際に、イベントデータストアに使用する料金オプションを選択します。料金オプションによって、イベントの取り込みと保存にかかる料金、および、そのイベントデータストアのデフォルトと最長の保持期間が決まります。CloudTrail の料金の詳細については、「AWS CloudTrail の料金」を参照してください。

CloudTrail の Systems Manager データイベント

データイベントでは、リソース上またはリソース内で実行されるリソースオペレーション (コントロールチャネルの作成やオープンなど) についての情報が得られます。これらのイベントは、データプレーンオペレーションとも呼ばれます。データイベントは、多くの場合、高ボリュームのアクティビティです。デフォルトでは、CloudTrail はデータイベントを口グ記録しません。CloudTrail [イベント履歴] にはデータイベントは記録されません。

追加の変更がイベントデータに適用されます。CloudTrail の料金の詳細については、「AWS CloudTrail の料金」を参照してください。

CloudTrail コンソール、AWS CLI、または CloudTrail API オペレーションを使用して、Systems Manager リソースタイプのデータイベントを口グ記録できます。データイベントを口グに記録する方法の詳細については、「AWS CloudTrail ユーザーガイド」の「AWS Management Console を使用

したデータイベントのログ記録」および「AWS Command Line Interface を使用したデータイベントのログ記録」を参照してください。

次の表に、データイベントをログに記録できる Systems Manager リソースタイプの一覧を示します。データイベントタイプ (コンソール) 列には、CloudTrail コンソールの [データイベントタイプ] リストから選択する値が表示されます。resources.type 値列には、AWS CLI または CloudTrail API を使用して高度なイベントセレクタを設定するときに指定する `resources.type` 値が表示されます。CloudTrail に記録されたデータ API 列には、リソース タイプの CloudTrail にログ記録された API コールが表示されます。

データイベントタイプ (コンソール)	resources.type 値	CloudTrail にログ記録されたデータ API
Systems Manager	`AWS::SSMMessages::ControlChannel`	• `CreateControlChannel` • `OpenControlChannel` これらのオペレーションの詳細については、「サービス認可リファレンス」の「Amazon Message Gateway Service で定義されるアクション」を参照してください。
Systems Manager マネージドノード	`AWS::SSM::ManagedNode`	• `RequestManagedInstanceRoleToken` – このイベントは、Systems Manager が管理するノードで実行されている AWS Systems Manager Agent (SSM Agent) が Systems Manager 認証情報サービスからの認証情報をリクエストするときに生成されます。

データイベントタイプ (コンソール)	resources.type 値	CloudTrail にログ記録されたデータ API
		`RequestManagedInstanceRoleToken` 操作の詳細については、「ハードウェアフィンガープリントを使用したハイブリッドアクティベーションマシンの検証」を参照してください

`eventName`、`readOnly`、および `resources.ARN` フィールドでフィルタリングして、自分にとって重要なイベントのみをログに記録するように高度なイベントセレクタを設定できます。オブジェクトの詳細については、「AWS CloudTrail API リファレンス」の「AdvancedFieldSelector」を参照してください。

CloudTrail の Systems Manager 管理イベント

管理イベントでは、AWS アカウント のリソースに対して実行される管理オペレーションについての情報が得られます。これらのイベントは、コントロールプレーンオペレーションとも呼ばれます。CloudTrail は、デフォルトで管理イベントをログ記録します。

Systems Manager は、CloudTrail に対するすべてのコントロールプレーンオペレーションを管理イベントとしてログに記録します。Systems Manager API オペレーションは「AWS Systems Manager API リファレンス」にドキュメント化されています。例えば、`CreateMaintenanceWindows`、`PutInventory`、`SendCommand`、`StartSession` の各アクションを呼び出すと、CloudTrail ログファイルにエントリが生成されます。Systems Manager API コールをモニタリングするために CloudTrail を設定する例については、「Amazon EventBridge を使用してセッションアクティビティをモニタリングする (コンソール)」を参照してください。

Systems Manager のイベント例

各イベントは任意の送信元からの単一のリクエストを表し、リクエストされた API オペレーション、オペレーションの日時、リクエストパラメータなどに関する情報を含みます。CloudTrail ログファイルは、パブリック API コールの順序付けられたスタックトレースではないため、イベントは特定の順序で表示されません。

例:

- 管理イベントの例
- データイベントの例

管理イベントの例

例 1: **DeleteDocument**

次の例は、米国東部 (オハイオ) リージョン (us-east-2) での example-Document という名前のドキュメントに対する DeleteDocument オペレーションを示す CloudTrail イベントを示しています。

```
{
    "eventVersion": "1.04",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAI44QH8DHBEXAMPLE:203.0.113.11",
        "arn": "arn:aws:sts::123456789012:assumed-role/example-role/203.0.113.11",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-03-06T20:19:16Z"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAI44QH8DHBEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/example-role",
                "accountId": "123456789012",
                "userName": "example-role"
            }
        }
    },
    "eventTime": "2018-03-06T20:30:12Z",
    "eventSource": "ssm.amazonaws.com",
    "eventName": "DeleteDocument",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "203.0.113.11",
    "userAgent": "example-user-agent-string",
    "requestParameters": {
        "name": "example-Document"
    },
```

```
    "responseElements": null,
    "requestID": "86168559-75e9-11e4-8cf8-75d18EXAMPLE",
    "eventID": "832b82d5-d474-44e8-a51d-093ccEXAMPLE",
    "resources": [
        {
            "ARN": "arn:aws:ssm:us-east-2:123456789012:document/example-Document",
            "accountId": "123456789012"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

例 2: **StartConnection**

次の例は、米国東部 (オハイオ) リージョン (us-east-2) で Fleet Manager を使用して RDP 接続を開始するユーザーの CloudTrail イベントを示しています。基本となる API アクションは StartConnection です。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAI44QH8DHBEXAMPLE",
        "arn": "arn:aws:sts::123456789012:assumed-role/exampleRole",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAI44QH8DHBEXAMPLE",
                "arn": "arn:aws:sts::123456789012:assumed-role/exampleRole",
                "accountId": "123456789012",
                "userName": "exampleRole"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2021-12-13T14:57:05Z",
                "mfaAuthenticated": "false"
            }
        }
    },
```

```
    "eventTime": "2021-12-13T16:50:41Z",
    "eventSource": "ssm-guiconnect.amazonaws.com",
    "eventName": "StartConnection",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "34.230.45.60",
    "userAgent": "example-user-agent-string",
    "requestParameters": {
        "AuthType": "Credentials",
        "Protocol": "RDP",
        "ConnectionType": "SessionManager",
        "InstanceId": "i-02573cafcfEXAMPLE"
    },
    "responseElements": {
        "ConnectionArn": "arn:aws:ssm-guiconnect:us-east-2:123456789012:connection/
fcb810cd-241f-4aae-9ee4-02d59EXAMPLE",
        "ConnectionKey": "71f9629f-0f9a-4b35-92f2-2d253EXAMPLE",
        "ClientToken": "49af0f92-d637-4d47-9c54-ea51aEXAMPLE",
        "requestId": "d466710f-2adf-4e87-9464-055b2EXAMPLE"
    },
    "requestID": "d466710f-2adf-4e87-9464-055b2EXAMPLE",
    "eventID": "fc514f57-ba19-4e8b-9079-c2913EXAMPLE",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

データイベントの例

例 1: **CreateControlChannel**

次の例は、CreateControlChannel オペレーションを示す CloudTrail イベントを示しています。

```
{
  "eventVersion":"1.08",
  "userIdentity":{
    "type":"AssumedRole",
    "principalId":"AKIAI44QH8DHBEXAMPLE",
    "arn":"arn:aws:sts::123456789012:assumed-role/exampleRole",
    "accountId":"123456789012",
    "accessKeyId":"AKIAI44QH8DHBEXAMPLE",
    "sessionContext":{
```

```
      "sessionIssuer":{
        "type":"Role",
        "principalId":"AKIAI44QH8DHBEXAMPLE",
        "arn":"arn:aws:iam::123456789012:role/exampleRole",
        "accountId":"123456789012",
        "userName":"exampleRole"
      },
      "attributes":{
        "creationDate":"2023-05-04T23:14:50Z",
        "mfaAuthenticated":"false"
      }
    }
  },
  "eventTime":"2023-05-04T23:53:55Z",
  "eventSource":"ssm.amazonaws.com",
  "eventName":"CreateControlChannel",
  "awsRegion":"us-east-1",
  "sourceIPAddress":"192.0.2.0",
  "userAgent":"example-agent",
  "requestParameters":{
    "channelId":"44295c1f-49d2-48b6-b218-96823EXAMPLE",
    "messageSchemaVersion":"1.0",
    "requestId":"54993150-0e8f-4142-aa54-3438EXAMPLE",
    "userAgent":"example-agent"
  },
  "responseElements":{
    "messageSchemaVersion":"1.0",
    "tokenValue":"Value hidden due to security reasons.",
    "url":"example-url"
  },
  "requestID":"54993150-0e8f-4142-aa54-3438EXAMPLE",
  "eventID":"a48a28de-7996-4ca1-a3a0-a51fEXAMPLE",
  "readOnly":false,
  "resources":[
    {
      "accountId":"123456789012",
      "type":"AWS::SSMMessages::ControlChannel",
      "ARN":"arn:aws:ssmmessages:us-east-1:123456789012:control-
channel/44295c1f-49d2-48b6-b218-96823EXAMPLE"
    }
  ],
  "eventType":"AwsApiCall",
  "managementEvent":false,
  "recipientAccountId":"123456789012",
```

```
  "eventCategory":"Data"
}
```

例 2: **RequestManagedInstanceRoleToken**

次の例は、RequestManagedInstanceRoleToken オペレーションを示す CloudTrail イベントを示しています。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "123456789012:aws:ec2-instance:i-02854e4bEXAMPLE",
        "arn": "arn:aws:sts::123456789012:assumed-role/aws:ec2-instance/
i-02854e4bEXAMPLE",
        "accountId": "123456789012",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "123456789012:aws:ec2-instance",
                "arn": "arn:aws:iam::123456789012:role/aws:ec2-instance",
                "accountId": "123456789012",
                "userName": "aws:ec2-instance"
            },
            "attributes": {
                "creationDate": "2023-08-27T03:34:46Z",
                "mfaAuthenticated": "false"
            },
            "ec2RoleDelivery": "2.0"
        }
    },
    "eventTime": "2023-08-27T03:37:15Z",
    "eventSource": "ssm.amazonaws.com",
    "eventName": "RequestManagedInstanceRoleToken",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Apache-HttpClient/UNAVAILABLE (Java/1.8.0_362)",
    "requestParameters": {
        "fingerprint": "i-02854e4bf85EXAMPLE"
    },
    "responseElements": null,
    "requestID": "2582cced-455b-4189-9b82-7b48EXAMPLE",
```

```
    "eventID": "7f200508-e547-4c27-982d-4da0EXAMLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::SSM::ManagedNode",
            "ARN": "arn:aws:ec2:us-east-1:123456789012:instance/i-02854e4bEXAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data"
}
```


CloudTrail レコードの内容については、「AWS CloudTrail ユーザーガイド」の「CloudTrail record contents」を参照してください。

CloudWatch Logs を使用した自動アクション出力のログ記録

AWS Systems Manager のツールである Automation には Amazon CloudWatch Logs が統合されています。ランブック内にある `aws:executeScript` アクションからの出力は、指定したロググループに送信できます。Systems Manager は、`aws:executeScript` アクションを使用しないドキュメント用にはロググループまたはログストリームを作成しません。ドキュメントが `aws:executeScript` を使用する場合、CloudWatch Logs に送信される出力は、それらのアクションにのみ関係します。デバッグおよびトラブルシューティングの目的で CloudWatch Logs のロググループに保存された `aws:executeScript` アクション出力を使用できます。暗号化されたロググループを選択した場合、`aws:executeScript` アクション出力も暗号化されます。`aws:executeScript` アクションからのログの出力は、アカウントレベルの設定です。

アクションの出力を CloudWatch Logs for Amazon が所有するランブックに送信するには、オートメーションを実行するユーザーまたはロールに、次のオペレーションへのアクセス許可が必要です。

- `logs:CreateLogGroup`
- `logs:CreateLogStream`
- `logs:DescribeLogGroups`
- `logs:DescribeLogStreams`
- `logs:PutLogEvents`

所有しているランブックで、ランブックの実行に使用する IAM サービスロール (または AssumeRole) に同じアクセス許可を追加する必要があります。

アクション出力を CloudWatch Logs に送信するには (コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで [オートメーション] を選択します。
3. [Preferences (設定)] タブを選択してから、[Edit (編集)] を選択します。
4. [CloudWatch Logs への出力の送信] の隣にあるチェックボックスをオンにします。
5. (推奨) [Encrypt log data (ログデータの暗号化)] の隣にあるチェックボックスをオンにします。ログデータの暗号化。このオプションが有効になっている場合、ログデータはロググループに指定されたサーバー側の暗号化キーを使用して暗号化されます。CloudWatch Logs に送信されるログデータを暗号化しない場合は、このチェックボックスをオフにします。ロググループで暗号化が許可されていない場合は、このチェックボックスをオフにします。
6. [CloudWatch Logs ロググループ] の場合、アクション出力の送信先である AWS アカウント の既存の CloudWatch Logs ロググループを指定するには、次のいずれかを選択します。
   - デフォルトのロググループに出力を送信する — デフォルトのロググループが存在しない場合 (`/aws/ssm/automation/executeScript`)、オートメーションによって自動的に作成されます。
   - [Choose from a list of log groups (ロググループ一覧から選択する)]: アカウントに既に作成されたロググループを選択してアクション出力を保存します。
   - [Enter a log group name (ロググループ名を入力)]: アクション出力を保存するためにアカウントにすでに作成されているテキストボックスにロググループの名前を入力します。
7. [Save (保存)] を選択します。

アクション出力を CloudWatch Logs に送信するには (コマンドライン)

1. 任意のコマンドラインツールを開き、次のコマンドを実行することによって、アクションの出力先を更新します。

   Linux & macOS

```
aws ssm update-service-setting \
    --setting-id arn:aws:ssm:region:account-id:servicesetting/ssm/automation/
customer-script-log-destination \
```

```
    --setting-value CloudWatch
```

Windows

```
aws ssm update-service-setting ^
    --setting-id arn:aws:ssm:region:account-id:servicesetting/ssm/automation/
customer-script-log-destination ^
    --setting-value CloudWatch
```

PowerShell

```
Update-SSMServiceSetting `
    -SettingId "arn:aws:ssm:region:account-id:servicesetting/ssm/automation/
customer-script-log-destination" `
    -SettingValue "CloudWatch"
```

コマンドが成功した場合、出力はありません。

2. 以下のコマンドを実行して、アクション出力の送信先となるロググループを指定します。

Linux & macOS

```
aws ssm update-service-setting \
    --setting-id arn:aws:ssm:region:account-id:servicesetting/ssm/automation/
customer-script-log-group-name \
    --setting-value my-log-group
```

Windows

```
aws ssm update-service-setting ^
    --setting-id arn:aws:ssm:region:account-id:servicesetting/ssm/automation/
customer-script-log-group-name ^
    --setting-value my-log-group
```

PowerShell

```
Update-SSMServiceSetting `
    -SettingId "arn:aws:ssm:region:account-id:servicesetting/ssm/automation/
customer-script-log-group-name" `
    -SettingValue "my-log-group"
```

コマンドが成功した場合、出力はありません。

3. 次のコマンドを実行して、AWS アカウント および AWS リージョン での Automation アクションログイン設定の現在のサービス設定を表示します。

Linux & macOS

```
aws ssm get-service-setting \
    --setting-id arn:aws:ssm:region:account-id:servicesetting/ssm/automation/
customer-script-log-destination
```

Windows

```
aws ssm get-service-setting ^
    --setting-id arn:aws:ssm:region:account-id:servicesetting/ssm/automation/
customer-script-log-destination
```

PowerShell

```
Get-SSMServiceSetting `
    -SettingId "arn:aws:ssm:region:account-id:servicesetting/ssm/automation/
customer-script-log-destination"
```

このコマンドによって以下のような情報が返されます。

```
{
    "ServiceSetting": {
        "Status": "Customized",
        "LastModifiedDate": 1613758617.036,
        "SettingId": "/ssm/automation/customer-script-log-destination",
        "LastModifiedUser": "arn:aws:sts::123456789012:assumed-role/Administrator/
User_1",
        "SettingValue": "CloudWatch",
        "ARN": "arn:aws:ssm:us-east-2:123456789012:servicesetting/ssm/automation/
customer-script-log-destination"
    }
}
```

Run Command の Amazon CloudWatch Logs の設定

AWS Systems Manager のツールである Run Command を使用してコマンドを送信するときは、コマンド出力の送信先を指定できます。デフォルトでは、Systems Manager はコマンド出力の最初の 24,000 文字のみを返します。コマンド出力の完全な詳細を表示する場合は、Amazon Simple Storage Service (Amazon S3) バケットを指定できます。または、Amazon CloudWatch Logs を指定することもできます。CloudWatch Logs を指定すると、Run Command はすべてのコマンド出力とエラーログを CloudWatch Logs に定期的に送信します。出力ログはほぼリアルタイムでモニタリングし、特定の語句、値、またはパターンを検索して、検索に基づいてアラームを作成できます。

AWS Identity and Access Management (IAM) マネージドポリシー `AmazonSSMManagedInstanceCore` および `CloudWatchAgentServerPolicy` を使用するようにマネージドノードを設定した場合、CloudWatch Logs に出力を送信するためにノードで追加の設定を行う必要はありません。コンソールからコマンドを送信する場合は、このオプションを選択するだけです。または、AWS Command Line Interface (AWS CLI)、AWS Tools for Windows PowerShell、API オペレーションを使用している場合は、`cloud-watch-output-config` セクションと `CloudWatchOutputEnabled` パラメータを追加します。`cloud-watch-output-config` セクションおよび `CloudWatchOutputEnabled` パラメータについては、このトピックの後半で詳しく説明します。

EC2 インスタンス用のインスタンスプロファイルをポリシーに追加する詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」を参照してください。マネージドノードとして使用する予定のオンプレミスサーバーと仮想マシンのサービスロールへのポリシーの追加については、「ハイブリッドおよびマルチクラウド環境で Systems Manager に必要な IAM サービス ロールを作成する」を参照してください。

ノードでカスタムポリシーを使用している場合は、出力と口グの CloudWatch Logs への送信を Systems Manager に許可するために、各ノードでポリシーを更新します。次のポリシーオブジェクトをカスタムポリシーに追加します。IAM ポリシーの詳細については、IAM ユーザーガイドの「IAM ポリシーの編集」を参照してください。

```
{
    "Effect": "Allow",
    "Action": "logs:DescribeLogGroups",
    "Resource": "*"
},
{
   "Effect":"Allow",
   "Action":[
```

```
      "logs:CreateLogGroup",
      "logs:CreateLogStream",
      "logs:DescribeLogStreams",
      "logs:PutLogEvents"
   ],
   "Resource":"arn:aws:logs:*:*:log-group:/aws/ssm/*"
},
```

コマンド送信時に CloudWatch Logs を指定する

AWS Management Console からコマンドを送信するとき、出力として CloudWatch Logs を指定するには、[Output options (出力オプション)] セクションで [CloudWatch Output (CloudWatch 出力)] を選択します。オプションで、コマンド出力を送信する CloudWatch Logs グループの名前を指定できます。グループ名を指定しない場合、Systems Manager によってロググループが自動的に作成されます。ロググループの名前は `/aws/ssm/SystemsManagerDocumentName` 形式に従います。

AWS CLI を使用してコマンドを実行する場合は、コマンドで `cloud-watch-output-config` セクションを指定します。このセクションでは、`CloudWatchOutputEnabled` パラメータを指定することができ、オプションで `CloudWatchLogGroupName` パラメータを指定できます。以下はその例です。

Linux & macOS

```
aws ssm send-command \
    --instance-ids "instance ID" \
    --document-name "AWS-RunShellScript" \
    --parameters "commands=echo helloWorld" \
    --cloud-watch-output-config
 "CloudWatchOutputEnabled=true,CloudWatchLogGroupName=log group name"
```

Windows

```
aws ssm send-command ^
    --document-name "AWS-RunPowerShellScript" ^
    --parameters commands=["echo helloWorld"] ^
    --targets "Key=instanceids,Values=an instance ID” ^
    --cloud-watch-output-config '{"CloudWatchLogGroupName":"log group
 name","CloudWatchOutputEnabled":true}'
```

CloudWatch Logs でのコマンド出力の表示

コマンド実行が開始されるとすぐに、Systems Manager はほぼリアルタイムで CloudWatch Logs に出力を送信します。CloudWatch Logs の出力は次の形式になります。

CommandID/*InstanceID*/*PluginID*/stdout

CommandID/*InstanceID*/*PluginID*/stderr

実行の出力は 30 秒ごと、またはバッファが 200 KB を超えたときのどちらか早い時点でアップロードされます。

> **Note**
>
> ログストリームは、出力データが利用可能であるときのみ作成されます。たとえば、実行のエラーデータがない場合、stderr ストリームは作成されません。

CloudWatch Logs に表示されるコマンド出力の例を次に示します。

```
Group - /aws/ssm/AWS-RunShellScript
Streams –
1234-567-8910/i-abcd-efg-hijk/AWS-RunPowerShellScript/stdout
24/1234-567-8910/i-abcd-efg-hijk/AWS-RunPowerShellScript/stderr
```

Amazon EventBridge を使用して Systems Manager イベントをモニタリングする

Amazon EventBridge は、アプリケーションをさまざまなソースのデータに接続できるようにするサーバーレスイベントバスサービスです。EventBridge は、お客様独自のアプリケーション、SaaS (Software-as-a-Service) アプリケーション、AWS のサービスからリアルタイムデータのストリームを配信し、そのデータを AWS Lambda などのターゲットにルーティングします。お客様は、データの送信先を判断するためのルーティングルールを設定して、すべてのデータソースにリアルタイムで反応するアプリケーションアーキテクチャを構築できます。EventBridge を使用すると、疎結合かつ分散型のイベント駆動型アーキテクチャの構築が可能になります。

EventBridge は、以前は Amazon CloudWatch Events と呼ばれていました。EventBridge には、SaaS パートナーやお客様独自のアプリケーションからイベントを受信できる新しい機能

が含まれています。既存の CloudWatch Events ユーザーは、新しい EventBridge コンソールと CloudWatch Events コンソールで、既存のデフォルトのバス、ルール、およびイベントにアクセスできます。EventBridge では同じ CloudWatch Events API を使用するため、既存の CloudWatch Events API の使用法に変化はありません。

EventBridge は数十件の AWS のサービスのイベントをルールに追加し、20 以上の AWS のサービスのターゲットを追加できます。

EventBridge は、AWS Systems Manager イベントと Systems Manager ターゲットの両方をサポートしています。

サポート対象の Systems Manager のイベントタイプ

EventBridge が検出できる Systems Manager イベントには、次のようなものがあります。

- 手動承認のための、ジャストインタイムノードアクセスのリクエストステータスの更新。
- 失敗したジャストインタイムノードアクセスのリクエスト。
- メンテナンスウィンドウがオフになっています。
- Automation ワークフローが正常に完了しました。Automation は AWS Systems Manager のツールです。
- パッチコンプライアンスに違反しているマネージドノード。
- 更新中のパラメータ値。

EventBridge は、次の AWS Systems Manager ツールのイベントをサポートしています。

- ジャストインタイムノードアクセス (イベントは、ベストエフォートベースで出力されます)。
- オートメーション (イベントはベストエフォートベースで出力されます)。
- Change Calendar (イベントは、ベストエフォートベースで出力されます。)
- コンプライアンス
- インベントリ (イベントは、ベストエフォートベースで出力されます)。
- Maintenance Windows (イベントは、ベストエフォートベースで出力されます。)
- Parameter Store (イベントは、ベストエフォートベースで出力されます。)
- Run Command (イベントは、ベストエフォートベースで出力されます。)
- State Manager (イベントは、ベストエフォートベースで出力されます。)

サポートされている Systems Manager イベントタイプの詳細については、「リファレンス: Systems Manager 用の Amazon EventBridge イベントパターンとタイプ」と「Systems Manager 用の Amazon EventBridge イベントの例」を参照してください。

サポート対象の Systems Manager のターゲットタイプ

EventBridge は、イベントルールのターゲットとして、次の 3 つの Systems Manager ツールをサポートしています。

- 自動化ワークフローを実行する
- Run Command Command ドキュメントを実行する (イベントはベストエフォートベースで出力されます)
- OpsCenter OpsItem の作成

これらのターゲットの推奨される使用方法については、「サンプルシナリオ: Amazon EventBridge ルールのSystems Manager ターゲット」を参照してください。

EventBridge の使用を開始してルールを設定する方法の詳細については、Amazon EventBridge ユーザーガイドの「Amazon EventBridge の開始方法」を参照してください。EventBridge の使用の詳細については、Amazon EventBridge ユーザーガイドを参照してください。

トピック

- Systems Manager イベント用の EventBridge を設定する
- Systems Manager 用の Amazon EventBridge イベントの例
- サンプルシナリオ: Amazon EventBridge ルールのSystems Manager ターゲット

Systems Manager イベント用の EventBridge を設定する

サポートされている AWS Systems Manager のステータス変更、状態の変更、またはその他の条件が発生した場合に、Amazon EventBridge を使用してターゲットイベントを実行できます。状態またはステータスの遷移があると実行されるルールや、関心のある 1 以上の遷移があると実行されるルールを作成できます。

次の手順では、指定したイベントが Systems Manager によって発行されたときに適用される EventBridge ルールを作成するための一般的な手順を示します。特定のシナリオに対応するこのユーザーガイドの手順の一覧については、このトピックの最後にある「詳細情報」を参照してください。

> **Note**
>
> AWS アカウント のサービスがイベントを発行すると、常にアカウントのデフォルトのイベントバスに移動します。AWS のサービスのイベントに応答するルールを作成するには、デフォルトのイベントバスに関連付けます。AWS のサービスからイベントを検索するカスタムイベントバスでルールを作成できますが、このルールは、クロスアカウントイベント配信を介して別のアカウントからそのようなイベントを受信した場合にのみ発動します。詳細については、Amazon EventBridge ユーザーガイドの「AWS アカウント 間での Amazon EventBridge イベントの送受信」を参照してください。

Systems Manager のイベント用に EventBridge を設定するには

1. Amazon EventBridge コンソール (https://console.aws.amazon.com/events/) を開きます。
2. ナビゲーションペインで ルール] を選択します。
3. [ルールの作成] を選択します。
4. ルールの名前と説明を入力します。

   ルールには、同じ AWS リージョン 内および同じイベントバス上の別のルールと同じ名前を付けることはできません。
5. [イベントバス] で、このルールに関連付けるイベントバスを選択します。このルールを使用して、自分の AWS アカウント の一致するイベントに応答する場合は、[default] (デフォルト) を選択します。アカウントの AWS のサービスで発生したイベントは、常にアカウントのデフォルトのイベントバスに移動します。
6. [ルールタイプ] で、[イベントパターンを持つルール] を選択してください。
7. [Next] を選択します。
8. [Event source] (イベントソース) で、[AWS events or EventBridge partner events] (イベントまたは EventBridge パートナーイベント) を選択してください。
9. [Event pattern] (イベントパターン) セクションで [Event pattern form] (イベントパターンフォーム) を選択します。
10. [イベントソース] で、[AWS のサービス] を選択してください。
11. [AWS のサービス] で、[Systems Manager] を選択します。
12. [イベントタイプ] の場合は、次のいずれかの操作を実行します。

    - [すべてのイベント] を選択します。

[すべてのイベント] を選択した場合、Systems Manager によって出力されるすべてのイベントがルールと一致します。このオプションを使用すると、多くのイベントターゲットアクションが発生する可能性があります。

- このルールに使用する Systems Manager のイベントタイプを選択します。EventBridge は、次の AWS Systems Manager ツールのイベントをサポートしています。
  - Automation
  - Change Calendar
  - コンプライアンス
  - インベントリ
  - Maintenance Windows
  - Parameter Store
  - Run Command
  - State Manager

> **Note**
>
> EventBridge でサポートされていない Systems Manager のアクションの場合、[AWS API call through CloudTrail] を選択して、CloudTrail によって記録される API コールに基づくイベントルールを作成できます。例については、「Amazon EventBridge を使用してセッションアクティビティをモニタリングする (コンソール)」を参照してください。

13. (オプション) ルールをより具体的にしたいときは、フィルタ値を追加します。例えば、State Manager を選択し、関連付けのターゲットである単一のマネージドインスタンスの状態にルールを制限する場合、[Specific type(s)] (特定のタイプ) に [EC2 ステートマネージャーインスタンスの関連付けの状態の変更] を選択します。

    サポートされている詳細タイプの詳細については、「 リファレンス: Systems Manager 用の Amazon EventBridge イベントパターンとタイプ」を参照してください。

    一部の詳細タイプには、ステータスなど、サポートされる他のオプションがあります。使用可能なオプションは、選択したツールに応じて異なります。

14. [Next] を選択します。
15. [ターゲットタイプ] で、[AWS のサービス] を選択します。

16. [Select a target] (ターゲットを選択) でターゲット (Amazon SNS トピックまたは AWS Lambda 関数) を選択します。ターゲットは、ルールで定義したイベントパターンに一致するイベントが返されたときにトリガーされます。
17. 多くのターゲットタイプで、EventBridge はターゲットにイベントを送信するためのアクセス許可が必要です。これらの場合、EventBridge は、イベントの実行に必要な AWS Identity and Access Management (IAM) ロールを作成できます。

    - 自動的に IAM ロールを作成するには、[Create a new role for this specific resource (この特定のリソースに対して新しいロールを作成する)] を選択します。
    - 以前に作成した IAM ロールを使用するには、[Use existing role (既存のロールの使用)] を選択します。
18. (オプション) 別のターゲットを追加] を選択して、このルールに別のターゲットを追加します。
19. [Next] を選択します。
20. (オプション) ルールに 1 つ以上のタグを入力します。詳細については、Amazon EventBridge ユーザーガイドのAmazon EventBridge のタグを参照してください。
21. 次へをクリックします。
22. ルールの詳細を確認し、ルールの作成 を選択します。

詳細情報

- ランブックを使用する EventBridge イベントを作成する (コンソール)
- 入力トランスフォーマーを使用したオートメーションへのデータの受け渡し
- EventBridge を使用してコンプライアンス問題を修復する
- EventBridge でインベントリ削除アクションを表示する
- EventBridge ルールを設定して OpsItems を作成する
- パラメータおよびパラメータポリシー用の EventBridge ルールを設定する

Systems Manager 用の Amazon EventBridge イベントの例

JSON 形式で、AWS Systems Manager のサポートされている EventBridge イベントの例は以下のとおりです。

Systems Manager のイベントタイプ

- AWS Systems Manager Automation のイベント
- AWS Systems ManagerChange Calendar のイベント

- AWS Systems ManagerイベントChange Manager
- AWS Systems Manager Compliance のイベント
- AWS Systems Manager Maintenance Windows のイベント
- AWS Systems Manager Parameter Store のイベント
- AWS Systems ManagerOpsCenter のイベント
- AWS Systems ManagerRun Command のイベント
- AWS Systems ManagerState Manager のイベント

AWS Systems Manager Automation のイベント

Automation ステップステータス変更の通知

```
{
  "version": "0",
  "id": "eeca120b-a321-433e-9635-dab369006a6b",
  "detail-type": "EC2 Automation Step Status-change Notification",
  "source": "aws.ssm",
  "account": "123456789012",
  "time": "2024-11-29T19:43:35Z",
  "region": "us-east-1",
  "resources": ["arn:aws:ssm:us-east-2:123456789012:automation-
execution/333ba70b-2333-48db-b17e-a5e69c6f4d1c",
    "arn:aws:ssm:us-east-2:123456789012:automation-definition/runcommand1:1"],
  "detail": {
    "ExecutionId": "333ba70b-2333-48db-b17e-a5e69c6f4d1c",
    "Definition": "runcommand1",
    "DefinitionVersion": 1.0,
    "Status": "Success",
    "EndTime": "Nov 29, 2024 7:43:25 PM",
    "StartTime": "Nov 29, 2024 7:43:23 PM",
    "Time": 2630.0,
    "StepName": "runFixedCmds",
    "Action": "aws:runCommand"
  }
}
```

Automation 実行ステータス変更の通知

```
{
```

```
  "version": "0",
  "id": "d290ece9-1088-4383-9df6-cd5b4ac42b99",
  "detail-type": "EC2 Automation Execution Status-change Notification",
  "source": "aws.ssm",
  "account": "123456789012",
  "time": "2024-11-29T19:43:35Z",
  "region": "us-east-2",
  "resources": ["arn:aws:ssm:us-east-2:123456789012:automation-
execution/333ba70b-2333-48db-b17e-a5e69c6f4d1c",
    "arn:aws:ssm:us-east-2:123456789012:automation-definition/runcommand1:1"],
  "detail": {
    "ExecutionId": "333ba70b-2333-48db-b17e-a5e69c6f4d1c",
    "Definition": "runcommand1",
    "DefinitionVersion": 1.0,
    "Status": "Success",
    "StartTime": "Nov 29, 2024 7:43:20 PM",
    "EndTime": "Nov 29, 2024 7:43:26 PM",
    "Time": 5753.0,
    "ExecutedBy": "arn:aws:iam::123456789012:user/userName"
  }
}
```

AWS Systems ManagerChange Calendar のイベント

以下は、AWS Systems ManagerChange Calendar のイベントの例です。

> **Note**
>
> 他の AWS アカウントから共有されているカレンダーの状態の変更は現在サポートされていません。

カレンダーは開いています

```
{
    "version": "0",
    "id": "47a3f03a-f30d-1011-ac9a-du3bdEXAMPLE",
    "detail-type": "Calendar State Change",
    "source": "aws.ssm",
    "account": "123456789012",
    "time": "2024-09-19T18:00:07Z",
    "region": "us-east-2",
```

```
    "resources": [
        "arn:aws:ssm:us-east-2:123456789012:document/MyCalendar"
    ],
    "detail": {
        "state": "OPEN",
        "atTime": "2024-09-19T18:00:07Z",
        "nextTransitionTime": "2024-10-11T18:00:07Z"
    }
}
```

カレンダーは閉じています

```
{
    "version": "0",
    "id": "f30df03a-1011-ac9a-47a3-f761eEXAMPLE",
    "detail-type": "Calendar State Change",
    "source": "aws.ssm",
    "account": "123456789012",
    "time": "2024-09-17T21:40:02Z",
    "region": "us-east-2",
    "resources": [
        "arn:aws:ssm:us-east-2:123456789012:document/MyCalendar"
    ],
    "detail": {
        "state": "CLOSED",
        "atTime": "2024-08-17T21:40:00Z",
        "nextTransitionTime": "2024-09-19T18:00:07Z"
    }
}
```

AWS Systems ManagerイベントChange Manager

変更要求ステータス更新通知-例 1

```
{
  "version": "0",
  "id": "feab80c1-a8ff-c721-b8b1-96ce70939696",
  "detail-type": "Change Request Status Update",
  "source": "aws.ssm",
  "account": "123456789012",
  "time": "2024-10-24T10:51:52Z",
  "region": "us-east-1",
  "resources": [
```

```
    "arn:aws:ssm:us-west-2:123456789012:opsitem/oi-12345abcdef",
    "arn:aws:ssm:us-west-2:123456789012:document/MyRunbook1"
  ],
  "detail": {
    "change-request-id": "d0585556-80f6-4522-8dad-dada6d45b67d",
    "change-request-title": "A change request title",
    "ops-item-id": "oi-12345abcdef",
    "ops-item-created-by": "arn:aws:iam::123456789012:user/JohnDoe",
    "ops-item-created-time": "2024-10-24T10:50:33.180334Z",
    "ops-item-modified-by": "arn:aws:iam::123456789012:user/JohnDoe",
    "ops-item-modified-time": "2024-10-24T10:50:33.180340Z",
    "ops-item-status": "InProgress",
    "change-template-document-name": "MyChangeTemplate",
    "runbook-document-arn": "arn:aws:ssm:us-west-2:123456789012:document/MyRunbook1",
    "runbook-document-version": "1",
    "auto-approve": true,
    "approvers": [
      "arn:aws:iam::123456789012:user/JaneDoe"
    ]
  }
}
```

変更要求ステータス更新通知-例 2

```
{
  "version": "0",
  "id": "25ce6b03-2e4e-1a2b-2a8f-6c9de8d278d2",
  "detail-type": "Change Request Status Update",
  "source": "aws.ssm",
  "account": "123456789012",
  "time": "2024-10-24T10:51:52Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ssm:us-west-2:123456789012:opsitem/oi-abcdef12345",
    "arn:aws:ssm:us-west-2:123456789012:document/MyRunbook1"
  ],
  "detail": {
    "change-request-id": "d0585556-80f6-4522-8dad-dada6d45b67d",
    "change-request-title": "A change request title",
    "ops-item-id": "oi-abcdef12345",
    "ops-item-created-by": "arn:aws:iam::123456789012:user/JohnDoe",
    "ops-item-created-time": "2024-10-24T10:50:33.180334Z",
    "ops-item-modified-by": "arn:aws:iam::123456789012:user/JohnDoe",
```

```
    "ops-item-modified-time": "2024-10-24T10:50:33.997163Z",
    "ops-item-status": "Rejected",
    "change-template-document-name": "MyChangeTemplate",
    "runbook-document-arn": "arn:aws:ssm:us-west-2:123456789012:document/MyRunbook1",
    "runbook-document-version": "1",
    "auto-approve": true,
    "approvers": [
      "arn:aws:iam::123456789012:user/JaneDoe"
    ]
  }
}
```

AWS Systems Manager Compliance のイベント

以下は、AWS Systems Manager Compliance のイベントの例です。

関連付けの準拠

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Configuration Compliance State Change",
  "source": "aws.ssm",
  "account": "123456789012",
  "time": "2024-07-17T19:03:26Z",
  "region": "us-east-2",
  "resources": [
    "arn:aws:ssm:us-east-2:123456789012:managed-instance/i-01234567890abcdef"
  ],
  "detail": {
    "last-runtime": "2024-01-01T10:10:10Z",
    "compliance-status": "compliant",
    "resource-type": "managed-instance",
    "resource-id": "i-01234567890abcdef",
    "compliance-type": "Association"
  }
}
```

関連付けの非準拠

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
```

```
  "detail-type": "Configuration Compliance State Change",
  "source": "aws.ssm",
  "account": "123456789012",
  "time": "2024-07-17T19:02:31Z",
  "region": "us-east-2",
  "resources": [
    "arn:aws:ssm:us-east-2:123456789012:managed-instance/i-01234567890abcdef"
  ],
  "detail": {
    "last-runtime": "2024-01-01T10:10:10Z",
    "compliance-status": "non_compliant",
    "resource-type": "managed-instance",
    "resource-id": "i-01234567890abcdef",
    "compliance-type": "Association"
  }
}
```

パッチの準拠

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Configuration Compliance State Change",
  "source": "aws.123456789012",
  "account": "123456789012",
  "time": "2024-07-17T19:03:26Z",
  "region": "us-east-2",
  "resources": [
    "arn:aws:ssm:us-east-2:123456789012:managed-instance/i-01234567890abcdef"
  ],
  "detail": {
    "resource-type": "managed-instance",
    "resource-id": "i-01234567890abcdef",
    "compliance-status": "compliant",
    "compliance-type": "Patch",
    "patch-baseline-id": "PB789",
    "severity": "critical"
  }
}
```

パッチの非準拠

```
{
```

```
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Configuration Compliance State Change",
  "source": "aws.ssm",
  "account": "123456789012",
  "time": "2024-07-17T19:02:31Z",
  "region": "us-east-2",
  "resources": [
    "arn:aws:ssm:us-east-2:123456789012:managed-instance/i-01234567890abcdef"
  ],
  "detail": {
    "resource-type": "managed-instance",
    "resource-id": "i-01234567890abcdef",
    "compliance-status": "non_compliant",
    "compliance-type": "Patch",
    "patch-baseline-id": "PB789",
    "severity": "critical"
  }
}
```

AWS Systems Manager Maintenance Windows のイベント

以下は、Systems Manager Maintenance Windows のイベントの例です。

ターゲットの登録

有効なステータス値は、REGISTERED および DEREGISTERED です。

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-0123456789ab",
   "detail-type":"Maintenance Window Target Registration Notification",
   "source":"aws.ssm",
   "account":"123456789012",
   "time":"2024-11-16T00:58:37Z",
   "region":"us-east-2",
   "resources":[
      "arn:aws:ssm:us-east-2:123456789012:maintenancewindow/mw-0ed7251d3fcf6e0c2",
      "arn:aws:ssm:us-east-2:123456789012:windowtarget/
e7265f13-3cc5-4f2f-97a9-7d3ca86c32a6"
   ],
   "detail":{
      "window-target-id":"e7265f13-3cc5-4f2f-97a9-7d3ca86c32a6",
```

```
      "window-id":"mw-0ed7251d3fcf6e0c2",
      "status":"REGISTERED"
   }
}
```

ウィンドウの実行タイプ

有効なステータス値は、PENDING、IN_PROGRESS、SUCCESS、FAILED、TIMED_OUT および SKIPPED_OVERLAPPING です。

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-0123456789ab",
   "detail-type":"Maintenance Window Execution State-change Notification",
   "source":"aws.ssm",
   "account":"123456789012",
   "time":"2025-06-02T14:52:18Z",
   "region":"us-east-2",
   "resources":[
      "arn:aws:ssm:us-east-2:123456789012:maintenancewindow/mw-0c50858d01EXAMPLE"
   ],
   "detail":{
      "start-time":"2025-06-02T14:48:28.039273Z",
      "end-time":"2025-06-02T14:52:18.083773Z",
      "window-id":"mw-0ed7251d3fcf6e0c2",
      "window-execution-id":"14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE",
      "status":"SUCCESS"
   }
}
```

タスクの実行タイプ

有効なステータス値は、IN_PROGRESS、SUCCESS、FAILED および TIMED_OUT です。

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-0123456789ab",
   "detail-type":"Maintenance Window Task Execution State-change Notification",
   "source":"aws.ssm",
   "account":"123456789012",
   "time":"2025-06-02T14:52:18Z",
   "region":"us-east-2",
```

```
   "resources":[
      "arn:aws:ssm:us-east-2:123456789012:maintenancewindow/mw-0c50858d01EXAMPLE"
   ],
   "detail":{
      "start-time":"2025-06-02T14:48:28.039273Z",
      "task-execution-id":"6417e808-7f35-4d1a-843f-123456789012",
      "end-time":"2025-06-02T14:52:18.083773Z",
      "window-id":"mw-0ed7251d3fcf6e0c2",
      "window-execution-id":"14bea65d-5ccc-462d-a2f3-e99c8EXAMPLE",
      "status":"SUCCESS"
   }
}
```

処理されるタスクのターゲット

有効なステータス値は、IN_PROGRESS、SUCCESS、FAILED および TIMED_OUT です。

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-0123456789ab",
   "detail-type":"Maintenance Window Task Target Invocation State-change Notification",
   "source":"aws.ssm",
   "account":"123456789012",
   "time":"2025-06-02T14:52:18Z",
   "region":"us-east-2",
   "resources":[
      "arn:aws:ssm:us-east-2:123456789012:maintenancewindow/mw-1234567890123456789"
   ],
   "detail":{
      "start-time":"2025-06-02T14:48:28.039273Z",
      "end-time":"2025-06-02T14:52:18.083773Z",
      "window-id":"mw-0ed7251d3fcf6e0c2",
      "window-execution-id":"791b72e0-f0da-4021-8b35-f95dfEXAMPLE",
      "task-execution-id":"c9b05aba-197f-4d8d-be34-e73fbEXAMPLE",
      "window-target-id":"e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE",
      "status":"SUCCESS",
      "owner-information":"Owner"
   }
}
```

ウィンドウの状態の変更

有効なステータス値は、ENABLED および DISABLED です。

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-0123456789ab",
   "detail-type":"Maintenance Window State-change Notification",
   "source":"aws.ssm",
   "account":"123456789012",
   "time":"2024-11-16T00:58:37Z",
   "region":"us-east-2",
   "resources":[
      "arn:aws:ssm:us-east-2:123456789012:maintenancewindow/mw-0c50858d01EXAMPLE"
   ],
   "detail":{
      "window-id":"mw-0c50858d01EXAMPLE",
      "status":"DISABLED"
   }
}
```

AWS Systems Manager Parameter Store のイベント

以下は、Systems Manager Parameter Store のイベントの例です。

パラメータの作成

```
{
  "version": "0",
  "id": "6a7e4feb-b491-4cf7-a9f1-bf3703497718",
  "detail-type": "Parameter Store Change",
  "source": "aws.ssm",
  "account": "123456789012",
  "time": "2024-05-22T16:43:48Z",
  "region": "us-east-2",
  "resources": [
    "arn:aws:ssm:us-east-2:123456789012:parameter/MyExampleParameter"
  ],
  "detail": {
    "operation": "Create",
    "name": "MyExampleParameter",
    "type": "String",
    "description": "Sample Parameter"
  }
}
```

パラメータの更新


```
{
  "version": "0",
  "id": "9547ef2d-3b7e-4057-b6cb-5fdf09ee7c8f",
  "detail-type": "Parameter Store Change",
  "source": "aws.ssm",
  "account": "123456789012",
  "time": "2024-05-22T16:44:48Z",
  "region": "us-east-2",
  "resources": [
    "arn:aws:ssm:us-east-2:123456789012:parameter/MyExampleParameter"
  ],
  "detail": {
    "operation": "Update",
    "name": "MyExampleParameter",
    "type": "String",
    "description": "Sample Parameter"
  }
}
```


パラメータの削除


```
{
  "version": "0",
  "id": "80e9b391-6a9b-413c-839a-453b528053af",
  "detail-type": "Parameter Store Change",
  "source": "aws.ssm",
  "account": "123456789012",
  "time": "2024-05-22T16:45:48Z",
  "region": "us-east-2",
  "resources": [
    "arn:aws:ssm:us-east-2:123456789012:parameter/MyExampleParameter"
  ],
  "detail": {
    "operation": "Delete",
    "name": "MyExampleParameter",
    "type": "String",
    "description": "Sample Parameter"
  }
}
```

AWS Systems ManagerOpsCenter のイベント

OpsCenterOpsItem通知の作成


```
{
  "version": "0",
  "id": "aae66adc-7aac-f0c0-7854-7691e8c079b8",
  "detail-type": "OpsItem Create",
  "source": "aws.ssm",
  "account": "123456789012",
  "time": "2024-10-19T02:48:11Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ssm:us-west-2:123456789012:opsitem/oi-123456abcdef"
  ],
  "detail": {
    "created-by": "arn:aws:iam::123456789012:user/JohnDoe",
    "created-time": "2024-10-19T02:46:53.629361Z",
    "source": "aws.ssm",
    "status": "Open",
    "ops-item-id": "oi-123456abcdef",
    "title": "An issue title",
    "ops-item-type": "/aws/issue",
    "description": "A long description may appear here"
  }
}
```


OpsCenterOpsItem通知の更新


```
{
  "version": "0",
  "id": "2fb5b168-b725-41dd-a890-29311200089c",
  "detail-type": "OpsItem Update",
  "source": "aws.ssm",
  "account": "123456789012",
  "time": "2024-10-19T02:48:11Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ssm:us-west-2:123456789012:opsitem/oi-123456abcdef"
  ],
  "detail": {
    "created-by": "arn:aws:iam::123456789012:user/JohnDoe",
    "created-time": "2024-10-19T02:46:54.049271Z",
```

```
    "modified-by": "arn:aws:iam::123456789012:user/JohnDoe",
    "modified-time": "2024-10-19T02:46:54.337354Z",
    "source": "aws.ssm",
    "status": "Open",
    "ops-item-id": "oi-123456abcdef",
    "title": "An issue title",
    "ops-item-type": "/aws/issue",
    "description": "A long description may appear here"
  }
}
```

AWS Systems ManagerRun Command のイベント

Run Command ステータス変更通知

```
{
    "version": "0",
    "id": "51c0891d-0e34-45b1-83d6-95db273d1602",
    "detail-type": "EC2 Command Status-change Notification",
    "source": "aws.ssm",
    "account": "123456789012",
    "time": "2024-07-10T21:51:32Z",
    "region": "us-east-2",
    "resources": ["arn:aws:ec2:us-east-2:123456789012:instance/i-02573cafcfEXAMPLE"],
    "detail": {
        "command-id": "e8d3c0e4-71f7-4491-898f-c9b35bee5f3b",
        "document-name": "AWS-RunPowerShellScript",
        "expire-after": "2024-07-14T22:01:30.049Z",
        "parameters": {
            "executionTimeout": ["3600"],
            "commands": ["date"]
        },
        "requested-date-time": "2024-07-10T21:51:30.049Z",
        "status": "Success"
    }
}
```

Run Command 呼び出しステータス変更通知

```
{
    "version": "0",
    "id": "4780e1b8-f56b-4de5-95f2-95dbEXAMPLE",
    "detail-type": "EC2 Command Invocation Status-change Notification",
```

```
    "source": "aws.ssm",
    "account": "123456789012",
    "time": "2024-07-10T21:51:32Z",
    "region": "us-east-2",
    "resources": ["arn:aws:ec2:us-east-2:123456789012:instance/i-02573cafcfEXAMPLE"],
    "detail": {
        "command-id": "e8d3c0e4-71f7-4491-898f-c9b35bee5f3b",
        "document-name": "AWS-RunPowerShellScript",
        "instance-id": "i-02573cafcfEXAMPLE",
        "requested-date-time": "2024-07-10T21:51:30.049Z",
        "status": "Success"
    }
}
```

AWS Systems ManagerState Manager のイベント

State Manager 関連付け状態の変更

```
{
   "version":"0",
   "id":"db839caf-6f6c-40af-9a48-25b2ae2b7774",
   "detail-type":"EC2 State Manager Association State Change",
   "source":"aws.ssm",
   "account":"123456789012",
   "time":"2024-05-16T23:01:10Z",
   "region":"us-east-2",
   "resources":[
      "arn:aws:ssm:us-east-2::document/AWS-RunPowerShellScript"
   ],
   "detail":{
      "association-id":"6e37940a-23ba-4ab0-9b96-5d0a1a05464f",
      "document-name":"AWS-RunPowerShellScript",
      "association-version":"1",
      "document-version":"Optional.empty",
      "targets":"[{\"key\":\"InstanceIds\",\"values\":[\"i-12345678\"]}]",
      "creation-date":"2024-02-13T17:22:54.458Z",
      "last-successful-execution-date":"2024-05-16T23:00:01Z",
      "last-execution-date":"2024-05-16T23:00:01Z",
      "last-updated-date":"2024-02-13T17:22:54.458Z",
      "status":"Success",
      "association-status-aggregated-count":"{\"Success\":1}",
      "schedule-expression":"cron(0 */30 * * * ? *)",
      "association-cwe-version":"1.0"
```

```
    }
}
```

State Manager インスタンス関連付け状態の変更

```
{
   "version":"0",
   "id":"6a7e8feb-b491-4cf7-a9f1-bf3703467718",
   "detail-type":"EC2 State Manager Instance Association State Change",
   "source":"aws.ssm",
   "account":"123456789012",
   "time":"2024-02-23T15:23:48Z",
   "region":"us-east-2",
   "resources":[
      "arn:aws:ec2:us-east-2:123456789012:instance/i-12345678",
      "arn:aws:ssm:us-east-2:123456789012:document/my-custom-document"
   ],
   "detail":{
      "association-id":"34fcb7e0-9a14-4984-9989-0e04e3f60bd8",
      "instance-id":"i-02573cafcfEXAMPLE",
      "document-name":"my-custom-document",
      "document-version":"1",
      "targets":"[{\"key\":\"instanceids\",\"values\":[\"i-02573cafcfEXAMPLE\"]}]",
      "creation-date":"2024-02-23T15:23:48Z",
      "last-successful-execution-date":"2024-02-23T16:23:48Z",
      "last-execution-date":"2024-02-23T16:23:48Z",
      "status":"Success",
      "detailed-status":"",
      "error-code":"testErrorCode",
      "execution-summary":"testExecutionSummary",
      "output-url":"sampleurl",
      "instance-association-cwe-version":"1"
   }
}
```

サンプルシナリオ: Amazon EventBridge ルールのSystems Manager ターゲット

Amazon EventBridge ルールで呼び出すターゲットを指定する場合、20 を超えるターゲットタイプから選択し、各ルールに最大 5 つのターゲットを追加できます。

さまざまなターゲットのうち、EventBridge イベントが発生したときのターゲットアクションとして、Automation、OpsCenter、Run Command (いずれも AWS Systems Manager のツール) から選択できます。

次に、これらのツールを EventBridge ルールのターゲットとして使用する方法の例をいくつか示します。

自動化の例

次のようなイベントが発生したときに、オートメーションワークフローを開始するように EventBridge ルールを設定できます。

- マネージドノードがステータスチェック (`StatusCheckFailed_Instance=1`) に失敗したことが Amazon CloudWatch アラームによってレポートされた場合、ノードで `AWSSupport-ExecuteEC2Rescue` Automation ランブックを実行します。
- 新しい Amazon Elastic Compute Cloud (Amazon EC2) インスタンスが実行されているために `EC2 Instance State-change Notification` イベントが発生した場合は、インスタンスで `AWS-AttachEBSVolume` Automation ランブックを実行します。
- Amazon Elastic Block Store (Amazon EBS) ボリュームが作成され、利用可能になったら、そのボリュームで `AWS-CreateSnapshot` Automation ランブックを実行します。

OpsCenter の例

次のようなインシデントが発生した場合に、新しい OpsItem を作成するように EventBridge ルールを設定できます。

- Amazon DynamoDB のスロットリングイベントが発生するか、Amazon EBS ボリュームのパフォーマンスが低下しています。
- Amazon EC2 Auto Scaling グループがノードの起動に失敗したか、Systems Manager Automation ワークフローが失敗しました。
- EC2 インスタンスの状態が `Running` から `Stopped` に変わります。

Run Command の例

次のようなイベントが発生したときに、Run Command で Systems Manager コマンドドキュメントを実行するように EventBridge ルールを設定できます。

- Auto Scaling グループが間もなく終了するとき、Run Command スクリプトは終了する前にノードからログファイルをキャプチャできます。
- 新しいノードが Auto Scaling グループ内に作成されると、Run Command ターゲットアクションによってウェブサーバーロールが有効になるか、ノードにソフトウェアがインストールされる可能性があります。
- マネージドノードがコンプライアンス違反であることが判明した場合、Run Command ターゲットアクションは、`AWS-RunPatchBaseline` ドキュメントを実行してノード上のパッチを更新する可能性があります。

Amazon SNS 通知を使用した Systems Manager のステータス変更のモニタリング

Amazon Simple Notification Service (Amazon SNS) を設定し、AWS Systems Manager のツールである Run Command または Maintenance Windows を使用して送信したコマンドのステータスに関する通知を送信できます。Amazon SNS は、Amazon SNS トピックをサブスクライブしているクライアントまたはエンドポイントへの通知の送信および配信を管理します。コマンドが新しい状態に変更、または失敗やタイムアウトのような状態に変更されるたびに通知を受け取ることができます。複数のノードにコマンドを送信する場合、特定ノードに送信されたコマンドの各コピーに対して通知を受けることができます。各コピーは、その呼び出しと呼ばれます。

Amazon SNS は、HTTP または HTTPS POST、E メール (SMTP、プレーンテキストまたは JSON 形式のいずれか)、あるいは Amazon Simple Queue Service (Amazon SQS) キューに投稿されるメッセージとして通知を配信できます。詳細については、Amazon Simple Notification Service デベロッパーガイドの「Amazon SNS とは」を参照してください。Run Command と Maintenance Windows が提供する Amazon SNS 通知に含まれる JSON データの構造の例については、「AWS Systems Manager の Amazon SNS 通知の例」を参照してください。

> **Important**
>
> 次の重要な情報に注意してください。
>
> - Amazon Simple 通知サービスの FIFO トピックはサポートされていません。
> - チャットアプリケーションの Amazon Q Developer は、Amazon SNS を使用した Systems Manager のモニタリングではサポートされていません。チャットアプリケーションの Amazon Q Developer を使って Systems Manager をモニタリングする場合は、Amazon EventBridge を使用します。EventBridge を使用して Systems Manager をモニタリングす

る方法については、「Amazon EventBridge を使用して Systems Manager イベントをモニタリングする」を参照してください。チャットアプリケーションの Amazon EventBridge と Amazon Q Developer の詳細については、Amazon Q Developer in chat applications Administrator Guide の「Tutorial: Create an EventBridge rule that send notifications to Amazon Q Developer in chat applications」を参照してください。

AWS Systems Manager の Amazon SNS 通知の設定

メンテナンスウィンドウに登録されている Run Command および Maintenance Windows のタスクは、以下のステータスに入るコマンドタスクについて Amazon SNS 通知を送信できます。

- 進行中
- 成功
- 失敗
- タイムアウト
- Cancelled (キャンセル)

これらのステータスのいずれかを入力するコマンドの条件については、「コマンドのステータスについて」を参照してください。

> **Note**
>
> Run Command を使用してコマンドを送信すると、キャンセル中および保留中のステータスも報告されます。これらのステータスは、Amazon SNS 通知ではキャプチャされません。

Amazon SNS 通知のコマンド概要

Amazon SNS 通知のメンテナンスウィンドウにある Run Command または Run Command のタスクを設定する場合、Amazon SNS は次の情報を含む概要メッセージを送信します。

フィールド	タイプ	説明
eventTime	文字列	イベントが開始された時刻。Amazon SNS はメッセージの配信順序を保証しないた

フィールド	タイプ	説明
		め、タイムスタンプは重要です。例: 2016-04-26T13:15:30Z
documentName	文字列	このコマンドの実行に使用された SSM ドキュメントの名前。
commandId	String	コマンドが送信された後に Run Command によって生成された ID です。
expiresAfter	日付	この時間が経過したときにコマンドの実行がまだ開始されていない場合、コマンドは実行されません。
outputS3BucketName	文字列	コマンド実行に対する応答を保存する Amazon Simple Storage Service (Amazon S3) バケットです。
outputS3KeyPrefix	文字列	コマンド実行に対する応答を保存するバケット内の Amazon S3 のディレクトリパスです。
requestedDateTime	String	リクエストがこの特定のノードに送信された日時です。

フィールド	タイプ	説明
instanceIds	StringList	コマンドの対象となるノードです。 **Note** インスタンス ID が概要メッセージに含まれるのは、Run Command タスクがインスタンス ID を直接ターゲットにしている場合のみです。Run Command タスクがタグベースのターゲティングを使用して発行された場合、インスタンス ID は概要メッセージに含まれません。
ステータス	文字列	コマンドのコマンドステータスです。

呼び出しベースの Amazon SNS 通知

コマンドを複数のノードに送信する場合、Amazon SNS はコマンドの各コピーまたは呼び出しに関するメッセージを送信できます。メッセージには次の情報が含まれます。

フィールド	タイプ	説明
eventTime	文字列	イベントが開始された時刻。Amazon SNS はメッセージの配信順序を保証しないため、タイムスタンプは重要で

フィールド	タイプ	説明
		す。例: 2016-04-26T13:15:30Z
documentName	文字列	このコマンドの実行に使用された Systems Manager ドキュメント (SSM ドキュメント) の名前。
requestedDateTime	String	リクエストがこの特定のノードに送信された日時です。
commandId	String	コマンドが送信された後に Run Command によって生成された ID です。
instanceId	文字列	コマンドの対象となるインスタンスを選択します。
status	文字列	この呼び出しのコマンドステータス。

コマンドがステータスを変更したときに Amazon SNS 通知をセットアップするには、次のタスクを完了する必要があります。

> **Note**
>
> メンテナンスウィンドウの Amazon SNS 通知を設定していない場合は、このトピックの「タスク 5」をスキップできます。

トピック

- タスク 1: Amazon SNS トピックを作成してサブスクライブする
- タスク 2: Amazon SNS 通知用の IAM ポリシーを作成する
- タスク 3: Amazon SNS 通知の IAM ロールを作成する
- タスク 4: ユーザーアクセスを設定する

- タスク 5: iam:PassRole ポリシーをメンテナンスウィンドウロールにアタッチする

タスク 1: Amazon SNS トピックを作成してサブスクライブする

Amazon SNS トピックは、メンテナンスウィンドウに登録されている Run Command および Run Command タスクがコマンドのステータスに関する通知を送信するために使用する通信チャネルです。Amazon SNS では、HTTP/S、E メールに加え、Amazon Simple Queue Service (Amazon SQS) のような AWS のサービスをサポートしています。開始するには、E メールプロトコルを使用して開始することをお勧めします。トピックの作成方法の詳細については、Amazon Simple Notification Service デベロッパーガイドの「Amazon SNS トピックの作成」を参照してください。

> **Note**
>
> トピックを作成した後に [Topic ARN (トピック ARN)] をコピー、または書き留めます。ステータスの通知を返すように設定されたコマンドを送信するときに、この ARN を指定します。

トピックを作成したら、[エンドポイント] を指定してサブスクライブします。E メールプロトコルを選択した場合、エンドポイントは、通知を受け取る E メールアドレスです。トピックにサブスクライブする方法の詳細については、Amazon Simple Notification Service デベロッパーガイドの「Amazon SNS トピックへのサブスクライブ」を参照してください。

Amazon SNS は、AWS通知の確認メールをお客様が指定した E メールアドレスに送信します。E メールを開き、[サブスクリプションを確認] へのリンクを選択します。

AWS からの確認メッセージが届きます。Amazon SNS は、通知を受信し、通知を E メールとして指定された E メールアドレスに送信するように設定されました。

タスク 2: Amazon SNS 通知用の IAM ポリシーを作成する

以下の手順を使用して、Amazon SNS 通知を開始するためのアクセス許可を提供するカスタム AWS Identity and Access Management (IAM) ポリシーを作成します。

Amazon SNS 通知用のカスタム IAM ポリシーを作成するには

1. https://console.aws.amazon.com/iam/ で IAM コンソール を開きます。
2. ナビゲーションペインで、Policies を選択し、Create Policy を選択します。([Get Started] ボタンが表示された場合は、そのボタンを選択してから、[Create Policy] を選択します)。

3. [JSON] タブを選択します。
4. Amazon SNS トピックが AWS KMS 暗号化を使用しているかどうかに応じて、デフォルトの内容を次のいずれかに置き換えます。

   SNS topic not encrypted

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sns:Publish"
            ],
            "Resource": "arn:aws:sns:region:account-id:sns-topic-name"
        }
    ]
}
```

   region は、米国東部 (オハイオ) リージョンの us-east-2 のように、AWS Systems Manager でサポートされている AWS リージョン の識別子を表します。サポートされている *region* 値の一覧については、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」にある Region 列を参照してください。

   account-id は、AWS アカウントの 12 桁の識別子を 123456789012 形式で表します。

   sns-topic-name は、通知の発行に使用する Amazon SNS トピックの名前を表します。

   SNS topic encrypted

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sns:Publish"
            ],
            "Resource": "arn:aws:sns:region:account-id:sns-topic-name"
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:region:account-id:key/kms-key-id"
        }
    ]
}
```

region は、米国東部 (オハイオ) リージョンの us-east-2 のように、AWS Systems Manager でサポートされている AWS リージョン の識別子を表します。サポートされている *region* 値の一覧については、「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスエンドポイント」にある Region 列を参照してください。

account-id は、AWS アカウントの 12 桁の識別子を 123456789012 形式で表します。

sns-topic-name は、通知の発行に使用する Amazon SNS トピックの名前を表します。

kms-key-id は、トピックの暗号化と復号に使用する AWS KMS の対称暗号化 KMS キーの ID を、1234abcd-12ab-34cd-56ef-12345EXAMPLE という形式で表しています。

> **Note**
>
> AWS KMS 暗号化の使用には料金がかかります。詳細については、「AWS Key Management Service デベロッパーガイド」の「Managing Amazon SNS encryption keys and costs」を参照してください。

5. [Next: Tags] (次へ: タグ) を選択します。
6. (オプション) 1 つ以上のタグキーと値のペアを追加して、このポリシーのアクセスを整理、追跡、または制御します。
7. [次へ: レビュー] を選択します。
8. [Review policy (ポリシーの確認)] ページで、[Name (名前)] にインラインポリシーの名前を入力します。例: **my-sns-publish-permissions**。
9. (オプション) [Description (説明)] に、ポリシーの説明を入力します。
10. [Create policy] を選択します。

タスク 3: Amazon SNS 通知の IAM ロールを作成する

Amazon SNS 通知の IAM ロールを作成するには、次の手順を使用します。このサービスロールは、Systems Manager で Amazon SNS 通知を開始するために使用されます。以降の手順では、このロールは Amazon SNS IAM ロールと呼ばれます。

Amazon SNS 通知の IAM サービスロールを作成するには

1. AWS Management Console にサインインして、IAM コンソール https://console.aws.amazon.com/iam/ を開きます。
2. IAM コンソールのナビゲーションペインで、[ロール]、[ロールを作成] を選択します。
3. [AWS のサービス]、[Systems Manager] の順にクリックします。
4. [Systems Manager のユースケース] を選択します。[次へ] を選択します。
5. [Attach permissions policies (アクセス許可ポリシーのアタッチ)] ページで、タスク 2 で作成したカスタムポリシーの名前の左側にあるチェックボックスをオンにします。例: **`my-sns-publish-permissions`**。
6. (オプション) アクセス許可の境界を設定します。このアドバンスド機能は、サービスロールで使用できますが、サービスにリンクされたロールではありません。

   [Permissions boundary] (アクセス許可の境界) セクションを展開し、[Use a permissions boundary to control the maximum role permissions] (アクセス許可の境界を使用して、ロールのアクセス許可の上限を設定する) を選択します。IAM には、あなたのアカウント内の AWS 管理ポリシーとカスタマー管理ポリシーのリストがあります。アクセス許可の境界に使用するポリシーを選択するか、[ポリシーを作成] を選択して新しいブラウザタブを開き、新しいポリシーをゼロから作成します。詳細については、『IAM ユーザーガイド』の「IAM ポリシーの作成」を参照してください。ポリシーを作成したら、そのタブを閉じて元のタブに戻り、アクセス許可の境界として使用するポリシーを選択します。
7. [次へ] を選択します。
8. 可能な場合は、このロールの目的を識別するのに役立つロール名またはロール名サフィックスを入力します。ロール名は AWS アカウント アカウント内で一意である必要があります。大文字と小文字は区別されません。例えば、**`PRODROLE`** と **`prodrole`** というロール名を両方作成することはできません。多くのエンティティによりロールが参照されるため、作成後にロール名を変更することはできません。
9. (オプション) [Description (説明)] には、新しいロールの説明を入力します。

10. [Step 1: Select trusted entities] (ステップ 1: 信頼済みエンティティの選択) または [Step 2: Select permissions] (ステップ 2: 権限の選択) のセクションで [Edit] (編集) を選択し、ロールのユースケースと権限を変更します。
11. (オプション) タグをキーバリューペアとしてアタッチして、メタデータをユーザーに追加します。IAM でのタグの使用に関する詳細については、「IAM ユーザーガイド」の「IAM リソースにタグを付ける」を参照してください。
12. ロール情報を確認し、ロールの作成 を選択します。
13. ロールの名前を選択してから、[Role ARN] (ロール ARN) 値をコピーまたはメモします。Amazon SNS 通知を返すように設定されたコマンドを送信するときに、ロールのこの Amazon リソースネーム (ARN) が使用されます。
14. [Summary (概要)] ページは開いたままにします。

タスク 4: ユーザーアクセスを設定する

IAM エンティティ (ユーザー、ロール、またはグループ) に管理者許可が割り当てられている場合、ユーザーまたはロールには Run Command と Maintenance Windows へのアクセスと AWS Systems Manager ツールが付与されます。

管理者許可のないエンティティの場合、管理者は IAM エンティティに次のアクセス許可を付与する必要があります。

- `AmazonSSMFullAccess` マネージドポリシー、または同等のアクセス許可を付与するポリシー。
- `iam:PassRole` で作成されたロールの タスク 3: Amazon SNS 通知の IAM ロールを作成する アクセス許可。例:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::account-id:role/sns-role-name"
        }
    ]
}
```

アクセス権限を付与するにはユーザー、グループ、またはロールにアクセス許可を追加します。

- AWS IAM Identity Center のユーザーとグループ:

  アクセス許可セットを作成します。「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」の手順に従ってください。
- IAM 内で、ID プロバイダーによって管理されているユーザー:

  ID フェデレーションのロールを作成します。詳細については「IAM ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) 用のロールを作成する」を参照してください。
- IAM ユーザー:
  - ユーザーが担当できるロールを作成します。手順については「IAM ユーザーガイド」の「IAM ユーザーのロールの作成」を参照してください。
  - (お奨めできない方法) ポリシーをユーザーに直接アタッチするか、ユーザーをユーザーグループに追加します。詳細については「IAM ユーザーガイド」の「ユーザー (コンソール) へのアクセス権限の追加」を参照してください。

ユーザーアクセスを設定し、**iam:PassRole** ポリシーをユーザーアカウントにアタッチするには

1. IAM のナビゲーションペインで、[ユーザー] を選択し、設定するユーザーアカウントを選択します。
2. [Permissions (アクセス許可)] タブのポリシーリストで、**AmazonSSMFullAccess** ポリシーがリストにあるか、またはアカウントに Systems Manager へのアクセス許可を与える同等のポリシーがあるかどうかを確認します。
3. [Add inline policy (インラインポリシーの追加)] を選択します。
4. [Create policy (ポリシーの作成)] ページの [Visual editor (ビジュアルエディタ)] タブを選択します。
5. [Choose a service (サービスの選択)] を選んでから、[IAM] を選択します。
6. [Actions] (アクション) の場合は、[Filter actions] (フィルタアクション) テキストボックスに「**PassRole**」を入力し、[PassRole] の横にあるチェックボックスを選択します。
7. [Resources (リソース)] の場合は、[Specific (固有)] が選択されていることを確認し、[Add ARN (ARN の追加)] を選択します。
8. [Specify ARN for role (ロールの ARN の指定)] フィールドに、タスク 3 の終わりでコピーした Amazon SNS IAM ロールの ARN を貼り付けます。システムによって、[アカウント] と [Role name with path (ロール名とパス)] フィールドが自動的に入力されます。

9. [Add] (追加) をクリックします。
10. [Review policy (ポリシーの確認)] を選択します。
11. [Review Policy] (ポリシーの確認) ページに名前を入力し、[Create Policy] (ポリシーの作成) を選択します。

タスク 5: iam:PassRole ポリシーをメンテナンスウィンドウロールにアタッチする

Run Command タスクをメンテナンスウィンドウに登録する場合、サービスロール Amazon リソースネーム (ARN) を指定します。このサービスロールは、メンテナンスウィンドウに登録されているタスクを実行するために Systems Manager によって使用されます。登録された Run Command タスクの Amazon SNS 通知を設定するには、指定されたメンテナンスウィンドウサービスロールに `iam:PassRole` ポリシーをアタッチします。登録されたタスクを Amazon SNS 通知に設定しない場合、このタスクはスキップしてください。

`iam:PassRole` ポリシーを使用すると、Maintenance Windows サービスロールは、タスク 3 で作成した Amazon SNS IAM ロールを Amazon SNS サービスに渡すことができます。次の手順は、`iam:PassRole` ポリシーを Maintenance Windows サービスロールにアタッチする方法を示しています。

> **Note**
>
> 登録された Run Command タスクに関連する通知を送信するには、メンテナンスウィンドウのカスタムサービスロールを使用します。詳細については、「Maintenance Windows を設定する」を参照してください。
> メンテナンスウィンドウのタスク用にカスタムサービスロールを作成する必要がある場合は、「Maintenance Windows を設定する」を参照してください。

`iam:PassRole` ポリシーを Maintenance Windows ロールにアタッチするには

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. ナビゲーションペインで [Roles (ロール)] を選択し、タスク 3 で作成した Amazon SNS IAM ロールを選択します。
3. [Role ARN (ロールの ARN)] をコピー、または書き留めて、IAM コンソールの[Roles (ロール)] セクションに戻ります。
4. [Role name] (ロール名) リストから、作成したカスタム Maintenance Windows のサービスロールを選択します。

5. [Permissions] (許可) タブで、AmazonSSMMaintenanceWindowRole ポリシーが一覧に表示されていること、または Systems Manager API に対するメンテナンスウィンドウの許可を与える同等のポリシーがあることを確認します。付与されていない場合は、[アクセス許可をアタッチ、ポリシーをアタッチ] をクリックして、アタッチします。
6. [Add permissions, Create inline policy] (アクセス許可の追加、インラインポリシーの作成) を選択します。
7. [Visual Editor (ビジュアルエディタ)] タブを選択します。
8. [Service (サービス)] で、[IAM] を選択します。
9. [Actions] (アクション) の場合は、[Filter actions] (フィルタアクション) テキストボックスに「**PassRole**」を入力し、[PassRole] の横にあるチェックボックスを選択します。
10. [Resources (リソース)] で、[Specific (特定)]、[Add ARN (ARN の追加)] の順に選択します。
11. [Specify ARN for role (ロールの ARN を指定)] ボックスで、タスク 3 で作成した Amazon SNS IAM ロールの ARN を貼り付けて、[Add (追加)] を選択します。
12. [ポリシーの確認] を選択します。
13. [ポリシーの確認] ページで PassRole ポリシーの名前を入力し、[ポリシーの作成] をクリックします。

AWS Systems Manager の Amazon SNS 通知の例

Amazon Simple Notification Service (Amazon SNS) を設定し、AWS Systems Manager のツールである Run Command または Maintenance Windows を使用して送信したコマンドのステータスに関する通知を送信できます。

> **Note**
>
> このガイドでは、Run Command または Maintenance Windows の通知を設定する方法は説明していません。Run Command または Maintenance Windows を設定してコマンドのステータスに関する Amazon SNS 通知を送信する方法については、「AWS Systems Manager の Amazon SNS 通知の設定」を参照してください。

次の例は、Run Command または Maintenance Windows に設定されている場合に Amazon SNS 通知によって返される JSON 出力の構造を示しています。

インスタンス ID ターゲティングを使用したコマンド概要メッセージの JSON 出力例

```
{
    "commandId": "a8c7e76f-15f1-4c33-9052-0123456789ab",
    "documentName": "AWS-RunPowerShellScript",
    "instanceIds": [
        "i-1234567890abcdef0",
        "i-9876543210abcdef0"
    ],
    "requestedDateTime": "2019-04-25T17:57:09.17Z",
    "expiresAfter": "2019-04-25T19:07:09.17Z",
    "outputS3BucketName": "amzn-s3-demo-bucket",
    "outputS3KeyPrefix": "runcommand",
    "status": "InProgress",
    "eventTime": "2019-04-25T17:57:09.236Z"
}
```

タグベースのターゲティングを使用したコマンド概要メッセージの JSON 出力例

```
{
    "commandId": "9e92c686-ddc7-4827-b040-0123456789ab",
    "documentName": "AWS-RunPowerShellScript",
    "instanceIds": [],
    "requestedDateTime": "2019-04-25T18:01:03.888Z",
    "expiresAfter": "2019-04-25T19:11:03.888Z",
    "outputS3BucketName": "",
    "outputS3KeyPrefix": "",
    "status": "InProgress",
    "eventTime": "2019-04-25T18:01:05.825Z"
}
```

呼び出しメッセージの JSON 出力例

```
{
    "commandId": "ceb96b84-16aa-4540-91e3-925a9a278b8c",
    "documentName": "AWS-RunPowerShellScript",
    "instanceId": "i-1234567890abcdef0",
    "requestedDateTime": "2019-04-25T18:06:05.032Z",
    "status": "InProgress",
    "eventTime": "2019-04-25T18:06:05.099Z"
}
```

Run Command を使用してステータス通知を返すコマンドを送信する

以下の手順は、AWS Command Line Interface (AWS CLI) または AWS Systems Manager コンソールを使用し、ステータス通知を返すように設定されている Run Command (AWS Systems Manager のツール) 経由でコマンドを送信する方法を示しています。

通知を返す Run Command の送信 (コンソール)

Systems Manager コンソールを使用してステータス通知を返すように設定されているコマンドを Run Command 経由で送信するには、以下の手順を使用します。

通知を返すコマンドを送信するには (コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Run Command] を選択します。
3. [Run command (コマンドの実行)] を選択します。
4. [Command document] リストで、Systems Manager ドキュメントを選択します。
5. [Command parameters] セクションで、必須パラメータの値を指定します。
6. [Targets] (ターゲット) セクションで、タグの指定、インスタンスやエッジデバイスの手動選択、リソースグループの指定により、このオペレーションを実行するマネージドノードを選択します。

   > **Tip**
   >
   > 表示されるはずのマネージドノードが表示されない場合は、トラブルシューティングのヒントについて「マネージドノードの可用性のトラブルシューティング」を参照してください。

7. [その他のパラメータ] で、以下の操作を行います。
   - [コメント] に、このコマンドに関する情報を入力します。
   - [タイムアウト (秒)] に、コマンドの実行全体が失敗するまでにシステムが待機する秒数を指定します。
8. [レート制御] の場合:
   - [同時実行数] の場合、コマンドを同時に実行するマネージドノードの数または割合を指定します。

> **Note**
>
> マネージドノードに適用されるタグを指定するか、AWS リソースグループを指定してターゲットを選択し、ターゲットとなるマネージドノードの数が不明な場合は、割合を指定してドキュメントを同時に実行できるターゲットの数を制限します。

- [エラーのしきい値] で、ノードの数または割合のいずれかで失敗した後、他のマネージドノードでのコマンドの実行をいつ停止するか指定します。例えば、3 つのエラーを指定した場合、4 番目のエラーが受信されると、システムマネージャー はコマンドの送信を停止します。コマンドを処理しているマネージドノードもエラーを送信する可能性があります。

9. (オプション) コマンド出力をファイルに保存する場合は、[出力オプション] の [S3 バケットにコマンド出力を書き込む] ボックスを選択します。ボックスにバケット名とプレフィックス (フォルダ) 名を入力します。

> **Note**
>
> S3 バケットにデータを書き込む機能を許可する S3 許可は、このタスクを実行する IAM ユーザーのものではなく、インスタンスに割り当てられたインスタンスプロファイル (EC2 インスタンスの場合) または IAM サービスロール (ハイブリッドアクティベーションマシン) のものです。詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」または「ハイブリッド環境に IAM サービスロールを作成する」を参照してください。さらに、指定された S3 バケットが別の AWS アカウント にある場合は、マネージドノードに関連付けられたインスタンスプロファイルまたは IAM サービスロールが、そのバケットへの書き込みに必要なアクセス許可があることを確認してください。

10. [SNS Notifications (SNS 通知)] セクションで、[Enable SNS notifications (SNS 通知の有効化)] を選択します。
11. [IAM role] (IAM ロール) で、Amazon SNS 通知を使用した Systems Manager のステータス変更のモニタリング のタスク 3 で作成した Amazon SNS IAM ロール ARN を選択します。
12. [SNS topic (SNS トピック)] では、使用する Amazon SNS トピック ARN を入力します。
13. [Event notifications (イベント通知)] の場合は、通知を受け取るイベントを選択します。
14. [Change notifications] (変更通知) で、コマンドの概要のみ ([Command status changes] (コマンドステータスの変更)) または複数のノードに送信されたコマンドの各コピー ([Command status

on each instance changes] (各インスタンスのコマンドステータスの変更)) の通知を受信するように選択します。

15. [Run (実行)] を選択します。
16. Amazon SNS からのメッセージが E メールされていることを確認し、E メールを開きます。Amazon SNS では、E メールメッセージの送信に数分かかる場合があります。

通知を返す Run Command の送信 (CLI)

次の手順を使用して、AWS CLI を使用してステータス通知を返すように設定されたコマンドを Run Command 経由で送信します。

通知を返すコマンドを送信するには (CLI)

1. AWS CLI を開きます。
2. 以下のコマンドで、マネージドインスタンス ID に基づいてターゲットとなるパラメータを指定します。

```
aws ssm send-command --instance-ids "ID-1, ID-2" --document-name "Name"
 --parameters '{"commands":["input"]}' --service-role "SNSRoleARN" --
notification-config '{"NotificationArn":"SNSTopicName","NotificationEvents":
["All"],"NotificationType":"Command"}'
```

次に例を示します。

```
aws ssm send-command --instance-ids "i-02573cafcfEXAMPLE, i-0471e04240EXAMPLE"
 --document-name "AWS-RunPowerShellScript" --parameters '{"commands":
["Get-Process"]}' --service-role "arn:aws:iam::111122223333:role/
SNS_Role" --notification-config '{"NotificationArn":"arn:aws:sns:us-
east-1:111122223333:SNSTopic","NotificationEvents":
["All"],"NotificationType":"Command"}'
```

代替コマンド

タグを使用してマネージドインスタンスをターゲットにするには、以下のコマンドでパラメータを指定します。

```
aws ssm send-command --targets "Key=tag:TagName,Values=TagKey" --document-name
 "Name" --parameters '{"commands":["input"]}' --service-role "SNSRoleARN" --
```

```
notification-config '{"NotificationArn":"SNSTopicName","NotificationEvents":
["All"],"NotificationType":"Command"}'
```

次に例を示します。

```
aws ssm send-command --targets "Key=tag:Environment,Values=Dev" --
document-name "AWS-RunPowerShellScript" --parameters '{"commands":
["Get-Process"]}' --service-role "arn:aws:iam::111122223333:role/
SNS_Role" --notification-config '{"NotificationArn":"arn:aws:sns:us-
east-1:111122223333:SNSTopic","NotificationEvents":
["All"],"NotificationType":"Command"}'
```

3. [Enter] キーを押します。
4. Amazon SNS からのメッセージが E メールされていることを確認し、E メールを開きます。Amazon SNS では、E メールメッセージの送信に数分かかる場合があります。

詳細については、AWS CLI コマンドリファレンスの send-command を参照してください。

メンテナンスウィンドウを使用して、ステータス通知を返すコマンドを送信する

以下の手順は、AWS Systems Manager コンソールまたは AWS Command Line Interface (AWS CLI) を使用して、メンテナンスウィンドウで Run Command タスクを登録する方法を示しています。Run Command は AWS Systems Manager のツールです。この手順では、ステータス通知を返すように Run Command タスクを設定する方法についても説明します。

[開始する前に]

メンテナンスウィンドウを作成していない、またはターゲットを登録していない場合は、メンテナンスウィンドウを作成してターゲットを登録する方法の手順について、「コンソールを使用してメンテナンスウィンドウを作成および管理する」を参照してください。

Amazon Simple Notification Service (Amazon SNS) サービスから通知を受け取るには、登録されたタスクで指定された Maintenance Windows サービスロールに `iam:PassRole` ポリシーをアタッチします。Maintenance Windows サービスローに `iam:PassRole` アクセス許可を追加していない場合は、「タスク 5: iam:PassRole ポリシーをメンテナンスウィンドウロールにアタッチする」を参照してください。

通知を返す Run Command タスクをメンテナンスウィンドウに登録する (コンソール)

以下の手順で、Systems Manager コンソールを使用してステータス通知をメンテナンスウィンドウに返すように設定されている Run Command タスクを登録します。

通知を返す Run Command タスクをメンテナンスウィンドウに登録するには (コンソール)

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Maintenance Windows] を選択します。
3. Amazon Simple Notification Service (Amazon SNS) 通知を送信するように設定された Run Command タスクを登録するメンテナンスウィンドウを選択します。
4. [Actions (アクション)] を選択し、[Register Run command task (Run command タスクの登録)] を選択します。
5. (オプション) [Name (名前)] フィールドにタスクの名前を入力します。
6. (オプション) [Description (説明)] にリポジトリの説明を入力します。
7. [Command document] (コマンドドキュメント) で、コマンドドキュメントを選択します。
8. [タスクの優先順位] で、このタスクの優先度を指定します。ゼロ (0) が最高の優先度になります。メンテナンスウィンドウのタスクは、優先順位に従ってスケジュールされます。優先度が同じタスクは並行してスケジュールされます。
9. [Targets (ターゲット)] セクションで登録済みのターゲット グループを選択するか、未登録のターゲットを選択します。
10. [レート制御] の場合:

    - [同時実行数] の場合、コマンドを同時に実行するマネージドノードの数または割合を指定します。

      > **Note**
      >
      > マネージドノードに適用されるタグを指定するか、AWS リソースグループを指定してターゲットを選択し、ターゲットとなるマネージドノードの数が不明な場合は、割合を指定してドキュメントを同時に実行できるターゲットの数を制限します。

    - [エラーのしきい値] で、ノードの数または割合のいずれかで失敗した後、他のマネージドノードでのコマンドの実行をいつ停止するか指定します。例えば、3 つのエラーを指定した

場合、4 番目のエラーが受信されると、システムマネージャー はコマンドの送信を停止します。コマンドを処理しているマネージドノードもエラーを送信する可能性があります。

11. [IAM service role (IAM サービスロール)] 領域で、SNS ロールへの `iam:PassRole` アクセス許可を持つ Maintenance Windows サービスを選択します。

> **Note**
>
> `iam:PassRole` アクセス許可を Maintenance Windows ロールに追加すると、Systems Manager は SNS ロールを Amazon SNS に渡せるようになります。`iam:PassRole` アクセス許可を追加していない場合は、トピック Amazon SNS 通知を使用した Systems Manager のステータス変更のモニタリング の「タスク 5」を参照してください。

12. (オプション) [出力オプション] で、コマンド出力をファイルに保存するには、[S3 への出力の書き込みを有効にします] ボックスをオンにします。ボックスにバケット名とプレフィックス (フォルダ) 名を入力してください。

> **Note**
>
> S3 バケットにデータを書き込む機能を許可する S3 アクセス許可は、このタスクを実行する IAM ユーザーのものではなく、マネージドノードに割り当てられたインスタンスプロファイルのものです。詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」または「ハイブリッド環境に IAM サービスロールを作成する」を参照してください。さらに、指定された S3 バケットが別の AWS アカウント にある場合は、マネージドノードに関連付けられたインスタンスプロファイルまたは IAM サービスロールに、そのバケットへの書き込みに必要なアクセス許可があることを確認してください。

13. [SNS notifications (SNS 通知)] セクションで、以下を実行します。

- [Enable SNS Notifications (SNS 通知を有効にする)] を選択します。
- [IAM role (IAM ロール)] では、Amazon SNS 通知を使用した Systems Manager のステータス変更のモニタリング のタスク 3 で作成した Amazon SNS IAM ロール Amazon リソースネーム (ARN) を選択して、Amazon SNS を開始します。
- [SNS topic (SNS トピック)] では、使用する Amazon SNS トピック ARN を入力します。
- [Event type (イベントのタイプ)] では、通知を受け取るイベントを選択します。
- [Notification type] (通知のタイプ) の場合は、複数のインスタンス (呼び出し) またはコマンドの概要に送信されたコマンドの各コピーの通知を受け取るよう選択します。

14. [Parameters (パラメータ)] セクションで、選択したコマンドドキュメントに基づいて必要なパラメータを入力します。
15. [Register Run command task (Run command タスクの登録)] を選択します。
16. メンテナンスウィンドウを次回実行した後、E メールで Amazon SNS からのメッセージを確認し、Eメールを開いてください。Amazon SNS では、E メールメッセージの送信に数分かかる場合があります。

通知を返す Run Command タスクをメンテナンスウィンドウに登録 (CLI)

AWS CLI を使用してステータス通知をメンテナンスウィンドウに返すように設定されている Run Command タスクを登録するには、次の手順を使用します。

通知を返す Run Command タスクをメンテナンスウィンドウに登録するには (CLI)

> **Note**
>
> タスクオプションをより効率的に管理するために、この手順ではコマンドオプション `--cli-input-json` を使用します。オプション値は、JSON ファイルに保存されています。

1. ローカルマシンで、`RunCommandTask.json` という名前のファイルを作成します。
2. ファイルに次の内容を貼り付けます。

```
{
    "Name": "Name",
    "Description": "Description",
    "WindowId": "mw-0c50858d01EXAMPLE",
    "ServiceRoleArn": "arn:aws:iam::account-id:role/MaintenanceWindowIAMRole",
    "MaxConcurrency": "1",
    "MaxErrors": "1",
    "Priority": 3,
    "Targets": [
        {
            "Key": "WindowTargetIds",
            "Values": [
                "e32eecb2-646c-4f4b-8ed1-205fbEXAMPLE"
            ]
        }
    ],
```

```
    "TaskType": "RUN_COMMAND",
    "TaskArn": "CommandDocumentName",
    "TaskInvocationParameters": {
        "RunCommand": {
            "Comment": "Comment",
            "TimeoutSeconds": 3600,
            "NotificationConfig": {
                "NotificationArn": "arn:aws:sns:region:account-id:SNSTopicName",
                "NotificationEvents": [
                    "All"
                ],
                "NotificationType": "Command"
            },
            "ServiceRoleArn": "arn:aws:iam::account-id:role/SNSIAMRole"
        }
    }
}
```

3. サンプル値を自分のリソースの情報に置き換えます。

   この例で省略されているオプションを使用する場合は、復元することもできます。たとえば、コマンドの出力を S3 バケットに保存することができます。

   詳細については、AWS CLI コマンドリファレンスの「register-task-with-maintenance-window」を参照してください。

4. ファイルを保存します。
5. ファイルを保存したローカルマシン上のディレクトリで、次のコマンドを実行します。

```
aws ssm register-task-with-maintenance-window --cli-input-json file://
RunCommandTask.json
```

> **Important**
>
> ファイル名の前に必ず `file://` を含めてください。このコマンドでは必須です。

成功した場合、このコマンドは次のような情報を返します。

```
{
    "WindowTaskId": "j2l8d5b5c-mw66-tk4d-r3g9-1d4d1EXAMPLE"
}
```

6. メンテナンスウィンドウを次に実行した後、E メールで Amazon SNS からのメッセージを確認し、Eメールを開いてください。Amazon SNS では、E メールメッセージの送信に数分かかる場合があります。

コマンドラインからメンテナンスウィンドウのタスクを登録する方法の詳細については、「メンテナンスウィンドウにタスクを登録する」を参照してください。

Systems Manager との製品およびサービスの統合

デフォルトで、AWS Systems Manager は AWS のサービスおよびその他の製品やサービスと統合されます。以下の情報は、使用する製品やサービスを統合するための Systems Manager の設定に役立ちます。

- AWS のサービス との統合
- その他の製品やサービスとの統合

AWS のサービス との統合

Systems Manager コマンドドキュメント (SSM ドキュメント) と Automation ランブックを使用すると、AWS Systems Manager を利用して AWS のサービスと統合できます。これらのリソースの詳細については、「AWS Systems Manager ドキュメント」を参照してください。

Systems Manager は、以下の AWS のサービスと統合されています。

コンピューティング

Amazon Elastic Compute Cloud (Amazon EC2)	Amazon EC2 は、AWS クラウド でスケーラブルなコンピューティング能力を提供します。Amazon EC2 の使用により、ハードウェアに事前投資する必要がなくなり、アプリケーションをより速く開発およびデプロイできます。Amazon EC2 を使用すると、必要な数 (またはそれ以下) の仮想サーバーの起動、セキュリティおよびネットワーキングの構成、ストレージの管理ができます。 Systems Manager により、EC2 インスタンスでいくつものタスクを実行できます。例えば、EC2 インスタンスを起動、設定、管理、保守、トラブルシューティングしたり、安全に接続したりできます。Systems Manager を使用して、ソフトウェアのデプロイ、コンプライアン

	スステータスの判定、EC2 インスタンスからのインベントリの収集を行うこともできます。 詳細はこちら • マネージドノードの使用 • AWS Systems Manager State Manager • AWS Systems Manager Run Command • AWS Systems Manager Patch Manager • AWS Systems Manager Session Manager • AWS Systems Manager Distributor • AWS Systems Manager のコンプライアンス • AWS Systems Manager インベントリ
Amazon EC2 Auto Scaling (日本語)	Auto Scaling によって、アプリケーションの負荷を処理するために適切な数の EC2 インスタンスを利用できるように準備することができます。Auto Scaling グループと呼ばれる EC2 インスタンスの集合を作成します。 Systems Manager を使用すると、Auto Scaling グループの Auto Scaling テンプレートで使用される Amazon Machine Image (AMI) へのパッチ適用など、一般的な手順を自動化できます。 詳細はこちら Auto Scaling グループ用の AMIs の更新

Amazon Elastic Container Service (Amazon ECS)	Amazon ECS は、クラスターで Docker コンテナを実行、停止、管理できる非常にスケーラブルで高速なコンテナ管理サービスです。 Systems Manager では、Systems Manager のツールである Parameter Store のパラメータに機密データを保存してコンテナの定義でそれを参照することによって、リモートでコンテナインスタンスを管理し、コンテナに機密データを挿入できます。 詳細はこちら • AWS Systems Manager を使用してコンテナインスタンスをリモート管理する • Systems Manager Parameter Store を使用して機密データを指定する

AWS Lambda	Lambda はサーバーをプロビジョニングしたり管理しなくてもコードを実行できるコンピューティングサービスです。Lambda は必要に応じてコードを実行し、1 日あたり数個のリクエストから 1 秒あたり数千のリクエストまで自動的にスケールします。 Systems Manager では、`aws:invokeLambdaFunction` アクションを使用して、オートメーションランブックのコンテンツ内で Lambda 関数を使用できます。 AWS Lambda 関数内の Parameter Store からパラメーターを使用するには、AWS Parameters and Secrets Lambda Extension を使用してパラメーター値を取得し、今後使用できるようにキャッシュすることができます。 詳細はこちら Automation、AWS Lambda、Parameter Store を使用してゴールデン AMI を更新する AWS Lambda 関数での Parameter Store パラメーターの使用

IoT

AWS IoT Greengrass コアデバイス	AWS IoT Greengrass は、デバイス上で IoT アプリケーションを構築、デプロイ、管理するのに役立つオープンソースの IoT エッジランタイムおよびクラウドサービスです。Systems Manager は AWS IoT Greengrass コアデバイスをネイティブでサポートします。 詳細はこちら

	Systems Manager を利用したエッジデバイスの管理
AWS IoT コアデバイス	AWS IoT は、IoT デバイスを他のデバイスおよび AWS クラウドサービスに接続するクラウドサービスを提供します。AWS IoT は、IoT デバイスを AWS IoT ベースのソリューションに統合するのに役立つデバイスソフトウェアを提供します。デバイスが AWS IoT に接続できる場合、AWS IoT は それらデバイスをAWS が提供するクラウドサービスに接続できます。Systems Manager は AWS IoT コアデバイスをサポートしますが、これらのデバイスがハイブリッドおよびマルチクラウド環境でマネージドノードとして設定されている必要があります。 詳細はこちら Systems Manager を利用したハイブリッド環境およびマルチクラウド環境でのノードの管理

[Storage (ストレージ)]

Amazon Simple Storage Service (Amazon S3)	Amazon S3 はインターネット用のストレージサービスです。また、ウェブスケールのコンピューティングをデベロッパーが簡単に利用できるよう設計されています。Amazon S3 のウェブサービスインターフェイスはシンプルで、いつでも、ウェブのどこからでも容量に関係なくデータを格納および取得できます。 Systems Manager では、Amazon S3 に保存されているリモートスクリプトと SSM ドキュメントを実行できます。AWS Systems Manager のツールである Distributor は Amazon S3 を使用してパッケージを保存します。ま

	た、AWS Systems Manager のツールである Run Command と Session Manager の出力を Amazon S3 に送信することもできます。 詳細はこちら • Amazon S3 からのスクリプトの実行 • 遠隔で ドキュメントを実行する • AWS Systems Manager Distributor • Amazon S3 を使用してセッションデータをログ記録する (コンソール)

開発者用ツール

AWS CodeBuild	CodeBuild とは、クラウド上のフルマネージドビルドサービスです。CodeBuild はソースコードをコンパイルし、単体テストを実行して、すぐにデプロイできるアーティファクトを生成します。CodeBuild では自分のビルドサーバーをプロビジョニング、管理、スケールする必要がありません。 Parameter Store を使用すると、ビルド仕様およびプロジェクトの機密情報を保存できます。 詳細はこちら • CodeBuild のビルド仕様に関するリファレンス • AWS CodeBuild でのビルドプロジェクトの作成
AWS CDK	AWS Cloud Development Kit (AWS CDK) は、クラウドインフラストラクチャをプログラミング言語を含むコードとして定義し、AWS

	CloudFormation を介してデプロイするためのフレームワークです。 Application Manager により、Application Manager コンソールでアプリケーションとしてグループ化された CDK コンストラクトを表示したり、基盤となるリソースを含むアプリケーション構造を表示したり、アラートを表示したり、運用上の問題を調査および修正したり、コストを追跡したりできます。 詳細はこちら • アプリケーションの概要情報を表示する • アプリケーションリソースの表示

セキュリティ、アイデンティティ、およびコンプライアンス

AWS Identity and Access Management (IAM)	IAM は、AWS リソースへのアクセスを安全に管理するためのウェブサービスです。IAM により、誰を認証 (サインイン) し、誰にリソースの使用を承認する (アクセス権限を持たせる) かを制御します。 Systems Manager により、IAM を使用してサービスへのアクセスを制御できます。 詳細はこちら • AWS Systems Manager と IAM の連携方法 • AWS Systems Manager のアクション、リソース、条件キー • Systems Manager に必要なインスタンスのアクセス許可を設定する
AWS Secrets Manager	Secrets Manager では、シークレットの管理を簡単に行えます。シークレットとは、データ

	ベース認証情報、パスワード、サードパーティーの API キーなどの任意のテキストです。 Parameter Store を使用すると、Parameter Store パラメータへの参照が既にサポートされている他の AWS のサービスを使用する際に、Secrets Manager のシークレットを取得できます。 詳細はこちら Parameter Store パラメータからの AWS Secrets Manager シークレットの参照

AWS Security Hub	Security Hub では、AWS アカウント 全体で高優先度のセキュリティアラートとコンプライアンス状況を包括的に確認できます。Security Hub は、複数の AWS のサービスからセキュリティアラート (検出結果) を集計、整理、優先順位付けします。 AWS Systems Manager のツールである Security Hub と Patch Manager の統合を有効にすると、Security Hub はセキュリティの観点からフリートのパッチ適用ステータスをモニタリングできます。パッチコンプライアンスの詳細は Security Hub に自動的にエクスポートされます。これにより、単一のビューを使用して、パッチのコンプライアンス状態を一元的に監視し、その他のセキュリティ調査結果を追跡できます。フリート内のノードがパッチコンプライアンスから外れたときにアラートを受け取り、Security Hub コンソールでパッチコンプライアンス結果を確認できます。 Security Hub は、AWS Systems Manager のツールである Explorer および OpsCenter と統合することも可能です。Security Hub との統合により、Explorer と OpsCenter で Security Hub から検出結果を受け取ることができます。Security Hub の検出結果は、Explorer と OpsCenter で使用できるセキュリティ情報を提供します。この情報を使用して、AWS Systems Manager のセキュリティ、パフォーマンス、および運用上の問題を集計し、アクションを実行できます。 Security Hub の使用には料金が発生します。詳細については、「Security Hub の料金」をご覧ください。

	詳細はこちら • Explorer の AWS Security Hub から結果を受け取る • OpsCenter と AWS Security Hub の統合について • Patch Managerと AWS Security Hub の統合

暗号化と PKI

AWS Key Management Service (AWS KMS)	AWS KMS は、データの暗号化に使用される暗号化キーであるカスタマーマネージドキー (CMK) の作成と管理を可能にするマネージド型サービスです。 Systems Manager では、AWS KMS を使用して `SecureString` パラメータを作成し、Session Manager セッションデータを暗号化できます。 詳細はこちら • AWS Systems ManagerParameter Store SecureString パラメータの AWS KMS 暗号化 • セッションデータの KMS キー暗号化を有効にする (コンソール)

マネジメントとガバナンス

AWS CloudFormation	AWS CloudFormation は Amazon Web Services リソースのモデル化およびセットアップに役立つサービスです。リソース管理に割く時間を減らし、AWS で実行するアプリケーションにより注力できるようになります。

	Parameter Store は動的参照のソースです。動的なリファレンスでは、他のサービスに格納および管理されている外部値を AWS CloudFormation スタックテンプレートに指定するためのコンパクトで強力な方法が提供されます。 詳細はこちら 動的な参照を使用してテンプレート値を指定する
AWS CloudTrail	CloudTrail は、AWS アカウント のガバナンス、コンプライアンス、および運用とリスクの監査を行えるように認可する AWS のサービスです。ユーザー、ロール、または AWS のサービスによって実行されたアクションは、CloudTrail にイベントとして記録されます。イベントには、AWS Management Console、AWS Command Line Interface (AWS CLI)、および AWS SDK と API で実行されたアクションが含まれます。 Systems Manager は CloudTrail と統合されており、ほとんどの Systems Manager API コールをイベントとしてキャプチャします。この対象には、Systems Manager コンソールから開始される API コールや、 Systems Manager API コールが含まれています。 詳細はこちら AWS Systems Manager による AWS CloudTrail API コールのログ記録

Amazon CloudWatch Logs	Amazon CloudWatch Logs により、使用中のすべてのシステム、アプリケーション、AWS のサービスからのログを、一元管理することができます。これにより、ログを表示したり、特定のエラーコードやパターンを検索したり、特定のフィールドに基づいてフィルタリングしたり、将来の分析のために安全にアーカイブしたりできます。 Systems Manager では、SSM Agent、Run Command、Session Manager のログを CloudWatch Logs に送信できます。 詳細はこちら • 統合された CloudWatch Logs へのノードログの送信 (CloudWatch エージェント) • Run Command の Amazon CloudWatch Logs の設定 • Amazon CloudWatch Logs を使用してセッションデータを log 記録する (コンソール)

Amazon EventBridge	EventBridge は、Amazon Web Services リソースの変更を示すシステムイベントのほぼリアルタイムのストリームを提供します。すぐに設定できる簡単なルールを使用して、ルールに一致したイベントを 1 つ以上のターゲット関数またはストリームに振り分けることができます。オペレーションの変更が発生すると、EventBridge はその変更を認識します。EventBridge は、これらのオペレーション上の変更に応答し、必要に応じて是正措置を講じます。これらのアクションには、環境に応答するメッセージの送信、機能のアクティブ化、状態情報のキャプチャが含まれます。 Systems Manager には、これらのイベントの内容に基づいてアクションを実行できるようにすることで、EventBridge でサポートされる複数のイベントがあります。 詳細はこちら Amazon EventBridge を使用して Systems Manager イベントをモニタリングする **Note** イベントを管理するには、Amazon EventBridge が好ましい方法です。CloudWatch Events と EventBridge は同じ基盤となるサービスと API ですが、EventBridge はより多くの機能を提供します。CloudWatch または EventBridge のいずれかで行った変更は、各コンソールに反映されます。詳細については、「Amazon EventBrid

	ge ユーザーガイド」を参照してください。
AWS Config	AWS Config は、AWS アカウント にある AWS リソースの設定詳細ビューを提供します。これには、リソースがどのように相互に関連しているかと、それらの構成方法が含まれます。これにより、構成と関係が時間の経過とともにどのように変化するかを確認できます。 Systems Manager は AWS Config と統合されており、EC2 インスタンスを可視化するのに役立つ複数のルールを提供します。これらのルールは、Systems Manager が管理する EC2 インスタンス、オペレーティングシステム構成、システムレベルの更新、インストールされているアプリケーション、ネットワーク設定などを特定するのに役立ちます。 詳細はこちら • AWS Config がサポートしているリソースタイプ • マネージドインスタンスのソフトウェア設定の記録 • インベントリ履歴と変更の追跡の表示

AWS Trusted Advisor	Trusted Advisor はリアルタイムのガイダンスを提供し、AWS のベストプラクティス通りにリソースをプロビジョニングするのに役立つオンラインツールです。 Systems Manager は Trusted Advisor をホストし、Explorer で Trusted Advisor データを表示できます。 詳細はこちら • AWS Systems Manager Explorer • AWS Trusted Advisor の開始方法

AWS Organizations	Organizations は、複数の AWS アカウントを、お客様が作成して集中管理する組織に統合できるようにする、アカウント管理サービスです。Organizations には、お客様のビジネスの予算、セキュリティ、コンプライアンスのニーズをより適切に満たせるように一括請求 (コンソリデーティッドビリング) およびアカウント管理機能が備わっています。 AWS Systems Manager のツールである Change Manager と組織の統合により、委任された管理者アカウントを使用して、この単一のアカウントを通じて組織全体の変更要求、変更テンプレート、および承認を管理できます。 Organizations と、AWS Systems Manager のツールである Inventory、および Explorer を統合すると、複数の AWS リージョンおよび AWS アカウントからインベントリとオペレーションデータ (OpsData) を集計できます。 AWS Systems Manager のツールである Quick Setup、および Organizations の統合により、一般的なサービスセットアップタスクが自動化され、組織単位 (OU) 全体のベストプラクティスに基づいてサービス設定がデプロイされます。

ネットワークとコンテンツ配信

AWS PrivateLink	AWS PrivateLink により、Virtual Private Cloud (VPC) をサポート対象の AWS のサービスや VPC エンドポイントサービスに VPC をプライベートに接続できます。インターネットゲートウェイ、NAT デバイス、VPN 接続、および AWS Direct Connect 接続は必要ありません。

	Systems Manager は、AWS PrivateLink を使用してSystems Manager API に接続するマネージドノードをサポートします。AWS PrivateLink は、マネージドノード、Systems Manager、および Amazon EC2 間のすべてのネットワークトラフィックを Amazon ネットワークに制限するため、マネージドノードのセキュリティ体制が向上します。つまり、マネージドノードはインターネットにアクセスする必要はありません。 詳細はこちら Systems Manager のために VPC エンドポイントを使用して EC2 インスタンスのセキュリティを強化する

分析

Amazon Athena	Athena は、標準 SQL を使用して Amazon Simple Storage Service (Amazon S3) 内のデータを直接分析できるようにするインタラクティブなクエリサービスです。AWS Management Console でいくつかのアクションを実行するだけで、Athena にデータの保存先の Amazon S3 を設定し、標準 SQL を使用してワンタイムクエリの実行を開始できます。結果は数秒で返されます。 Systems Manager Inventory は Athena と統合されており、複数の AWS リージョン および AWS アカウント からのインベントリデータのクエリに役立ちます。Athena 統合では、リソースデータ同期が使用されるため、Systems Manager のインベントリコンソールの [詳細

	ビュー] ページで、すべてのマネージドノードのインベントリデータを表示できます。 詳細はこちら • 複数のリージョンとアカウントからのインベントリデータをクエリする • チュートリアル: リソースデータの同期を使用してインベントリデータを集計する
AWS Glue	AWS Glue は、簡単でコスト効果の高い方法でデータの分類、クリーニング、エンリッチ、信頼性の高い方法でのデータストアおよびデータストリームへの移動が可能な、完全マネージド型 ETL (抽出、変換、ロード) サービスです。 Systems Manager は AWS Glue を使用して S3 バケット内の Inventory データをクロールします。 詳細はこちら 複数のリージョンとアカウントからのインベントリデータをクエリする

Amazon QuickSight	QuickSight は、視覚化の構築、ワンタイム分析の実行、データからのビジネス上の洞察の取得に使用できるビジネス分析サービスです。AWS データソースを自動的に検出でき、お客様のデータソースにも使用できます。 Systems Manager のリソースデータの同期によって、すべてのマネージドノードから収集されたインベントリデータが 1 つの Amazon S3 バケットに送信されます。QuickSight を使用して、集計データをクエリおよび分析できます。 詳細はこちら • インベントリのリソースデータ同期を作成する • チュートリアル: リソースデータの同期を使用してインベントリデータを集計する

アプリケーション統合

Amazon Simple Notification Service (Amazon SNS)	Amazon SNS は、サブスクライブしているエンドポイントまたはクライアントへのメッセージの配信または送信を、調整および管理するウェブサービスです。 Systems Manager は、Amazon SNS 通知によって取得できる複数のサービスのステータスを生成します。 詳細はこちら • Amazon SNS 通知を使用した Systems Manager のステータス変更のモニタリング • Parameter Store イベントに基づいた通知の設定またはアクションのトリガー

AWS Management Console

AWS Resource Groups	Resource Groups は、AWS リソースを整理します。リソースグループを使用すると、多数のリソース上のタスクを一度に管理、監視、自動化しやすくなります。 マネージドノード、SSM ドキュメント、メンテナンスウィンドウ、Parameter Store パラメータ、パッチベースラインなど Systems Managerのリソースタイプをリソースグループに追加できます。 詳細はこちら AWS Resource Groups とは

トピック

- Amazon S3 からのスクリプトの実行
- Parameter Store パラメータからの AWS Secrets Manager シークレットの参照
- AWS Systems ManagerParameter Store SecureString パラメータの AWS KMS 暗号化
- Amazon Elastic Kubernetes Service での Parameter Store パラメータの使用
- AWS Lambda 関数での Parameter Store パラメーターの使用

Amazon S3 からのスクリプトの実行

このセクションでは、Amazon Simple Storage Service (Amazon S3) からスクリプトをダウンロードして実行する方法について説明します。以下のトピックでは、Amazon S3 に関する情報と用語について説明します。Amazon S3 の詳細については、「Amazon S3 とは」を参照してください。Ansible Playbooks、Python、Ruby、Shell、PowerShell など、さまざまな種類のスクリプトを実行できます。

複数のスクリプトを含むディレクトリをダウンロードすることもできます。ディレクトリ内でプライマリスクリプトを実行すると、AWS Systems Manager はディレクトリに含まれている参照されるスクリプトも実行します。

Amazon S3 からのスクリプトの実行に関する以下の重要な詳細をメモします。

- Systems Manager は、スクリプトがノードで実行できるかどうかを検証しません。スクリプトをダウンロードして実行する前に、必要なソフトウェアがノードにインストールされていることを確認してください。または、複合ドキュメントを作成することで、Run Command か、AWS Systems Manager のツールである State Manager のいずれかを使用してソフトウェアをインストールし、さらにスクリプトをダウンロードして実行することができます。
- ユーザー、ロール、またはグループに、S3 バケットからの読み取りに必要な AWS Identity and Access Management (IAM) アクセス許可が付与されていることを確認します。
- Amazon Elastic Compute Cloud (Amazon EC2) インスタンス上のインスタンスプロファイルに、`s3:ListBucket` および `s3:GetObject` アクセス許可があることを確認します。インスタンスプロファイルにこれらのアクセス許可がない場合、システムは S3 バケットからのスクリプトのダウンロードに失敗します。詳細については、IAM ユーザーガイドの「インスタンスプロファイルの使用」を参照してください。

Amazon S3 からシェルスクリプトを実行する

以下に、AWS Systems Manager コンソールまたは AWS Command Line Interface (AWS CLI) を使用して、Amazon Simple Storage Service (Amazon S3) からスクリプトを実行するための手順について説明します。例ではシェルスクリプトを使用していますが、他のタイプのスクリプトに置き換えることができます。

Amazon S3 からシェルスクリプトを実行する (コンソール)

Amazon S3 からシェルスクリプトを実行する

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Run Command] を選択します。
3. [コマンドの実行] を選択します。
4. [コマンドのドキュメント] リストで、[**`AWS-RunRemoteScript`**] を選択します。
5. [Command parameters] で、以下の作業を行います。
   - [Source Type (ソースタイプ)] で、[S3] を選択します。
   - [Source Info (ソース情報)] テキストボックスに、ソースにアクセスするために必要な情報を次の形式で入力します。各`##############`をユーザー自身の情報に置き換えます。

> **Note**
>
> https://s3.*aws-api-domain* をバケットの URL に置き換えます。Amazon S3 のバケット URL は [Objects] (オブジェクト) タブでコピーできます。

```
{"path":"https://s3.aws-api-domain/path to script"}
```

以下に例を示します。

```
{"path":"https://amzn-s3-demo-bucket.s3.us-east-2.amazonaws.com/scripts/shell/
helloWorld.sh"}
```

- [コマンドライン] フィールドに、スクリプトの実行に必要なパラメータを入力します。以下はその例です。

```
helloWorld.sh argument-1 argument-2
```

- (オプション) [作業ディレクトリ] に、スクリプトをダウンロードして実行する先の、ノードのディレクトリの名前を入力します。
- (オプション) [実行タイムアウト] に、スクリプトコマンドの実行を失敗とするまでにシステムが待機する秒数を指定します。

6. [ターゲット] セクションで、タグの指定、インスタンスやエッジデバイスの手動選択、リソースグループの指定により、このオペレーションを実行するマネージドノードを選択します。

> **Tip**
>
> 表示されるはずのマネージドノードが表示されない場合は、トラブルシューティングのヒントについて「マネージドノードの可用性のトラブルシューティング」を参照してください。

7. [その他のパラメータ] で、以下の操作を行います。

   - [コメント] に、このコマンドに関する情報を入力します。
   - [タイムアウト (秒)] に、コマンドの実行全体が失敗するまでにシステムが待機する秒数を指定します。

8. [レート制御] の場合:

- [同時実行数] の場合、コマンドを同時に実行するマネージドノードの数または割合を指定します。

> **Note**
>
> マネージドノードに適用されるタグを指定するか、AWS リソースグループを指定してターゲットを選択し、ターゲットとなるマネージドノードの数が不明な場合は、割合を指定してドキュメントを同時に実行できるターゲットの数を制限します。

- [エラーのしきい値] で、ノードの数または割合のいずれかで失敗した後、他のマネージドノードでのコマンドの実行をいつ停止するか指定します。例えば、3 つのエラーを指定した場合、4 番目のエラーが受信されると、システムマネージャー はコマンドの送信を停止します。コマンドを処理しているマネージドノードもエラーを送信する可能性があります。

9. (オプション) コマンド出力をファイルに保存する場合は、[出力オプション] の [S3 バケットにコマンド出力を書き込む] ボックスを選択します。ボックスにバケット名とプレフィックス (フォルダ) 名を入力します。

> **Note**
>
> S3 バケットにデータを書き込む機能を許可する S3 許可は、このタスクを実行する IAM ユーザーのものではなく、インスタンスに割り当てられたインスタンスプロファイル (EC2 インスタンスの場合) または IAM サービスロール (ハイブリッドアクティベーションマシン) のものです。詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」または「ハイブリッド環境に IAM サービスロールを作成する」を参照してください。さらに、指定された S3 バケットが別の AWS アカウント にある場合は、マネージドノードに関連付けられたインスタンスプロファイルまたは IAM サービスロールが、そのバケットへの書き込みに必要なアクセス許可があることを確認してください。

10. [SNS Notifications (SNS 通知)] セクションで、コマンドの実行状態に関する通知を受け取る場合は、[Enable SNS notifications (SNS 通知を有効にする)] チェックボックスをオンにします。

    Run Command 用の Amazon SNS 通知の設定の詳細については、「Amazon SNS 通知を使用した Systems Manager のステータス変更のモニタリング」を参照してください。

11. [Run (実行)] を選択します。

Amazon S3 からシェルスクリプトを実行する (コマンドライン)

1. まだ AWS Command Line Interface (AWS CLI) をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」を参照してください。

2. 以下のコマンドを実行してください。各*###############*をユーザー自身の情報に置き換えます。

   > **Note**
   >
   > https://s3.*aws-api-domain*/*########*をユーザーバケットの URL に置き換えます。Amazon S3 のバケット URL は [Objects] (オブジェクト) タブでコピーできます。

   Linux & macOS

   ```
   aws ssm send-command \
       --document-name "AWS-RunRemoteScript" \
       --output-s3-bucket-name "amzn-s3-demo-bucket" \
       --output-s3-key-prefix "key-prefix" \
       --targets "Key=InstanceIds,Values=instance-id" \
       --parameters '{"sourceType":["S3"],"sourceInfo":["{\"path\":\"https://
   s3.aws-api-domain/script path\"}"],"commandLine":["script name and arguments"]}'
   ```

   Windows

   ```
   aws ssm send-command ^
       --document-name "AWS-RunRemoteScript" ^
       --output-s3-bucket-name "amzn-s3-demo-bucket" ^
       --output-s3-key-prefix "key-prefix" ^
       --targets "Key=InstanceIds,Values=instance-id" ^
       --parameters "sourceType"="S3",sourceInfo='{\"path\":\"https://s3.aws-api-
   domain/script path\"}',"commandLine"="script name and arguments"
   ```

   PowerShell

   ```
   Send-SSMCommand `
       -DocumentName "AWS-RunRemoteScript" `
   ```

```
    -OutputS3BucketName "amzn-s3-demo-bucket" `
    -OutputS3KeyPrefix "key-prefix" `
    -Target @{Key="InstanceIds";Values=@("instance-id")} `
    -Parameter @{
        sourceType = "S3";
        sourceInfo = '{"path": "s3://bucket-name/path/to/script"}';
        commandLine = "script name and arguments"
    }
```

Parameter Store パラメータからの AWS Secrets Manager シークレットの参照

AWS Secrets Manager は、認証情報、パスワード、ライセンスキーなどの重要な設定データの整理や管理に役立ちます。AWS Systems Manager のツールである Parameter Store は Secrets Manager と統合されたため、Parameter Store パラメータへの参照が既にサポートされている他の AWS のサービスを使用するときに、Secrets Manager シークレットを取得できます。これらのサービスには、Amazon Elastic Compute Cloud (Amazon EC2)、Amazon Elastic Container Service (Amazon ECS)、AWS Lambda、AWS CloudFormation、AWS CodeBuild、AWS CodeDeploy、およびその他の Systems Manager のツールが含まれます。Parameter Store を使用して Secrets Manager のシークレットを参照することによって、安全で一貫したプロセスを作成し、コードおよび設定スクリプトでシークレットや参照データを呼び出して使用できます。

Secrets Manager の詳細については、AWS Secrets Manager ユーザーガイドの「AWS Secrets Manager とは」を参照してください。

制限事項

Parameter Store を使用して Secrets Manager のシークレットを参照する場合は、次の制限に注意してください。

- GetParameter および GetParameters API オペレーションを使用して取得できるのは、Secrets Manager のシークレットのみです。DescribeParameters や GetParametersByPath などの変更オペレーションや高度なクエリの API オペレーションは、Secrets Manager に対してはサポートされていません。
- Parameter Store を使用してシークレットを取得するには、AWS Command Line Interface (AWS CLI)、AWS Tools for Windows PowerShell、および SDK を使用できます。
- Parameter Store の Secrets Manager シークレットには `/aws/reference/secretsmanager` のプレフィックスが必要です。次に例を示します。

```
/aws/reference/secretsmanager/CFCreds1

/aws/reference/secretsmanager/myapp/db/password
```

- Parameter Store では、Secrets Manager のシークレットにアタッチされた AWS Identity and Access Management (IAM) ポリシーが尊重されます。たとえば、ユーザー 1 にシークレット A へのアクセス権がない場合、ユーザー 1 は Parameter Store を使用してシークレット A を取得することはできません。
- Secrets Manager のシークレットを参照するパラメータは、Parameter Store のバージョン管理機能または履歴機能を使用できません。
- Parameter Store は、Secrets Manager のバージョンステージを尊重します。バージョンステージを参照する場合、英字、数字、ピリオド (.)、ハイフン (-)、アンダースコア (_) を使用できます。バージョンステージで他の記号を使用すると、その参照は失敗します。

Parameter Store を使用して Secrets Manager のシークレットを参照する方法

次の手順では、Parameter Store API を使用して Secrets Manager のシークレットを参照する方法について説明します。この手順では AWS Secrets Manager ユーザーガイドで説明されている他の手順を参照しています。

> **Note**
>
> この手順を開始する前に、Parameter Store パラメータで Secrets Manager のシークレットを参照するアクセス許可があることを確認してください。Secrets Manager および Systems Manager で管理者アクセス許可を持っている場合は、Parameter Store API を使用してシークレットを参照または取得できます。Parameter Store パラメータで Secrets Manager シークレットを参照する場合、そのシークレットへのアクセス許可を持っていなければ、その参照は失敗します。詳細については、AWS Secrets Manager ユーザーガイドの「AWS Secrets Manager に対する認証とアクセスコントロール」を参照してください。

> **Important**
>
> Parameter Store は Secrets Manager シークレットを参照するためのパススルーサービスとして機能します。Parameter Store はシークレットに関するデータやメタデータを保持しません。この参照はステートレスです。

Parameter Store を使用して Secrets Manager のシークレットを参照するには

1. Secrets Manager でシークレットを作成します。詳細については、「AWS Secrets Manager を使用したシークレットの作成および管理」を参照してください。
2. AWS CLI、AWS Tools for Windows PowerShell、または SDK を使用してシークレットを参照する Secrets Manager シークレットを参照する場合、名前は、「`/aws/reference/secretsmanager/`」の予約済みパスで始まる必要があります。このパスを指定することで、Systems Manager は Parameter Store ではなく Secrets Manager からシークレットを取得することを認識します。Parameter Store を使用して `CFCreds1` と `DBPass` の Secrets Manager シークレットを正しく参照する名前の例を次に示します。

   - `/aws/reference/secretsmanager/CFCreds1`
   - `/aws/reference/secretsmanager/DBPass`

   次の Java コード例では、Secrets Manager に保存されているアクセスキーとシークレットキーを参照しています。このコード例では、Amazon DynamoDB クライアントを設定します。このコードでは、Parameter Store から設定データと認証情報を取得しています。設定データは、Parameter Store に文字列パラメータとして格納され、認証情報は Secrets Manager に格納されます。設定データと認証情報が異なるサービスに保存されている場合でも、`GetParameter` API を使用して Parameter Store から両方データにアクセスできます。

```
/**
* Initialize Systems Manager client with default credentials
*/
AWSSimpleSystemsManagement ssm =
 AWSSimpleSystemsManagementClientBuilder.defaultClient();

...

/**
* Example method to launch DynamoDB client with credentials different from default
* @return DynamoDB client
*/
AmazonDynamoDB getDynamoDbClient() {
    //Getting AWS credentials from Secrets Manager using GetParameter
    BasicAWSCredentials differentAWSCreds = new BasicAWSCredentials(
            getParameter("/aws/reference/secretsmanager/access-key"),
            getParameter("/aws/reference/secretsmanager/secret-key"));

    //Initialize the DynamoDB client with different credentials
```

```
    final AmazonDynamoDB client = AmazonDynamoDBClient.builder()
            .withCredentials(new AWSStaticCredentialsProvider(differentAWSCreds))
            .withRegion(getParameter("region")) //Getting configuration from
 Parameter Store
            .build();
    return client;
}

/**
* Helper method to retrieve parameter value
* @param parameterName identifier of the parameter
* @return decrypted parameter value
*/
public GetParameterResult getParameter(String parameterName) {
    GetParameterRequest request = new GetParameterRequest();
    request.setName(parameterName);
    request.setWithDecryption(true);
    return ssm.newGetParameterCall().call(request).getParameter().getValue();
}
```

AWS CLI の例を次に示します。`aws secretsmanager list-secrets` コマンドを使用して、シークレットの名前を検索します。

AWS CLI 例 1: シークレットの名前を使用した参照

Linux & macOS

```
aws ssm get-parameter \
    --name /aws/reference/secretsmanager/s1-secret \
    --with-decryption
```

Windows

```
aws ssm get-parameter ^
    --name /aws/reference/secretsmanager/s1-secret ^
    --with-decryption
```

このコマンドによって以下のような情報が返されます。

```
{
    "Parameter": {
```

```
        "Name": "/aws/reference/secretsmanager/s1-secret",
        "Type": "SecureString",
        "Value": "Fl*MEishm!al875",
        "Version": 0,
        "SourceResult":
              "{
                   \"CreatedDate\": 1526334434.743,
                   \"Name\": \"s1-secret\",
                   \"VersionId\": \"aaabbbccc-1111-222-333-123456789\",
                   \"SecretString\": \"Fl*MEishm!al875\",
                   \"VersionStages\": [\"AWSCURRENT\"],
                   \"ARN\": \"arn:aws:secretsmanager:us-
east-2:123456789012:secret:s1-secret-E18LRP\"
               }"
        "LastModifiedDate": 2018-05-14T21:47:14.743Z,
        "ARN": "arn:aws:secretsmanager:us-east-2:123456789012:secret:s1-secret-
              E18LRP",
      }
}
```

AWS CLI 例 2: バージョン ID が含まれている参照

Linux & macOS

```
aws ssm get-parameter \
    --name /aws/reference/secretsmanager/s1-secret:11111-aaa-bbb-ccc-123456789 \
    --with-decryption
```

Windows

```
aws ssm get-parameter ^
    --name /aws/reference/secretsmanager/s1-secret:11111-aaa-bbb-ccc-123456789 ^
    --with-decryption
```

このコマンドによって以下のような情報が返されます。

```
{
    "Parameter": {
        "Name": "/aws/reference/secretsmanager/s1-secret",
        "Type": "SecureString",
        "Value": "Fl*MEishm!al875",
```

```
        "Version": 0,
        "SourceResult":
              "{
                   \"CreatedDate\": 1526334434.743,
                   \"Name\": \"s1-secret\",
                   \"VersionId\": \"11111-aaa-bbb-ccc-123456789\",
                   \"SecretString\": \"Fl*MEishm!al875\",
                   \"VersionStages\": [\"AWSCURRENT\"],
                   \"ARN\": \"arn:aws:secretsmanager:us-
east-2:123456789012:secret:s1-secret-E18LRP\"
               }"
        "Selector": ":11111-aaa-bbb-ccc-123456789"
      }
        "LastModifiedDate": 2018-05-14T21:47:14.743Z,
        "ARN": "arn:aws:secretsmanager:us-east-2:123456789012:secret:s1-secret-
               E18LRP",
}
```

AWS CLI 例 3: バージョンステージが含まれている参照

Linux & macOS

```
aws ssm get-parameter \
    --name /aws/reference/secretsmanager/s1-secret:AWSCURRENT \
    --with-decryption
```

Windows

```
aws ssm get-parameter ^
    --name /aws/reference/secretsmanager/s1-secret:AWSCURRENT ^
    --with-decryption
```

このコマンドによって以下のような情報が返されます。

```
{
    "Parameter": {
        "Name": "/aws/reference/secretsmanager/s1-secret",
        "Type": "SecureString",
        "Value": "Fl*MEishm!al875",
        "Version": 0,
        "SourceResult":
```

```
                "{
                     \"CreatedDate\": 1526334434.743,
                     \"Name\": \"s1-secret\",
                     \"VersionId\": \"11111-aaa-bbb-ccc-123456789\",
                     \"SecretString\": \"Fl*MEishm!al875\",
                     \"VersionStages\": [\"AWSCURRENT\"],
                     \"ARN\": \"arn:aws:secretsmanager:us-
east-2:123456789012:secret:s1-secret-E18LRP\"
                 }"
          "Selector": ":AWSCURRENT"
       }
       "LastModifiedDate": 2018-05-14T21:47:14.743Z,
       "ARN": "arn:aws:secretsmanager:us-east-2:123456789012:secret:s1-secret-
                 E18LRP",
}
```

AWS Systems ManagerParameter Store SecureString パラメータの AWS KMS 暗号化

AWS Systems Manager Parameter Store を使用すると、プレーンテキストのパラメータ名と暗号化されたパラメータ値を持つ SecureString パラメータを作成できます。Parameter Store は AWS KMS を使用して、`SecureString` パラメータのパラメータ値を暗号化および復号します。

Parameter Store を使用すると、値を持つパラメータとしてデータを作成、保存、管理できます。Parameter Store にパラメータを作成し、それを設計したポリシーとアクセス許可の対象となる複数のアプリケーションやサービスで使用することができます。パラメータの値を変更する必要がある場合は、エラーが発生しやすい変更を多数のソースで管理するのではなく、1 つのインスタンスを変更します。Parameter Store はパラメータ名の階層構造をサポートしているため、特定の用途に応じてパラメータを選別できます。

機密データを管理するために、`SecureString` パラメータを作成できます。Parameter Store は、`SecureString` パラメータを作成または変更する際に、AWS KMS keysを使用してそのパラメータ値を暗号化します。また、アクセス時に KMS キーを使用してパラメータ値を復号します。Parameter Store がアカウント用に作成した AWS マネージドキーを使用することも、独自のカスタマーマネージドキーを指定することもできます。

> **Important**
>
> Parameter Store は、対称 KMS キーのみをサポートします。非対称 KMS キーを使用してパラメータを暗号化することはできません。KMS キーが対称か非対称かを判断する方法については、「AWS Key Management Service デベロッパーガイド」の「さまざまなキータイプの特定」を参照してください。

Parameter Store では、2 つの階層 (標準とアドバンスト) の `SecureString` パラメータをサポートしています。スタンダードパラメータは 4,096 バイトを上限とし、ユーザーが指定した KMS キーで直接、暗号化および復号されます。アドバンストの `SecureString` パラメータを暗号化および復号化するには、Parameter Store は AWS Encryption SDK を使用したエンベロープ暗号化を行います。標準の `SecureString` パラメータをアドバンストパラメータに変換することはできますが、アドバンストパラメータを標準パラメータに変換することはできません。標準とアドバンストの `SecureString` パラメータの違いの詳細については、「パラメータ層の管理」を参照してください。

トピック

- 標準 SecureString パラメータの保護
- アドバンスト SecureString パラメータの保護
- パラメータ値を暗号化および復号するためのアクセス許可の設定
- Parameter Store の暗号化コンテキスト
- Parameter Store における KMS キーの問題のトラブルシューティング

標準 SecureString パラメータの保護

Parameter Store は暗号化オペレーションを実行しません。代わりに、AWS KMS を使用して、`SecureString` パラメータ値を暗号化および復号します。標準の `SecureString` パラメータ値を作成または変更すると、Parameter Store は AWS KMS暗号化オペレーションを呼び出します。このオペレーションは、KMS キーを使用してデータキーを生成するのではなく、対称暗号化 KMS キーを直接使用してパラメータ値を暗号化します。

Parameter Store がパラメータ値を暗号化するために使用する KMS を選択できます。KMS キーを指定しない場合、Parameter Store は、Systems Manager がアカウント内に自動的に作成した AWS マネージドキーを使用します。この KMS キー には `aws/ssm` エイリアスがあります。

アカウントのデフォルトの aws/ssm KMS キーを表示するには、AWS KMS API で DescribeKey オペレーションを使用します。次の例では、aws/ssm エイリアス名を持つ AWS Command Line Interface (AWS CLI) の describe-key コマンドを使用します。

```
aws kms describe-key \
    --key-id alias/aws/ssm
```

標準 SecureString パラメータを作成するには、Systems Manager API で PutParameter オペレーションを使用します。Tier パラメータを省略するか、デフォルトの値である Standard を指定します。値が SecureString の Type パラメータを含めます。KMS キーを指定するには、KeyId パラメータを使用します。デフォルトは、アカウントの AWS マネージドキー である aws/ssm です。

その後、Parameter Store は KMS キーとプレーンテキストのパラメータ値を使用して AWS KMS Encrypt オペレーションを呼び出します。AWS KMS が暗号化されたパラメータ値を返し、その値は Parameter Store によってパラメータ名と一緒に保存されます。

次の例では、AWS CLI で Systems Manager の put-parameter コマンドとその --type パラメータを使用して、SecureString パラメータを作成します。このコマンドはオプションの --tier および --key-id パラメータを省略するため、Parameter Store は標準 SecureString パラメータを作成し、それを AWS マネージドキーで暗号化します。

```
aws ssm put-parameter \
    --name MyParameter \
    --value "secret_value" \
    --type SecureString
```

次の類似した例では、--key-id パラメータを使用してカスタマーマネージドキーを指定します。この例では、KMS キー ID を使用して KMS キーを識別しますが、任意の有効な KMS キー識別子を使用することができます。このコマンドは Tier パラメータ (--tier) を省略するため、Parameter Store は、アドバンストではなく標準の SecureString パラメータを作成します。

```
aws ssm put-parameter \
    --name param1 \
    --value "secret" \
    --type SecureString \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

Parameter Store から SecureString パラメータを取得すると、その値が暗号化されます。パラメータを取得するには、Systems Manager API で GetParameter オペレーションを使用します。

次の例では、AWS CLI で Systems Manager の get-parameter コマンドを使用して、Parameter Store から値を復号せずに MyParameter パラメータを取得します。

```
aws ssm get-parameter --name MyParameter
```

```
{
    "Parameter": {
        "Type": "SecureString",
        "Name": "MyParameter",
        "Value": "AQECAHgnOkMROh5LaLXkA4j0+vYi6tmM17Lg"
    }
}
```

返す前にパラメータ値を復号するには、GetParameter の WithDecryption パラメータを true に設定します。WithDecryption を使用すると、Parameter Store はユーザーに代わって AWS KMS Decrypt オペレーションを呼び出して、パラメータ値を復号します。その結果、GetParameter リクエストは、次の例に示すように、プレーンテキストパラメータ値を持つパラメータを返します。

```
aws ssm get-parameter \
    --name MyParameter \
    --with-decryption
```

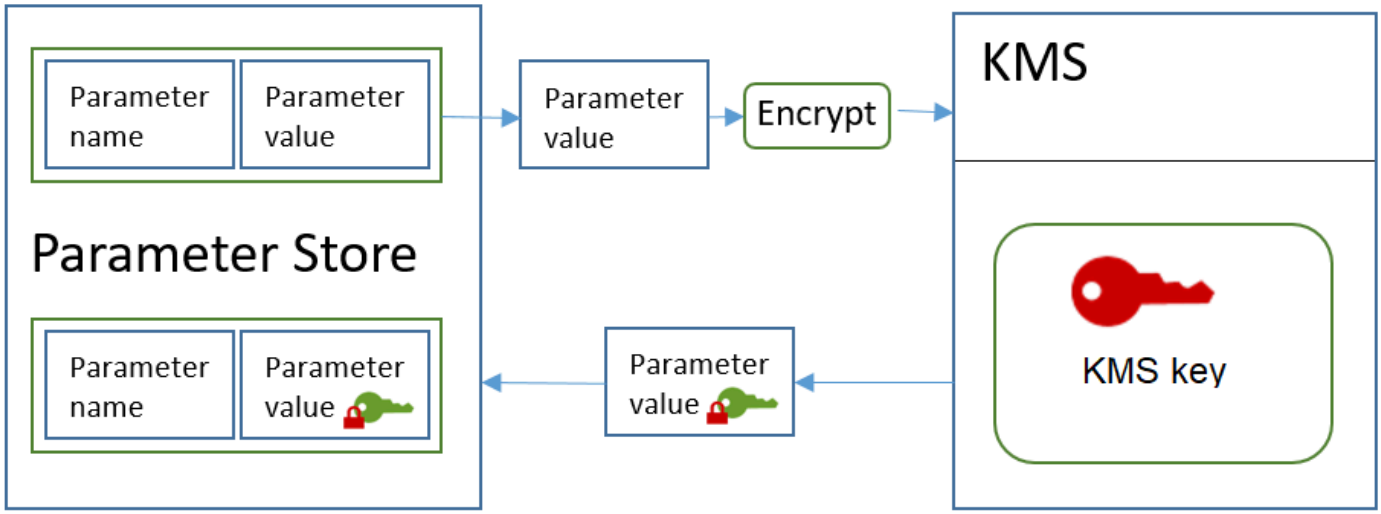
```
{
    "Parameter": {
        "Type": "SecureString",
        "Name": "MyParameter",
        "Value": "secret_value"
    }
}
```

次のワークフローは、Parameter Store が KMS キーを使用して標準 SecureString パラメータを暗号化および復号する方法を示しています。

スタンダードパラメータの暗号化

1. PutParameter を使って SecureString パラメータを作成する場合、Parameter Store は、AWS KMS に Encrypt リクエストを送信します。このリクエストには、プレーンテキストのパラメータ値、ユーザーが選択した KMS キー、Parameter Store 暗号化コンテキストが含まれます。AWS KMS への送信時に、SecureString パラメータのプレーンテキスト値は、Transport Layer Security (TLS) によって保護されます。

2. AWS KMS は、指定された KMS キーと暗号化コンテキストを使用して、パラメータ値を暗号化します。暗号化テキストを Parameter Store に返し、そこでパラメータ名と暗号化された値が保存されます。



標準パラメータの復号

1. `GetParameter` リクエストに `WithDecryption` パラメータを含めた場合、Parameter Store は、暗号化された `SecureString` パラメータ値と Parameter Store 暗号化コンテキストを `Decrypt` リクエストと一緒に AWS KMS に送信します。
2. AWS KMS は、同じ KMS キーと指定された暗号化コンテキストを使用して、暗号化された値を復号します。これは、プレーンテキストの (復号化された) パラメータ値を Parameter Store に返します。送信中、プレーンテキストのデータは TLS によって保護されます。
3. Parameter Store は、プレーンテキストパラメータ値を `GetParameter` レスポンスで返します。

アドバンスト SecureString パラメータの保護

`PutParameter` を使用してアドバンスト `SecureString` パラメータを作成する場合、Parameter Store は AWS Encryption SDK および対称暗号化 AWS KMS keyによるエンベロープ暗号化を使用してパラメータ値を保護します。アドバンストパラメータ値は、それぞれ一意のデータキーで暗号化され、そのデータキーは KMS キーで暗号化されます。アカウントの AWS マネージドキー (`aws/ssm`) または任意のカスタマーマネージドキーを使用できます。

AWS Encryption SDK は、オープンソースのクライアント側ライブラリで、業界標準とベストプラクティスに沿ったデータの暗号化および復号に役立ちます。これは、複数のプラットフォームと、コマ

ンドラインインターフェイスを含む複数のプログラミング言語でサポートされています。ソースコードを表示し、GitHub での開発に貢献することができます。

各 SecureString パラメータ値に対して、Parameter Store は AWS Encryption SDK を呼び出し、AWS KMS が生成する一意のデータキー (GenerateDataKey) を使ってパラメータ値を暗号化します。AWS Encryption SDK は、暗号化されたパラメータ値と一意のデータキーの暗号化コピーを含む、暗号化されたメッセージを Parameter Store に返します。Parameter Store は、暗号化されたメッセージ全体を SecureString パラメータ値として保存します。その後、アドバンスト SecureString パラメータ値を取得すると、Parameter Store は AWS Encryption SDK を使ってパラメータ値を復号化します。これには、AWS KMS を呼び出して、暗号化されたデータを復号する必要があります。

アドバンスト SecureString パラメータを作成するには、Systems Manager API で PutParameter オペレーションを使用します。Tier パラメータの値を Advanced に設定します。値が SecureString の Type パラメータを含めます。KMS キーを指定するには、KeyId パラメータを使用します。デフォルトは、アカウントの AWS マネージドキー である aws/ssm です。

```
aws ssm put-parameter \
    --name MyParameter \
    --value "secret_value" \
    --type SecureString \
    --tier Advanced
```

次の類似した例では、--key-id パラメータを使用してカスタマーマネージドキーを指定します。例では、KMS キーの Amazon リソースネーム (ARN) を使用していますが、任意の有効な KMS キー識別子を使用することもできます。

```
aws ssm put-parameter \
    --name MyParameter \
    --value "secret_value" \
    --type SecureString \
    --tier Advanced \
    --key-id arn:aws:kms:us-
east-2:987654321098:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

Parameter Store から SecureString パラメータを取得すると、その値は、AWS Encryption SDK が返した暗号化されたメッセージとなります。パラメータを取得するには、Systems Manager API で GetParameter オペレーションを使用します。

次の例では、Systems Manager の GetParameter オペレーションを使用して、Parameter Store から値を復号せずに MyParameter パラメータを取得します。

```
aws ssm get-parameter --name MyParameter
```

```
{
    "Parameter": {
        "Type": "SecureString",
        "Name": "MyParameter",
        "Value": "AQECAHgnOkMROh5LaLXkA4j0+vYi6tmM17Lg"
    }
}
```

返す前にパラメータ値を復号するには、GetParameter の WithDecryption パラメータを true に設定します。WithDecryption を使用すると、Parameter Store はユーザーに代わって AWS KMS Decrypt オペレーションを呼び出して、パラメータ値を復号します。その結果、GetParameter リクエストは、次の例に示すように、プレーンテキストパラメータ値を持つパラメータを返します。

```
aws ssm get-parameter \
    --name MyParameter \
    --with-decryption
```

```
{
    "Parameter": {
        "Type": "SecureString",
        "Name": "MyParameter",
        "Value": "secret_value"
    }
}
```

アドバンスト SecureString パラメータを標準パラメータに変換することはできますが、標準 SecureString をアドバンストに変換することはできません。標準 SecureString パラメータをアドバンスト SecureString に変換するには、Overwrite パラメータを使った PutParameter オペレーションを実行します。Type は SecureString、 Tier 値は Advanced である必要があります。カスタマーマネージドキーを識別する KeyId パラメータはオプションです。このパラメータを省略すると、Parameter Store は、アカウント用の AWS マネージドキーを使用します。スタンダードパラメータの暗号化に異なる KMS キーを使用した場合でも、プリンシパルが使用を許可されている任意の KMS キーを指定することができます。

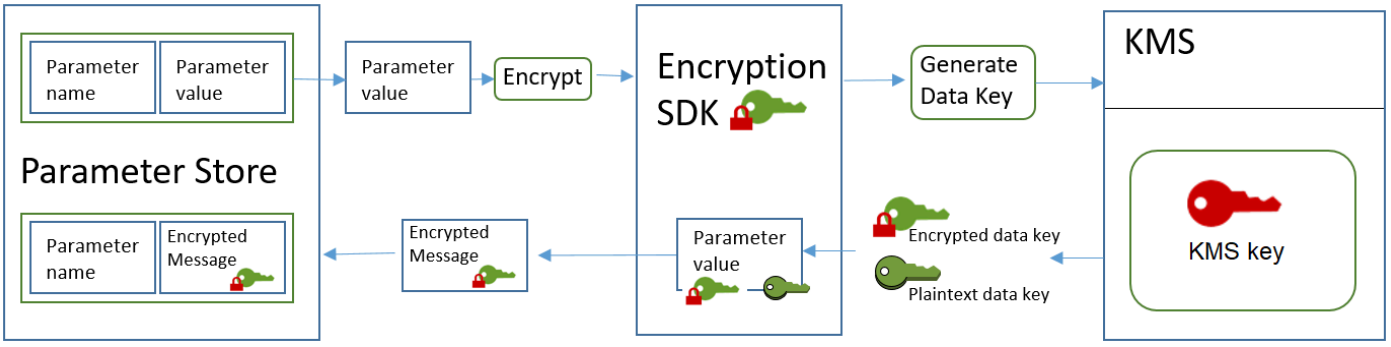
Overwrite パラメータを使用すると、Parameter Store は AWS Encryption SDK を使用してパラメータ値を暗号化します。続いて、新たに暗号化されたメッセージを Parameter Store に保存します。

```
aws ssm put-parameter \
    --name myStdParameter \
    --value "secret_value"  \
    --type SecureString \
    --tier Advanced \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --overwrite
```

次のワークフローは、Parameter Store が KMS キーを使用してアドバンスト SecureString パラメータを暗号化および復号する方法を示しています。

アドバンストパラメータの暗号化

1. PutParameter を使用してアドバンスト SecureString パラメータを作成する場合、Parameter Store は AWS Encryption SDK および AWS KMS を使用してパラメータ値を暗号化します。Parameter Store は、パラメータ値、ユーザーが指定した KMS キー、および Parameter Store 暗号化コンテキストを使用して AWS Encryption SDK を呼び出します。
2. AWS Encryption SDK は、ユーザーが指定した KMS キーの識別子と Parameter Store 暗号化コンテキストを GenerateDataKey リクエストと一緒に AWS KMS に送信します。AWS KMS は一意のデータキーの 2 つのコピーを返します。1 つはプレーンテキストで、もう 1 つは KMS キーで暗号化されています。(暗号化コンテキストは、データキーを暗号化するときに使用します)。
3. AWS Encryption SDK はプレーンテキストのデータキーを使ってパラメータ値を暗号化し、暗号化されたメッセージを戻します。このメッセージは、暗号化されたパラメータ値、暗号化されたデータキー、そして Parameter Store 暗号化コンテキストなどのその他のデータを含みます。
4. Parameter Store は、暗号化されたメッセージをパラメータ値として保存します。



アドバンストパラメータの復号

1. アドバンスト SecureString パラメータを取得するための GetParameter リクエストに、WithDecryption パラメータを含めることができます。これを行うと、Parameter Store は暗号化されたメッセージをパラメータ値から AWS Encryption SDK の復号化メソッドに渡します。
2. AWS Encryption SDK は AWS KMS Decrypt オペレーションを呼び出します。これは、暗号化されたメッセージから暗号化されたデータキーと Parameter Store 暗号化コンテキストを渡します。
3. AWS KMS は、KMS キーと Parameter Store 暗号化コンテキストを使用して、暗号化されたデータキーを復号します。続いて、プレーンテキストの (復号化された) データキーを AWS Encryption SDK に返します。
4. AWS Encryption SDK は、プレーンテキストのデータキーを使ってパラメータ値を復号し、プレーンテキストのパラメータ値を Parameter Store に返します。
5. Parameter Store は暗号化コンテキストを検証し、プレーンテキストパラメータ値を GetParameter レスポンスで返します。

パラメータ値を暗号化および復号するためのアクセス許可の設定

ユーザーが標準 SecureString パラメータの値を暗号化するには、kms:Encrypt アクセス許可が必要です。ユーザーがアドバンスト SecureString パラメータの値を暗号化するには、kms:GenerateDataKey アクセス許可が必要です。ユーザーがいずれかのタイプの SecureString パラメータの値を復号化するには、kms:Decrypt アクセス許可が必要です。

AWS Identity and Access Management (IAM) ポリシーを使用して、ユーザーが Systems Manager の PutParameter および GetParameter オペレーションを呼び出すアクセス許可を許可または拒否できます。

カスタマーマネージドキーを使用して SecureString パラメータ値を暗号化している場合は、IAM ポリシーとキーポリシーを使用して、暗号化と復号のアクセス許可を管理できます。ただし、デフォルトの aws/ssm KMS キーに対してアクセス制御ポリシーを確立することはできません。カスタマーマネージドキーへのアクセスを制御する方法の詳細については、「AWS Key Management Service デベロッパーガイド」の「KMS キーのアクセスとアクセス許可」を参照してください。

次の例は、標準 SecureString パラメータ用に設計された IAM ポリシーを示しています。これにより、ユーザーは FinancialParameters パス内のすべてのパラメータに対して Systems Manager PutParameter オペレーションを呼び出すことができます。このポリシーにより、ユー

ザーはサンプルカスタマーマネージドキーで AWS KMS Encrypt オペレーションを呼び出すこともできます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:PutParameter"
            ],
            "Resource": "arn:aws:ssm:us-east-2:111122223333:parameter/
FinancialParameters/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt"
            ],
            "Resource": "arn:aws:kms:us-
east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ]
}
```

次の例は、アドバンスト SecureString パラメータ用に設計された IAM ポリシーを示しています。これにより、ユーザーは ReservedParameters パス内のすべてのパラメータに対して Systems Manager PutParameter オペレーションを呼び出すことができます。このポリシーにより、ユーザーはサンプルカスタマーマネージドキーで AWS KMS GenerateDataKey オペレーションを呼び出すこともできます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:PutParameter"
            ],
            "Resource": "arn:aws:ssm:us-east-2:111122223333:parameter/
ReservedParameters/*"
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:us-
east-2:987654321098:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ]
}
```

最後の例も、標準またはアドバンスト SecureString パラメータに使用できる IAM ポリシーを示します。これにより、ユーザーは ITParameters パス内のすべてのパラメータに対して Systems Manager の GetParameter オペレーション (および関連する操作) を呼び出すことができます。このポリシーにより、ユーザーはサンプルカスタマーマネージドキーで AWS KMS Decrypt オペレーションを呼び出すこともできます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:GetParameter*"
            ],
            "Resource": "arn:aws:ssm:us-east-2:111122223333:parameter/ITParameters/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:us-
east-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ]
}
```

Parameter Store の暗号化コンテキスト

暗号化コンテキスト は、一連のキー値のペアおよび任意非シークレットデータを含みます。データを暗号化するリクエストに暗号化コンテキストを組み込むと、AWS KMS は暗号化コンテキストを暗

号化されたデータに暗号化してバインドします。データを復号するには、同じ暗号化コンテキストに渡す必要があります。

また、暗号化コンテキストを使用して、監査レコードおよびログ内の暗号化オペレーションを識別することもできます。暗号化コンテキストは、AWS CloudTrail ログなどのログにプレーンテキストで表示されます。

AWS Encryption SDK も暗号化コンテキストを取りますが、その処理方法は異なります。Parameter Store が暗号化メソッドの暗号化コンテキストを指定します。AWS Encryption SDK は、暗号化コンテキストを暗号化されたデータに暗号化してバインドします。また、暗号化されたメッセージを返す際、ヘッダーに暗号化コンテキストをプレーンテキストとして含めます。ただし、AWS KMS とは異なり、AWS Encryption SDK の復号メソッドは、入力として暗号化コンテキストを取りません。その代わり、AWS Encryption SDK は、データを復号化する際に暗号化されたメッセージから暗号化コンテキストを取得します。Parameter Store は、暗号化コンテキストに指定の値が含まれていることを検証してから、プレーンテキストパラメータ値を返します。

Parameter Store は、暗号化オペレーションで次の暗号化コンテキストを使用します。

- キー: PARAMETER_ARN
- 値: 暗号化されるパラメータの Amazon リソースネーム (ARN)。

暗号化コンテキストの形式は以下のとおりです。

```
"PARAMETER_ARN":"arn:aws:ssm:region-id:account-id:parameter/parameter-name"
```

例えば、Parameter Store は、サンプルの AWS アカウントとリージョンで、MyParameter パラメータを暗号化および復号する呼び出しにこの暗号化コンテキストを含めます。

```
"PARAMETER_ARN":"arn:aws:ssm:us-east-2:111122223333:parameter/MyParameter"
```

パラメータが Parameter Store 階層パスにある場合、パスと名前は暗号化コンテキストに組み込まれます。例えば、サンプルの AWS アカウント およびリージョンの /ReadableParameters パスで MyParameter パラメータを暗号化および復号するときに、この暗号化コンテキストが使用されます。

```
"PARAMETER_ARN":"arn:aws:ssm:us-east-2:111122223333:parameter/ReadableParameters/
MyParameter"
```

正しい暗号化コンテキストと、Systems Manager の GetParameter オペレーションによって返される暗号化されたパラメータ値を使用して AWS KMS Decrypt オペレーションを呼び出すことで、暗号化された SecureString パラメータ値を復号することができます。ただし、Parameter Store パラメータ値の復号化には、GetParameter オペレーションと WithDecryption パラメータを使用することをお勧めします。

暗号化コンテキストを IAM ポリシーに含めることもできます。例えば、ユーザーが特定の 1 つのパラメータ値またはパラメータ値のセットのみを復号できるようにすることができます。

次の IAM ポリシーステートメントの例では、ユーザーが MyParameter パラメータの get 値と、指定した KMS キーを使用してその値を復号できるようにします。ただし、アクセス許可は、暗号化コンテキストが指定された文字列と一致する場合にのみ適用されます。これらのアクセス許可は他のパラメータや KMS キーには適用されません。また、暗号化コンテキストが文字列と一致しない場合、GetParameter への呼び出しは失敗します。

このようなポリシーステートメントを使用する場合は、事前に*##### ARN* を有効な値で置き換えてください。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:GetParameter*"
            ],
            "Resource": "arn:aws:ssm:us-east-2:111122223333:parameter/MyParameter"
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:us-
east-2:987654321098:key/1234abcd-12ab-34cd-56ef-1234567890ab",
            "Condition": {
                "StringEquals": {
                    "kms:EncryptionContext:PARAMETER_ARN":"arn:aws:ssm:us-
east-2:111122223333:parameter/MyParameter"
                }
            }
        }
```

```
    ]
}
```

Parameter Store における KMS キーの問題のトラブルシューティング

`SecureString` パラメータに対してオペレーションを実行するには、Parameter Store は、ユーザーが意図したオペレーションに対して指定した AWS KMS KMS キーを使用できる必要があります。KMS キーに関連する Parameter Store の失敗のほとんどは、次の問題が原因で発生します。

- アプリケーションが使用している認証情報には、KMS キーで指定されたアクションを実行するアクセス許可はありません。

  このエラーを解決するには、異なる認証情報を使用してアプリケーションを実行するか、オペレーションを妨げている IAM またはキーポリシーを修正します。AWS KMS IAM ポリシーとキーポリシーの詳細については、「AWS Key Management Service デベロッパーガイド」の「KMS キーのアクセスとアクセス許可」を参照してください。
- KMS キーが見つからない。

  これは通常、KMS キーに誤った識別子を使用した場合に発生します。KMS キーの正しい識別子を見つけて、再度コマンドを試行します。
- KMS キーが有効になっていない。これが発生すると、Parameter Store は からの詳細なエラーメッセージとともに InvalidKeyIdAWS KMS 例外を返します。KMS キーのキーステータスが `Disabled` の場合は、有効にします。`Pending Import` の場合は、インポート手順を実施してください。キーステータスが `Pending Deletion` の場合は、キーの削除をキャンセルするか、別の KMS キーを使用します。

  KMS キーのキー状態を検索するには、DescribeKey オペレーションを使用します。

Amazon Elastic Kubernetes Service での Parameter Store パラメータの使用

AWS Systems Manager のツールである Parameter Store のパラメータを、Amazon EKS ポッドにマウントされたファイルとして表示するには、Kubernetes Secrets Store CSI ドライバーの AWS Secrets and Configuration Provider を使用できます。ASCP は、Amazon EC2 ノードグループを実行する Amazon Elastic Kubernetes Service 1.17 以降で動作します。AWS Fargate ノードグループはサポートされていません。

ASCP を使用すると、Parameter Store でパラメータを保存および管理し、Amazon EKS で実行されているワークロードからパラメータを取得できます。パラメータに JSON 形式の複数のキーと値のペアが含まれている場合は、Amazon EKS にマウントするキーと値のペアを選択できます。ASCP は JMESPath 構文を使用して、シークレット内のキーと値のペアをクエリします。ASCP は AWS Secrets Manager のシークレットでも機能します。

ASCP には、Amazon EKS による 2 つの認証方法が用意されています。最初のアプローチでは、サービスアカウントの IAM ロール (IRSA) を使用します。2 番目のアプローチでは、Pod Identity を使用します。各アプローチにはそれぞれの利点とユースケースがあります。

サービスアカウントの IAM ロール (IRSA) を使用した ASCP

サービスアカウントの IAM ロール (IRSA) を使用した ASCP では、Parameter Store のパラメータを Amazon EKS ポッドのファイルとしてマウントできます。このアプローチは、次の場合に適しています。

- パラメータをポッドのファイルとしてマウントする必要がある。
- Amazon EC2 ノードグループで Amazon EKS バージョン 1.17 以降を使用している。
- JSON 形式のパラメータから特定のキーと値のペアを取得する。

詳細については、「the section called “Amazon EKS 用に ASCP を IRSA と統合する”」を参照してください。

Pod Identity を使用した ASCP

EKS Pod Identity を使用した ASCP

Pod Identity を使用した ASCP の方法では、セキュリティが強化され、Parameter Store のパラメータにアクセスするための設定が簡素化されます。このアプローチは、次の場合に役立ちます。

- ポッドレベルでより詳細にアクセス許可を管理する必要がある。
- Amazon EKS バージョン 1.24 以降を使用している。
- パフォーマンスとスケーラビリティを向上させる必要がある。

詳細については、「the section called “Amazon EKS 用に ASCP を Pod Identity と統合する”」を参照してください。

適切なアプローチの選択

IRSA を使用した ASCP と Pod Identity を使用した ASCP のどちらを選択するかを決めるときは、次の要素を考慮します。

- Amazon EKSversion: Pod Identity には Amazon EKS 1.24 以降が必要ですが、CSI ドライバーは Amazon EKS 1.17 以降で動作します。
- セキュリティ要件: Pod Identity は、ポッドレベルでのより詳細な制御を提供します。
- パフォーマンス: 通常、大規模な環境では Pod Identity の方がパフォーマンスが向上します。
- 複雑さ: Pod Identity には個別のサービスアカウントが必要ないため、設定が簡素化されます。

特定の要件と Amazon EKS 環境に最適な方法を選択します。

Amazon EKS 用の ASCP をインストールする

このセクションでは、Amazon EKS 用の AWS Secrets and Configuration Provider をインストールする方法について説明します。ASCP を使用すると、Parameter Store からのパラメータと AWS Secrets Manager からのシークレットを Amazon EKS ポッドのファイルとしてマウントできます。

前提条件

- Amazon EKS クラスター
  - Pod Identity 用にバージョン 1.24 以降
  - IRSA 用にバージョン 1.17 以降
- AWS CLI がインストールされ、設定されている
- kubectl が、Amazon EKS クラスター用にインストールされ、設定されている
- Helm (バージョン 3.0 以降)

ASCP をインストールして設定する

ASCP は secrets-store-csi-provider-aws リポジトリの GitHub で入手できます。リポジトリには、`objectType` 値を `secretsmanager` から `ssmparameter` に変更することで、シークレットを作成してマウントするための YAML ファイルの例も含まれています。

インストール中に、FIPS エンドポイントを使用するように ASCP を設定できます。Systems Manager のエンドポイントの一覧については、「Amazon Web Services 全般のリファレンス」の「Systems Manager のサービスエンドポイント」を参照してください。

Helm を使用して ASCP をインストールするには

1. リポジトリが最新のチャートを指していることを確認するには、`helm repo update.` を使用します。
2. Secrets Store CSI ドライバーチャートを追加します。

```
helm repo add secrets-store-csi-driver https://kubernetes-sigs.github.io/secrets-store-csi-driver/charts
```

3. グラフをインストールします。スロットリングを設定するには、`--set-json 'k8sThrottlingParams={"qps": "`*`number of queries per second`*`", "burst": "`*`number of queries per second`*`"}'` のフラグを追加します。

```
helm install -n kube-system csi-secrets-store secrets-store-csi-driver/secrets-store-csi-driver
```

4. ASCP チャートを追加します。

```
helm repo add aws-secrets-manager https://aws.github.io/secrets-store-csi-driver-provider-aws
```

5. グラフをインストールします。FIPS エンドポイントを使用するには、`--set useFipsEndpoint=true` のフラグを追加します。

```
helm install -n kube-system secrets-provider-aws aws-secrets-manager/secrets-store-csi-driver-provider-aws
```

リポジトリ内の YAML を使用してインストールするには

- 次のコマンドを使用します。

```
helm repo add secrets-store-csi-driver https://kubernetes-sigs.github.io/secrets-store-csi-driver/charts
helm install -n kube-system csi-secrets-store secrets-store-csi-driver/secrets-store-csi-driver
kubectl apply -f https://raw.githubusercontent.com/aws/secrets-store-csi-driver-provider-aws/main/deployment/aws-provider-installer.yaml
```

インストールを検証する

EKS クラスター、Secrets Store CSI ドライバー、ASCP プラグインのインストールを検証するには、次の手順に従います。

1. EKS クラスターを検証します。

   ```
   eksctl get cluster --name clusterName
   ```

   このコマンドは、クラスターに関する情報を返します。

2. Secrets Store CSI ドライバーのインストールを検証します。

   ```
   kubectl get pods -n kube-system -l app=secrets-store-csi-driver
   ```

   `csi-secrets-store-secrets-store-csi-driver-xxx` のような名前の実行されているポッドが表示されます。

3. ASCP プラグインのインストールを検証します。

   YAML installation

   ```
   $ kubectl get pods -n kube-system -l app=csi-secrets-store-provider-aws
   ```

   出力例:

   ```
   NAME                                     READY   STATUS    RESTARTS   AGE
   csi-secrets-store-provider-aws-12345      1/1     Running   0          2m
   ```

   Helm installation

   ```
   $  kubectl get pods -n kube-system -l app=secrets-store-csi-driver-provider-aws
   ```

   出力例:

   ```
   NAME                                                READY   STATUS    RESTARTS
    AGE
   secrets-provider-aws-secrets-store-csi-driver-provider-67890       1/1
    Running   0          2m
   ```

Running 状態のポッドが表示されます。

これらのコマンドを実行した後に、すべてが正しく設定されている場合は、すべてのコンポーネントがエラーなく実行されます。問題が発生した場合は、問題が発生している特定のポッドのログを確認してトラブルシューティングする必要がある場合があります。

トラブルシューティング

1. ASCP プロバイダーのログを確認するには、以下を実行します。

```
kubectl logs -n kube-system -l app=csi-secrets-store-provider-aws
```

2. kube-system 名前空間内のすべてのポッドのステータスを確認します。

   default placeholder text を独自のポッド ID に置き換えます。

```
kubectl -n kube-system get pods
```

```
kubectl -n kube-system logs pod/pod-id
```

   CSI ドライバーと ASCP に関連するすべてのポッドが「Running」状態である必要があります。

3. CSI ドライバーのバージョンを確認します。

```
kubectl get csidriver secrets-store.csi.k8s.io -o yaml
```

   このコマンドは、インストールされている CSI ドライバーに関する情報を返します。

追加リソース

Amazon EKS での ASCP の使用に関する詳細については、次のリソースを参照してください。

- Amazon EKS で Pod Identity を使用する
- GitHub の AWS Secrets Store CSI ドライバー

Amazon EKS 用に AWS Secrets and Configuration Provider CSI を Pod Identity と使用する

Amazon Elastic Kubernetes Service 用の Pod Identity Agent との AWS Secrets and Configuration Provider の統合により、Amazon EKS で実行されているアプリケーションのセキュリティが強化され、設定が簡素化され、パフォーマンスが向上します。Pod Identity により、AWS Systems Manager Parameter Store からパラメータを取得するとき、または Secrets Manager からシークレットを取得するときに、Amazon EKS の AWS Identity and Access Management (IAM) 認証が簡素化されます。

Amazon EKS Pod Identity によって Amazon EKS インターフェイスを介してアクセス許可を直接設定できるようになるため、Kubernetes アプリケーションの IAM アクセス許可を設定するプロセスが合理化され、ステップ数が減少し、Amazon EKS と IAM サービスを切り替える必要がなくなります。Pod Identity では、信頼ポリシーを更新することなく複数のクラスターで 1 つの IAM ロールを使用でき、より詳細なアクセスコントロールのためのロールセッションタグがサポートされます。このアプローチでは、ロール間でアクセス許可ポリシーを再利用できるようにすることでポリシー管理が簡素化されるだけでなく、一致するタグに基づいて AWS リソースへのアクセスを有効にすることでセキュリティが強化されます。

仕組み

1. Pod Identity はポッドに IAM ロールを割り当てます。
2. ASCP はこのロールを使用して AWS のサービスで認証します。
3. 承認されると、ASCP はリクエストされたパラメータを取得し、ポッドで使用できるようにします。

詳細については、「Amazon EKS ユーザーガイド」の「EKS Pod Identity の仕組みを理解する」を参照してください。

前提条件

> **Important**
>
> Pod Identity は、クラウド内の Amazon EKS でのみサポートされています。Amazon EC2 インスタンスの Amazon EKS Anywhere、Red Hat OpenShift Service on AWS、またはセルフマネージド Kubernetes クラスターではサポートされていません。

- Amazon EKS クラスター (バージョン 1.24 以降)
- `kubectl` を介した AWS CLI および Amazon EKS クラスターへのアクセス
- (オプション) クロスアカウントアクセス用の 2 つの AWS アカウントへのアクセス

Amazon EKS Pod Identity Agent をインストールする

クラスターで Pod Identity を使用するには、Amazon EKS Pod Identity Agent アドオンをインストールする必要があります。

Pod Identity Agent をインストールするには

- Pod Identity Agent アドオンをクラスターにインストールします。

  `default placeholder text` を独自の値に置き換えます。

```
eksctl create addon \
  --name eks-pod-identity-agent \
  --cluster clusterName \
  --region region
```

Pod Identity を使用して ASCP を設定する

1. ポッドがアクセスする必要があるパラメータに `ssm:GetParameters` と `ssm:DescribeParameters` のアクセス許可を付与するアクセス許可ポリシーを作成します。
2. Pod Identity の Amazon EKS サービスプリンシパルが引き受けることができる IAM ロールを作成します。

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Principal": {
          "Service": "pods.eks.amazonaws.com"
        },
        "Action": [
          "sts:AssumeRole",
          "sts:TagSession"
        ]
```

```
      }
    ]
  }
```

IAM ポリシーをロールにアタッチします。

default placeholder text を独自の値に置き換えます。

```
aws iam attach-role-policy \
  --role-name MY_ROLE \
  --policy-arn POLICY_ARN
```

3. Pod Identity の関連付けを作成します。例については、「Amazon EKS ユーザーガイド」の「Pod Identity の関連付けを作成する」を参照してください。
4. ポッドにマウントするパラメータまたはシークレットを指定する SecretProviderClass を作成します。

```
kubectl apply -f kubectl apply -f https://raw.githubusercontent.com/aws/
secrets-store-csi-driver-provider-aws/main/examples/ExampleSecretProviderClass-
PodIdentity.yaml
```

SecretProviderClass における IRSA と Pod Identity の主な違いは、オプションのパラメータ usePodIdentity です。これは、認証アプローチを決定するオプションのフィールドです。指定しない場合、デフォルトではサービスアカウントの IAM ロール (IRSA) が使用されます。

- EKS Pod Identity を使用するには、"true", "True", "TRUE", "t", "T" のいずれかの値を使用します。
- IRSA を明示的に使用するには、"false", "False", "FALSE", "f", or "F" のいずれかの値に設定します。

5. /mnt/secrets-store の下に、パラメータまたはシークレットをマウントするポッドをデプロイします。

```
kubectl apply -f kubectl apply -f https://raw.githubusercontent.com/aws/secrets-
store-csi-driver-provider-aws/main/examples/ExampleDeployment-PodIdentity.yaml
```

6. プライベート Amazon EKS クラスターを使用する場合は、クラスターがある VPC に、AWS STS エンドポイントが存在していることを確認してください。エンドポイントの作成の詳細に

ついては、「AWS Identity and Access Management ユーザーガイド」の「インターフェイス VPC エンドポイント」を参照してください。

シークレットのマウントを検証する

パラメータまたはシークレットが正しくマウントされていることを検証するには、次のコマンドを実行します。

default placeholder text を独自の値に置き換えます。

```
kubectl exec -it $(kubectl get pods | awk '/pod-identity-deployment/{print $1}' | head
 -1) -- cat /mnt/secrets-store/MyParameter
```

Parameter Store のパラメータにアクセスするために Amazon EKS Pod Identity を設定するには

1. ポッドがアクセスする必要があるパラメータに `ssm:GetParameters` と `ssm:DescribeParameters` のアクセス許可を付与するアクセス許可ポリシーを作成します。
2. パラメータがまだない場合は、Parameter Store で作成します。詳細については、「Systems Manager での Parameter Store パラメータの作成」を参照してください。

トラブルシューティング

ポッドのデプロイを記述すると、ほとんどのエラーを表示できます。

コンテナのエラーメッセージを表示するには

1. 次のコマンドで、ポッド名のリストを取得します。デフォルトの名前空間を使用していない場合は、`-n` *namespace* を使用してください。

   ```
   kubectl get pods
   ```

2. 次のコマンドでポッドを記述するには、*pod-id* に前のステップで見つけたポッドのポッド ID を使用します。デフォルトの名前空間を使用していない場合は、`-n` *NAMESPACE* を使用してください。

   ```
   kubectl describe pod/pod-id
   ```

ASCP のエラーを表示するには

- プロバイダーログで詳細情報を検索するには、次のコマンドの *PODID* に、csi-secrets-store-provider-aws ポッドの ID を入力します。

```
kubectl -n kube-system get pods
kubectl -n kube-system logs pod/pod-id
```

AWS Secrets and Configuration Provider CSI をサービスアカウントの IAM ロール (IRSA) と使用する

トピック

- 前提条件
- アクセス制御を設定する
- マウントするパラメータを特定する
- トラブルシューティング

前提条件

- Amazon EKS クラスター (バージョン 1.17 以降)
- `kubectl` を介した AWS CLI および Amazon EKS クラスターへのアクセス

アクセス制御を設定する

ASCP は Amazon EKS Pod Identity を取得し、IAM ロールと交換します。その IAM ロールの IAM ポリシーでアクセス許可を設定します。ASCP が IAM ロールを引き受けると、承認されたパラメータへのアクセス許可が付与されます。他のコンテナは、IAM ロールに関連付けない限り、パラメータにアクセスできません。

Amazon EKS ポッドに Parameter Store のパラメータへのアクセスを許可するには

1. ポッドがアクセスする必要があるパラメータに `ssm:GetParameters` と `ssm:DescribeParameters` のアクセス許可を付与するアクセス許可ポリシーを作成します。
2. クラスター用に IAM OpenID Connect (OIDC) プロバイダーがない場合は作成します。詳細については、「Amazon EKS ユーザーガイド」の「クラスターに IAM OIDC プロバイダーを作成する」を参照してください。

3. サービスアカウントの IAM ロールを作成して、ポリシーをアタッチします。詳細については、「Amazon EKS ユーザーガイド」の「サービスアカウントの IAM ロールを作成する」を参照してください。
4. プライベート Amazon EKS クラスターを使用する場合は、クラスターがある VPC に、AWS STS エンドポイントが存在していることを確認してください。エンドポイントの作成の詳細については、「AWS Identity and Access Management ユーザーガイド」の「インターフェイス VPC エンドポイント」を参照してください。

マウントするパラメータを特定する

ASCP が (ファイルシステム上のファイルとして) Amazon EKS 内にマウントするパラメータを判別するには、the section called “SecretProviderClass” YAML ファイルを作成します。`SecretProviderClass` では、マウントするパラメータと、それらのマウントに使用されるファイル名がリストされます。`SecretProviderClass` は、参照する Amazon EKS ポッドと同じ名前空間にある必要があります。

パラメータをファイルとしてマウントする

次の手順は、サンプル YAML ファイル (ExampleSecretProviderClass.yaml と ExampleDeployment.yaml) を使用してパラメータをファイルとしてマウントする方法を示します。

Amazon EKS でパラメータをマウントするには

1. `SecretProviderClass` をポッドに適用します。

```
kubectl apply -f ExampleSecretProviderClass.yaml
```

2. ポッドをデプロイします。

```
kubectl apply -f ExampleDeployment.yaml
```

3. ASCP はファイルをマウントします。

トラブルシューティング

ポッドのデプロイを記述すると、ほとんどのエラーを表示できます。

コンテナのエラーメッセージを表示するには

1. 次のコマンドで、ポッド名のリストを取得します。デフォルトの名前空間を使用していない場合は、-n *name-space* を使用してください。

```
kubectl get pods
```

2. 次のコマンドでポッドを記述するには、*pod-id* に前のステップで見つけたポッドのポッド ID を使用します。デフォルトの名前空間を使用していない場合は、-n *nameSpace* を使用してください。

```
kubectl describe pod/pod-id
```

ASCP のエラーを表示するには

- プロバイダーログで詳細情報を検索するには、次のコマンドで *pod-id* 用に csi-secrets-store-provider-aws ポッドの ID を使用します。

```
kubectl -n kube-system get pods
kubectl -n kube-system logs Pod/pod-id
```

- **SecretProviderClass** CRD がインストールされていることを確認します。

```
kubectl get crd secretproviderclasses.secrets-store.csi.x-k8s.io
```

このコマンドは、SecretProviderClass カスタムリソース定義に関する情報を返します。

- SecretProviderClass オブジェクトが作成されたことを確認します。

```
kubectl get secretproviderclass SecretProviderClassName -o yaml
```

AWS Secrets and Configuration Provider のコード例

ASCP の認証とアクセスコントロールの例

例: Amazon EKS Pod Identity サービス (pods.eks.amazonaws.com) がロールを引き受け、セッションにタグを付けることを許可する IAM ポリシー:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "pods.eks.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:TagSession"
      ]
    }
  ]
}
```

SecretProviderClass

ASCP を使用して Amazon EKS にマウントするパラメータを YAML で記述します。例については「the section called “SecretProviderClass の使用”」を参照してください。

SecretProviderClass YAML 構造

```
apiVersion: secrets-store.csi.x-k8s.io/v1
kind: SecretProviderClass
metadata:
   name: name
spec:
  provider: aws
  parameters:
    region:
    failoverRegion:
    pathTranslation:
    usePodIdentity:
    preferredAddressType:
    objects:
```

パラメータフィールドには、以下のマウントリクエストの詳細が含まれます。

region

(オプション) パラメータの AWS リージョン。このフィールドを使用しない場合、ASCP はノード上のアノテーションからリージョンを検索します。この検索では、マウントリクエストにオーバーヘッドが追加されるため、大量のポッドを使用するクラスターでリージョンを指定することをお勧めします。

同時に `failoverRegion` も指定すると、ASCP は両方のリージョンからパラメータの取得を試行します。どちらかのリージョンが認証の問題などで `4xx` エラーを返した場合、ASCP はいずれのパラメータもマウントしません。パラメータが `region` から正常に取得されると、ASCP はそのパラメータ値をマウントします。`region` からはパラメータが正常に取得されないものの、`failoverRegion` からは正常に取得された場合、ASCP は取得された方のパラメータ値をマウントします。

`failoverRegion`

(オプション) このフィールドを含めると、ASCP は `region` で定義されているリージョンと、このフィールドで定義されているリージョンからのパラメータ取得を試行します。どちらかのリージョンが認証の問題などで `4xx` エラーを返した場合、ASCP はいずれのパラメータもマウントしません。パラメータが `region` から正常に取得されると、ASCP はそのパラメータ値をマウントします。`region` からはパラメータが正常に取得されないものの、`failoverRegion` からは正常に取得された場合、ASCP は取得された方のパラメータ値をマウントします。このフィールドの使用例については、「マルチリージョンパラメータのフェイルオーバー」を参照してください。

pathTranslation

(オプション) Amazon EKS のファイル名に、Linux のスラッシュ (/) のようなパス区切り文字が含まれている場合に使用する単一の置換文字。ASCP では、パス区切り文字が含まれているファイルを作成し、マウントすることはできません。代わりに、ASCP はパス区切り文字を別の文字に置き換えます。このフィールドを使用しない場合、置換文字にはアンダースコア (_) が使用されます。例えば、`My/Path/Parameter` は `My_Path_Parameter` としてマウントされます。

文字の置換を防ぐには、文字列 `False` を入力してください。

`usePodIdentity`

(オプション) 認証アプローチを決定します。指定しない場合、デフォルトではサービスアカウントの IAM ロール (IRSA) になります。

- EKS Pod Identity を使用するには、"true"、"True"、"TRUE"、"t"、または "T" のいずれかの値を使用します。
- IRSA を明示的に使用するには、"false"、"False"、"FALSE"、"f"、または "F""= のいずれかの値に設定します。

preferredAddressType

(オプション) Pod Identity Agent のエンドポイント通信の優先 IP アドレスタイプを指定します。このフィールドは EKS Pod Identity 機能を使用する場合にのみ適用され、サービスアカウントの IAM ロールを使用する場合は無視されます。値では大文字と小文字は区別されません。次の値を指定できます:

- "ipv4"、"IPv4"、または "IPV4" – Pod Identity Agent IPv4 エンドポイントの使用を強制します
- "ipv6"、"IPv6"、または "IPV6" – Pod Identity Agent IPv6 エンドポイントの使用を強制します
- 指定なし – 自動エンドポイント選択を使用し、最初に IPv4 エンドポイントを試して、IPv4 が失敗した場合は IPv6 エンドポイントにフォールバックします

objects

マウントするシークレットの YAML 宣言を含む文字列 YAML 複数行の文字列またはパイプ (|) 文字を使用することをお勧めします。

objectName

必須。取得するパラメータまたはシークレットの名前を指定します。Parameter Store の場合、これはパラメータの Name であり、パラメータの名前または完全な ARN のいずれかを使用できます。Secrets Manager の場合、これは SecretId パラメータであり、シークレットのわかりやすい名前または完全な ARN のいずれかを使用できます。

objectType

objectName で Secrets Manager ARN を使用しない場合は必須。Parameter Store の場合は、ssmparameter を使用します。Secrets Manager の場合は、secretsmanager を使用します。

objectAlias

(オプション) Amazon EKS ポッド内のシークレットのファイル名。このフィールドを指定しなかった場合、objectName がファイル名として表示されます。

objectVersion

(オプション) パラメータのバージョン ID。バージョン ID は、パラメータを変更するたびに更新の必要が生じるため、これは推奨されません。デフォルトでは、最新バージョンが使用されます。failoverRegion を含めると、このフィールドはプライマリの objectVersion になります。

objectVersionLabel

(オプション) バージョンのエイリアス デフォルトは最新バージョンの AWSCURRENT です。failoverRegion を含めると、このフィールドはプライマリの objectVersionLabel になります。

jmesPath

(オプション) パラメータのキーと、Amazon EKS にマウントされるファイルのマップ。このフィールドを使用するには、パラメータ値を JSON 形式にする必要があります。

以下の例は、JSON エンコードパラメータがどのようになるのかを示しています。

```
{
    "username" : "myusername",
    "password" : "mypassword"
}
```

キーは username と password です。username に関連付けられている値は myusername、password に関連付けられている値は mypassword です。

このフィールドを使用する場合は、サブフィールド path および objectAlias を含める必要があります。

パス

パラメータ値の JSON 内のキーと値のペアからのキー。フィールドにハイフンが含まれている場合は、一重引用符でエスケープします。例: path: '"hyphenated-path"'

objectAlias

Amazon EKS ポッドにマウントされるファイル名。フィールドにハイフンが含まれている場合は、一重引用符でエスケープします。例: objectAlias: '"hyphenated-alias"'

failoverObject

(オプション) このフィールドを指定した場合、ASCP はプライマリ objectName で指定されたパラメータと、failoverObject、objectName サブフィールドで指定されたパラメータ

の両方の取得を試行します。どちらかが認証の問題などで 4xx エラーを返した場合、ASCP はいずれのパラメータもマウントしません。パラメータがプライマリ objectName から正常に取得されると、ASCP はそのパラメータ値をマウントします。プライマリ objectName からはパラメータが正常に取得されないものの、フェイルオーバー objectName からは正常に取得された場合、ASCP は取得された方のパラメータ値をマウントします。このフィールドを含める場合は、フィールド objectAlias も含める必要があります。このフィールドの使用例については、「別のパラメータにフェイルオーバーする」を参照してください。

通常、このフィールドはフェイルオーバーパラメータがレプリカではない場合に使用します。レプリカを指定する際の例については、「マルチリージョンパラメータのフェイルオーバー」を参照してください。

objectName

フェイルオーバーパラメータの名前または完全な ARN。ARN を使用する場合、ARN 内のリージョンはフィールド failoverRegion と一致する必要があります。

objectVersion

(オプション) パラメータのバージョン ID。プライマリ objectVersion と一致している必要があります。バージョン ID は、パラメータを変更するたびに更新の必要が生じるため、これは推奨されません。デフォルトでは、最新バージョンが使用されます。

objectVersionLabel

(オプション) バージョンのエイリアス デフォルトは最新バージョンの AWSCURRENT です。

Amazon EKS ポッドにパラメータをマウントするための基本的な SecretProviderClass 設定を作成します。

Pod Identity

同じ Amazon EKS クラスターのパラメータを使用する SecretProviderClass:

```
apiVersion: secrets-store.csi.x-k8s.io/v1
kind: SecretProviderClass
metadata:
  name: aws-parameter-store
spec:
  provider: aws
  parameters:
```

```
    objects: |
      - objectName: "MyParameter"
        objectType: "ssmparameter"
    usePodIdentity: "true"
```

IRSA

```
apiVersion: secrets-store.csi.x-k8s.io/v1
kind: SecretProviderClass
metadata:
  name: deployment-aws-parameter
spec:
  provider: aws
  parameters:
    objects: |
        - objectName: "MyParameter"
          objectType: "ssmparameter"
```

SecretProviderClass の使用

これらの例を使用して、さまざまなシナリオの SecretProviderClass 設定を作成します。

例: 名前または ARN でパラメータをマウントする

この例では、3 つの異なるタイプのパラメータをマウントする方法を示します。

- 完全な ARN で指定されたパラメータ
- 名前で指定されたパラメータ
- シークレットのパラメータバージョン

```
apiVersion: secrets-store.csi.x-k8s.io/v1
kind: SecretProviderClass
metadata:
  name: aws-parameters
spec:
  provider: aws
  parameters:
    objects: |
      - objectName: "arn:aws:ssm:us-east-2:777788889999:parameter:MyParameter2-d4e5f6"
      - objectName: "MyParameter3"
```

```
        objectType: "ssmparameter"
      - objectName: "MyParameter4"
        objectType: "ssmparameter"
        objectVersionLabel: "AWSCURRENT"
```

例: パラメータからのキーと値のペアをマウントする

この例では、JSON 形式のパラメータから特定のキーと値のペアをマウントする方法を示します。

```
apiVersion: secrets-store.csi.x-k8s.io/v1
kind: SecretProviderClass
metadata:
  name: aws-parameters
spec:
  provider: aws
  parameters:
    objects: |
      - objectName: "arn:aws:ssm:us-east-2:777788889999:parameter:MyParameter-a1b2c3"
        jmesPath:
            - path: username
              objectAlias: dbusername
            - path: password
              objectAlias: dbpassword
```

例: フェイルオーバー設定の例

これらの例では、パラメータのフェイルオーバーを設定する方法を示します。

マルチリージョンパラメータのフェイルオーバー

この例では、複数のリージョンにレプリケートされたパラメータの自動フェイルオーバーを設定する方法を示します。

```
apiVersion: secrets-store.csi.x-k8s.io/v1
kind: SecretProviderClass
metadata:
  name: aws-parameters
spec:
  provider: aws
  parameters:
    region: us-east-1
    failoverRegion: us-east-2
    objects: |
```

```
      - objectName: "MyParameter"
```

別のパラメータにフェイルオーバーする

この例では、(レプリカではない) 別のパラメータへのフェイルオーバーを設定する方法を示します。

```
apiVersion: secrets-store.csi.x-k8s.io/v1
kind: SecretProviderClass
metadata:
  name: aws-parameters
spec:
  provider: aws
  parameters:
    region: us-east-1
    failoverRegion: us-east-2
    objects: |
      - objectName: "arn:aws:ssm:us-east-1:777788889999:parameter:MyParameter-a1b2c3"
        objectAlias: "MyMountedParameter"
        failoverObject:
          - objectName: "arn:aws:ssm:us-
east-2:777788889999:parameter:MyFailoverParameter-d4e5f6"
```

追加リソース

Amazon EKS での ASCP の使用に関する詳細については、次のリソースを参照してください。

- Amazon EKS で Pod Identity を使用する
- GitHub の AWS Secrets Store CSI ドライバー

AWS Lambda 関数での Parameter Store パラメーターの使用

AWS Systems Manager のツールである Parameter Store は、設定データ管理と機密管理のための安全な階層型ストレージを提供します。パスワード、データベース文字列、Amazon Machine Image (AMI) ID、ライセンスコードなどのデータをパラメータ値として保存することができます。

SDK を使用せずに AWS Lambda 関数の Parameter Store からパラメーターを使用するには、AWS パラメーターとシークレットの Lambda 拡張機能を使用できます。この拡張機能は、パラメータ値を取得して、今後使用するためにキャッシュします。Lambda 拡張機能を使用すると、Parameter Store への API コール回数が減り、コストを削減できます。拡張機能を使用すると、キャッシュされたパラメータを取得する方が、Parameter Store から取得するよりも高速になるため、待ち時間を短縮することもできます。

Lambda 拡張機能は、Lambda 関数の機能を強化するコンパニオンプロセスです。拡張機能は、Lambda 呼び出しと並行して実行されるクライアントのようなものです。この並列クライアントは、ライフサイクル中の任意の時点で関数とインターフェイスできます。Lambda 拡張機能の詳細については、AWS Lambda デベロッパーガイドの「Lambda 拡張機能 API」を参照してください。

AWS パラメータとシークレット Lambda 拡張機能は、Parameter Store と AWS Secrets Manager の両方で機能します。Secrets Manager のシークレットで Lambda 拡張機能を使用する方法については、AWS Secrets Manager ユーザーガイドの「AWS Lambda 関数での AWS Secrets Manager シークレットの使用」を参照してください。

関連情報

「パラメータとシークレット Lambda 拡張機能を使用して AWS パラメータとシークレットをキャッシュする」(AWS Compute ブログ)

拡張機能の仕組み

Lambda 拡張機能を利用せずに Lambda 関数でパラメータを使用する場合、Parameter Store の `GetParameter` API アクションと統合して、Lambda 関数が設定の更新を受信するように設定する必要があります。

AWS パラメータとシークレット Lambda 拡張機能を使用すると、拡張機能は Parameter Store からパラメータ値を取得し、ローカルキャッシュに保存します。その後、キャッシュされた値は、有効期限が切れるまで以降の呼び出しに使用されます。キャッシュ値は、期限 (TTL) を過ぎると期限切れになります。このトピックで後述するように、`SSM_PARAMETER_STORE_TTL` 環境変数 を使用して TTL 値を設定できます。

設定されたキャッシュ TTL の有効期限が切れていない場合は、キャッシュされたパラメータ値が使用されます。時間が経過すると、キャッシュされた値は無効になり、パラメータ値は Parameter Store から取得されます。

また、システムは頻繁に使用されるパラメータ値を検出し、期限切れまたは未使用のパラメータ値をクリアしながらキャッシュに保持します。

> **Important**
>
> この拡張機能は、Lambda オペレーションの `INVOKE` フェーズでのみ呼び出すことができ、`INIT` フェーズで呼び出すことはできません。

実装の詳細

AWS パラメータとシークレット Lambda 拡張機能の設定に役立つ以下の詳細情報を参考にしてください。

認証

Parameter Store リクエストを認可および認証するために、拡張機能は Lambda 関数自体の実行に使用されたものと同じ認証情報を使用します。そのため、関数の実行に使用する AWS Identity and Access Management (IAM) ロールには、Parameter Store と対話するための次の権限が必要です。

- `ssm:GetParameter` — Parameter Store からパラメータの取得に必要
- `kms:Decrypt` — Parameter Store から `SecureString` パラメータを取得するために必要

詳細については、「AWS Lambda デベロッパーガイド」の「AWS Lambda 実行ロール」を参照してください。

インスタンス化

Lambda は、関数が必要とする同時実行レベルに対応する個別のインスタンスをインスタンス化します。各インスタンスは分離され、設定データの独自のローカルキャッシュが保持されます。Lambda インスタンスと同時実行の詳細については、「AWS Lambda デベロッパーガイド」の「予約済同時実行数の設定」を参照してください。

SDK への依存なし

AWS パラメータとシークレット Lambda 拡張機能は、どの AWS SDK 言語ライブラリからも独立して動作します。Parameter Store に GET リクエストを行うのに AWS SDK は必要ありません。

Localhost ポート

GET リクエストに `localhost` を使用します。拡張機能は、localhost ポート 2773 に送信されます。拡張機能を使用する場合、外部または内部エンドポイントを指定する必要はありません。このポートを設定するには、環境変数 `PARAMETERS_SECRETS_EXTENSION_HTTP_PORT` を設定します。

たとえば、Python では、GET URL は次の例のようになります。

```
parameter_url = ('http://localhost:' + port + '/systemsmanager/parameters/get/?
name=' + ssm_parameter_path)
```

TTL 期限が切れる前にパラメータ値を変更します

拡張機能はパラメータ値の変更を検出せず、TTL の有効期限が切れる前に自動更新を実行しません。パラメータ値を変更すると、キャッシュされたパラメータ値を使用する操作は、キャッシュが次に更新されるまで失敗する可能性があります。パラメータ値が頻繁に変更されることが予想される場合は、TTL 値を短く設定することをお勧めします。

ヘッダー要件

拡張キャッシュからパラメータを取得するには、GET リクエストのヘッダーに `X-Aws-Parameters-Secrets-Token` 参照を含める必要があります。トークンを `AWS_SESSION_TOKEN` に設定します。これは実行中のすべての関数に対して Lambda によって提供されます。このヘッダーを使用すると、呼び出し元が Lambda 環境内にあることがわかります。

例

次の Python の例は、キャッシュされたパラメータの値を取得する基本的なリクエストを示しています。

```
import urllib.request
import os
import json

aws_session_token = os.environ.get('AWS_SESSION_TOKEN')

def lambda_handler(event, context):
    # Retrieve /my/parameter from Parameter Store using extension cache
    req = urllib.request.Request('http://localhost:2773/systemsmanager/parameters/
get?name=%2Fmy%2Fparameter')
    req.add_header('X-Aws-Parameters-Secrets-Token', aws_session_token)
    config = urllib.request.urlopen(req).read()

    return json.loads(config)
```

ARM サポート

この拡張機能は、x86_64 および x86 アーキテクチャがサポートされているほとんどの AWS リージョンで、ARM アーキテクチャをサポートしています。ARM アーキテクチャを使用している場合は、そのアーキテクチャがサポートされていることを確認することをお勧めします。拡張 ARN の完全なリストについては、AWS Parameters and Secrets Lambda Extension の ARN を参照してください。

ログ記録

Lambda は、Amazon CloudWatch Logs を使用して、Lambda 関数と共に Lambda 拡張機能に関する実行情報をログに記録します。デフォルトでは、Lambda 拡張機能は最小限の情報を CloudWatch に記録します。詳細をログに記録するには、環境変数 `PARAMETERS_SECRETS_EXTENSION_LOG_LEVEL` を `DEBUG` に設定します。

Lambda 関数への拡張機能の追加

AWS Parameters and Secrets Lambda Extension を使用するには、拡張機能を Lambda 関数にレイヤーとして追加します。

関数に拡張機能を追加するには、以下のいずれかの方法を使用します。

AWS Management Console (レイヤーオプションの追加)

1. AWS Lambda コンソールの https://console.aws.amazon.com/lambda/ を開いてください。
2. 関数を選択します。[Layers] (レイヤー) エリアで、[Add a layer] (レイヤーの追加) を選択します。
3. [Choose a layer] (レイヤーを選択) エリアで、[AWS layers] オプションを選択します。
4. [AWS layers] で、[AWS-Parameters-and-Secrets-Lambda-Extension] を選択し、バージョンを選択してから [Add] (追加) を選択します。

AWS Management Console (ARN オプションを指定)

1. AWS Lambda コンソールの https://console.aws.amazon.com/lambda/ を開いてください。
2. 関数を選択します。[Layers] (レイヤー) エリアで、[Add a layer] (レイヤーの追加) を選択します。
3. [Choose a layer] (レイヤーの選択) エリアで、[Specify an ARN] (ARN の指定) オプションを選択します。
4. [Specify an ARN] (ARN の指定) に、AWS リージョン およびアーキテクチャの拡張子 ARN を入力し、[Add] (追加) を選択します。

AWS Command Line Interface

AWS CLI で、次のコマンドを実行します。各##############をユーザー自身の情報に置き換えます。

```
aws lambda update-function-configuration \
```

```
    --function-name function-name \
    --layers layer-ARN
```

関連情報

Lambda 関数でのレイヤーの使用

拡張子の設定 (.zip ファイルアーカイブ)

AWS Parameters and Secrets Lambda Extension の環境変数

拡張機能を設定するには、次の 環境変数を変更します。現在の設定を表示するには、PARAMETERS_SECRETS_EXTENSION_LOG_LEVEL を DEBUG に設定します。詳細については、「AWS Lambda デベロッパーガイド」の「AWS Lambda 環境変数の使用」を参照してください。

> **Note**
>
> AWS Lambda は、Lambda 拡張機能と Lambda 関数に関する操作の詳細を Amazon CloudWatch Logs に記録します。

環境変数	詳細	必須	有効な値	デフォルト値
SSM_PARAMETER_STORE_TIMEOUT_MILLIS	Parameter Store へのリクエストのタイムアウト (ミリ秒単位)。 0 (ゼロ) 値は、タイムアウトは発生しません。	いいえ	すべての整数	0 (ゼロ)
SECRETS_MANAGER_TIMEOUT_MILLIS	Secrets Manager へのリクエストのタイムアウト (ミリ秒単位)。	いいえ	すべての整数	0 (ゼロ)

環境変数	詳細	必須	有効な値	デフォルト値
	0 (ゼロ) 値は、タイムアウトは発生しません。			
SSM_PARAMETER_STORE_TTL	キャッシュ内のパラメータが無効になるまでの最大有効期間 (秒単位)。0 (ゼロ) 値は、キャッシュをバイパスする必要があることを示します。PARAMETERS_SECRETS_EXTENSION_CACHE_SIZE の値が 0 (ゼロ) の場合、この変数は無視されます。	いいえ	0 (ゼロ) から 300 秒 (5 分)	300 秒 (5 分)

環境変数	詳細	必須	有効な値	デフォルト値
SECRETS_MANAGER_TTL	キャッシュ内のシークレットが無効になるまでの最大有効期間 (秒単位)。0 (ゼロ) 値は、キャッシュがバイパスされたことを示します。PARAMETERS_SECRETS_EXTENSION_CACHE_SIZE の値が 0 (ゼロ) の場合、この変数は無視されます。	いいえ	0 (ゼロ) から 300 秒 (5 分)	300 秒 (5 分)
PARAMETERS_SECRETS_EXTENSION_CACHE_ENABLED	拡張機能のキャッシュが有効になっているかどうかを決定します。重要な値: TRUE | FALSE	いいえ	TRUE、FALSE	正

環境変数	詳細	必須	有効な値	デフォルト値
PARAMETERS_SECRETS_EXTENSION_CACHE_SIZE	アイテム数に関するキャッシュの最大サイズ。0 (ゼロ) 値は、キャッシュがバイパスされたことを示します。両方のキャッシュ TTL 値が 0 (ゼロ) の場合、この変数は無視されます。	いいえ	0 (ゼロ) から 1000	1,000
PARAMETERS_SECRETS_EXTENSION_HTTP_PORT	ローカル HTTP サーバーのポート。	いいえ	1 - 65535	2773

環境変数	詳細	必須	有効な値	デフォルト値
PARAMETERS_SECRETS_EXTENSION_MAX_CONNECTIONS	拡張機能が Parameter Store または Secrets Manager へのリクエストに使用する HTTP クライアントの最大接続数。これは、Secrets Manager クライアントと Parameter Store クライアントの両方がバックエンドサービスに対して行う接続数のクライアントごとの設定です。	いいえ	最小 1、上限なし。	3

環境変数	詳細	必須	有効な値	デフォルト値
PARAMETERS_SECRETS_EXTENSION_LOG_LEVEL	拡張機能の口グに報告された詳細レベル。 拡張機能をセットアップしてテストする際は、キャッシュ構成に関する最も詳細に知るには DEBUG を使用することをお勧めします。 Lambda 操作の口グは、関連する CloudWatch Logs 口ググループに自動的にプッシュ配信されます。	いいえ	DEBUG | WARN | ERROR | NONE | INFO	INFO

AWS Systems Manager、Parameter Store および AWS Secrets Manager 拡張機能を使用するサンプルコマンド

このセクションの例は、AWS Systems Manager、Parameter Store および AWS Secrets Manager 拡張機能で使用する API アクションを示しています。

Parameter Store に対するサンプルコマンド

Lambda 拡張機能は、GetParameter API アクションへの読み取り専用アクセスを使用します。

このアクションを呼び出すには、次のような HTTP GET 呼び出しを行います。このコマンド形式では、標準パラメータ層のパラメータにアクセスできます。

```
GET http://localhost:port/systemsmanager/parameters/get?name=parameter-
name&version=version&label=label&withDecryption={true|false}
```

このサンプルの *parameter-name* は、階層内にないパラメータのための MyParameter、または階層の一部である /Dev/Production/East/Project-ABC/MyParameter という名前のパラメータのための %2FDev%2FProduction%2FEast%2FProject-ABC%2FMyParameter などの完全なパラメータ名を表しています。

> **Note**
>
> GET 呼び出しを使用する場合、特殊文字を保存するために、パラメータ値を HTTP 用にエンコードする必要があります。たとえば、/a/b/c のように階層パスをフォーマットする代わりに、%2Fa%2Fb%2Fc など、URL の一部として解釈できる文字をエンコードします。

version と *label* は、GetParameter アクションとの使用に利用できるセレクターです。

```
GET http://localhost:port/systemsmanager/parameters/get/?name=MyParameter&version=5
```

階層内のパラメータを呼び出すには、次のような HTTP GET 呼び出しを行います。

```
GET http://localhost:port/systemsmanager/parameters/get?name=%2Fa%2Fb%2F&label=release
```

パブリック (グローバル) のパラメータを呼び出すには、次のような HTTP GET 呼び出しを行います。

```
GET http://localhost:port/systemsmanager/parameters/get/?name=%2Faws%2Fservice%20list
%2F…
```

Parameter Store 参照を使用して Secrets Manager シークレットに HTTP GET 呼び出しを行うには、次のような HTTP GET 呼び出しを行います。

```
GET http://localhost:port/systemsmanager/parameters/get?name=%2Faws%2Freference
%2Fsecretsmanager%2F…
```

パラメータの Amazon リソースネーム(ARN) を使用して呼び出しを行うには、次のような HTTP GET 呼び出しを行います。

```
GET http://localhost:port/systemsmanager/parameters/get?name=arn:aws:ssm:us-
east-1:123456789012:parameter/MyParameter
```

復号化を使用して SecureString パラメータにアクセスする呼び出しを行うには、次のような HTTP GET 呼び出しを行います。

```
GET http://localhost:port/systemsmanager/parameters/get?
name=MyParameter&withDecryption=true
```

withDecryption を省略するか、明示的に false に設定することで、パラメータが復号化されないように指定できます。バージョンまたはラベルのいずれかを指定することもできますが、両方を指定することはできません。その場合、URL のクエスチョンマーク (?) の後に置かれた最初のものだけが使用されます。

AWS Parameters and Secrets Lambda Extension の ARN

次の表は、サポートされているアーキテクチャとリージョンの拡張 ARN を示しています。

トピック

- x86_64 および x86 アーキテクチャの拡張 ARN
- ARM64 および Mac with Apple silicon アーキテクチャの拡張 ARN

x86_64 および x86 アーキテクチャの拡張 ARN

最終更新日: 2025 年 4 月 23 日

リージョン	ARN
米国東部(オハイオ)	arn:aws:lambda:us-east-2:590474943231:layer:AWS-Parameters-and-Secrets-Lambda-Extension:21
米国東部 (バージニア北部)	arn:aws:lambda:us-east-1:177933569100:layer:AWS-Parameters-and-Secrets-Lambda-Extension:17

リージョン	ARN
米国西部 (北カリフォルニア)	arn:aws:lambda:us-west-1:997803712105:layer:AWS-Parameters-and-Secrets-Lambda-Extension:17
米国西部 (オレゴン)	arn:aws:lambda:us-west-2:345057560386:layer:AWS-Parameters-and-Secrets-Lambda-Extension:17
アフリカ (ケープタウン)	arn:aws:lambda:af-south-1:317013901791:layer:AWS-Parameters-and-Secrets-Lambda-Extension:17
アジアパシフィック (香港)	arn:aws:lambda:ap-east-1:768336418462:layer:AWS-Parameters-and-Secrets-Lambda-Extension:19
アジアパシフィック (ハイデラバード) リージョン	arn:aws:lambda:ap-south-2:070087711984:layer:AWS-Parameters-and-Secrets-Lambda-Extension:14
アジアパシフィック (ジャカルタ)	arn:aws:lambda:ap-southeast-3:490737872127:layer:AWS-Parameters-and-Secrets-Lambda-Extension:17
アジアパシフィック (メルボルン)	arn:aws:lambda:ap-southeast-4:090732460067:layer:AWS-Parameters-and-Secrets-Lambda-Extension:7

リージョン	ARN
アジアパシフィック (マレーシア)	arn:aws:lambda:ap-southeast-5:381492012281:layer:AWS-Parameters-and-Secrets-Lambda-Extension:6
アジアパシフィック (ムンバイ)	arn:aws:lambda:ap-south-1:176022468876:layer:AWS-Parameters-and-Secrets-Lambda-Extension:17
アジアパシフィック (大阪)	arn:aws:lambda:ap-northeast-3:576959938190:layer:AWS-Parameters-and-Secrets-Lambda-Extension:17
アジアパシフィック (ソウル)	arn:aws:lambda:ap-northeast-2:738900069198:layer:AWS-Parameters-and-Secrets-Lambda-Extension:17
アジアパシフィック (シンガポール)	arn:aws:lambda:ap-southeast-1:044395824272:layer:AWS-Parameters-and-Secrets-Lambda-Extension:17
アジアパシフィック (シドニー)	arn:aws:lambda:ap-southeast-2:665172237481:layer:AWS-Parameters-and-Secrets-Lambda-Extension:17
アジアパシフィック (タイ)	arn:aws:lambda:ap-southeast-7:941377119484:layer:AWS-Parameters-and-Secrets-Lambda-Extension:5

リージョン	ARN
アジアパシフィック (東京)	arn:aws:lambda:ap-northeast-1:133490724326:layer:AWS-Parameters-and-Secrets-Lambda-Extension:17
カナダ (中部)	arn:aws:lambda:ca-central-1:200266452380:layer:AWS-Parameters-and-Secrets-Lambda-Extension:19
カナダ西部 (カルガリー)	arn:aws:lambda:ca-west-1:243964427225:layer:AWS-Parameters-and-Secrets-Lambda-Extension:7
中国 (北京)	arn:aws-cn:lambda:cn-north-1:287114880934:layer:AWS-Parameters-and-Secrets-Lambda-Extension:17
中国 (寧夏)	arn:aws-cn:lambda:cn-northwest-1:287310001119:layer:AWS-Parameters-and-Secrets-Lambda-Extension:17
欧州 (フランクフルト)	arn:aws:lambda:eu-central-1:187925254637:layer:AWS-Parameters-and-Secrets-Lambda-Extension:17
欧州 (アイルランド)	arn:aws:lambda:eu-west-1:015030872274:layer:AWS-Parameters-and-Secrets-Lambda-Extension:17

リージョン	ARN
欧州 (ロンドン)	arn:aws:lambda:eu-west-2:133256977650:layer:AWS-Parameters-and-Secrets-Lambda-Extension:17
欧州 (ミラノ)	arn:aws:lambda:eu-south-1:325218067255:layer:AWS-Parameters-and-Secrets-Lambda-Extension:17
欧州 (パリ)	arn:aws:lambda:eu-west-3:780235371811:layer:AWS-Parameters-and-Secrets-Lambda-Extension:17
欧州 (スペイン) リージョン	arn:aws:lambda:eu-south-2:524103009944:layer:AWS-Parameters-and-Secrets-Lambda-Extension:16
欧州 (ストックホルム)	arn:aws:lambda:eu-north-1:427196147048:layer:AWS-Parameters-and-Secrets-Lambda-Extension:17
イスラエル (テルアビブ)	arn:aws:lambda:il-central-1:148806536434:layer:AWS-Parameters-and-Secrets-Lambda-Extension:7
欧州 (チューリッヒ) リージョン	arn:aws:lambda:eu-central-2:772501565639:layer:AWS-Parameters-and-Secrets-Lambda-Extension:14

リージョン	ARN
メキシコ (中部) リージョン	arn:aws:lambda:mx-central-1:241533131596:layer:AWS-Parameters-and-Secrets-Lambda-Extension:4
中東 (バーレーン)	arn:aws:lambda:me-south-1:832021897121:layer:AWS-Parameters-and-Secrets-Lambda-Extension:17
中東 (アラブ首長国連邦)	arn:aws:lambda:me-central-1:858974508948:layer:AWS-Parameters-and-Secrets-Lambda-Extension:17
南米 (サンパウロ)	arn:aws:lambda:sa-east-1:933737806257:layer:AWS-Parameters-and-Secrets-Lambda-Extension:17
AWS GovCloud (米国東部)	arn:aws-us-gov:lambda:us-gov-east-1:129776340158:layer:AWS-Parameters-and-Secrets-Lambda-Extension:17
AWS GovCloud (米国西部)	arn:aws-us-gov:lambda:us-gov-west-1:127562683043:layer:AWS-Parameters-and-Secrets-Lambda-Extension:17

ARM64 および Mac with Apple silicon アーキテクチャの拡張 ARN

最終更新日: 2025 年 4 月 23 日

リージョン	ARN
米国東部(オハイオ)	arn:aws:lambda:us-east-2:590474943231:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:21
米国東部 (バージニア北部)	arn:aws:lambda:us-east-1:177933569100:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:17
US West (N. California) リージョン	arn:aws:lambda:us-west-1:997803712105:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:14
米国西部 (オレゴン)	arn:aws:lambda:us-west-2:345057560386:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:17
アフリカ (ケープタウン) リージョン	arn:aws:lambda:af-south-1:317013901791:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:14
アジアパシフィック (香港) リージョン	arn:aws:lambda:ap-east-1:768336418462:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:16
アジアパシフィック (ハイデラバード) リージョン	arn:aws:lambda:ap-south-2:070087711984:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:6

リージョン	ARN
アジアパシフィック (ジャカルタ) リージョン	arn:aws:lambda:ap-southeast-3:490737872127:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:14
アジアパシフィック (メルボルン)	arn:aws:lambda:ap-southeast-4:090732460067:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:6
アジアパシフィック (マレーシア)	arn:aws:lambda:ap-southeast-5:381492012281:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:6
アジアパシフィック (ムンバイ)	arn:aws:lambda:ap-south-1:176022468876:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:17
アジアパシフィック (大阪)	arn:aws:lambda:ap-northeast-3:576959938190:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:14
アジアパシフィック (ソウル) リージョン	arn:aws:lambda:ap-northeast-2:738900069198:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:14
アジアパシフィック (シンガポール)	arn:aws:lambda:ap-southeast-1:044395824272:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:17

リージョン	ARN
アジアパシフィック (シドニー)	arn:aws:lambda:ap-southeast-2:665172237481:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:17
アジアパシフィック (タイ)	arn:aws:lambda:ap-southeast-7:941377119484:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:4
アジアパシフィック (東京)	arn:aws:lambda:ap-northeast-1:133490724326:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:17
カナダ (中部) リージョン	arn:aws:lambda:ca-central-1:200266452380:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:16
カナダ西部 (カルガリー)	arn:aws:lambda:ca-west-1:243964427225:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:6
中国 (北京)	arn:aws-cn:lambda:cn-north-1:287114880934:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:6
中国 (寧夏)	arn:aws-cn:lambda:cn-northwest-1:287310001119:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:6

リージョン	ARN
欧州 (フランクフルト)	arn:aws:lambda:eu-central-1:187925254637:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:17
欧州 (アイルランド)	arn:aws:lambda:eu-west-1:015030872274:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:17
欧州 (ロンドン)	arn:aws:lambda:eu-west-2:133256977650:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:17
欧州 (ミラノ) リージョン	arn:aws:lambda:eu-south-1:325218067255:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:14
欧州 (パリ) リージョン	arn:aws:lambda:eu-west-3:780235371811:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:14
欧州 (スペイン) リージョン	arn:aws:lambda:eu-south-2:524103009944:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:8
欧州 (ストックホルム) リージョン	arn:aws:lambda:eu-north-1:427196147048:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:14

リージョン	ARN
イスラエル (テルアビブ)	arn:aws:lambda:il-central-1:148806536434:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:6
欧州 (チューリッヒ) リージョン	arn:aws:lambda:eu-central-2:772501565639:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:6
メキシコ (中部) リージョン	arn:aws:lambda:mx-central-1:241533131596:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:3
中東 (バーレーン) リージョン	arn:aws:lambda:me-south-1:832021897121:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:14
中東 (アラブ首長国連邦)	arn:aws:lambda:me-central-1:858974508948:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:6
南米 (サンパウロ) リージョン	arn:aws:lambda:sa-east-1:933737806257:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:14
AWS GovCloud (米国東部)	arn:aws-us-gov:lambda:us-gov-east-1:129776340158:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:6

リージョン	ARN
AWSGovCloud(米国西部)	`arn:aws-us-gov:lambda:us-gov-west-1:127562683043:layer:AWS-Parameters-and-Secrets-Lambda-Extension-Arm64:6`

その他の製品やサービスとの統合

AWS Systems Manager には、次の表に示す製品とサービスの統合が組み込まれています。

Ansible	Ansible は、アプリケーションとシステムのデプロイを容易にする IT オートメーションプラットフォームです。 Systems Manager には、Systems Manager ドキュメント (SSM ドキュメント) `AWS-ApplyAnsiblePlaybooks` が用意されています。これにより、Ansible プレイブックを実行する State Manager の関連付けを作成できます。 詳細はこちら Ansible プレイブックを実行する関連付けの作成
Chef	Chef は、アプリケーションとシステムのデプロイを容易にする IT オートメーションツールです。 Systems Manager には `AWS-ApplyChefRecipes` SSM ドキュメントが用意されています。これにより、Chef レシピを実行する、AWS Systems Manager のツールである State Manager の関連付けを作成できます。 詳細はこちら

	Chef recipe を実行する関連付けの作成 Systems Manager は Chef InSpec プロファイルとも統合されるため、コンプライアンススキャンを実行したり、準拠および非準拠のノードを表示したりできます。 詳細はこちら Systems Manager Compliance で Chef InSpec プロファイルを使用する
GitHub	GitHub は、ソフトウェア開発のバージョン管理とコラボレーションのためのホスティングを提供します。 Systems Manager には、GitHub に格納されている他の SSM ドキュメントを実行できる SSM ドキュメント AWS-RunDocument と、GitHub に格納されているスクリプトを実行できる SSM ドキュメント AWS-RunRemoteScript が用意されています。 詳細はこちら • 遠隔で ドキュメントを実行する • GitHub からのスクリプトの実行

Jenkins	Jenkins は、デベロッパーがソフトウェアを確実に構築、テスト、デプロイできるようにするオープンソースのオートメーションサーバーです。 Systems Manager のツールである Automation は、Amazon Machine Images (AMIs) にアプリケーションリリースをプレインストールするためのビルド後のステップとして使用できます。 詳細はこちら オートメーションと Jenkins を使用した AMIs の更新
ServiceNow	ServiceNow は、IT サービスと運用を管理できるエンタープライズサービス管理システムです。 Automation、Change Manager、Incident Manager、および OpsCenter (すべて Systems Manager のツール) は、AWS Service Management Connector を使用して ServiceNow と統合できます。この統合により、ServiceNow から AWS サポート ケースの表示、作成、更新、対応の追加、および解決を行うことができます。 詳細はこちら ServiceNow との統合

Terraform	HashiCorp Terraform は、さまざまなクラウドサービスを管理するためのコマンドラインインターフェイス (CLI) ワークフローを提供するオープンソースの Infrastructure as code (IaC) ソフトウェアツールです。Systems Manager では、Terraform を使用して以下の要素を管理またはプロビジョニングできます。 リソース • aws_ssm_activation • aws_ssm_association • aws_ssm_default_patch_baseline • aws_ssm_document • aws_ssm_maintenance_window • aws_ssm_maintenance_window_target • aws_ssm_maintenance_window_task • aws_ssm_parameter • aws_ssm_patch_baseline • aws_ssm_patch_group • aws_ssm_resource_data_sync • aws_ssm_service_setting データソース • aws_ssm_document • aws_ssm_instances • ssm_maintenance_windows • aws_ssm_parameter • aws_ssm_parameters_by_path • aws_ssm_patch_baseline

トピック

- GitHub からのスクリプトの実行
- Systems Manager Compliance で Chef InSpec プロファイルを使用する
- ServiceNow との統合

GitHub からのスクリプトの実行

このトピックでは、事前定義された Systems Manager ドキュメント (SSM ドキュメント) `AWS-RunRemoteScript` を使用して、Ansible プレイブック、Python、Ruby、および PowerShell スクリプトなどのスクリプトを GitHub からダウンロードする方法について説明します。この SSM ドキュメントを使用することで、スクリプトを手動で Amazon Elastic Compute Cloud (Amazon EC2) にポーティングしたり、SSM ドキュメントにラップしたりする必要はなくなりました。AWS Systems Manager と GitHub との統合により、Infrastructure as Code (コードとしてのインフラストラクチャ) が促進され、フリート全体の設定を標準化しながらノードを管理する時間が短縮されます。

リモートの場所からスクリプトやその他の SSM ドキュメントをダウンロードして実行できる、カスタム SSM ドキュメントを作成することもできます。詳細については、「複合ドキュメントの作成」を参照してください。

複数のスクリプトを含むディレクトリをダウンロードすることもできます。ディレクトリ内でプライマリスクリプトを実行すると、Systems Manager はディレクトリに含まれている参照されるスクリプトも実行します。

GitHub からのスクリプトの実行に関する以下の重要な詳細をメモします。

- Systems Manager は、スクリプトがノードで実行できるかどうかを検証しません。スクリプトをダウンロードして実行する前に、必要なソフトウェアがノードにインストールされていることを確認してください。または、複合ドキュメントを作成することで、Run Command か、AWS Systems Manager のツールである State Manager のいずれかを使用してソフトウェアをインストールし、さらにスクリプトをダウンロードして実行することができます。
- お客様には、すべての GitHub 要件が満たされていることを確認する責任があります。これには、必要に応じてアクセストークンを更新することが含まれます。また、認証されたリクエストまたは認証されていないリクエストの数が超過しないようにしてください。詳細については、GitHub ドキュメントを参照してください。
- GitHub Enterprise リポジトリはサポートされていません。

トピック

- GitHub から Ansible プレイブックを実行する
- GitHub から Python スクリプトを実行する

GitHub から Ansible プレイブックを実行する

このセクションでは、コンソールまたは AWS Command Line Interface (AWS CLI) を使用して、GitHub から Ansible プレイブックを実行する手順を説明します。

開始する前に

プライベート GitHub リポジトリに保存されているスクリプトを実行する場合は、GitHub セキュリティアクセストークンの AWS Systems Manager `SecureString` パラメータを作成します。SSH 経由でトークンを手動で渡すことで、プライベート GitHub リポジトリのスクリプトにアクセスすることはできません。アクセストークンは、Systems Manager `SecureString` パラメータとして渡す必要があります。`SecureString` パラメータの作成の詳細については、「Systems Manager での Parameter Store パラメータの作成」を参照してください。

GitHub から Ansible プレイブックを実行する (コンソール)

GitHub から Ansible プレイブックを実行する

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Run Command] を選択します。
3. [コマンドの実行] を選択します。
4. [コマンドのドキュメント] リストで、[**AWS-RunRemoteScript**] を選択します。
5. [コマンドパラメータ] で、以下の作業を行います。
   - [ソースタイプ] で、[GitHub] を選択します。
   - [ソース情報] ボックスに、ソースにアクセスするために必要な情報を次の形式で入力します。

```
{
  "owner": "owner_name",
  "repository": "repository_name",
  "getOptions": "branch:branch_name",
  "path": "path_to_scripts_or_directory",
  "tokenInfo": "{{ssm-secure:SecureString_parameter_name}}"
}
```

この例では、webserver.yml という名前のファイルがダウンロードされます。

```
{
    "owner": "TestUser1",
    "repository": "GitHubPrivateTest",
    "getOptions": "branch:myBranch",
    "path": "scripts/webserver.yml",
    "tokenInfo": "{{ssm-secure:mySecureStringParameter}}"
}
```

> **Note**
>
> "branch" は、SSM ドキュメントが 以外のブランチに保存されている場合にのみ必要です。master
> リポジトリ内の特定のコミットにあるバージョンのスクリプトを使用するには、commitID ではなく、getOptions を指定して branch を使用します。以下に例を示します。
> "getOptions": "commitID:bbc1ddb94...b76d3bEXAMPLE",

- [コマンドライン] フィールドに、スクリプトの実行に必要なパラメータを入力します。以下はその例です。

  ansible-playbook -i “localhost,” --check -c local webserver.yml

- (オプション) [作業ディレクトリ] に、スクリプトをダウンロードして実行する先の、ノードのディレクトリの名前を入力します。
- (オプション) [実行タイムアウト] に、スクリプトコマンドの実行を失敗とするまでにシステムが待機する秒数を指定します。

6. [ターゲット] セクションで、タグの指定、インスタンスやエッジデバイスの手動選択、リソースグループの指定により、このオペレーションを実行するマネージドノードを選択します。

> **Tip**
>
> 表示されるはずのマネージドノードが表示されない場合は、トラブルシューティングのヒントについて「マネージドノードの可用性のトラブルシューティング」を参照してください。

7. [その他のパラメータ] で、以下の操作を行います。

- [コメント] に、このコマンドに関する情報を入力します。
- [タイムアウト (秒)] に、コマンドの実行全体が失敗するまでにシステムが待機する秒数を指定します。

8. [レート制御] の場合:

   - [同時実行数] の場合、コマンドを同時に実行するマネージドノードの数または割合を指定します。

     > **Note**
     >
     > マネージドノードに適用されるタグを指定するか、AWS リソースグループを指定してターゲットを選択し、ターゲットとなるマネージドノードの数が不明な場合は、割合を指定してドキュメントを同時に実行できるターゲットの数を制限します。

   - [エラーのしきい値] で、ノードの数または割合のいずれかで失敗した後、他のマネージドノードでのコマンドの実行をいつ停止するか指定します。例えば、3 つのエラーを指定した場合、4 番目のエラーが受信されると、Systems Manager はコマンドの送信を停止します。コマンドを処理しているマネージドノードもエラーを送信する可能性があります。

9. (オプション) コマンド出力をファイルに保存する場合は、[出力オプション] の [S3 バケットにコマンド出力を書き込む] ボックスを選択します。ボックスにバケット名とプレフィックス (フォルダ) 名を入力します。

   > **Note**
   >
   > S3 バケットにデータを書き込む機能を許可する S3 許可は、このタスクを実行する IAM ユーザーのものではなく、インスタンスに割り当てられたインスタンスプロファイル (EC2 インスタンスの場合) または IAM サービスロール (ハイブリッドアクティベーションマシン) のものです。詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」または「ハイブリッド環境に IAM サービスロールを作成する」を参照してください。さらに、指定された S3 バケットが別の AWS アカウント にある場合は、マネージドノードに関連付けられたインスタンスプロファイルまたは IAM サービスロールが、そのバケットへの書き込みに必要なアクセス許可があることを確認してください。

10. [SNS Notifications (SNS 通知)] セクションで、コマンドの実行状態に関する通知を受け取る場合は、[Enable SNS notifications (SNS 通知を有効にする)] チェックボックスをオンにします。

Run Command 用の Amazon SNS 通知の設定の詳細については、「Amazon SNS 通知を使用した Systems Manager のステータス変更のモニタリング」を参照してください。

11. [Run (実行)] を選択します。

AWS CLI を使用して、GitHub から Ansible プレイブックを実行する

1. まだ AWS Command Line Interface (AWS CLI) をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」を参照してください。

2. GitHub からスクリプトをダウンロードして実行するには、次のコマンドを実行します。

```
aws ssm send-command \
    --document-name "AWS-RunRemoteScript" \
    --instance-ids "instance-IDs"\
    --parameters '{"sourceType":["GitHub"],"sourceInfo":["{\"owner
\":\"owner_name\", \"repository\": \"repository_name\", \"path
\": \"path_to_file_or_directory\", \"tokenInfo\":\"{{ssm-
secure:name_of_your_SecureString_parameter}}\" }"],"commandLine":
["commands_to_run"]}'
```

   ローカル Linux マシン上で実行するコマンドの例を次に示します。

```
aws ssm send-command \
    --document-name "AWS-RunRemoteScript" \
    --instance-ids "i-02573cafcfEXAMPLE" \
    --parameters '{"sourceType":["GitHub"],"sourceInfo":["{\"owner\":\"TestUser1\",
 \"repository\": \"GitHubPrivateTest\", \"path\": \"scripts/webserver.yml\",
 \"tokenInfo\":\"{{ssm-secure:mySecureStringParameter}}\" }"],"commandLine":
["ansible-playbook -i “localhost,” --check -c local webserver.yml"]}'
```

GitHub から Python スクリプトを実行する

このセクションでは、AWS Systems Manager コンソールまたは AWS Command Line Interface (AWS CLI) を使用して、GitHub から Python スクリプトを実行する手順を説明します。

GitHub から Python スクリプトを実行する (コンソール)

GitHub から Python スクリプトを実行する

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[Run Command] を選択します。
3. [コマンドの実行] を選択します。
4. [Command document (コマンドのドキュメント)] リストで、[**AWS-RunRemoteScript**] を選択します。
5. [コマンドのパラメータ] で、以下の作業を行います。

   - [ソースタイプ] で、[GitHub] を選択します。
   - [Source Info (ソース情報)] ボックスに、ソースにアクセスするために必要な情報を次の形式で入力します。

```
{
    "owner": "owner_name",
    "repository": "repository_name",
    "getOptions": "branch:branch_name",
    "path": "path_to_document",
    "tokenInfo": "{{ssm-secure:SecureString_parameter_name}}"
}
```

   たとえば次の例では、complex-script という名前のスクリプトのディレクトリをダウンロードします。

```
{
    "owner": "TestUser1",
    "repository": "SSMTestDocsRepo",
    "getOptions": "branch:myBranch",
    "path": "scripts/python/complex-script",
    "tokenInfo": "{{ssm-secure:myAccessTokenParam}}"
}
```

> **Note**
>
> "branch" は、スクリプトが 以外のブランチに保存されている場合にのみ必要です。master

リポジトリ内の特定のコミットにあるバージョンのスクリプトを使用するには、commitID ではなく、getOptions を指定して branch を使用します。以下に例を示します。
"getOptions": "commitID:bbc1ddb94...b76d3bEXAMPLE",

- [Command Line (コマンドライン)] に、スクリプト実行用のパラメータを入力します。以下はその例です。

```
mainFile.py argument-1 argument-2
```

この例では mainFile.py を実行し、complex-script ディレクトリ内の他のスクリプトを実行できます。

- (オプション) [Working Directory] (作業ディレクトリ) に、スクリプトをダウンロードして実行する先の、ノードのディレクトリの名前を入力します。
- (オプション) [Execution Timeout (実行タイムアウト)] に、スクリプトコマンドの実行が失敗するまでにシステムが待機する秒数を指定します。

6. [Targets] (ターゲット) セクションで、タグの指定、インスタンスやエッジデバイスの手動選択、リソースグループの指定により、このオペレーションを実行するマネージドノードを選択します。

> **Tip**
>
> 表示されるはずのマネージドノードが表示されない場合は、トラブルシューティングのヒントについて「マネージドノードの可用性のトラブルシューティング」を参照してください。

7. [その他のパラメータ] で、以下の操作を行います。

- [コメント] に、このコマンドに関する情報を入力します。
- [タイムアウト (秒)] に、コマンドの実行全体が失敗するまでにシステムが待機する秒数を指定します。

8. [レート制御] の場合:

- [同時実行数] の場合、コマンドを同時に実行するマネージドノードの数または割合を指定します。

> **Note**
>
> マネージドノードに適用されるタグを指定するか、AWS リソースグループを指定してターゲットを選択し、ターゲットとなるマネージドノードの数が不明な場合は、割合を指定してドキュメントを同時に実行できるターゲットの数を制限します。

- [エラーのしきい値] で、ノードの数または割合のいずれかで失敗した後、他のマネージドノードでのコマンドの実行をいつ停止するか指定します。例えば、3 つのエラーを指定した場合、4 番目のエラーが受信されると、Systems Manager はコマンドの送信を停止します。コマンドを処理しているマネージドノードもエラーを送信する可能性があります。

9. (オプション) コマンド出力をファイルに保存する場合は、[出力オプション] の [S3 バケットにコマンド出力を書き込む] ボックスを選択します。ボックスにバケット名とプレフィックス (フォルダ) 名を入力します。

> **Note**
>
> S3 バケットにデータを書き込む機能を許可する S3 許可は、このタスクを実行する IAM ユーザーのものではなく、インスタンスに割り当てられたインスタンスプロファイル (EC2 インスタンスの場合) または IAM サービスロール (ハイブリッドアクティベーションマシン) のものです。詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」または「ハイブリッド環境に IAM サービスロールを作成する」を参照してください。さらに、指定された S3 バケットが別の AWS アカウント にある場合は、マネージドノードに関連付けられたインスタンスプロファイルまたは IAM サービスロールが、そのバケットへの書き込みに必要なアクセス許可があることを確認してください。

10. [SNS Notifications (SNS 通知)] セクションで、コマンドの実行状態に関する通知を受け取る場合は、[Enable SNS notifications (SNS 通知を有効にする)] チェックボックスをオンにします。

    Run Command 用の Amazon SNS 通知の設定の詳細については、「Amazon SNS 通知を使用した Systems Manager のステータス変更のモニタリング」を参照してください。

11. [Run (実行)] を選択します。

AWS CLI を使用して、GitHub から Python スクリプトを実行する

1. まだ AWS Command Line Interface (AWS CLI) をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」を参照してください。

2. GitHub からスクリプトをダウンロードして実行するには、次のコマンドを実行します。

```
aws ssm send-command --document-name "AWS-RunRemoteScript" --instance-
ids "instance-IDs" --parameters '{"sourceType":["GitHub"],"sourceInfo":
["{\"owner\":\"owner_name\", \"repository\":\"repository_name\", \"path\":
 \"path_to_script_or_directory\"}"],"commandLine":["commands_to_run"]}'
```

   以下はその例です。

```
aws ssm send-command --document-name "AWS-RunRemoteScript" --instance-ids
 "i-02573cafcfEXAMPLE" --parameters '{"sourceType":["GitHub"],"sourceInfo":
["{\"owner\":\"TestUser1\", \"repository\":\"GitHubTestPublic\", \"path\":
 \"scripts/python/complex-script\"}"],"commandLine":["mainFile.py argument-1
 argument-2 "]}'
```

   この例では、complex-script というスクリプトのディレクトリをダウンロードします。commandLine エントリが mainFile.py を実行し、complex-script ディレクトリ内の他のスクリプトを実行できます。

Systems Manager Compliance で Chef InSpec プロファイルを使用する

AWS Systems Manager は Chef InSpec に統合されています。Chef InSpec はオープンソースのテストフレームワークで、人が読み取り可能なプロファイルを作成して GitHub または Amazon Simple Storage Service (Amazon S3) に保存できます。その後、Systems Manager を使用してコンプライアンススキャンを実行し、準拠または非準拠のノードを表示できます。プロファイルは、コンピューティング環境のセキュリティ、コンプライアンス、またはポリシー要件です。例えば、AWS Systems Manager のツールである Compliance でノードをスキャンするとき、次のチェックを実行するプロファイルを作成できます

- 特定のポートが開いているか閉じているかをチェックします。
- 特定のアプリケーションが実行中かどうかをチェックします。

- 特定のパッケージがインストールされているかどうかをチェックします。
- 特定のプロパティの Windows レジストリキーをチェックします。

Amazon Elastic Compute Cloud (Amazon EC2) インスタンスと、Systems Manager で管理しているオンプレミスサーバーまたは仮想マシン (VM) 用の InSpec プロファイルを作成できます。次のサンプル Chef InSpec プロファイルでは、ポート 22 が開いているかどうかをチェックします。

```
control 'Scan Port' do
impact 10.0
title 'Server: Configure the service port'
desc 'Always specify which port the SSH server should listen to.
Prevent unexpected settings.'
describe sshd_config do
its('Port') { should eq('22') }
end
end
```

InSpec には、チェックや監査コントロールを迅速に書き込みするのに役立つリソースのコレクションが含まれています。InSpec は InSpec ドメイン固有言語 (DSL) を使用して、これらのコントロールを Ruby で書き込みます。InSpec ユーザーの大規模なコミュニティで作成されたプロファイルを使用することもできます。例えば、GitHub の DevSec chef-os-hardening プロジェクトには、ノードをセキュリティで保護するのに役立つ数多くのプロファイルが含まれています。プロファイルを記述して GitHub または Amazon S3 に保存できます。

仕組み

ここでは、Compliance で InSpec プロファイルを使用するプロセスの仕組みを説明します。

1. 事前定義された InSpec プロファイルを使用するよう指定するか、独自に作成します。GitHub の事前定義されたプロファイルを使用して開始できます。独自の InSpec プロファイルを作成する方法については、Chef InSpec プロファイルに関するページを参照してください。
2. パブリックまたはプライベートの GitHub リポジトリ、または S3 バケットにプロファイルを保存します。
3. Systems Manager ドキュメント (SSM ドキュメント) `AWS-RunInspecChecks` を使用して、InSpec プロファイルで Compliance を実行します。Compliance スキャンは、AWS Systems Manager のツールである Run Command を使用してオンデマンドスキャンを開始することも、AWS Systems Manager のツールである State Manager を使用して定期的な Compliance スキャンをスケジュールすることもできます。

4. Compliance API または Compliance コンソールを使用して、準拠していないノードを識別します。

> **Note**
>
> 以下の情報に注意してください。
>
> - Chef はノードのクライアントを使用してプロファイルを処理します。クライアントをインストールする必要はありません。Systems Manager が SSM ドキュメント `AWS-RunInspecChecks` を実行すると、システムはクライアントがインストールされているかどうかをチェックします。インストールされていない場合、Systems Manager はスキャン中に Chef クライアントをインストールし、スキャンが完了した後にクライアントをアンインストールします。
> - このトピックで説明するように、SSM ドキュメント `AWS-RunInspecChecks` を実行すると、対象となる各ノードにタイプ `Custom:Inspec` のコンプライアンスエントリが割り当てられます。このコンプライアンスタイプを割り当てるために、ドキュメントは PutComplianceItems API オペレーションを呼び出します。

InSpec コンプライアンススキャンの実行

このセクションでは、Systems Manager コンソールと AWS Command Line Interface (AWS CLI) を使用して InSpec コンプライアンススキャンを実行する方法について説明します。コンソールの手順では、State Manager を設定してスキャンを実行する方法を示します。AWS CLI の手順では、Run Command を設定してスキャンを実行する方法を示します。

State Manager (コンソール) を使用して InSpec コンプライアンススキャンを実行する

AWS Systems Manager コンソールを使用して State Manager で InSpec コンプライアンススキャンを実行するには

1. AWS Systems Manager コンソール (https://console.aws.amazon.com/systems-manager/) を開きます。
2. ナビゲーションペインで、[State Manager] を選択します。
3. [関連付けの作成] を選択します。
4. [関連付けの詳細の指定] セクションで、名前を入力します。
5. [ドキュメント] リストで、[**AWS-RunInspecChecks**] を選択します。

6. [ドキュメントのバージョン] リストで、[ランタイムの最新] を選択します。
7. [パラメータ] セクション内の [ソースタイプ] リストで、[GitHub] または [S3] を選択します。

   [GitHub] を選択した場合は、[ソース情報] フィールドのパブリックまたはプライベート GitHub リポジトリに InSpec プロファイルへのパスを入力します。Systems Manager チームによって提供された以下の場所からのパブリックプロファイルの例です https://github.com/awslabs/amazon-ssm/tree/master/Compliance/InSpec/PortCheck。

   ```
   {"owner":"awslabs","repository":"amazon-ssm","path":"Compliance/InSpec/
   PortCheck","getOptions":"branch:master"}
   ```

   [S3] を選択した場合は、[ソース情報] フィールドの S3 バケットの InSpec プロファイルに有効な URL を入力します。

   Systems Manager が GitHub および Amazon S3 と統合する方法の詳細については、「GitHub からのスクリプトの実行」を参照してください。
8. [ターゲット] セクションで、タグの指定、インスタンスやエッジデバイスの手動選択、リソースグループの指定により、このオペレーションを実行するマネージドノードを選択します。

   > **Tip**
   >
   > 表示されるはずのマネージドノードが表示されない場合は、トラブルシューティングのヒントについて「マネージドノードの可用性のトラブルシューティング」を参照してください。
9. [スケジュールを指定] セクションで、スケジュールビルダーオプションを使用してコンプライアンススキャンを実行するタイミングを指定するスケジュールを作成します。
10. [レート制御] の場合:

    - [同時実行数] の場合、コマンドを同時に実行するマネージドノードの数または割合を指定します。

      > **Note**
      >
      > マネージドノードに適用されるタグを指定するか、AWS リソースグループを指定してターゲットを選択し、ターゲットとなるマネージドノードの数が不明な場合は、割合を指定してドキュメントを同時に実行できるターゲットの数を制限します。

- [エラーのしきい値] で、ノードの数または割合のいずれかで失敗した後、他のマネージドノードでのコマンドの実行をいつ停止するか指定します。例えば、3 つのエラーを指定した場合、4 番目のエラーが受信されると、システムマネージャー はコマンドの送信を停止します。コマンドを処理しているマネージドノードもエラーを送信する可能性があります。

11. (オプション) コマンド出力をファイルに保存する場合は、[出力オプション] の [S3 バケットにコマンド出力を書き込む] ボックスを選択します。ボックスにバケット名とプレフィックス (フォルダ) 名を入力します。

> **Note**
>
> S3 バケットにデータを書き込む機能を許可する S3 許可は、このタスクを実行する IAM ユーザーのものではなく、インスタンスに割り当てられたインスタンスプロファイル (EC2 インスタンスの場合) または IAM サービスロール (ハイブリッドアクティベーションマシン) のものです。詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」または「ハイブリッド環境に IAM サービスロールを作成する」を参照してください。さらに、指定された S3 バケットが別の AWS アカウント にある場合は、マネージドノードに関連付けられたインスタンスプロファイルまたは IAM サービスロールが、そのバケットへの書き込みに必要なアクセス許可があることを確認してください。

12. [関連付けの作成] を選択します。システムにより関連付けが作成され、コンプライアンススキャンが自動的に実行されます。
13. スキャンが完了するまで数分待ってから、ナビゲーションペインの [コンプライアンス] を選択します。
14. [対応するマネージドインスタンス] で、[コンプライアンスタイプ] の列が [Custom:Inspec] であるノードを見つけます。
15. 非準拠ステータスの詳細を表示するには、ノード ID を選択します。

Run Command (AWS CLI) を使用した InSpec コンプライアンススキャンの実行

1. まだ AWS Command Line Interface (AWS CLI) をインストールして設定していない場合は、インストールして設定します。

   詳細については、「AWS CLI の最新バージョンをインストールまたは更新します。」を参照してください。

2. 以下のいずれかのコマンドを実行して GitHub または Amazon S3 から InSpec プロファイルを実行します。

   コマンドでは、以下のパラメータを使用します。

   - sourceType: GitHub またはAmazon S3
   - sourceInfo: GitHub または S3 バケットのいずれかの InSpec プロファイルフォルダへの URL。フォルダには、基本 InSpec ファイル (*.yml) およびすべての関連するコントロール (*.rb) が含まれている必要があります。

   GitHub

```
aws ssm send-command --document-name "AWS-RunInspecChecks" --targets
 '[{"Key":"tag:tag_name","Values":["tag_value"]}]' --parameters '{"sourceType":
["GitHub"],"sourceInfo":["{\"owner\":\"owner_name\", \"repository\":
\"repository_name\", \"path\": \"Inspec.yml_file"}"]}'
```

   以下はその例です。

```
aws ssm send-command --document-name "AWS-RunInspecChecks" --targets
 '[{"Key":"tag:testEnvironment","Values":["webServers"]}]' --parameters
 '{"sourceType":["GitHub"],"getOptions":"branch:master","sourceInfo":["{\"owner\":
\"awslabs\", \"repository\":\"amazon-ssm\", \"path\": \"Compliance/InSpec/PortCheck
\"}"]}'
```

   Amazon S3

```
aws ssm send-command --document-name "AWS-RunInspecChecks" --targets
 '[{"Key":"tag:tag_name","Values":["tag_value"]}]' --parameters'{"sourceType":
["S3"],"sourceInfo":["{\"path\":\"https://s3.aws-api-domain/amzn-s3-demo-
bucket/Inspec.yml_file\"}"]}'
```

   以下はその例です。

```
aws ssm send-command --document-name "AWS-RunInspecChecks" --targets
 '[{"Key":"tag:testEnvironment","Values":["webServers"]}]' --
parameters'{"sourceType":["S3"],"sourceInfo":["{\"path\":\"https://s3.aws-api-
domain/amzn-s3-demo-bucket/InSpec/PortCheck.yml\"}"]}'
```

3. コンプライアンススキャンの概要を表示するには、次のコマンドを実行します。

```
aws ssm list-resource-compliance-summaries --filters
 Key=ComplianceType,Values=Custom:Inspec
```

4. 次のコマンドを実行して、準拠していないノードの詳細を表示します。

```
aws ssm list-compliance-items --resource-ids node_ID --resource-type
 ManagedInstance --filters Key=DocumentName,Values=AWS-RunInspecChecks
```

ServiceNow との統合

ServiceNow は、IT サービス、チケットシステム、サポートなど、組織レベルのワークフローを作成および管理するためのクラウドベースのサービス管理システムを提供します。AWS Service Management Connector は、ServiceNow を Systems Manager と統合して、ServiceNow から AWS リソースをプロビジョニング、管理、運用します。AWS Service Management Connector を使用すると、Automation、Change Manager、Incident Manager、および OpsCenter (すべて AWS Systems Manager のツール) と ServiceNow を統合できます。

ServiceNow を使用して、以下のタスクを実行できます。

- Systems Manager からオートメーションプレイブックを実行します。
- Systems Manager OpsItems からインシデントを表示、更新、および解決します。
- Systems Manager OpsCenter を使用して、インシデントなどの運用アイテムを表示および管理します。
- 事前承認された変更テンプレートのキュレートされたリストから Systems Manager 変更リクエストを表示して実行します。
- Incident Manager と統合することで、AWS ホストアプリケーションに関連するインシデントの管理と解決を行います。

> **Note**
>
> ServiceNow との統合方法については、「AWS サービスマネジメントコネクタ管理者ガイド」の「AWS サービスの統合の設定」を参照してください。

AWS Systems Manager リファレンス

以下の情報とトピックは、AWS Systems Manager ソリューションをより効果的に実装するのに役立ちます。

プリンシパル

AWS Identity and Access Management (IAM) では、プリンシパルポリシー要素を使用して、リソースへのサービスアクセスを許可または拒否することができます。Systems Manager のプリンシパルポリシー要素の値は `ssm.amazonaws.com` です。

サポート対象の AWS リージョン とエンドポイント

「Amazon Web Services 全般のリファレンス」の「Systems Manager サービスのエンドポイント」を参照してください。

Service Quotas

「Amazon Web Services 全般のリファレンス」の「Systems Manager Service Quotas」を参照してください。

API リファレンス

「 AWS Systems Manager API リファレンス」を参照してください。

AWS CLI コマンドリファレンス

「AWS CLI コマンドリファレンスの AWS Systems Manager セクション」を参照してください。

AWS Tools for PowerShell コマンドレットリファレンス

「AWS Tools for PowerShellコマンドレットリファレンスの AWS Systems Manager セクション」を参照してください。

GitHub の SSM Agent リポジトリ

aws/amazon-ssm-agent を参照してください。

質問をどうぞ

AWS re:Post における Systems Manager の問題

AWS ニュースブログ

管理ツール

その他のリファレンストピック

- このサービスを AWS SDK で使用する
- 参照: パッチ適用オペレーション用の Amazon S3 バケット
- リファレンス: Systems Manager 用の Amazon EventBridge イベントパターンとタイプ
- リファレンス: Systems Manager の Cron 式および rate 式
- リファレンス: ec2messages、ssmmessages およびその他の API オペレーション
- リファレンス: Systems Manager の日付および時刻の文字列のフォーマットを作成する

このサービスを AWS SDK で使用する

AWS ソフトウェア開発キット (SDK) は、多くの一般的なプログラミング言語で使用できます。各 SDK には、デベロッパーが好みの言語でアプリケーションを簡単に構築できるようにする API、コード例、およびドキュメントが提供されています。

SDK ドキュメント	コードの例
AWS SDK for C++	AWS SDK for C++ コードの例
AWS CLI	AWS CLI コードの例
AWS SDK for Go	AWS SDK for Go コードの例
AWS SDK for Java	AWS SDK for Java コードの例
AWS SDK for JavaScript	AWS SDK for JavaScript コードの例
AWS SDK for Kotlin	AWS SDK for Kotlin コードの例
AWS SDK for .NET	AWS SDK for .NET コードの例
AWS SDK for PHP	AWS SDK for PHP コードの例
AWS Tools for PowerShell	Tools for PowerShell のコード例
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) コードの例
AWS SDK for Ruby	AWS SDK for Ruby コードの例

SDK ドキュメント	コードの例
AWS SDK for Rust	AWS SDK for Rust コードの例
AWS SDK for SAP ABAP	AWS SDK for SAP ABAP コードの例
AWS SDK for Swift	AWS SDK for Swift コードの例

> **可用性の例**
>
> 必要なものが見つからなかった場合。このページの下側にある [Provide feedback (フィードバックを送信)] リンクから、コードの例をリクエストしてください。

参照: パッチ適用オペレーション用の Amazon S3 バケット

さまざまな Patch Manager パッチ適用オペレーションを実行する過程において、AWS Systems Manager Agent (SSM Agent) は、Amazon Web Services (AWS) が所有して維持する特定の Amazon Simple Storage Service (Amazon S3) バケットにアクセスします。これらの S3 バケットはパブリックにアクセス可能です。デフォルトで、SSM Agent は HTTP 呼び出しを使用してこれに接続します。

ただし、Systems Manager のオペレーションで仮想プライベートクラウド (VPC) エンドポイントを使用している場合は、Systems Manager の Amazon Elastic Compute Cloud (Amazon EC2) インスタンスプロファイル、またはハイブリッドおよびマルチクラウド環境の非 EC2 マシンのサービスロールで、明示的なアクセス許可を付与する必要があります。それ以外の場合、リソースからこれらのパブリックバケットにアクセスすることはできません。

この参照トピックでは、サポートされている各 AWS リージョンのためのパッチ適用関連のバケットをリストアップします。

EC2 インスタンスプロファイルでのこれらの S3 バケットの指定については、「SSM Agent と AWS マネージド S3 バケットとの通信」を参照してください。

Systems Manager での VPC エンドポイントの使用については、「Systems Manager のために VPC エンドポイントを使用して EC2 インスタンスのセキュリティを強化する」を参照してください。

トピック

- パッチ適用オペレーション用の SSM Command ドキュメントが含まれるバケット (Linux および Windows Server)
- パッチ適用オペレーション用の SSM Command ドキュメントが含まれるバケット (macOS)
- AWS が管理するパッチベースラインのスナップショットが含まれるバケット

パッチ適用オペレーション用の SSM Command ドキュメントが含まれるバケット (Linux および Windows Server)

`aws-patch-manager-`*`region`*`-`*`unique-suffix` 形式のバケットには、Linux および Windows Server オペレーティングシステムでの Patch Manager パッチ適用オペレーションで使用される以下のドキュメントが含まれています。

- `AWS-RunPatchBaseline`
- `AWS-RunPatchBaselineAssociation`
- `AWS-RunPatchBaselineWithHooks`
- `AWS-InstanceRebootWithHooks`
- `AWS-PatchAsgInstance`
- `AWS-PatchInstanceWithRollback`

リージョン名	リージョンコード	**`aws-patch-manager-`*`region`*`-`*`suffix`** バケット
米国東部 (オハイオ)	us-east-2	aws-patch-manager-us-east-2-552881074
米国東部 (バージニア北部)	us-east-1	aws-patch-manager-us-east-1-1970c647d
米国西部 (北カリフォルニア)	us-west-1	aws-patch-manager-us-west-1-8badb4304
米国西部 (オレゴン)	us-west-2	aws-patch-manager-us-west-2-34d7f99f8

リージョン名	リージョンコード	**aws-patch-manager-*region*-*suffix*** バケット
アフリカ (ケープタウン)	af-south-1	aws-patch-manager-af-south-1-bdd5f65a9
アジアパシフィック (香港)	ap-east-1	aws-patch-manager-ap-east-1-632356271
アジアパシフィック (ハイデラバード)	ap-south-2	aws-patch-manager-ap-south-2-32f4b4128
アジアパシフィック (ジャカルタ)	ap-southeast-3	aws-patch-manager-ap-southeast-3-aa48fc462
アジアパシフィック (メルボルン)	ap-southeast-4	aws-patch-manager-ap-southeast-4-01e2c40d3
アジアパシフィック (ムンバイ)	ap-south-1	aws-patch-manager-ap-south-1-cb7c62ff9
アジアパシフィック (大阪)	ap-northeast-3	aws-patch-manager-ap-northeast-3-67373598a
アジアパシフィック (ソウル)	ap-northeast-2	aws-patch-manager-ap-northeast-2-10467995c
アジアパシフィック (シンガポール)	ap-southeast-1	aws-patch-manager-ap-southeast-1-7fdfd9ef7
アジアパシフィック (シドニー)	ap-southeast-2	aws-patch-manager-ap-southeast-2-17283a275
アジアパシフィック (東京)	ap-northeast-1	aws-patch-manager-ap-northeast-1-4849fa78f
カナダ (中部)	ca-central-1	aws-patch-manager-ca-central-1-3148e69e3

リージョン名	リージョンコード	**aws-patch-manager-*region*-*suffix*** バケット
カナダ西部 (カルガリー)	ca-west-1	aws-patch-manager-ca-west-1-9e3a4b2f9
欧州 (フランクフルト)	eu-central-1	aws-patch-manager-eu-central-1-9163fdaaf
欧州 (アイルランド)	eu-west-1	aws-patch-manager-eu-west-1-5522fb710
欧州 (ロンドン)	eu-west-2	aws-patch-manager-eu-west-2-902a2bc74
欧州 (ミラノ)	eu-south-1	aws-patch-manager-eu-south-1-c52f3f594
欧州 (パリ)	eu-west-3	aws-patch-manager-eu-west-3-29bf85721
欧州 (スペイン)	eu-south-2	aws-patch-manager-eu-south-2-a4cf248b1
欧州 (ストックホルム)	eu-north-1	aws-patch-manager-eu-north-1-795879e9b
欧州 (チューリッヒ)	eu-central-2	aws-patch-manager-eu-central-2-184ce43c8
イスラエル (テルアビブ)	il-central-1	aws-patch-manager-il-central-1-e221cb57b
中東 (バーレーン)	me-south-1	aws-patch-manager-me-south-1-a53fc9dce
中東 (アラブ首長国連邦)	me-central-1	aws-patch-manager-me-central-1-2932f2f80

リージョン名	リージョンコード	**aws-patch-manager-*region*-*suffix*** バケット
南米（サンパウロ）	sa-east-1	aws-patch-manager-sa-east-1-ddf4b6a09

パッチ適用オペレーション用の SSM Command ドキュメントが含まれるバケット (macOS)

aws-patchmanager-macos-*region*-*unique-suffix* 形式のバケットには、macOS オペレーティングシステムでの Patch Manager パッチ適用オペレーションで使用される以下のドキュメントが含まれています。

- AWS-RunPatchBaseline
- AWS-RunPatchBaselineAssociation
- AWS-RunPatchBaselineWithHooks
- AWS-InstanceRebootWithHooks
- AWS-PatchAsgInstance
- AWS-PatchInstanceWithRollback

リージョン名	リージョンコード	**aws-patchmanager-macos-*region*-*suffix*** バケット
米国東部（オハイオ）	us-east-2	aws-patchmanager-macos-us-east-2-552881074
米国東部 (バージニア北部)	us-east-1	aws-patchmanager-macos-us-east-1-1970c647d
米国西部（北カリフォルニア）	us-west-1	aws-patchmanager-macos-us-west-1-8badb4304
米国西部（オレゴン）	us-west-2	aws-patchmanager-macos-us-west-2-34d7f99f8

リージョン名	リージョンコード	**aws-patchmanager-macos-** ***region-suffix*** バケット
アフリカ (ケープタウン)	af-south-1	aws-patchmanager-macos-af-south-1-bdd5f65a9
アジアパシフィック (香港)	ap-east-1	aws-patchmanager-macos-ap-east-1-632356271
アジアパシフィック (ハイデラバード)	ap-south-2	aws-patchmanager-macos-ap-south-2-32f4b4128
アジアパシフィック (ジャカルタ)	ap-southeast-3	aws-patchmanager-macos-ap-southeast-3-aa48fc462
アジアパシフィック (メルボルン)	ap-southeast-4	aws-patchmanager-macos-ap-southeast-4-01e2c40d3
アジアパシフィック (ムンバイ)	ap-south-1	aws-patchmanager-macos-ap-south-1-cb7c62ff9
アジアパシフィック (大阪)	ap-northeast-3	aws-patchmanager-macos-ap-northeast-3-67373598a
アジアパシフィック (ソウル)	ap-northeast-2	aws-patchmanager-macos-ap-northeast-2-10467995c
アジアパシフィック (シンガポール)	ap-southeast-1	aws-patchmanager-macos-ap-southeast-1-7fdfd9ef7
アジアパシフィック (シドニー)	ap-southeast-2	aws-patchmanager-macos-ap-southeast-2-17283a275
アジアパシフィック (東京)	ap-northeast-1	aws-patchmanager-macos-ap-northeast-1-4849fa78f
カナダ (中部)	ca-central-1	aws-patchmanager-macos-ca-central-1-3148e69e3

リージョン名	リージョンコード	**aws-patchmanager-macos-** ***region-suffix*** バケット
カナダ西部 (カルガリー)	ca-west-1	aws-patchmanager-macos-ca-west-1-9e3a4b2f9
欧州 (フランクフルト)	eu-central-1	aws-patchmanager-macos-eu-central-1-9163fdaaf
欧州 (アイルランド)	eu-west-1	aws-patchmanager-macos-eu-west-1-5522fb710
欧州 (ロンドン)	eu-west-2	aws-patchmanager-macos-eu-west-2-902a2bc74
欧州 (ミラノ)	eu-south-1	aws-patchmanager-macos-eu-south-1-c52f3f594
欧州 (パリ)	eu-west-3	aws-patchmanager-macos-eu-west-3-29bf85721
欧州 (スペイン)	eu-south-2	aws-patchmanager-macos-eu-south-2-a4cf248b1
欧州 (ストックホルム)	eu-north-1	aws-patchmanager-macos-eu-north-1-795879e9b
欧州 (チューリッヒ)	eu-central-2	aws-patchmanager-macos-eu-central-2-184ce43c8
イスラエル (テルアビブ)	il-central-1	aws-patchmanager-macos-il-central-1-e221cb57b
中東 (バーレーン)	me-south-1	aws-patchmanager-macos-me-south-1-a53fc9dce
中東 (アラブ首長国連邦)	me-central-1	aws-patchmanager-macos-me-central-1-2932f2f80

リージョン名	リージョンコード	**aws-patchmanager-macos-*region-suffix*** バケット
南米 (サンパウロ)	sa-east-1	aws-patchmanager-macos-sa-east-1-ddf4b6a09

AWS が管理するパッチベースラインのスナップショットが含まれるバケット

patch-baseline-snapshot-*region* または patch-baseline-snapshot-*region*-*unique-suffix* 形式のバケットには、AWS が管理するパッチベースラインのスナップショットが含まれています。以下の SSM ドキュメントのいずれかを使用する場合は、この S3 バケットへのアクセス権が必要です。

- AWS-RunPatchBaseline
- AWS-RunPatchBaselineAssociation
- AWS-RunPatchBaselineWithHooks
- AWS-ApplyPatchBaseline (レガシー SSM ドキュメント)

リージョン名	リージョンコード	**patch-baseline-snapshot-*** バケット
米国東部 (オハイオ)	us-east-2	patch-baseline-snapshot-us-east-2
米国東部 (バージニア北部)	us-east-1	patch-baseline-snapshot-us-east-1
米国西部 (北カリフォルニア)	us-west-1	patch-baseline-snapshot-us-west-1
米国西部 (オレゴン)	us-west-2	patch-baseline-snapshot-us-west-2

リージョン名	リージョンコード	**patch-baseline-snapshot-*** バケット
アフリカ (ケープタウン)	af-south-1	patch-baseline-snapshot-af-south-1-tbxdb5b9
アジアパシフィック (香港)	ap-east-1	patch-baseline-snapshot-ap-east-1
アジアパシフィック (ハイデラバード)	ap-south-2	patch-baseline-snapshot-ap-south-2-50209442
アジアパシフィック (ジャカルタ)	ap-southeast-3	patch-baseline-snapshot-ap-southeast-3-be0a3174
アジアパシフィック (メルボルン)	ap-southeast-4	patch-baseline-snapshot-ap-southeast-4-dc6f76ce
アジアパシフィック (ムンバイ)	ap-south-1	patch-baseline-snapshot-ap-south-1
アジアパシフィック (大阪)	ap-northeast-3	patch-baseline-snapshot-ap-northeast-3
アジアパシフィック (ソウル)	ap-northeast-2	patch-baseline-snapshot-ap-northeast-2
アジアパシフィック (シンガポール)	ap-southeast-1	patch-baseline-snapshot-ap-southeast-1
アジアパシフィック (シドニー)	ap-southeast-2	patch-baseline-snapshot-ap-southeast-2
アジアパシフィック (東京)	ap-northeast-1	patch-baseline-snapshot-ap-northeast-1
カナダ (中部)	ca-central-1	patch-baseline-snapshot-ca-central-1

リージョン名	リージョンコード	**patch-baseline-snapshot-*** バケット
カナダ西部 (カルガリー)	ca-west-1	patch-baseline-snapshot-ca-west-1
欧州 (フランクフルト)	eu-central-1	patch-baseline-snapshot-eu-central-1
欧州 (アイルランド)	eu-west-1	patch-baseline-snapshot-eu-west-1
欧州 (ロンドン)	eu-west-2	patch-baseline-snapshot-eu-west-2
欧州 (ミラノ)	eu-south-1	patch-baseline-snapshot-eu-south-1
欧州 (パリ)	eu-west-3	patch-baseline-snapshot-eu-west-3
欧州 (スペイン)	eu-south-2	patch-baseline-snapshot-eu-south-2-df2c9d70
欧州 (ストックホルム)	eu-north-1	patch-baseline-snapshot-eu-north-1
欧州 (チューリッヒ)	eu-central-2	patch-baseline-snapshot-eu-central-2
イスラエル (テルアビブ)	il-central-1	patch-baseline-snapshot-il-central-1
中東 (バーレーン)	me-south-1	patch-baseline-snapshot-me-south-1-uduvl7q8
中東 (アラブ首長国連邦)	me-central-1	patch-baseline-snapshot-me-central-1

リージョン名	リージョンコード	**patch-baseline-snapshot-*** バケット
南米 (サンパウロ)	sa-east-1	patch-baseline-snapshot-sa-east-1

リファレンス: Systems Manager 用の Amazon EventBridge イベントパターンとタイプ

> **Note**
>
> イベントを管理するには、Amazon EventBridge が好ましい方法です。CloudWatch Events と EventBridge は同じ基盤となるサービスと API ですが、EventBridge はより多くの機能を提供します。CloudWatch または EventBridge のいずれかで行った変更は、各コンソールに反映されます。詳細については、「Amazon EventBridge ユーザーガイド」を参照してください。

Amazon EventBridge を使用すると、受信イベントを照合し、処理のためにターゲットにルーティングするルールを作成できます。

イベントは、独自のアプリケーション、SaaS (Software-as-a-Service) アプリケーション、または AWS のサービスの環境の変更を示します。イベントは、ベストエフォートベースで生成されます。ルールで指定されているイベントタイプが検出されると、EventBridge は指定したターゲットにルーティングして処理します。ターゲットには、Amazon Elastic Compute Cloud (Amazon EC2) インスタンス、AWS Lambda 関数、Amazon Kinesis Streams、Amazon Elastic Container Service (Amazon ECS) タスク、AWS Step Functions ステートマシン、Amazon Simple Notification Service (Amazon SNS) トピック、Amazon Simple Queue Service (Amazon SQS) キュー、組み込みターゲットなどが含まれます。

EventBridge ルール作成の詳細については、以下の各トピックを参照してください。

- Amazon EventBridge を使用して Systems Manager イベントをモニタリングする
- Systems Manager 用の Amazon EventBridge イベントの例
- Amazon EventBridge ユーザーガイドの「Amazon EventBridge の開始方法」

このトピックの残りの部分では、EventBridge ルールに含めることができる Systems Manager のイベントタイプについて説明します。

イベントタイプ: オートメーション

イベントタイプ名	ルールに追加できるイベントの説明
EC2 オートメーション実行ステータス変更の通知	オートメーションワークフローの全体的なステータスが変化します。イベントルールには、次のステータスの変更を 1 つ以上追加できます。 • APPROVED • Canceled • 失敗 • PendingApproval • PendingChangeCalendarOverride • 拒否 • 予定 • 成功 • TimedOut
EC2 オートメーションステップステータス変更の通知	オートメーションワークフローの特定のステップのステータスが変化します。イベントルールには、次のステータスの変更を 1 つ以上追加できます。 • Canceled • 失敗 • 成功 • TimedOut

イベントタイプ: Change Calendar

イベントタイプ名	ルールに追加できるイベントの説明
カレンダーステートの変更	Change Calendar の状態を変更します。イベントルールには、次の状態の変更を 1 つ、または両方追加できます。 • オープン • クローズ 他の AWS アカウント から共有されているカレンダーの状態の変更はサポートされていません。

イベントタイプ: Change Manager

イベントタイプ名	ルールに追加できるイベントの説明
変更要求ステータスの更新	Change Manager の変更要求の状態。イベントルールでは以下の状態を使用できます。 • APPROVED • 拒否 • InProgress

イベントタイプ: 設定コンプライアンス

イベントタイプ名	ルールに追加できるイベントの説明
設定コンプライアンスのステータスの変更	関連付けのコンプライアンスまたはパッチコンプライアンスのいずれかで、マネージドノードの状態が変更されます。イベントルールには、次の状態の変更を 1 つ以上追加できます。

イベントタイプ名	ルールに追加できるイベントの説明
	• compliant • non_compliant

イベントタイプ: インベントリ

イベントタイプ名	ルールに追加できるイベントの説明
インベントリリソースの状態の変更	カスタムインベントリの削除と、古いスキーマバージョンを使用する PutInventory 呼び出し。イベントルールには、次の状態の変更を 1 つ以上追加できます。 • カスタムインベントリタイプは、特定のノードでイベントを削除しました。EventBridge は、カスタム イベントリタイプごとに、ノードあたり 1 つのイベントを送信します。 • カスタムインベントリタイプは、すべてのノードでイベントを削除します。 • 古いスキーマバージョンイベントを持つ PutInventory 呼び出し。EventBridge は、スキーマのバージョンが現在のスキーマよりも小さい場合にこのイベントを送信します。このイベントは、すべてのインベントリタイプに適用されます。 詳細については、「EventBridge を使用して Inventory イベントをモニタリングする」を参照してください。

イベントタイプ: メンテナンスウィンドウ

イベントタイプ名	ルールに追加できるイベントの説明
メンテナンスウィンドウのステータス変更通知	1 つまたは複数のメンテナンスウィンドウの全体的なステータスが変化します。イベントルールには、次の状態の変更を 1 つ以上追加できます。 • DISABLED • ENABLED
メンテナンスウィンドウのターゲット登録通知	1 つまたは複数のメンテナンスウィンドウターゲットのステータスが変化します。イベントルールには、次の状態の変更を 1 つ以上追加できます。 • DEREGISTERED • REGISTERED • UPDATED
メンテナンスウィンドウの実行状態変更通知	メンテナンスウィンドウの全体的なステータスが、実行中に変化します。イベントルールには、次の状態の変更を 1 つ以上追加できます。 • CANCELLED • CANCELLING • FAILED • IN_PROGRESS • 保留中 • SKIPPED_OVERLAPPING • SUCCESS • TIMED_OUT

イベントタイプ名	ルールに追加できるイベントの説明
メンテナンスウィンドウタスクの実行状態変更通知	メンテナンスウィンドウ内のタスクの状態が、実行中に変化します。イベントルールには、次の状態の変更を 1 つ以上追加できます。 • CANCELLED • CANCELLING • FAILED • IN_PROGRESS • SUCCESS • TIMED_OUT
メンテナンスウィンドウタスクターゲットの呼び出しの状態変更通知。	特定のターゲットのメンテナンスウィンドウタスクの状態が変化します。 この通知は、Run Command タスクに対してのみ完全にサポートされています。このタイプのタスクでは、次の状態の変更を 1 つ以上、イベントルールに追加できます。 • CANCELLED • CANCELLING • FAILED • IN_PROGRESS • SUCCESS • TIMED_OUT オートメーション、AWS Lambda、および AWS Step Functions タスクでは、EventBridge はステート `IN_PROGRESS` および `COMPLETE` のみをレポートします。`COMPLETE` は、タスクが成功したかどうかを報告します。

イベントタイプ名	ルールに追加できるイベントの説明
メンテナンスウィンドウのタスク登録通知	1 つまたは複数のメンテナンスウィンドウタスクの状態が変化します。イベントルールには、次の状態の変更を 1 つ以上追加できます。 • DEREGISTERED • REGISTERED • UPDATED

イベントタイプ: OpsCenter

イベントタイプ名	ルールに追加できるイベントの説明
OpsItem 作成	OpsItem が作成されるときに発生します。以下のいずれかの OpsItem タイプにルールを追加することができます。 • /aws/問題 • /aws/タスク • /aws/インサイト • /aws/アクションアイテム
OpsItem 更新	OpsItem が更新されるときに発生します。以下のいずれかの OpsItem タイプにルールを追加することができます。 • /aws/問題 • /aws/タスク • /aws/インサイト • /aws/アクションアイテム

イベントタイプ: Parameter Store

イベントタイプ名	ルールに追加できるイベントの説明
パラメータストアの変更	パラメータの状態が変化します。イベントルールには、次の状態の変更を 1 つ以上追加できます。 • 作成 • 更新 • 削除 • LabelParameterVersion 詳細については、「パラメータおよびパラメータポリシー用の EventBridge ルールを設定する」を参照してください。
パラメータストアポリシーのアクション	詳細パラメータポリシーの変更の条件が満たされます。イベントルールには、次のステータスの変更を 1 つ以上追加できます。 • 有効期限 • ExpirationNotification • NoChangeNotification 詳細については、「パラメータおよびパラメータポリシー用の EventBridge ルールを設定する」を参照してください。

イベントタイプ: Run Command

イベントタイプ名	ルールに追加できるイベントの説明
EC2 コマンド呼び出しステータス変更の通知	個々のマネージドインスタンスに送信されるコマンドのステータスが変化します。イベント

イベントタイプ名	ルールに追加できるイベントの説明
	ルールには、次のステータスの変更を 1 つ以上追加できます。 • 成功 • InProgress • TimedOut • Canceled • 失敗
EC2 コマンドステータス変更の通知	コマンドの全体的なステータスが変化します。イベントルールには、次のステータスの変更を 1 つ以上追加できます。 • 成功 • InProgress • TimedOut • Canceled • [失敗]

イベントタイプ: State Manager

イベントタイプ名	ルールに追加できるイベントの説明
EC2 State Manager 関連付け状態の変更	関連付けの全体的な状態は、適用に応じて変化します。イベントルールには、次の状態の変更を 1 つ以上追加できます。 • 失敗 • Pending • 成功
EC2 State Manager インスタンスの関連付け状態の変更	関連付けの対象となる 1 つのマネージドインスタンスの状態が変更されます。イベントルール

イベントタイプ名	ルールに追加できるイベントの説明
	には、次の状態の変更を 1 つ以上追加できます。 • 失敗 • Pending • 成功

リファレンス: Systems Manager の Cron 式および rate 式

AWS Systems Manager で State Manager の関連付けまたはメンテナンスウィンドウを作成するときは、ウィンドウまたは関連付けを実行するスケジュールを指定します。スケジュールは、時間ベースのエントリ (cron 式) または頻度ベースのエントリ (rate 式) を使用して指定できます。

cron 式または rate 式に関する一般情報

次の情報は、メンテナンスウィンドウとアソシエーションの両方の cron および rate 式に適用されます。

単一実行のスケジュール

メンテナンスウィンドウの関連付けを作成するときは、指定された時刻に 1 回実行されるように、協定世界時 (UTC) 形式でタイムスタンプを指定できます。例: `"at(2020-07-07T15:55:00)"`

スケジュールオフセット

関連付けおよびメンテナンスウィンドウでサポートされるのは、cron 式のスケジュールオフセットだけです。スケジュールオフセットは、cron 式で指定された日時から関連付けまたはメンテナンスウィンドウを実行するまでに待機する日数です。

Maintenance window example

たとえば、以下の cron 式では、毎月第 3 火曜日の午後 11:30 にメンテナンスウィンドウがスケジュールされます。スケジュールオフセットが 2 の場合、メンテナンスウィンドウは 2 日後の 11:30 PM まで実行されません。

```
aws ssm create-maintenance-window \
```

```
    --name "My-Cron-Offset-Maintenance-Window" \
    --allow-unassociated-targets \
    --schedule "cron(30 23 ? * TUE#3 *)" \
    --duration 4 \
    --cutoff 1 \
    --schedule-offset 2
```

Association example

次のコマンドの cron 式は、毎月第 2 木曜日にアソシエーションを実行するようにスケジュールしています。ただし、スケジュールのオフセットは 3 なので、アソシエーションは 3 日後の次の日曜日まで実行されません。

```
aws ssm create-association \
    --name "AWS-UpdateSSMAgent" \
    --targets "Key=instanceids,Values=i-0cb2b964d3e14fd9f" \
    --schedule-expression "cron(0 0 ? * THU#2 *)"  \
    --schedule-offset 3
    --apply-only-at-cron-interval
```

> **Note**
>
> アソシエーションでオフセットを使用するには、`--apply-only-at-cron-interval` オプションを指定する必要があります。このオプションにより、関連付けを作成した後、すぐに実行されないように に指示できます。

既に経過した日を対象とした cron 式を使用して現在の期間で関連付けまたはメンテナンスウィンドウを作成し、将来のスケジュールオフセット日を追加した場合、その期間に関連付けまたはメンテナンスウィンドウは実行されません。後続の期間に有効となります。例えば、メンテナンスウィンドウの実行日を昨日とした cron 式を指定し、2 日間のスケジュールオフセットを追加しても、メンテナンスウィンドウは明日実行されません。

必須フィールド

メンテナンスウィンドウの cron 式には 6 つの必須フィールドがあります。関連付けの cron 式には 5 つの必須フィールドがあります。 (現在、State Manager では、関連付けの cron 式で月を指定することはできません。) 追加のフィールドである Seconds フィールド (cron 式の最初のフィールド) はオプションです。フィールドは空白で区切ります。

cron 式の例

分	時間	日	月	曜日	年	意味
0	10	*	*	?	*	毎日午前 10:00 (UTC) に実行
15	12	*	*	?	*	毎日午後 12:15 (UTC) に実行
0	18	?	*	MON-FRI	*	毎週月曜日から金曜日まで午後 6:00 (UTC) に実行
0	8	1	*	?	*	毎月 1 日の午前 8:00 (UTC) に実行

サポートされる値

次の表は、サポートされている必須 cron エントリの値の一覧です。

cron 式でサポートされている値

フィールド	値	ワイルドカード
分	0-59	, - * /
時間	0-23	, - * /

フィールド	値	ワイルドカード
日	1-31	, - * ? / L W
月 (メンテナンスウィンドウのみ)	1~12 または JAN~DEC	, - * /
曜日	1~7 または SUN~SAT	, - * ? / L #
年	1970-2199	, - * /

> **Note**
>
> 同じ cron 式で日フィールドと曜日フィールドの両方に値を指定することはできません。一方のフィールドに値を指定する場合、もう一方のフィールドで ? (疑問符) を使用してください。

cron 式のワイルドカード

以下の表に示しているのは、cron 式がサポートするワイルドカード値です。

> **Note**
>
> 5 分より短いレートを導き出す Cron 式はサポートされていません。曜日フィールドと日フィールドの値の両方を指定することはまだ完全にはサポートされていません。これらのフィールドのいずれかで疑問符 (?) 文字を使用してください。

cron 式でサポートされているワイルドカード

ワイルドカード	説明
,	, (カンマ) ワイルドカードには追加の値が含まれます。月フィールドの、「JAN,FEB,MAR」は、1 月、2 月、3 月を含みます。

ワイルドカード	説明
-	- (ダッシュ) ワイルドカードは範囲を指定します。日フィールドの、「1-15」は、指定した月の 1 日から 15 日を含みます。
*	* (アスタリスク) ワイルドカードにはフィールドのすべての値が含まれます。時間フィールドの、* にはすべての時間が含まれています。
/	/ (スラッシュ) ワイルドカードは増分を指定します。Minutes フィールドで、「1/10」と入力して、その時間の最初の分から始めて、10 分毎を指定できます。したがって、「1/10」は、1 分、11 分、21 分、31 分などを指定します。
?	? (疑問符) ワイルドカードは任意の文字を意味します。[日] フィールドに 7 と入力し、7 日が何曜日であってもかまわない場合、[曜日] フィールドに ? を入力できます。
L	Day-of-month (日) フィールドまたは Day-of-week (曜日) フィールドの L ワイルドカードは、月または週の最終日を指定します。
W	Day-of-month フィールドのワイルドカード W は、平日を指定します。Day-of-month フィールドで、「3W」は月の 3 番目の平日に最も近い日を指定します。
#	Day-of-week (曜日) フィールドの # ワイルドカードの後に 1 ~ 5 の数値を入力すると、その月の特定の曜日が指定されます。5#3 は、その月の第 3 木曜日を指定します。

rate 式

rate 式には以下の 2 つの必須フィールドがあります。フィールドはスペースで区切ります。

rate 式の必須フィールド

フィールド	値
値	正数、1 や 15 など

単位	`minute`
	`minutes`
	`hour`
	`hours`
	`day`
	`days`

値が 1 に等しい場合、単位は単数形であることが必要です。同様に、1 より大きい値の場合、単位は複数であることが必要です。例えば、`rate(1 hours)` と `rate(5 hour)` は有効ではありませんが、`rate(1 hour)` と `rate(5 hours)` は有効です。

トピック

- 関連付けのための cron および rate 式
- メンテナンスウィンドウの関連付けに使用する cron 式および rate 式

関連付けのための cron および rate 式

このセクションには、State Manager の関連付けのための cron および rate 式の例が含まれています。これらの式のうちの 1 つを作成する前に、次の点に注意してください。

- 関連付けは、1/2、1、2、4、8、または 12 時間ごと、毎日、毎週、n 日ごと、またはその月の最後の x 曜日などの特定の時間の cron 式をサポートしています。
- 関連付けは、30 分以上 31 日未満の間隔の rate 式をサポートします。

- オプションの Seconds フィールドを指定した場合、その値は 0 (ゼロ) が可能です。例: `cron(0 */30 * * * ? *)`
- AWS Systems Manager のツールである Inventory の、メタデータを収集する関連付けには、rate 式を使用することをお勧めします。
- 現在、State Manager では、関連付けの cron 式での月の指定はサポートされていません。

関連付けは、曜日と番号記号 (#) を含む cron 式をサポートしており、その月の n 番目の日を指定して関連付けを実行します。毎月、第 3 火曜日の 23:30 UTC に cron スケジュールを実行する例を次に示します。

```
cron(30 23 ? * TUE#3 *)
```

毎月第 2 木曜日の深夜 UTC に実行する例を次に示します。

```
cron(0 0 ? * THU#2 *)
```

関連付けは、その月の最後の X 曜日を示す (L) 記号もサポートしています。毎月、最後の火曜日の深夜 UTC に cron スケジュールを実行する例を次に示します。

```
cron(0 0 ? * 3L *)
```

パッチした火曜日の 2 日後に関連付けを実行するなど、関連付けを実行するタイミングをさらに制御するには、オフセットを指定できます。オフセットでは、関連付けの実行がスケジュールされている日の後に待機する日数を定義します。例えば、cron スケジュールを `cron(0 0 ? * THU#2 *)` とした場合、[Schedule offset] (スケジュールのオフセット) フィールドで番号 3 を指定して、その月の第 2 木曜日の後の毎週日曜日に関連付けを実行できます。

オフセットを使用するには、コンソールで [Apply association only at the next specified Cron interval] (次に指定した Cron の間隔でのみ関連付けを適用する) オプションを選択するか、コマンドラインから `--apply-only-at-cron-interval` パラメータの使用を指定する必要があります。このオプションにより、関連付けを作成した後、すぐに実行されないように State Manager に指示できます。

以下の表は、関連付けの cron 式の例を示します。

関連付けの cron の例

例	詳細
cron(0/30 * * * ? *)	30分毎

例	詳細
cron(0 0/1 * * ? *)	1 時間毎
cron(0 0/2 * * ? *)	2 時間毎
cron(0 0/4 * * ? *)	4 時間毎
cron(0 0/8 * * ? *)	8 時間毎
cron(0 0/12 * * ? *)	12時間毎
cron(15 13 ? * * *)	毎日午後 1:15
cron(15 13 ? * MON *)	毎週月曜日の午後 1:15
cron(30 23 ? * TUE#3 *)	毎月第 3 火曜日の午後 11:30

関連付けのためのいくつかの rate の例を示します。

関連付けの rate の例

例	詳細
rate(30 minutes)	30分毎
rate(1 hour)	1 時間毎
rate(5 hours)	5時間毎
rate(15 days)	15日毎

関連付けの AWS CLI の例

AWS CLI を使用して State Manager の関連付けを作成するには、`--schedule-expression` パラメータに cron 式または rate 式を含めます。以下の例では、ローカル Linux マシンで AWS CLI を使用します。

> **Note**
>
> デフォルトでは、新しい関連付けを作成すると、その作成直後にシステムによってその関連付けは実行され、以降は指定したスケジュールに従って実行されます。関連付けが作成直後に実行されないように `--apply-only-at-cron-interval` を指定します。このパラメータは、rate 式ではサポートされていません。

```
aws ssm create-association \
    --association-name "My-Cron-Association" \
    --schedule-expression "cron(0 2 ? * SUN *)" \
    --targets Key=tag:ServerRole,Values=WebServer \
    --name AWS-UpdateSSMAgent
```

```
aws ssm create-association \
    --association-name "My-Rate-Association" \
    --schedule-expression "rate(7 days)" \
    --targets Key=tag:ServerRole,Values=WebServer \
    --name AWS-UpdateSSMAgent
```

```
aws ssm create-association \
    --association-name "My-Rate-Association" \
    --schedule-expression "at(2020-07-07T15:55:00)" \
    --targets Key=tag:ServerRole,Values=WebServer \
    --name AWS-UpdateSSMAgent \
    --apply-only-at-cron-interval
```

メンテナンスウィンドウの関連付けに使用する cron 式および rate 式

このセクションには、メンテナンスウィンドウの関連付けに使用する cron 式および rate 式の例が含まれています。

State Manager 関連付けとは異なり、メンテナンスウィンドウはすべての cron および rate 式をサポートします。秒フィールドでの値もサポートします

例えば、次の 6 フィールドの Cron 式は、毎日午前 9:30 にメンテナンスウィンドウを実行します。

```
cron(30 09 ? * * *)
```

Seconds フィールドに値を追加することで、次の 7 フィールドの Cron 式は、毎日午前 9:30:24 にメンテナンスウィンドウを実行します。

```
cron(24 30 09 ? * * *)
```

次の表は、メンテナンスウィンドウの追加の 6 フィールドの cron 式の例を示します。

メンテナンスウィンドウの cron の例

例	詳細
cron(0 2 ? * THU#3 *)	毎月第 3 木曜日の午前 02:00
cron(15 10 ? * * *)	毎日午前 10:15
cron(15 10 ? * MON-FRI *)	毎週月〜金の午前 10:15
cron(0 2 L * ? *)	毎月最終日の午前 02:00
cron(15 10 ? * 6L *)	毎月の最終金曜日の午前 10:15

次の表にメンテナンスウィンドウの rate 式の例を示します。

メンテナンスウィンドウの rate の例

例	詳細
rate(30 minutes)	30分毎
rate(1 hour)	1 時間毎
rate(5 hours)	5時間毎
rate(25 days)	25日毎

メンテナンスウィンドウの AWS CLI の例

AWS CLI を使用してメンテナンスウィンドウを作成するには、`--schedule` パラメータに cron 式または rate 式またはタイムスタンプを含めます。以下の例では、ローカル Linux マシンで AWS CLI を使用します。

```
aws ssm create-maintenance-window \
    --name "My-Cron-Maintenance-Window" \
    --allow-unassociated-targets \
    --schedule "cron(0 16 ? * TUE *)" \
    --schedule-timezone "America/Los_Angeles" \
    --start-date 2021-01-01T00:00:00-08:00 \
    --end-date 2021-06-30T00:00:00-08:00 \
    --duration 4 \
    --cutoff 1
```

```
aws ssm create-maintenance-window \
    --name "My-Rate-Maintenance-Window" \
    --allow-unassociated-targets \
    --schedule "rate(7 days)" \
    --duration 4 \
    --schedule-timezone "America/Los_Angeles" \
    --cutoff 1
```

```
aws ssm create-maintenance-window \
    --name "My-TimeStamp-Maintenance-Window" \
    --allow-unassociated-targets \
    --schedule "at(2021-07-07T13:15:30)" \
    --duration 4 \
    --schedule-timezone "America/Los_Angeles" \
    --cutoff 1
```

詳細情報

Wikipedia ウェブサイトの「CRON expression」(cron 式)

リファレンス: ec2messages、ssmmessages およびその他の API オペレーション

API オペレーションをモニタリングしていると、以下のオペレーションへの呼び出しが表示されることがあります。

- ec2messages:AcknowledgeMessage
- ec2messages:DeleteMessage
- ec2messages:FailMessage

- ec2messages:GetEndpoint
- ec2messages:GetMessages
- ec2messages:SendReply
- ssmmessages:CreateControlChannel
- ssmmessages:CreateDataChannel
- ssmmessages:OpenControlChannel
- ssmmessages:OpenDataChannel
- ssm:DescribeDocumentParameters
- ssm:DescribeInstanceProperties
- ssm:GetCalendar
- ssm:GetManifest
- ssm:ListInstanceAssociations
- ssm:PutCalendar
- ssm:PutConfigurePackageResult
- ssm:RegisterManagedInstance
- ssm:RequestManagedInstanceRoleToken
- ssm:UpdateInstanceAssociationStatus
- ssm:UpdateInstanceInformation
- ssm:UpdateManagedInstancePublicKey

これらは、このトピックの残りの部分で説明されているとおり、AWS Systems Manager で使用される特別なオペレーションです。

エージェント関連の API オペレーション (**ssmmessages** および **ec2messages** エンドポイント)

ssmmessages API オペレーション

Systems Manager は、次のタイプの API オペレーションに ssmmessages エンドポイントを使用します。

- Systems Manager Agent (SSM Agent) からクラウド内の Systems Manager サービスへのオペレーション。

- クラウドでの、SSM Agent から、AWS Systems Manager のツールである Session Manager へのオペレーション。このエンドポイントは、クラウド内の Session Manager サービスでセッションチャネルを作成および削除するために必要です。さらに、接続が許可されている場合、SSM Agent はこの Amazon Message Gateway Service 経由で Command ドキュメントを受信します。接続が許可されていない場合、SSM Agent は Amazon Message Delivery Service 経由で Command ドキュメントを受信します。詳細については、「Amazon Message Gateway Service のアクション、リソース、および条件キー」を参照してください。
- Run Command からのオペレーション。

ec2messages API オペレーション

ec2messages:* API オペレーションは、Amazon Message Delivery Service エンドポイントにする必要があります。Systems Manager は、Systems Manager Agent (SSM Agent) からクラウド上の Systems Manager サービスへの API オペレーションにこのエンドポイントを使用します。

> **Important**
>
> ec2messages:* API オペレーションは、2024 年より前にローンチされた AWS リージョンでのみサポートされます。2024 年以降にローンチされたリージョンでは、ssmmessages:* API オペレーションのみがサポートされます。

エンドポイント接続の優先順位

SSM Agent のバージョン 3.3.40.0 以降、Systems Manager は、使用可能な場合には ec2messages:* エンドポイント (Amazon Message Delivery Service) の代わりに ssmmessages:* エンドポイント (Amazon Message Gateway Service) を使用するようになりました。

AWS Identity and Access Management (IAM) アクセス許可ポリシーで ssmmessages:* へのアクセスを許可すると、IAM インスタンスプロファイルが両方のエンドポイントを許可するように設定されている場合でも、SSM Agent は ssmmessages:* エンドポイントに接続できます。これには、自分で作成した IAM インスタンスプロファイルと IAM サービスロールのポリシー、および Quick Setup ホスト管理設定とデフォルトのホスト管理設定で作成した IAM インスタンスプロファイルのポリシーが含まれます。

両方のエンドポイントにアクセス許可を付与し、CloudWatch Metrics などを使用して API オペレーションをモニタリングしている場合、ec2messages:* への呼び出しは表示されません。

2024 年より前にローンチされた AWS リージョン の場合: 現時点では、ec2messages:* アクセス許可はポリシーから安全に削除できます。

エンドポイント接続のフェイルオーバー

2024 年より前にローンチされた AWS リージョン のみ: エージェントの起動時に、IAM インスタンスプロファイルから ssmmessages:* のアクセス許可ではなく、ec2messages:* のアクセス許可のみが提供される場合、SSM Agent は ec2messages:* エンドポイントに接続します。SSM Agent の起動時に、ssmmessages:* と ec2messages:* の両方が存在していたが、エージェントの起動後に ssmmessages:* を削除した場合、SSM Agent はすぐに接続を ec2messages:* エンドポイントに切り替えます。2024 年以降にローンチされたリージョンでは、ssmmessages:* エンドポイントのみがサポートされます。

ssmmessages エンドポイントと ec2messages:* エンドポイントの詳細については、「AWS サービス認可リファレンス」を参照してください。

- Amazon Message Gateway Service のアクション、リソース、および条件キー (ssmmessages)
- Amazon Message Delivery Service のアクション、リソース、および条件キー (ec2messages:*)

ssm:* 名前空間インスタンス関連の API オペレーション

DescribeDocumentParameters

Systems Manager はこの API オペレーションを実行して、Amazon EC2 コンソールで指定されるノードをレンダリングします。 DescribeDocumentParameters オペレーションの結果は、[ドキュメント] ノードに表示されます。

DescribeInstanceProperties

Systems Manager はこの API オペレーションを実行して、Amazon EC2 コンソールで指定されるノードをレンダリングします。 DescribeInstanceProperties オペレーションの結果は、[Fleet Manager] ノードに表示されます。

GetCalendar

Systems Manager はこの API オペレーションを実行して、Change Calendar コンソールで Change Calendar タイプのドキュメントをレンダリングします。

GetManifest

SSM Agent はこの API オペレーションを実行して、指定されたバージョンの AWS Systems Manager Distributor パッケージをインストールまたは更新するためのシステム要件を決定しま

す。これはレガシーの API オペレーションであり、2017 年以降に AWS リージョン でリリースされた場合は使用できません。

`ListInstanceAssociations`

SSM Agent はこの API オペレーションを実行して、新しい State Manager の関連付けが利用可能かどうかを確認します。この API オペレーションは、State Manager が機能するために必要です。

`PutCalendar`

Systems Manager はこの API オペレーションを実行して、Change Calendar コンソールで Change Calendar タイプのドキュメントを更新します。

`PutConfigurePackageResult`

SSM Agent はこの API オペレーションを実行して、パブリックディストリビューターパッケージのインストールエラーとレイテンシーのメトリクスをパッケージ所有者のアカウントに公開します。

`RegisterManagedInstance`

SSM Agent は、次のシナリオでこの API オペレーションを実行します。

- アクティベーションコードと ID を使用して Systems Manager にオンプレミスサーバーや仮想マシン (VM) をマネージドインスタンスとして登録します。
- AWS IoT Greengrass Version 2 認証情報を登録します。

このオペレーションは、SSM Agentバージョン 3.1.x 以降を実行している Amazon EC2 インスタンスからも呼び出されます。

`RequestManagedInstanceRoleToken`

SSM Agent はこの API オペレーションを実行して、マネージドノードにアクセスするための一時的な認証情報を取得します。

`UpdateInstanceAssociationStatus`

SSM Agent はこの API オペレーションを実行して関連付けを更新します。この API オペレーションは、AWS Systems Manager のツールである State Manager が機能するために必要です。

`UpdateInstanceInformation`

SSM Agent はクラウドの Systems Manager サービスを 5 分ごとに呼び出して、ハートビート情報を提供します。この呼び出しはエージェントのハートビートを維持するために必要となり、こうしてエージェントが想定どおり機能していることがサービスによって確認されます。

`UpdateManagedInstancePublicKey`

SSM Agent は、マネージドノードでキーペアをローテーションした後、この API オペレーションを実行してパブリックキーを提供します。パブリックキーは、プライベートキーで署名されたリクエストを認証し、Systems Manager から一時的な認証情報を取得するために使用されます。

ssm:* 名前空間の他の API オペレーション

`ExecuteApi`

OpsCenter で OpsItems を管理する Systems Manager の委任管理者は、複数の AWS アカウントにわたる OpsItems に関する関連リソースの詳細を表示できるよう、この API アクションへのアクセスが必要です。具体的には、この API は、AWS Management Console で OpsItem の詳細 (OpsItem の説明、タグ、AWS CloudFormation テンプレート、AWS Config の変更、CloudWatch Logs アラーム、AWS CloudTrail イベント) を表示するアクセス許可を委任管理者に付与します。複数のアカウントにわたる OpsItems の操作に関する詳細については、「(オプション) OpsCenter の手動設定により、複数のアカウント間で OpsItems を一元管理する」を参照してください。OpsItems の関連リソースの詳細については、「関連リソースを OpsItem に追加する」を参照してください。

リファレンス: Systems Manager の日付および時刻の文字列のフォーマットを作成する

AWS Systems Manager API オペレーションは、リクエストによって返される結果の数を制限するフィルターを受け入れます。これらの API オペレーションの中には、特定の日時を表す、フォーマットされた文字列を必要とするフィルターを受け入れるものがあります。例えば、`DescribeSessions` API アクションは、`InvokedAfter` オブジェクトの有効な値の一部として `InvokedBefore` キーと `SessionFilter` キーを受け入れます。もう 1 つの例は、`DescribeAutomationExecutions` API オペレーションです。これは、`StartTimeBefore` オブジェクトの有効な値の一部として `StartTimeAfter` キーと `AutomationExecutionFilter` キーを受け入れます。リクエストをフィルタリングするときにこれらのキーに指定する値は、ISO 8601 標準と一致する必要があります。ISO 8601 については、ISO 8601 を参照してください。

これらのフォーマットされた日付および時刻文字列は、フィルタに限定されません。リクエストパラメータの値を指定するときに、特定の日時を表す ISO 8601 形式の文字列を必要とする API オペレーションもあります。例えば、`AtTime` オペレーションの `GetCalendarState` リクエストパラメー

タです。これらの文字列は作成が困難です。このトピックの例を使用して、Systems Manager API オペレーションで使用する、書式設定された日付および時刻文字列を作成します。

Systems Manager の日付と時刻文字列を書式設定する

ISO 8601 形式の日付および時刻文字列の例を次に示します。

```
2024-05-08T15:16:43Z
```

これは、協定世界時 (UTC) 2024 年 5 月 8 日の 15:16 を表しています。文字列のカレンダー日付部分は、ハイフンで区切られた 4 桁の年、2 桁の月、および 2 桁の日で表されます。これは、次の形式で表すことができます。

```
YYYY-MM-DD
```

文字列の時刻部分は、区切り記号として文字「T」で始まり、コロンで区切られた 2 桁の時間、2 桁の分、2 桁の秒で表されます。これは、次の形式で表すことができます。

```
hh:mm:ss
```

文字列の時刻部分は、UTC 標準を示す文字「Z」で終わります。

Systems Manager のカスタム日付と時刻文字列を作成する

任意のコマンドラインツールを使用して、ローカルマシンからカスタムの日付および時刻文字列を作成できます。ISO 8601 形式の日付および時刻文字列の作成に使用する構文は、ローカルマシンのオペレーティングシステムによって異なります。以下は、Linux のGNU coreutils の `date` または Windows の PowerShell を使用して ISO 8601 形式の日付および時刻文字列を作成する方法の例です。

coreutils

```
date '+%Y-%m-%dT%H:%M:%SZ'
```

PowerShell

```
(Get-Date).ToString("yyyy-MM-ddTH:mm:ssZ")
```

Systems Manager API オペレーションで作業する場合、レポート作成またはトラブルシューティングのために、日付および時刻の履歴文字列を作成する必要がある場合があります。以下は、AWS Tools for PowerShell および AWS Command Line Interface (AWS CLI) の ISO 8601 形式の日付と時刻のカスタム履歴文字列を作成し、使用する方法の例です。

AWS CLI

- SSM ドキュメントの過去 1 週間のコマンド履歴を取得します。

```
lastWeekStamp=$(date '+%Y-%m-%dT%H:%M:%SZ' -d '7 days ago')

docFilter='{"key":"DocumentName","value":"AWS-RunPatchBaseline"}'
timeFilter='{"key":"InvokedAfter","value":'\"$lastWeekStamp\"'}'

commandFilters=[$docFilter,$timeFilter]

aws ssm list-commands \
    --filters $commandFilters
```

- 過去 1 週間のオートメーションの実行履歴を取得します。

```
lastWeekStamp=$(date '+%Y-%m-%dT%H:%M:%SZ' -d '7 days ago')

aws ssm describe-automation-executions \
    --filters Key=StartTimeAfter,Values=$lastWeekStamp
```

- 過去 1 か月間のセッション履歴を取得します。

```
lastWeekStamp=$(date '+%Y-%m-%dT%H:%M:%SZ' -d '30 days ago')

aws ssm describe-sessions \
    --state History \
    --filters key=InvokedAfter,value=$lastWeekStamp
```

AWS Tools for PowerShell

- SSM ドキュメントの過去 1 週間のコマンド履歴を取得します。

```
$lastWeekStamp = (Get-Date).AddDays(-7).ToString("yyyy-MM-ddTH:mm:ssZ")

$docFilter = @{
```

```
    Key="DocumentName"
    Value="AWS-InstallWindowsUpdates"
}
$timeFilter = @{
    Key="InvokedAfter"
    Value=$lastWeekStamp
}

$commandFilters = $docFilter,$timeFilter

Get-SSMCommand `
    -Filters $commandFilters
```

- 過去 1 週間のオートメーションの実行履歴を取得します。

```
$lastWeekStamp = (Get-Date).AddDays(-7).ToString("yyyy-MM-ddTH:mm:ssZ")

Get-SSMAutomationExecutionList `
    -Filters @{Key="StartTimeAfter";Values=$lastWeekStamp}
```

- 過去 1 か月間のセッション履歴を取得します。

```
$lastWeekStamp = (Get-Date).AddDays(-30).ToString("yyyy-MM-ddTH:mm:ssZ")

Get-SSMSession `
    -State History `
    -Filters @{Key="InvokedAfter";Value=$lastWeekStamp}
```

ユースケースとベストプラクティス

このトピックでは、AWS Systems Manager ツールの一般的ユースケースやベストプラクティスを示します。使用可能な場合は、他にも、関連するブログの投稿や技術文書へのリンクが含まれます。

> **Note**
>
> 次の各セクションのタイトルは、技術ドキュメントの該当セクションへの有効なリンクです。

オートメーション

- インフラストラクチャ用のセルフサービス Automation ランブックを作成します。
- AWS Systems Manager のツールである Automation を使用して、パブリック Systems Manager ドキュメント (SSM ドキュメント) を使用して、または独自のワークフローを作成して、AWS Marketplace またはカスタム AMIs から Amazon Machine Images (AMIs) を簡単に作成できます。
- AMIs を構築および維持するには、`AWS-UpdateLinuxAmi` および `AWS-UpdateWindowsAmi` Automation ランブック、または作成したカスタムの Automation ランブックを使用します。

コンプライアンス

- セキュリティのベストプラクティスとして、マネージドノードで使用される AWS Identity and Access Management (IAM) ロールを更新して、ノードが PutComplianceItems API アクションを使用する機能を制限することをお勧めします。この API アクションは、Amazon EC2 インスタンスやマネージドノードなど、指定されたリソースにコンプライアンスタイプやその他のコンプライアンスの詳細を登録します。詳細については、「Compliance のアクセス許可の設定」を参照してください。

インベントリ

- AWS Systems Manager のツールである Inventory と AWS Config を使用して、時間をかけてアプリケーション設定を監査します。

Maintenance Windows

- ノードで破壊的になり得るアクション (オペレーティングシステム (OS) のパッチ適用、ドライバーの更新、ソフトウェアのインストール) を実行するスケジュールを定義します。
- AWS Systems Manager のツールである State Manager と Maintenance Windows の違いについては、「State Manager または Maintenance Windows の選択」を参照してください。

Parameter Store

- AWS Systems Manager のツールである Parameter Store を使用して、グローバル設定を一元的に管理します。
- AWS Systems ManagerParameter Store で AWS KMS を使用する方法
- Parameter Store パラメータから AWS Secrets Manager シークレットを参照します。

Patch Manager

- AWS Systems Manager のツールである Patch Manager を使用してパッチを大規模にロールアウトし、フリートコンプライアンスの可視性をノード全体で強化します。
- Patch Manager を AWS Security Hub と統合して、フリートのノードがコンプライアンス違反になったときにアラートを受け取ったり、セキュリティの観点からフリートのパッチ適用ステータスを監視したりします。Security Hub の使用には料金が発生します。詳細については、「料金」を参照してください。
- パッチコンプライアンス用のマネージドノードのスキャンでは、コンプライアンスデータが意図せず上書きされることを防ぐため、一度に 1 つの方法のみを実行します。

Run Command

- EC2 Run Command を使用して、SSH アクセスなしで大規模なインスタンスを管理します。
- AWS CloudTrail を使用して、AWS Systems Manager のツールである Run Command によって、またはそのために行われたすべての API コールを監査します。
- Run Command を使用してコマンドを送信する場合は、パスワード、設定データ、その他のシークレットなどの機密情報をプレーンテキスト形式で含めないでください。アカウント内のすべての Systems Manager API アクティビティは、AWS CloudTrail ログの S3 バケットにログ記録されます。つまり、その S3 バケットへのアクセス権を持つユーザーは、これらの秘密のプレーンテキス

ト値を表示できます。このため、Systems Manager オペレーションで使用する機密データを暗号化するために、SecureString パラメータを作成して使用することをお勧めします。

詳細については、「IAM ポリシーを使用して Parameter Store パラメータへのアクセスを制限する」を参照してください。

> **Note**
>
> デフォルトでは、CloudTrail によってバケットに配信されるログファイルは、Amazon の Amazon S3 で管理された暗号化キーによるサーバー側の暗号化 (SSE-S3) によって暗号化されます。直接管理可能なセキュリティレイヤーを提供するには、代わりに CloudTrail ログファイルのAWS KMS によって管理されたキー (SSE-KMS) を使用したサーバー側の暗号化 を使用できます。
> 詳細については、「AWS CloudTrail ユーザーガイド」の「AWS KMS マネージドキー (SSE-KMS) による CloudTrail ログファイルの暗号化」を参照してください。

- Run Command のターゲットおよびレート制御機能を使用して、ステージングされたコマンドオペレーションを実行します。
- AWS Identity and Access Management (IAM) ポリシーを使用して、Run Command (およびすべての Systems Manager ツール) にきめ細かいアクセス許可を適用します。

Session Manager

- AWS CloudTrail を使用して、AWS アカウントのセッションアクティビティを口グに記録します。
- Amazon CloudWatch Logs または Amazon S3 を使用して、AWS アカウント にセッションデータを口グ記録します。
- インスタンスへのユーザーセッションアクセスを制御します。
- セッションでコマンドへのアクセスを制限します。
- ssm-user アカウントの管理権限をオフにしたり、オンにしたりします。

State Manager

- 事前設定済みの AWS-UpdateSSMAgent ドキュメントを使用して、少なくとも 1 か月に 1 回、SSM Agent をアップデートします。
- (Windows の場合) PowerShell または DSC モジュールを Amazon Simple Storage Service (Amazon S3) にアップロードして、AWS-InstallPowerShellModule を使用します。

- タグを使用して、ノードのアプリケーショングループを作成します。個々のノード ID を指定するのではなく、`Targets` パラメータを使用してターゲットノードを作成します。
- Systems Manager を使用して、Amazon Inspector によって生成された結果を自動的に修復します。
- 一元化された設定のリポジトリに SSM ドキュメントを保存し、組織全体でドキュメントを共有します。
- State Manager と Maintenance Windows との違いについては、「State Manager または Maintenance Windows の選択」を参照してください。

マネージドノード

- Systems Manager では、オペレーションを実行するために正確な時間の参照が必要です。ノードの日時が正しく設定されていない場合、その日時は API リクエストの署名の日付と一致しないことがあります。これにより、エラーが発生したり、機能が不完全になったりする可能性があります。例えば、時刻設定が正しくないノードは、マネージドノードのリストには含まれません。

  ノードの時刻設定の詳細については、「Amazon EC2 インスタンスの時刻を設定する」を参照してください。
- Linux 管理対象ノードでは、SSM Agent の署名を確認します。

詳細情報

- Systems Manager のセキュリティに関するベストプラクティス

Systems Manager リソースとアーティファクトの削除

ベストプラクティスとして、Systems Manager のリソースとアーティファクトについては、これらのリソースに関するデータを表示したり、アーティファクトを使用したりする必要がなくなれば、削除することをお勧めします。次の表に、Systems Manager の各ツールまたはアーチファクトのほか、Systems Manager によって作成されたリソースまたはアーチファクトの削除に関する詳細へのリンクを示します。

機能またはアーティファクト	詳細
Application Manager	Application Manager ではアプリケーションを削除できませんが、基盤となるタグ、リソー

機能またはアーティファクト	詳細
	スグループ、または AWS CloudFormation スタックを削除すると、サービスからアプリケーションを削除できます。
Automation	Systems Manager オートメーションを使用して AWS リソースを作成した場合は、該当する AWS Management Console を使ってこれらのリソースを手動で削除する必要があります。カスタムランブックを作成した場合は、基になる SSM ドキュメントを削除できます。詳細については、「カスタム SSM ドキュメントの削除」を参照してください。
Change Calendar	Change Calendar および Change Calendar イベントを削除できます。詳細については、Change Calendar の削除およびChange Calendar イベントの削除を参照してください。
Change Manager	変更テンプレートを削除できます。詳細については、「変更テンプレートの削除」を参照してください。
コンプライアンス	Systems Manager のコンプライアンスには、Patch Manager のパッチ適用と State Manager の関連付けに関するコンプライアンスデータが自動的に表示されます。このデータは削除できません。S3 バケットのコンプライアンスデータを一元化するようにリソースデータ同期を設定している場合は、同期を削除できます。詳細については、「Compliance のためのリソースデータ同期の削除」を参照してください。

機能またはアーティファクト	詳細
Distributor	パッケージは Distributor で削除できます。詳細については、「Distributor パッケージを削除する」を参照してください。
Explorer	Explorer が OpsData を収集するソースから切断することができます。詳しくは、「Systems Manager Explorer のデータソースを編集する」を参照してください。 また、Explorer を使用してリソースデータ同期を削除し、OpsData と OpsItems を複数の AWS リージョンとアカウントから単一の Amazon Simple Storage Service (Amazon S3) バケットに集約することもできます。詳細については、「Systems Manager Explorer のリソースデータ同期を削除する」を参照してください。S3 バケットを削除する方法については、「Amazon Simple Email Service デベロッパーガイド」の「バケットの削除」を参照してください。
Fleet Manager	Fleet Manager を使用してマネージドノードを削除することはできません。Amazon Elastic Compute Cloud (Amazon EC2) を使用する必要があります。詳細については、「インスタンスの終了 (Linux)」と「インスタンスの終了 (Windows)」を参照してください。

機能またはアーティファクト	詳細
インベントリ	インベントリデータの収集を停止するには、メタデータの収集元となるスケジュールとリソースを定義する State Manager の関連付けを削除してください。詳細については、「データ収集の停止とインベントリデータの削除」を参照してください。 AWS リソースに関するメタデータを表示するために AWS Systems Manager インベントリを使用する必要がなくなった場合は、インベントリデータ収集に使用したリソースデータの同期も削除するようお勧めします。詳細については、「インベントリリソースデータ同期の削除」を参照してください。
Maintenance Windows	メンテナンスウィンドウ、メンテナンスウィンドウターゲット、およびメンテナンスウィンドウタスクを削除できます。詳細については、「コンソールを使用してメンテナンスウィンドウリソースを更新または削除する」を参照してください。
OpsCenter	AWS Command Line Interface または AWS SDK を使用して DeleteOpsItem API 操作を呼び出すと、個々の OpsItem を削除できます。AWS Management Console で OpsItem を削除することはできません。詳細については、「OpsItems を削除する」を参照してください。
Parameter Store	作成したパラメータは削除できます。詳細については、「Parameter Store からのパラメータの削除」を参照してください。

機能またはアーティファクト	詳細
Patch Manager	カスタムパッチベースラインは削除できます。詳細については、「カスタムパッチベースラインの更新または削除」を参照してください。
Quick Setup	Quick Setup によって作成された関連付けは削除できます。関連付けは、State Manager によって保存、処理されます。詳細については、「関連付けを削除する」を参照してください。
Run Command	コマンドの処理が終了すると、そのコマンドに関する情報は [Command history (コマンド履歴)] タブに保存されます。[コマンド履歴] タブから情報を削除することはできません。
Automation	オートメーションの処理が完了すると、それに関する情報が [実行] タブに保存されます。[実行] タブから情報を削除することはできません。
サービスリンクロール	Systems Manager は一部のツールについて、サービスにリンクされたロールを自動的に作成します。これらのロールは削除できます。詳細については、「Systems Manager の AWSServiceRoleForAmazonSSM サービスにリンクされたロールの削除」を参照してください。
Session Manager	Session Manager はセッション終了後、リソースに関するデータを保持しません。セッションを終了するには、「セッションを終了する」を参照してください。

機能またはアーティファクト	詳細
SSM Agent	SSM Agent はノードから手動でアンインストールできます。詳細については、以下のトピックを参照してください。 • Linux: Linux 用 EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする • macOS: macOS 用の EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする • Windows Server: コントロールパネルを開き、[プログラムの追加/削除] を選択します。
State Manager	関連付けは削除できます。詳細については、「関連付けを削除する」を参照してください。
Systems Manager のドキュメントサービス	AWS または AWS サポート から提供されているランブックは削除できませんが、カスタムランブックは削除できます。詳細については、「カスタム SSM ドキュメントの削除」を参照してください。

State Manager または Maintenance Windows の選択

State Manager と Maintenance Windows (どちらも AWS Systems Manager のツール) は、マネージドノードで同様の種類の更新を実行できます。どちらを選択するかは、システムコンプライアンスを自動化する必要があるか、指定した期間中に優先度の高い、時間的制約のあるタスクを実行するかによって異なります。

State Manager および Maintenance Windows: 主要なユースケース

AWS Systems Manager のツールである State Manager は、AWS アカウント内のマネージドノードおよび AWS リソースに対して必要な構成状態を設定および維持します。構成とターゲットの組み合わせを関連付けオブジェクトとして定義できます。State Manager は、アカウント内のすべてのマネージドノードを一貫性のある状態で維持する場合、Amazon EC2 Auto Scaling を使用して新しい

ノードを生成する場合、またはアカウント内のマネージドノードに対して厳格なコンプライアンスレポート要件がある場合は、推奨されるツールです。

State Manager の主なユースケースは次のとおりです。

- Auto Scaling シナリオ: State Manager は、アカウント内で起動されたすべての新しいノードを手動または Auto Scaling グループを通じて監視できます。その新しいノードを対象とする関連付けがアカウント内に存在する場合 (タグまたはすべてのノード経由)、その特定の関連付けは新しいノードに自動的に適用されます。
- コンプライアンスレポート作成: State Manager はアカウント内のリソースに必要な状態のコンプライアンスレポート作成を促進できます。
- すべてのノードをサポート: State Manager は特定のアカウント内のすべてのノードを対象にできます。

メンテナンスウィンドウ は、特定のタイムウィンドウにある AWS リソースに対して 1 つ以上のアクションを実行します。開始時刻と終了時刻を持つメンテナンスウィンドウを 1 つ定義できます。このメンテナンスウィンドウ内で実行するタスクは複数指定できます。マネージドノードのパッチ適用、更新期間中のノードでの複数のタイプのタスクの実行、ノードで更新オペレーションを実行できるタイミングの制御などが優先度の高いオペレーションに含まれる場合に、AWS Systems Manager のツールである Maintenance Windows を使用します。

Maintenance Windows の主なユースケースは次のとおりです。

- 複数のドキュメントの実行: メンテナンスウィンドウで複数のタスクを実行できます。タスクごとに異なるドキュメントタイプを使用できます。その結果、1 つのメンテナンスウィンドウ内でさまざまなタスクを使用して、複雑なワークフローを構築できます。
- パッチ適用: メンテナンスウィンドウでは、特定のタグまたはリソースグループでタグ付けされた 1 つのリージョン内のすべてのマネージドノードのパッチ適用サポートを提供できます。パッチ適用には通常、ノードの停止 (例: ロードバランサーからのノードの削除)、パッチ適用、後処理 (ノードを本番環境に戻す) が含まれるため、パッチ適用は特定のパッチ時間枠内で一連のタスクとして実行できます。

> **Note**
>
> メンテナンスウィンドウを使用すると、パッチ適用操作は 1 つのアカウント内の 1 つのリージョンに限定されます。Systems Manager のツールである Quick Setup で作成されたパッチポリシーを使用して、代わりに AWS Organizations で作成された組織の一部ま

たはすべてのアカウントとリージョンのパッチ適用を設定できます。詳細については、「Quick Setup でのパッチポリシー設定」を参照してください。

- ウィンドウアクション: メンテナンスウィンドウでは、1 つまたは複数のアクションセットを、特定のタイムウィンドウ内で開始できます。メンテナンスウィンドウは、そのウィンドウの外では開始されません。既に開始されたアクションは、タイムウィンドウの外で終了した場合でも、終了するまで続行されます。

次の表は、State Manager と Maintenance Windows の主な機能を比較したものです。

機能	State Manager	Maintenance Windows
AWS CloudFormation の統合	AWS CloudFormation テンプレートは State Manager 関連付けをサポートします。	AWS CloudFormation テンプレートは、メンテナンスウィンドウ、ウィンドウターゲット、ウィンドウタスクをサポートします。
コンプライアンス	すべての State Manager 関連付けは、ターゲットリソースの目的の状態に関するコンプライアンスをレポートします。コンプライアンスダッシュボードを使用して、レポートされたコンプライアンスを集計して表示できます。	該当しません。
設定管理の統合	State Manager は、Microsoft PowerShell Desired State Configuration (DSC)、Ansible プレイブック、Chef レシピなどの外部のターゲットの状態ソリューションをサポートします。State Manager 関連付けを使用して、Configuration Management ソリューションが機能するかテストし、準備	該当なし。

機能	State Manager	Maintenance Windows
	ができたら設定変更をノードに適用できます。	
ドキュメント	State Manager 設定は、ポリシードキュメント (インベントリ情報の収集用)、オートメーションランブック (Amazon Simple Storage Service (Amazon S3) バケットなどの AWS リソース用)、またはマネージドノード用の Systems Manager コマンドドキュメント (SSM ドキュメント) として定義できます。	Maintenance Windows 構成は、オートメーションドキュメント (オプションの承認ワークフローを使用した複数ステップのアクション) または SSM ドキュメント (マネージドノードの目的の状態) として定義できます。
モニタリング	State Manager は、ノードの設定、関連付け、または状態の変化 (オンラインになった新しいノードなど) を監視します。State Manager がこれらの変更を検出すると、指定された関連付けは、その関連付けを最初にターゲットとするノードに再適用されます。	該当なし。

機能	State Manager	Maintenance Windows
タスク内の優先度	該当しません。	メンテナンスウィンドウ内のタスクには、優先順位を割り当てることができます。同じ優先順位にあるすべてのタスクは並行して実行されます。優先順位の低いタスクは、優先順位の高いタスクが最終状態に達した後に実行されます。条件付きでタスクを実行する方法はありません。優先順位の高いタスクが最終状態に達すると、前のタスクの状態に関係なく、次の優先順位のタスクが実行されます。
安全管理	State Manager は、大規模なフリートにまたがって構成を展開する際に、2 つの安全管理をサポートします。最大同時実行性を使用して、設定を適用する同時ノードまたはリソースの数を定義できます。フリート全体で特定の数または割合のエラーが発生した場合に State Manager 関連付けを一時停止するために使用できる、最大エラー率を定義できます。	メンテナンスウィンドウは、大規模なフリートにまたがって構成を展開する際に、2 つの安全管理をサポートします。最大同時実行性を使用して、設定を適用する同時ノードまたはリソースの数を定義できます。フリート全体で特定の数または割合のエラーが発生した場合にメンテナンスウィンドウ内のアクションを一時停止するために使用できる、最大エラー率を定義できます。

機能	State Manager	Maintenance Windows
スケジューリング	State Manager 関連付けは、オンデマンド、特定の cron 間隔、特定のレート、または作成後に 1 回実行できます。これは、リソースの目的の状態を、一貫してタイムリーに維持する場合に便利です。 **Important** State Manager の関連付けの cron 式は、3 月を表す場合に `03` や `MAR` ような月フィールドをサポートしていません。月次または四半期ごとの設定更新が必要な場合は、メンテナンスウィンドウがニーズに最も適しています。詳しくは、「リファレンス: Systems Manager の Cron 式および rate 式」を参照してください。	メンテナンスウィンドウは、at 式 (例: `"at(2021-07-07T13:15:30)"`)、cron および rate 式、オフセット付きの cron、メンテナンスウィンドウの実行開始時間と終了時間、特定の時間ウィンドウ内でスケジュールを停止するタイミングを指定するカットオフ時間など、複数のスケジューリングオプションをサポートしています。

機能	State Manager	Maintenance Windows
ターゲティング	State Manager 関連付けは、ノード ID、タグ、またはリソースグループを使用して、1 つ以上のノードをターゲットにすることができます。State Manager は、特定のアカウント内のすべてのマネージドノードをターゲットにできます。	メンテナンスウィンドウは、ノード ID、タグ、またはリソースグループを使用して、1 つ以上のノードをターゲットにすることができます。
メンテナンスウィンドウ内のタスク	該当しません。	メンテナンスウィンドウは、各タスクが特定の Automation ランブックまたはコマンドドキュメントのアクションを対象とする 1 つ以上のタスクをサポートできます。メンテナンスウィンドウ内のすべてのタスクは、タスクごとに異なる優先順位が設定されていない限り、並行して実行されます。 メンテナンスウィンドウでは、次の 4 つのタスクタイプがサポートされています。 • AWS Systems Manager Run Command コマンド • AWS Systems Manager Automation ワークフロー • AWS Lambda 関数 • AWS Step Functions タスク

関連情報

このサービスを利用する際に役立つ関連リソースは次のとおりです。

料金

Systems Manager ツールの中には料金が発生するものもあります。詳細については、「AWS Systems Manager 料金表」を参照してください。

AWS Systems Manager ドキュメントライブラリ

「AWS Systems Manager ドキュメント」- AWS AppConfig、Incident Manager、および SAP 用 AWS Systems Manager を含む Systems Manager のすべてのユーザーマニュアルにアクセスできます。

AWS re:Post

AWS re:Post — AWS が運営する質疑応答 (Q & A)。技術的な質問に対して、専門家がレビューしたクラウドソーシングによる回答を提供します。

AWS ブログとポッドキャスト

AWS 管理ツールカテゴリーの Systems Manager に関するブログ記事と、#Systems Manager タグが付いているその他の記事をお読みください。

Service Quotas

「Amazon Web Services 全般のリファレンス」の「Systems Manager Service Quotas」をご覧ください。特に明記されていない限り、各クォータは AWS アカウント の単一のリージョンに適用されます。

Systems Manager 用サービス認可リファレンス

「AWS サービス認可リファレンス」で、Systems Manager の AWS Identity and Access Management (IAM) ポリシーで使用できるアクション、リソース、および条件コンテキストキーに関する情報をご覧ください。

AWS Systems Manager サービスレベルアグリーメント

「AWS Systems Manager サービスレベルアグリーメント」(SLA) は、Systems Manager の使用を規定するポリシーであり、Systems Manager を使用する AWS アカウント ごとに個別に適用されます。

一般的な AWS リソース

AWS を利用する際に役立つ一般的なリソースは以下の通りです。

- クラスとワークショップ – AWS のスキルを磨き、実践的な経験を得るために役立つセルフペースラボに加えて、ロールベースのコースと特別コースへのリンクです。
- AWS デベロッパーセンター – チュートリアルの検索、ツールのダウンロード、AWS デベロッパーイベントの確認を行います。
- AWS デベロッパーツール - AWS アプリケーションを開発および管理するためのデベロッパーツール、SDK、IDE ツールキット、およびコマンドラインツールへのリンクです。
- ご利用開始のためのリソースセンター — AWS アカウント をセットアップする方法、AWS コミュニティに参加する方法、最初のアプリケーションを起動する方法を説明します。
- ハンズオンチュートリアル - ステップ バイ ステップのチュートリアルに従って、最初のアプリケーションを AWS で起動します。
- AWS ホワイトペーパー – アーキテクチャ、セキュリティ、エコノミクスなどのトピックについて、AWS のソリューションアーキテクトや他の技術エキスパートが記述した AWS の技術ホワイトペーパーの包括的なリストへのリンクです。
- AWS サポート センター – AWS サポート のケースを作成して管理するためのハブです。フォーラム、技術上のよくある質問、サービスヘルスステータス、AWS Trusted Advisor など、他の役立つリソースへのリンクも含まれています。
- サポート – サポート に関する情報のメインウェブページです。クラウド内でのアプリケーションの構築および実行を支援するために 1 対 1 での迅速な対応を行うサポートチャネルとして機能します。
- お問い合わせ - AWS の請求、アカウント、イベント、不正使用、その他の問題などに関するお問い合わせの受付窓口です。
- AWS サイトの利用規約 – 当社の著作権、商標、お客様のアカウント、ライセンス、サイトへのアクセス、その他のトピックに関する詳細情報。

ドキュメント履歴

次の表に、 の前回のリリース以後に行われた、文書の重要な変更を示しますAWS Systems Manager このドキュメントの更新に関する通知については、RSS フィードを購読してください。

変更	説明	日付
ジャストインタイムノードアクセスのための強化された RDP 記録	AWS Systems Manager ジャストインタイムノードアクセスで、RDP 記録の設定に関する追加情報が表示されるようになりました。記録が保存される S3 バケットで AWS KMS 暗号化を使用する場合は、バケット暗号化に使用される KMS キーへのアクセスを `ssm-guiconnect` サービスプリンシパルに付与する必要があります。このリリースでは、新しい記録ステータス `ProcessingError` も導入されました。これは、動画処理中の中間障害を示し、サービス依存関係の障害またはアクセス許可の欠落が原因である可能性があります。詳細については、「Recording RDP connections」を参照してください。	2025 年 6 月 13 日
Patch Manager のパッチの選択とインストールに関する情報を更新	パッチの選択とインストール中に Patch Manager が古いパッケージを処理する方法を説明する情報を追加しました。詳細については、「セキュリティに関連するパッチ	2025 年 6 月 12 日

	の選択方法」および「パッチのインストール方法」を参照してください。	
Quick Setup のマネージドポリシーを更新: AWSQuickSetupDeploymentRolePolicy	Systems Manager では、Quick Setup がインラインポリシーの代わりにこの管理ポリシーを使用して関連付けを作成できるように、管理ポリシー `AWSQuickSetupDeploymentRolePolicy` が更新されました。詳細については、「AWS マネージドポリシーの Systems Manager 更新」を参照してください。	2025 年 6 月 10 日
Patch Manager への導入を拡張	潜在的な顧客とユーザーに対し、Patch Manager をよりよく紹介するために、Patch Manager の章に次の 3 つのセクションを追加しました。 • Patch Manager はどのように組織にとってメリットになりますか? • Patch Manager はどのようなユーザーに適していますか? • Patch Manager の主な特徴は何ですか?	2025 年 5 月 21 日

Quick Setup のマネージドポリシーを更新: AWSQuickSetupSSMDeploymentRolePolicy	Systems Manager では、統合コンソール用に作成された IAM ロールと Lambda リソースにタグ付けするためのアクセス許可を付与するようにマネージドポリシー `AWSQuickSetupSSMDeploymentRolePolicy` を更新しました。詳細については、「AWS マネージドポリシーの Systems Manager 更新」を参照してください。	2025 年 5 月 7 日
統合コンソールに関する機能設定オプション	Systems Manager では統合コンソールの設定時に機能設定オプションを利用できるようになりました。これにより、デフォルトのホスト管理設定 (DHMC)、インベントリメタデータの収集、SSM Agent の自動更新をセットアップするかどうかを選択できます。詳細については、「組織用の Systems Manager 統合コンソールのセットアップ」および「単一のアカウントとリージョン用の Systems Manager 統合コンソールのセットアップ」を参照してください。	2025 年 5 月 7 日

Quick Setup のマネージドポリシーを更新: AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy	Systems Manager では、ジャストインタイムノードアクセス用に AWS Resource Access Manager によって共有されるリソースにタグ付けするアクセス許可を付与するようにマネージドポリシー `AWSSystemsManagerJustInTimeNodeAccessRolePropagationPolicy` を更新しました。詳細については、「AWS マネージドポリシーの Systems Manager 更新」を参照してください。	2025 年 4 月 29 日
Quick Setup のマネージドポリシーを更新: AWSQuickSetupManageJITNAResourcesExecutionPolicy	Systems Manager では、ジャストインタイムノードアクセス用に作成された IAM ロールにタグ付けするアクセス許可を付与するようにマネージドポリシー `AWSQuickSetupManageJITNAResourcesExecutionPolicy` を更新しました。詳細については、「AWS マネージドポリシーの Systems Manager 更新」を参照してください。	2025 年 4 月 29 日

Systems Manager がジャストインタイムノードアクセスを導入	AWS Systems Manager がジャストインタイムアクセスでマネージドノードに接続する方法をサポートするようになりました。この新しい方法でマネージドノードに接続すると、ノードへのアクセスを必要な場合にのみ期限付きで一時的に付与し、長期的なアクセスを不可能にすることで、ノードのセキュリティを強化できるようになります。また、Systems Manager では Windows Server ノードへの RDP セッションを記録できるので、コンプライアンス要件を満たす、根本原因を分析するといったことができるようになります。詳細については、「Systems Manager を使用したジャストインタイムノードアクセス」を参照してください。	2025 年 4 月 29 日
ジャストインタイムノードアクセス用の新しいマネージドポリシー	Systems Manager では、ジャストインタイムノードアクセスをサポートするために新しいマネージドポリシーをいくつかリリースしました。詳細については、「AWS マネージドポリシーの Systems Manager 更新」を参照してください。	2025 年 4 月 29 日

AWS Parameters and Secrets Lambda Extension の新バージョン	AWS Parameters and Secrets Lambda Extension の新バージョンが、サポートされているすべてのリージョンとアーキテクチャで利用可能になりました。	2025 年 4 月 23 日
新しいトピック:「Patch Manager におけるコンプライアンスとは」	フリート内のマネージドノードのパッチコンプライアンスは、AWSまたは他のサードパーティーによって定義されていません。新しいトピック「Patch Manager におけるコンプライアンスとは」では、Systems Manager によって管理されるノードのパッチコンプライアンスが、関連するパッチベースラインで指定された承認基準を満たす、すべてのパッチがノードにインストールされていることを意味します。コンプライアンスは、パッチベースラインで設定したルール、またはパッチ適用オペレーション用に選択する AWS が提供する事前定義されたパッチベースラインで定義されます。	2025 年 4 月 11 日

AWS Parameters and Secrets Lambda Extension の新バージョン	AWS Parameters and Secrets Lambda Extension の新バージョンが利用可能になりました。さらに、次のリージョンのために拡張機能のサポートが追加されました。 • アジアパシフィック (タイ) (ap-southeast-7) • メキシコ (中部) (mx-central-1)	2025 年 4 月 3 日
新しいトピック: Compliance のアクセス許可の設定	セキュリティのベストプラクティスとして、マネージドノードで使用される AWS Identity and Access Management (IAM) ロールを更新して、ノードが PutComplianceItems API アクションを使用する機能を制限することをお勧めします。この API アクションは、Amazon EC2 インスタンスやマネージドノードなど、指定されたリソースにコンプライアンスタイプやその他のコンプライアンスの詳細を登録します。詳細については、「Compliance のアクセス許可の設定」を参照してください。	2025 年 3 月11 日

更新されたトピック: ノードインサイトの確認	Systems Manager の統合コンソールでは、[ノードのインサイトを確認] ページに、組織またはアカウント内のマネージド EC2 インスタンスとアンマネージド EC2 インスタンスの数が表示されます。Systems Manager が `Stopped` 状態にあるときに EC2 インスタンスを「アンマネージド」の数に含めることを明確にしました。詳細については、「アンマネージドインスタンスとは」を参照してください。	2025 年 2 月 25 日
更新されたトピック: SSM Agent の署名を確認する	Linux インスタンス用の AWS Systems Manager Agent (SSM Agent) RPM および Debian インストーラーパッケージは、暗号化で署名されています。パブリックキーを使用して、エージェントのパッケージがオリジナルであり、変更されていないことを確認できます。ファイルが損傷していたり、改変されていた場合、検証は失敗します。RPM または GPG を使用して、インストーラーパッケージの署名を確認できます。トピックには、SSM Agent の新しいパブリックキーが含まれています。詳細については、「SSM Agent の署名の確認」を参照してください。	2025 年 2 月 14 日

新しいトピック: Session Manager プラグインの署名を確認する	Linux インスタンス用の Session Manager プラグイン RPM および Debian インストーラパッケージは、暗号化で署名されています。パブリックキーを使用して、プラグインバイナリとパッケージがオリジナルであり、変更されていないことを確認できます。ファイルが改変されていたり、損傷があった場合、確認は失敗します。GNU Privacy Guard (GPG) ツールを使用して、インストーラパッケージの署名を確認できます。詳細については、「Session Manager プラグインの署名の確認」を参照してください。	2025 年 2 月 13 日
Session Manager プラグインが更新されました	Session Manager プラグインは最近、次の機能強化で更新されました。Dockerfile で Go バージョンを 1.23 にアップグレードしました。README のバージョン設定ステップが更新されました。Session Manager プラグインの詳細については、「AWS CLI 用の Session Manager プラグインのインストール」を参照してください。	2025 年 2 月 6 日

Automation API のアクション向け TPS クォータが公開	Systems Manager Automation 関連の API アクションの、トランザクション/秒 (TPS) クォータ (以前の「制限」) を公開しました。詳細については、「Amazon Web Services 全般のリファレンス」の「System Manager Service Quotas」を参照してください。	2025 年 1 月 21 日
用語の変更: Systems Manager の「機能」は「ツール」に名称を変更しました。	これまで、Systems Manager を構成する機能ユニットは、「オートメーション機能」や「Parameter Store 機能」のように機能と呼ばれていました。今後、こうした機能ユニットはツールに改称され、例えば「Automation ツール」や「Parameter Store ツール」といった名称になります。本ユーザーガイドはこの変更を反映して更新されています。	2025 年 1 月 10 日
Patch Manager が macOS の新しいバージョンをサポート (Amazon EC2 AMI)	Patch Manager が macOS のバージョン 12.7、13.6、13.7、15.x を新たにサポートしました。Patch Manager がサポートしている OS とバージョンの完全なリストは、「Patch Manager でサポートされているオペレーティングシステム」を参照してください。	2025 年 1 月 8 日

追加バージョン向けの SSM Agent と Patch Manager のサポート: CentOS Stream、Ubuntu Server、Windows Server	Patch Manager は CentOS Stream 9、Ubuntu Server 24.10、Windows Server 2025 をサポートするようになりました。SSM Agent は、Ubuntu Server 24.10 と Windows Server 2025 をサポートするようになりました。(CentOS Stream 9 に対するエージェントのサポートは以前にリリースされました。) サポートされている OS およびバージョンの詳細なリストについては、以下のトピックを参照してください。 • System Manager でサポートされているオペレーティングシステム • Patch Manager でサポートされているオペレーティングシステム	2024 年 11 月 22 日
新しいトピック: Parameter Store SecureString パラメータの AWS KMS 暗号化	以下のトピックでは、AWS Systems Manager Parameter Store が AWS Key Management Service を使用して Parameter Store の `SecureString` パラメータの値を暗号化する方法について説明します。 • Parameter Store での SecureString パラメータの AWS KMS 暗号化	2024 年 11 月 22 日

Systems Manager の新規および更新されたマネージドポリシー	Systems Manager の新機能をサポートするために、新しい Systems Manager の設定とオペレーションをサポートするマネージドポリシーを新たにいくつかリリースし、さらに他のマネージドポリシーを更新します。詳細については、「AWS マネージドポリシーの Systems Manager 更新」を参照してください。	2024 年 11 月 21 日

Systems Manager の新しい簡素化されたノード管理エクスペリエンス	AWS Systems Manager では、アカウントとリージョン全体にわたって広範にノードを管理するための新しい統合コンソールエクスペリエンスがリリースされました。組織の AWS アカウントとリージョン全体のすべてのマネージドノードとアンマネージドノードを 1 か所で確認できるようになりました。また、アンマネージドノードを特定、診断、および修復することもできます。さらに、Systems Manager も Amazon Q Developer (Amazon Q) と統合されました。これにより、自然言語プロンプトを入力することで、AWS Management Console内の任意の場所からノードを表示および制御できるように機能が強化されました。このリリースでは、AWS Organizations を使用して委任管理者アカウントに組織全体で一元的にノードを管理することを許可できるようになりました。詳細については、以下の各トピックを参照してください。 • What is AWS Systems Manager? • AWS Systems Manager のセットアップ	2024 年 11 月 21 日

	• AWS Systems Manager によるノードタスクの完了	
Session Manager プラグインのバグ修正	先日、OpenDataChannel リクエストに認証情報を追加した変更がロールバックされるというバグを修正して、Session Manager プラグインを更新しました。	2024 年 11 月 20 日
Session Manager プラグインの機能強化	このバージョンは 2024 年 11 月 20 日に廃止されました。 このほど、以下の機能を強化して Session Manager プラグインを更新しました。 • OpenDataChannel リクエストに認証情報が追加されました。 • `testify` および `objx` 依存パッケージがアップグレードされました。	2024 年 11 月 6 日
macOS の OS バージョンの追加サポート	Systems Manager は、macOS オペレーティングシステムのバージョン 15.x (Sequoia) をサポートするようになりました (EC2 インスタンスのみ)。サポートされているすべての OS およびバージョンのリストについては、「Supported operating systems for Systems Manager でサポートされているオペレーティングシステム」を参照してください。	2024 年 11 月 6 日

Patch Manager: 承認済みリストと拒否されたリストでサポートされるパッケージ名形式の更新	一部のオペレーティングシステムで、パッチベースラインの [承認済みパッチ] リストと [拒否されたパッチ] リストに指定できるパッケージ名形式のリストを更新および拡大しました。詳細については、「Package name formats for Amazon Linux 1, Amazon Linux 2, Amazon Linux 2022, Amazon Linux 2023, CentOS, Oracle Linux, and Red Hat Enterprise Linux (RHEL)」を参照してください。	2024 年 11 月 1 日
Patch Manager のオペレーティングバージョンの追加のサポート	Patch Manager は、Oracle Linux (8.10 と 9.4) と Ubuntu Server (23.10 と 24.04) のバージョンを新たにサポートするようになりました。サポートされているすべてのオペレーティングシステムとバージョンのリストについては、以下のトピックを参照してください。 • System Manager でサポートされているオペレーティングシステム • Patch Manager でサポートされているオペレーティングシステム	2024 年 11 月 1 日

追加バージョン向けの SSM Agent サポート: CentOS Stream、Oracle Linux、Ubuntu Server	SSM Agent は、以前のサポートされているバージョンに加えて、CentOS Stream 9、Oracle Linux 8.10 と 9.4、Ubuntu Server 24.04 LTS をサポートするようになりました。サポートされている OS およびバージョンの完全なリストについては、「System Manager でサポートされているオペレーティングシステム」を参照してください。	2024 年 10 月 25 日
Session Manager プラグインの機能強化	OpenDataChannel リクエストでプラグインバージョンを渡すためのサポートが追加されました。	2024 年 10 月 10 日
新規: Fleet Manager を使用して行われた RDP 接続の詳細を表示する	AWS アカウントでユーザーが行ったリモートデスクトッププロトコル接続に関する情報を表示できるようになりました。詳細については、「現在および完了した接続に関する情報の表示」を参照してください。	2024 年 10 月 10 日

Patch Manager で SLES バージョン 15.6 のサポートを開始	SUSE Linux Enterprise Server (SLES) 15.6 のパッチ適用サポートがリリースされました。Patch Manager を使用して SLES 15.6 マシンにパッチを適用できるようになりました。Patch Manager によってサポートされているオペレーティングシステムとバージョンの詳細なリストについては、「Patch Manager でサポートされているオペレーティングシステム」を参照してください。	2024 年 9 月 29 日

AWS Parameters and Secrets Lambda Extension の新バージョン	AWS Parameters and Secrets Lambda Extension の新バージョンが利用可能になりました。アジアパシフィック (マレーシア) リージョン (ap-southeast-5) では、すべてのアーキテクチャのサポートが導入されています。さらに、次のリージョンのために ARM64 および Mac with Apple silicon アーキテクチャの拡張機能のサポートが追加されました。 • アジアパシフィック (ハイデラバード) (ap-south-2) • アジアパシフィック (メルボルン) (ap-southeast-4) • カナダ西部 (カルガリー) (ca-west-1) • 欧州 (チューリッヒ) (eu-central-2) • 欧州 (スペイン) (eu-south-2) • 中東 (UAE) (me-central-) • 中国 (北京) (cn-north-1) • 中国 (寧夏) (cn-northwest-1) • イスラエル (テルアビブ) (il-central-1) • AWS GovCloud (米国東部) (us-gov-east-1) • AWS GovCloud (米国西部) (us-gov-west-1)	2024 年 9 月 19 日

新しいトピック: AWS CLI を使用したメンテナンスウィンドウのアクセス許可の設定	トピック「AWS CLI を使用したメンテナンスウィンドウのアクセス許可の設定」では、ユーザーに代わってメンテナンスウィンドウタスクを実行するカスタムサービスロール (およびそのポリシー) を作成する手順について説明します。	2024 年 8 月 19 日
SSM Agent および Patch Manager の追加バージョンのサポート: AlmaLinux、Oracle Linux、および Rocky Linux	SSM Agent および Patch Manager は、これまでのサポート対象バージョンに加えて、AlmaLinux および Rocky Linux のバージョン 8.10、9.3、9.4、および Oracle Linux のバージョン 9.3 をサポートするようになりました。サポートされている OS およびバージョンの詳細なリストについては、以下のトピックを参照してください。 • System Manager でサポートされているオペレーティングシステム • Patch Manager でサポートされているオペレーティングシステム	2024 年 8 月 14 日

Parameter Store サポートの新しい IAM ポリシー条件: ssm:Policies	IAM ポリシーで新しくサポートされる条件である `ssm:Policies` を使用して、エンティティがパラメータポリシーを含むパラメータを作成または更新できないように設定することができます。詳細については、以下の各トピックを参照してください。 • ssm:Policies: パラメータポリシーを使用するパラメータの作成または更新を禁止する • サービス承認リファレンス 内の AWS Systems Managerの条件キー。	2024 年 8 月 14 日
Quick Setup のマネージドポリシーの更新: SSMQuickSetupRolePolicy	Systems Manager は、追加の AWS CloudFormation スタックセットへのアクセスを提供するようマネージドポリシー `SSMQuickSetupRolePolicy` を更新しました。詳細については、「AWS マネージドポリシーの Systems Manager 更新」を参照してください。	2024 年 8 月 13 日

Terraform を使用した Systems Manager リソースのプロビジョニングと管理のサポート	Systems Manager でサポートされているサードパーティー統合のリストに HashiCorp Terraform が追加されました。Terraform はオープンソースの infrastructure as code (IaC) ソフトウェアツールで、さまざまなクラウドサービスを管理するためのコマンドラインインターフェイス (CLI) ワークフローを提供します。Terraform を使用して、よく使用される多数の Systems Manager リソースとデータソースのプロビジョニングと管理を実行できます。Systems Manager と Terraform およびその他サードパーティーとの統合については、「その他の製品やサービスとの統合」を参照してください。	2024 年 8 月 1 日

新しい Quick Setup コンソールエクスペリエンスおよび API	Systems Manager Quick Setup が、新しいコンソールエクスペリエンスと API をリリースしました。今後は、コンソール、AWS CLI、AWS CloudFormation、および SDK を使用してこの API を操作できます。新しいコンソールには、 Quick Setup コンソールを使用してオプトインできます。新しい Quick Setup エクスペリエンスへのオンボーディングに関する詳細については、「Quick Setup の開始方法」を参照してください。Quick Setup API 経由で利用できる API オペレーションの詳細については、「Quick Setup API リファレンス」を参照してください。	2024 年 8 月 1 日

新しいトピック: カスタムパッチベースラインでの拒否されたパッチリストのオプション	Patch Manager でカスタムパッチベースラインを使用するパッチ適用オペレーションについて、拒否されたパッチリストに追加されたパッチにアクション `Allow as dependency` が割り当てられたときの動作を明確にしました。Windows Server はパッチ依存関係の概念をサポートしないため、マネージドノードにまだインストールされていないパッチはスキップされます。ノードに既にインストールされているパッチには、ステータス `INSTALLED_REJECTED` が割り当てられます。詳細については、「カスタムパッチベースラインでの拒否されたパッチリストのオプション」および「その他のオペレーティングシステムのパッチコンプライアンスの値」を参照してください。	2024 年 7 月 23 日
新しいトピック: 連邦情報処理規格 (FIPS) での使用のための SSM Agent の設定	連邦情報処理規格 (FIPS) での使用のために SSM Agent を設定する手順を提供しました。詳細については、「連邦情報処理規格 (FIPS) での使用のための SSM Agent の設定」を参照してください。	2024 年 7 月 22 日

更新: Fleet Manager ユーザー名での @ 記号のサポートを明確化	IAM アイデンティティセンターユーザー名に 1 つ、または複数の @ 記号が含まれている場合、Fleet Manager RDP は、@ が E メールアドレスのドメイン部分の先頭に使用されているかどうかにかかわらず、最初の @ 記号とその後に続くすべての文字を無視します。Fleet Manager RDP 接続のユーザー名でサポートされている文字の詳細については、「リモートデスクトップ接続の認証」を参照してください。	2024 年 7 月 21 日
更新されたマネージドポリシー: AmazonSSMManagedEC2InstanceDefaultPolicy	Systems Manager は、各ポリシーステートメントの目的を明確にするためのインラインステートメント ID (Sid) を提供することで、マネージドポリシー `AmazonSSMManagedEC2InstanceDefaultPolicy` を更新しました。詳細については、「AWS マネージドポリシーの Systems Manager 更新」を参照してください。	2024 年 7 月 18 日

Patch Manager パッチ適用オペレーション用の AWS マネージドバケットの名前変更	AWS は、さまざまな Patch Manager パッチ適用オペレーションを実行する過程で SSM Agent がアクセスする、多数の Amazon S3 バケットを所有し、維持しています。これらの S3 バケットはパブリックにアクセス可能です。デフォルトで、SSM Agent は HTTP 呼び出しを使用してこれに接続します。ただし、Systems Manager オペレーションで仮想プライベートクラウド (VPC) エンドポイントを使用している場合は、Systems Manager の Amazon EC2 インスタンスプロファイル、またはハイブリッドおよびマルチクラウド環境内にある EC2 以外のマシンのサービスロールで、明示的な許可を付与する必要があります。それ以外の場合、リソースからこれらのパブリックバケットにアクセスすることはできません。ほとんどの場合、これらのバケットの名前は変更されています。例えば、パッチ適用オペレーションの場合、バケット `aws-patchmanager-macos-us-east-2` は `aws-patchmanager-macos-us-east-2-552881074` に置き換えられ、バケット `aws-ssm-us-east-2` は `aws-patch-manager-`	2024 年 7 月 18 日

	us-east-2-552881074 に置き換えられます。詳細については、以下の各トピックを参照してください。 • SSM Agent と AWS マネージド S3 バケットとの通信 • 参照: パッチ適用オペレーション用の Amazon S3 バケット	
Quick Setup 用の新しいサービスにリンクされたロール	Systems Manager は、新しいサービスにリンクされたロール AWSServiceRoleForSSMQuickSetup をリリースしました。Systems Manager はこのロールを使用して、Quick Setup を使用して設定されたリソースの設定の正常性をチェックし、パラメータとプロビジョニングされたリソースが確実に一貫して使用されるようにするとともに、ドリフトが検出された場合にリソースを修復します。このロールに関連付けられているマネージドポリシーは SSMQuickSetupRolePolicy です。詳細については、「AWSServiceRoleForSSMQuickSetup service-linked role permissions for Systems Manager」を参照してください。	2024 年 7 月 3 日

Quick Setup 設定タイプ用の新しいマネージドポリシー	Systems Manager は、さまざまな Quick Setup 設定タイプとプロセスをサポートするために、さらに 12 個の新しいマネージドポリシーをリリースしました。詳細については、「AWS マネージドポリシーの Systems Manager 更新」を参照してください。	2024 年 7 月 3 日
RHEL 8.10 および 9.4 のサポート	Systems Manager と Patch Manager は現在、Red Hat Enterprise Linux バージョン 8.10 および 9.4 をサポートしています。詳細については、「サポートされているオペレーティングシステムとマシンタイプ」および「Patch Manager でサポートされているオペレーティングシステム」を参照してください。	2024 年 6 月 26 日
8.8 および 8.9 バージョンの Patch Manager サポート: AlmaLinux、Oracle Linux、および Rocky Linux	Patch Manager は、以前の 8.x バージョンに加えて、AlmaLinux、Oracle Linux、および Rocky Linux のバージョン 8.8 と 8.9 をサポートするようになりました。Patch Manager でサポートされている OS およびバージョンの詳細なリストについては、「Patch Manager でサポートされているオペレーティングシステム」を参照してください。	2024 年 6 月 17 日

macOS Amazon EC2 AMIs の新しいパブリックパラメータ	macOS Amazon Elastic Compute Cloud インスタンスのために Amazon Machine Images をサポートするパブリックパラメータがリリースされました。詳細については、以下のトピックを参照してください。 • パブリックパラメータの検索 • macOS のための AMI パブリックパラメータの呼び出し • 「Amazon EC2 ユーザーガイド」の「Mac インスタンスを起動する」 • 「Amazon EC2 ユーザーガイド」の「Amazon EC2 Mac インスタンス」 • 「Amazon EC2 Auto Scaling ユーザーガイド」の「Use AWS Systems Manager parameters instead of AMI IDs in launch templates」	2024 年 6 月 17 日

更新: /aws/service/global-infrastructure パラメータパスを使用できるリージョン	/aws/service/global-infrastructure パブリックパラメータパスをクエリできる商用リージョンと、別の商用 AWS リージョン で作業している場合にパスのクエリを実行する方法を明確にしました。詳細については、「AWS サービス、リージョン、エンドポイント、アベイラビリティーゾーン、Local Zones、Wavelength ゾーンのパブリックパラメータの呼び出し」を参照してください。	2024 年 6 月 12 日
New: コード例の章	新しい章の「Code examples for Systems Manager using AWS SDKs」では、Systems Manager サービスとの連携方法の例をさまざまな SDK 言語で示しています。	2024 年 5 月 8 日

ec2messages:* エンドポイントサポートの変更	2024 年以降にローンチされた AWS リージョン では、ec2messages:* エンドポイントのステータスと実行情報を Systems Manager サービスに送り返す機能が SSM Agent でサポートされません。これらのリージョンのアカウントは ssmmessages:* を使用する必要があります。2024 年より前にローンチされたリージョンでは、ssmmessages:* と ec2messages:* の両方が引き続きサポートされていますが、現在は ssmmessages:* エンドポイント (Amazon Message Gateway Service) のみを使用することをお勧めします。現時点では、ec2messages:* アクセス許可はポリシーから安全に削除できます。詳細については、「SSM Agent の使用」および「Agent 関連の API オペレーション (ssmmessages および ec2messages エンドポイント)」を参照してください。	2024 年 5 月 3 日

オートメーションランブックでスクリプトを実行するための追加のランタイム	`aws:executeScript` アクションは、Python 3.9、3.10、および 3.11 ランタイムをサポートするようになりました。このアクションを使用する方法の詳細については、「`aws:executeScript` 」を参照してください。	2024 年 4 月 23 日
8.8 および 8.9 バージョンのサポート: AlmaLinux、Oracle Linux、および Rocky Linux	Systems Manager は、以前の 8.x バージョンに加えて、AlmaLinux、Oracle Linux、および Rocky Linux のバージョン 8.8 と 8.9 をサポートするようになりました。サポートされている OS およびバージョンの全リストについては、「Supported operating systems for Systems Manager でサポートされているオペレーティングシステム」を参照してください。	2024 年 4 月 22 日

Patch Manager: パッチ適用ステータス「INSTALLED_PENDING_REBOOT」に変更	以前は、Patch Manager によってインストールされたパッチだけが「INSTALLED_PENDING_REBOOT 」とマークされました。このステータスは、Patch Manager の外部でインストールされたパッチには適用されませんでした。現在、「INSTALLED_PENDING_REBOOT 」は、マネージドノードが最後に再起動されてから適用されたパッチすべてに適用できるようになります。これには、NoReboot オプションを選択して Patch Manager によってインストールされたパッチと、ノードの直近の再起動以降に Patch Manager の外部でインストールされたパッチが含まれます。すべての Patch Manager のパッチ適用ステータス値の説明については、「Understanding patch compliance state values」を参照してください。	2024 年 4 月 16 日
RHEL 8.9 および 9.3 のサポート	Systems Manager (Patch Manager を含む) は、以前の 8.x および 9.x バージョンに加えて、Red Hat Enterprise Linux (RHEL) バージョン 8.9 および 9.3 をサポートするようになりました。	2024 年 3 月 26 日

トピックの更新: AWS Systems Manager の AWS マネージドポリシー	トピック「AWS Systems Manager の AWS マネージドポリシー」では、2021 年 3 月 12 日以降に導入または更新された Systems Manager の 4 つのマネージドポリシーに関する情報が提供されています。このトピックに、その日付より前に作成または最終更新された、Systems Manager で使用する他の 12 のマネージドポリシーに関する情報を記載したセクションを追加しました。詳細については、「Systems Manager 用の追加のマネージドポリシー」を参照してください。	2024 年 3 月 1 日
Parameter Store がクロスアカウント共有のサポートを開始	リソース共有を設定することで、AWS アカウント 間または AWS の組織内で詳細パラメータを安全かつ効率的に共有できるようになりました。リソース共有により、アプリケーションの構成管理を一元化し、所有するすべてのアカウントでパラメータを共有する際の運用上のオーバーヘッドを削減できます。パラメータは、Parameter Store コンソール、AWS RAM コンソール、または AWS CLI を使用して、アカウント間で共有できます。詳細については、「共有パラメータの操作」を参照してください。	2024 年 2 月 21 日

Automation アクションの強化	`aws:approve` アクションで `onFailure` および `isCritical` プロパティを使用できるようになりました。`aws:approve` アクションの詳細については、「aws:approve – Pause an automation for manual approval」を参照してください。	2024 年 2 月 12 日
Patch Manager のオペレーティングバージョンの追加のサポート	Patch Manager でサポートされているオペレーティングシステムのバージョンのリストに追加しました。以下のサポートが追加されました。 • Debian Server 11.x および 12.x • macOS 14.x (Sonoma) • SUSE Linux Enterprise Server (SLES) 15.5 • Ubuntu Server 23.04	2024 年 1 月 4 日
Application Manager コンソールを使用して自動 SSM Agent 更新を設定	Application Manager コンソールを使用してアプリケーションインスタンスの SSM Agent 更新を自動化できるようになりました。詳細については、「アプリケーションインスタンスの使用」を参照してください。	2023 年 12 月 21 日

ハイブリッド環境とマルチクラウド環境で Amazon EC2 以外のマシンを登録するプロセスを更新	Systems Manager で、Amazon Elastic Compute Cloud (Amazon EC2) 以外のマシンをハイブリッド環境とマルチクラウド環境に登録する際に役立つ `ssm-setup-cli` が利用できるようになりました。詳細については、「ハイブリッド Linux ノードで SSM Agent をインストールする方法」および「ハイブリッド Windows ノードで SSM Agent をインストールする方法」を参照してください。	2023 年 12 月 20 日
Fleet Manager を使用して Amazon EBS ボリュームを管理	マネージドインスタンス上の Amazon Elastic Block Store ボリュームを、AWS Systems Manager のツールである Fleet Manager を使って管理できるようになりました。例えば、EBS ボリュームを初期化し、パーティションをフォーマットして、ボリュームをマウントして使用できるようにする、といったことが行えます。詳細については、「EBS volume management」を参照してください。	2023 年 12 月 14 日
Session Manager プラグインの機能強化	StartSession API レスポンスを環境変数としてセッションマネージャープラグインに渡すサポートが追加されました。	2023 年 12 月 4 日

オートメーションランブックの新しいビジュアルデザインエクスペリエンス	Systems Manager Automation が開発した新しいビジュアルデザインエクスペリエンスを使用して、ランブックを作成および編集できるようになりました。ビジュアルデザインエクスペリエンスには、コードの少ないドラッグアンドドロップインターフェイスが用意されているため、ランブックをより簡単に作成および編集できます。詳しくは、「Automation ランブックのビジュアルデザインエクスペリエンス」を参照してください。	2023 年 11 月 26 日

Systems Manager の新しい自動化アクション、データ要素、およびランブックの機能強化	aws:loop アクションを使用してランブック内の複数のアクションをループオーバーできるようになりました。この新しいアクションは、do while と for each スタイルのループに対応しています。さらに、新しい変数データ要素を使用すると、ランブックのコンテキスト内で値を動的に定義、参照、更新できます。ランブック内の変数の値を更新するには、新しい aws:updateVariable アクションを使用します。オートメーションでは、出力の動的データ型変換のサポートも追加されました。つまり、出力の値が指定したデータ型と一致しない場合、オートメーションはデータ型を変換しようとします。例えば、返される値が Integer で、指定された Type が String の場合、最終的な出力値は String 値です。最後に、オートメーションはセレクター用の JSONPath フィルター式をサポートするようになりました。詳細については、以下の各トピックを参照してください。 • aws:loop — オートメーション内のステップを反復処理します	2023 年 11 月 17 日

	• aws:updateVariable — ランブック変数の値を更新します • データ要素とパラメータ — 最上位のデータ要素 • アクション出力の入力としての使用。 • ランブックでの JSONPath の使用。	
Remote Desktop Protocol (RDP) 接続のリージョンサポートが更新されました	Amazon DCV を利用した Fleet Manager リモートデスクトップでは、Systems Manager コンソールから直接 Windows Server インスタンスに安全に接続できます。Fleet Manager リモートデスクトップ接続では、次の 3 つのリージョンが追加で有効になりました。 • アフリカ (ケープタウン) (af-south-1) • アジアパシフィック (ジャカルタ) (ap-southeast-3) • イスラエル (テルアビブ) (il-central-1)	2023 年 11 月 15 日

Patch Manager: RHEL および macOS の拡張 OS バージョンのサポート	現在、Patch Manager では、次のオペレーティングシステムのバージョンが追加でサポートされています。 • Red Hat Enterprise Linux: バージョン 8.8 • macOS: 11.5–11:7 (Big Sur) • macOS: 12.0 ~ 12.6 (Monterey) • macOS: 13.0 ~ 13.5 (Ventura)	2023 年 10 月 23 日
新しい OpsCenter API - DeleteOpsItem	OpsCenter で個々の OpsItems を削除する DeleteOpsItem API の提供が開始されました。詳細については、AWS Systems Manager API リファレンスの「DeleteOpsItem」を参照してください。	2023 年 10 月 20 日
新しい Quick Setup 設定タイプ: 組織全体の SSM Agent の更新	新しい設定タイプ [デフォルトのホスト管理設定] では、AWS Organizations で定義されているとおり、組織管理者は組織のアカウントとリージョンのすべての EC2 インスタンスで SSM Agent の自動確認と更新を促すことができます。詳細については、「Default Host Management for an organization」を参照してください。	2023 年 10 月 16 日

CloudWatch Application Insights によって作成された OpsItems の新しいタイトルと説明フォーマット	CloudWatch Application Insights によって作成された OpsItems のタイトルと説明は、2023 年 10 月 16 日に改良されたフォーマットに変更されます。新しいフォーマットを確認するには、「Amazon CloudWatch Application Insights」を参照してください。	2023 年 9 月 29 日

Fleet Manager RDP 接続で複数のディスプレイの解像度をサポート	Fleet Manager のリモートデスクトッププロトコル (RDP) オプションを使用して Windows Server マネージドノードに接続するときに、ディスプレイの解像度を選択できるようになりました。以前は、すべての接続で 720P (1366 x 768) の固定解像度が使用されていました。接続ごとに次の中から選択できるようになりました。 • 自動的に適応 (検出された画面サイズに基づいて最適な解像度を決定する) • 1920 x 1080 • 1400 x 900 • 1366 x 768 • 800 x 600 詳細については、「Remote Desktop を使用してマネージドノードに接続するには」を参照してください。	2023 年 9 月 22 日

新しいトピック: パッチポリシー操作におけるランダムパッチベースライン ID	Quick Setup パッチポリシーが AWS-RunPatchBaseline SSM Command ドキュメントの BaselineOverride パラメータを使用して、パッチポリシー操作が実行されるたびにパッチベースラインのランダム ID を生成する方法を説明するコンテンツを追加しました。詳細については、「パッチポリシー操作におけるランダムパッチベースライン」を参照してください。	2023 年 9 月 22 日
OpsItems の管理に役立つ新しい運用上のインサイト	現在、OpsCenter には、[OpsItems を最も多く生成するリソース] という運用上のインサイトが含まれています。このタイプのインサイトは、AWS に 10 件の未処理の OpsItems リソースができると生成されます。このインサイトを使用して、問題のあるリソースを特定します。インサイト内の AWS-BulkResolveOpsItems ランブックを利用すると、リソースに関連する OpsItems を迅速に解決できます。詳細については、「運用上のインサイトを分析して、重複する OpsItems を減らす」を参照してください。	2023 年 9 月 22 日

更新済みの GPG パブリックキー	SSM Agent の署名を検証するための新しい公開鍵が作成されました。詳細については、「SSM Agent の署名の確認」を参照してください。	2023 年 9 月 5 日
AlmaLinux、Oracle Linux、RHEL、Rocky Linux の追加バージョンに対するサポートが追加されました。	AWS Systems Manager と Patch Manager の対応しているオペレーティングシステムのリストが、以下の追加 OS バージョンのサポートを反映するように更新されました。 • AlmaLinux: 9.2 • Oracle Linux: 8.7 と 9.2 • Red Hat Enterprise Linux (RHEL): 8.7, 9.1, and 9.2 • Rocky Linux: 8.6 と 8.7、9.0 ～ 9.2	2023 年 8 月 30 日

OpsCenter が OpsItem 説明フィールドでの Markdown フォーマットのサポートを追加しました。	OpsCenter が OpsItem 説明フィールドで、Markdown フォーマットをサポートするようになりました。以下の種類の Markdown フォーマットがサポートされています。 • 段落 • 線の間隔 • 水平線 • ヘッダー • テキストのフォーマット • リンク • Lists 詳細については、「AWS Management Console 入門ガイド」の「コンソールでの Markdown の使用」を参照してください。	2023 年 8 月 18 日
AWS Parameters and Secrets Lambda Extension の新バージョン	AWS Parameters and Secrets Lambda Extension の新バージョンが利用可能になりました。さらに、アジアパシフィック (メルボルン) (ap-southeast-4) およびイスラエル (テルアビブ) (il-central-1) リージョン (x86_64 と x86 アーキテクチャのみ) の拡張サポートが追加されました。詳細については、「AWS Lambda 関数での Parameter Store パラメータの使用」を参照してください。	2023 年 8 月 16 日

更新: Quick Setup パッチポリシーバケットに必要な許可に関する情報を追加しました	パッチポリシーを作成すると、Quick Setup は `baseline_overrides.json` という名前のファイルを含む Amazon S3 バケットを作成します。このファイルには、パッチポリシー用に指定したパッチベースラインに関する情報が保存されます。パッチポリシーを設定する際に、[インスタンスにアタッチされている既存のインスタンスプロファイルに必要な IAM ポリシーを追加] チェックボックスをオンにするオプションを使用できます。このオプションを選択しない場合は、このバケットにアクセスするための許可を特定のリソースに手動で提供する必要があります。そうしないと、ポリシーオペレーションが失敗する可能性があります。詳細については、以下の各トピックを参照してください。 • パッチポリシー S3 バケットの許可 • 問題:「Invoke-PatchBaselineOperation」:`baseline_overrides.json` についての「アクセスが拒否されました」エラーまたは	2023 年 7 月 6 日

	「S3 からファイルをダウンロードできません」エラー	
Quick Setup を使用して OpsCenter を設定し、マルチアカウント OpsItem 管理に対応	OpsCenter の Quick Setup を使用すると、複数のアカウント間で OpsItems を管理するために次のタスクを実行できます。 • 委任された管理者のアカウントを指定する • 必要な AWS Identity and Access Management (IAM) ポリシーとロールを作成する • 委任管理者が複数のアカウント間で OpsItems を管理できる AWS Organizations 組織、またはメンバーアカウントのサブセットを指定する 詳細については、「(オプション) Quick Setup を使用して、複数のアカウント間で OpsItems を管理するように OpsCenter を設定」を参照してください。	2023 年 6 月 19 日

Quick Setup を使用して Amazon EC2 起動エージェントを更新する	Systems Manager がインスタンスにインストールされている起動エージェントの新しいバージョンを 30 日ごとに確認するのを許可できるようになりました。新しいバージョンが利用可能である場合、Systems Manager はインスタンスのエージェントを更新します。詳細については、「Quick Setup ホストの管理」を参照してください。	2023 年 6 月 19 日
Patch Manager は、Ubuntu Server 22.04 LTS をサポートするようになりました	Ubuntu Server 22.04 LTS ノードのパッチ適用に Patch Manager を使用できるようになりました。Ubuntu Server のサポートされている他のバージョンと同様に、バージョン 22.04 LTS は AWS マネージド `AWS-UbuntuDefaultPatchBaseline` パッチベースラインを使用します。	2023 年 5 月 15 日

Systems Manager が Patch Manager を含む AlmaLinux をサポートするようになりました	Systems Manager を使用して、AlmaLinux 8.3 ~ 8.7、9.0 ~ 9.1 ノードを管理できるようになりました。RHEL 8 のパッチ適用に適用されるルールの多くは、AlmaLinux にも適用されます。AlmaLinux は新しい `AWS-DefaultAlmaLinuxPatchBaseline` を使用しています。詳細については、以下の各トピックを参照してください。 • AlmaLinux インスタンスに SSM Agent を手動でインストールする • セキュリティに関連するパッチの選択方法 • パッチのインストール方法 • AlmaLinux、RHEL および Rocky Linux でのパッチベースラインルールの動作方法。	2023 年 5 月 8 日
Quick Setup を使用して EC2Launch v2 エージェントをデプロイするには	Quick Setup を使用して EC2Launch v2 エージェントをデプロイできるようになりました。詳細については、「Quick Setup で Distributor パッケージをデプロイする」を参照してください。	2023 年 4 月 13 日

Systems Manager が Amazon Linux 2023 のサポートを開始	Systems Manager は、Patch Manager オペレーションのサポートを含めて、新しい Amazon Linux 2023 (AL2023) EC2 インスタンスタイプをサポートするようになりました。Amazon Linux 2 に適用されるパッチ適用ルールの多くは、Amazon Linux 2023 にも適用されます。(Patch Manager は Amazon Linux 2022 のプレビューリリースも引き続きサポートしています。) 詳細については、以下の各トピックを参照してください。 • セキュリティに関連するパッチの選択方法 • パッチのインストール方法 • Amazon Linux 1、Amazon Linux 2、Amazon Linux 2022、および Amazon Linux 2023 でのパッチベースラインルールの動作方法	2023 年 3 月 23 日

Amazon EC2 インスタンスの設定内容の改訂	Amazon EC2 インスタンスのセットアップコンテンツを改訂しました。インスタンスアクセス許可には、新しくリリースされたデフォルトのホスト管理構成を使用することが推奨されるようになりました。詳細については、「Systems Manager に必要なインスタンスのアクセス許可を設定する」を参照してください。	2023 年 2 月 15 日
デフォルトのホスト管理設定による自動インスタンス管理	Systems Manager を使用して Amazon EC2 インスタンス AWS リージョン 全体を自動的に管理できるようになりました。詳細については、「デフォルトのホスト管理設定」を参照してください。	2023 年 2 月 15 日
SSM ドキュメントをお気に入りに追加	頻繁に使用する SSM ドキュメントを見つけやすいように、ドキュメントをお気に入りに追加できるようになりました。1 つのドキュメントタイプ、AWS アカウント および AWS リージョン 1 つにつき、最大 20 のドキュメントをお気に入りに追加できます。Systems Manager の [ドキュメント] コンソールからお気に入りを選択、変更、表示できます。詳細については、「お気に入りへの文書の追加」を参照してください。	2023 年 2 月 7 日

Change Calendar を使用して自動化の変更管理を実装	オートメーションを Change Calendar と統合することで、社内のすべての AWS アカウント オートメーションに変更管理を実装できるようになりました。詳細については、「自動化の変更管理の実装」を参照してください。	2023 年 1 月 24 日
新しい Change Manager 承認ワークフロー	Change Manager 承認ワークフローは、行ごとの承認ではなく、レベルごとの承認をサポートするようになりました。以前は、承認レベルに追加したすべての承認者が変更リクエストを承認する必要がありました。それ以外の場合、レベルは承認されませんでした。ここで、レベルに必要な承認数を指定し、その数以上の承認者を追加できます。例えば、1 つのレベルに 3 人の承認を要求する一方で、承認者を 5 人まで指定できます。レベルを承認するには、そのうち 3 人の承認者からの承認で十分です。詳細については「変更テンプレートの承認について」を参照してください。	2023 年 1 月 23 日

新規: Quick Setup のパッチポリシーを使用した組織全体のパッチ適用の設定	Systems Manager のツールである Quick Setup で、Patch Manager を使用してパッチポリシーを作成できるようになりました。パッチポリシーは、マネージドノードに自動的にパッチを適用する際に使用するパッチベースラインとスケジュールを定義します。1 つのパッチポリシー設定を使用して、組織内のすべてのリージョンにおける全アカウント、選択したアカウントとリージョンのみ、または 1 つのアカウントとリージョンのペアにパッチを定義できます。詳細については、以下のトピックを参照してください。 • Quick Setup パッチポリシーの使用 • Quick Setup パッチポリシーを使用して組織全体のパッチ適用を自動化する	2022 年 12 月 22 日

Application Manager が Amazon EC2 と統合し、アプリケーションのコンテキストでインスタンスに関する情報を表示できるようになりました。	Application Manager は、選択したアプリケーションのインスタンスの状態、ステータス、および Amazon EC2 Auto Scaling の正常性をグラフ形式で表示します。[Instances] (インスタンス) タブには、アプリケーション内の各インスタンスに関する以下の情報を示すための表も含まれています。
	• インスタンスの状態 (保留中、停止中、実行中、停止済み)
	• SSM Agent の ping ステータス
	• インスタンス上で最後に処理された、Systems Manager Automation ランブックのステータスと名前
	• 状態ごとの Amazon CloudWatch Logs アラームの数。
	  • ALARM – メトリクスまたは式が、定義されているしきい値を超えています。
	  • OK – メトリクスや式は、定義されているしきい値の範囲内です。
	  • INSUFFICIENT_DATA – アラームが開始直後であるか、メトリクスが利用できないか、メトリクス用のデータが不足してい
		2022 年 12 月 22 日

	るため、アラームの状態を判定できません。 • 親および個別の Auto Scaling グループに関する正常性	
Quick Setup を使用した Amazon EC2 インスタンスの起動と停止のスケジュール	Quick Setup を使用して、Amazon EC2 インスタンスの起動と停止を自動化する Resource Scheduler ソリューションをデプロイできるようになりました。詳細については、「Resource Scheduler」(リソーススケジューラ) を参照してください。	2022 年 12 月 19 日

OpsCenter がアカウント間で OpsItems をサポートするようになりました	OpsCenter で、管理アカウント (AWS Organizations の管理アカウントまたは Systems Manager の委任された管理者アカウントのいずれか) と 1 つのメンバーアカウントからの OpsItems の単一セッションでの作業がサポートされます。設定が完了すると、ユーザーは次のタイプのアクションを実行できます。 • メンバーアカウントでの OpsItems の作成、表示、更新 • メンバーアカウントでの、OpsItems で指定されている AWS リソースに関する詳細情報の表示 • Systems Manager Automation ランブックを開始して、メンバーアカウントで AWS リソースに関する問題を修正 詳細については、「アカウントをまたいで OpsItems と連携するように OpsCenter を設定する」を参照してください。	2022 年 11 月 16 日

AWS CloudTrail Lake を使用した Change Manager の変更リクエストの詳細の追跡	AWS CloudTrail Lake のイベントデータストアを使用して、組織またはアカウントに対して Change Manager で実行された変更リクエストの詳細をキャプチャおよび確認できるようになりました。この情報には、変更リクエストが作成されたユーザー ID についての監査可能な詳細、リクエストが行われた IP アドレス、変更が行われた AWS リージョン、対象リソースなどが含まれます。詳細については、「変更リクエストイベントのモニタリング」および「変更リクエストの詳細、タスク、およびタイムラインの確認」を参照してください。	2022 年 11 月 11 日

CloudWatch アラームを使用した追加の Systems Manager Automation タスクの管理	CloudWatch アラームを使用して、複数のアカウントやリージョンにわたってオートメーションを実行する際、追加で制御を強化できるようになりました。オートメーションにメトリクスアラームや CloudWatch の複合アラームを適用することで、定義したメトリクスに基づきオートメーションが停止するタイミングを制御できます。複数のアカウントとリージョンで実行されるオートメーションへの CloudWatch アラームの適用について詳しくは、「複数のリージョン とアカウントでのオートメーションの実行」を参照してください。	2022 年 11 月 9 日
更新：「AWS Lambda 関数で Parameter Store パラメータの使用」	AWS Parameters and Secrets Lambda Extension を使用してパラメーター値を取得し、今後 Lambda 関数で使用するためにキャッシュするのに役立つ追加情報を提供しました。Lambda 拡張機能を使用すると、Parameter Store への API コール回数が減り、コストを削減できます。詳細については、「AWS Lambda 関数での Parameter Store パラメーターの使用」を参照してください。	2022 年 10 月 25 日

CloudWatch アラームを使用したその他の Systems Manager タスクの管理	CloudWatch アラームを使用して、オートメーションやコマンドを実行するときの制御を強化できるようになりました。CloudWatch アラームは、State Manager 関連付けまたはメンテナンスウィンドウタスクに登録されていると、オートメーションまたはコマンドにも追加できます。複合 CloudWatch アラームをオートメーションまたはコマンドに適用することで、定義したメトリクスに基づいてオートメーションまたはコマンドがいつ停止するかを制御できます。CloudWatch アラームをオートメーションまたはコマンドに適用する方法の詳細については、以下の手順を参照してください。 • セキュリティに関連するパッチの選択方法 • パッチのインストール方法 • Amazon Linux 1、Amazon Linux 2、および Amazon Linux 2022 でのパッチベースラインルールの動作方法。	2022 年 9 月 26 日

CloudWatch アラームを使用したその他の Systems Manager タスクの管理	CloudWatch アラームを使用して、オートメーションやコマンドを実行するときの制御を強化できるようになりました。CloudWatch アラームは、State Manager 関連付けまたはメンテナンスウィンドウタスクに登録されていると、オートメーションまたはコマンドにも追加できます。複合 CloudWatch アラームをオートメーションまたはコマンドに適用することで、定義したメトリクスに基づいてオートメーションまたはコマンドがいつ停止するかを制御できます。CloudWatch アラームをオートメーションまたはコマンドに適用する方法の詳細については、以下の手順を参照してください。 • シンプルなオートメーションワークフローを実行する • コンソールからコマンドを実行する • 関連付けを作成する • メンテナンスウィンドウにタスクを割り当てるには	2022 年 9 月 26 日
アドバンストインスタンス層の要件の明確化	お客様からのフィードバックに基づいて、「インスタンス層の設定」で、アドバンストインスタンス層をアクティブ化する必要があるシナリオを明確にしました。	2022 年 9 月 21 日

Quick Setup を使用して Amazon CloudWatch エージェントをデプロイする	Quick Setup を使用して Amazon CloudWatch エージェントをデプロイできます。詳細については、「Quick Setup で Distributor パッケージをデプロイする」を参照してください。	2022 年 9 月 20 日
EC2 インスタンスメタデータが許可されている場合、パッチグループで「PatchGroup」キーがサポートされるようになりました	EC2 インスタンスのメタデータでタグを許可するときには、作成するタグキーにスペースを含めないでください。以前は、これにより、Patch Manager で EC2 インスタンスの一部をのパッチグループに追加することができませんでした。タグキー `Patch Group` をインスタンスに適用する必要があったためです。現在は、Patch Manager で `Patch Group` (スペースあり) および `PatchGroup` (スペースなし) の両方が、パッチグループのインスタンスを識別するためのタグキーとしてサポートされています。インスタンスメタデータでタグが許可されている EC2 インスタンスを、Patch Manager のパッチグループに追加できるようになりました。パッチグループの詳細については、「パッチグループについて」を参照してください。	2022 年 8 月 31 日

新しいトピック:「パッケージのリリース日と更新日の計算方法」	AWS で管理されているパッチベースラインでは、新しいパッチはリリースまたは更新されてから 7 日後に自動承認されます。作成したカスタムパッチベースラインでは、リリースまたは更新されてからインストールが自動承認されるまでの待機日数をオプションで指定できます。Amazon Linux 1 と Amazon Linux 2 では、さまざまな要因が最新のリリース日と更新日の計算方法に影響します。自動承認の遅延を選択する際に予期しない結果にならないように、これらの要因について、トピック「パッケージのリリース日と更新日の計算方法」で説明します。	2022 年 8 月 24 日
更新された内容: AMI にパッチを適用し、Auto Scaling グループを更新する	起動設定の代わりに起動テンプレートを使用するように「Auto Scaling グループ用の AMIs を更新する」のチュートリアルを更新しました。さらに、最新の Automation アクションとランタイムをランブックの内容に実装しました。	2022 年 6 月 22 日

Change Manager: ユーザーが自動承認可能なリクエストを作成できないようにする	Change Manager で変更テンプレートを設定し、自動承認に対応できるようになりました。つまり、必要な IAM アクセス許可を持つユーザーは、追加承認の必要なしに変更リクエストを開始できます。また、変更テンプレートでサポートされている場合でも、個々のユーザー、グループ、IAM ロールが自動承認リクエストを送信しないよう制限することもできるようになりました。これは、新しい IAM 条件キーである `ssm:AutoApprove` を使用して行われます。詳細については、「Controlling access to auto-approval runbook workflows」(自動承認ランブックのワークフローへのアクセス制御) を参照してください。	2022 年 6 月 15 日

メンテナンスウィンドウのタスクロールのガイダンスを更新	以前は、Systems Manager コンソールが、AWS マネージド IAM サービスリンクロール AWSServiceRoleForAmazonSSM を選択して、タスクのメンテナンスロールとして使用する機能を提供していました。メンテナンスウィンドウのタスクにおける、このロールとそれに関連するポリシーである AmazonSSMServiceRolePolicy の使用は推奨されなくなりました。代わりに、メンテナンスウィンドウのタスク用にカスタムポリシーとロールを作成する必要があります。詳細については Maintenance Windows「のセットアップ」を参照してください。	2022 年 6 月 9 日
Session Manager をサポートするリモートホストへのポート転送	Session Manager がリモートホストへのポート転送セッションをサポートするようになりました。リモートホストは Systems Manager によって管理される必要はありません。詳細については、「Starting a session (port forwarding to remote host)」(セッションの開始 (リモートホストへのポート転送)) を参照してください。	2022 年 5 月 25 日

更新されたコンテンツ: Amazon EC2 Linux インスタンスで SSM Agent を手動インストールする手順	お客様からのフィードバックにお応えして、Amazon EC2 インスタンスで SSM Agent を手動インストールする手順を説明するトピックを見直しました。これらのトピックでは、あらゆる AWS リージョン の EC2 インスタンスにすばやくインストールしてコピー/ペーストできる、グローバルに利用可能なファイルを使用するコマンドについて説明しています。また、これらのトピックでは、独自の作業リージョンで使用可能なファイルを使用するインストールコマンドの作成に役立つ情報を提供しています。スクリプトまたはテンプレートを使用して複数のインスタンスにエージェントをインストールする場合は、後者の方法をお勧めします。詳細については、「Linux 用の EC2 インスタンスに手動で SSM Agent をインストールする」セクションの Linux オペレーティングシステムに関する説明を参照してください。	2022 年 5 月 9 日

新しいトピック: SSM Agent がプリインストールされた Amazon Machine Images (AMIs)	お客様からのフィードバックにお応えして、プリインストールされた SSM Agent を含む AWS マネージド AMIs に関する情報を一元化しました。このトピックでは、これらの AMIs から作成された Amazon EC2 インスタンスが正常にインストールされ、実行中であることを確認する方法についても説明しています。エージェントが正常にインストールされない、インストールされても起動しないというまれなケースに関して、これらのインスタンスでエージェントを開始または手動でインストールする情報も提供しています。詳細については、「SSM Agent がプリインストールされた Amazon Machine Images (AMIs) 」を参照してください。	2022 年 5 月 8 日
新規 State Manager セクション	State Manager が関連付けを実行する時期の詳細を説明する新しいセクションを追加しました。詳細については、「About association scheduling」(関連付けのスケジューリングについて) を参照してください。	2022 年 4 月 27 日

Patch Manager で Rocky Linux がサポートされるようになりました	Rocky Linux ノードのパッチ適用に Patch Manager を使用できるようになりました。RHEL 8 のパッチ適用に適用されるルールの多くは、Rocky Linux にも適用されます。Rocky Linux 8 では新しい `AWS-DefaultRockyLinuxPatchBaseline` が使用されます。詳細については、以下の各トピックを参照してください。 • セキュリティに関連するパッチの選択方法 • パッチのインストール方法 • RHEL、CentOS Stream、および Rocky Linux でのパッチベースラインルールの動作方法)	2022 年 4 月 14 日

Patch Manager で CentOS Stream 8 がサポートされるようになりました	Patch Manager を使用して、CentOS Stream 8 インスタンスおよび Red Hat Enterprise Linux (RHEL) 4.4-4.5 インスタンスにパッチを適用できるようになりました。RHEL 8 のパッチ適用に適用されるルールの多くは、CentOS Stream 8 にも適用されます。CentOS Stream 8 では `AWS-DefaultCentOSPatchBaseline` が使用されます。詳細については、以下の各トピックを参照してください。 • セキュリティに関連するパッチの選択方法 • パッチのインストール方法 • RHEL および CentOS Stream でのパッチベースラインルールの動作方法)	2022 年 4 月 4 日

Change Manager のロールの継承ポリシーを作成する	新しいセクションでは、Change Manager のロールの継承の作成および実装の要件について説明しています。ロールの継承は、ユーザーに代わって Change Manager が承認済み変更リクエストで指定された Runbook ワークフローを安全に実行できる AWS Identity and Access Management (IAM) サービスロールです。このロールは、AWS Systems Manager (AWS STS) `AssumeRole` の信頼を Change Manager に付与します。詳細については、「Configuring roles and permissions for Change Manager」を参照してください。	2022 年 3 月 18 日
Change Manager 変更リクエストを一括で承認または拒否する	Systems Manager コンソールで、1 回のオペレーションで複数の変更リクエストを選択して承認または却下できるようになりました。詳細については、「変更リクエストの確認と、承認または拒否 (コンソール)」を参照してください。	2022 年 3 月 8 日

Rocky Linux および Windows Server 2022 のマネージドノードを対象にしたサポート	Systems Manager は、Rocky Linux および Windows Server 2022 マネージドノード (オンプレミスまたは他のクラウドプロバイダーと配置されたエッジデバイスおよびハイブリッドマシンを含む) をサポートします。これらのオペレーティングシステムで Systems Manager を使用するには、ハイブリッド環境やエッジデバイスの手順を始めとする必要なすべての Systems Manager セットアップ手順 (該当する場合) を完了する必要があります。詳細については、「Systems Manager のセットアップ」を参照してください。Rocky Linux マシンの場合、手動で SSM Agent をインストールする必要もあります。詳細については、「Manually install SSM Agent on Rocky Linux instances」を参照してください。Windows Server 2022 Amazon Elastic Compute Cloud (Amazon EC2) インスタンスの場合、SSM Agent は、デフォルトでインストールされます。	2022 年 3 月 1 日

Automation で同時実行のニーズへの適応を有効にし、Automation 使用状況メトリクスを表示できるようにする	同時自動実行クォータのオートメーションによる自動的な調整と、オートメーションの使用状況に関して CloudWatch にパブリッシュされたメトリクスを表示することが可能になりました。適応的な同時実行の詳細については、「Allowing Automation to adapt to your concurrency needs」(同時実行のニーズに適応することをオートメーションに許可する) を参照してください。オートメーションの使用状況に関するメトリクスを表示する方法については、「Monitoring Automation metrics using Amazon CloudWatch」(Amazon CloudWatch を使用したオートメーションメトリクスのモニタリング) を参照してください。	2022 年 1 月 27 日

Automation で同時実行のニーズへの適応を有効にし、Automation 使用状況メトリクスを表示できるようにする	同時自動実行クォータのオートメーションによる自動的な調整と、オートメーションの使用状況に関して CloudWatch にパブリッシュされたメトリクスを表示することが可能になりました。適応的な同時実行の詳細については、「Allowing Automation to adapt to your concurrency needs」(同時実行のニーズに適応することをオートメーションに許可する) を参照してください。オートメーションの使用状況に関するメトリクスを表示する方法については、「Monitoring Automation metrics using Amazon CloudWatch」(Amazon CloudWatch を使用したオートメーションメトリクスのモニタリング) を参照してください。	2022 年 1 月 27 日
カテゴリ別に編成された Systems Manager のドキュメント	Systems Manager に関して Amazon が提供しているドキュメントがタイプとカテゴリ別に整理され、必要なドキュメントを見つけやすくなりました。	2022 年 1 月 13 日

オートメーション用の統合を作成して呼び出す	統合を作成することで、オートメーション中にウェブフックを使用したメッセージの送信ができるようになりました。統合は、ランブック内で新しい `aws:invokeWebhook` アクションを使用することで、オートメーション中に呼び出せます。統合の作成についての詳細は、「Creating webhook integrations for Automation」(オートメーション用の webhook 統合を作成する) を参照してください。`aws:invokeWebhook` アクションの詳細については、「aws:invokeWebhook – オートメーションのウェブフック統合を呼び出す」を参照してください。	2022 年 1 月 13 日
新しい AWS リージョン では使用できない機能	次の Systems Manager ツールは、現在、新しいアジアパシフィック (ジャカルタ) リージョンでは使用できません。 • Application Manager • Change Calendar • Change Manager • Explorer • Fleet Manager • Incident Manager • Quick Setup	2021 年 12 月 13 日

アプリケーションのリソースコストの詳細の表示	Application Manager は、Cost Explorer ウィジェットを介して AWS Billing and Cost Management と統合されています。請求およびコストマネジメントコンソールで Cost Explorer を有効にした後、Application Manager の Cost Explorer ウィジェットに、特定の非コンテナアプリケーションまたはアプリケーションコンポーネントのコストデータが表示されます。ウィジェットでフィルターを使用して、棒グラフまたは折れ線グラフで、異なる期間、粒度、およびコストタイプに基づいてコストデータを表示できます。詳細については、「Viewing overview information about an application」(アプリケーションの概要情報を表示する) を参照してください。	2021 年 12 月 7 日
Fleet Manager を使用したプロセスの管理	ノード上のプロセスを管理するために Fleet Manager を使用できるようになりました。詳細については、「Working with processes」(プロセスの操作) を参照してください。	2021 年 12 月 6 日

用語の変更: マネージドインスタンスがマネージドノードになりました	AWS IoT Greengrass コアデバイスのサポートに伴い、Systems Manager ドキュメントのほとんどで、[managed instance] (マネージドインスタンス) という語句が [managed node] (マネージドノード) に変更されています。Systems Manager コンソール、API コール、エラーメッセージ、および SSM ドキュメントでは、依然としてインスタンスの条件が使用されます。	2021 年 11 月 29 日

エッジデバイスへのサポート	Systems Manager は、次のエッジデバイス構成をサポートしています。 • AWS IoT Greengrass: Systems Manager は、AWS IoT Greengrass に設定され、AWS IoT Greengrass Core ソフトウェアを実行するすべてのデバイスをサポートするようになりました。AWS IoT Greengrass コアデバイスをオンボードするには、AWS Identity and Access Management (IAM) サービスロールを作成する必要があります。AWS IoT Greengrass コンソールを使用して、SSM Agent を AWS IoT Greengrass コンポーネントとしてデバイス上にデプロイする必要もあります。詳細については、「エッジデバイス用に AWS Systems Manager のセットアップ」を参照してください。 • Edge devices in a hybrid environment: また、Systems Manager は、オンプレミスマシンとして構成した後、AWS IoT コアデバイスと非 AWS IoT デバイスをサポートします。デバイスをオンボーディングするには、IAM サービスロール	2021 年 11 月 29 日

	を作成し、ハイブリッド環境のマネージドノードアクティベーションを作成し、デバイスに SSM Agent を手動でインストールする必要があります。詳細については、「ハイブリッド環境で AWS Systems Manager を設定する」を参照してください。	
リモートデスクトップを使用してマネージドインスタンスに接続	Fleet Manager を使用して、マネージド Windows インスタンスにリモートデスクトッププロトコル (RDP) で接続できるようになりました。Amazon DCV を利用したリモートデスクトップセッションでは、ブラウザから直接インスタンスに安全に接続することができます。詳細については、「Connect using Remote Desktop」(リモートデスクトップを使用した接続) を参照してください。	2021 年 11 月 23 日

最大セッション期間を指定し、セッションの理由を提示する	AWS アカウント の AWS リージョン で Session Manager セッションのすべてに対し、最大セッション期間を指定できるようになりました。セッションが指定した期間に達すると終了します。セッションの開始時に、オプションで理由を追加することもできるようになりました。詳細については、「Specify maximum session duration」(最大セッション時間の指定) を参照してください。	2021 年 11 月 16 日

Patch Manager で、Raspberry Pi OS オペレーティングシステムがサポートされるようになりました	Patch Manager を使用して Raspberry Pi OS インスタンスにパッチを適用できるようになりました。Patch Manager は Raspberry Pi OS 9 (Stretch) および 10 (Buster) へのパッチ適用をサポートします。Raspberry Pi OS は Debian ベースの OS であるため、Debian Server と同じパッチ適用のルールが多く適用されます。詳細については、以下の各トピックを参照してください。 • セキュリティに関連するパッチの選択方法 • パッチのインストール方法 • Debian Server および Raspberry Pi OS でのパッチベースラインルールの動作方法	2021 年 11 月 16 日
Red Hat ナレッジベースポータルにアクセス	Fleet Manager を使用して、RHEL ナレッジベースポータルにアクセスして、Red Hat 製品の使用に関するソリューション、記事、ドキュメント、およびビデオをご覧ください。詳細については、「Red Hat ナレッジベースポータルへのアクセス」を参照してください。	2021 年 11 月 3 日

OpsItems を一括編集	OpsCenter が一括編集をサポートするようになりました OpsItems。複数の OpsItems を選択し、次のフィールドのいずれかを編集できます。ステータス、優先度、重要度、カテゴリ。詳細については、「OpsItems の編集」を参照してください。	2021 年 10 月 15 日
AWS リソースを設定する入力パラメータの作成	AWS Management Console で AWS リソースを設定するオートメーションランブックで入力パラメータを作成できるようになりました。詳細については、「AWS リソースを設定する入力パラメータの作成」を参照してください。	2021 年 10 月 14 日
メンテナンスウィンドウ用の新しいタスク呼び出しカットオフオプション	メンテナンス期間に指定されたカットオフ時間に達した後、新しいタスク呼び出しの開始をブロックするように選択できるようになりました。詳細については、「メンテナンスウィンドウにタスクを割り当てる (コンソール)」を参照してください。	2021 年 10 月 13 日

macOS 11.3.1 および 11.4 (Big Sur) 向けの Patch Manager サポート	macOS 11.3.1 および 11.4 (Big Sur) の Amazon Elastic Compute Cloud (Amazon EC2) インスタンスは、Patch Manager を使用してパッチ適用ができます。これは、既存の macOS 10.14.x (Mojave) と 10.15.x (Catalina) のサポートに追加されます。Patch Manager の操作方法の詳細については、「AWS Systems ManagerPatch Manager」を参照してください。	2021 年 10 月 1 日

Application Manager の Application Insights	Application Manager は、Amazon CloudWatch Application Insights と統合できます。Application Insights は、アプリケーションリソースとテクノロジースタック全体の主要なメトリクス、ログ、アラームを識別して設定します。また、メトリクスとログを継続的にモニタリングし、異常やエラーを検出して相互に関連付けます。エラーや異常が検出されると、Application Insights は CloudWatch Events を生成します。これを使用すると、通知を設定したり、アクションを実行したりできます。Application Insights は、Application Manager の [Overview (概要)] と [Monitoring (モニタリング)] タブで有効にして表示できます。Application Insights の詳細については、Amazon CloudWatch ユーザーガイドの「Amazon CloudWatch Application Insights とは」を参照してください。	2021 年 9 月 21 日

他のカレンダーから Change Calendar にイベントをインポート	サードパーティーのカレンダーから Change Calendar のカレンダーにイベントをインポートできるようになりました。以前は、各イベントをカレンダーに手動で入力する必要がありました。サポートされているサードパーティーのカレンダープロバイダから iCalendar (`.ics`) ファイルにカレンダーをエクスポートして、Change Calendar にインポートします。そのイベントは、Systems Manager で開いているカレンダーまたは閉じているカレンダーのルールに含まれます。サポートされているプロバイダとしては、iCloud カレンダー、Google カレンダー、Microsoft Outlook などがあります。詳細については、「サードパーティーのカレンダーからのイベントのインポートと管理」を参照してください。	2021 年 9 月 8 日

Application Manager での新しいタグ付けとランブック機能	タグ付けの機能強化には、Application Manager アプリケーションの特定のリソースまたはあらゆるリソースからのタグタグの追加または削除が含まれます。ランブックの機能強化には、特定のリソースタイプのランブックのフィルター処理された一覧の表示や、同じタイプのすべてのリソースでのランブックの開始が含まれます。詳細については、「Application Manager でのタグの使用」と「Application Manager でのランブックの使用」を参照してください。	2021 年 8 月 31 日
新しい例: AWS CLI を使用して変更リクエストを作成する	AWS CLI を使用して変更リクエストを作成する例が Change Manager の章に追加されました。この例では、`AWS-HelloWorldChangeTemplate` 変更テンプレートのサンプルと`AWS-HelloWorld runbook` を使用しています。 • 変更リクエストの作成 (AWS CLI)	2021 年 8 月 20 日

新しいセクション: Amazon EKS でパラメータを使用する	新しいセクションが Parameter Store の章に追加されました。このトピックは、Amazon EKS クラスターでパラメータを使用する方法のチュートリアルです。詳細については、「Parameter Store パラメータを Amazon Elastic Kubernetes Service で使用する」を参照してください。	2021 年 8 月 19 日
Patch Manager ライフサイクルフックの更新	Patch Manager でライフサイクルフックを利用できるようになりました。これは、Systems Manager コマンドドキュメントを実行する機能で、[Patch now (今すぐパッチ適用)] のパッチ適用オペレーション中に追加ポイントとなります。[今すぐパッチ適用] の実行後にインスタンスの再起動をスケジュールする際、再起動の完了後に実行されるようライフサイクルフックを指定できます。詳細については、「[今すぐパッチ適用] ライフサイクルフックの使用」と「AWS-RunPatchBaselineWithHooks SSM ドキュメントについて」を参照してください。	2021 年 8 月 9 日

Change Manager リクエストで自動承認をサポート	Change Manager で変更テンプレートを設定し、自動承認に対応できるようになりました。つまち、必要な IAM アクセス許可のあるユーザーは、追加の承認がなくても変更リクエストを開始できます。自動承認テンプレートにアクセスできるユーザーは、承認者を指定できます。Change Manager プロセスを管理しやすくするため、変更の凍結期間中も、すべてのリクエストに対して承認が必要です。詳細については、以下の各トピックを参照してください。 • 変更テンプレートの作成 • 変更リクエストの作成 • AWS マネージド Hello World 変更テンプレートの試用	2021 年 7 月 30 日

OpsCenter オペレーションインサイト	OpsCenter はアカウントで OpsItems を自動的に分析し、インサイトを作成します。インサイトには、アカウントに含まれている重複する OpsItems の数と、それを作成しているソースを把握できる情報が含まれています。また、インサイトには、重複する OpsItems を解決するために推奨されるベストプラクティスとオートメーションランブックも用意されています。詳細については、「オペレーションインサイトの使用」を参照してください。	2021 年 7 月 13 日
Fleet Manager で停止したインスタンスを表示	running に含まれているインスタンスと、Fleet Manager コンソールからのstoppedインスタンスを表示できるようになりました。詳細については、「AWS Systems ManagerFleet Manager」を参照してください。	2021 年 7 月 12 日
新しいトピック: Automation ランブックを作成する	新しいトピック「オートメーションランブックを作成する」では、カスタムオートメーションランブックのコンテンツを作成する方法に関するガイダンスおよび説明例を提供します。	2021 年 7 月 8 日

Application Manager での AWS CloudFormation スタックとテンプレートの作成	Application Manager は、CloudFormation と統合することで、アプリケーションのリソースのプロビジョニングと管理に役立ちます。AWS CloudFormation テンプレートとスタックは、Application Manager で作成、編集、削除できます。Application Manager には、テンプレートのクローン、作成、および格納が可能なテンプレートライブラリも含まれています。Application Manager と CloudFormation には、スタックの現在のステータスに関する同じ情報が表示されます。テンプレートとテンプレートの更新は、スタックをプロビジョニングするまで Systems Manager に格納されます。このとき、変更内容は CloudFormation にも表示されます。詳細については、「Application Manager での AWS CloudFormation スタックの使用」を参照してください。	2021 年 7 月 8 日

新しいトピック: ハイブリッドインスタンスで SSM Agent のプライベートキーを自動的にローテーション	新しいトピック「プライベートキーの自動ローテーションの設定」では、ハイブリッド環境でプライベートキーを自動的にローテーションするよう SSM Agent を設定することで、セキュリティ体制を強化する方法を説明しています。	2021 年 6 月 15 日
AWS CLI バージョン 1.2.205.0 の Session Manager プラグイン	新しいバージョンの AWS CLI の Session Manager プラグインがリリースされました。詳細については、「Session Manager プラグインの最新バージョンとリリース履歴」を参照してください。	2021 年 6 月 10 日
新しい IAM サービスリンクロール	OpsCenter オペレーションインサイトを有効にすると、Systems Manager は `AWSSSMOpsInsightsServiceRolePolicy` という名前の新しい AWS Identity and Access Management (IAM) サービスリンクロールを作成します。このロールの詳細については、「ロールを使用して Systems Manager でオペレーションインサイト OpsItems を作成するOpsCenter: `AWSSSMOpsInsightsServiceRolePolicy` 」を参照してください。	2021 年 6 月 9 日

Linux 用の新しい Patch Manager のトラブルシューティングの内容	新しいトピック「Linux で、AWS-RunPatchBaseline 実行時のエラー」では、Linux オペレーティングシステムを使用して管理対象インスタンスにパッチを適用するときに発生する可能性があるいくつかの問題の説明と解決策を提供します。	2021 年 6 月 8 日

指定されたターゲットを必要としないメンテナンスウィンドウタスクのサポートが向上 (コンソール)	必要でない場合、タスクでターゲットを指定しなくても、コンソールでメンテナンスウィンドウタスクを作成できるようになりました。以前は、このオプションは AWS CLI または API を使用する場合にのみ使用可能でした。このオプションは、オートメーション、 AWS Lambda および AWS Step Functions タスクタイプに適用されます。例えば、オートメーションタスクを作成し、更新するリソースがオートメーションドキュメントパラメーターで指定されている場合、タスク自体にターゲットを指定する必要がなくなります。詳細については、「ターゲットのないメンテナンスウィンドウタスクを登録」、「メンテナンスウィンドウにタスクを割り当てる (コンソール)」および「Schedule automations with maintenance windows」(メンテナンスウィンドウでオートメーションをスケジュールする) 参照してください。	2021 年 5 月 28 日
Automation ランブックのリファレンスが移動	Automation ランブックリファレンスが新しい場所に移動しました。詳細については、Systems Manager Automation ランブックリファレンスを参照してください。	2021 年 5 月 10 日

AWS Systems Manager Incident Manager の起動	Incident Manager は、AWS がホストするアプリケーションに影響を与えるインシデントを、ユーザーが緩和したりそのようなインシデントから復旧したりできるように設計された、インシデントマネジメントコンソールです。詳細については AWS Systems Manager Incident Manager ユーザーガイドを参照してください。	2021 年 5 月 10 日
State Manager が Change Calendar をサポート	State Managerの関連付けを作成するか更新する際、Change Calendar の名前または Amazon リソースネーム (ARN) を指定できるようになりました。State Manager は、変更カレンダーが開いている場合にのみ関連付けを適用します。閉じているときは適用しません。詳細については、「関連付けの作成」および「関連付けの編集と新しいバージョンの作成」を参照してください。	2021 年 5 月 6 日

Systems Manager のドキュメントのクローンを作成する。	Systems Manager のドキュメントコンソールを使用して、既存のドキュメントから新しいドキュメントにコンテンツをコピーし、変更できるようになりました。詳細については、「SSM ドキュメントのクローンを作成する」を参照してください。	2021 年 5 月 4 日
Security Hub を Explorer および OpsCenter と統合	Explorer と OpsCenter を AWS Security Hub に統合できるようになりました。Security Hub では、AWS のセキュリティ状態を包括的に把握し、セキュリティ業界標準およびベストプラクティスに照らして環境をチェックするのに役立ちます。Explorer と統合すると、Explorer ダッシュボードの Security Hub ウィジェットにセキュリティ結果を表示できます。OpsCenter と統合すると、Security Hub の検出結果に対して OpsItems を作成できます。詳細については、「Explorer での AWS Security Hub の結果の受信」と「OpsCenter での AWS Security Hub の結果の受信」を参照してください。	2021 年 4 月 27 日

新しいトピック: ドキュメントの表記規則	AWS Systems Manager ユーザーガイドの一般的な表記規則を理解しやすくするために、新しいトピックを追加しました。詳細については、「ドキュメントの表記規則」を参照してください。	2021 年 4 月 21 日
トピックの更新: Windows Server で Microsoft がリリースしたアプリケーションのパッチ適用について	「Windows Server で Microsoft がリリースしたアプリケーションのパッチ適用について」のトピックで、Patch Manager が Microsoft からリリースされたアプリケーションを Windows Server マネージドインスタンス適用できるようにするために、インスタンスで Windows 更新オプション [Windows の更新時に他の Microsoft 製品の更新プログラムも入手します。] を有効にする必要があることを明確にしました。	2021 年 4 月 12 日
オートメーションランブックのリファレンスの再編成	必要なランブックを検索し、より効率的にリファレンスできるように、オートメーションランブックのリファレンスのコンテンツを関連する AWS のサービス別に再編成しました。これらの変更を表示するには、Systems Manager Automation ランブックリファレンスを参照してください。	2021 年 4 月 12 日

Patch Manager: .csv パッチコンプライアンスレポートの生成	Patch Manager では、インスタンスのパッチコンプライアンスレポートを生成し、任意の S3 バケットに .csv 形式でレポートを保存できるようになりました。その後、Amazon QuickSight などのツールを使用して、パッチコンプライアンスレポートのデータを分析できます。単一のインスタンス、または 内のすべてのインスタンスについて、パッチコンプライアンスレポートを生成できますAWS アカウントオンデマンドで 1 回限りのレポートを生成することも、レポートが自動的に作成されるようにスケジュールを設定することもできます。Amazon Simple Notification Service トピックを指定して、レポートの生成時に通知を受け取ることもできます。詳細については、「CSV パッチコンプライアンスレポートの生成」を参照してください。	2021 年 4 月 9 日
Parameter Store パラメータラベルを削除	Systems Manager コンソールまたは AWS CLI を使用して、Parameter Store のパラメータラベルを削除できるようになりました。詳細については、「パラメータラベルの使用」を参照してください。	2021 年 4 月 6 日

[Patch Now] (今すぐパッチを適用) を使用する際のインスタンスの再起動をスケジュールする	Patch Manager では、[Patch Now] (今すぐパッチ) 機能を使用してパッチがインストールされた後にインスタンスが再起動する時間をスケジュールできるようになりました。これは、パッチのインストールを完了するために必要な場合にのみインスタンスを再起動するか、パッチ適用オペレーション後にすべての再起動をスキップする既存のオプションに加えて提供されます。詳細については、「オンデマンドでのインスタンスへのパッチ適用」を参照してください。	2021 年 4 月 1 日
新しいトピック: パブリックパラメータを検出する	Parameter Store のパブリックパラメータは、AWS CLI または Systems Manager コンソールを使用して見つけることができます。詳細については、「パブリックパラメータの検索」を参照してください。	2021 年 4 月 1 日

更新を今すぐパッチ適用する: S3 にログを保存し、ライフサイクルフックを実行する	Patch Manager の [Patch now (今すぐパッチ適用)] オペレーションを実行すると、パッチ適用ログを自動的に格納する S3 バケットを選択できます。さらに、オペレーション中に、Before installation (インストール前)、After installation (インストール後)、On exit (終了時) の 3 つの時点で Systems Manager コマンドドキュメント (SSM ドキュメント) をライフサイクルフックとして実行することもできます。詳細については、「オンデマンドでのインスタンスへのパッチ適用」を参照してください。	2021 年 3 月 31 日
Systems Manager が AWS 管理ポリシーの変更をレポートするようになりました	2021 年 3 月 24 日以降、管理ポリシーへの変更は、「AWS 管理ポリシーの Systems Manager の更新」に関するトピックでレポートされます。記載される最初の変更は、複数のアカウントとリージョンからの OpsData および OpsItems をレポートする Explorer ツールのサポートの追加です。	2021 年 3 月 24 日

Explorer は、AWS Organizations のアカウントに基づいてリソースデータ同期のあらゆる OpsData ソースを自動的に許可	リソースデータ同期を作成するときに、AWS Organizations オプションのいずれかを選択すると、Systems Manager は、組織内 (または選択した組織単位内) のすべての AWS アカウント について、選択した AWS リージョン のすべての OpsData ソースを自動的に許可します。つまり、例えば、AWS リージョン で Explorer を許可していない場合でも、リソースデータ同期で AWS Organizations オプションを選択すると、Systems Manager はそのリージョンから OpsData を自動的に収集します。詳細については、「複数のアカウントとリージョンのリソースデータ同期について」を参照してください。	2021 年 3 月 24 日
Systems Manager オートメーションがランブック向けの新しいシステム変数を提供する	新しい `global:AWS_PARTITION` システム変数を使用して、ランブックの作成時にリソースが配置される AWS パーティションを指定できます。詳細については、オートメーションシステム変数を参照してください。	2021 年 3 月 18 日

Change Manager の変更リクエストに対して複数のレベルの承認を許可	Change Manager 変更テンプレートを作成するとき、複数のレベルの承認者に対して変更リクエストを実行するためのアクセス許可を付与するよう要求できるようになりました。例えば、まずテクニカルレビューワーに変更テンプレートから作成された変更リクエストを承認してもらってから、1 人以上のマネージャに第 2 レベルの承認を求めます。詳細については、「変更テンプレートの作成」を参照してください。	2021 年 3 月 4 日
Patch Manager で Oracle Linux 8.x がサポートされるようになりました	Patch Manager を使用して、バージョン 8.3 で Oracle Linux 8.x インスタンスにパッチを適用できるようになりました。詳細については、以下の各トピックを参照してください。 • セキュリティに関連するパッチの選択方法 • パッチのインストール方法 • Oracle Linux でのパッチベースラインルールの動作方法	2021 年 3 月 1 日

OpsCenter は選択されたリソースの他の OpsItems を表示	問題を調査し、問題のコンテキストを示すために、特定の AWS リソースの OpsItems のリストを表示できます。リストには、各 OpsItem のステータス、重要度、およびタイトルが表示されます。リストには、各 OpsItem へのディープリンクも含まれています。詳細については、「特定のリソースのその他の OpsItems を表示」を参照してください。	2021 年 3 月 1 日
実行時のパッチ定義設定の定義	ベースラインオーバーライド機能を使用して、実行時にパッチ適用設定を定義できるようになりました。詳細については、「BaselineOverride パラメータの使用」を参照してください。	2021 年 2 月 25 日

新しい Systems Manager のドキュメントタイプ	AWS CloudFormation テンプレートを Systems Manager ドキュメントとして保存できるようになりました。CloudFormation テンプレートを Systems Manager ドキュメントとして保存すると、バージョニング、バージョンコンテンツの比較、アカウントとの共有など、Systems Manager ドキュメント機能の利点を享受できます。詳細については、「AWS Systems Manager のドキュメントとは」を参照してください。	2021 年 2 月 9 日

オプションのフックを使用したパッチインスタンス	新しい SSM ドキュメント AWS-RunPatchBaselineWithHooks には、インスタンスのパッチ適用サイクル中に 3 つのポイントで SSM ドキュメントを実行するために使用できるフックが用意されています。AWS-RunPatchBaselineWithHooks の詳細については、AWS-RunPatchBaselineWithHooks SSM ドキュメントについてを参照してください。3 つのフックすべてを使用するパッチ適用オペレーションのサンプルチュートリアルについては、「チュートリアル: アプリケーションの依存関係の更新、インスタンスへのパッチ適用、およびアプリケーション固有のヘルスチェックの実行」を参照してください。	2021 年 2 月 2 日

新しいトピック: ハードウェアフィンガープリントを使用したオンプレミスサーバーと仮想マシンの検証	SSM Agent は、コンピューティングされたフィンガープリントを使用して、サービスに登録するオンプレミスサーバー、仮想マシン、および VM の ID を確認します。フィンガープリントは不透明な文字列で、エージェントが特定の Systems Manager API に渡す Vault に保存されます。ハードウェアフィンガープリントと、マシンの検証に役立つ類似性のしきい値を設定する手順については、「ハードウェアフィンガープリントを使用したオンプレミスサーバーおよび仮想マシンの検証」を参照してください。	2021 年 1 月 25 日
新しいトピック: SSM Agent テクニカルリファレンス	SSM Agentテクニカルリファレンスのトピックには、AWS Systems Manager SSM Agent の実装とエージェントの仕組みの理解に役立つ情報がまとめられています。このトピックには、「AWS リージョン別の SSM Agent ローリング更新」という、まったく新しいセクションが含まれています。	2021 年 1 月 21 日

Windows Server 2008 での SSM Agent	2020 年 1 月 14 日現在、Microsoft による Windows Server 2008 の機能またはセキュリティ更新プログラムのサポートは終了しています。Windows Server 2008 AMIs には SSM Agent が含まれていますが、このオペレーティングシステムでは、このエージェントは更新されません。	2021 年 1 月 5 日
ターゲットの指定を必要としないメンテナンスウィンドウタスクに対するサポートを向上 (AWS CLI および API のみ)	必要でない場合、タスクでターゲットを指定しなくても、メンテナンスウィンドウタスクを作成できるようになりました (AWS CLI および API のみ)。これは、オートメーション、AWS Lambda および AWS Step Functions タスクタイプに適用されます。例えば、Automation タスクを作成し、更新するリソースが Automation ランブックパラメータで指定されている場合、タスク自体にターゲットを指定する必要がなくなります。詳細については、「メンテナンスウィンドウにタスクを割り当てる (コンソール)」および「Schedule automations with maintenance windows」(メンテナンスウィンドウでオートメーションをスケジュールする) を参照してください。	2020 年 12 月 23 日

新しいオートメーション機能	Systems Manager Automation のランブックに新しい共有プロパティが追加されました。onCancel プロパティを使用すると、ユーザーがオートメーションをキャンセルした場合にオートメーションが進むステップを指定できます。詳細については、「すべてのアクションで共有されるプロパティ」を参照してください。	2020 年 12 月 21 日
新しいトピック: IAM を使用した関連付け作業	IAM を使用して関連付けを作成するためのベストプラクティスを説明するための新しいトピックが、Systems Manager State Manager の章に追加されました。詳細については、「IAM を使用した関連付けの作業」を参照してください。	2020 年 12 月 18 日
State Manager でマルチリージョンとマルチアカウントのサポートを開始	複数のリージョンまたはアカウントを使用して、関連付けを作成または更新できるようになりました。詳細については、「関連付けの作成」を参照してください。	2020 年 12 月 15 日

新しいツール: Fleet Manager	AWS Systems Manager のツールである Fleet Manager は、AWS またはオンプレミスで実行されているサーバー群をリモートで管理するのに役立つ、統合されたユーザーインターフェイス (UI) エクスペリエンスです。Fleet Manager では、1 つのコンソールからサーバーフリート全体の正常性とパフォーマンスステータスを表示できます。個々のインスタンスからデータを収集し、コンソールから一般的なトラブルシューティングと管理タスクを実行することもできます。詳細については、「AWS Systems ManagerFleet Manager」を参照してください。	2020 年 12 月 15 日

新しいツール: Change Manager	Amazon Web Services はアプリケーションの設定やインフラストラクチャに対する運用上の変更を要求、承認、実装、レポート作成するためのエンタープライズ変更管理フレームワークである Change Manager をリリースしました。AWS Organizations を使用すると、単一の委任された管理者アカウントから、複数の AWS リージョン の複数の AWS アカウント にまたがる変更を管理できます。または、ローカルアカウントを使用して、単一の AWS アカウント の変更を管理できます。AWSリソースとオンプレミスリソースの両方に対する変更を管理する場合に Change Manager を使用します。詳細については、「AWS Systems ManagerChange Manager」を参照してください。	2020 年 12 月 15 日

新しいツール: Application Manager	Application Manager は、AWS リソースに関する問題をアプリケーションの背景に対応して調査および修正する際に役立ちます。Application Manager は、複数の AWS のサービスや Systems Manager ツールのオペレーション情報を、単一の AWS Management Consoleに集約します。詳細については、「AWS Systems ManagerApplication Manager」を参照してください。	2020 年 12 月 15 日

AWS Systems Manager は macOS の Amazon EC2 インスタンスをサポート	macOS インスタンスに対する Amazon Elastic Compute Cloud (Amazon EC2) サポートが開始されたのと並行して、Systems Manager は macOS に対して EC2 インスタンスで多くのオペレーションをサポートするようになりました。サポートされているバージョンは、macOS 10.14.x (Mojave) と 10.15.x (Catalina) です。詳細については、以下のトピックを参照してください。 • macOS 用の EC2 インスタンスでの SSM Agent のインストールの詳細については、「macOS 用の EC2 インスタンスで SSM Agent をインストール、設定する」を参照してください。 • macOS 用の EC2 インスタンスにパッチを適用する方法については、「パッチのインストール方法」、および「カスタムパッチベースラインの作成 (macOS)」を参照してください。 • macOS に対する EC2 インスタンスのサポートに関する一般的な情報については、「Amazon EC2 ユーザーガイド」の「Amazon EC2 Mac インスタンス」を参照してください。	2020 年 11 月 30 日

メンテナンスウィンドウの疑似パラメータ: {{TARGET_ID}} および {{RESOURCE_ID}} でサポートされる新しいリソースタイプ	1 つの追加のリソースタイプが、疑似パラメータ {{TARGET_ID}} および {{RESOURCE_ID}} とともに使用できるようになりました。これで、リソースタイプ AWS::RDS::DBCluster をこれらの擬似パラメータとともに使用できるようになりました。メンテナンスウィンドウの疑似パラメータの詳細については、「Using pseudo parameters when registering maintenance window tasks」を参照してください。	2020 年 11 月 27 日
AWS CLI バージョン 1.2.30.0 用の Session Manager プラグイン	新しいバージョンの AWS CLI の Session Manager プラグインがリリースされました。詳細については、「Session Manager プラグインの最新バージョンとリリース履歴」を参照してください。	2020 年 11 月 24 日
新しいトピック: SSM ドキュメントのバージョンを比較する	Systems Manager ドキュメントコンソールで、SSM ドキュメントのバージョン間のコンテンツの違いを比較できるようになりました。詳細については、「SSM ドキュメントのバージョンの比較」を参照してください。	2020 年 11 月 24 日

Systems Manager で VPC エンドポイントポリシーのサポートを開始	これで、Systems Manager の VPC インターフェイスエンドポイントのポリシーを作成できるようになりました。詳細については、「インターフェイス VPC エンドポイントポリシーの作成」を参照してください。	2020 年 11 月 18 日
新しいトピック: アイドルセッションタイムアウト値の指定	セッションが Session Manager で終了するまでユーザーを非アクティブにできる時間を指定できるようになりました。詳細については、「アイドルセッションのタイムアウト値を指定する」を参照してください。	2020 年 11 月 18 日
新しい Session Manager ログ機能	JSON 形式のセッションデータログの連続ストリームを Amazon CloudWatch Logs に送信できるようになりました。詳細については、「Amazon CloudWatch Logs を使用したセッションデータのストリーミング」を参照してください。	2020 年 11 月 18 日
新しいトピック: SSM Agent の署名を検証	今後は Linux インスタンスにある SSM Agent のインストーラーパッケージの暗号化署名を確認できます。詳細については、「SSM ドキュメントのスキーマと機能」を参照してください。	2020 年 11 月 17 日

新しいトピック: オートメーションステータスの理解	アクションとオートメーションのステータスについて説明する新しいトピックが「Systems Manager Automation」の章に追加されました。詳細については、「オートメーションステータスの理解」を参照してください。	2020 年 11 月 17 日
aws:downloadContent プラグインの新しいソースタイプ	Git と HTTP が aws:downloadContent プラグインのソースタイプとしてサポートされるようになりました。詳細については、「aws:downloadContent 」を参照してください。	2020 年 11 月 17 日
新しい Systems Manager ドキュメント (SSM ドキュメント) スキーマ機能	スキーマバージョン 2.2 以降の SSM ドキュメントでは、precondition パラメータでドキュメントの入力パラメータの参照がサポートされるようになりました。詳細については、「SSM ドキュメントのスキーマと機能」を参照してください。	2020 年 11 月 17 日

Explorer の新しいデータソース: AWS Config	Explorerでは、AWS Config の準拠ルールと非準拠ルールの全体的なサマリー、準拠リソースと非準拠リソースの数、各リソースに関する具体的な詳細 (非準拠ルールまたはリソースにドリルダウンした場合) など、AWS Config コンプライアンスに関する情報が表示されるようになりました。詳細については、「Systems Manager Explorer のデータソースを編集する」を参照してください。	2020 年 11 月 11 日
新しいトピック: 関連付けを使用して Auto Scaling グループを実行する	Auto Scaling グループを実行するための関連付けを作成するためのベストプラクティスを説明する新しいセクションが State Manager に追加されました。詳細については、「Auto Scaling グループを関連付けで実行する」を参照してください。	2020 年 11 月 10 日
Quick Setup でリソースグループのターゲット設定がサポートされるようになりました	Quick Setup で、ローカルセットアップタイプのターゲットとしてリソースグループの選択がサポートされるようになりました。詳細は、「Quick Setup のターゲットの選択」を参照してください。	2020 年 11 月 5 日

Patch Manager で Debian Server 10 LTS、Oracle Linux 7.9 LTS、および Ubuntu Server 20.10 STR のサポートが追加されました	これで、Debian Server 10 LTS、Oracle Linux 7.9 LTS、および Ubuntu Server 20.10 STR インスタンスにパッチを適用する Patch Manager を使用できます。詳細については、以下の各トピックを参照してください。 • Patch Manager の前提条件 • セキュリティに関連するパッチの選択方法 • パッチのインストール方法 • Debian Server でのパッチベースラインルールの動作方法 • Oracle Linux でのパッチベースラインルールの動作方法 • Ubuntu Server でのパッチベースラインルールの動作方法	2020 年 11 月 4 日

AWS Systems ManagerChange Calendar に対する新しい EventBridge サポート	Amazon EventBridge では、イベントルールで Change Calendar イベントがサポートされるようになりました。カレンダーの状態に変更があると、EventBridge は、EventBridge ルールを定義したターゲットアクションを開始できます。EventBridge イベントおよび Systems Manager イベントの使用については、次のトピックを参照してください。 • Systems Manager イベント用の EventBridge を設定する • リファレンス: Systems Manager 用の Amazon EventBridge イベントパターンとタイプ	2020 年 11 月 4 日
アラームから OpsItems を作成するように CloudWatch を設定	アラームが ALARM 状態になったときに、Systems Manager OpsCenter で OpsItem が自動的に作成されるように Amazon CloudWatch を設定できます。こうすることで、単一のコンソールを使用しながら、AWS リソースでの問題の診断と修復を素早く実施できるようになります。詳細については、「アラームから OpsItems を作成するための CloudWatch の設定」を参照してください。	2020 年 11 月 4 日

Ubuntu Server 20.10 のサポート	AWS Systems Manager が Ubuntu Server 20.10 短期リリース (STR) をサポートするようになりました。詳細については、以下の各トピックを参照してください。 • サポートされるオペレーティングシステム • ハイブリッド環境に SSM Agent をインストールする (Linux) • Ubuntu Server インスタンスに SSM Agent を手動でインストールする • SSM Agent ステータスの確認とエージェントの起動	2020 年 10 月 22 日
新しいトピック: 設定可能なシェルプロファイルを有効にする	Session Manager で設定可能なシェルプロファイルを有効にできるようになりました。設定可能なシェルプロファイルを許可すると、セッション開始時に、シェルの設定、環境変数、作業ディレクトリ、複数のコマンドの実行など、セッション内の設定をカスタマイズできます。詳細については、「設定可能なシェルプロファイルを許可する」を参照してください。	2020 年 10 月 21 日

パッチコンプライアンスの結果により、どの CVE がどのパッチによって解決されるかが報告されるようになりました	サポート対象のほとんどの Linux システムでは、管理対象インスタンスのパッチコンプライアンスの結果を表示するときに、どの共通脆弱性識別子 (CVE) の速報問題がどのパッチで解決されるかを詳しく表示できるようになりました。この情報は、不足または失敗したパッチのインストールを緊急に行う必要があるかどうかを判断するために役立ちます。詳細については、「パッチコンプライアンスの結果の表示」を参照してください。	2020 年 10 月 20 日

Linux パッチメタデータのサポートの拡張	利用可能な Linux パッチに関する多くの詳細を Patch Manager で表示できるようになりました アーキテクチャ、エポック、バージョン、CVE ID、アドバイザリ ID、Bugzilla ID、リポジトリなどのパッチデータを表示することができます。さらに、DescribeAvailablePatches API オペレーションが更新され、Linux オペレーティングシステムをサポートし、これらの新たに利用可能なパッチメタデータタイプに従ってフィルタリングできるようになりました。詳細については、以下の各トピックを参照してください。 • 利用可能なパッチの表示 • AWS Systems Manager API リファレンス の「DescribeAvailablePatches」および「パッチ」 • 「AWS CLI コマンドリファレンスの AWS Systems Manager セクション」内、「describe-available-patches」	2020 年 10 月 16 日

AWS CLI バージョン 1.2.7.0 用のSession Manager プラグイン	新しいバージョンの AWS CLI の Session Manager プラグインがリリースされました。詳細については、「Session Manager プラグインの最新バージョンとリリース履歴」を参照してください。	2020 年 10 月 15 日
新しいトピック: セッションドキュメントスキーマ	新しいトピック「セッションドキュメントスキーマ」では、セッションドキュメントのスキーマ要素について説明します。この情報は、Session Manager で使用するセッションの種類に関する設定を指定するカスタムセッションドキュメントの作成に役立ちます。	2020 年 10 月 15 日
新しいトピック: SSM ドキュメントのフリーテキスト検索	Systems Manager ドキュメント ページの検索ボックスで、フリーテキスト検索がサポートされるようになりました。フリーテキスト検索では、入力した検索語を各 SSM ドキュメントのドキュメント名と比較します。詳細については、「フリーテキスト検索の使用」を参照してください。	2020 年 10 月 15 日

新しいトピック: Amazon EC2 マネージドインスタンスの可用性のトラブルシューティング	新しいトピック「Amazon EC2 マネージドインスタンスの可用性のトラブルシューティング」では、実行が確認された Amazon EC2 インスタンスが Systems Manager の利用可能なマネージドインスタンスのリストにない理由を調査できます。	2020 年 10 月 6 日
Parameter Store の章の再編成	必要な情報をより効率的に見つけられるようにするために、AWS Systems Manager ユーザーガイドの「Parameter Store」の章でコンテンツが再編成されました。ほとんどのコンテンツは、「設定」 Parameter Storeと「Parameter Store の操作」セクションにまとめられています 。さらに、トピック「AWS Systems ManagerParameter Store」が拡張され、次のセクションを含むようになりました。 • Parameter Store はどのように組織にとってメリットになりますか? • Parameter Store はどのようなユーザーに適していますか? • Parameter Store の特徴は何ですか? • パラメータとは何ですか?	2020 年 10 月 1 日

新しいパッチコンプライアンス関連トピック	パッチコンプライアンス違反のマネージドインスタンスを特定し、さまざまなタイプのパッチコンプライアンススキャンを理解して、インスタンスをコンプライアンスに適合するための適切な手順を実行するのに役立つよう、以下のトピックが追加されました。 • 非準拠インスタンスの特定 • 非準拠インスタンスへのパッチ適用 • パッチコンプライアンス結果の表示	2020 年 9 月 24 日
SSM Agent バージョン 3.0	Systems Manager は、SSM Agent の新しいバージョンをローンチしました。	2020 年 9 月 21 日

新しいトピックと更新されたトピック: イベント管理用の CloudWatch Events に代わる Amazon EventBridge	CloudWatch Events と EventBridge の基盤となるサービスと API は同じですが、EventBridge はより多くの機能を提供し、 でイベントを管理するために推奨される方法ですAWS (CloudWatch または EventBridge のいずれかで行った変更は、各コンソールに反映されます)。AWS Systems Manager ユーザーガイド全体の CloudWatch Events および既存の手順への参照箇所が更新され、EventBridge がサポートされるようになったことが反映されました。さらに、以下の新しいトピックが追加されました。 • Systems Manager のイベントをモニタリングする • Systems Manager イベント用の EventBridge を設定する • Systems Manager のターゲットタイプの例 • リファレンス: Systems Manager 用の Amazon EventBridge イベントパターンとタイプ	2020 年 9 月 18 日

AWS Security Hub と Patch Manager の統合	Patch Manager を AWS Security Hub に統合できるようになりました。Security Hub では、AWS のセキュリティ状態を包括的に把握し、セキュリティ業界標準およびベストプラクティスに照らして環境をチェックするのに役立ちます。Patch Manager と統合されている場合、Security Hub はセキュリティの観点からフリートのパッチ適用ステータスをモニタリングします。詳細については、「Patch Manager および AWS Security Hub との統合」を参照してください。	2020 年 9 月 17 日

メンテナンスウィンドウの疑似パラメータ: {{TARGET_ID}} および {{RESOURCE_ID}} でサポートされる新しいリソースタイプ	メンテナンスウィンドウタスクを登録するときに、--task-invocation-parameters オプションを使用して、4 つのタスクタイプのそれぞれに固有のパラメータを指定します。{{TARGET_ID}} や {{RESOURCE_ID}} などの擬似パラメータ構文を使用して、特定の値を参照することもできます。メンテナンスウィンドウタスクが実行されると、擬似パラメータプレースホルダーの代わりに正しい値を渡します。2 つの追加のリソースタイプが、疑似パラメータ {{TARGET_ID}} および {{RESOURCE_ID}} とともに使用できるようになりました。これで、リソースタイプ AWS::RDS::DBInstance と AWS::SSM::ManagedInstance をこれらの擬似パラメータとともに使用できるようになりました。メンテナンスウィンドウの疑似パラメータの詳細については、「Using pseudo parameters when registering maintenance window tasks」を参照してください。	2020 年 9 月 14 日

新しい [今すぐパッチ適用] オプションによりオンデマンドでインスタンスにパッチを適用	Systems Manager コンソールを使用して、いつでもインスタンスにパッチを適用したり、不足しているパッチをスキャンしたりできるようになりました。スケジュールを作成または変更することなく、すぐにパッチを適用する必要に対応するために完全なパッチ適用設定オプションを指定することもできます。パッチをスキャンするかインストールするかを指定し、操作の対象インスタンスを特定するだけです。Patch Manager は、インスタンスタイプの現在のデフォルトのパッチベースラインを自動的に適用し、一度にパッチが適用されるインスタンスの数、および操作が失敗する前に許可されるエラーの数に関するベストプラクティスオプションを適用します。詳細については、「オンデマンドでのインスタンスへのパッチ適用」を参照してください。	2020 年 9 月 9 日

新しいトピック: SSM Agent ステータスの確認とエージェントの起動	新しいトピック「SSM Agent ステータスの確認とエージェントの起動」には、SSM Agent がサポートする各オペレーティングシステムで実行されているかどうかを確認するコマンドが用意されています。また、エージェントが実行中でない場合にエージェントを起動するためのコマンドも用意されています。	2020 年 9 月 7 日
Patch Manager で Ubuntu Server 20.04 LTS がサポートされるようになりました	Patch Manager を使用して Ubuntu Server 20.04 LTS インスタンスにパッチを適用できるようになりました。詳細については、以下の各トピックを参照してください。 • セキュリティに関連するパッチの選択方法 • パッチのインストール方法 • Ubuntu Server でのパッチベースラインルールの動作方法	2020 年 8 月 31 日
ユースケースとベストプラクティスの新しいトピック	ユーザーが Maintenance Windows と State Manager の違いをすばやく理解できるように、新しいトピックを追加しました。詳細については、「State Manager または Maintenance Windows の選択」を参照してください。	2020 年 8 月 28 日

OpsCenter の新機能	OpsCenter には、Automation ランブックをすばやく見つけて実行し、問題を修復するための新機能が含まれています。詳細については、「OpsCenter の Automation ランブックの機能」を参照してください。	2020 年 8 月 19 日
Explorer の新しいデータソース: AWS サポート ケース	Explorer は サポート ケースに関する情報を表示するようになりました。エンタープライズアカウントまたはビジネスアカウントが サポート で設定されている必要があります。詳細については、「Systems Manager Explorer のデータソースを編集する」を参照してください。	2020 年 8 月 13 日
Distributor で Trend Micro のサードパーティーパッケージが提供されるようになりました。	Distributor に Trend Micro のサードパーティー製パッケージが含まれるようになりました。Distributor を使用して、マネージドインスタンスに Trend Micro Cloud One エージェントをインストールできます。Trend Micro Cloud One は、クラウド内のワークロードをセキュリティで保護するのに役立ちます。詳細については、「AWSDistributor」を参照してください。	2020 年 8 月 12 日

aws:configurePackage ドキュメントプラグインに additionalArguments パラメータが含まれるようになりました。	Systems Manager コマンドドキュメントプラグイン aws:configurePackage は、新しい additionalArguments パラメータを使用して、スクリプトへの追加パラメータ (インストール、アンインストール、更新) を提供できるようになりました。詳細については、「aws:configurePackage 」のトピックを参照してください。	2020 年 8 月 11 日
AppConfig の内容を別個のユーザーガイドに移動	AWS AppConfig に関する情報は、別のユーザーガイドに移動されました。詳細については、「AWSAppConfig とは」を参照してください。AppConfig では、ユーザーガイド、AppConfig API リファレンス、および新しい AppConfig ワークショップへのリンクを含む、個別のドキュメントランディングページも用意しています。	2020 年 8 月 3 日

Quick Setup で AWS Organizations がサポートされるようになりました	Quick Setup では、AWS Organizations がサポートされるようになりました。これにより、複数のアカウントとリージョン間で必要なセキュリティロールと一般的に使用される Systems Manager ツールをすばやく設定できます。詳細については、「AWS Systems ManagerQuick Setup」を参照してください。	2020 年 7 月 23 日
Explorer の新しいデータソース: 関連付けのコンプライアンス	Explorer では、State Manager から関連付けのコンプライアンスデータが表示されるようになりました。詳細については、「Systems Manager Explorer のデータソースを編集する」を参照してください。	2020 年 7 月 23 日

Kernel Live Patchingを有効および無効にするための新しいSystems Manager コマンドドキュメント	Amazon Linux 2 インスタンスで Kernel Live Patching を有効または無効にするときに、Run Command でドキュメント `AWS-ConfigureKernelLivePatching` を使用できるようになりました。このドキュメントにより、これらのタスクのために独自のカスタムコマンドドキュメントを作成する必要性がなくなります。詳細については、「Amazon EC2 インスタンスでのカーネルライブパッチの使用」を参照してください。	2020 年 7 月 22 日
更新済みの自動化クォータ	レート制御の自動化の個別のキューを含め、自動化のサービスクォータが更新されました。詳細については、「AWS Systems Manager オートメーション」を参照してください。	2020 年 7 月 20 日

コンソールを使用せずにメンテナンスウィンドウのスケジュールオフセット日数を指定する	Systems Manager コンソールを使用して、CRON 式で指定された日時からメンテナンスウィンドウを実行するまでに待機する日数を指定できるようになりました。(以前は、このオプションは AWS SDK またはコマンドラインツールを使用する場合にのみ使用できました)。例えば、毎月第 3 火曜日の午後 11:30 にメンテナンスウィンドウを実行するように CRON 式でスケジュールされている場合 (`cron(0 30 23 ? * TUE#3 *)`) に、スケジュールオフセットを 2 に指定した場合、このウィンドウは 2 日後の午後 11:30 まで実行されません。詳細については、「Systems Manager の cron 式または rate 式」および「メンテナンスウィンドウのスケジュールオフセット日数を指定する」を参照してください。	2020 年 7 月 17 日
Run Command を使用して PowerShell を更新する	Windows Server 2012 および 2012 R2 インスタンスで PowerShell をバージョン 5.1 にアップデートできるように、AWS Systems Manager ユーザーガイドにチュートリアルを追加しました。詳細については、「Run Command を使用して PowerShell を更新する」を参照してください。	2020 年 6 月 30 日

Patch Manager が CentOS 8.0 および 8.1 をサポートするようになりました	Patch Manager を使用して CentOS 8.0 および 8.1 インスタンスにパッチを適用できるようになりました。詳細については、以下のトピックを参照してください。 • セキュリティに関連するパッチの選択方法 • パッチのインストール方法 • CentOS でのパッチベースラインルールの動作方法 • CentOS インスタンスに SSM Agent を手動でインストールする • ハイブリッド Linux ノードで SSM Agent をインストールする方法	2020 年 6 月 27 日

AppConfig と AWS CodePipeline の統合	AppConfig は AWS CodePipeline (CodePipeline) の統合デプロイアクションです。CodePipeline はフルマネージド型の継続的デリバリーサービスで、アプリケーションとインフラストラクチャの更新を迅速かつ高い信頼性で行うために、パイプラインのリリースを自動化します。CodePipeline はお客様が定義したリリースモデルに基づき、コードチェンジがあった場合のフェーズの構築、テスト、およびデプロイを自動化します。AppConfig と CodePipeline の統合には次のような利点があります。詳細については、「CodePipeline との AppConfig の統合」を参照してください。 • オーケストレーションを管理するために CodePipeline を使用するお客様は、コードベース全体をデプロイすることなく、アプリケーションに設定変更をデプロイする軽量な手段が利用できるようになりました。 • AppConfig を使用して設定のデプロイを管理したいが、AppConfig が現在のコードまたは設定ストアをサポートしていないために制限されているお客	2020 年 6 月 25 日

	様には、オプションが追加されました。CodePipeline は AWS CodeCommit、GitHub、BitBucket などをサポートしています。	
新しい章: 製品とサービスの統合	Systems Manager が AWS のサービスおよびその他の製品およびサービスとどのように統合されるかを理解するために、AWS Systems Manager ユーザーガイドに新しい章が追加されました。詳細については、「Systems Manager との製品およびサービスの統合」を参照してください。	2020 年 6 月 23 日
自動化の章の再編成	必要なものを見つけるために、AWS Systems Manager ユーザーガイドの「Automation」の章のトピックを再編成しました。例えば、Automation アクションと Automation ランブック参照が、章の最上位レベルのセクションになりました。詳細については、「AWS Systems Manager オートメーション」を参照してください。	2020 年 6 月 23 日

メンテナンスウィンドウのスケジュールオフセット日数を指定する	コマンドラインツールまたは AWS SDK を使用して、CRON 式で指定された日時からメンテナンスウィンドウを実行するまでに待機する日数を指定できるようになりました。例えば、毎月第 3 火曜日の午後 11:30 にメンテナンスウィンドウを実行するように CRON 式でスケジュールされている場合 (`cron(0 30 23 ? * TUE#3 *)`) に、スケジュールオフセットを 2 に指定した場合、このウィンドウは 2 日後の午後 11:30 まで実行されません。詳細については、「Systems Manager の cron 式または rate 式」および「メンテナンスウィンドウのスケジュールオフセット日数を指定する」を参照してください。	2020 年 6 月 19 日

Patch Manager で Amazon Linux 2 インスタンスでのカーネルライブパッチをサポート	Amazon Linux 2 のカーネルライブパッチを使用すると、実行中のアプリケーションを再起動や中断せずに、実行中の Linux カーネルにセキュリティの脆弱性や重大なバグのパッチを適用することができます。Patch Manager を使用して、この機能を有効にし、カーネルライブパッチを適用できるようになりました。詳細については、「Amazon Linux 2 インスタンスでのカーネルライブパッチの使用」を参照してください。	2020 年 6 月 16 日
Patch Manager での Oracle Linux バージョンサポートの向上	以前は、Patch Manager でバージョン 7.6 の Oracle Linux のみがサポートされていました 。「Patch Manager の前提条件」に記載されているように、バージョン 7.5 ~ 7.8 もサポート対象になりました。	2020 年 6 月 16 日

パッチ適用オペレーションで InstallOverrideList パラメータを使用するためのサンプルシナリオ	新しいトピック「InstallOverrideList パラメータを使用する場合のサンプルシナリオ」では、単一のパッチベースラインを使用しつつ、InstallOverrideList ドキュメント内で AWS-RunPatchBaseline パラメータを使用して、異なるタイプのパッチを異なるメンテナンスウィンドウスケジュールでターゲットグループに適用する方法について説明しています。	2020 年 6 月 11 日
AppConfig の定義済みデプロイ戦略	AppConfig では、定義済みのデプロイ戦略が提供されるようになりました。詳細については、「デプロイパッケージの作成」を参照してください。	2020 年 6 月 10 日

Patch Manager は Red Hat Enterprise Linux (RHEL) 7.8-8.2 をサポート	Patch Manager を使用して RHEL 7.8～8.2 インスタンスにパッチを適用できるようになりました。詳細については、以下のトピックを参照してください。 • セキュリティに関連するパッチの選択方法 • パッチのインストール方法 • RHEL でのパッチベースラインルールの動作方法 • Red Hat Enterprise Linux インスタンスに SSM Agent を手動でインストールする • ハイブリッド Linux ノードで SSM Agent をインストールする方法	2020 年 6 月 9 日

Explorer が委任された管理者をサポート	AWS Organizations とのリソースデータの同期を使用して、複数の AWS リージョン と AWS アカウント から Explorer データを集約する場合は、Explorer の委任管理者を設定することをお勧めします。委任管理者は、マルチアカウントおよびリージョンのリソースデータの同期を作成または削除できる Explorer の管理者の数を 1 人だけに制限することで、Explorer のセキュリティを強化します。また、Explorer でリソースデータ同期を管理するために、AWS Organizations 管理アカウントにログインする必要がなくなりました。詳細については、「委任管理者の設定」を参照してください。	2020 年 6 月 3 日
次に指定された Cron の間隔でのみ State Manager の関連付けを適用する	作成直後に State Manager 関連付けを実行しない場合は、Systems Manager コンソールで [Apply association only at the next specified Cron interval (次に指定した Cron 間隔でのみ関連付けを適用する)] オプションを選択できます。詳細については、「関連付けの作成」を参照してください。	2020 年 6 月 3 日

Explorer の新しいデータソース: AWS Compute Optimizer	Explorer で AWS Compute Optimizer からのデータが表示されるようになりました。これには、アンダープロビジョニングおよびオーバープロビジョニングされた EC2 インスタンスの数、最適化の結果、オンデマンド料金の詳細、インスタンスタイプと価格の推奨事項が含まれます。詳細については、「関連サービスの設定」で AWS Compute Optimizer のセットアップに関するトピックを参照してください。	2020 年 5 月 26 日
Patch Manager を使用して Windows サービスパックと Linux マイナーバージョンのアップグレードをインストールする	新しいトピック「チュートリアル: Windows サービスパックをインストールするためのパッチベースラインを作成する (コンソール)」では、Windows サービスパックのインストール専用のパッチベースラインを作成する方法を示します。「カスタムパッチベースラインの作成 (Linux)」トピックが更新され、Linux オペレーティングシステムのマイナーバージョンアップグレードをパッチベースラインに含めることができるようになりました。	2020 年 5 月 21 日

Parameter Store の章の再編成	Parameter Store オペレーションのオプションの構成または設定に関するすべてのトピックが、「Parameter Store のセットアップ」セクションに統合されました。ここでは、「パラメータ層の管理」と「Parameter Store スループットの向上」のトピックについて説明します。これらのトピックは、章の他の部分から再配置されています。	2020 年 5 月 18 日
Systems Manager API オペレーション用に日付と時刻の文字列を作成するための新しいトピック。	新しいトピック「Systems Manager の書式設定された日付と時刻の文字列を作成する」では、Systems Manager API オペレーションを操作するための書式設定された日付と時刻の文字列を作成する方法について説明します。	2020 年 5 月 13 日
SecureString パラメータを暗号化するためのアクセス許可について	新しいトピック「IAM ポリシーを使用して Systems Manager パラメータへのアクセスを制限する」では、AWS KMS key を使用して `SecureString` パラメータを暗号化することと、AWS によって提供される AWS マネージドキー を使用することの違いについて説明します。	2020 年 5 月 13 日

Patch Manager で、Debian Server および Oracle Linux 7.6 オペレーティングシステムがサポートされるようになりました	Patch Manager を使用して、Debian Server および Oracle Linux インスタンスにパッチを適用できるようになりました。Patch Manager では、Debian Server 8.x および 9.x および Oracle Linux 7.6 バージョンのパッチ適用がサポートされています。詳細については、以下の各トピックを参照してください。 • セキュリティに関連するパッチの選択方法 • パッチのインストール方法 • Debian Server でのパッチベースラインルールの動作方法 • Oracle Linux でのパッチベースラインルールの動作方法	2020 年 5 月 7 日
AWS Resource Groups をターゲットにした State Manager の関連付けを作成する	AWS アカウント のタグ、個々のインスタンス、すべてのインスタンスをターゲットにすることに加えて、AWS Resource Groups のインスタンスをターゲットにする State Manager 関連付けを作成できるようになりました。詳細については、「State Manager 関連付けのターゲットとレート制御について」を参照してください。	2020 年 5 月 7 日

AMI ID を検証するための Parameter Store の新しい aws:ec2:image データタイプ	String パラメータを作成するときに、データ型を aws:ec2:image として指定して、入力するパラメータ値が有効な Amazon Machine Image (AMI) ID 形式に確実になるようにできます。AMI ID 形式のサポートにより、プロセスで使用する AMI が変更されるたびに、すべてのスクリプトとテンプレートを新しい ID で更新する必要がなくなりました。データ型 aws:ec2:image のパラメータを作成し、その値として、AMI の ID を入力できます。この AMI が新しいインスタンスの作成元になります。このパラメータをテンプレート、コマンドで参照します。別の AMI を使用する準備ができたら、パラメータ値を更新します。 Parameter Store によって新しい AMI ID が検証されます。手動でスクリプトとテンプレートを更新する必要はありません。詳細については、「Amazon Machine Image ID のネイティブパラメータサポート」を参照してください。	2020 年 5 月 5 日

Run Command コマンドでの終了コードの管理	Run Command を使用して、スクリプトで終了コードを処理する方法を定義できます。デフォルトでは、スクリプトで最後に実行されたコマンドの終了コードは、スクリプト全体の終了コードとしてレポートされます。ただし、シェルの条件ステートメントを含めて以下の方法で、最後のコマンドが失敗する前にいずれかのコマンドが失敗した場合にスクリプトを終了させることができます。例については、新しいトピック「Run Command コマンドでの終了コードの管理」を参照してください。	2020 年 5 月 5 日
アベイラビリティーゾーンとローカルゾーン用にリリースされた新しいパブリックパラメータ	AWS のアベイラビリティーゾーンとローカルゾーンに関する情報をプログラムで利用できるようにするパブリックパラメータがリリースされました。これらは、AWS のサービスおよび AWS リージョンの既存のグローバルインフラストラクチャパブリックパラメータに追加されます。詳細については、「AWS のサービス、リージョン、エンドポイント、アベイラビリティーゾーン、Local Zones、Wavelength ゾーンのパブリックパラメータの呼び出し」を参照してください。	2020 年 5 月 4 日

Explorer の新しいデータソース: AWS Trusted Advisor	Explorer で AWS Trusted Advisor からのデータが表示されるようになりました。このデータには、コストの最適化、セキュリティ、耐障害性、パフォーマンス、およびサービスクォータについて、ベストプラクティスチェックのステータスとレコメンデーションが含まれます。詳細については、「関連サービスの設定」で Trusted Advisor のセットアップに関するトピックを参照してください。	2020 年 5 月 4 日

Chef recipe を実行する State Manager の関連付けを作成する	AWS-ApplyChefRecipes ドキュメントを使用して、Chef のクックブックと recipe を実行する State Manager の関連付けを作成できます。このドキュメントには、Chef recipe の実行に関して次の利点があります。 • Chef の複数のリリース (Chef 11 から Chef 14) をサポートします。 • ターゲットインスタンスに Chef クライアントソフトウェアを自動的にインストールします。 • オプションで、ターゲットインスタンスで Systems Manager コンプライアンスチェックを実行し、コンプライアンスチェックの結果を S3 バケットに保存します。 • ドキュメントの 1 回の実行で複数のクックブックと recipe を実行します。 • オプションで、recipe を why-run モードで実行し、変更を加えずにターゲットインスタンスでどの recipe が変更されるかを示します。 • オプションで、カスタム JSON 属性を chef-client 実行に適用します。	2020 年 3 月 19 日

	詳細については、「Creating associations that run Chef recipes」を参照してください。	
複数の AWS アカウント のインベントリデータを中央の Amazon S3 バケットに同期する	複数の AWS アカウント の Systems Manager インベントリデータを中央 S3 バケットに同期できます。アカウントは で定義する必要がありますAWS Organizations 詳細については、AWS Organizations で定義された複数のアカウントのインベントリリソースデータ同期の作成を参照してください。	2020 年 3 月 16 日
Amazon S3 で AppConfig の設定を保存	以前は、AppConfig では、Systems Manager (SSM) ドキュメントまたは Parameter Store パラメータに保存されたアプリケーション設定のみがサポートされていました。これらのオプションに加えて、AppConfig では、Amazon S3 での設定の保存がサポートされるようになりました。詳細については、「Amazon S3 に保存される設定について」を参照してください。	2020 年 3 月 13 日

Amazon ECS 最適化 AMIs にデフォルトで SSM Agent をインストール	SSM Agent が Amazon ECS 最適化 AMIs にデフォルトでインストールされるようになりました。詳細については、「SSM Agent の使用」を参照してください。	2020 年 2 月 25 日
コンソールでの AppConfig 設定の作成	AppConfig では、設定プロファイルの作成時に、コンソールでアプリケーション設定を作成できるようになりました。詳細については、「設定および設定プロファイルの作成」を参照してください。	2020 年 2 月 13 日
指定した日付までにリリースされたパッチのみを自動承認する	パッチがリリースされてから、指定した日数後にパッチをインストール用に自動承認するオプションに加え、Patch Manager では、指定した日付以前にリリースされたパッチのみを自動承認する機能がサポートされるようになりました。例えば、パッチベースラインの期限日として 2020 年 7 月 7 日を指定した場合、2020 年 7 月 8 日以降にリリースされたパッチは自動的にインストールされません。詳細については、「カスタムベースラインについて」および「カスタムパッチベースラインの作成 (コンソール)」を参照してください。	2020 年 2 月 12 日

メンテナンスウィンドウタスクで {{RESOURCE_ID}} 擬似パラメータを使用する	メンテナンスウィンドウタスクを登録する場合は、タスクタイプに固有のパラメータを指定します。{{TARGET_ID}} 、{{TARGET_TYPE}} 、{{WINDOW_TARGET_ID}} などの擬似パラメータ構文を使用すると、特定の値を参照できます。メンテナンスウィンドウタスクが実行されると、擬似パラメータプレースホルダーの代わりに正しい値を渡します。リソースグループの一部であるリソースをターゲットとしてサポートするには、{{RESOURCE_ID}} 擬似パラメータを使用して、DynamoDB テーブル、S3 バケット、その他のサポートされているタイプのリソースの値を渡すことができます。詳細については、「チュートリアル: メンテナンスウィンドウを作成および設定するには (AWS CLI)」の次のトピックを参照してください。 • メンテナンスウィンドウタスクの登録時の疑似パラメータの使用 • 例: メンテナンスウィンドウにタスクを登録する	2020 年 2 月 6 日

コマンドをすばやく再実行する	Systems Manager には、AWS Systems Manager コンソールの [Run Command] ページからコマンドを再実行するのに役立つオプションが 2 つあります。Rerun (再実行): このボタンを使用すると、変更を加えずに同じコマンドを実行できます。Copy to new (新規にコピー): このボタンをクリックすると、1 つのコマンドの設定が新しいコマンドにコピーされ、実行前にこれらの設定を編集できます。詳細については、「コマンドを再実行する」を参照してください。	2020 年 2 月 5 日

アドバンストインスタンス層から標準インスタンス層に戻す	以前にハイブリッド環境で実行されているすべてのオンプレミスインスタンスでアドバンストインスタンス層を使用するように設定している場合は、これらのインスタンスで標準インスタンス層を使用するようにすばやく設定できるようになりました。標準インスタンス層に戻すプロセスは、AWS アカウント および単一 AWS リージョン 内のすべてのハイブリッドインスタンスに適用されます。標準インスタンス層に戻すと、一部の Systems Manager ツールの可用性が影響を受けます。詳細については、「アドバンストインスタンス層から標準インスタンス層に戻す」を参照してください。	2020 年 1 月 16 日

パッチのインストール後にインスタンスの再起動をスキップする新しいオプション	以前は、Patch Manager でマネージドインスタンスにパッチをインストールした後で、マネージドインスタンスを必ず再起動していました。SSM ドキュメント `AWS-RunPatchBaseline` の新しい `RebootOption` パラメータを使用すると、新しいパッチのインストール後にインスタンスを自動的に再起動するかどうかを指定できます。詳細については、「SSM ドキュメント AWS-RunPatchBaseline について」トピックの「パラメータ名: RebootOption」を参照してください。	2020 年 1 月 15 日
新しいトピック:「Linux インスタンスでの PowerShell スクリプトの実行」	Run Command を使用して Linux インスタンスで PowerShell スクリプトを実行する方法を説明する新しいトピック。詳細については、「Linux インスタンスでの PowerShell スクリプトの実行」を参照してください。	2020 年 1 月 10 日

「プロキシを使用するように SSM Agent を設定する」を更新	プロキシを使用するように SSM Agent を設定するときに指定する値が更新され、HTTP プロキシサーバーと HTTPS プロキシサーバーの両方のオプションが含まれるようになりました。詳細については、「プロキシを使用するように SSM Agent を設定する」を参照してください。	2020 年 1 月 9 日

新しい「セキュリティ」の章では、Systems Manager リソースを保護するためのプラクティスを概説しています	AWS Systems Manager ユーザーガイドの新しい「セキュリティ」の章では、Systems Manager を使用する際に責任共有モデルを適用する方法を確認することができます。本章のトピックでは、セキュリティおよびコンプライアンス目標を達成するために Systems Manager を設定する方法を説明しています。また、Systems Manager リソースのモニタリングや保護に役立つ他の AWS のサービスの使用方法についても説明します。 **Note** この更新の一環として、ユーザーガイドの章「認証とアクセス制御」が、新しくより簡素なセクション「AWS Systems Manager の Identity and Access Management」に置き換えられました。	2019 年 12 月 24 日

新しいサンプルカスタム Automation ランブック	サンプルカスタム Automation ランブックがユーザーガイドに追加されました。これらのサンプルは、さまざまな Automation アクションを使用して、デプロイ、トラブルシューティング、およびメンテナンスのタスクを簡素化する方法を説明しており、独自のカスタム Automation ランブックを作成できるように支援することを目的としています。詳細については、「カスタムの Automation ランブックサンプル」を参照してください。Systems Manager コンソールで Amazon マネージド Automation ランブックのコンテンツを表示することもできます。詳細については、Systems Manager Automation ランブックリファレンスを参照してください。	2019 年 12 月 23 日

Oracle Linux のサポート	Systems Manager で、Oracle Linux 7.5 および 7.7 がサポートされるようになりました。Oracle Linux インスタンス用の EC2 インスタンスに SSM Agent を手動でインストールする方法については、「Oracle Linux」を参照してください。ハイブリッド環境内の Oracle Linux サーバーへの SSM Agent のインストールについては、「ハイブリッド Linux ノードで SSM Agent をインストールする方法」を参照してください。	2019 年 12 月 19 日

Amazon EC2 コンソールからの Session Manager セッションの起動	Amazon Elastic Compute Cloud (Amazon EC2) コンソールから Session Manager セッションを開始できるようになりました。Amazon EC2 コンソールからセッション関連のタスクを操作するには、ユーザーと管理者の両方に異なる IAM アクセス許可が必要です。Session Manager コンソールと AWS CLI のみを使用するアクセス許可、Amazon EC2 コンソールのみを使用するアクセス許可、または 3 つのツールすべてを使用するアクセス許可を指定できます。詳細については、以下のトピックを参照してください。 • クイックスタート Session Manager のデフォルト IAM ポリシー • セッションを開始する (Amazon EC2 コンソール)	2019 年 12 月 18 日

CloudWatch の Run Command メトリクスとアラームのサポート	AWS Systems Manager は、Run Command コマンドのステータスに関するメトリクスを CloudWatch に公開するようになりました。これにより、このようなメトリクスに基づいてアラームを設定できます。コマンドの端末ステータス値で、メトリクスを追跡できるものには `Success`、`Failed`、および `Delivery Timed Out` があります。詳細については、「Amazon CloudWatch を使用した Run Command メトリクスのモニタリング」を参照してください。	2019 年 12 月 17 日
新しい Systems Manager ツール: Change Calendar	Systems Manager Change Calendar を使用して、リソースへのコード変更 (Systems Manager Automation ランブックや AWS Lambda 関数からのコード変更など) を制限または禁止する期間 (イベント) を指定します。変更カレンダーは、iCalendar 2.0 データをプレーンテキスト形式で格納する新しい Systems Manager ドキュメントタイプです。詳細については、「AWS Systems Manager Change Calendar」を参照してください。	2019 年 12 月 11 日

新しい Systems Manager ツール: AWSAppConfig	AppConfig を使用して、アプリケーション設定を作成、管理、迅速にデプロイします。AppConfig は、あらゆる規模のアプリケーションへの管理型デプロイをサポートします。AppConfig は、EC2 インスタンス、AWS Lambda、コンテナ、モバイルアプリケーション、または IoT デバイスでホストされているアプリケーションで使用できます。アプリケーション設定のデプロイ時のエラーを防ぐため、AppConfig にはバリデータが含まれています。バリデータは構文チェックまたはセマンティックチェックを実施して、デプロイする設定が意図したとおりに動作することを確認します。設定のデプロイ中、AppConfig はアプリケーションをモニタリングしてデプロイが正常に実施されたことを確認します。システムでエラーが発生した場合、またはデプロイによってアラームが起動した場合、AppConfig は変更をロールバックして、アプリケーションユーザーへの影響を最小限に抑えます。詳細については、「AWSAppConfig」を参照してください。	2019 年 11 月 25 日

Systems Manager の新ツール: Systems Manager Explorer	AWS Systems Manager Explorer は、AWS リソースに関する情報の報告に使用するカスタマイズ可能なオペレーションダッシュボードです。Explorer には、AWS アカウント および AWS リージョン全体のオペレーションデータ (OpsData) の集約的なビューが表示されます。Explorer では、OpsData に EC2 インスタンス、パッチコンプライアンスの詳細、および運用作業項目 (OpsItems) に関するメタデータが含まれています。Explorer では、OpsItems が事業部門またはアプリケーション全体にどのように分散されているか、それらが時間の経過とともにどのような傾向を示すか、およびカテゴリによってどのように異なるかに関するコンテキストが提供されます。Explorer で情報をグループ化およびフィルタリングすると、自身に関連する項目や、アクションが必要な項目に注目することができます。優先度の高い問題を特定したら、Systems Manager OpsCenter を使用してオートメーションランブックを実行すると、問題をすばやく解決できます。詳細については、「AWS Systems ManagerExplorer」を参照してください。	2019 年 11 月 18 日

> **Note**
>
> Systems Manager OpsCenter のセットアップは、Explorer のセットアップと統合されています。すでに OpsCenter をセットアップしている場合は、統合セットアップを完了して、設定とオプションを確認する必要があります。OpsCenter をセットアップしていない場合は、統合セットアップを使用することで両方のツールの使用を開始できます。詳細については、「Explorer および OpsCenter の開始方法」を参照してください。

パラメータ検索機能の改善	アカウントに多数のパラメータがある場合や、パラメータの正確な名前を思い出せない場合は、パラメータを検索するためのツールで簡単にパラメータを見つけることができます。検索ツールで、`contains` でフィルタリングできるようになりました。検索ツールでは以前は、パラメータ名の検索に `equals` と `begins-with` しか使用できませんでした。詳細については、「Systems Manager のパラメータを検索する」を参照してください。	2019 年 11 月 15 日

新しいコンソールベースのオートメーション用ドキュメントビルダー | 自動化ステップでのスクリプト実行のサポート	標準化した運営計画の作成と共有を Systems Manager オートメーションにより行うことで、ユーザー、AWS アカウント 、AWS リージョン での一貫性を確立できるようになりました。スクリプトを実行し、Markdown を使用して Automation ランブックにインラインドキュメントを追加するこの機能により、エラーを削減できるだけでなく、手動のステップ (例えば、Wiki 記事の検索、ターミナルでのコマンド実行) を排除できます。 詳細については、以下のトピックを参照してください。 • チュートリアル: ドキュメントビルダーを使用してカスタム Automation ランブックを作成する • aws:executeScript (オートメーションアクションのリファレンス) • ドキュメントビルダーを使用した Automation ランブックの作成 • AWS ニュースブログの「Systems Manager の新しい オートメーション機能」	2019 年 11 月 14 日

Distributor を使用してインプレースパッケージ更新を実行する	Distributor を使用してパッケージの更新をインストールする場合、従来は、パッケージ全体をアンインストールして新しいバージョンを再インストールする方法以外に選択肢はありませんでした。現在では、代替手段としてインプレース更新を選択することができます。インプレース更新中、Distributor は、パッケージに組み込まれた更新スクリプトに従って、最後のインストール以降に新たに追加または変更されたファイルのみをインストールします。このオプションを使用すると、パッケージアプリケーションを利用可能な状態に保つことができ、更新中にオフラインにすることはできません。詳細については、以下のトピックを参照してください。 • パッケージの作成 • パッケージのインストールまたは更新	2019 年 11 月 11 日

新しい SSM Agent の自動更新機能	ワンクリックで、AWS アカウント のすべてのインスタンスを設定して、新バージョンの SSM Agent を自動的にチェックしてダウンロードできます。これを行うには、AWS Systems Manager コンソールの [マネージドインスタンス] ページで [Agent auto update (エージェントの自動更新)] を選択します。詳細については、「SSM Agentへの更新の自動化」を参照してください。	2019 年 11 月 5 日
AWS が提供するタグを使用して Session Manager アクセスを制限する	セッションアクションへのユーザーアクセスを制御する 2 番目の方法が利用可能になりました。この新しい方法で、`{aws:username}` 変数を使用する代わりに AWS が提供するセッションタグを使用して IAM アクセスポリシーを作成します。AWS が提供するセッションタグを使用すると、フェデレーション ID を使用する組織がセッションへのユーザーアクセスを制御できます。詳細については、「ユーザーが開始したセッションのみを終了できるようにする」を参照してください。	2019 年 10 月 2 日

Ansible プレイブックを適用するための新しい SSM コマンドドキュメント	`AWS-ApplyAnsiblePlaybooks` ドキュメントを使用して、State Manager プレイブックを実行する Ansible の関連付けを作成できます。このドキュメントには、プレイブックを実行するための以下の利点があります。 • 複雑なプレイブックの実行のサポート • GitHub と Amazon Simple Storage Service (Amazon S3) からのプレイブックのダウンロードをサポート • 圧縮されたプレイブック構造のサポート • 高度なログ記録 • プレイブックがバンドルされているときに実行するプレイブックを指定する機能 詳細については、「Creating associations that run Ansible playbooks」を参照してください。	2019 年 9 月 24 日

Session Manager のポート転送をサポート	Session Manager はポート転送セッションをサポートするようになりました。ポート転送を使用すると、プライベートサブネットにデプロイされたインスタンス間にトンネルを安全に作成でき、サーバーで SSH サービスを開始したり、セキュリティグループで SSH ポートを開いたり、踏み台ホストを使用したりする必要はありません。SSH トンネルと同様に、ポート転送を使用すると、ラップトップ間でトラフィックを転送してインスタンスのポートを開くことができます。ポート転送を設定すると、ローカルポートに接続し、インスタンス内で実行されているサーバーアプリケーションにアクセスできます。詳細については、以下の各トピックを参照してください。 • AWS ニュースブログの AWS Systems ManagerSession Manager を使用したポート転送 • セッションの開始 (ポート転送)	2019 年 8 月 29 日

デフォルトのパラメータ階層を指定、または階層の選択を自動化する	階層を指定しないパラメータを作成または更新するリクエストに使用するデフォルトのパラメータ階層を指定できるようになりました。デフォルトの階層は、標準パラメータ、詳細パラメータ、または新しいオプション、Intelligent-Tiering に設定できます。Intelligent-Tiering は各 PutParameter リクエストを評価し、必要な場合にのみ高度なパラメータを作成します (パラメータ値のサイズが 4 KB を超える場合、パラメータポリシーがパラメータに関連付けられている場合、または標準階層でサポートされている最大 10,000 パラメータがすでに作成されている場合は、詳細パラメータが必要です)。デフォルト階層の指定と Intelligent-Tiering の使用の詳細については、「デフォルトのパラメータ階層の指定」を参照してください。	2019 年 8 月 27 日
CLI および PowerShell の手順で更新された「関連付けの使用」セクション	AWS CLI または AWS Tools for PowerShell を使用する関連付けを管理するための手順ドキュメントを含めるため、[関連付けの使用] セクションが更新されました。詳細については、「Systems Manager での関連付けの使用」を参照してください。	2019 年 8 月 26 日

CLI および PowerShell の手順で更新された「自動化実行の使用」セクション	AWS CLI または AWS Tools for PowerShell を使用する自動化ワークフローを実行するための手順ドキュメントを含めるため、[自動化実行の使用] セクションが更新されました。詳細については、「自動化実行の使用」を参照してください。	2019 年 8 月 20 日
OpsCenter と Application Insights の統合	OpsCenter は、.NET および SQL Server 用の Amazon CloudWatch Application Insights と統合されています。つまり、アプリケーションで検出された問題に対して自動的に OpsItems を作成できます。OpsItems を作成するように Application Insights を設定する方法については、Amazon CloudWatch ユーザーガイドの「モニタリング用にアプリケーションをセットアップ、構成、管理する」を参照してください。	2019 年 8 月 7 日

新しいコンソール機能: AWS Systems ManagerQuick Setup	Quick Setup は、EC2 インスタンスで複数の Systems Manager コンポーネントをすばやく設定できるようにする、Systems Manager コンソールの新機能です。具体的には、Quick Setup は、タグを使用して選択したかターゲットに指定したインスタンスで以下のコンポーネントを設定するのに役立ちます。 • Systems Manager の AWS Identity and Access Management (IAM) インスタンスプロファイルロール。 • SSM Agent のスケジュールされた隔月ごとの更新。 • 30 分ごとにスケジュールされたインベントリメタデータの収集。 • 欠落しているパッチを特定するために、インスタンスを毎日スキャン。 • Amazon CloudWatch エージェントの 1 回限りのインストールと設定。 • CloudWatch エージェントのスケジュールされた月次更新。 詳細については、「AWS Systems Manager Quick Setup」を参照してください。	2019 年 8 月 7 日

リソースグループをメンテナンスウィンドウターゲットとして登録する	メンテナンスウィンドウのターゲットとしてマネージドインスタンスを登録するだけでなく、リソースグループもメンテナンスウィンドウのターゲットとして登録できるようになりました。Maintenance Windows は、AWS Resource Groups にサポートされているすべての AWS リソースタイプ (`AWS::EC2::Instance` 、`AWS::DynamoDB::Table` 、`AWS::OpsWorks::Instance` 、`AWS::Redshift::Cluster` など) に対応します。このリリースでは、コマンドをリソースグループに送信することもできます。たとえば、Run Command コンソール、AWS CLI、または send-command コマンドを使用します。詳細については、以下の各トピックを参照してください。 • メンテナンスウィンドウにターゲットを割り当てる (コンソール) • 例: ターゲットをメンテナンスウィンドウに登録する • ターゲットとレート制御を使用してフリートにコマンドを送信する	2019 年 7 月 23 日

AWS Systems ManagerDistributor によるパッケージ作成とバージョニングの簡素化	Distributor には、パッケージマニフェスト、スクリプト、およびファイルハッシュを生成できる、新しく簡素化されたパッケージ作成ワークフローがあります。既存のパッケージにバージョンを追加する際、簡略化されたワークフローを使用することもできます。	2019 年 7 月 22 日
Systems Manager Automation の新しいドキュメントカテゴリペイン	Systems Manager には、コンソールでオートメーションを実行する場合の新しいドキュメントカテゴリペインが含まれます。このペインを使用して、目的に基づいて Automation ランブックをフィルタリングします。	2019 年 7 月 18 日
オペレーティングシステムのユーザー認証情報を使用した Session Manager セッション起動のサポート	デフォルトでは、Session Manager セッションは、マネージドインスタンスで作成されたシステム生成の `ssm-user` アカウントの認証情報を使用して起動されます。Linux マシンでは、代わりにオペレーティングシステムアカウントの認証情報を使用してセッションを起動できるようになりました。詳細については、「Linux インスタンスの Run As サポートを有効にする」を参照してください。	2019 年 7 月 9 日

SSH を使用して Session Manager セッションの起動をサポートする	AWS CLI で Session Manager を使用してマネージドインスタンスで SSH セッションを起動できるようになりました。Session Manager で SSH セッションを許可する方法については、「(オプション) SSH Session Manager セッションの有効化」を参照してください。Session Manager を使用して SSH セッションを開始する方法については、「セッションの開始 (SSH)」を参照してください。	2019 年 7 月 9 日
マネージドインスタンスのパスワード変更のサポート	Systems Manager を使用して管理するマシンのパスワードをリセットできるようになりました (マネージドインスタンス)。Systems Manager コンソールまたは AWS CLI を使用して、パスワードをリセットできます。詳細については、「マネージドインスタンスのパスワードのリセット」を参照してください。	2019 年 7 月 9 日

「AWS Systems Manager とは」の改訂	「AWS Systems Manager とは」の最初のトピックは、サービスの詳細な概要を提供し、最近リリースされた Systems Manager ツールを反映するように拡張されました。さらに、このセクションの他のコンテンツは、見つけやすいように個々のトピックに移動されました。	2019 年 6 月 10 日

新しい Systems Manager ツール: OpsCenter	OpsCenter は、オペレーションエンジニアや IT プロフェッショナルが AWS リソースに関連する運用作業項目 (OpsItems) を表示、調査、解決できる中心的な場所を提供します。OpsCenter は、AWS リソースに影響する問題の解決までの平均時間を短縮するように設計されています。Systems Manager のこのツールでは、各 OpsItem、関連 OpsItems、および関連リソースに関する状況に応じた調査データを提供しながら、サービス間で OpsItems を集約および標準化します。また、OpsCenter では、問題を迅速な解決に使用できる Systems Manager Automation ランブックも提供しています。検索可能なカスタムデータを OpsItem ごとに指定することができます。OpsItems に関する自動的に生成された概要レポートは、ステータスおよびソース別に表示することもできます。詳細については、「AWS Systems ManagerOpsCenter」を参照してください。	2019 年 6 月 6 日

中の Systems Manager の左側のナビゲーションペインへの変更AWS Management Console	AWS Management Consoleの [Systems Manager] 左側のナビゲーションペインに、OpsCenter の見出しなど、新しい見出しが追加されました。これにより、Systems Manager のツールがより論理的にグループ化されます。	2019 年 6 月 6 日

AWS CLI を使用したメンテナンスウィンドウの作成と設定に関するチュートリアルの改訂	「チュートリアル: メンテナンスウィンドウを作成および設定するには (AWS CLI)」を実際の手順をわかりやすく説明するために見直しました。1 つのメンテナンスウィンドウを作成し、1 つのターゲットを識別して、メンテナンスウィンドウで実行するシンプルなタスクを設定します。また、{{TARGET_ID}} などの疑似パラメータを使用するための情報など、独自のタスク登録コマンドを作成するために使用できる情報と例を提供しました。追加情報と例については、以下のトピックを参照してください。 • 例: ターゲットをメンテナンスウィンドウに登録する • 例: タスクをメンテナンスウィンドウに登録する • register-task-with-maintenance-windows オプションについて • メンテナンスウィンドウタスクの登録時の疑似パラメータの使用	2019 年 5 月 31 日
SSM Agent の更新に関する通知	SSM Agent の更新に関する通知を受け取るには、GitHub の「SSM Agent リリースノート」ページをサブスクライブします。	2019 年 5 月 24 日

Parameter Store の変更に基づく通知の受信やアクションの起動	トピック「Parameter Store イベントに基づき、通知の設定またはアクションのトリガーを行う」は、Parameter Store の変更に対応するための Amazon EventBridge ルールの設定に役立ちます。次のいずれかが発生すると、通知が送信されたり、他のアクションを起動したりできます。 • パラメータは作成、更新、または削除されます。 • パラメータラベルバージョンが作成、更新、または削除されます。 • パラメータが期限切れ、期限切れ間近、または指定された期間内に変更されていない。	2019 年 5 月 22 日

セットアップおよび開始方法のコンテンツに関する主な改訂点	AWS Systems Manager ユーザーガイドのセットアップと開始方法に関する内容を拡張して再編成しました。セットアップは、2 つのセクションに分かれています。一方のセクションでは、EC2 インスタンスを設定および管理するための Systems Manager のセットアップ作業に重点を置いています。もう一方のセクションでは、ハイブリッド環境でオンプレミスサーバーと仮想マシン (VM) を構成および管理するための Systems Manager のセットアップについて説明しています。どちらのセクションでも、すべてのセットアップトピックを番号付きの主なステップとして完了の推奨順に示しています。新しい開始方法の章は、アカウントとサービスの設定タスクの完了後に、エンドユーザーが Systems Manager の使用を開始しやすいように構成されています。 • AWS Systems Manager のセットアップ • ハイブリッド環境で AWS Systems Manager を設定する • AWS Systems Manager の開始方法	2019 年 5 月 15 日

Microsoft がリリースしたアプリケーションのパッチをパッチベースラインに含める (Windows)	Patch Manager は、Windows Server インスタンスで Microsoft がリリースしたアプリケーションのパッチ更新をサポートするようになりました。以前は、Windows Server オペレーティングシステムのパッチのみがサポートされていました。Patch Manager には、Windows Server インスタンス用に 2 つの定義済みパッチベースラインが用意されています。このパッチベースライン `AWS-WindowsPredefinedPatchBaseline-OS` は、オペレーティングシステムのパッチにのみ適用されます。`AWS-WindowsPredefinedPatchBaseline-OS-Applications` は、Microsoft がリリースした Windows Server オペレーティングシステムと アプリケーションの両方に Windows 上で適用されます。Microsoft がリリースしたアプリケーションのパッチを含むカスタムのパッチベースラインの作成の詳細については、「カスタムパッチベースラインの作成」の最初の手順を参照してください。また、この更新の一部である AWS が提供する事前定義されたパッチベースラインの名前を変更中です。詳細については、「事	2019 年 5 月 7 日

	前定義されたベースライン」を参照してください。	
AWS CLI を使用してメンテナンスウィンドウのターゲットを登録する例	新しいトピック「例: ターゲットをメンテナンスウィンドウに登録する」には、AWS CLI を使用するときにメンテナンスウィンドウのターゲットを指定できる様々な方法を示す 4 つのサンプルコマンドがあります。このトピックでは、各サンプルコマンドのベストなユースケースについても説明します。	2019 年 5 月 3 日

パッチグループトピックの更新	トピック「パッチグループについて」が更新され、パッチ適用オペレーションの間にマネージドインスタンスが使用する適切なバッチベースラインを決定する方法に関するセクションが含められました。さらに、AWS CLI または Systems Manager コンソールを使用して Patch Group または PatchGroup タグをマネージドインスタンスに追加する手順、および Patch Group または PatchGroup をパッチベースラインに追加する方法が追加されました。(EC2 インスタンスのメタデータでタグを許可している場合は、スペースなしで **PatchGroup** を使用する必要があります。) 詳細については、「パッチグループの作成」および「パッチベースラインにパッチグループを追加する」を参照してください。	2019 年 5 月 1 日

Parameter Store の新機能	Parameter Store は次の新機能を提供します。 • 高度なパラメータ: Parameter Store では、標準パラメータ階層 (デフォルト階層) または高度なパラメータ階層を使用するようにパラメータを個別に設定できるようになりました。アドバンストパラメータでは、パラメータ値の大きなサイズクォータ、AWS アカウント および AWS リージョン ごとに作成できるパラメータ数の多いクォータ、およびパラメータポリシーを使用する機能が提供されます。詳細パラメータの詳細については、「Systems Manager のアドバンスドパラメータについて」を参照してください。 • パラメータポリシー: パラメータポリシーを使用すると、有効期限または有効期限 (TTL) などの特定条件をパラメータに割り当てることができ、増え続けるパラメータのセットを管理できます。パラメータポリシーは、Parameter Store に保存されたパスワードと設定データを強制的に更新または削除するのに役立ちます。パラメータポリシー	2019 年 4 月 25 日

	は、高度なパラメータ階層を使用するパラメータにのみ利用できます。詳細については、「パラメータポリシーの使用」を参照してください。 • [Higher throughput] (高スループット): これで Parameter Store スループット クォータを 1 秒あたり最大 1,000 件のトランザクションに増やすことができるようになりました。詳細については、「Parameter Storeのスループットを向上する」を参照してください。	
自動化セクションの更新	自動化セクションが見つけやすさを向上するために更新されました。さらに、3 つの新しいトピックが自動化セクションに追加されました。 • オートメーションを段階的に実行する • 承認が必要なオートメーションを実行する • State Manager 関連付けでのオートメーションのスケジュール設定	2019 年 4 月 17 日

AWS KMS キーを使用してセッションデータを暗号化する	デフォルトでは、Session Manager は、TLS 1.2 を使用して、アカウント内のユーザーのローカルマシンと EC2 インスタンス間で送信されるセッションのデータを暗号化します。AWS Key Management Service で作成された AWS KMS key を使用して、そのデータをさらに暗号化することを選択できるようになりました。AWS アカウント、または他のアカウントから共有されたアカウントで作成された KMS キーを使用することができます。KSM キーを指定してセッションデータを暗号化する方法については、「セッションデータの AWS KMS キー暗号化を有効にする (コンソール)」、「Session Manager 設定 (AWS CLI) を作成する」、または「Session Manager 設定 (AWS CLI) の更新」を参照してください。	2019 年 4 月 4 日

AWS Systems Manager の Amazon SNS 通知の設定	AWS CLI または Systems Manager コンソールを使用して、メンテナンスウィンドウに登録された Run Command タスクと Run Command 用の Amazon SNS 通知を設定する手順を追加しました。詳細については、「AWS Systems Manager の Amazon SNS 通知の設定」を参照してください。	2019 年 3 月 6 日

ハイブリッド環境でのサーバーおよび VM の高度なインスタンス	AWS Systems Manager は、ハイブリッド環境のサーバーと VM 用に、スタンダードインスタンス層とアドバンストインスタンス層を提供します。スタンダードインスタンス層では、AWS リージョンリージョンごと、AWS アカウント アカウントごとに最大 1,000 のサーバーまたは VM を登録できます。1 つのアカウントとリージョンに 1,000 を超えるサーバーまたは VM を登録する必要がある場合は、アドバンストインスタンス層を使用します。アドバンストインスタンス層では、必要な分だけインスタンスを作成できますが、Systems Manager に設定されているインスタンスはすべて、従量課金制でご利用いただけます。アドバンストインスタンスでは、AWS Systems Manager Session Manager を使用してハイブリッドマシンに接続することも可能です。Session Manager では、インタラクティブシェルでインスタンスにアクセスできます。アドバンストインスタンスの有効化の詳細については、「アドバンストインスタンス層を使用する」を参照してください。	2019 年 3 月 4 日

共有 SSM ドキュメントを使用する State Manager 関連付けの作成	他の AWS アカウント から共有されている SSM コマンドおよび Automation ランブックを使用する State Manager の関連付けを作成できます 共有 SSM ドキュメントを使用して関連付けを作成すると、インスタンスが同じアカウントにない場合でも、Amazon EC2 とハイブリッドインフラストラクチャを一貫した状態に保つことができます。SSM ドキュメントの共有の詳細については、「AWS Systems Manager ドキュメント」を参照してください。State Manager 関連付けの作成の詳細については、「関連付けを作成する」を参照してください。	2019 年 2 月 28 日
Amazon EventBridge ルールでサポートされる Systems Manager イベントのリストを表示する	新しいトピック「Amazon EventBridge を使用して Systems Manager イベントをモニタリングする」では、Systems Manager によって生成されたさまざまなイベントの概要について説明します。これらのイベントに対して EventBridge でイベントのモニタリングルールを設定できます。	2019 年 2 月 25 日

Systems Manager リソースの作成時にタグを追加する	Systems Manager は、作成時に特定のリソースタイプにタグを追加する機能をサポートするようになりました。AWS CLI または SDK を使用して作成するときにタグ付けできるリソースには、メンテナンスウィンドウ、バッチベースライン、Parameter Store パラメータ、および SSM ドキュメントが含まれます。アクティベーションを作成するときに、タグをマネージドインスタンスに割り当てることもできます。Systems Manager コンソールを使用するときは、タグをメンテナンスウィンドウ、パッチベースライン、およびパラメータに追加できます。	2019 年 2 月 24 日

Systems Manager Inventory の IAM ロールを自動作成する	以前は、コンソールの [Inventory Detail View (インベントリの詳細表示)] ページにインベントリデータを表示するには、AWS Identity and Access Management (IAM) ロールを作成し、このロールに個別のポリシーをアタッチする必要がありました。このロールを作成したり、ポリシーをアタッチする必要はもうありません。[Inventory Detail View] (インベントリ詳細表示) ページでリモートデータの同期を選択すると、Systems Manager が自動的に `Amazon-GlueServicePolicyForSSM` ロールを作成し、そのロールに Amazon-GlueServicePolicyForSSM-{S3 bucket name} ポリシーおよび AWSGlueServiceRole ポリシーを割り当てます。詳細については、「複数のリージョンとアカウントからインベントリデータをクエリする」を参照してください。	2019 年 2 月 14 日

SSM Agent を更新するための Maintenance Windows チュートリアル	2 つの新しいチュートリアルを Maintenance Windows のドキュメントに追加しました。このチュートリアルでは、Systems Manager コンソールまたは AWS CLI を使用して、SSM Agent を自動的に最新の状態に保つメンテナンスウィンドウを作成する方法について詳しく説明しています。詳細については、「Maintenance Windows チュートリアル」を参照してください。	2019 年 2 月 11 日
Parameter Store パブリックパラメータの使用	Parameter Store パブリックパラメータを説明する短いセクションが追加されました。詳細については、「Systems Manager のパブリックパラメータを使用する」を参照してください。	2019 年 1 月 31 日
AWS CLI を使用した Session Manager 設定の作成	AWS CLI を使用して CloudWatch Logs や S3 バケットのログ記録オプション、セッションの暗号化設定などの Session Manager 設定を作成するための手順を追加しました。詳細については、「AWS CLI を使用して Session Manager 設定を作成する」を参照してください。	2019 年 1 月 22 日

State Manager を使用して Systems Manager のオートメーションワークフローを実行する	AWS Systems Manager State Manager は、SSM Automation ランブックを使用する関連付けの作成をサポートするようになりました。State Manager は以前、`command` および `policy` のドキュメントのみをサポートしており、マネージドインスタンスを対象とした関連付けしか作成できませんでした。SSM オートメーションランブックのサポートにより、AWS リソースのさまざまなタイプを対象とする関連付けを作成できるようになりました。詳細については、「State Manager を使用して Systems Manager Automation ワークフローを実行する」を参照してください。	2019 年 1 月 22 日

Cron 式と Rate 式およびメンテナンスウィンドウスケジュールオプションのリファレンスの更新	「Systems Manager の Cron 式および rate 式」のリファレンストピックが改訂されました。新しいバージョンではさらに多くの例が提供されており、cron 式と rate 式を使用してメンテナンスウィンドウと State Manager の関連付けをスケジューリングする方法の説明が改善されています。さらに、新しいトピック「Maintenance Windows のスケジュール設定と有効期間のオプション」では、メンテナンスウィンドウのスケジューリングに関連したさまざまなオプション (開始日、終了日、タイムゾーン、スケジュールの頻度) が他とどのように関連しているかが説明されています。	2018 年 12 月 6 日
SSM Agent デバッグログの有効化	seelog.xml.template ファイルをマネージドインスタンスで編集することに q より、SSM Agent のデバッグログ記録を有効にできます。詳細については、「SSM Agent のデバッグログを有効にする」を参照してください。	2018 年 11 月 30 日

ARM64 プロセッサアーキテクチャのサポート	AWS Systems Manager で、Amazon Linux 2、Red Hat Enterprise Linux 7.6、および Ubuntu Server (18.04 LTS および 16.04 LTS) オペレーティングシステムの ARM64 バージョンがサポートされるようになりました。詳細については、Amazon Linux 2、RHEL、およびスナップパッケージを含む Ubuntu Server 18.04 および 16.04 LTS のインストール手順を参照してください。A1 インスタンスタイプの詳細については、「Amazon EC2 ユーザーガイド」の「汎用インスタンス」を参照してください。	2018 年 11 月 26 日

AWS Systems ManagerDistributor を使用してパッケージを作成してデプロイする	AWS Systems Manager Distributor を使用して独自のソフトウェアをパッケージ化して (あるいは `AmazonCloudWatchAgent` などの AWS が提供するエージェントソフトウェアパッケージから選択して)、AWS Systems Manager マネージドインスタンスにインストールします。Distributor は、ソフトウェアパッケージなどのリソースを AWS Systems Manager マネージドインスタンス用に公開しています。パッケージを発行すると、パッケージのドキュメントの特定のバージョン – Distributor でパッケージを追加するときに作成する Systems Manager ドキュメントが、マネージドインスタンス ID、AWS アカウント ID、タグ、または AWS リージョン で識別されるマネージドインスタンスにアドバタイズされます。詳細については、「AWS Systems ManagerDistributor」を参照してください。	2018 年 11 月 20 日

中央アカウントから複数の AWS リージョン と AWS アカウント で AWS Systems Manager オートメーション ワークフローを同時に実行する	Automation アカウント管理から、複数の AWS リージョン と AWS アカウント または AWS 組織単位 (OU) にわたって AWS Systems Manager オートメーションワークフローを同時に実行できます。複数のリージョンやアカウント、または OU でオートメーションを同時に実行すると、AWS リソースの管理に必要な時間が短縮され、コンピューティング環境のセキュリティが強化されます。詳細については、「複数の AWS リージョン および AWS アカウント でのオートメーション ワークフローの実行」を参照してください。	2018 年 11 月 19 日

複数の AWS リージョン および AWS アカウント からインベントリデータをクエリする	Systems Manager Inventory は Amazon Athena と統合されているため、複数の AWS リージョン および AWS アカウント からインベントリデータをクエリするのに役立ちます。Athena 統合では、リソースデータ同期が使用されるため、AWS Systems Manager コンソールの [Inventory Detail View (Inventory 詳細表示)] ページで、すべてのマネージドインスタンスのインベントリデータを表示できます。詳細については、「複数のリージョンとアカウントからの Inventory データのクエリ」を参照してください。	2018 年 11 月 15 日

MOF ファイルを実行する State Manager の関連付けを作成する	Managed Object Format (MOF) ファイルを実行すると、AWS-ApplyDSCMofs SSM ドキュメントを使用して、State Manager によって Windows Server マネージドインスタンスで目的の状態を適用できます。AWS-ApplyDSCMofs ドキュメントには 2 つの実行モードがあります。最初のモードでは関連付けを設定して、マネージドインスタンスが現在、特定の MOF ファイルで定義されている目的の状態であるかどうかをスキャンおよびレポートできます。2 番目のモードでは MOF ファイルを実行して、MOF ファイルで定義されているリソースやその値に基づいてインスタンスの設定を変更できます。AWS-ApplyDSCMofs ドキュメントを使用すると、Amazon Simple Storage Service (Amazon S3)、ローカル共有、または HTTPS ドメインを持つ安全なウェブサイトから MOF 設定ファイルをダウンロードして実行できます。詳細については、「MOF ファイルを実行する関連付けの作成」を参照してください。	2018 年 11 月 15 日

Session Manager セッションの管理アクセスの制限	Session Manager セッションは、デフォルトルートまたは ssm-user という管理者許可を使用して作成されたユーザーアカウントの認証情報を使用して起動されます。このアカウントの管理上の制御を制限することについての情報は、現在、「ssm-user アカウントの管理権限を無効または有効にする」のトピックで入手できます。	2018 年 11 月 13 日
Automation アクションのリファレンスの YAML サンプル	「Automation アクションのリファレンス」に、既に JSON サンプルが含まれている各アクションに対して YAML サンプルが追加されました。	2018 年 10 月 31 日
コンプライアンス重要度レベルの関連付けへの割り当て	コンプライアンス重要度レベルを State Manager の関連付けに割り当てることができるようになりました。重要度レベルはコンプライアンスダッシュボードで報告されます。また、重要度レベルは、コンプライアンスレポートをフィルタリングするためにも使用できます。割り当てることができる重要度レベルには、「非常事態」、「高」、「中」、「低」、「未指定」の各レベルが含まれます。詳細については、「関連付けを作成する (コンソール)」を参照してください。	2018 年 10 月 26 日

オートメーションと State Manager を使ったターゲットとレート制御の使用	ターゲット、同時実行数、エラーのしきい値を使用して、リソースのフリート全体の自動化と State Manager 関連付けの実行を制御します。詳細については、「ターゲットとレート制御を使用する自動化ワークフローの実行」および「State Manager関連付けでのターゲットとレート制御の使用」を参照してください。	2018 年 10 月 23 日
メンテナンスウィンドウの有効期間および国際タイムゾーンを指定する	メンテナンスウィンドウを (開始日と終了日) の前後に実行しないように日付を指定できます。さらにメンテナンスウィンドウスケジュールの基となる国際タイムゾーンを指定することもできます。詳細については、「メンテナンスウィンドウの作成 (コンソール)」および「メンテナンスウィンドウの更新 (AWS CLI)」を参照してください。	2018 年 10 月 9 日

パッチベースラインのパッチのカスタムリストを S3 バケットに保持	SSM コマンドドキュメント `AWS-RunPatchBaseline` の新しい "InstallOverrideList" パラメータを使用すると、インストールするパッチのリストへの https URL または Amazon Simple Storage Service (Amazon S3) パス形式の URL を指定できます。このパッチインストールリストは YAML 形式で S3 バケットに保持され、デフォルトのパッチベースラインで指定されたパッチを上書きします。詳細については、「パラメータ名: InstallOverrideList」を参照してください。	2018 年 10 月 5 日
パッチ依存関係のインストールの有無に関する制御を拡張	以前には、拒否済みパッチリスト内のパッチが他のパッチの依存関係であると識別された場合でもインストールされていました。現在では、これらの依存関係をインストールまたはインストールをブロックするかどうかを選択できるようになりました。詳細については、「パッチベースラインの作成」を参照してください。	2018 年 10 月 5 日

条件分岐を使用した動的オートメーションワークフローの作成	`aws:branch` オートメーションアクションを使用すると、動的オートメーションワークフローを作成して、1 つのステップで複数の選択肢を評価し、その評価結果に基づいて オートメーションランブックの別のステップにジャンプできます。詳細については、「ランブックでの条件文の使用」を参照してください。	2018 年 9 月 26 日
AWS CLI を使用した Session Manager 設定の更新	CLI を使用して Session Manager の設定を更新する手順 (CloudWatch Logs や S3 バケットログオプションなど) が、AWS Systems Manager ユーザーガイドに追加されました。詳細については、「AWS CLI を使用して Session Manager 設定を更新する」を参照してください。	2018 年 9 月 25 日
Session Manager での SSM Agent 要件の更新	Session Manager では、SSM Agent バージョン 2.3.68.0 以降が必要です。Session Manager の前提条件の詳細については、「Session Manager の前提条件を完了する」を参照してください。	2018 年 9 月 17 日

インバウンドポートを開いたり Session Manager を使用して踏み台ホストを維持したりすることなくインスタンスを管理	Session Manager を使用すると、AWS Systems Manager のフルマネージドツールで、インタラクティブなワンクリックブラウザベースのシェル、または AWS CLI を介して EC2 インスタンスを管理できます。Session Manager を使用すると、インバウンドポートを開いたり、踏み台ホストを維持したり、SSH キーを管理したりすることなく、安全で監査可能なインスタンスの管理を実現できます。また、Session Manager は、EC2 インスタンスへの簡単なワンクリックのクロスプラットフォームアクセスをエンドユーザーに提供しつつ、インスタンスへの制御されたアクセス、厳格なセキュリティプラクティス、インスタンスアクセスの詳細を含む、完全に監査可能なログを必要とする企業ポリシーに準拠できるようになります。詳細については、「Session Manager について」を参照してください。	2018 年 9 月 11 日

Systems Manager のオートメーションワークフローから他の AWS のサービスを呼び出す	Automation ランブックで 3 つの新しい Automation アクション (またはプラグイン) を使用すると、Automation ワークフローで他の AWS のサービスや Systems Manager ツールを呼び出すことができます。詳細については、「アクション出力の入力としての使用」を参照してください。	2018 年 8 月 28 日
IAM ポリシーで Systems Manager 固有の条件キーを使用する	「ポリシーでの条件の指定」トピックが、ユーザーがポリシーに取り込むことができる Systems Manager 用の IAM 条件キーをリストするように更新されました。これらのキーを使用して、ポリシーが有効になる条件を指定できます。このトピックには、ポリシーの例や他の関連トピックへのリンクも含まれています。	2018 年 8 月 18 日
インベントリタイプを収集するように設定されている/設定されていないインスタンスを確認するためのグループによるインベントリデータの集計	グループを使用すると、1 つ以上のインベントリタイプを収集するように設定されている/設定されていないマネージドインスタンスのカウントを素早く確認できます。グループを使用して、`exists` オペレータを使用するフィルタと 1 つ以上のインベントリタイプを指定します。詳細については、「Inventory データの集計」を参照してください。	2018 年 8 月 16 日

インベントリおよび設定コンプライアンスの履歴および変更の追跡の表示	マネージドインスタンスから収集されたインベントリの履歴および変更の追跡を表示できるようになりました。設定コンプライアンスでレポートされた Patch Manager によるパッチ適用および State Manager による関連付けの履歴および変更の追跡を表示することもできます。詳細については、「Inventory 履歴と変更の追跡の表示」を参照してください。	2018 年 8 月 9 日

Parameter Store を Secrets Manager と統合する	Parameter Store が AWS Secrets Manager と統合されたので、Parameter Store パラメータへの参照がすでにサポートされている他の AWS のサービスを使用する際に Secrets Manager のシークレットを取得できます。これらのサービスには、Amazon EC2、Amazon Elastic Container Service、AWS Lambda、AWS CloudFormation、AWS CodeBuild、AWS CodeDeploy およびその他の Systems Manager ツールが含まれます。Parameter Store を使用して Secrets Manager シークレットを参照することによって、安全で一貫したプロセスを作成し、コードおよび設定スクリプトでシークレットや参照データを呼び出して使用できます。詳細については、「Parameter Store パラメータからの AWS Secrets Manager シークレットの参照」を参照してください。	2018 年 7 月 26 日

Parameter Store パラメータへのラベルのアタッチ	パラメータラベルは、ユーザー定義のエイリアスであり、異なるバージョンのパラメータの管理に役立ちます。パラメータを変更すると、Systems Manager は自動的に新しいバージョンを保存し、そのバージョン番号を 1 つ増やします。ラベルは、バージョンが複数ある場合にパラメータバージョンの用途を覚えておくのに役立ちます。詳細については、「パラメータのラベリング」を参照してください。	2018 年 7 月 26 日
動的自動化ワークフローの作成	デフォルトでは、ステップ (またはアクション) で定義した Automation ランブックの mainSteps セクションの順番に実行されます。1 つのアクションが完了した後、mainSteps セクションで指定された次のアクションが開始されます。このリリースでは、条件付きブランチ作成を実行する自動化ワークフローを作成できるようになりました。つまり、条件変更に動的に応答して、指定されたステップにジャンプする自動化ワークフローを作成できます。詳細については、「ランブックでの条件文の使用」を参照してください。	2018 年 7 月 18 日

Snap を使用して SSM Agent が Ubuntu Server 16.04 AMIs にプリインストールされるようになりました	20180627 で識別される Ubuntu Server 16.04 AMIs 以降から作成されたインスタンスでは、SSM Agent は Snap パッケージを使用してプリインストールされます。それより前の AMIs から作成されたインスタンスでは、deb インストーラパッケージを引き続き使用する必要があります。詳細については、「64 ビット Ubuntu Server 16.04 インスタンスでの SSM Agent のインストールについて」を参照してください。	2018 年 7 月 7 日
SSM Agent が必要とする最低限の S3 アクセス許可の確認	新しいトピック「SSM Agent の S3 バケットの最小 S3 バケットアクセス許可」では、リソースが Systems Manager オペレーションを実行するためにアクセスする必要がある Amazon Simple Storage Service (Amazon S3) バケットについて説明します。Systems Manager を使用するために最小限必要な、インスタンスプロファイルまたは VPC エンドポイントの、S3 バケットへのアクセスを制限する場合、カスタムポリシーでこれらのバケットを指定できます。	2018 年 7 月 5 日

特定の State Manager 関連付け ID の完全な実行履歴の表示	新しいトピック「関連付けの履歴の表示」では、特定の関連付け ID のすべての実行を表示して、1 つ以上のリソースの実行の詳細を表示する方法について説明しています。	2018 年 7 月 2 日
Patch Manager で Amazon Linux 2 のサポートを開始	Patch Manager を使用して、Amazon Linux 2 インスタンスにパッチを適用できるようになりました。Patch Manager オペレーティングシステムのサポートに関する一般的な情報については、「Patch Manager の前提条件」を参照してください。パッチフィルターの定義時に Amazon Linux 2 でサポートされているキーと値のペアについては、AWS Systems Manager API リファレンスの「PatchFilter」を参照してください。	2018 年 26 月 6 日
コマンド出力を Amazon CloudWatch Logs に送信する	新しいトピック「Run Command 用に Amazon CloudWatch Logs を設定する」では、Run Command の出力を CloudWatch Logs に送信する方法について説明します。	2018 年 6 月 18 日

を使用したインベントリのリソースデータ同期の迅速な作成または削除AWS CloudFormation	AWS CloudFormation を使用して、Systems Manager Inventory のリソースデータ同期を作成または削除できます。AWS CloudFormation を使用するには、AWS::SSM::ResourceDataSync リソースを AWS CloudFormation テンプレートに追加します。詳細については、 AWS CloudFormation ユーザーガイドの「AWS CloudFormation テンプレートの使用」を参照してください。また、「Inventory のリソースデータ同期の作成」で説明されているとおり、Inventory のリソースデータ同期を手動で作成することもできます。	2018 年 6 月 11 日

AWS Systems Managerユーザーガイドの更新の通知がRSS を介して利用可能に	HTML 版の Systems Manager ユーザーガイドで、「Systems Manager ドキュメントの更新履歴」ページに説明されている更新の RSS フィードがサポートされるようになりました。RSS フィードには、2018 年 6 月以降に行われた更新が含まれています。以前に発表された更新は、「Systems Manager ドキュメントの更新履歴」ページで引き続き利用できます。このフィードにサブスクライブするには、トップメニューパネルの RSS ボタンを使用します。	2018 年 6 月 6 日
スクリプトで終了コードを指定してマネージドインスタンスを再起動する	新しいトピック「スクリプトからのマネージドインスタンスの再起動」では、Run Command で実行するスクリプトで終了コードを指定して、マネージドインスタンスを再起動するように Systems Manager に指示する方法を説明しています。	2018 年 6 月 3 日
カスタムインベントリが削除されるたびに Amazon EventBridge でイベントを作成する	新しいトピック「EventBridge でのインベントリ削除アクションの表示」では、ユーザーがカスタムインベントリを削除するたびにイベントを作成するよう Amazon EventBridge を設定する方法について説明しています。	2018 年 6 月 1 日

2018 年 6 月以前のアップデート

次の表に、2018 年 6 月以前の「AWS Systems Manager ユーザーガイド」の各リリースにおける重要な変更点を示します。

変更	説明	リリース日
のすべてのマネージドインスタンスをインベントリするAWS アカウント	グローバルなインベントリの関連付けを作成することで、AWS アカウント のすべてのマネージドインスタンスをインベントリできます。詳細については、「AWS アカウント のすべてのマネージドイノードインベントリする」を参照してください。 **Note** グローバルなインベントリの関連付けは、SSM Agent バージョン 2.0.790.0 以降で使用できます。インスタンスで SSM Agent を更新する方法については、「Run Command を使用して SSM Agent を更新する」を参照してください。	2018 年 5 月 3 日
Ubuntu Server 18 にデフォルトでインストールされている SSM Agent	SSM Agent は、デフォルトで Ubuntu Server 18.04 LTS 64 ビットおよび 32 ビット AMIs にインストールされています。	2018 年 5 月 2 日
新しいトピック	新しいトピック、特定のドキュメントバージョンを使用したコマンドの実行 では、document-version パラメータを使用して、コマンドの実行時に使用する SSM ドキュメントのバージョンを指定する方法について説明します。	2018 年 5 月 1 日
新しいトピック	新しいトピック「カスタムインベントリの削除」では、AWS CLI を使用して Amazon S3 からカスタムインベントリデータを削除する方法について説明します。このトピックではまた、`SchemaDeleteOption` を使用してカスタムインベントリタイプを無効化または削除することでカスタムインベントリを管理する方法も説明しています。	2018 年 4 月 19 日

変更	説明	リリース日
	この新しい機能は DeleteInventory API オペレーションを使用します。	
SSM Agent の Amazon SNS 通知	Amazon SNS トピックをサブスクライブして、SSM Agent の新しいバージョンが利用可能になったときに通知を受け取ることができます。詳細については、「SSM Agent 通知にサブスクライブする」を参照してください。	2018 年 9 月 4 日
CentOS パッチ適用のサポート	Systems Manager で、CentOS インスタンスのパッチ適用がサポートされるようになりました。サポートされる CentOS のバージョンについては、Patch Manager の前提条件 を参照してください。パッチ適用の仕組みについては、「Patch Managerの動作の仕組み」を参照してください。	2018 年 3 月 29 日
新規セクション	AWS Systems Manager ユーザーガイドにあるリファレンス情報の単一のソースを提供するために、新しいセクション「AWS Systems Manager リファレンス」が導入されました。追加のコンテンツが利用可能になると、このセクションに追加されます。	2018 年 3 月 15 日
新しいトピック	新しいトピックの 承認されたパッチと拒否されたパッチのリストのパッケージ名の形式 では、カスタムパッチベースラインの承認されたパッチと拒否されたパッチのリストに入力できるパッケージ名の形式の詳細を示しています。Patch Manager でサポートされている各オペレーティングシステムのタイプごとにサンプルフォーマットが用意されています。	2018 年 3 月 9 日

変更	説明	リリース日
新しいトピック	Systems Manager が ChefChef InSpec と統合されるようになりました。InSpec は、GitHub または Amazon S3 で人間が読み取れるプロファイルを作成できるオープンソースのランタイムフレームワークです。その後、Systems Manager を使用してコンプライアンススキャンを実行し、準拠または非準拠のインスタンスを表示できます。詳細については、「Systems Manager Compliance で Chef InSpec プロファイルを使用する」を参照してください。	2018 年 3 月 7 日
新しいトピック	新しいトピック「Systems Manager のサービスにリンクされたロールの使用」では、AWS Identity and Access Management (IAM) のサービスにリンクされたロールを Systems Manager で使用する方法について説明しています。現在、サービスにリンクされたロールが必要なのは、Systems Manager Inventory を使用してタグとリソースグループに関するメタデータを収集する場合のみです。	2018 年 2 月 27 日

変更	説明	リリース日
新しく更新されたトピック	Patch Manager を使用して、インスタンスに設定されているデフォルトのリポジトリとは異なるソースリポジトリにあるパッチをインストールできるようになりました。これは、たとえば、セキュリティに関連しない更新プログラムにより、Ubuntu Server の PPA (Personal Package Archives) の内容により、社内アプリケーションの更新プログラムにより、インスタンスにパッチを適用するのに便利です。カスタムのパッチベースラインを作成するときは、代替パッチソースリポジトリを指定します。詳細については、以下の各トピックを参照してください。 • 代替パッチソースリポジトリを指定する方法 (Linux) • カスタムパッチベースラインの操作 • 異なる OS バージョン用にカスタムリポジトリのパッチベースラインを作成する さらに、Patch Manager を使用して SUSE Linux Enterprise Server インスタンスにパッチを適用できるようになりました。Patch Manager は SLES 12.* バージョンのパッチ適用をサポートしています (64 ビット版のみ)。詳細については、以下のトピックで SLES 固有の情報を参照してください。 • セキュリティに関連するパッチの選択方法 • パッチのインストール方法 • SUSE Linux Enterprise Server でのパッチベースラインルールの仕組み	2018 年 2 月 6 日
新しいトピック	新しいトピック (マネージドノードへのパッチ適用のための SSM コマンドドキュメント) では、最新のセキュリティアップデートでパッチを適用してマネージドインスタンスを維持できるように公開されている 7 種類の SSM ドキュメントを紹介します。	2018 年 1 月 10 日

変更	説明	リリース日
Linux サポートに関する重要な更新	更新されたトピックには、次の情報を含みます。 • SSM Agent は 2017 年 9 月以降の Amazon Linux 1 ベースの AMIs にデフォルトでインストールされています。 • 他の Linux のバージョンで SSM Agent を手動でインストールします (Amazon ECS 対応の AMIs のようにベースのないイメージなど)。	2018 年 1 月 9 日
新しいトピック	新しいトピック「パッチ適用のための SSM コマンドドキュメント: AWS-RunPatchBaseline 」では、この SSM ドキュメントが Windows と Linux の両システムで動作する方法について詳しく説明しています。AWS-RunPatchBaseline ドキュメントで使用できる 2 つパラメータとして Operation と Snapshot ID についても説明しています。	2018 年 1 月 5 日
新しいトピック	このセクション「Patch Managerの動作の仕組み」では、サポートされているオペレーティングシステム別に、どのセキュリティパッチをどのようにインストールするかを Patch Manager で決定する方法について、技術的に詳しく説明しています。また、Linux オペレーティングシステムのディストリビューション別に、パッチベースラインルールがどのように動作するかについても説明しています。	2018 年 1 月 2 日
Systems Manager オートメーションアクションのリファレンスのタイトルを変更し、移動しました	お客様からのフィードバックに基づいて、Automation アクションのリファレンスを 「Systems Manager Automation ランブックのリファレンス」という名前に変更しました。さらに、このリファレンスを「共有リソース > ドキュメント」ノードに移動し、コマンドドキュメントプラグインリファレンス に近づけました。詳細については、「Systems Manager Automation アクションのリファレンス」を参照してください。	2017 年 20 月 12 日

変更	説明	リリース日
モニタリングに関する新しい章と内容	新しい章の「AWS Systems Manager でのログ記録とモニタリング」では、メトリクスとログデータを Amazon CloudWatch Logs に送信する手順について説明しています。新しいトピック「統合された CloudWatch Logs へのノードログの送信 (CloudWatch エージェント)」では、64 ビットの Windows Server インスタンスに限り、インスタンス上のモニタリングタスクを SSM Agent から CloudWatch エージェントに移行手順について説明しています。	2017 年 12 月 14 日
新しい章	新しい章「AWS Systems Manager のためのアイデンティティおよびアクセス管理」では、認証情報を使用してリソースに安全にアクセスできるAWS Identity and Access Management(IAM) と AWS Systems Manager の使用方法について総合的な情報を提供しています。これらの認証情報は、S3 バケットに保存されたデータへのアクセス、EC2 インスタンスへのコマンドの送信、同インスタンスでのタグの読み取りなど、AWS リソースにアクセスするために必要なアクセス許可を提供します。	2017 年 12 月 11 日
左のナビゲーションに対する変更	このユーザーガイドでは、左側のナビゲーションの見出しを新しい AWS Systems Manager コンソールの見出しと一致させています。	2017 年 8 月 12 日
re:Invent 2017 におけるいくつかの変更	• AWS Systems Manager の公式起動: AWS Systems Manager (以前の Amazon EC2 Systems Manager) は、AWS リソース全体で運用データおよび自動化タスクを簡単に一元化できる統一されたインターフェイスです。新しい AWS Systems Manager コンソールには、こちらからアクセスできます。詳細については、「AWS Systems Manager とは」を参照してください。 • YAML サポート: YAML で SSM ドキュメントを作成できます。詳細については、「AWS Systems Manager ドキュメント」を参照してください。	2017 年 11 月 29 日

変更	説明	リリース日
Run Command を使用して、EBS ボリュームの VSS 有効化されたスナップショットを取得する	Run Command を使用すると、Amazon EC2 Windows インスタンスにアタッチされたすべての Amazon Elastic Block Store (Amazon EBS) ボリュームについて、アプリケーション整合性のあるスナップショットを取得できます。このスナップショットプロセスは、Windows Volume Shadow Copy Service (VSS) を使用して、アプリケーションとディスク間で保留中のトランザクションからのデータを含む VSS 対応アプリケーションのイメージレベルバックアップを取得します。また、すべてのアタッチされたボリュームのバックアップを実行する際に、インスタンスのシャットダウンあるいは切断を必要としません。詳細については、「Amazon EC2 ユーザーガイド」の「AWS Systems Manager を使用して Microsoft VSS 対応スナップショットを取得する」を参照してください。	2017 年 11 月 20 日
VPC エンドポイントを使用して、Systems Manager のセキュリティを強化する	インターフェース VPC エンドポイントを使用するように、Systems Manager を設定してマネージドインスタンス (ハイブリッド環境のマネージドインスタンスを含む) のセキュリティ体制を改善できます。インターフェースエンドポイントは、PrivateLink のテクノロジーで、プライベート IP アドレスを使用して Amazon EC2 および Systems Manager API にプライベートにアクセスできる技術です。PrivateLink は、マネージドインスタンス、Systems Manager および EC2 と Amazon ネットワーク間のすべてのネットワークトラフィックを制限します (マネージドインスタンスにはインターネットへのアクセスがありません)。また、インターネットゲートウェイ、NAT デバイスあるいは仮想プライベートゲートウェイの必要はありません。詳細については、「Systems Manager のために VPC エンドポイントを使用して EC2 インスタンスのセキュリティを強化する」を参照してください。	2017 年 11 月 7 日

変更	説明	リリース日
ファイル、サービス、Windows ロールおよび Windows レジストリへのインベントリサポート	SSM インベントリがマネージドインスタンスから以下の情報を収集できるサポートをするようになりました。 • ファイル: 名前、サイズ、バージョン、インストール日、変更および最新アクセス時間など。 • サービス: 名前、表示名、ステータス、依存サービス、サービスのタイプ、起動タイプなど。 • Windows レジストリ: レジストリキーのパス、値の名前、値タイプおよび値。 • Windows ロール: 名前、表示名、パス、機能タイプ、インストール日など。 これらのインベントリタイプの情報を収集開始する前に、インベントリを行うインスタンスで SSM Agent を更新してください。最新バージョンの SSM Agent を実行することで、すべてのサポートされるインベントリタイプのメタデータを収集することを確保できます。State Manager を使用して SSM Agent を更新する方法については、「チュートリアル: AWS CLI で SSM Agent を自動的に更新する」を参照してください。 インベントリの詳細については、「Systems Manager Inventory の詳細」を参照してください。	2017 年 11 月 6 日
自動化ドキュメントの更新	Systems Manager オートメーションのセットアップおよびアクセスの設定についての情報におけるいくつかの問題を修正しました。詳細については、「オートメーションの設定」を参照してください。	2017 年 10 月 31 日

変更	説明	リリース日
GitHub と Amazon S3 の統合	リモートスクリプトの実行: Systems Manager が、プライベートまたはパブリック GitHub リポジトリと Amazon S3 からのスクリプトのダウンロードと実行をサポートするようになりました。`AWS-RunRemoteScript` 事前定義済み SSM ドキュメントまたはカスタム SSM ドキュメントの `aws:downloadContent` プラグインのいずれかを使用して、Python、Ruby、または PowerShell などの Ansible プレイブックやスクリプトを実行できます。これらの変更により、Systems Manager を使用して EC2 インスタンスおよびオンプレミスマネージドインスタンスのハイブリッド環境内での構成およびデプロイのオートメーションを行う際に、Infrastructure as Code が強化されます。詳細については、「GitHub からのスクリプトの実行」および「Amazon S3 からのスクリプトの実行」を参照してください。 複合 SSM ドキュメントの作成: Systems Manager が、プライマリおよび SSM ドキュメントからの 1 つまたは複数のセカンダリ SSM ドキュメントの実行をサポートするようになりました。他のドキュメントを実行する主なドキュメントは、複合ドキュメントと呼ばれます。複合ドキュメントを使用すると、AWS アカウント 間で、セカンダリ SSM ドキュメントの標準セットを作成して共有し、ブートストラップアンチウイルスソフトウェアやドメイン結合インスタンスなどの一般的なタスクを実行できます。Systems Manager、GitHub、または Amazon S3 に保存されている複合ドキュメントとセカンダリドキュメントを実行できます。複合ドキュメントを作成したら、`AWS-RunDocument` 事前定義 SSM ドキュメントを使用して複合ドキュメントを実行できます。詳細については、「複合ドキュメントの作成」および「遠隔で ドキュメントを実行する」を参照してください。 SSM ドキュメントのプラグイン参照: より簡単にアクセスできるように、SSM ドキュメントの SSM プラグイン参照	2017 年 10 月 26 日

変更	説明	リリース日
	を Systems Manager API リファレンスユーザーガイドに移動しました。詳細については、「コマンドドキュメントプラグインリファレンス」を参照してください。	
Parameter Store のパラメータバージョンのサポート	パラメータを編集すると、Parameter Store は自動的にバージョン番号を 1 ずつ繰り返します。API コールと SSM ドキュメントでは、パラメータ名と特定のバージョン番号を指定できます。バージョン番号を指定しない場合は、自動的に最新バージョンが使用されます。 パラメータバージョンは、パラメータが誤って変更された場合の保護層を提供します。必要に応じて、すべてのバージョンの値を表示し、古いバージョンを参照できます。パラメータバージョンを使用して、一定期間にわたってパラメータが何回変更されたかを確認することもできます。詳細については、「Parameter Store でのパラメータバージョンの使用」を参照してください。	2017 年 10 月 24 日
Systems Manager ドキュメントのタグ付けのサポート	これで、AddTagToResource API、AWS CLI 、または AWS Tools for PowerShell を使用して、キーと値のペアを持つ Systems Manager ドキュメントにタグ付けできるようになりました。タグ付けは、割り当てられたタグに基づいて特定のリソースをすばやく特定するのに役立ちます。これは、マネージドインスタンス、メンテナンスウィンドウ、Parameter Store パラメータ、およびパッチベースラインの既存のタグ付けサポートに追加されています。	2017 年 10 月 3 日

変更	説明	リリース日
フィードバックに基づいてエラーを修正、内容を更新するためのさまざまなドキュメントの更新	• 「Systems Manager を利用したハイブリッド環境およびマルチクラウド環境でのノードの管理」の Raspbian Linux の情報を更新。 • Windows Server インスタンスの新しい要件に伴って、「Systems Manager を利用した EC2 インスタンスの管理」が更新されました。SSM Agent では、Windows Server インスタンスで特定の SSM ドキュメントを実行する際に Windows PowerShell 3.0 以降が必要です (レガシー `AWS-ApplyPatchBaseline` SSM ドキュメントなど)。Windows Server インスタンスで Windows Management Framework 3.0 以降を実行していることを確認します。このフレームワークには PowerShell が含まれます。詳細については、「Windows 管理フレームワーク 3.0」を参照してください。	2017 年 10 月 2 日
EC2Rescue の自動化ワークフローを使用した、接続できない Windows インスタンスのトラブルシューティング	EC2Rescue は、Amazon EC2 Windows Server インスタンスでの問題の診断とトラブルシューティングに役立ちます。AWSSupport-ExecuteEC2Rescue ドキュメントを使用して、Systems Manager のオートメーションワークフローとしてツールを実行できます。AWSSupport-ExecuteEC2Rescue ドキュメントは、Systems Manager アクション、AWS CloudFormation アクション、および Lambda 関数を組み合わせて実行するように設計されています。これにより、EC2Rescue の使用に通常必要なステップが自動化されます。詳細については、「到達不可能なインスタンスでの EC2Rescue ツールの実行」を参照してください。	2017 年 9 月 29 日
Amazon Linux にデフォルトで SSM Agent をインストール	SSM Agent は 2017 年 9 月以降の Amazon Linux AMIs にデフォルトでインストールされます。「Linux 用 EC2 インスタンスで SSM Agent を使用する」で説明されているとおり、Linux のその他のバージョンでは、手動で SSM Agent をインストールします。	2017 年 9 月 27 日

変更	説明	リリース日
Run Command の機能強化	Run Command には以下の機能強化が含まれています。 • 特定の Amazon EC2 タグが付けられたインスタンスでのみユーザーがコマンドを実行できるようにする条件を含む IAM ポリシーを作成しアサインして、特定のインスタンスにコマンドの実行を制限できます。詳細については、「タグによる Run Command アクセスを制限」を参照してください。 • Amazon EC2 タグを使用してインスタンスを対象にするためのオプションが、より多くなりました。コマンドを送信するときに、複数のタグキーおよび複数のタグ値を指定できるようになりました。詳細については、「コマンドを大規模に実行する」を参照してください。	2017 年 9 月 12 日
Systems Manager が Raspbian でサポート	Systems Manager は、Raspberry Pi (32 ビット) を含む Raspbian Jessie と Raspbian Stretch デバイスで実行できるようになりました。	2017 年 9 月 7 日
SSM Agent ログを Amazon CloudWatch Logs に自動的に送信する	インスタンスでの簡単な設定変更を行い、SSM Agent でログファイルを CloudWatch に送信できるようになりました。詳細については、「CloudWatch Logs に SSM Agent ログを送信する」を参照してください。	2017 年 9 月 7 日
リソースデータの同期の暗号化	Systems Manager リソースデータ同期では、数十または数百のマネージドインスタンスで収集された Inventory データを、中央 S3 バケットで集計できます。AWS Key Management Service キーを使用してリソースデータの同期を暗号化できるようになりました。詳細については、「チュートリアル: リソースデータの同期を使用してインベントリデータを集計する」を参照してください。	2017 年 9 月 1 日

変更	説明	リリース日
新しい State Manager のチュートリアル	2 つの新しいチュートリアルを State Manager のドキュメントに追加しました。 チュートリアル: AWS CLI で SSM Agent を自動的に更新する チュートリアル: Windows Server の EC2 インスタンスで PV ドライバーを自動的に更新する	2017 年 8 月 31 日
Systems Manager 設定コンプライアンス	設定コンプライアンスを使用すると、マネージドインスタンス群のスキャンを実行して、パッチコンプライアンスと設定の不一致を確認できます。複数の AWS アカウント と AWS リージョン からデータを収集して集計し、それに準拠していない特定のリソースにドリルダウンすることができます。デフォルトでは、設定コンプライアンスでは、Patch Manager によるパッチ適用と State Manager による関連付けに関するコンプライアンスデータが表示されます。サービスをカスタマイズし、IT またはビジネスの要件に基づいて独自のコンプライアンスタイプを作成することもできます。詳細については、「AWS Systems Manager のコンプライアンス」を参照してください。	2017 年 8 月 28 日
新しいオートメーションアクション: `aws:executeAutomation`	セカンダリ Automation ランブックを呼び出してセカンダリ Automation ワークフローを実行します。このアクションを使用すると、一般的なほとんどのワークフローの Automation ランブックを作成し、Automation の実行中にこれらのドキュメントを参照できます。このアクションでは、同じようなランブックで重複したステップが不要になり、Automation ランブックを簡素化できます。詳細については、「`aws:executeAutomation` – 別のオートメーションを実行する」を参照してください。	2017 年 8 月 22 日

変更	説明	リリース日
CloudWatch Events のターゲットとしてのオートメーション	Automation ランブックを Amazon CloudWatch イベントのターゲットとして指定することで、Automation ワークフローを開始できます。ワークフローは、スケジュールに従って、または特定の AWS システムイベントが発生したときに開始できます。詳細については、「EventBridge イベントに基づくオートメーションを実行する」を参照してください。	2017 年 8 月 21 日
State Manager の関連付けバージョニングおよび一般的な更新	State Manager の関連付けで異なるバージョンを作成できるようになりました。各関連付けのバージョンのクォータは 1,000 個です。関連付けの名前も指定できます。また、State Manager ドキュメントが更新され、古くなった情報や不整合性が対処されました。詳細については、「AWS Systems Manager State Manager」を参照してください。	2017 年 8 月 21 日

変更	説明	リリース日
Maintenance Windows の変更点	Maintenance Windows が次のように変更または強化されました。 • 以前は、Maintenance Windows は Run Command を使用してのみタスクを実行できました。Systems Manager Automation、AWS Lambda 、および AWS Step Functions を使用してタスクを実行できるようになりました。 • メンテナンスウィンドウのターゲットを編集して、ターゲット名、説明、所有者を指定できます。 • Run Command およびオートメーションタスクの新しい SSM ドキュメントを指定するなど、メンテナンスウィンドウのタスクを編集できます。 • DocumentHash、DocumentHashType、TimeoutSeconds、Comment、NotificationConfig を含むすべての Run Command パラメータがサポートされるようになりました。 • ターゲットの登録解除に `safe` フラグを使用できるようになりました。有効にすると、ターゲットがタスクから参照されている場合はシステムによって エラーが返されます。 詳細については、「AWS Systems Manager Maintenance Windows」を参照してください。	2017 年 8 月 16 日
新しいオートメーションアクション: `aws:approve`	Automation ランブックのこの新しいアクションは、指定されたプリンシパルによってアクションか承認または拒否されるまで、一時的に Automation の実行を停止します。必要な承認数が得られると、自動化の実行が再開されます。 詳細については、「Systems Manager Automation アクションのリファレンス」を参照してください。	2017 年 8 月 10 日

変更	説明	リリース日
オートメーションでロールの継承が不要になりました。	以前のオートメーションでは、ユーザーに代わってアクションを実行するための権限をサービスに持たせるために、サービスロールを指定 (ロールの継承) する必要がありました。サービスが実行を呼び出したユーザーのコンテキストを使用して処理するようになったため、自動化でこのロールが不要になりました。 ただし、次の条件では、引き続き自動化にサービスロールを指定する必要があります。 • リソースに対するユーザーのアクセス許可は制限するが、そのユーザーに昇格されたアクセス許可を必要とする自動化ワークフローを実行させる場合があるとします。このシナリオでは、昇格されたアクセス許可を持つサービスロールを作成して、このユーザーにワークフローの実行を許可できます。 • 12 時間を超えて実行されるオペレーションにはサービスロールが必要です。 詳細については、「オートメーションの設定」を参照してください。	2017 年 8 月 3 日
設定コンプライアンス	Amazon EC2 Systems Manager 設定コンプライアンスを使用し、マネージドインスタンスフリートのスキャンを実行して、パッチコンプライアンスと設定の不一致を確認します。複数の AWS アカウント と AWS リージョン からデータを収集して集計し、それに準拠していない特定のリソースにドリルダウンすることができます。詳細については、「AWS Systems Manager のコンプライアンス」を参照してください。	2017 年 8 月 8 日

変更	説明	リリース日
SSM ドキュメントの拡張	SSM コマンドおよびポリシードキュメントで、クロスプラットフォームのサポートが提供されるようになりました。つまり、単一の SSM ドキュメント内で Windows および Linux オペレーティングシステムのプラグインを処理できます。クロスプラットフォームのサポートにより、管理する多数のドキュメントを統合できます。クロスプラットフォームのサポートは、スキーマバージョン 2.2 以降を使用する SSM ドキュメントで提供されます。 スキーマバージョン 2.0 以降を使用する SSM コマンドドキュメントに、同じタイプの複数のプラグインを含めることができるようになりました。例えば、 `aws:runRunShellScript` プラグインを複数回呼び出すコマンドドキュメントを作成できます。 スキーマバージョン 2.2 の変更に関する詳細については、「AWS Systems Manager ドキュメント」を参照してください。SSM プラグインの詳細については、「コマンドドキュメントプラグインリファレンス」を参照してください。	2017 年 7 月 12 日

変更	説明	リリース日
Linux のパッチ	Patch Manager で次の Linux ディストリビューションにパッチを適用できるようになりました。 64 ビットおよび 32 ビットシステム • Amazon Linux 2014.03、2014.09 以降 • Ubuntu Server 16.04 LTS、14.04 LTS、または 12.04 LTS • Red Hat Enterprise Linux (RHEL) 6.5 以降 64 ビットシステムのみ • Amazon Linux 2015.03、2015.09 以降 • Red Hat Enterprise Linux (RHEL) 7.x 以降 詳細については、「AWS Systems Manager Patch Manager」を参照してください。 Note • Linux インスタンスにパッチを適用するには、インスタンスで SSM Agent バージョン 2.0.834.0 以降を実行している必要があります。エージェントの更新方法については、「コンソールからコマンドを実行する」の「例: SSM Agent の更新」のセクションを参照してください。 • `AWS-ApplyPatchBaseline` SSM ドキュメントが `AWS-RunPatchBaseline` ドキュメントに置き換えられています。	2017 年 6 月 7 日

変更	説明	リリース日
リソースデータの同期	Systems Manager リソースデータ同期を使用して、すべてのマネージドインスタンスから収集されたインベントリデータを単一の Amazon S3 バケットに送信できます。その後、リソースデータの同期により、新しいインベントリデータが収集されると、一元化されたデータが自動的に更新されます。ターゲット S3 バケットに保存されたすべてのインベントリデータに対して、Amazon Athena や Amazon QuickSight などのサービスを使用して集計データのクエリや分析を実行できます。詳細については、「インベントリのリソースデータ同期を作成する」を参照してください。リソースデータの同期の使用方法の例については、「チュートリアル: リソースデータの同期を使用してインベントリデータを集計する」を参照してください。	2017 年 6 月 29 日
Systems Manager のパラメータ階層	数十または数百の Systems Manager パラメータをフラットリストで管理することは、時間がかかり、エラーの原因となります。パラメータ階層を使用すると、Systems Manager パラメータの編成や管理がしやすくなります。階層は、スラッシュを使用して定義するパスを含むパラメータ名です。3 つの階層レベルを名前に使用して識別する例を以下に示します。 /Environment/Type of computer/Application/Data `/Dev/DBServer/MySQL/db-string13` 詳細については、「Parameter Store でのパラメータ階層の使用」を参照してください。	2017 年 6 月 22 日
SSM Agent による SUSE Linux Enterprise Server のサポート	SSM Agent を 64 ビット SUSE Linux Enterprise Server (SLES) にインストールできます。詳細については、「Linux 用 EC2 インスタンスで SSM Agent を使用する」を参照してください。	2017 年 6 月 14 日

ドキュメントの表記規則

以下に、「AWS Systems Manager ユーザーガイド」の一般的な表記規則を示します。

ローカルオペレーティングシステムまたはコマンドライン言語のさまざまな例

タブを使用して、ユーザーのローカルオペレーティングシステムのタイプに基づいてさまざまなコマンドの例を示します。Linux および macOS の例では、バックスラッシュ (\) 文字を、長いコマンドを複数の行に分割するために使用します。Windows Server の例では、キャレット (^) 文字を使用してコマンドを複数行に分割します。

例：

Linux & macOS

```
aws ssm update-service-setting \
    --setting-id arn:aws:ssm:region:aws-account-id:servicesetting/ssm/managed-instance/activation-tier \
    --setting-value advanced
```

Windows

```
aws ssm update-service-setting ^
    --setting-id arn:aws:ssm:region:aws-account-id:servicesetting/ssm/managed-instance/activation-tier ^
    --setting-value advanced
```

ユーザーインターフェイス内の要素

フォーマット: 太字のテキスト

例: [ファイル]、[プロパティ] の順に選択します。

ユーザー入力 (ユーザーが入力するテキスト)

フォーマット: 等幅フォントのテキスト

例: 名前として、**`my-new-resource`** を入力します。

必要な値のプレースホルダーテキスト

フォーマット: *##*のテキスト

例：

```
aws ec2 register-image --image-location amzn-s3-demo-bucket/image.manifest.xml
```