



AWS Systems Manager

State Manager 編

AWS Black Belt Online Seminar

小野 卓人

Solutions Architect
2023/06

AWS Black Belt Online Seminarとは

- 「サービス別」「ソリューション別」「業種別」などのテーマに分け、アマゾン ウェブ サービス ジャパン合同会社が提供するオンラインセミナーシリーズです
- AWSの技術担当者が、AWSの各サービスやソリューションについてテーマごとに動画を公開します
- 動画を一時停止・スキップすることで、興味がある分野・項目だけの聴講も可能、スキマ時間の学習にもお役立ていただけます
- 以下のURLより、過去のセミナー含めた資料などをダウンロードすることができます
 - <https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-service-cut/>
 - <https://www.youtube.com/playlist?list=PLzWGOASvSx6FIwIC2X1nObr1KcMCBBIqY>

内容についての注意点

- 本資料では2023年6月時点のサービス内容および価格についてご説明しています。最新の情報はAWS公式ウェブサイト(<https://aws.amazon.com/>)にてご確認ください
- 資料作成には十分注意しておりますが、資料内の価格とAWS公式ウェブサイト記載の価格に相違があった場合、AWS公式ウェブサイトの価格を優先とさせていただきます
- 価格は税抜表記となっております。日本居住者のお客様には別途消費税をご請求させていただきます

自己紹介

名前：小野 卓人 (Takuto Ono)

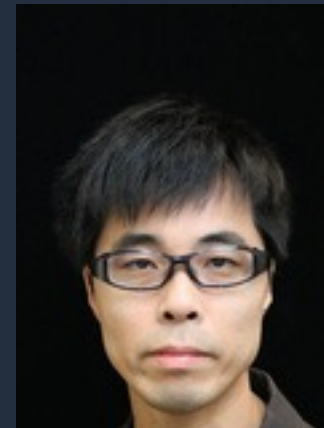
所属：技術統括本部 金融ソリューション本部
保険ソリューション部

経歴：

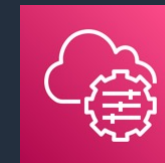
SIer で金融機関向けシステムの受託開発

インフラ設計・構築・運用保守

現在は、ソリューションアーキテクトとして主に保険業界のお客様を担当



好きなAWSサービス： AWS Systems Manager



本セミナーの対象者

AWS の運用をされている方、これから運用される予定の方

本セミナーの目的

- AWS Systems Manager State Manager の機能とユースケースをご理解いただく。

本日本話ししないこと

- AWS Systems Manager の全体的な説明
→ [AWS Systems Manager Overview](#) を参照ください
- AWS Systems Manager State Manager 以外の機能の詳細
→ 各機能にフォーカスしたセッションを参照ください（今後も続々と公開予定です！）

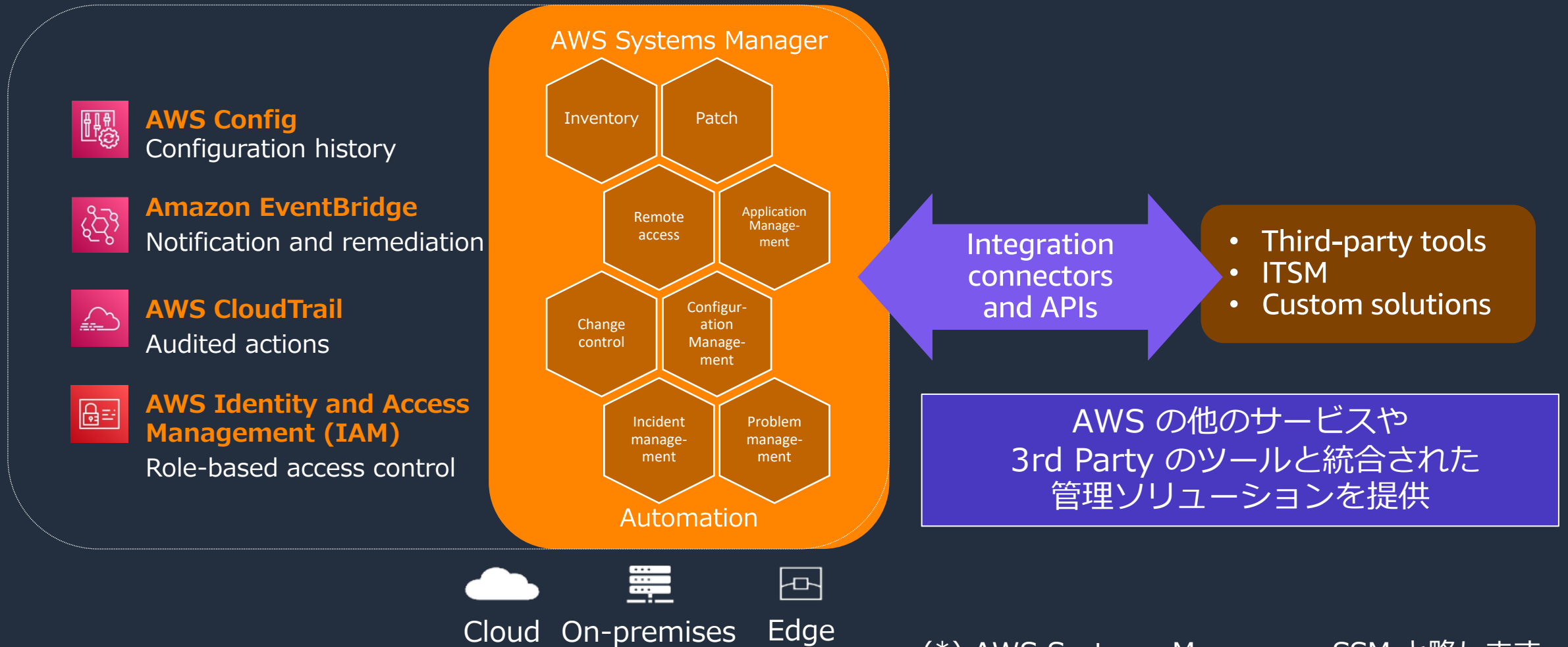
アジェンダ

1. State Manager の概要
2. State Manager の主要な構成要素
3. 関連付けの作成
4. 関連付けの実行結果
5. TIPS
6. まとめ

AWS Systems Manager State Manager の概要

AWS Systems Manager

ハイブリッドクラウド環境のための安全なエンドツーエンドの管理ソリューション



(*) AWS Systems Manager = SSM と略します。

AWS Systems Manager の機能

運用管理



Explorer



OpsCenter



Incident Manager

アプリケーション管理



Application Manager



AppConfig



Parameter Store

変更管理



Change Manager



Automation



Maintenance Windows



Change Calendar

ノード管理



Fleet Manager



Session Manager



Inventory



Run Command



Patch Manager



Distributor



State Manager




Quick Setup

AWS Systems Manager の機能





運用管理

-  Explorer
-  OpsCenter
-  Incident Manager








アプリケーション管理

-  Application Manager
-  AppConfig
-  Parameter Store

変更管理

-  Change Manager
-  Automation
-  Maintenance Windows
-  Change Calendar

ノード管理

-  Fleet Manager
-  Session Manager
-  Inventory
-  Run Command
-  Patch Manager
-  Distributor
-  State Manager

Quick Setup

AWS Systems Manager State Manager とは



安全でスケーラブルな設定管理サービス

- マネージドノードやその他の AWS リソースを“定義された状態”に保つためのプロセスを自動化
- “定義された状態”への準拠状況をダッシュボードで可視化
- AWS リソースの管理とガバナンスを改善し、設定のズレを軽減するのに役立つ
- State Manager は追加料金なしでご利用可能

関連 ID	関連付けの名前	ドキュメント名	最終実行日	ステータス	関連付けのバージョン	リソースのステータス数
b288296a-52d1-46f0-b69b-3d09f6094d57	AWS-QuickSetup-SSMHostMgmt-UpdateCloudWatchAgent-tb53k	UpdateCloudWatchDocument-tb53k	Wed, 17 May 2023 15:01:39 GMT	成功	1	Success:1
ba084271-08de-4502-b99b-6821b4cc4900	AWS-QuickSetup-SSMHostMgmt-AttachIAMToInstance-tb53k	AWSQuickSetup-CreateAndAttachIAMToInstance-tb53k	Tue, 25 Apr 2023 05:20:14 GMT	成功	1	Success:15
e8ce0d24-65d9-4b7e-81ce-ef0f4005d8d	AWS-QuickSetup-SSMHostMgmt-UpdateSSMAgent-tb53k	AWS-UpdateSSMAgent	Tue, 23 May 2023 05:19:06 GMT	成功	1	Success:1
eb37b0c6-85f9-4630-a056-7a1142c08883	AWS-QuickSetup-PatchPolicy-ScanForPatches-LA-1g37x	AWS-RunPatchBaseline	Wed, 24 May 2023 08:10:54 GMT	失敗	1	Failed:4
f110e458-9f16-4729-b943-3ba9369a794	AWS-GatherSoftwareInventory	AWS-GatherSoftwareInventory	Wed, 01 Feb 2023 06:25:45	保留中	2	

コンプライアンスタイプ	準拠ルール	非準拠ルール	重要なルール	高ルール	中ルール	低ルール	情報ルール
Association	12	0	0	0	0	0	0
Patch	461	0	0	0	0	0	0

State Manager のユースケース例

マネージドノード上での OS コマンド実行

- アンチウイルスソフトウェアのインストールと設定
- SSM Agent などのエージェントソフトウェアを定期的にアップデート
- ネットワーク設定
- Microsoft Active Directory ドメインへのノード参加

AWS リソースの制御

- EC2 インスタンスにロールをアタッチする
- セキュリティグループに Ingress ルールと Egress ルールを適用する
- AMI へのパッチ適用

リソースを **定義された状態** に維持する

Maintenance Windows との使い分け



State Manager

- SSM ドキュメントを定期実行し、「定義された状態」を維持するプロセスを自動化
- 「定義された状態」への準拠状況をレポート
- マネージドノードのブートストラップ (Auto Scaling シナリオにも有効)

リソースを定義された状態に維持する



Maintenance Windows

- 開始時刻と終了時刻を持つ「タイムウィンドウ」内で複数のタスクを実行
- パッチ適用など、ノードの停止を伴うような変更をスケジュール実行
- SSM ドキュメント以外にも Lambda 関数と Step Functions の実行をサポート

時間的制約のあるタスクを
タイムウィンドウ内に実行する

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/state-manager-vs-maintenance-windows.html

State Manager の 主要な構成要素

State Manager の主要な構成要素



State Manager Association (関連付け)

SSM ドキュメント



“定義された状態”を維持するためのアクションを定義したもの

スケジュール

アクションの実行タイミングに関する設定

ターゲット



“定義された状態”を維持する対象リソース

※その他の設定項目については後述します



実行結果の可視化
(AWS Systems Manager Compliance)

State Manager の主要な構成要素



State Manager Association (関連付け)

SSM ドキュメント



“定義された状態”を維持するためのアクションを定義したもの

スケジュール

アクションの実行タイミングに関する設定

ターゲット



“定義された状態”を維持する対象リソース

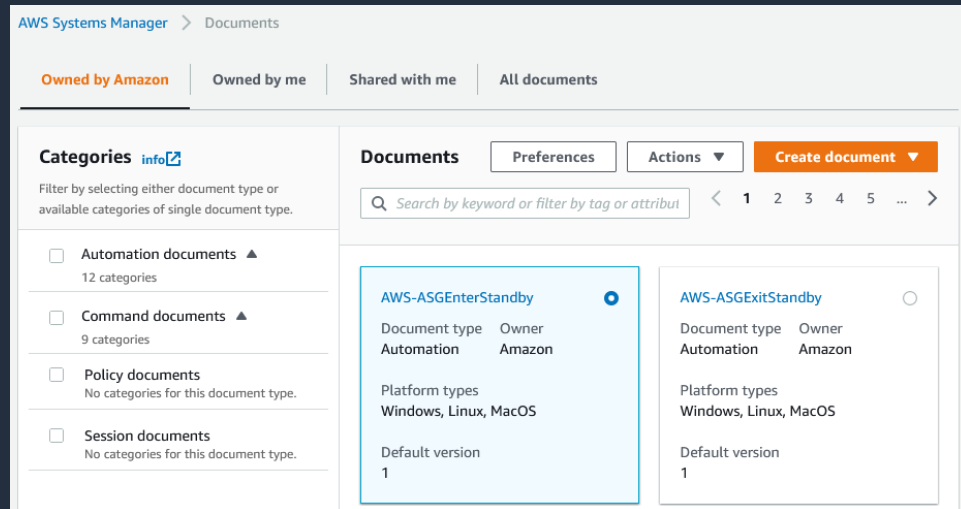
※その他の設定項目については後述します



実行結果の可視化
(AWS Systems Manager Compliance)

Systems Manager ドキュメントとは

- 実行するアクションを定義したもの
 - 一般的なタスクを自動化し、ヒューマンエラーを減らす
- 100以上の事前設定済みのドキュメント
 - カスタムドキュメントの作成も可能
- JSON or YAML 形式
- バージョニング、タグをサポート



```
{
  "schemaVersion": "2.2",
  "description": "Cross-platform demo document",
  "mainSteps": [
    {
      "action": "aws:runPowerShellScript",
      "precondition": {
        "StringEquals": ["platformType", "Windows"]
      },
      "name": "WindowsOpenPorts",
      "inputs": {
        "runCommand": ["netstat -a"]
      }
    },
    {
      "action": "aws:runShellScript",
      "precondition": {
        "StringEquals": ["platformType", "Linux"]
      },
      "name": "LinuxOpenPorts",
      "inputs": {
        "runCommand": ["netstat -lntu"]
      }
    }
  ]
}
```

State Manager がサポートするドキュメントタイプ

以下の3つのドキュメントタイプをサポート

Type	Usage with	主な用途
Automation (Runbook)	✓ Automation	<ul style="list-style-type: none">AWS リソースのメンテナンス、デプロイ、修復に関する一般的なタスクを簡素化するためのワークフローを定義
Command	✓ Run Command	<ul style="list-style-type: none">マネージドノード上で実行するコマンドを定義
Policy	✓ Inventory	<ul style="list-style-type: none">AWS-GatherSoftwareInventory ポリシードキュメントと State Manager の関連付けを使って、マネージドノードからインベントリデータを収集

Automation、Run Command、Inventory の各機能については、公式ドキュメントまたは今後公開予定の Black Belt オンラインセミナーのセッションを参照ください。

State Manager の主要な構成要素



State Manager Association (関連付け)

SSM ドキュメント



“定義された状態”を維持するためのアクションを定義したもの

スケジュール

アクションの実行タイミングに関する設定

ターゲット



“定義された状態”を維持する対象リソース

※その他の設定項目については後述します



実行結果の可視化
(AWS Systems Manager Compliance)

ターゲットの指定方法

Command または Policy ドキュメントの場合



対象は マネージドノード

- タグ指定
- ノードを手動で選択
- リソースグループ指定
- すべてのマネージドノード

Automation Runbook の場合



対象は主に AWS リソース

- シンプルな実行
 - Runbook を単体で実行
- レートの制御
 - 複数のターゲットに対して Runbook を実行

ターゲットの指定方法

Command または Policy ドキュメントの場合



対象は マネージドノード

- タグ指定
- ノードを手動で選択
- リソースグループ指定
- すべてのマネージドノード

ターゲットの選択

ターゲットの選択
ターゲットを選択する方法を選択します。

インスタスタグを指定
タグのキーと値のペアを1つ以上指定して、それらのタグを共有するインスタスタグを選択します。

インスタスタグを手動で選択
ターゲットとして登録するインスタスタグを手動で選択します。

リソースグループを選択
ターゲットとするリソースを含むリソースグループを選択します。

すべてのインスタスタグを選択
ターゲットとして登録するすべてのインスタスタグを選択します。

インスタスタグを指定

インスタスタグのキーと値のペアを1つ以上指定して、タスクを実行するインスタスタグを識別します。

ターゲットとするインスタスタグに適用された、タグキーとオプションの値を入力した後、追加を選択します。

ターゲットの指定方法

Automation Runbook の場合



対象は主に AWS リソース

- シンプルな実行
 - Runbook を単体で実行
- レートの制御
 - 複数のターゲットに対して Runbook を実行

Execution

シンプルな実行
ターゲットで実行します。

レートの制御
同時実行数とエラーのしきい値を定義して、複数のターゲットで安全に実行します。

入力パラメーター

InstanceID
(Required) ID of EC2 Instance to change standby state for within ASG
String

LambdaRoleArn
(Optional) The ARN of the role that allows Lambda created by Automation to perform the actions on your behalf. If not specified a transient role will be created to execute the Lambda function.

AutomationAssumeRole
(Required) The ARN of the role that allows Automation to perform the actions on your behalf.

Runbook の内容に応じて対象のリソースIDを直接指定

※入力パラメーターは一例です。実際は Runbook の内容によって変わります

ターゲットの指定方法

Automation Runbook の場合



対象は主に AWS リソース

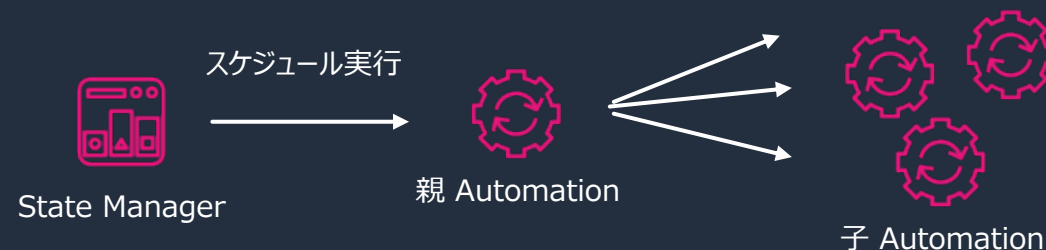
- シンプルな実行
 - Runbook を単体で実行
- レートの制御
 - 複数のターゲットに対して Runbook を実行

Execution

シンプルな実行
ターゲットで実行します。

レートの制御
同時実行数とエラーのしきい値を定義して、複数のターゲットで安全に実行します。

- 複数のリソースを対象に Automation Runbook を実行できる
※State Manager ではなく Automation の機能
- State Manager が呼び出す 親 Automation は、ターゲットとなるリソースごとに子 Automation を起動する



Automation のドキュメントも参照ください。

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/running-automations-scale.html

ターゲットの指定方法

Automation Runbook の場合

複数のターゲットの指定方法

- パラメータ値
- リソースグループ
- タグ
- すべてのインスタンス

1 の条件に合致するターゲットの

2 のパラメータ情報を

子 Automation の 3 に連携する

Execution

シンプルな実行
ターゲットで実行します。

レートの制御
同時実行数とエラーのしきい値を定義して、複数のターゲットで安全に実行します。

ターゲット
自動化ドキュメントを実行するターゲットを選択します。

パラメータの選択
オートメーションが分岐する方法を定義するパラメータを選択します。

InstanceId

ターゲットを選択します
ターゲットを選択する

入力パラメーター

InstanceId
(Required) ID of EC2 Instance to change standby state for within ASG
String

LambdaRoleArn
(Optional) The ARN of the role that allows Lambda created by Automation to perform the actions on your behalf. If not specified a transient role will be created to execute the Lambda function.
String

ターゲットの指定方法

Automation Runbook の場合

複数のターゲットの指定方法

- **パラメータ値**
- リソースグループ
- タグ
- すべてのインスタンス

カンマ区切りで複数のリソースの情報を指定可能

ターゲット
自動化ドキュメントを実行するターゲットを選択します。

パラメータの選択
オートメーションが分岐する方法を定義するパラメータを選択します。

Instanceld

ターゲットを選択します
パラメータ値

入力パラメーター

Instanceld
(Required) ID of EC2 Instance to change standby state for within ASG
i-xxxxxxxxx,i-yyyyyyyyyy,i-zzzzzzzzzz

LambdaRoleArn
(Optional) The ARN of the role that allows Lambda created by Automation to perform the actions on your behalf. If not specified a transient role will be created to execute the Lambda function.
String

ターゲットの指定方法

Automation Runbook の場合

複数のターゲットの指定方法

- パラメータ値
- **リソースグループ**
- タグ
- すべてのインスタンス

ターゲット
自動化ドキュメントを実行するターゲットを選択します。

パラメータの選択
オートメーションが分岐する方法を定義するパラメータを選択します。

Instanceld ▼

ターゲットを選択します
リソースグループ ▼

リソースグループ名を選択します
🔍 MyEc2Instances ✕

入力パラメーター

Instanceld
(Required) ID of EC2 Instance to change standby state for within ASG
String

LambdaRoleArn
(Optional) The ARN of the role that allows Lambda created by Automation to perform the actions on your behalf. If not specified a transient role will be created to execute the Lambda function.
String

ターゲットの指定方法

Automation Runbook の場合

複数のターゲットの指定方法

- パラメータ値
- リソースグループ
- **タグ**
- すべてのインスタンス

ターゲット

自動化ドキュメントを実行するターゲットを選択します。

パラメータの選択
オートメーションが分岐する方法を定義するパラメータを選択します。

Instanceld

ターゲットを選択します

タグ

タグ
1つ以上のタグキーと値のペアを指定します。

タグキー タグの値 (オプション) Add

ターゲットとするインスタンスに適用された、タグキーとオプションの値を入力した後、追加を選択します。

Env : Dev X

入力パラメーター

Instanceld
(Required) ID of EC2 Instance to change standby state for within ASG
String

LambdaRoleArn
(Optional) The ARN of the role that allows Lambda created by Automation to perform the actions on your behalf. If not specified a transient role will be created to execute the Lambda function.
String

ターゲットの指定方法

Automation Runbook の場合

複数のターゲットの指定方法

- パラメータ値
- リソースグループ
- タグ
- **すべてのインスタンス**

ターゲット
自動化ドキュメントを実行するターゲットを選択します。

パラメータの選択
オートメーションが分岐する方法を定義するパラメータを選択します。

InstancedId

ターゲットを選択します

All instances

Instance

*

入力パラメーター

InstancedId
(Required) ID of EC2 Instance to change standby state for within ASG
String

LambdaRoleArn
(Optional) The ARN of the role that allows Lambda created by Automation to perform the actions on your behalf. If not specified a transient role will be created to execute the Lambda function.
String

同時実行数とエラーしきい値

(Command/ Policy /Automation 共通)

▼ レートの制御

同時実行性
同時にタスクを実行するターゲットの数または割合 (%) を指定

10 ターゲット

パーセンテージ

エラーのしきい値
指定した数または割合 (%) のターゲットでタスクが失敗した後、タスクを停止

ターゲット

10 パーセンテージ

同時実行性

- 関連付けを同時に実行するターゲットの数、または割合を指定

エラーのしきい値

- この値を超えてタスクが失敗したら関連付けタスクの停止を指示したり、残りのターゲットに対する実行要求を停止する

State Manager の主要な構成要素



State Manager Association (関連付け)

SSM ドキュメント



“定義された状態”を維持するためのアクションを定義したもの

スケジュール

アクションの実行タイミングに関する設定

ターゲット



“定義された状態”を維持する対象リソース

※その他の設定項目については後述します



実行結果の可視化
(AWS Systems Manager Compliance)

スケジュールの指定方法

スケジュールを指定

スケジュールあり
cron/rate 間隔で関連付けを実行。

スケジュールなし
関連付けを 1 回実行。

スケジュールなし

関連付けを1回のみ実行

→ 関連付けの作成直後に1回実行される

スケジュールあり

cron/rate 式で指定した スケジュールで関連付けを実行

→ cron式、rate式による柔軟なスケジュール設定

加えて、以下のタイミングでも実行される

- ✓ 関連付けやドキュメントの修正時
- ✓ ターゲットとなるマネージドノードが初めてオンラインになったタイミング
(Command / Inventory の場合)
- ✓ マネジメントコンソールや AWS CLI / AWS SDK から即時実行した場合

(詳細は次スライド)

関連付けの実行タイミング

指定したスケジュールで実行されるほか、以下のタイミングでも関連付けが実行される

- ✓ 関連付けを新規作成または編集したとき ※1
- ✓ SSM ドキュメントを更新したとき
- ✓ 手動で関連付けを起動したとき
- ✓ ターゲット（マネージドノード）の状態が変更になったとき ※2
 - 対象インスタスが初めてオンラインになる
 - スケジュールを逃した後、インスタスが初めてオンラインになる
 - 30日以上停止していたノードがオンラインになる

※1 即時実行を抑止するオプションも有り

※2 Command または Policy ドキュメントの場合

[関連付けはいつリソースに適用されますか?]

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/sysman-state-about.html#state-manager-about-scheduling

Cron 式 / Rate 式

State Manager / Maintenance Windows で使われるスケジュール表記法

- cron 式 … 時間を指定

例) 毎月第3火曜日の午後11:30(UTC)

```
cron(30 23 ? * TUE#3 *)
```

※ 現在、State Manager では 関連付けの cron 式での月の指定はサポートされていません。

- rate 式 … 頻度を指定

例) 15分おき

```
rate(15 minutes)
```

- 1回限りのスケジュール実行

例) 2023年7月20日15時55分(UTC)

```
at(2023-07-20T15:55:00)
```

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/reference-cron-and-rate-expressions.html

Cron でスケジュール指定する場合のオプション

- ✓ ApplyOnlyAtCronInterval オプション
 - 関連付けの作成/修正直後の実行をSKIPする
- ✓ スケジュールオフセット
 - cron式で指定された日時から関連付けを実行するまでに待機する日数
 - 1日～6日まで指定可

指定

CRON スケジュールビルダー

Rate スケジュールビルダー

CRON/Rate 式

CRON/Rate 式
関連付けのスケジュールを CRON 式/間隔の式の形式で入力します。 [Learn More.](#)

例: "cron(0 10 * * ? *)" または "rate(7 days)"

次に指定された cron 間隔でのみ関連付けを適用する

スケジュールオフセット - オプション
CRON 式の日付から関連付けを実行するまでに待機する日数

日数

1 ~ 6 の値

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/reference-cron-and-rate-expressions.html

その他のオプション

関連付けの実行タイミングの制御に関する2つのオプション



Change Calendar (変更カレンダー)

- 対象のカレンダーが Close の場合、関連付けの実行をスキップ



Cloud Watch アラーム

- 対象のアラームが Active の場合、関連付けの実行をスキップ

詳細オプション

変更カレンダー
変更カレンダーを指定します。関連付けは、変更カレンダーが開いているときに実行され、変更カレンダーを閉じるとスキップされます。

Select change calendars ▼

CloudWatch alarm - オプション

Add error control to this association by choosing a CloudWatch alarm.

Alarm name
The name of the CloudWatch alarm that you want to apply to this association. [Create CloudWatch alarm](#)

Choose alarm ▼

Continue association if alarm status is unavailable
If State Manager is unable to retrieve information about the state of your CloudWatch alarm, the association continues to run.

関連付けの作成

関連付けの設定項目

Command または Policy ドキュメント	Automation Runbook
名前	名前
ドキュメントおよびパラメーター	ドキュメントおよびパラメーター
ターゲット	Execution（ターゲットに関する設定）
スケジュール	スケジュール
コンプライアンスの重要度	-
変更カレンダー	変更カレンダー
レートの制御	レートの制御
S3出力	-
Cloud Watch アラーム	Cloud Watch アラーム

関連付けの設定項目 (Command / Policy ドキュメント固有の設定項目)

● コンプライアンスの重要度

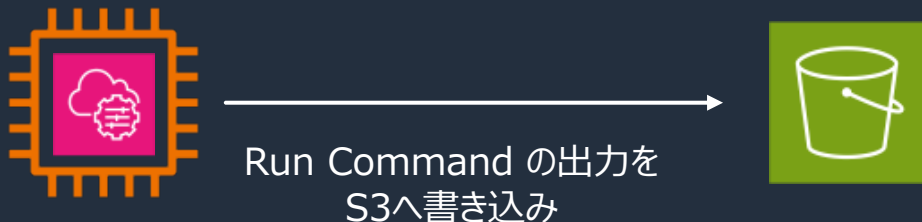
- ✓ Compliance のダッシュボード上に、関連付けの状態(準拠 or 非準拠)とともにここで指定した重要度 (非常事態/高い/ミディアム/低い) を表示する

コンプライアンスの重要度
関連付けのコンプライアンスの重要度を指定します。これはコンプライアンスダッシュボードに反映されます。

高い ▼

● S3 出力

- ✓ コマンド出力をS3上にファイルとして保存する



出力オプション

S3 への書き込み
すべてのコマンド出力を Amazon S3 バケットに書き込みます。コンソールでのコマンド出力は、2500 文字を超えると切り捨てられます。

S3 への出力の書き込みを有効にします

S3 バケット名
バケットの名前を指定します。

S3 キープレフィックス - 省略可能
出力を受け取るバケットのプレフィックス (たとえば、mycommands/domainjoin) を入力します。

関連付けの実行結果の確認

実行結果の確認 - State Manager のコンソール画面



関連 ID	関連付けの名前	ドキュメント名	最終実行日	ステータス	関連付けのバージョン	リソースのステータス数
b288296a-52d1-46f0-b698-3d09f6d04d57	AWS-QuickSetup-SSMHostMgmt-UpdateCloudWatchAgent-tb53k	UpdateCloudWatchDocument-tb53k	Wed, 17 May 2023 15:01:39 GMT	成功	1	Success:1
ba084271-08de-4502-b99b-6821b4cc4900	AWS-QuickSetup-SSMHostMgmt-AttachIAMToInstance-tb53k	AWSQuickSetup-CreateAndAttachIAMToInstance-tb53k	Tue, 25 Apr 2023 05:20:14 GMT	成功	1	Success:15
e8ce0d24-65d9-4b7e-81ce-dff0f400f5dd	AWS-QuickSetup-SSMHostMgmt-UpdateSSMAgent-tb53k	AWS-UpdateSSMAgent	Wed, 17 May 2023 14:02:34 GMT	成功	1	Success:2
eb37b0c6-85f9-4630-a05d-3a1142cd8883	AWS-QuickSetup-PatchPolicy-ScanForPatches-LA-tg37x	AWS-RunPatchBaseline	Mon, 22 May 2023 08:11:17 GMT	失敗	1	Failed:4
ff10e458-9f16-4729-b943-3ba9369a7949		AWS-GatherSoftwareInventory	Wed, 01 Feb 2023 06:25:45 GMT	成功	1	Skipped:1

- State Manager のマネジメントコンソールで、関連付けごとの状況をリスト表示または詳細表示で確認できる
- 詳細表示画面では過去の実行履歴を確認したり、関連付けを即時実行することが可能

Association ID: b288296a-52d1-46f0-b698-3d09f6d04d57

Apply association now Edit Delete

説明	リソース	パラメーター	ターゲット	バージョン	実行履歴
関連付けの実行					
検索					
実行 ID	関連付けのバージョン	ステータス	状況の詳細	作成日	リソースのステータス
34914338-e197-4a70-b7fb-061aa9f8bdca	1	成功	Success	Wed, 17 May 2023 14:31:36 GMT	Success:1
24c4abba-5221-4b39-ac09-716517ae3ea1	1	成功	Success	Tue, 25 Apr 2023 05:18:45 GMT	Success:2
477d9bb2-40d7-4718-a4f8-4313b3bfe00c	1	成功	Success	Sun, 26 Mar 2023 05:18:56 GMT	Success:1

実行結果の確認 - Compliance のコンソール画面



- Compliance は AWS Systems Manager の一機能
- 以下の情報をコンプライアンスデータとして収集・表示することができる
 - Patch Manager によるパッチ適用のステータス
 - State Manager の関連付けに関するデータ
 - マネージドノードに対して指定したカスタムコンプライアンスタイプ

AWS Systems Manager > コンプライアンス

コンプライアンスダッシュボードのフィルタリング

ダッシュボードの結果をグループ化する条件

コンプライアンスタイプ パッチグループ リソースグループ

さらにフィルタ リソース ルール

コンプライアンスリソースの概要

コンプライアンスタイプ	準拠リソース	非準拠リソース	重要なリソース	高リソース	中リソース	低リソース	情報リソース	未指定リソース
Association	2	0	0	0	0	0	0	0
Patch	2	0	0	0	0	0	0	0

Compliance ダッシュボードでサマリーを確認

- ステータスが準拠／非準拠のマネージドノード数
- ステータスが準拠／非準拠の関連付けの数

TIPS



AWS Config で関連付けのコンプライアンス履歴を追跡

- AWS Config で State Manager の関連付けのコンプライアンス履歴と変更の追跡を表示可能
- AWS Config の記録対象として「**SSM:AssociationCompliance**」のリソースタイプを有効にしておく必要がある

イベント
すべての時刻 Asia/Tokyo (UTC+09:00)

開始日 2023/06/07 今すぐ

イベントタイプ すべてのイベントタイプ ▼

2023年6月7日

18:12:13	☑ ルールのコンプライアンス	⚠ 2 非準拠ルール	2 適用されたルール
18:11:58	☑ 設定変更		4 フィールドの変更
14:22:17	☑ 設定変更		1 フィールドの変更

2023年6月6日

14:22:19	☑ ルールのコンプライアンス	🟢 すべて準拠	2 適用されたルール
14:22:06	☑ 設定変更		5 フィールドの変更

マルチアカウント・マルチリージョン 実行

- ドキュメントタイプが Automation Runbook の場合、クロスアカウント・クロスリージョンでの関連付けの実行が可能
- マネジメントコンソールでは操作できないため、AWS CLI/AWS SDK から関連付けを作成する必要がある

```
aws ssm create-association \  
--association-name association name \  
--targets Key=ResourceGroup,Values=resource group name \  
--name runbook name \  
--parameters AutomationAssumeRole=arn:aws:iam::123456789012:role/RunbookAssumeRole \  
--automation-target-parameter-name target parameter \  
--schedule "cron or rate expression" \  
--target-locations Accounts=111122223333,444455556666,444455556666,Regions=region,region
```

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/scheduling-automations-state-manager-associations.html#create-automation-association-cli

構成管理ツールとの連携例

- **AWS-ApplyAnsiblePlaybooks SSM ドキュメント**

State Manager の関連付け経由で Ansible プレイブックを実行する

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/systems-manager-state-manager-ansible.html

- **AWS-ApplyChefRecipes SSM ドキュメント**

State Manager の関連付け経由で Chef recipe を実行する

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/systems-manager-state-manager-chef.html

- **AWS-ApplyDSCMofs SSM ドキュメント**

Windows PowerShell Desired State Configuration (PowerShell DSC) の Managed Object Format (MOF) ファイルを State Manager の関連付け経由で実行する

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/systems-manager-state-manager-using-mof-file.html

まとめ

まとめ

Systems Manager State Manager の特徴

- State Manager は安全でスケーラブルな設定管理サービス
- マネージドノードおよび他の AWS リソースを定義された状態に保つプロセスを自動化
- Systems Manager Inventory で利用されるほか、Command ドキュメントや Automation Runbook の定期実行も可能

本資料に関するお問い合わせ・ご感想

技術的な内容に関しましては、有料のAWSサポート窓口へお問い合わせください

<https://aws.amazon.com/jp/premiumsupport/>

料金面でのお問い合わせに関しましては、カスタマーサポート窓口へお問い合わせください（マネジメントコンソールへのログインが必要です）

<https://console.aws.amazon.com/support/home#/case/create?issueType=customer-service>

具体的な案件に対する構成相談は、後述する個別相談会をご活用ください



ご感想はTwitterへ！ハッシュタグは以下をご利用ください
#awsblackbelt

その他コンテンツのご紹介

ウェビナーなど、AWSのイベントスケジュールをご参照いただけます

<https://aws.amazon.com/jp/events/>

ハンズオンコンテンツ

<https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-hands-on/>

AWS 個別相談会

AWSのソリューションアーキテクトと直接会話いただけます

<https://pages.awscloud.com/JAPAN-event-SP-Weekly-Sales-Consulting-Seminar-2021-reg-event.html>



Thank you!