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=PLzWGOASvSx6FIwIC2X1nObr1KcMCBBlqY

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います。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。

本日お話ししないこと

- 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

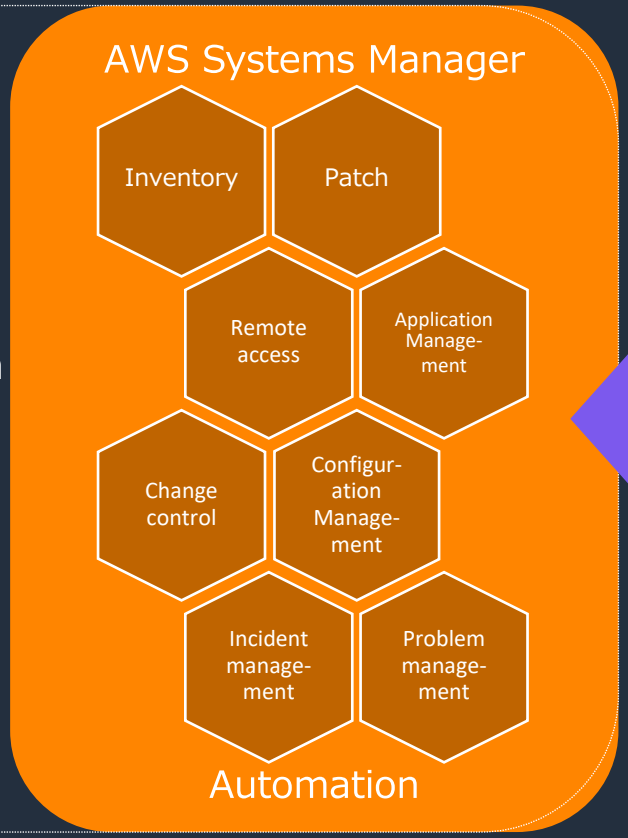
ハイブリッドクラウド環境のための安全なエンドツーエンドの管理ソリューション

AWS Config
Configuration history

Amazon EventBridge
Notification and remediation

AWS CloudTrail
Audited actions

AWS Identity and Access Management (IAM)
Role-based access control



Integration connectors and APIs

- Third-party tools
- ITSM
- Custom solutions

AWS の他のサービスや
3rd Party のツールと統合された
管理ソリューションを提供

Cloud On-premises Edge

(*) AWS Systems Manager = SSM と略します。

AWS Systems Manager の機能

運用管理	アプリケーション管理	変更管理	ノード管理
Explorer	Application Manager	Change Manager	Fleet Manager
OpsCenter	AppConfig	Automation	Session Manager
Incident Manager	Parameter Store	Maintenance Windows	Inventory
		Change Calendar	Run Command
			Patch Manager
			Distributor
			State Manager

Quick Setup

AWS Systems Manager の機能

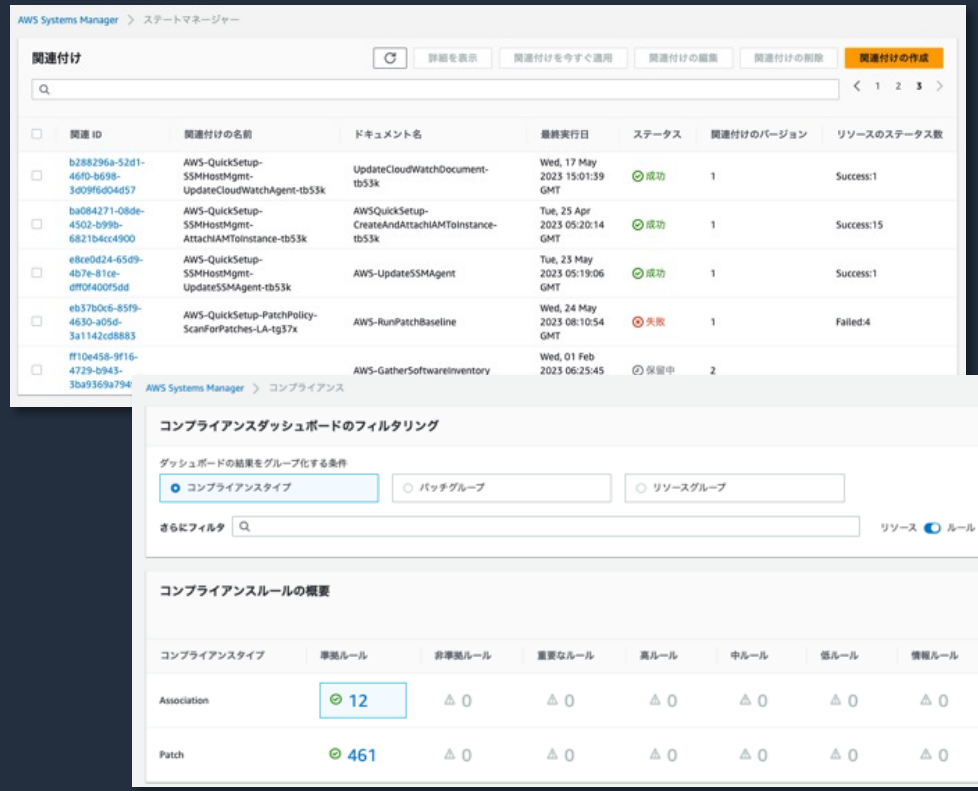
運用管理	アプリケーション管理	変更管理	ノード管理
Explorer	Application Manager	Change Manager	Fleet Manager
OpsCenter	AppConfig	Automation	Session Manager
Incident Manager	Parameter Store	Maintenance Windows	Inventory
		Change Calendar	Run Command
			Patch Manager
			Distributor
			State Manager

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



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
- Microsft 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「タイムウインドウ」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 Fucntions の実行をサポート

時間的制約のあるタスクを
タイムウイ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

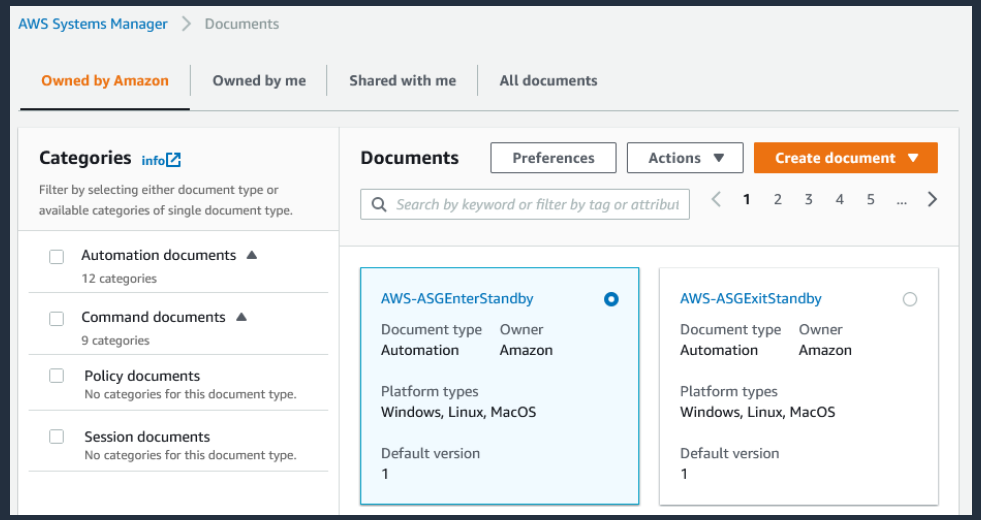
”定義された状態”を維持する
対象リソース

※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"]
   }
  }
 ]
}
```

ドキュメントについて詳細は[こちら]

State Manager がサポートするドキュメントタイプ

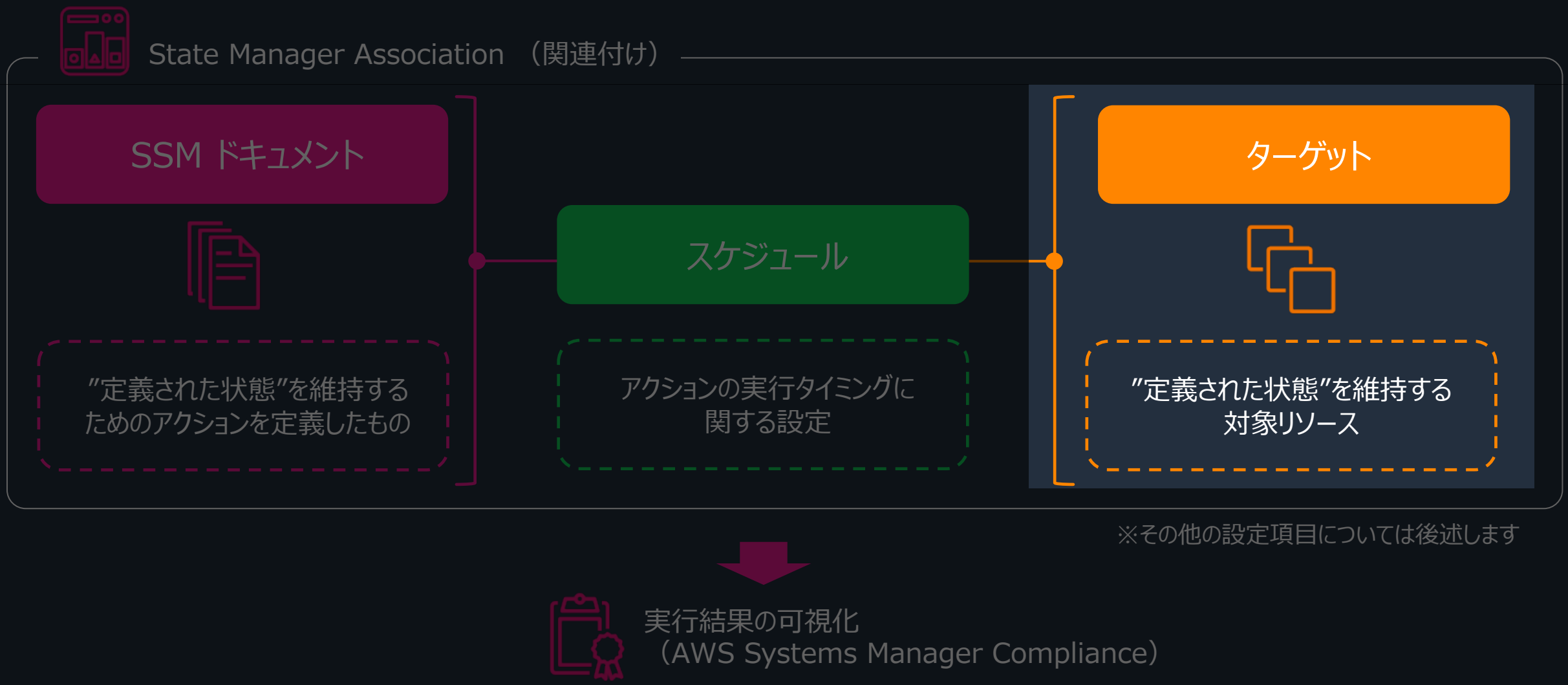
以下の 3 つのドキュメントタイプをサポート

Type	Usage with	主な用途
Automation (Runbook)	✓ Automation	• 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	• マネージドノード上で実行するコマンドを定義
Policy	✓ Inventory	• 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。

全てのドキュメントタイプはこちら

State Manager の主要な構成要素



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

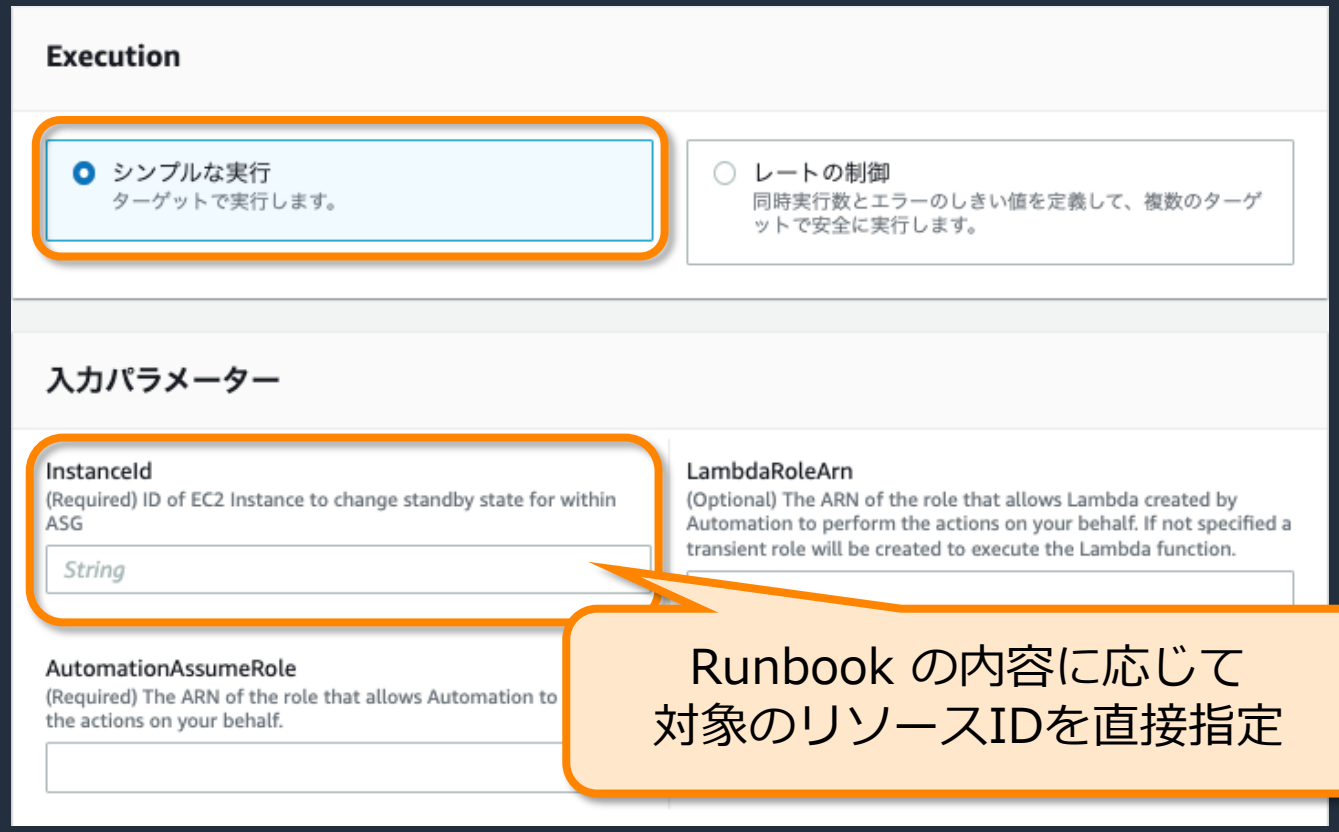
- タグ指定
- ノードを手動で選択
- リソースグループ指定
- すべてのマネージドノード

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



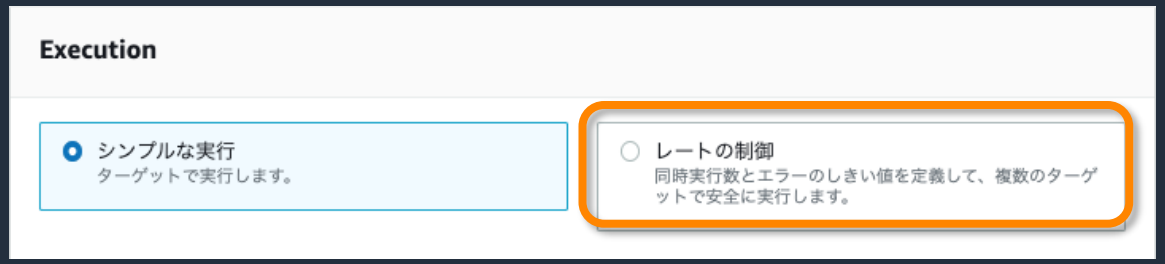
※入力パラメーターは一例です。実際は Runbook の内容によって変わります

ターゲットの指定方法

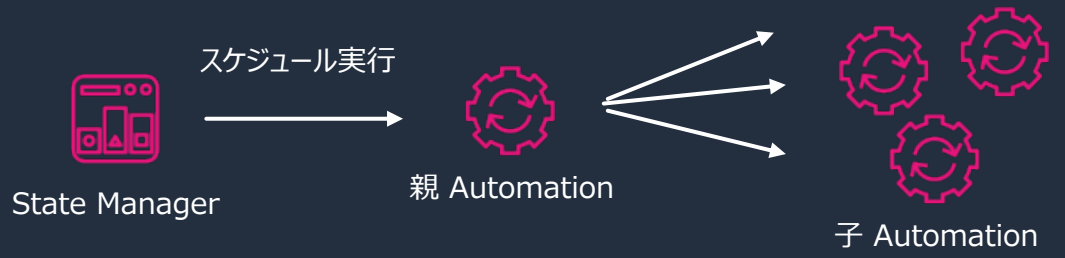
Automation Runbook の場合

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



- 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

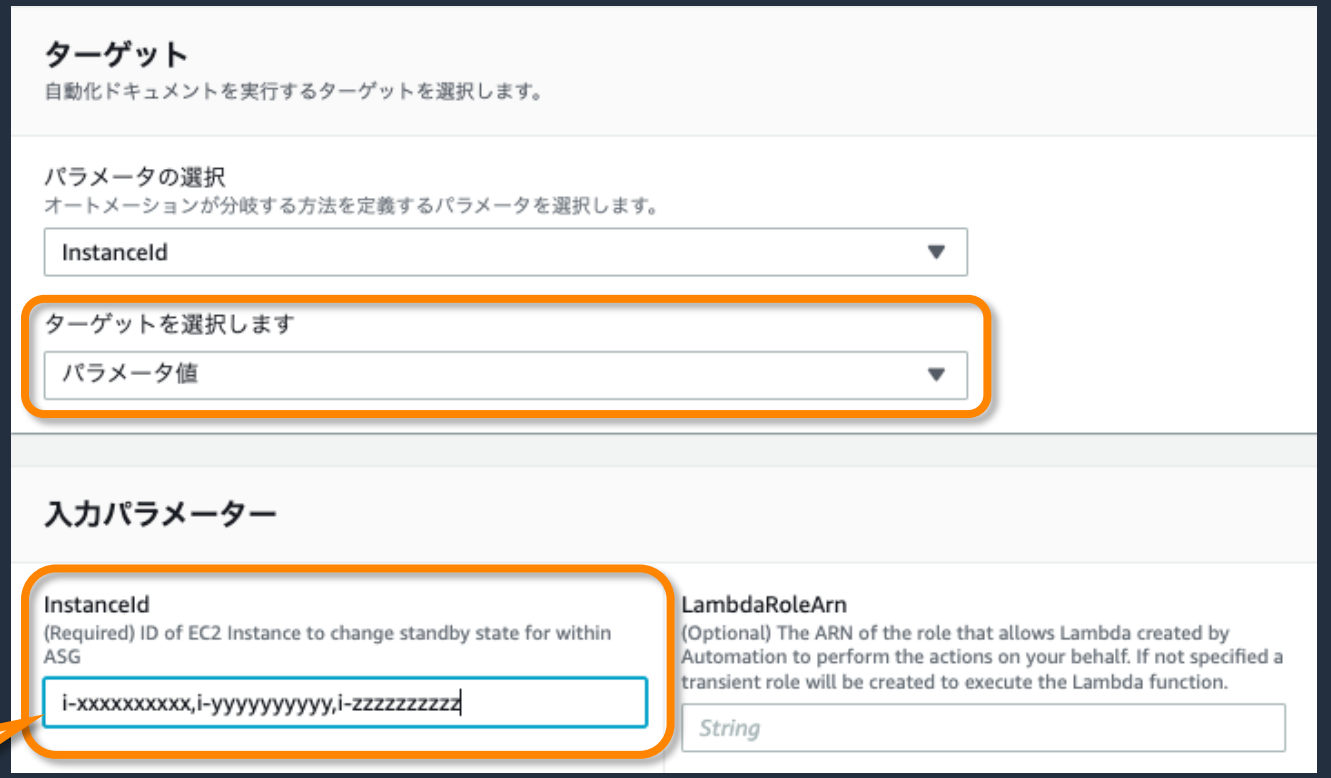
子 Automation の 3 に連携する

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



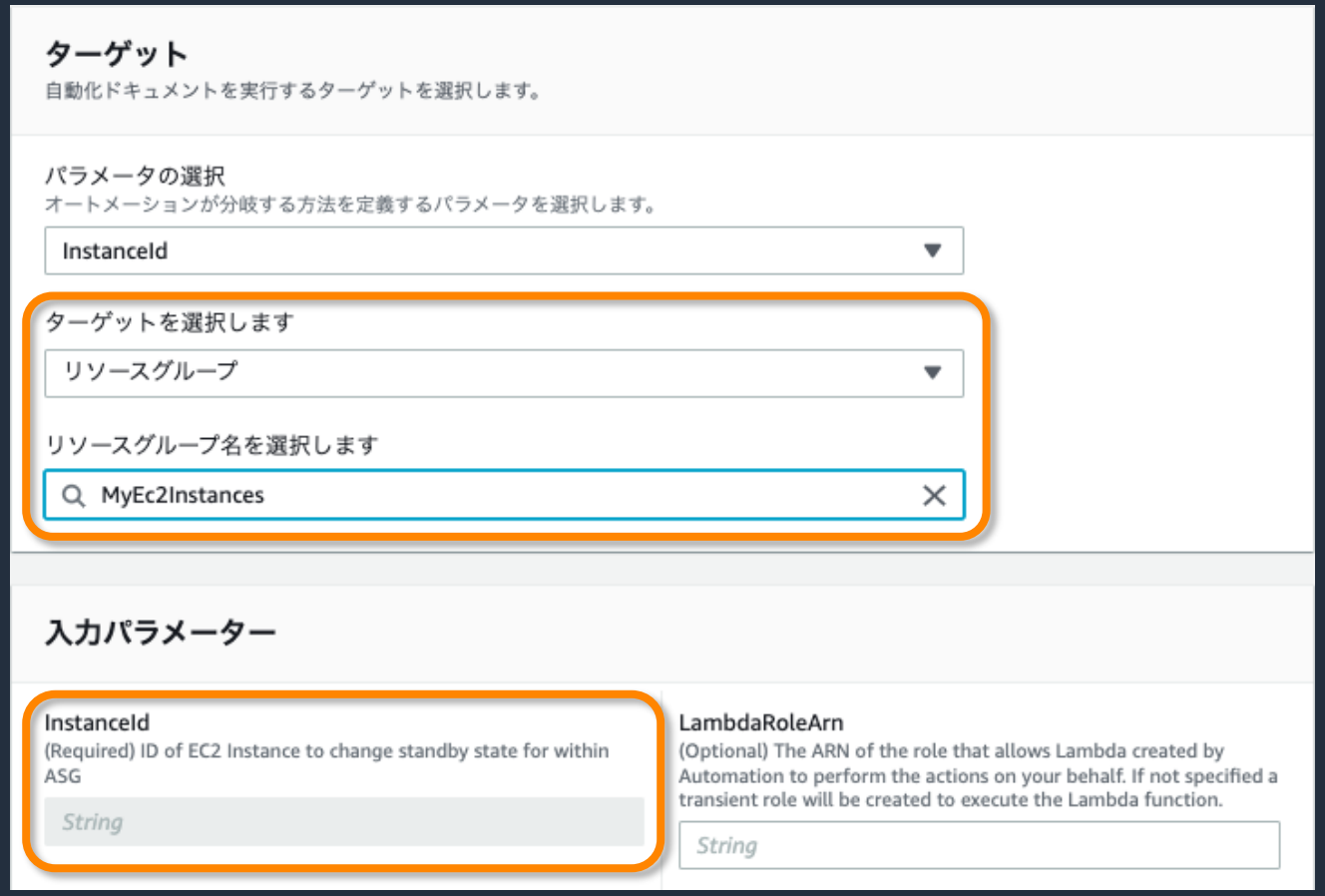
カンマ区切りで複数の
リソースの情報を指定可能

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**

同時実行数とエラーしきい値　（Command/ Policy /Automation 共通）

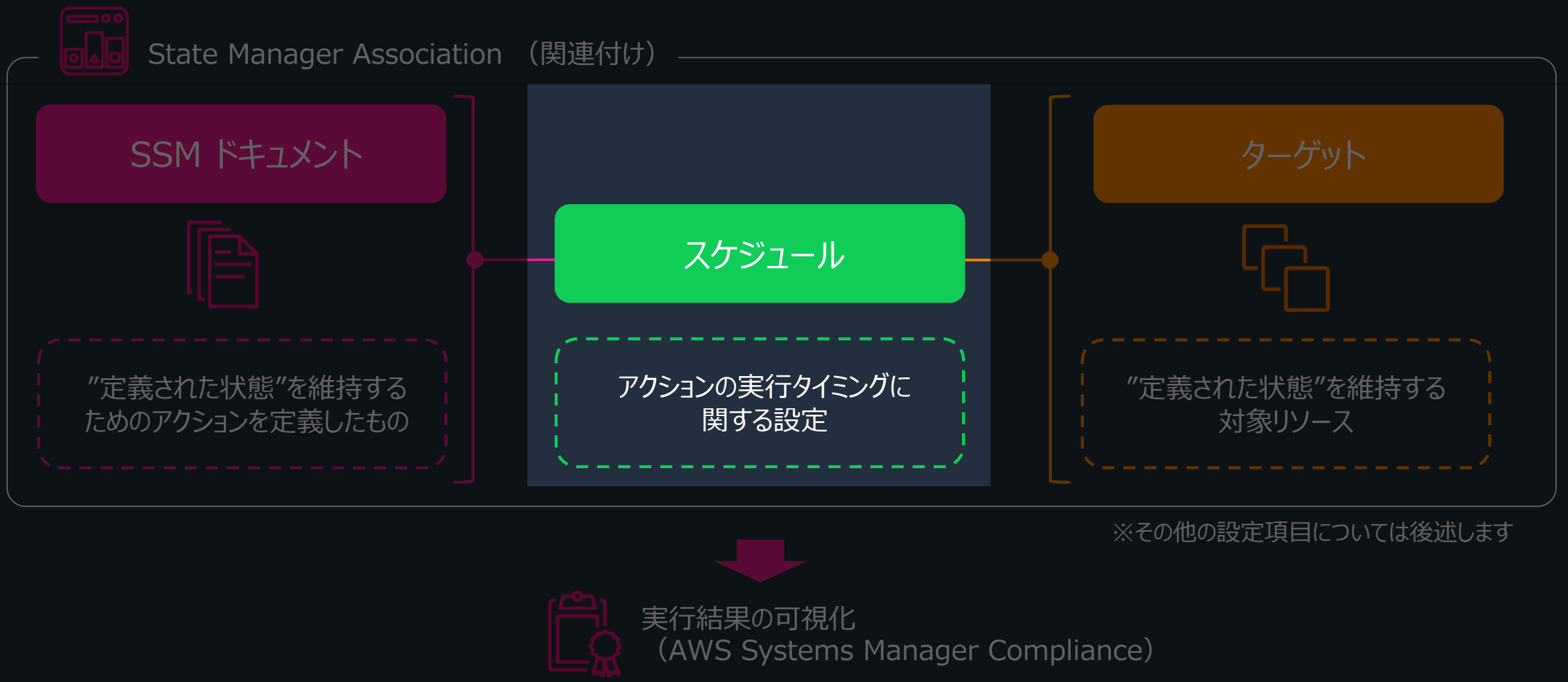
同時実行性

- 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



スケジュールの指定方法

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
  - 対象インスタンスが初めてオンラインになる
  - スケジュールを逃した後、インスタン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

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

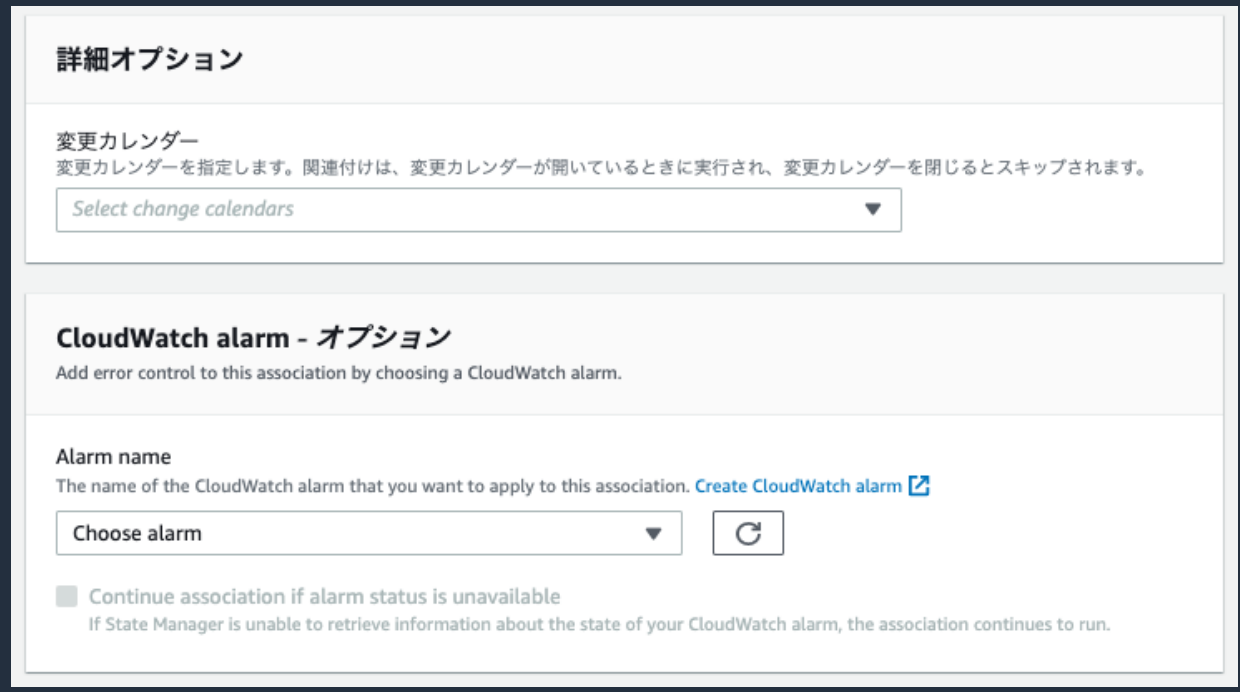
関連付けの実行タイミングの制御に関する 2 つのオプション

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



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

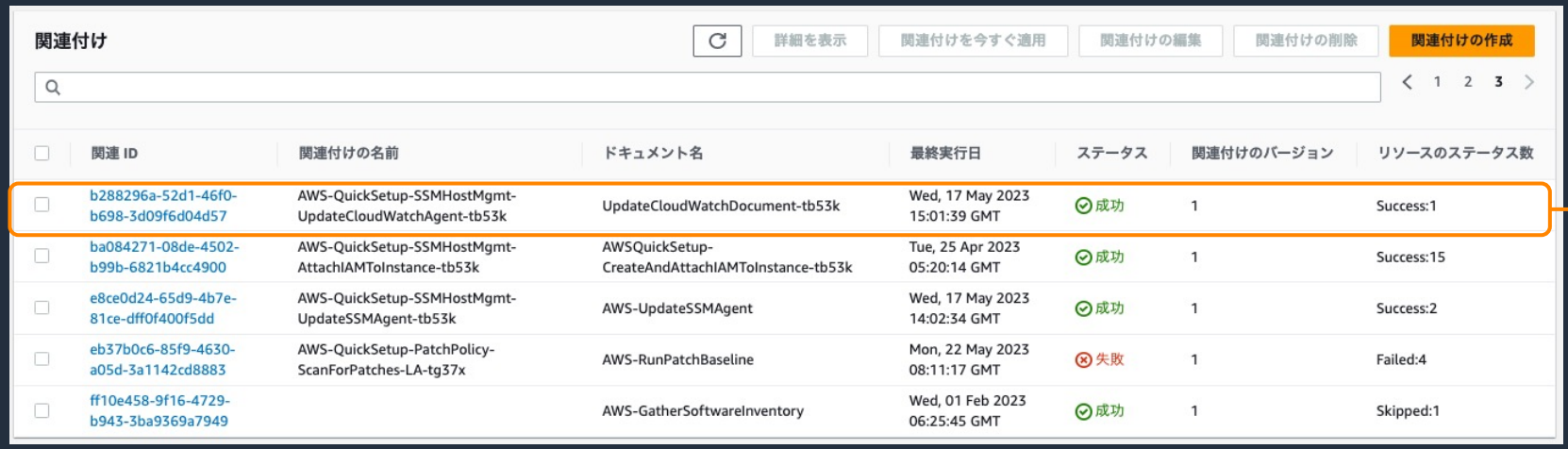
関連付けの設定項目　（Command / Policy ドキュメント固有の設定項目）

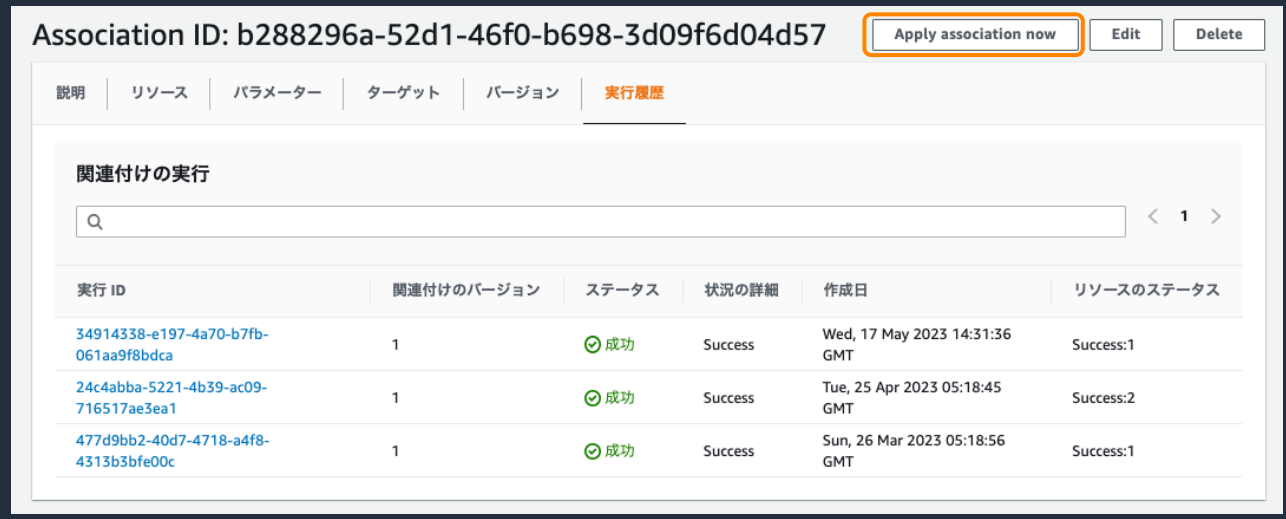
- コンプライアンスの重要度
  - ✓ Compliance のダッシュボード上に、関連付けの状態(準拠 or 非準拠)とともにここで指定した重要度（非常事態/高い/ミディアム/低い）を表示する

- S3 出力
  - ✓ コマンド出力をS3上にファイルとして保存する

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





- 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

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

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

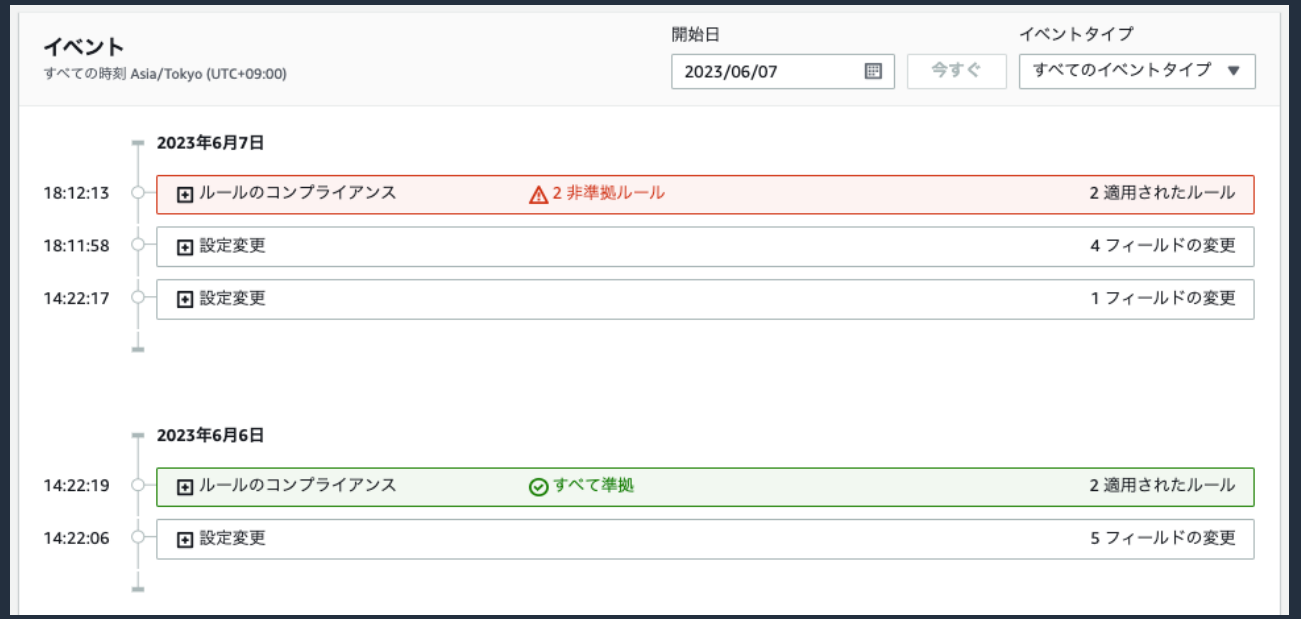
Compliance ダッシュボードでサマリーを確認

- 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



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

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!