



AWS Systems Manager Overview

AWS Black Belt Online Seminar

石橋 香代子

Senior Solutions Architect
2023/02

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02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：石橋 香代子

所属：エンタープライズ技術本部
小売・消費財ソリューション部

経歴：-2018/06 @外資SIer
2018/07- ソリューションアーキテクト @AWS
• 小売・消費財のお客様を担当
• Cloud Operations サービスの推進も



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 の全体像をご理解いただく。
- AWS Systems Manager の各機能の概要を掴んでいただき、どんなことができるのか、イメージを持っていただく。

本日お話ししないこと

- AWS Systems Manager の各機能の詳細
- 今後公開を予定している、各機能にフォーカスしたセッションをお待ちください。

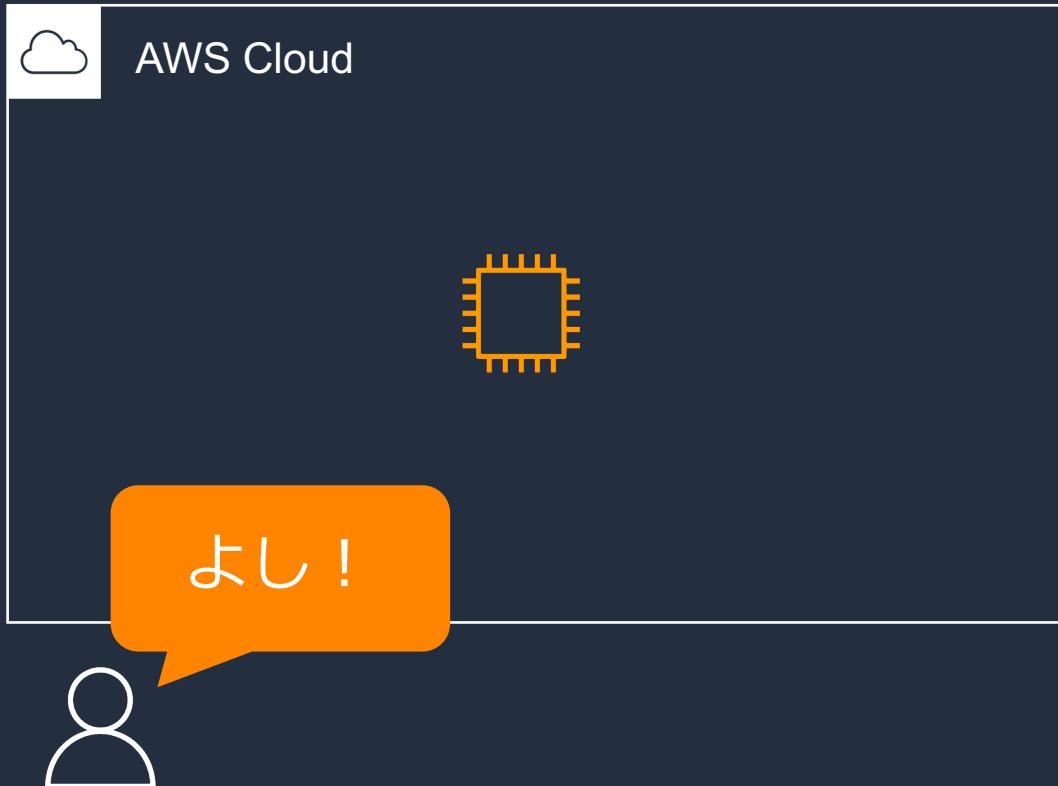
アジェンダ

1. 運用管理における課題と AWS Systems Manager
2. AWS Systems Manager を使うには？
3. AWS Systems Manager で始める運用管理
4. 3rd Party の ITSM ツールとの連携
5. まとめ

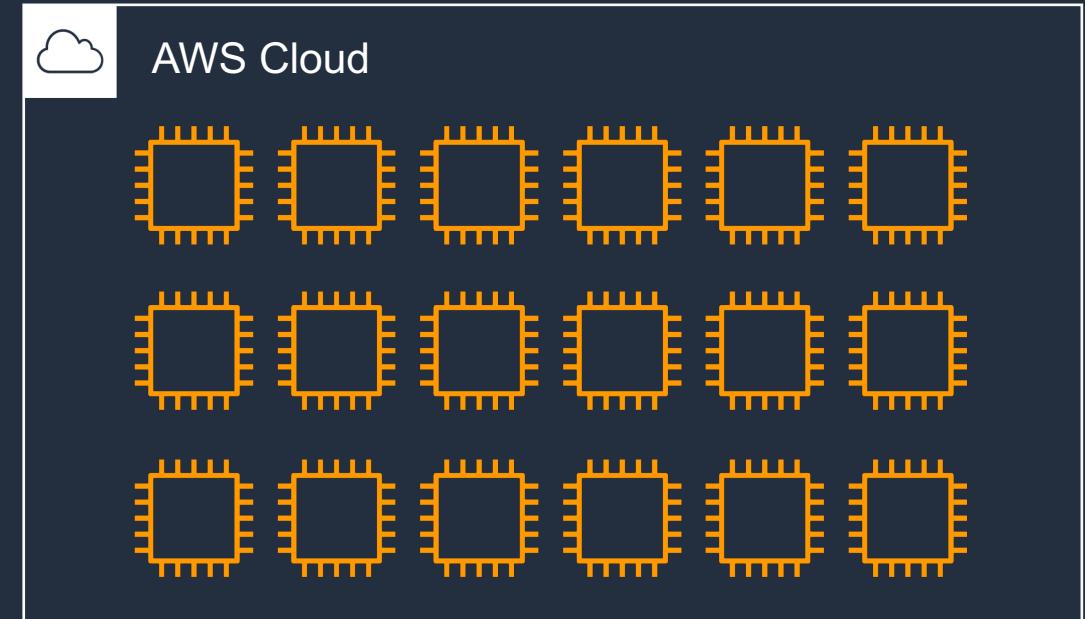
運用管理における課題と AWS Systems Manager

運用管理における課題

使い始め

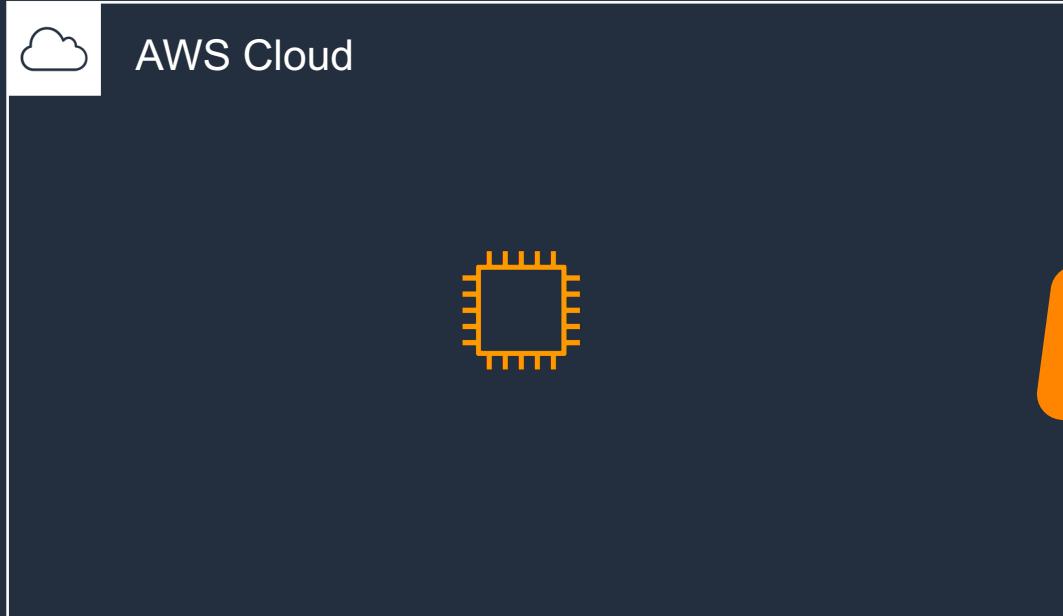


利用が進むと

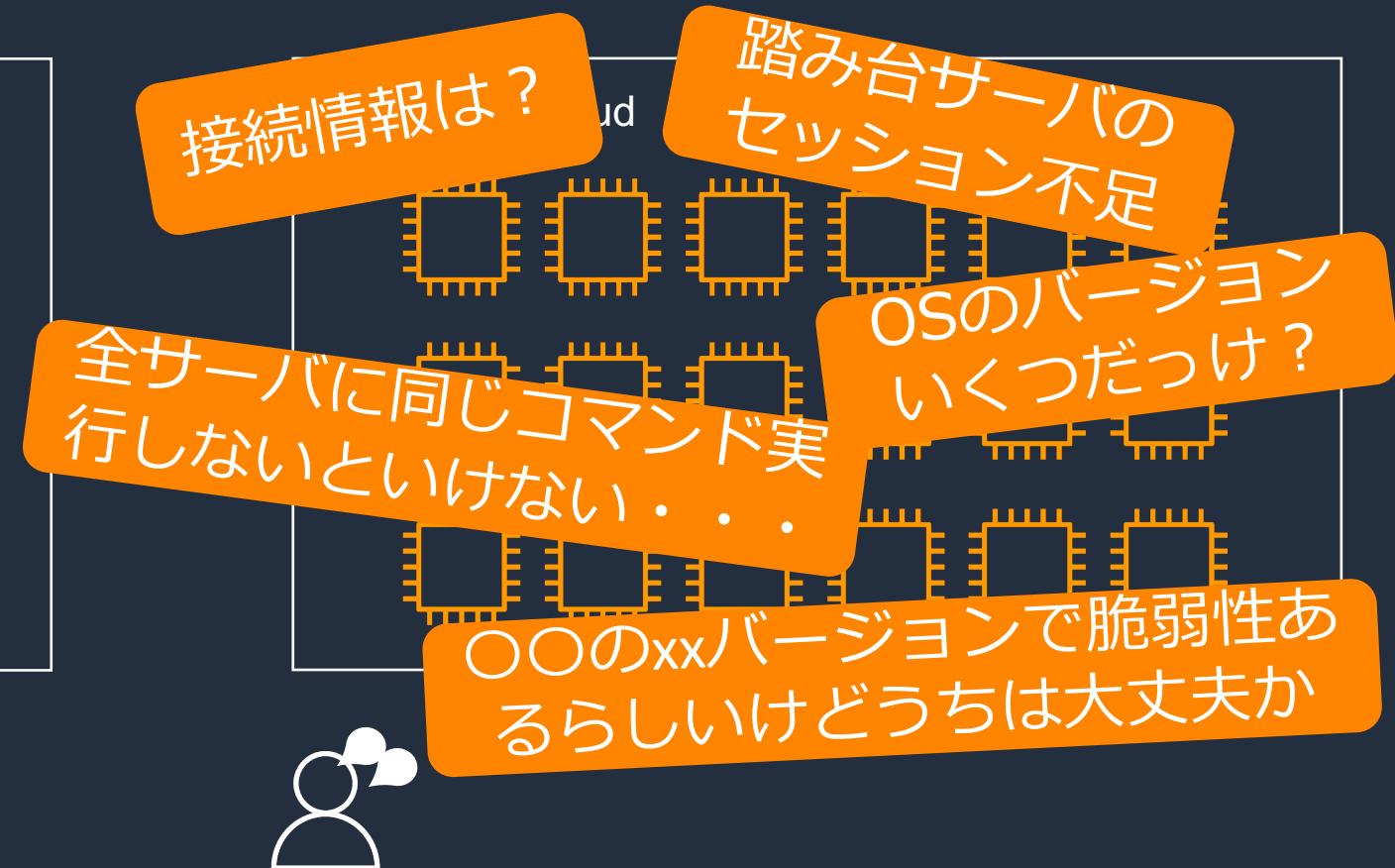


運用管理における課題

使い始め

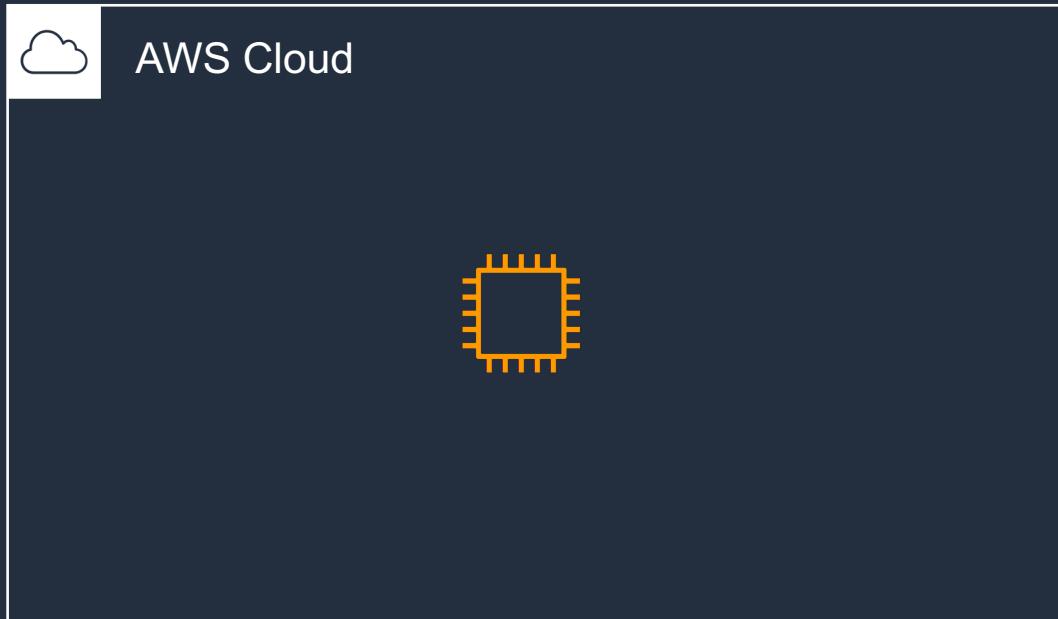


利用が進むと



運用管理における課題

使い始め

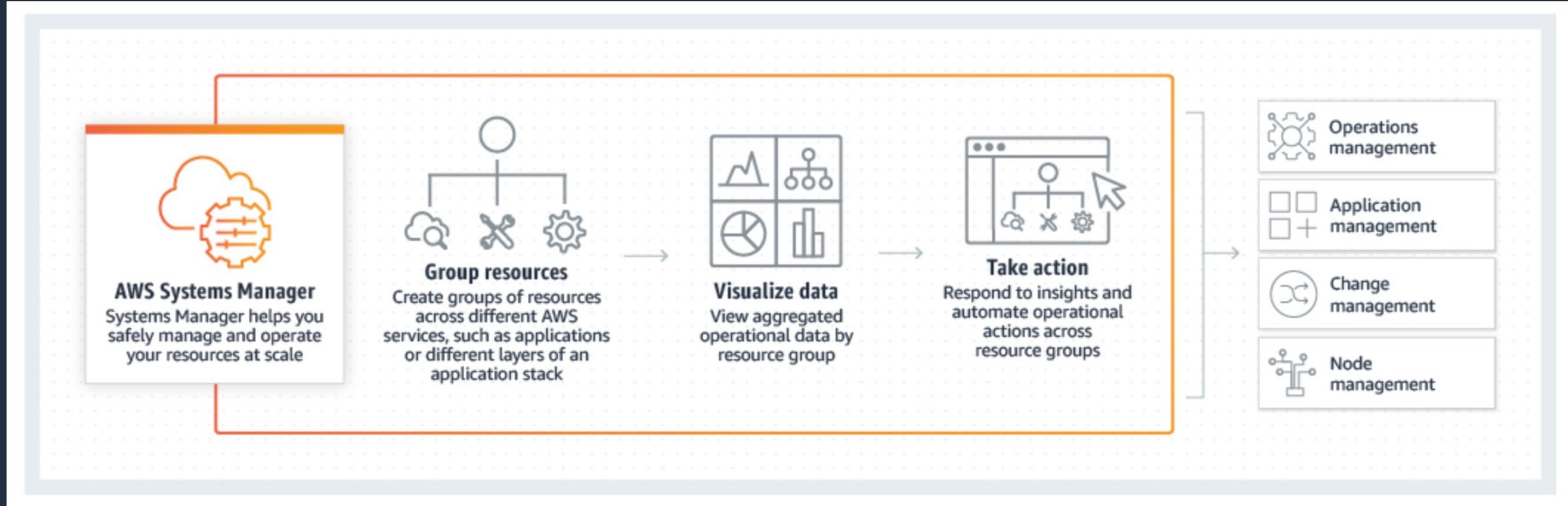


利用が進むと



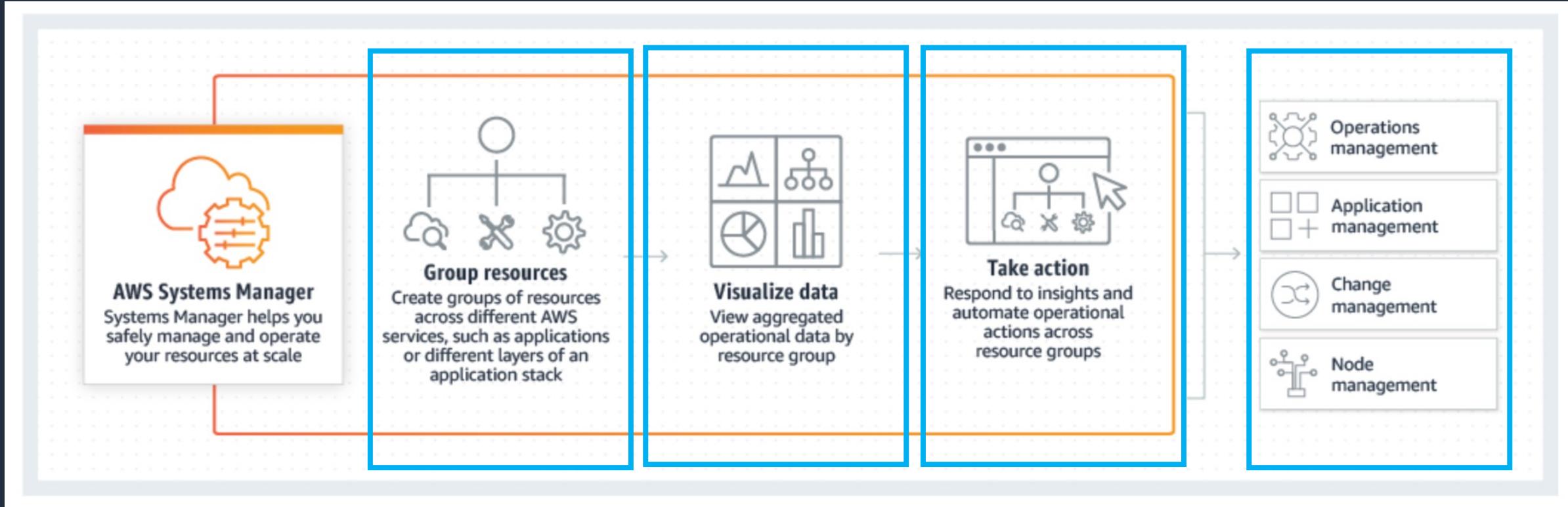
AWS Systems Manager (SSM) とは

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) とは

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) とは



AWS Config
Configuration history



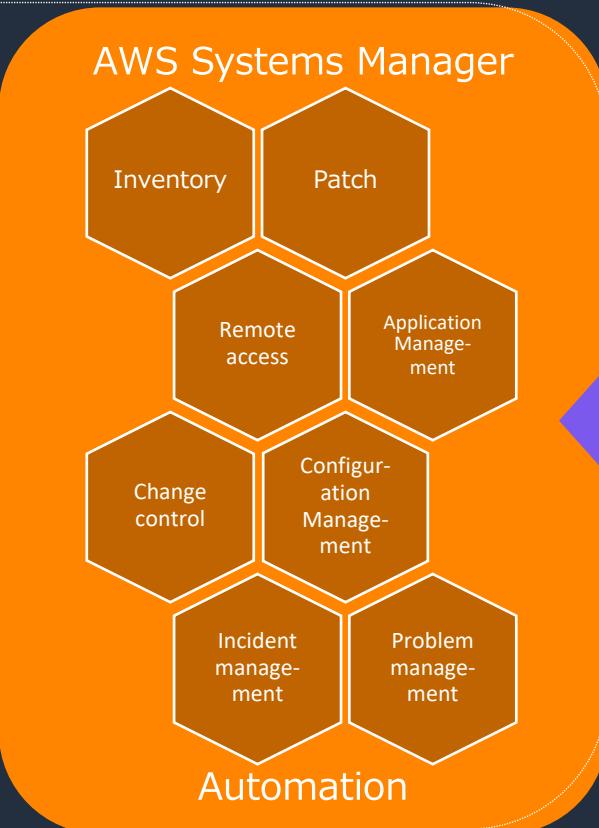
Amazon EventBridge
Notification and remediation



AWS CloudTrail
Audited actions



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



Cloud



On-premises



Edge

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

(*) 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 を使うには？

AWS Systems Manager を使ってサーバ管理を行うためには

サーバを“マネージドノード”にする

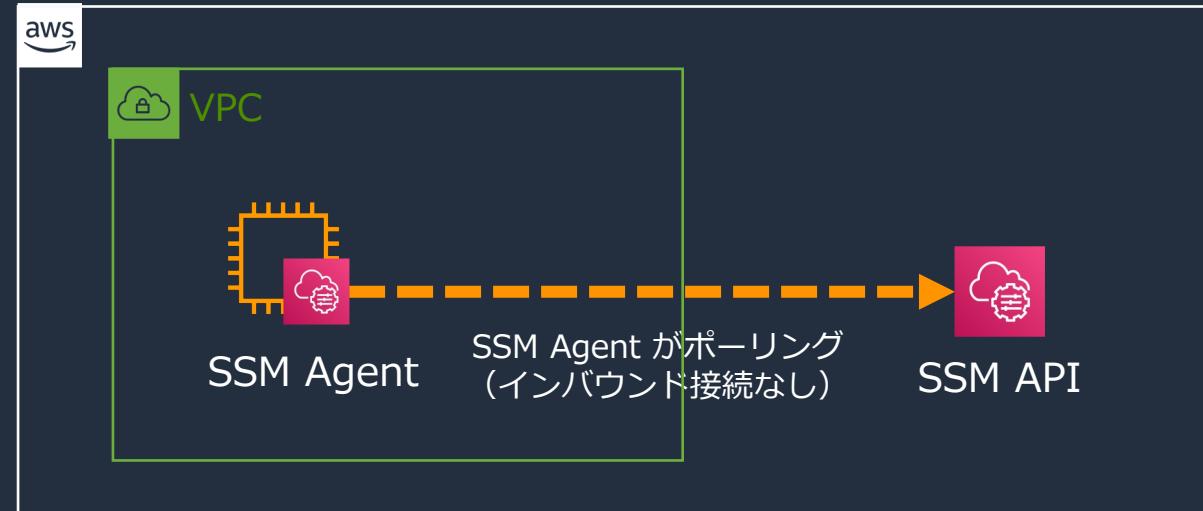
ここに一覧で出てくるようになります

□	ノード ID	ノードの... ▾	ノード名	プラット... ▾	オペレーティ... ▾	ソースタイプ	ソ...
□	i-04970a7f373ac630b	実行中	LaunchedByS...	Linux	Amazon Linux AMI	EC2 インスタンス	-
□	mi-0623bfeef040aa8...	-	On-perm-Linux	Linux	Amazon Linux	AWS::SSM::Manage...	-
□	i-016d04a4ae49531af	実行中	instance-ph@	Linux	Amazon Linux	EC2 インスタンス	-

マネージドノード：
➤ SSM管理下のインスタンス群
➤ EC2インスタンスのほか、
オンプレミスのインスタンスも
含まれられる。

マネージドノードにするために ①SSM Agent の導入

- SSM Agent が Systems Manager と連携し各種操作、コントロールを行う。
- Amazon Linux やWindows、Ubuntu などの一部のオフィシャルイメージ(AMIs) には導入済み
 - プリインストールされたAMIsの一覧は[こちら](#)
- それ以外のAMI、及びオンプレミスサーバは、手動でインストール



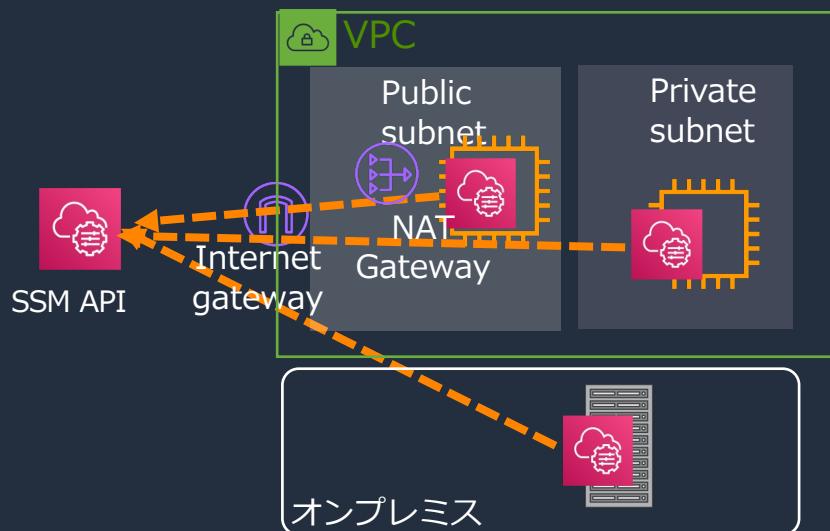
aws SSMS Agent の詳細は[こちら](#)

マネージドノードにするために ②アウトバウンド経路確保

- 以下 2 パターンのどちらかで、SSM Agent からのアウトバウンド経路を確保する。
- インバウンドアクセスは不要

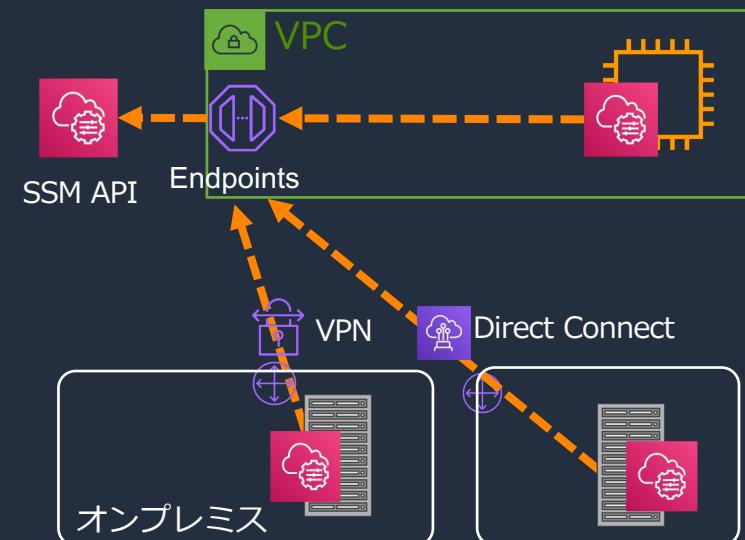
1. インターネット経由

- ・パブリックサブネットや
NAT Gateway を使用



2. VPC エンドポイント経由

- ・プライベートネットワークによる接続が可能
- ・オンプレミスからも AWS Direct Connect や
VPN 経由で閉域網経由のアクセスが可能



マネージドノードにするために ③権限付与

- Systems Manager に接続するための権限を付与する。
付与方法は以下の二通り。
- (方法 1) Systems Manager の管理下におきたい EC2 に明示的に付与 (従来の方法)
 - IAM ロールを作成し、EC2 にアタッチする。
 - 1, IAMポリシーについては、まず「AmazonSSMManagedInstanceCore」でコア機能をアタッチ(必須)
 - 2, 必要に応じて、S3などのポリシーをアタッチ(option)
- (方法 2) 「デフォルトのホスト管理設定(DHMC)」を有効にし、アカウント内の全 EC2 を自動で管理下にする。 (次ページ)



デフォルトのホスト管理設定

Default Host Management Configuration (DHMC)



- 明示的に EC2 にロール付与せずとも、 Systems Manager がアカウント内のすべてのインスタンスを管理する権限を持つようにできる機能
 - 設定は、アカウントごと、リージョンごとの単位
 - DHMC で指定したロールを SSM Agent が使用する。
 - デフォルトで「AWSSystemsManagerDefaultEC2InstanceManagementRole」が用意
 - EC2 にロールがアタッチされている場合には、 SSM Agent はまずそれを使用しようとする。
- 対象の EC2 は、以下が前提
 - SSM Agent は Ver.3.2.582.0 以降がインストールされていること
 - Instance Metadata Service Version 2 (IMDSv2) が有効化されていること

この機能により、自動で全インスタンスをマネージドノードにすることが可能に！



DHMCについての詳細は[こちら](#)

© 2023, Amazon Web Services, Inc. or its affiliates.

マネージドノードまでの 3ステップ まとめ



1、SSM Agentの導入

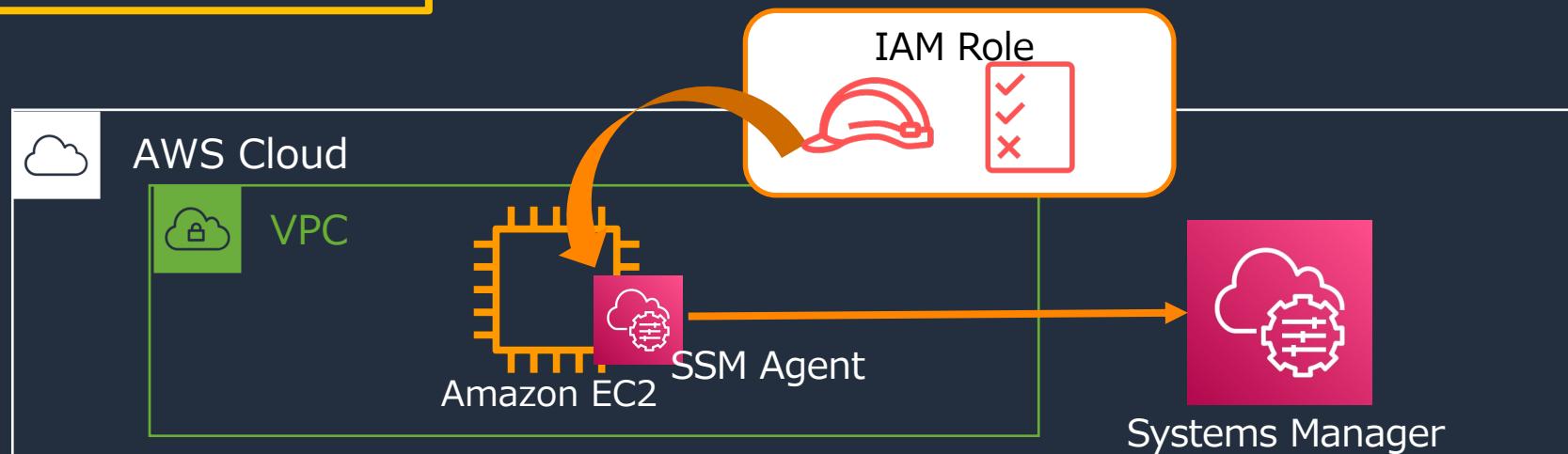
- ✓ SSM Agent が Systems Manager と連携して動作する
- ✓ 一部のオフィシャルイメージにはプリインストール済み

2、アウトバウンド経路の確保

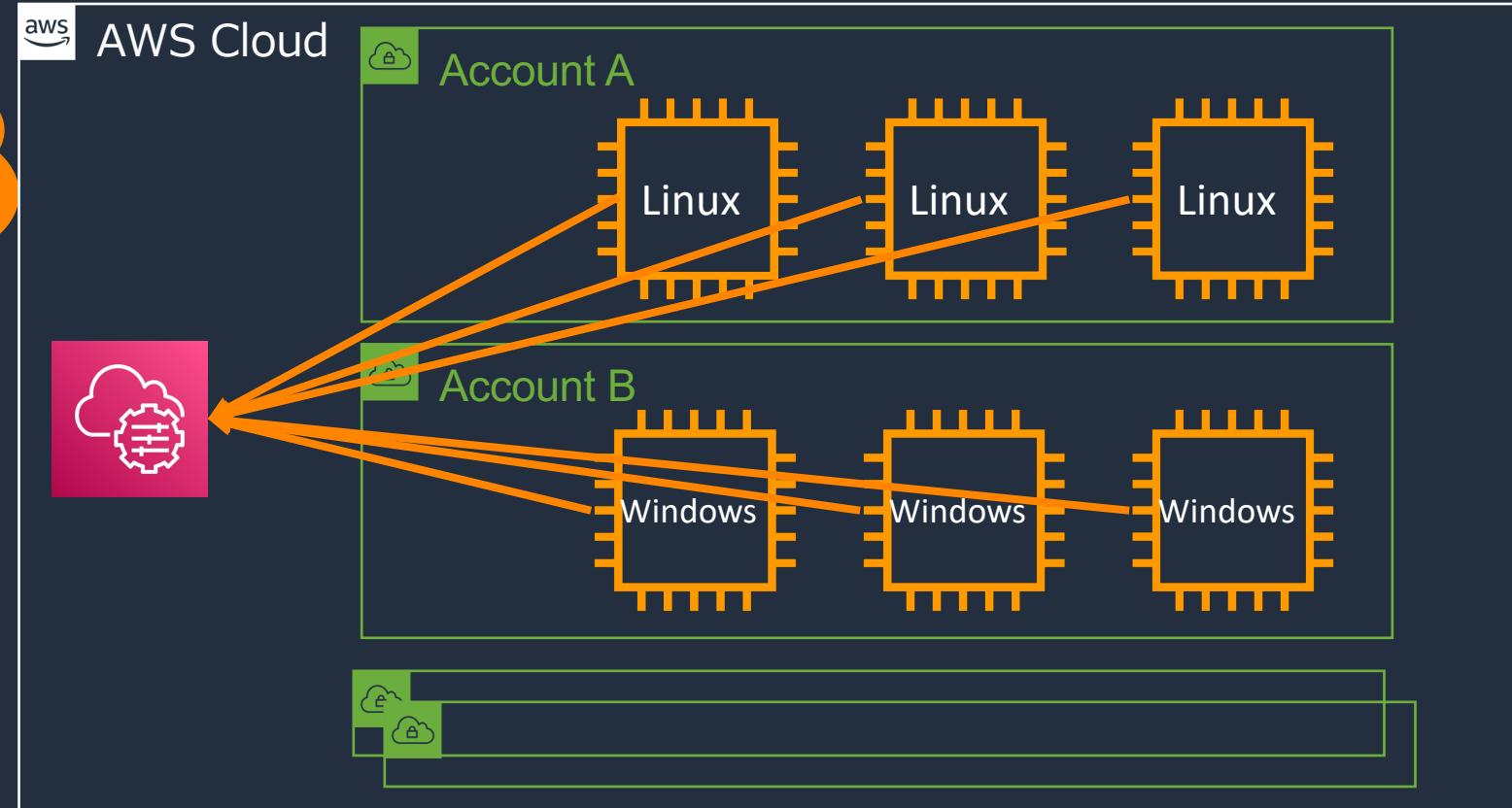
- ✓ インターネット 経由
- ✓ Or VPC Endpoint 経由 (閉域でのアクセスも可能)

3、Systems Manager 権限の付与

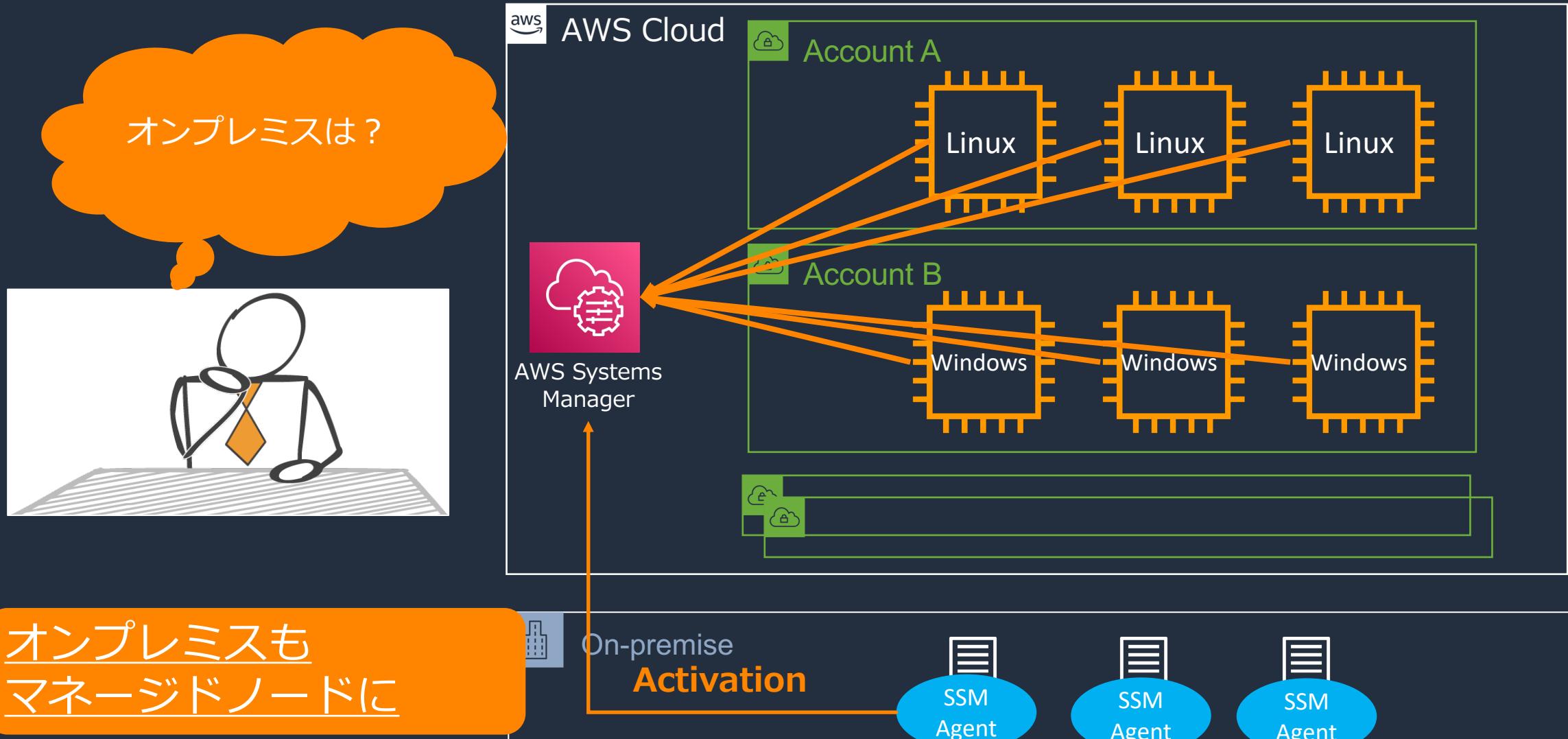
- ✓ 管理下におきたい EC2 に明示的にロールを付与
- ✓ Or DHMC を有効にして、アカウント内の全インスタンスを自動で管理下に



ここまでやれば、晴れてマネージドノードに！

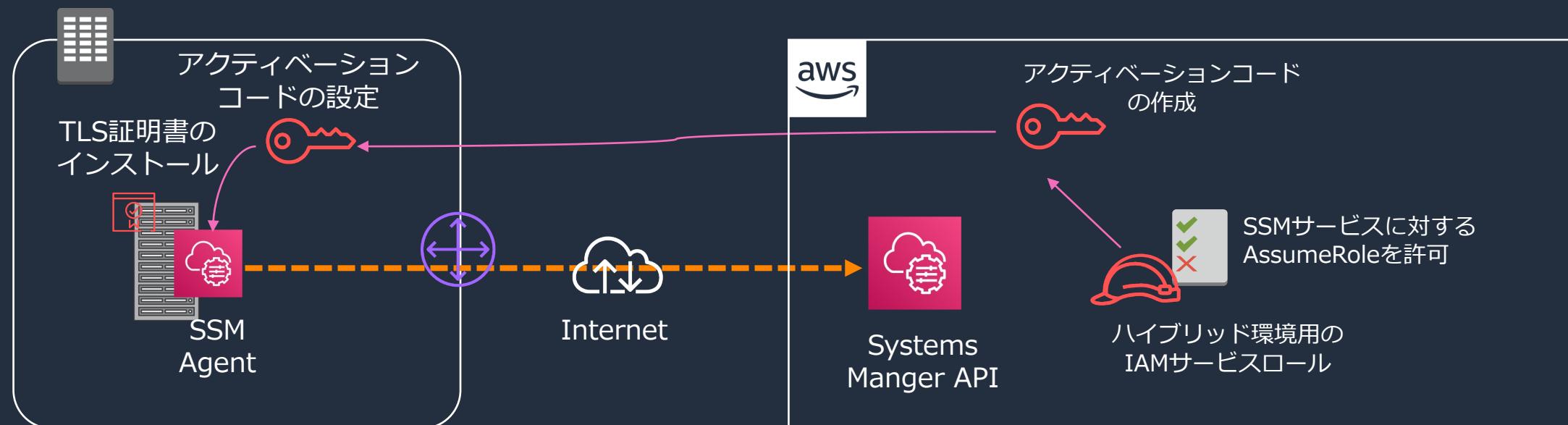


ここまでやれば、晴れてマネージドノードに！



オンプレミスのサーバをマネージドノードにするには

1. (Option) TLS 証明書のインストール
2. ハイブリッド環境用の IAM ロールを作成 (初回のみ)
3. SSM でアクティベーションコードを生成
4. インスタンスにアクティベーションコードを設定



aws ハイブリッド環境での設定の詳細は[こちら](#)

AWS Systems Manager で始める 運用管理



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

Systems Manager Fundamentals

Systems Manager Agent (SSM Agent)



- 任意のノードをリモートで管理
 - EC2 インスタンス
 - IoT Greengrass を使用したエッジデバイス
 - オンプレミスや他のクラウドサーバ、VMs
- Linux, macOS, Raspberry Pi, Windows Server をサポート
 - サポート OS の一覧は[こちら](#)
 - Amazon Linux やWindows、Ubuntu などの一部のオフィシャルイメージには導入済み。プリインストールされた AMIs の一覧は[こちら](#)
- SSM Agent は、SYSTEM (Windows) 、 root (Linux) で稼働
- SSM Agent はオープンソース。[GitHub](#)にて公開されている

Systems Manager ドキュメント (1/3)

- 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

The screenshot shows the AWS Systems Manager Documents interface. On the left, there's a sidebar with categories like Automation documents, Command documents, Policy documents, and Session documents. The main area displays two documents: 'AWS-ASGEnterStandby' and 'AWS-ASGEExitStandby'. Both documents are listed under the 'Automation' category and are owned by Amazon. They support Windows, Linux, and MacOS platforms. The 'AWS-ASGEnterStandby' document is currently selected.

aws ドキュメントについて詳細は[こちら](#)

© 2023, Amazon Web Services, Inc. or its affiliates.

```
{  
  "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"]  
      }  
    }  
  ]  
}
```

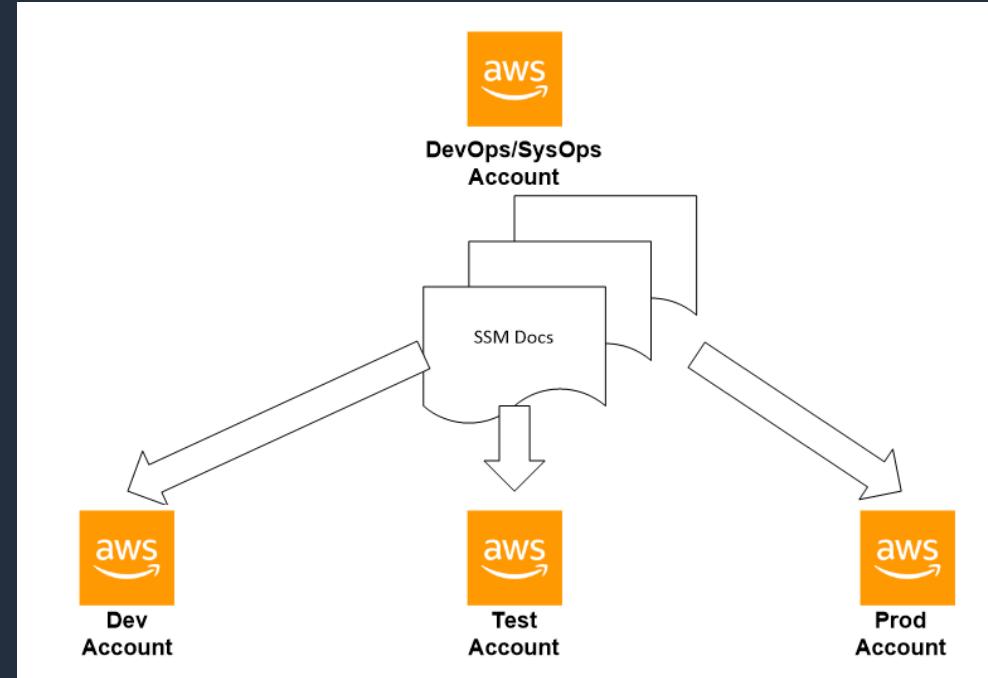
Systems Manager ドキュメント (2/3)

- ・主なドキュメントタイプ

Type	Usage with	Usage with
Automation (runbook)	✓ Automation	Automation runbook として 自動化ワークフローを定義
Command	✓ Run Command	Run Command にて使用する、 サーバで実行するコマンドを定義
Session	✓ Session Manager	Session Manager にて開始する セッションのタイプを定義
Policy	✓ Inventory	Inventory にてインベントリデータを 収集する際に使用

Systems Manager ドキュメント (3/3)

- ドキュメントの共有が可能
 - 中央リポジトリを維持すれば良い
 - ベストプラクティスの共有を容易に実現

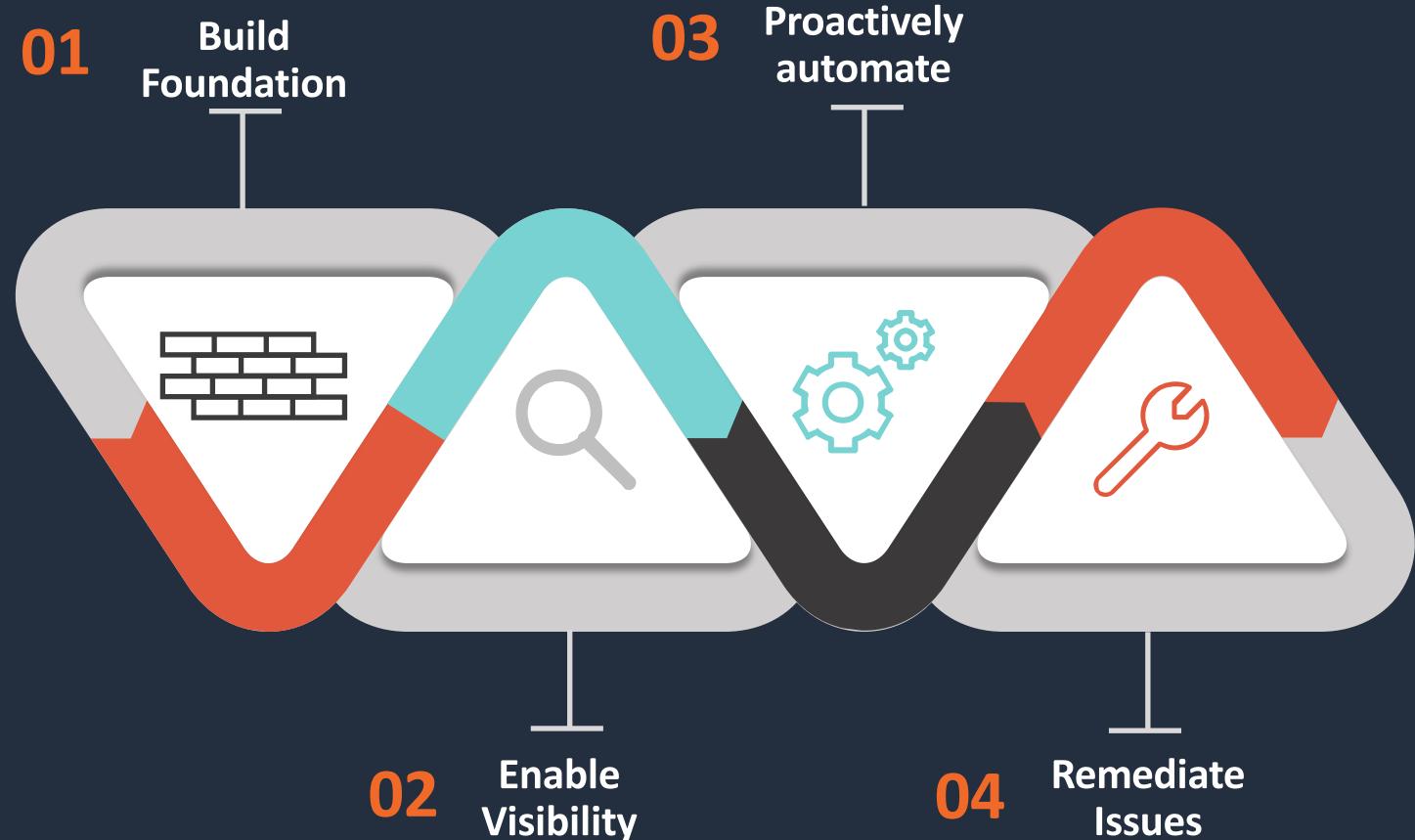


Systems Manager Features

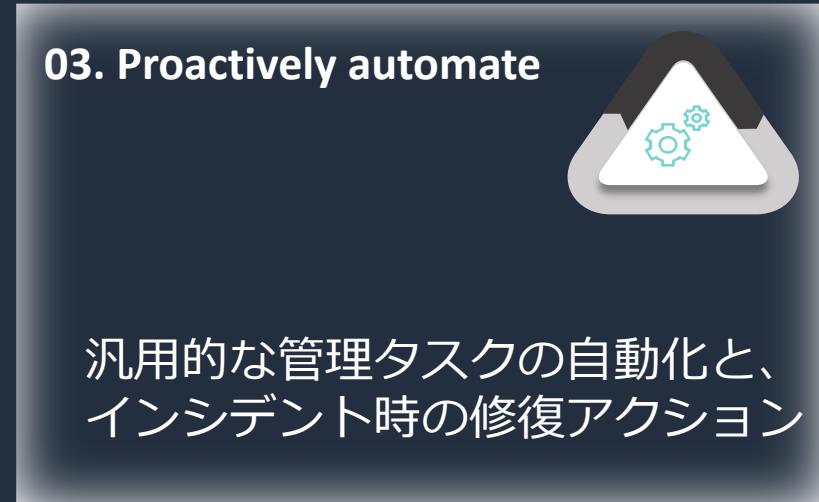
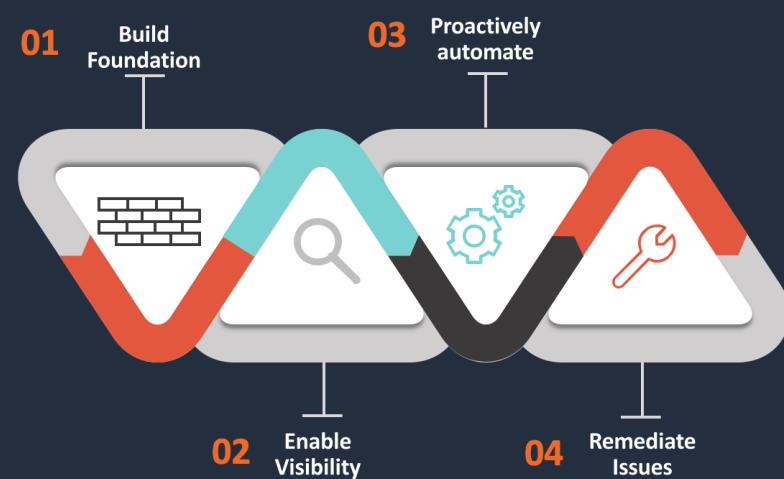
AWS Systems Manager の機能



コンプライアンスを実現するための 4 段階の実装



コンプライアンスを実現するための 4 段階の実装



01. Build Foundation

運用のベストプラクティスを展開し、それを維持する仕組みを確立



運用上のベストプラクティスを展開

Quick Setup

展開したベストプラクティスを維持する仕組み



State Manager



Build Foundation

Quick Setup

運用のベストプラクティスを簡単に展開

→ マルチアカウント、マルチリージョンに、
ベストプラクティスを展開できる。

Host Management

AWS Systems Manager

Config Recording

AWS Config

Conformance packs

AWS Config

Patch Manager

AWS Systems Manager

Change Manager

AWS Systems Manager

DevOps Guru

Amazon DevOps Guru

Distributor

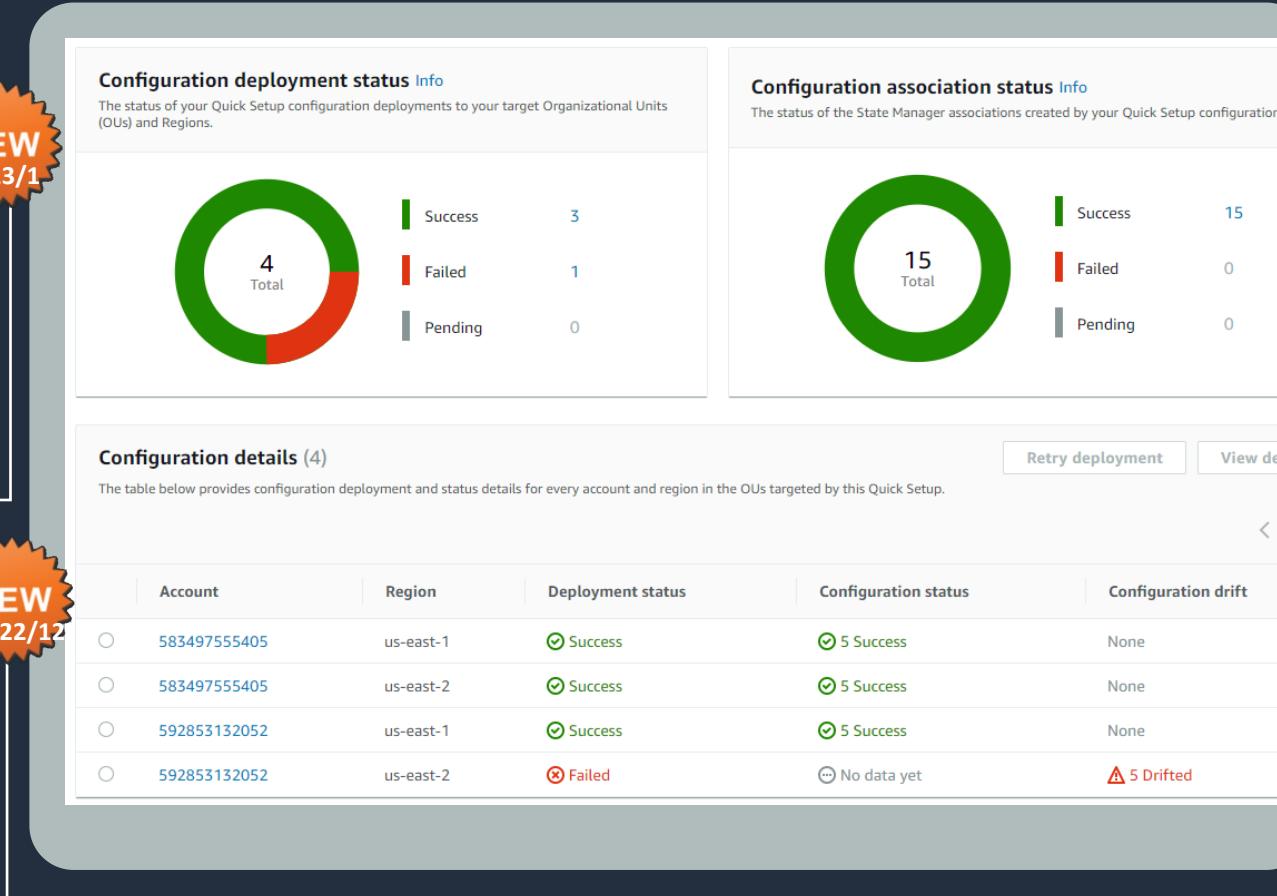
AWS Systems Manager

Resource Scheduler

AWS Solutions

NEW
2023/1

NEW
2022/12



Quick Setup の詳細は[こちら](#)

© 2023, Amazon Web Services, Inc. or its affiliates.

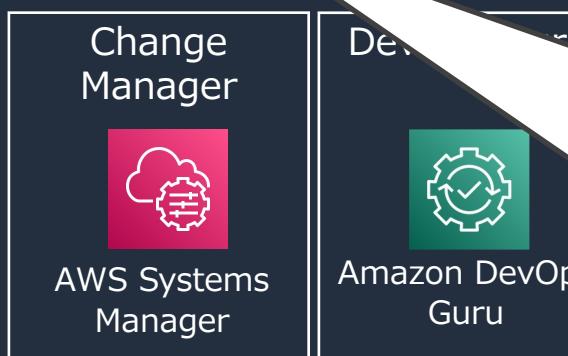
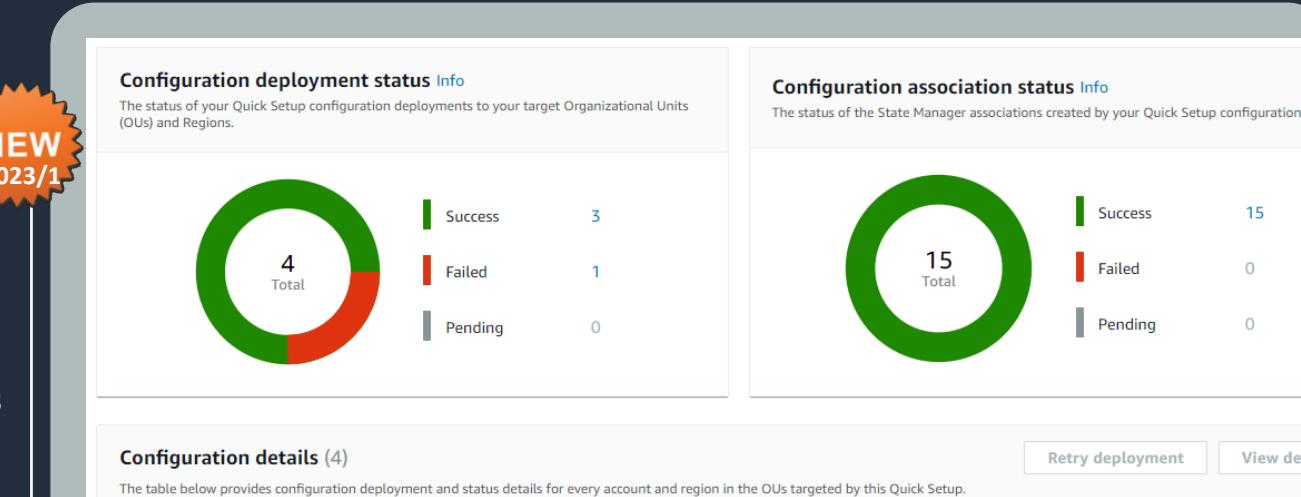
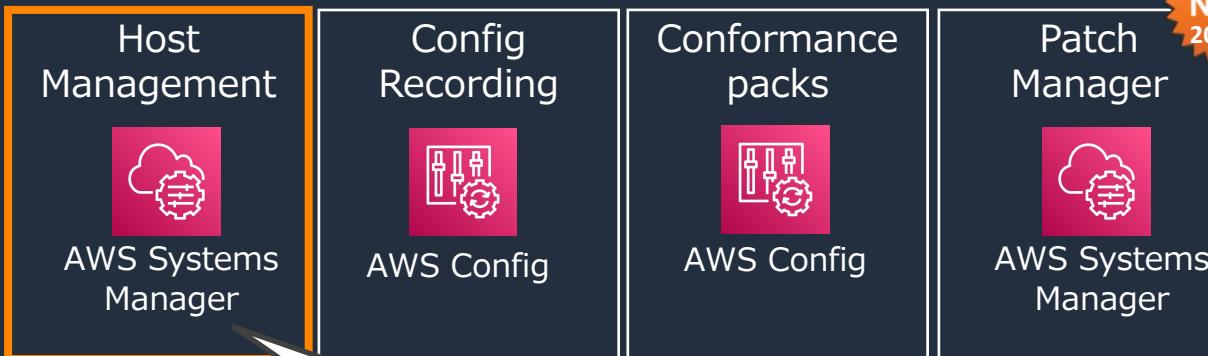


Build Foundation

Quick Setup

運用のベストプラクティスを簡単に展開

→ マルチアカウント、マルチリージョンに、
ベストプラクティスを展開できる。



SSM が提供するベストプラクティスの構築

- SSM Agent の定期更新
- Inventory の定期収集
- パッチスキヤンの定期実行
- CloudWatch Agent のインストールと構成
- CloudWatch Agent の定期更新



Host Management の詳細は[こちら](#)

© 2023, Amazon Web Services, Inc. or its affiliates.



Build Foundation

Quick Setup

運用のベストプラクティスを簡単に展開

→ マルチアカウント、マルチリージョンに、
ベストプラクティスを展開できる。

Host Management
 AWS Systems Manager

Config Recording
 AWS Config

Conformance packs
 AWS Config

Patch Manager
 AWS Systems Manager

NEW
2023/1

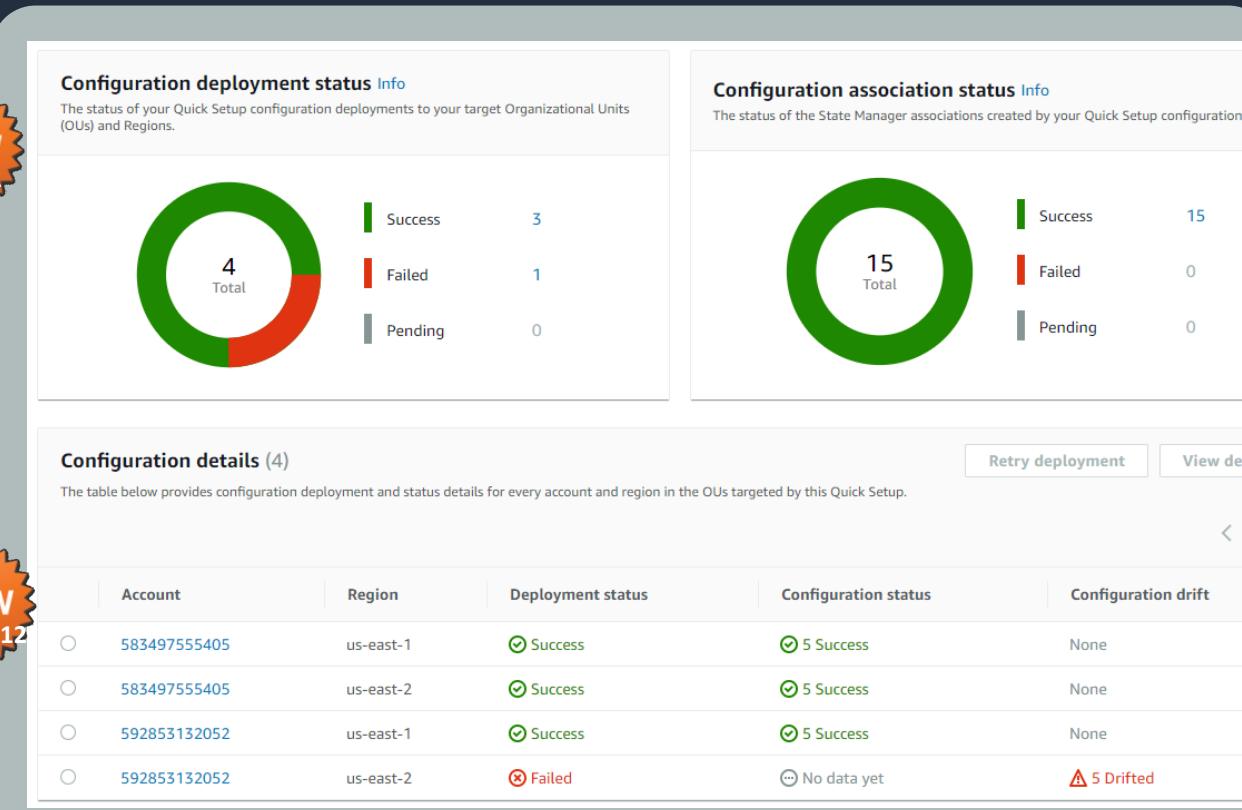
Change Manager
 AWS Systems Manager

DevOps Guru
 Amazon DevOps Guru

Distributor
 AWS Systems Manager

Resource Scheduler
 AWS Solutions

NEW
2022/12



EC2 の自動起動・停止が実装できる新機能



Resource Scheduler の詳細は[こちら](#)

© 2023, Amazon Web Services, Inc. or its affiliates.

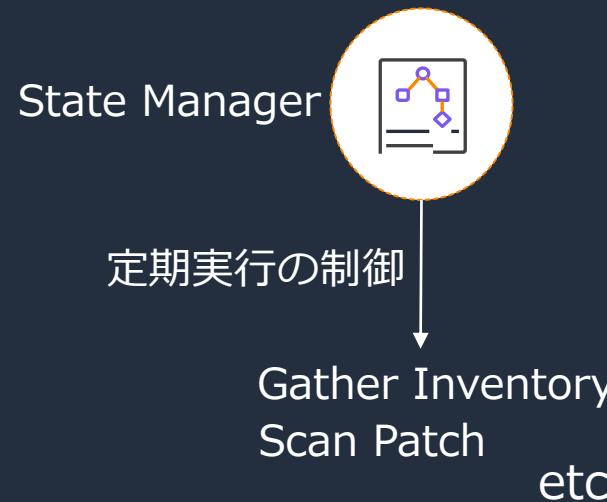


Build Foundation

State Manager

フリート全体の設定管理ソリューション

- Quick Setup で展開した SSM の定期実行処理は State Manager にて管理される。
- State Manager は、ノードを定義された状態に保つためのプロセスを自動化する。



The screenshot shows the AWS Systems Manager Compliance dashboard. The top navigation bar reads "AWS Systems Manager > Compliance". The main section is titled "Compliance dashboard filtering" with a sub-section "Compliance resources summary". It displays data for two categories: "Association" and "Patch". Under "Association", there are 4 compliant resources and 0 non-compliant resources. Under "Patch", there are 0 compliant resources and 4 non-compliant resources. Below this, a section titled "Details overview for resources" lists one resource: "i-00bcf16c41d508093" (ManagedInstance, Association, Unspecified, Compliant).

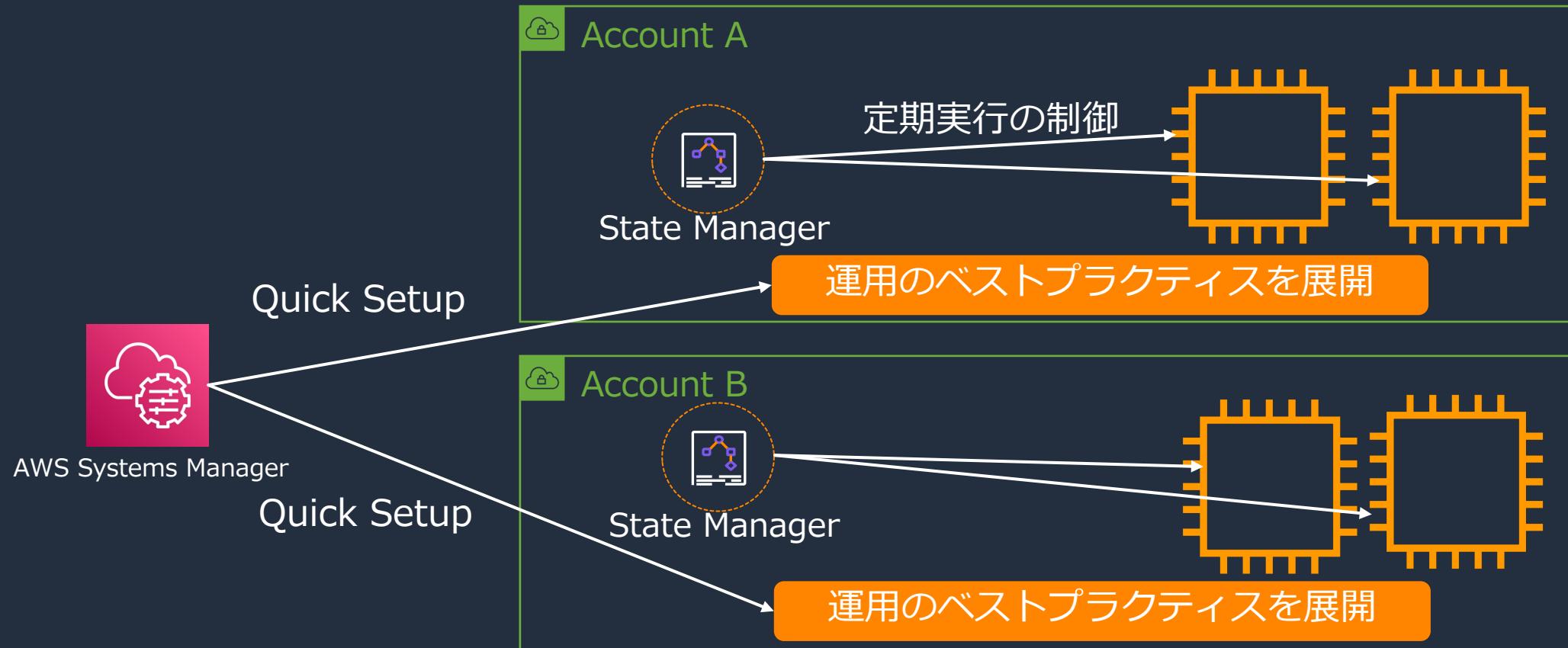


State Manager については、[こちら](#)。

© 2023, Amazon Web Services, Inc. or its affiliates.

おさらい

ここまで何ができたかというと・・・

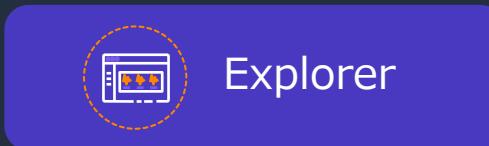


02. Enable Visibility

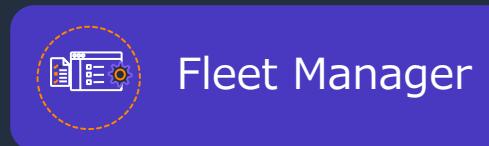
ハイレベルやノードレベルのダッシュボードと管理



AWS 環境全体を俯瞰・確認する



ノードの状態を俯瞰・確認する





Explorer

ハイレベルの運用ダッシュボード

Enable Visibility

- マルチアカウント・マルチリージョンのハイレベルな運用ダッシュボード。
- 複数のサービスからの情報が集約される。

Instance / Compute Optimizer

Amazon Elastic Compute Cloud (Amazon EC2)

AWS Config Compliance

AWS Config

Trusted Advisor (※)

AWS Trusted Advisor

Security Hub Findings

AWS Security Hub

- Patch Compliance
- OpsItems
- Inventory
- Association

AWS Systems Manager

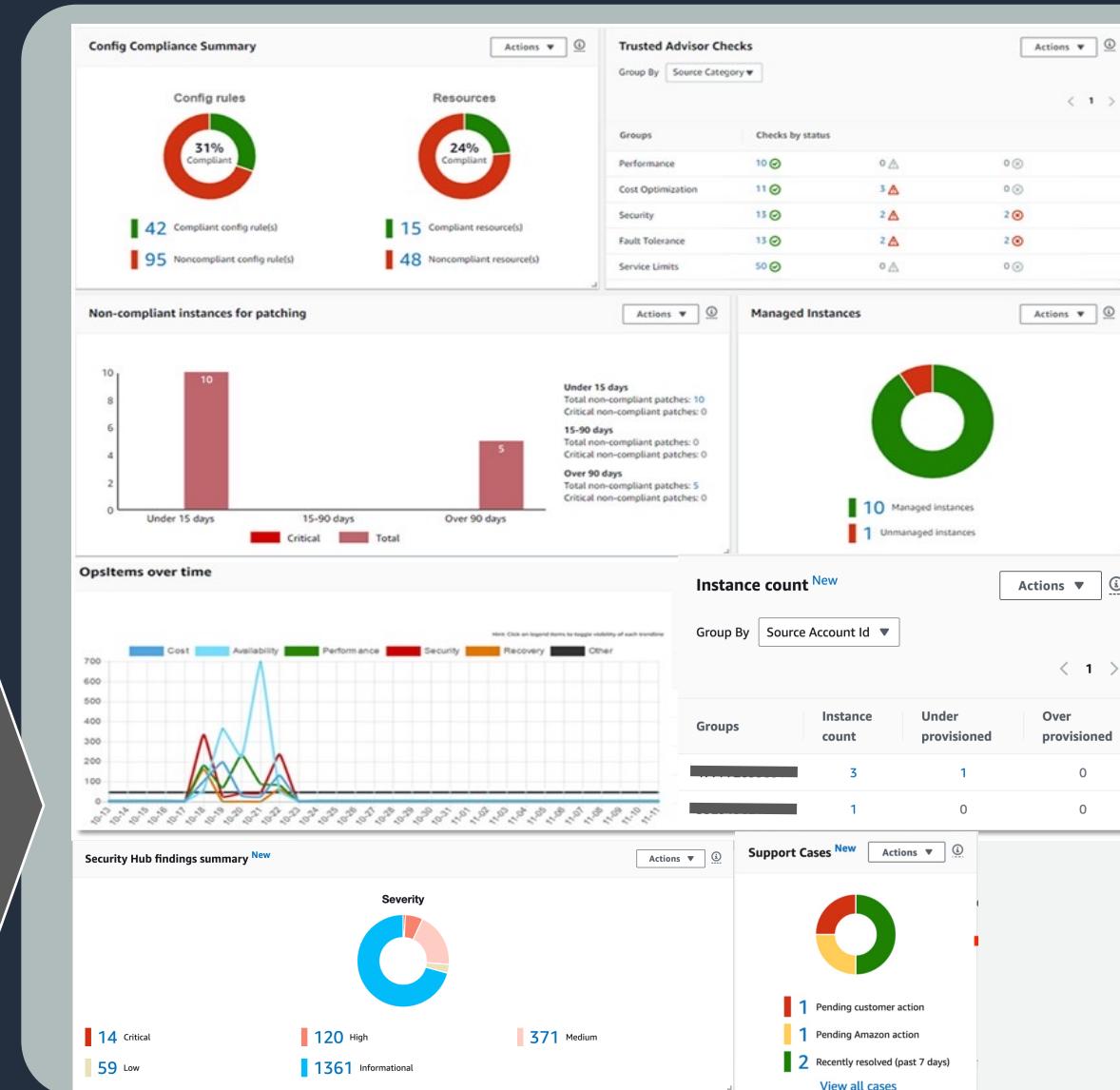
Support Center (※)

AWS Support

aws Explorerについての詳細は[こちら](#)。

※ Enterprise Support、Business Support プランが必要

© 2023, Amazon Web Services, Inc. or its affiliates.



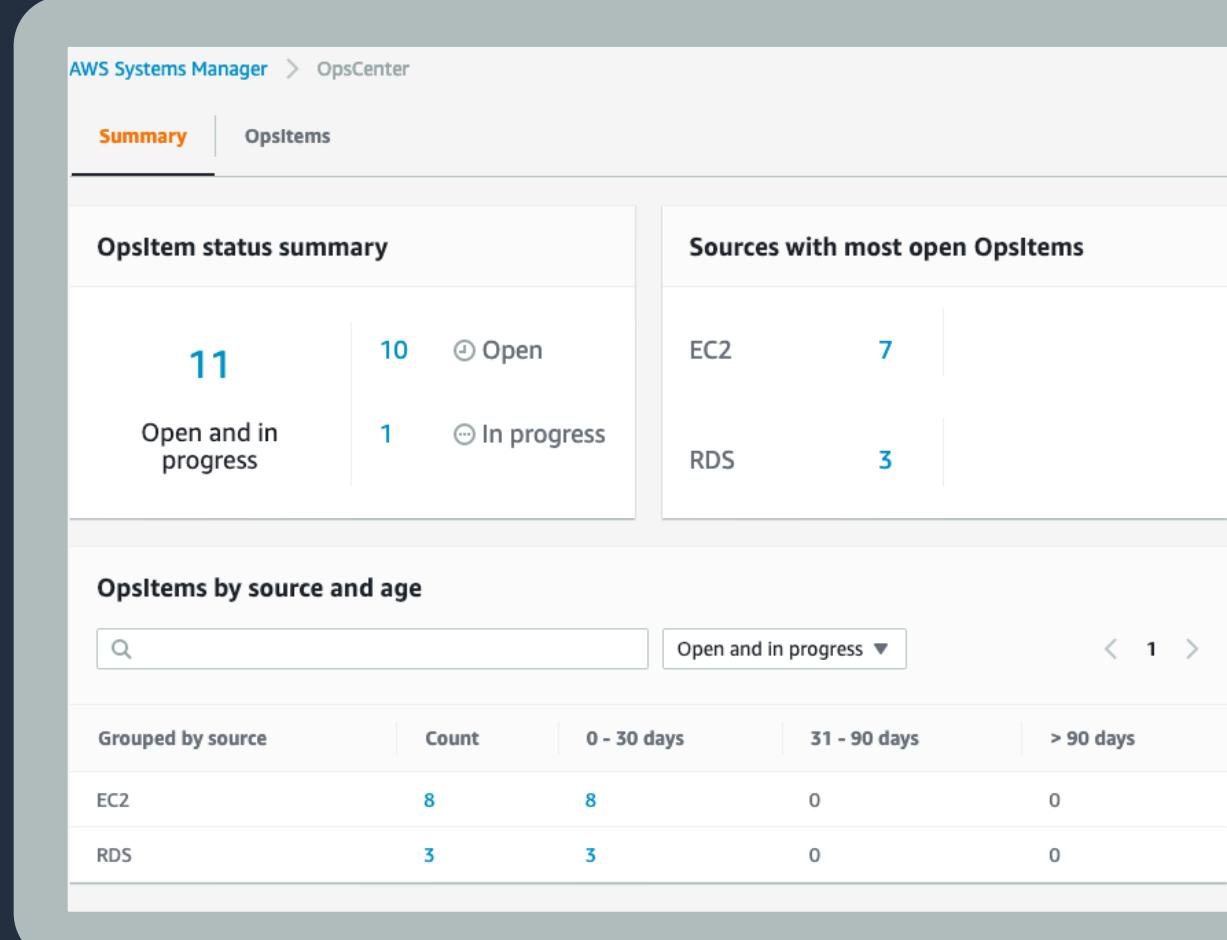


OpsCenter

対応すべき運用アイテムの可視化、問題解決の支援

Enable Visibility

- 運用上の問題 (OpsItem) の集約ビューを提供。
- OpsItem に関するデータを一元的に提供し、問題解決までの時間短縮を支援する。
- マルチアカウントでの OpsItem の表示や操作も可能。
- ServiceNow, Jira Service Management と連携も。



The screenshot shows the AWS Systems Manager OpsCenter interface. At the top, there are two tabs: "Summary" (which is selected) and "Opsitems". The main area is titled "OpsItem status summary" and displays the following data:

Status	Count
Open	10
Open and in progress	11
In progress	1

Below this is a section titled "Sources with most open OpsItems", which lists EC2 (7) and RDS (3). The bottom section is titled "OpsItems by source and age" and includes a search bar and a dropdown menu set to "Open and in progress". It shows the following distribution of items by source and age group:

Grouped by source	Count	0 - 30 days	31 - 90 days	> 90 days
EC2	8	8	0	0
RDS	3	3	0	0

 OpsCenterについての詳細は[こちら](#)。

© 2023, Amazon Web Services, Inc. or its affiliates.



OpsCenter

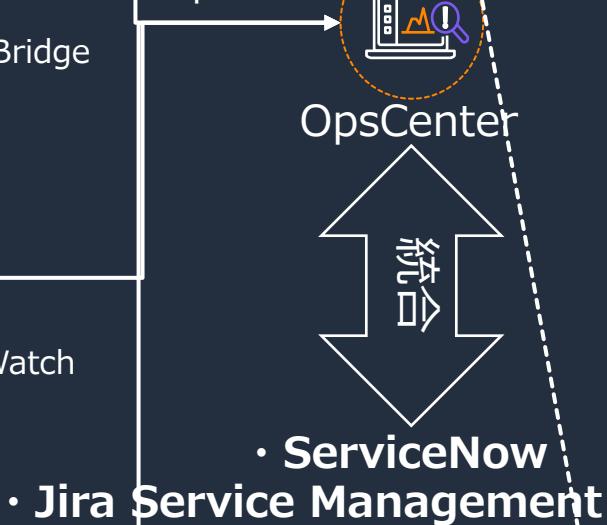
対応すべき運用アイテムの可視化、問題解決の支援

Enable Visibility



aws

etc



© 2023, Amazon Web Services, Inc. or its affiliates.

Runbook の提供



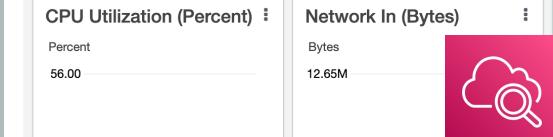
Automation

ランブック (361)

名前	タイプ
AWS-CreateManagedWindowsInstance	Associated AWS:SSM:Automation
AWS-CreateManagedLinuxInstance	Associated AWS:SSM:Automation

関連リソースの情報

▼ CloudWatch メトリクス



Amazon CloudWatch

▼ AWS Config の詳細

検出された時間	キー	値から
3 hours ago	imageId	ami-08d56ac42
3 hours ago	instanceId	i-03695dbe27e
3 hours ago	instanceType	t2.micro

AWS Config

▼ CloudTrail ログ (4)

イベント時間	ユーザー名
3 hours ago	imagebuilder08cd5-4a36-47e6-ab15-c15ba95745d1
3 hours ago	-
3 hours ago	-

AWS CloudTrail

45



Enable Visibility

Fleet Manager

ノードフリートの管理

④ マネジメントコンソールからノードフリートの管理ができるビジュアルツール

- ・ファイルシステム
- ・パフォーマンスカウンタ
- ・プロセス
- ・ユーザー・グループ
- ・Windows レジストリ (Windows のみ)
- ・Windows イベントログ (Windows のみ)

ログのTail

プレビューファイル: messages

テールファイル

```
Feb 25 23:19:34 ip-172-31-46-152 dhclient[2208]: XMT: Solicit on eth0, interval 122570ms.
Feb 25 23:21:36 ip-172-31-46-152 dhclient[2208]: XMT: Solicit on eth0, interval 112900ms.
Feb 25 23:23:29 ip-172-31-46-152 dhclient[2208]: XMT: Solicit on eth0, interval 109720ms.
Feb 25 23:25:19 ip-172-31-46-152 dhclient[2208]: XMT: Solicit on eth0, interval 118120ms.
Feb 25 23:27:17 ip-172-31-46-152 dhclient[2208]: XMT: Solicit on eth0, interval 127520ms.
Feb 25 23:29:25 ip-172-31-46-152 dhclient[2208]: XMT: Solicit on eth0, interval 108910ms.
Feb 25 23:31:14 ip-172-31-46-152 dhclient[2208]: XMT: Solicit on eth0, interval 122110ms.
Feb 25 23:33:16 ip-172-31-46-152 dhclient[2208]: XMT: Solicit on eth0, interval 109760ms.
Feb 25 23:35:06 ip-172-31-46-152 dhclient[2208]: XMT: Solicit on eth0, interval 129830ms.
Feb 25 23:37:16 ip-172-31-46-152 dhclient[2208]: XMT: Solicit on eth0, interval 124770ms.
```

プロセス稼働状況

AWS Systems Manager > Fleet Manager > Instance ID: i-03170a

Instance ID: i-03170a

Tools

- Node overview
- File system
- Performance counters
- Processes New
- Users and groups
- Windows event logs
- Windows registry

Instance overview

Instance ID i-03170a	OS name Microsoft Windows Server 2019 Datacenter	Availability zone us-east-1a
Platform type Windows	SSM Agent version 3.0.529.0	SSH key name -
Instance type t2.small	IP address 10.0.1.8	IAM role arn:aws:iam::2869:instance-profile/ManagedInstanceProfile
SSM Agent ping status Online		

Tags

Key	Value
Name	Windows

Processes (56/56)

The table provides information about the processes that are currently running on your node.

Process name	Process ID	CPU usage	Memory usage
svchost#11	1184	0	9.47
svchost#5	492	0	8.56

aws Fleet Manager についての詳細は[こちら](#)。

© 2023, Amazon Web Services, Inc. or its affiliates.

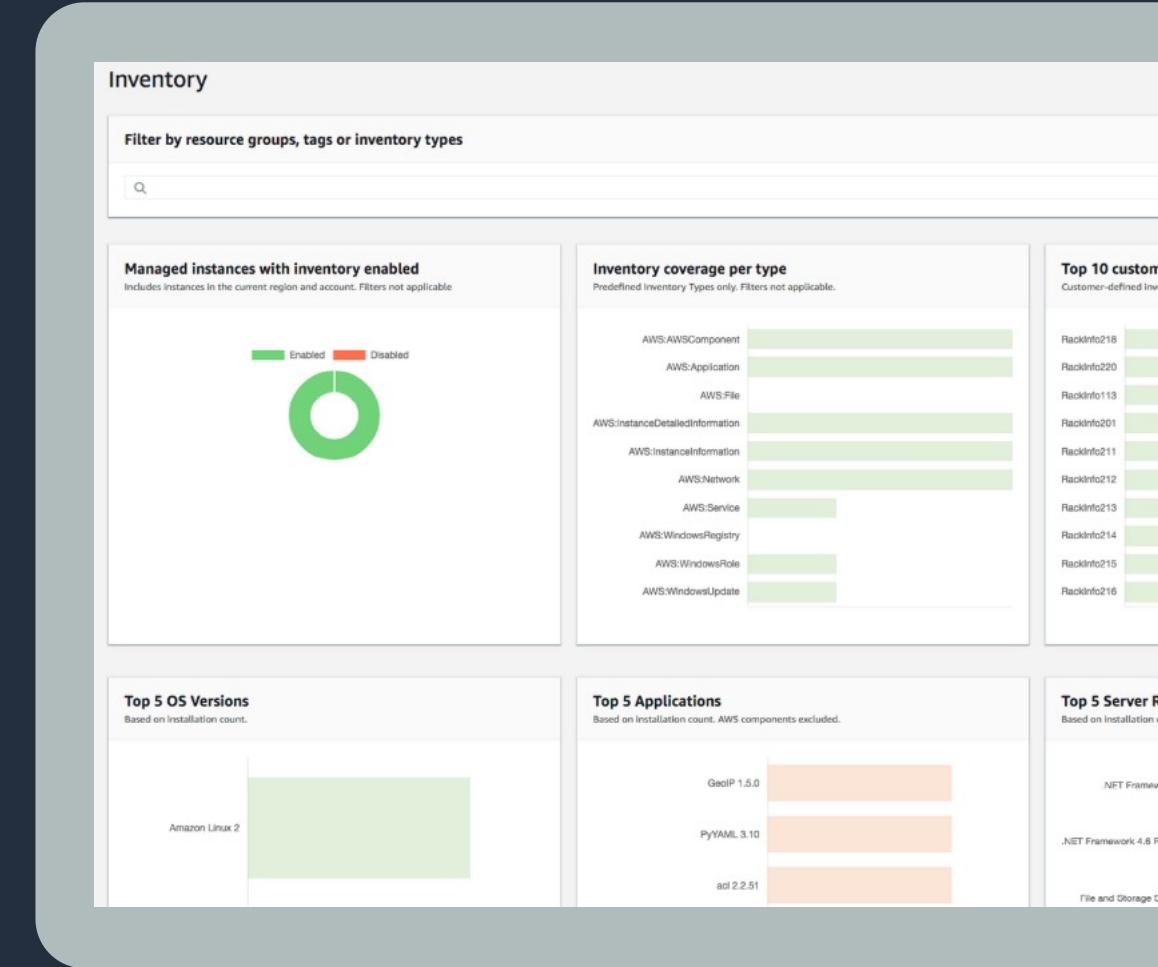


Inventory

ノードのメタデータ可視化

Enable Visibility

- ④ マネージドノードのメタデータを収集。
アプリケーション、ファイル、NW構成
インスタンス情報など
- ④ カスタムインベントリとして独自アイテムも
収集可能
- ④ リソースデータの同期を行うことで、自身
でマルチアカウント、マルチリージョンの
ダッシュボードを作成可能

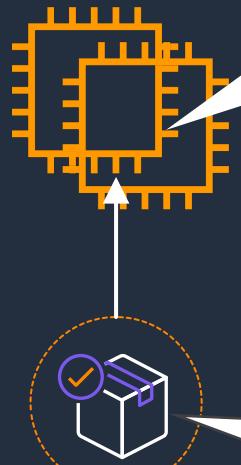


Inventoryについての詳細は[こちら](#)。

© 2023, Amazon Web Services, Inc. or its affiliates.

Inventory の活用例：Log4j の探索

- カスタムインベントリを活用することで、独自の収集項目が取得できる。
- この例では、Log4j の使用有無を探索し、それをカスタムインベントリとして登録している。



Inventory

詳細は[こちらのブログ](#)を参照

aws 「AWS Systems Manager カスタムインベントリを使ったマネージドノード上の Log4j ファイル検索」

Amazon Athena

Query 1

```
1 SELECT
2     resourceid, accountid, filename, path
3 FROM
4     custom_log4j
```

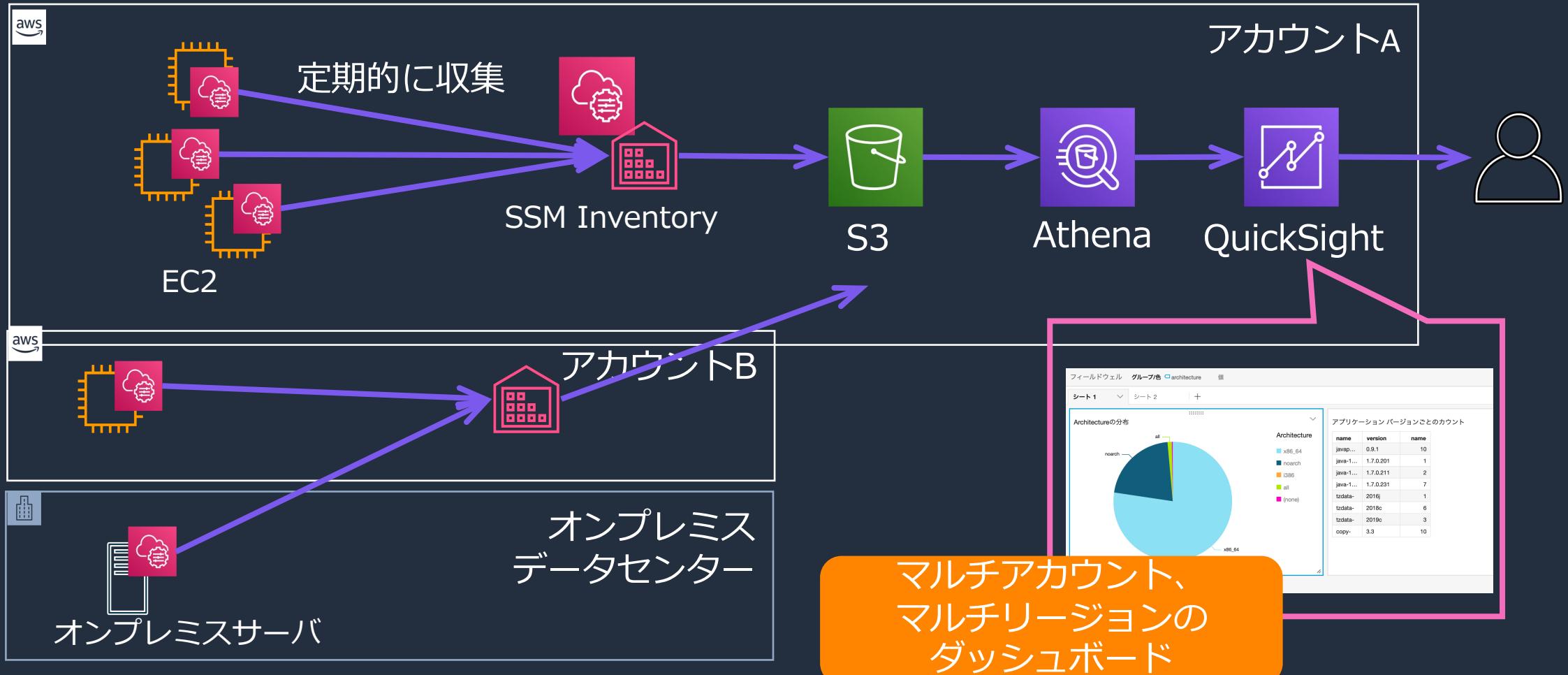
Completed

Time in queue: 0.149 sec Run time: 0.954 sec Data scanned: 1.10 KB

resourceid	accountid	filename	path
i-0f500...	31734	log4j-core-2.12.0.jar	C:\SampleApp\apache-log4j-2.12.0-bin\apache-log4j-2.12.0-bin\lo...
i-0f500...	31734	log4j-core-2.11.0.jar	C:\Users\Administrator\Desktop\apache-log4j-2.11.0-bin\apache-l...
mi-06eb5...	31734	log4j-core-2.11.0.jar	C:\Users\Administrator\Downloads\apache-log4j-2.11.0-bin\apach...
i-00d87...	31734	log4j-core-2.12.0.jar	/tmp/log4j/apache-log4j-2.12.0-bin/log4j-core-2.12.0.jar
i-00d87...	31734	log4j-core-2.11.0.jar	/tmp/log4j-2.11/apache-log4j-2.11.0-bin/log4j-core-2.11.0.jar

© 2023, Amazon Web Services, Inc. or its affiliates.

Inventory の活用例： マルチアカウント/マルチリージョンのダッシュボードの作成



詳細はこちらの[チュートリアル](#)参照

aws 「チュートリアル: リソースデータの同期を使用してインベントリデータを集約する」

© 2023, Amazon Web Services, Inc. or its affiliates.

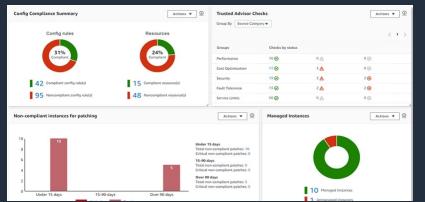
おさらい

ここまで何ができたかというと・・・

AWS環境全体を
俯瞰・確認する

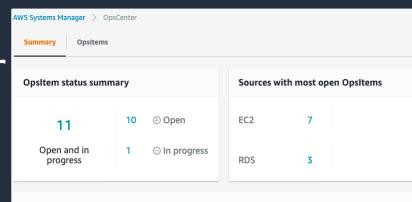


ハイレベルの運用ダッシュボード



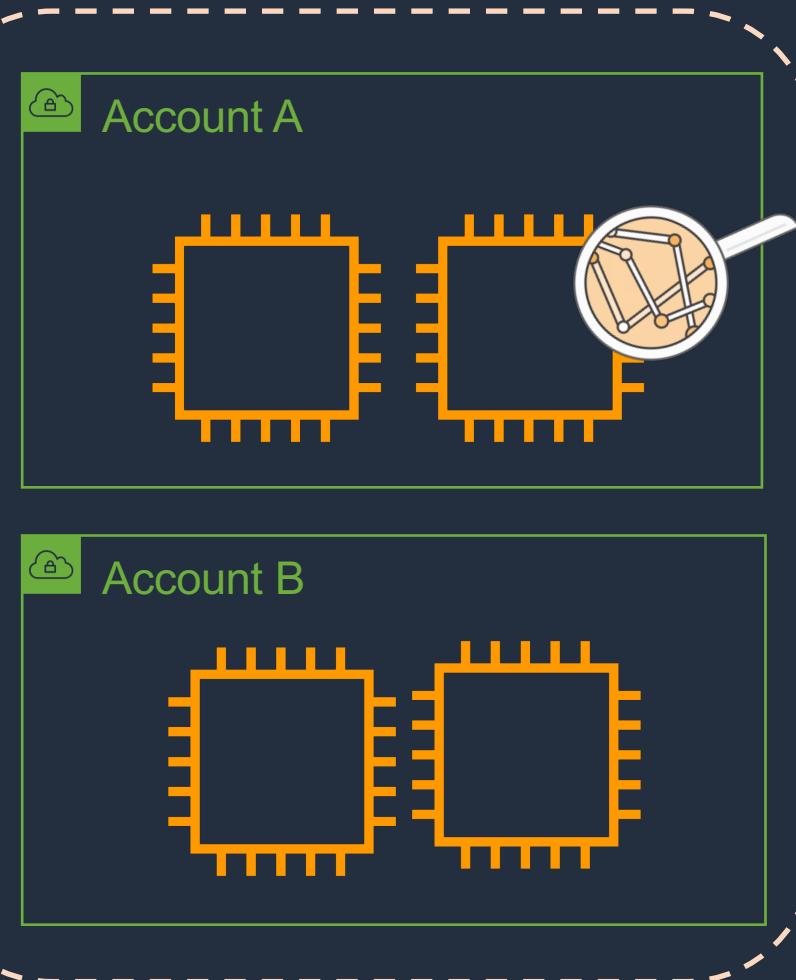
Explorer

運用アイテムの管理



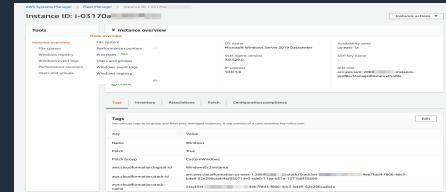
OpsCenter

aws



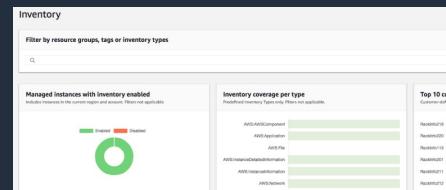
ノードの状態を
俯瞰・確認する

ノードフリート管理



Fleet
Manager

ノードのメタデータ可視化



Inventory

03. Proactively Automate

汎用的な管理タスクの自動化と、インシデント時の修復アクション



汎用的な管理作業の自動化



Patch Manager



Distributor



Automation

自動化処理のタイミング制御



Maintenance
Windows



Change Calendar

自動修復の実装



Automation



Patch Manager

パッチ適用を自動化

Proactively Automate

- ④ マネージドノードに対して、パッチの自動スキャン、自動パッチ適用を実現。
- ④ Patch Manager サポート OS は SSM Agent サポートOSとは異なるので注意。サポート OS は[こちら](#)。
- ④ パッチポリシーをマルチアカウント、マルチリージョンにデプロイ可能

パッチベースラインの設定例

OS : Amazon Linux / Windows など

製品 : Amazon Linux2 など

分類 : All, Security, Bugfix など

重要度 : All, Critical, Important など

自動承認 : リリースされてからX日後に適用 or

特定の日付までにリリースされたパッチを適用

パッチの例外 : 承認済みパッチ、拒否パッチ

aws Patch Manager についての詳細は[こちら](#)。

© 2023, Amazon Web Services, Inc. or its affiliates.

The screenshot shows the AWS Systems Manager Patch Manager dashboard. At the top, there's a navigation bar with links for Dashboard, Reporting, Patch baselines, Patches, Patch groups, and Settings. On the right, there are two orange buttons: 'Configure patching' and 'Patch now'. The main area is divided into several sections:

- Instance Patch Compliance Summary:** A donut chart showing patch compliance status: 5 Compliant (green), 0 Critical non compliant (red), 1 Other non compliant (yellow), and 0 High non compliant (orange). Below it, statistics for total managed instances (6), instances with missing patches (1), instances with failed patches (0), and instances pending reboot (0) are displayed.
- Instance Patch States:** Shows counts for most common reasons for non-compliance.
- Compliance Reporting Age:** A donut chart showing reporting age for all managed instances: 6 Reported within the past 7 days (green), 0 Not reported within the past 7 days (yellow), and 0 Never reported (red).
- Recent Patch Operations:** A table listing recent patching commands. It includes columns for Patch Operation (Scan, Install), Execution Mechanism (Other, Association), Document name (AWS-RunPatchBaseline, AWS-RunPatchBaselineAssociation), End time, Status (Success), and Targets (resource-groups:Name, Instance IDs, resource-group:Name, tag:Patch: True, instance IDs, resource-groups:Name). There are 15 entries listed.
- Recurring Patching Tasks:** A table listing associations and maintenance windows. It includes columns for Patching task name (AWS-PatchNowAssociation, AWS-QuickSetup-SSMHostMgmt-ScanForPatches-b5mbv, PatchingTask), Task type (Association, MW Task), Document name (AWS-RunPatchBaseline, AWS-RunPatchBaselineAssociation, AWS-RunPatchBaseline), and Schedule (cron(0 00 02 ? * *), rate(1 day), cron(58 21 ? * MON *)).



Distributor

ソフトウェアのインストール・更新の自動化

Proactively Automate

- ④ ソフトウェアパッケージのデプロイ自動化を実現。
- ④ 一つのパッケージで Windows も Linux も。
- ④ 独自で定義したパッケージのデプロイはもちろん、CloudWatch Agent など AWS 提供のパッケージや 3rd Party のパッケージの利用もおすすめ

利用できる3rd Party パッケージ

- TrendMicro-CloudOne-WorkloadSecurity
- DynatraceOneAgent
- AlertLogic-MDR

NEW
2022/2

The screenshot shows the AWS Systems Manager Distributor interface. At the top, there are tabs for 'Owned by Amazon' (which is selected), 'Owned by me', 'Shared with me', 'Third Party', and 'All documents'. Below this is a search bar labeled 'Search by keyword or filter by tag or attributes'. The main area displays a grid of package cards, each with a name, owner information, and a circular selection button. The packages listed are: AmazonCloudWatchAgent, AWSupport-EC2Rescue, AWSSAP-Backint, AWSEC2Launch-Agent, AmazonEFSUtils, AWSObservabilityExporter-JMXExporterInstallAndConfigure, AWSCodeDeployAgent, AWSKinesisTap, AwsVssComponents, AWSPVDriver, AWSNVMe, and AwsEnaNetworkDriver. All packages are owned by Amazon.

aws Distributor についての詳細は[こちら](#)。

© 2023, Amazon Web Services, Inc. or its affiliates.

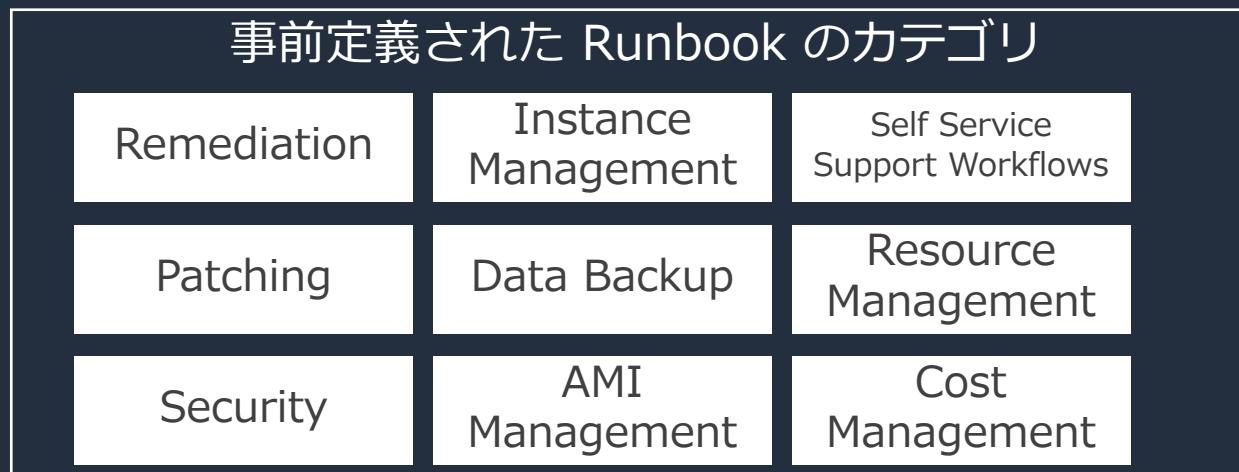


Automation

カスタム処理の自動化と修復アクション

Proactively Automate

- 自動化ワークフローである Runbook を実行できる。
- マルチアカウント/マルチリージョンでの実行も可能。
- 事前定義された Runbook が多数あるので、それを利用するのがおすすめ。



Execute automation document

Step 2 of 2

Simple execution
Execute on targets.

Multi-account and Region
Execute in multiple accounts and Regions.

Rate control
Execute safely on multiple targets by defining concurrency and error thresholds.

Manual execution
Step-by-step runbook mode.

Document details

Document name	Document version
AWS-PatchAsgInstance	\$DEFAULT
▼ Document description	
Systems Manager Automation - Patch instances in an Auto Scaling Group	

aws Automation についての詳細は[こちら](#)。

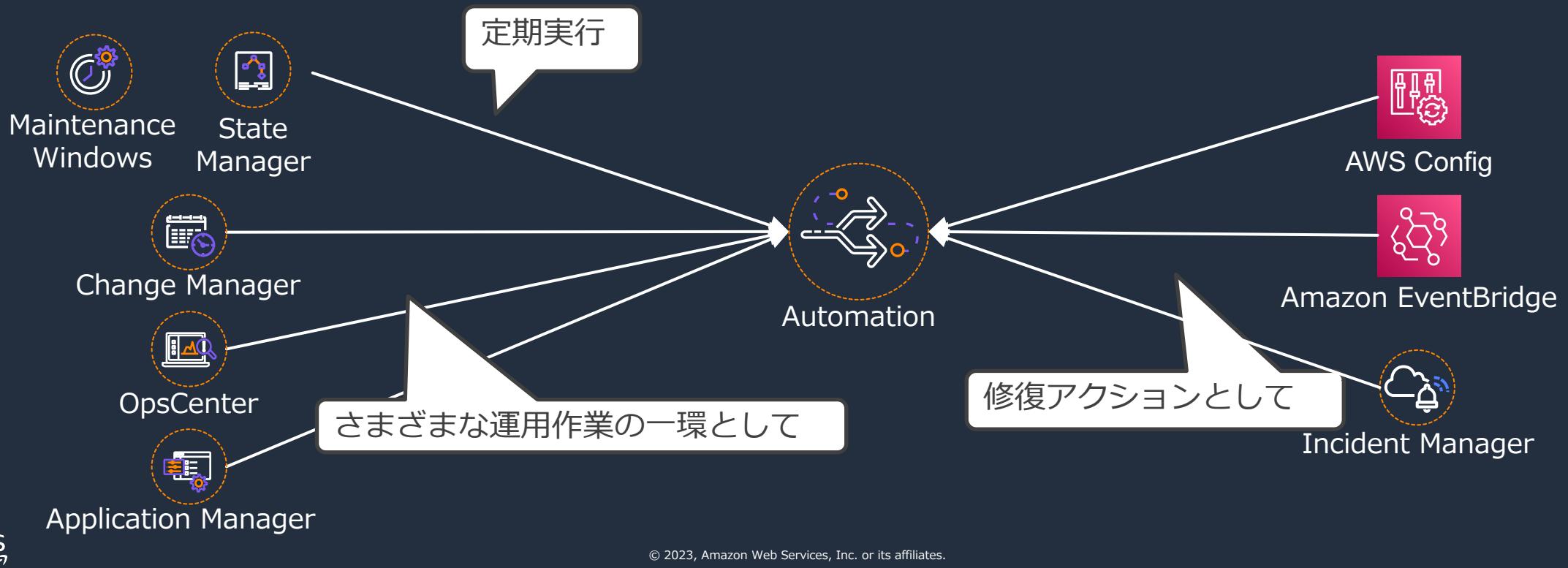
© 2023, Amazon Web Services, Inc. or its affiliates.



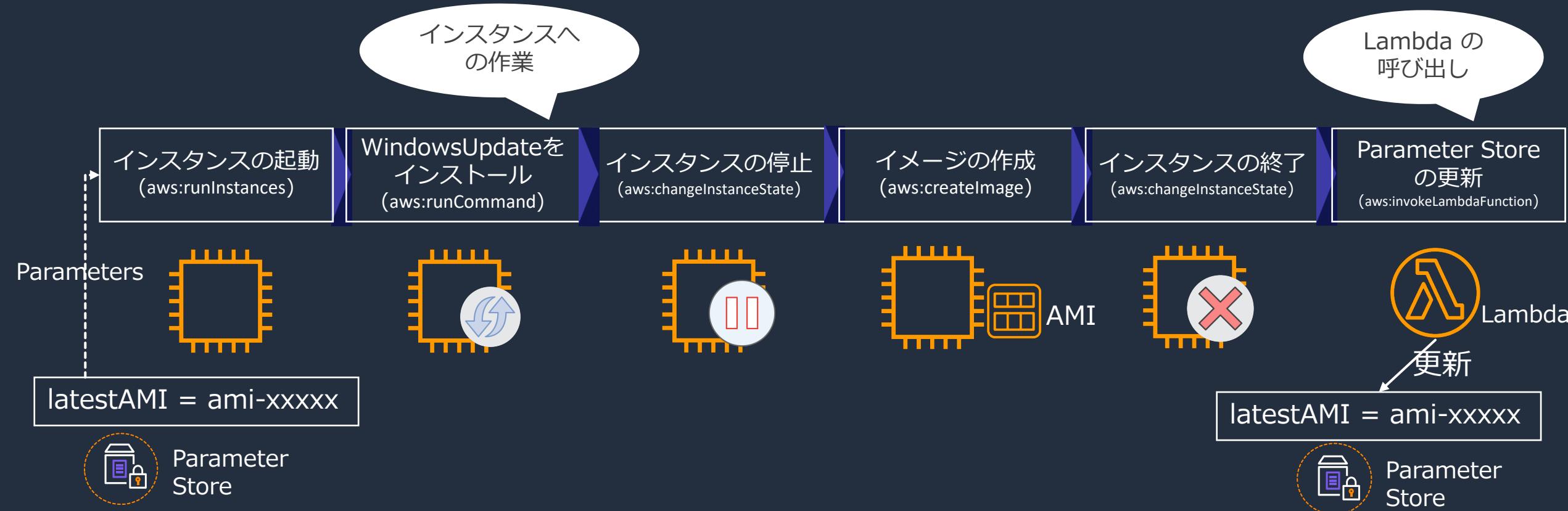
Proactively Automate

Automation – さまざまなトリガーで起動 カスタム処理の自動化と修復アクション

- Runbook はさまざまなサービスからトリガーできる。
- コンプライアンス違反やインシデント発生時の、自動で修復するアクションの定義としても活躍。



Runbook 例：カスタム AMI パッチ適用

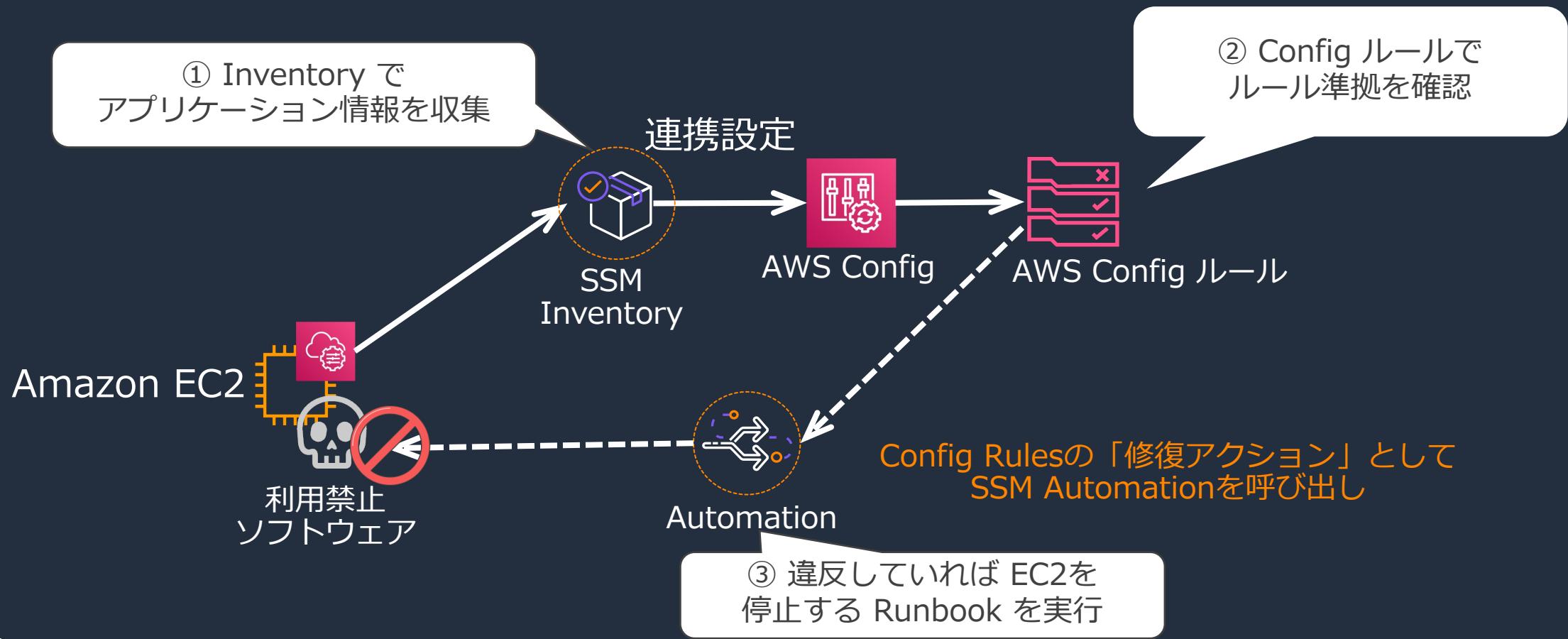


詳細は[こちら](#)のチュートリアルを参照
aws 「チュートリアル: オートメーション、AWS Lambda、Parameter Store を使用した AMI パッチ適用の簡素化」

© 2023, Amazon Web Services, Inc. or its affiliates.

修復自動化例：不正 SW の検知・自動停止

- ④ SSM Inventory でインベントリ情報を収集。
- ⑤ 不正 SW を検知したら、ノードを停止する Runbook を実行。



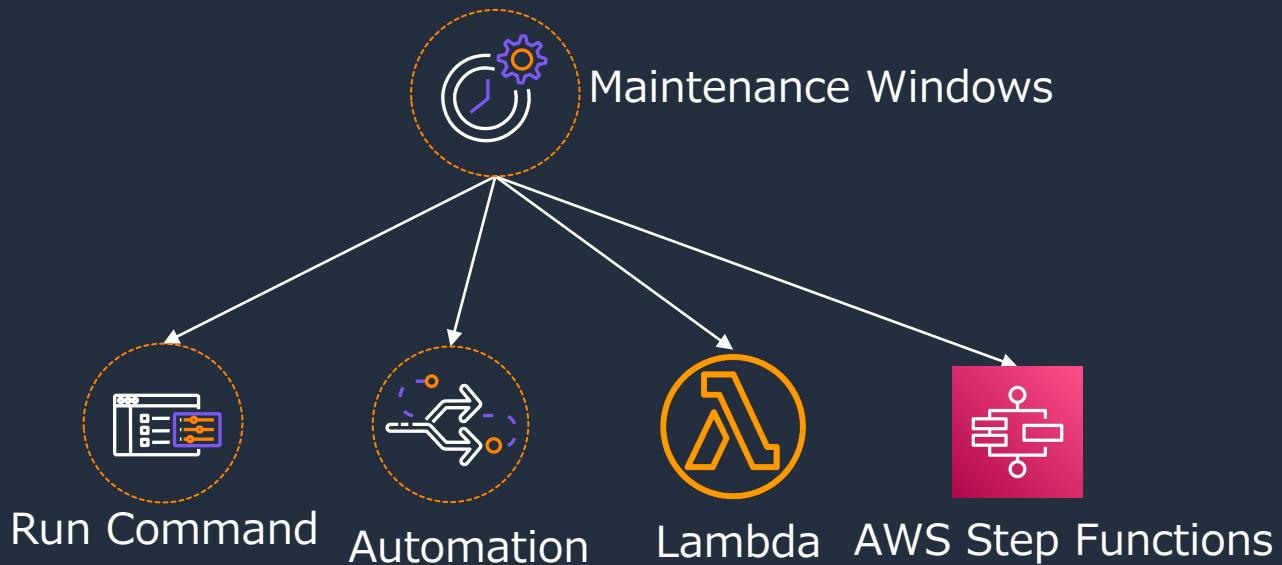


Maintenance Windows

タイムウィンドウ内のタスクを実行制御

Proactively Automate

- タスクのスケジュール制御ができる。
- 複数のタスクを登録でき、優先度に応じて実行順序を制御する。



aws Maintenance Windows についての詳細は[こちら](#)。© 2023, Amazon Web Services, Inc. or its affiliates.

AWS Systems Manager > Maintenance Windows > Create maintenance window

Create maintenance window

A maintenance windows lets you specify when a target set of managed instances should install updates or perform maintenance activities. Specify the details below to create a new maintenance window:

Provide maintenance window details

Name
Type a name for this maintenance window.

It has to be between 3 and 128 characters. Valid characters contain the following: a-z, A-Z, 0-9, and _.

Description - optional
Type description for this maintenance window.

It has to be between 1 and 128 characters.

Unregistered targets
Allow maintenance tasks scheduled for this maintenance window to run on targets that are not currently registered with this maintenance window.
 Allow unregistered targets

Schedule

Specify with
 Cron schedule builder
 Rate schedule builder
 CRON/Rate expression

Window starts
 Every 30 minutes
 Every hours

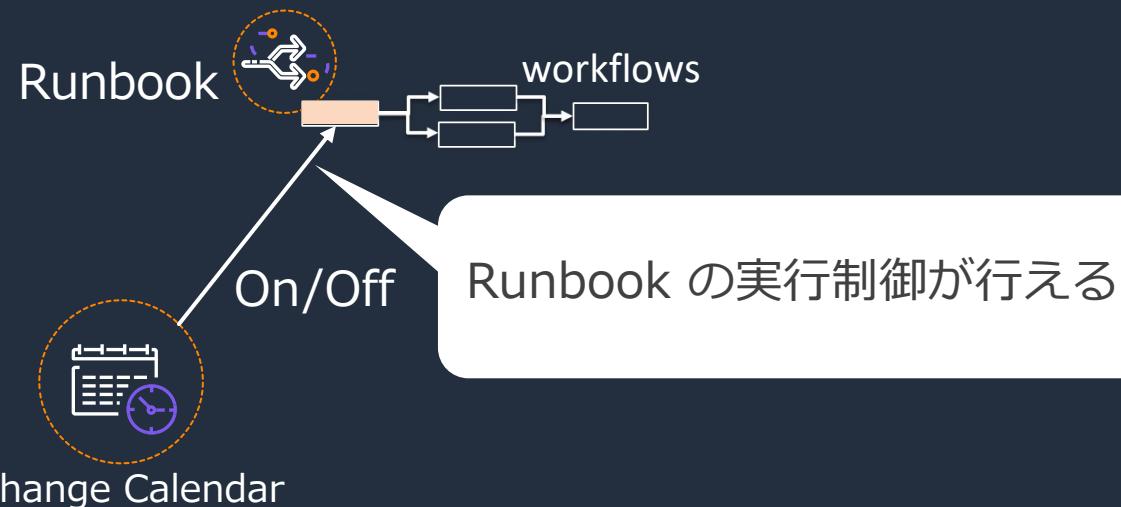


Change Calendar

自動処理のタイミング制御

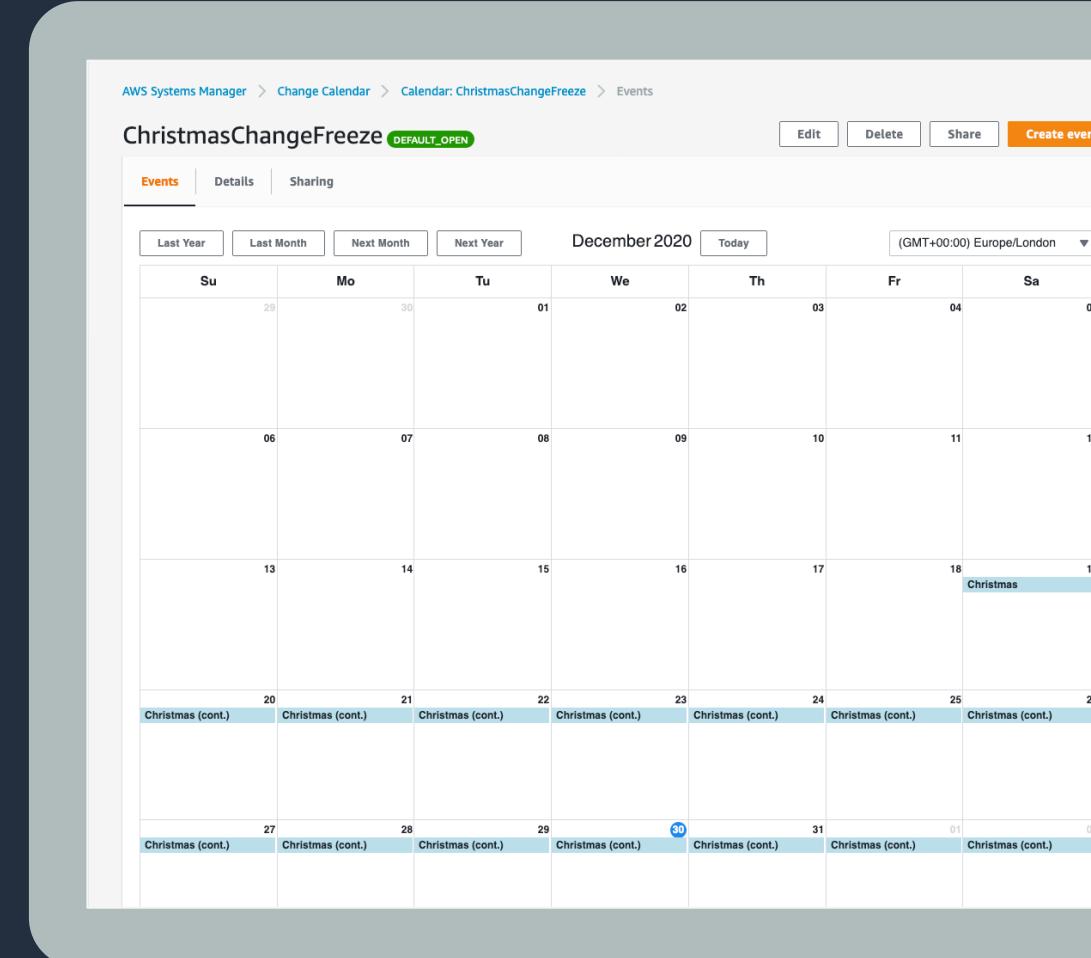
Proactively Automate

- ④ カレンダーイベントを作成し、そのイベント有無で実行を制御できる。
- ④ 3rd Partyのカレンダーのインポートも。Google Calendar, Microsoft Outlook, iCloud カレンダー
- ④ 作成したカレンダーは他のアカウントにも共有可能。



aws Change Calendarについての詳細は[こちら](#)。

© 2023, Amazon Web Services, Inc. or its affiliates.



おさらい

汎用的な管理作業の自動化

- パッチ適用



Patch Manager

- SW インストール、更新



Distributor

- その他カスタム処理



Automation



AWS Systems Manager



タイミング制御

- 定期実行



Maintenance Windows

- カレンダーでの制御



Change Calendar

問題発生時のアクション自動化



- 修復アクション



Automation

おさらい

汎用的な管理作業の自動化



Patch Manager

Distributor

Automation



問題発生時のアクション自動化



修復アクション



重要な変更は、
変更管理が必要だ・・・



Change Manager

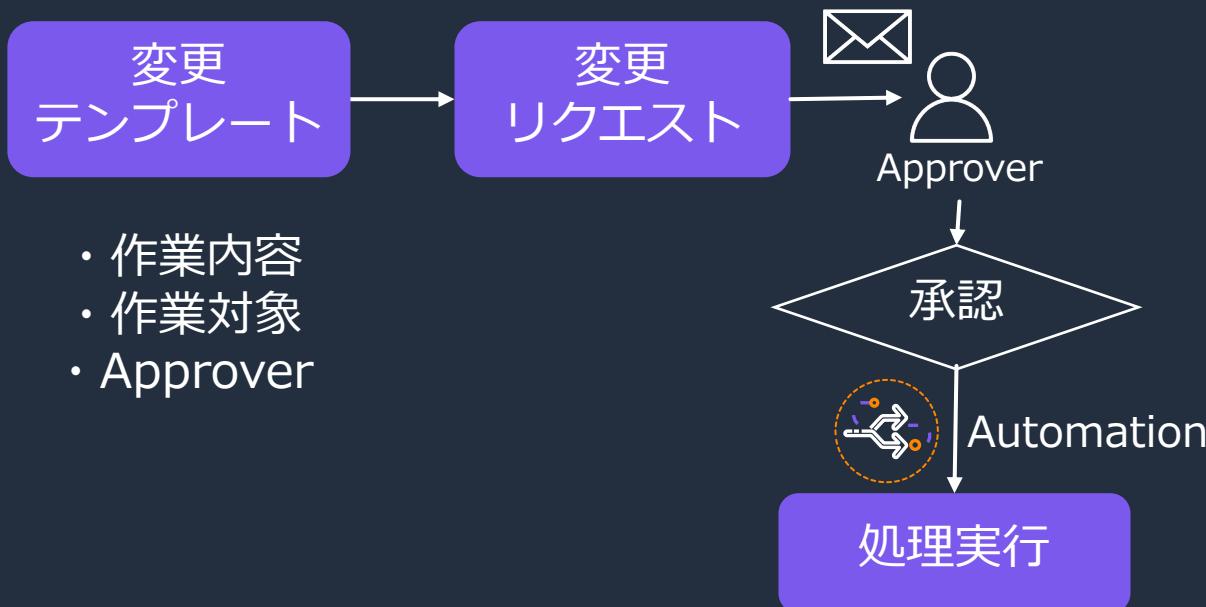


Change Manager

変更を安全に行うための承認ワークフローの自動化

Proactively Automate

- 承認ワークフローを使用して意図しない変更が発生しないことを防ぐ。
- Service Now との連携も可能。



aws Change Managerについての詳細は[こちら](#)。

© 2023, Amazon Web Services, Inc. or its affiliates.

The screenshot shows the AWS Change Manager console's Overview page. It includes sections for Change overview, Change requests, Change templates, Pending requests by time, Top 5 templates used in the last 30 days, and Scheduled changes for August 2020. Key data points shown include 0 My active requests, 0 Pending my approval, 0 My templates, 1 Pending my review, and a bar chart for the top templates used.

おさらい

汎用的な管理作業の自動化

- パッチ適用



Patch Manager

- SWインストール、更新



Distributor

- その他カスタム処理



Automation



タイミング制御

- 定期実行



Maintenance Windows

- カレンダーでの制御



Change Calendar

© 2023, Amazon Web Services, Inc. or its affiliate



問題発生時のアクション自動化

- 修復アクション



Automation



変更管理

- 承認ワークフローの自動化



Change Manager

04. Remediate Issues

ノードへの一括コマンド発行や、安全な特権アクセス



ノードへの一括コマンド発行



ノードへのセキュアな特権アクセス





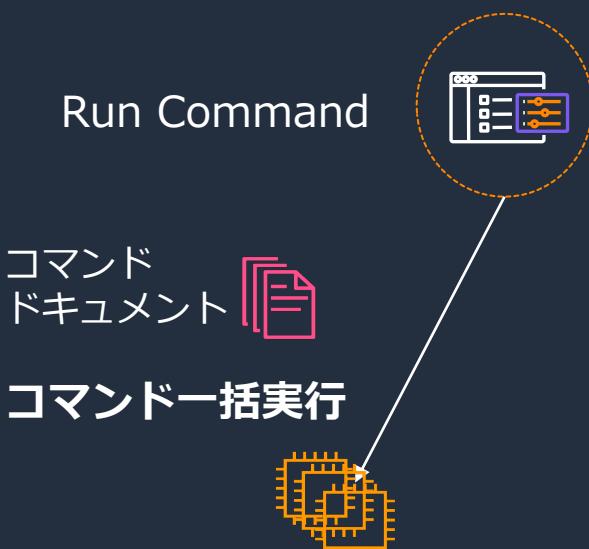
Remediate Issues

Run Command

ノードへの一括コマンド発行

- ④ サーバにログインすることなく、マネージドノードに対してコマンドを一括実行。
- ④ “コマンドドキュメント”を実行する。

任意のシェルスクリプトを流せる **AWS-RunShellScript** や Ansible を流せる **AWS-ApplyAnsiblePlaybooks** などが用意されていて便利！



aws → Run Command についての詳細は[こちら](#)。

© 2023, Amazon Web Services, Inc. or its affiliates.

Command parameters

Action
(Required) Specify whether or not to install or uninstall the package.
Install

Installation Type
(Optional) Specify the type of installation. Uninstall and reinstall: The application is taken offline until the reinstallation process completes. In-place update: The application is available while new or updated files are added to the installation.
Uninstall and reinstall

Name
(Required) The package to install/uninstall.
AmazonCloudWatchAgent

Version
(Optional) The version of the package to install or uninstall. If you don't specify a version, the system installs the latest published version by default. The system will only attempt to uninstall the version that is currently installed. If no version of the package is installed, the system returns an error.

Targets

Choose a method for selecting targets.

Specify instance tags
Specify one or more tag key-value pairs to select instances that share those tags.

Choose instances manually
Manually select the instances you want to register as targets.

Choose a resource group
Choose a resource group that includes the resources you want to target.

Resource group
Select the resource group that you want to use as a target. [View resource groups](#)
EC2Instances

Resource types - optional
Select one or more available resource types to narrow down the target group.
Select resource types
All available resource types X

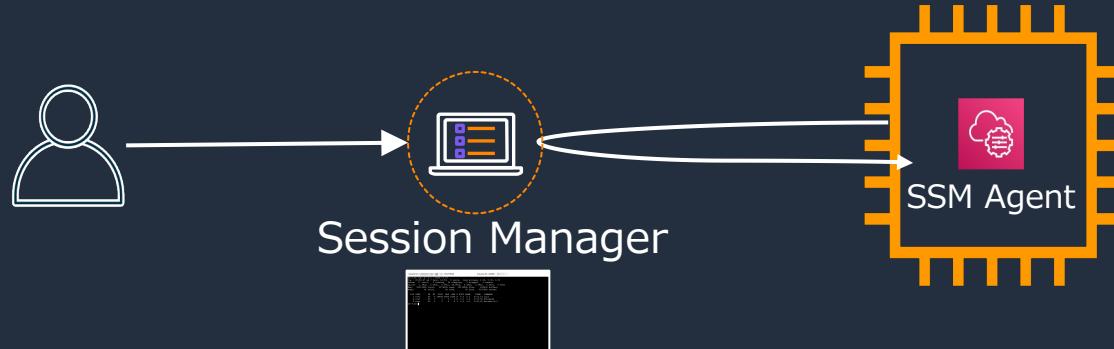


Remediate Issues

Session Manager

ノードへのセキュアな特権アクセス

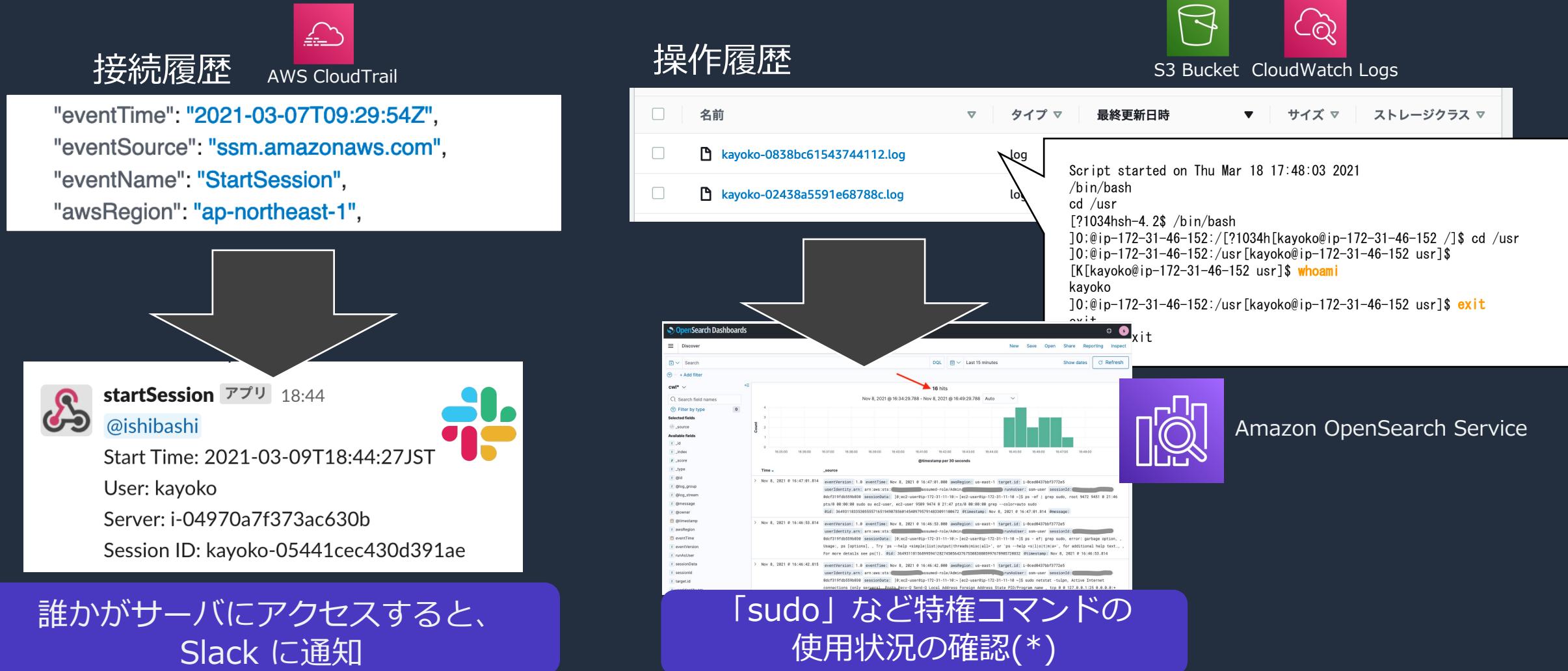
- インバウンドポートを開くことなく、ブラウザや CLI からインタラクティブなシェルアクセスを実現。
- ポートフォワーディングでのアクセスも可能。



Session Managerについての詳細は[こちら](#)。

© 2023, Amazon Web Services, Inc. or its affiliates.

Session Manager でのアクセス統制例



誰かがサーバにアクセスすると、
Slack に通知

「sudo」など特権コマンドの使用状況の確認(*)

(*) 詳細は[こちらのブログ](#)を参照
 「AWS Systems Manager Session Manager コンソールログを探索する」
© 2023, Amazon Web Services, Inc. or its affiliates.

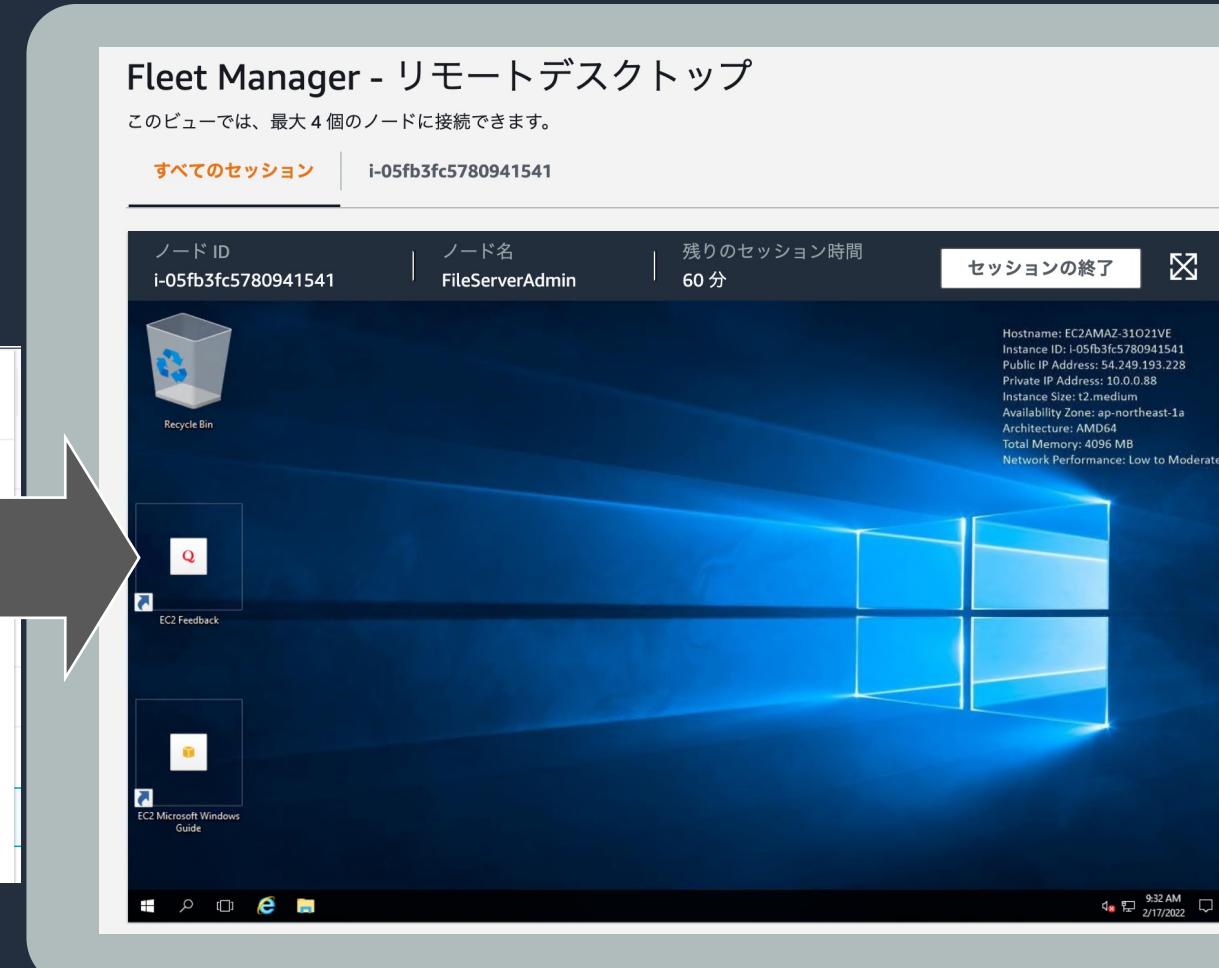
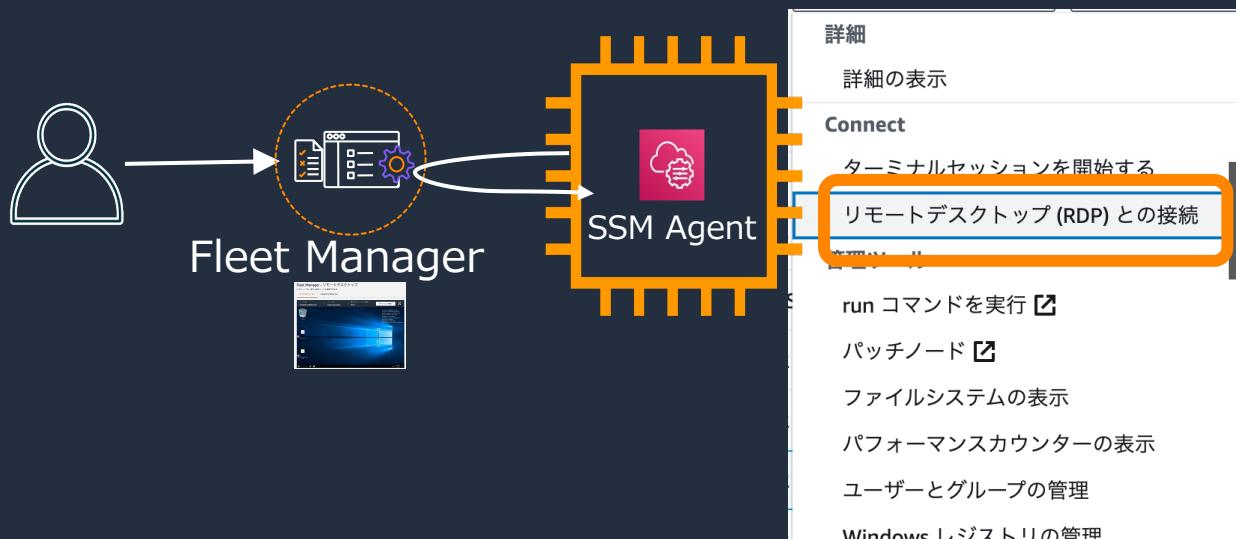


Remediate Issues

Fleet Manager

Windows サーバへのリモートデスクトップ機能

- Windows サーバーには、マネジメントコンソールからリモートデスクトップ (RDP) 接続も可能。

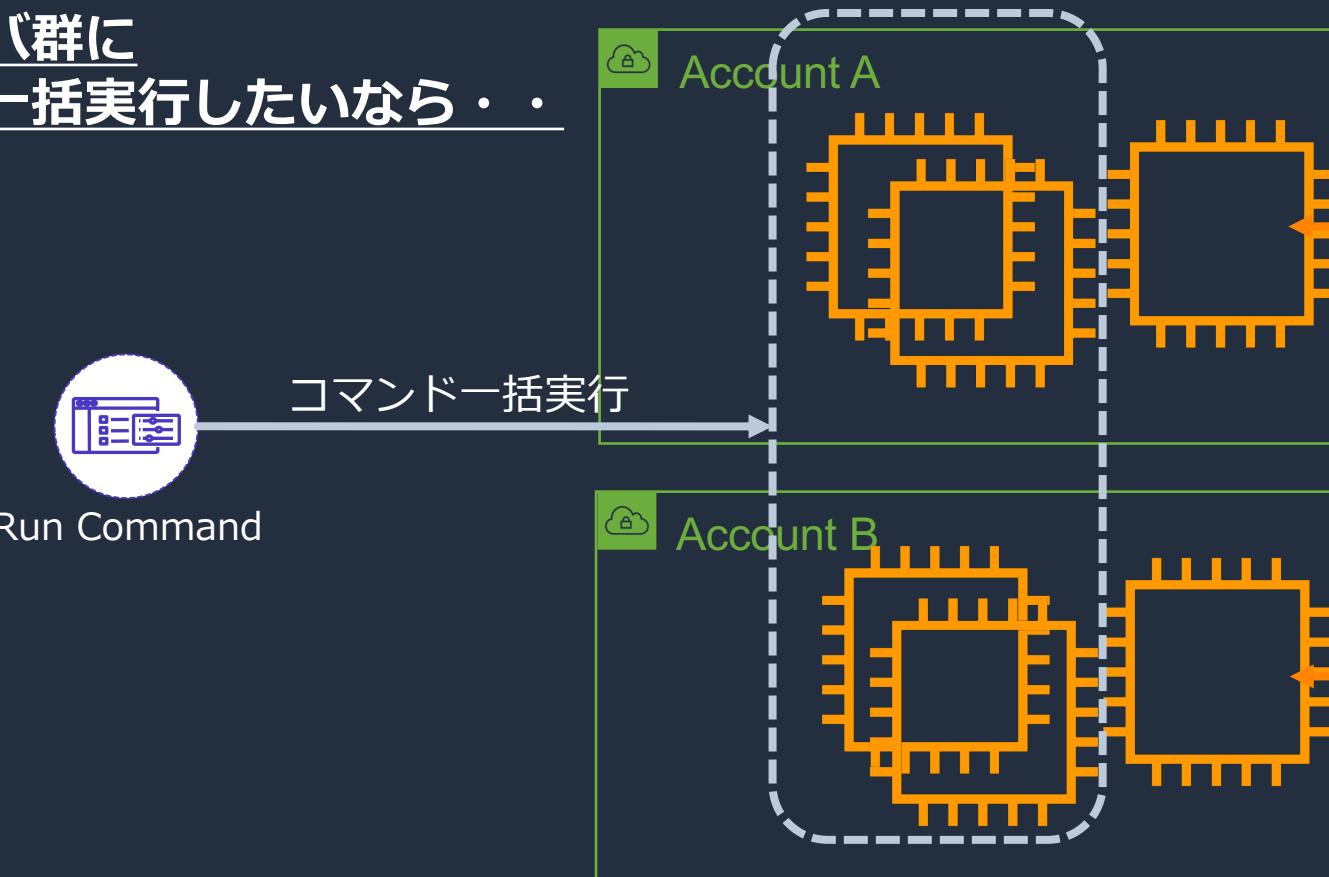


aws Fleet Manager の RDP 接続機能については[こちら](#)

© 2023, Amazon Web Services, Inc. or its affiliates.

おさらい

対象サーバ群に
コマンド一括実行したいなら・・



個々のサーバに対して
インタラクティブにコマンド
操作したいなら・・



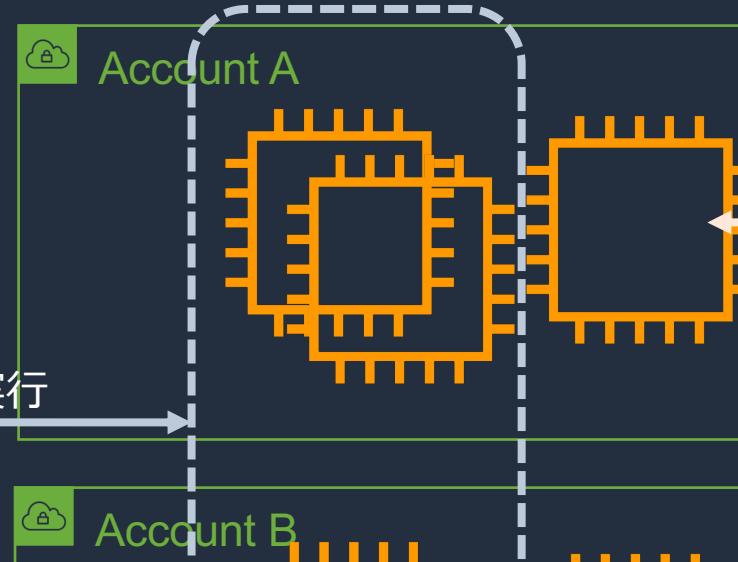
おさらい

対象サーバ群に
コマンド一括実行したいなら・・



Run Command

コマンド一括実行



個々のサーバに対して
インタラクティブにコマンド
操作したいなら・・

シェルアクセスなど



Session Manager

インシデント管理って
どうしたらしいいの？



Incident Manager



Incident Manager

事前に準備された対応計画、ランブック、分析による改善

Remediate Issues

- アラームへの対応計画を指定し、適切な連絡先に自動通知、Runbook を自動起動し、迅速な対応が可能になる。
- チームはチャットで共同作業を行いながら問題を解決できる。
- インシデント後の分析ができ、将来の再発を防止できる。
- ServiceNow, Jira Service Management と連携可能



The screenshot shows the AWS Systems Manager Incident Manager interface. At the top, there's a navigation bar with 'AWS Systems Manager > Incident Manager > [BananaStand] Customer checkout failures'. On the right, there's a 'Resolve Incident' button. Below the navigation, there's a summary card with the title '[BananaStand] Customer checkout failures', impact level 'Critical', chat channel '#order-processor', duration '8m', and an 'Edit' button. The main area is divided into sections: 'Overview' (selected), 'Metrics', 'Timeline', 'Runbook', 'Contacts', and 'Related items'. The 'Overview' section contains a 'Summary' card with the status 'Incident in Progress' indicated by three orange icons. It also includes a 'Summary of Incident' section with a message about customers unable to checkout due to connectivity failures, and a 'Current Status' section with three yellow icons. Below these are 'Recent timeline events' listed from April 8, 2021, including metrics added, summary updated, runbook status updated, and custom events.

aws Incident Manager についての詳細は[こちら](#)。

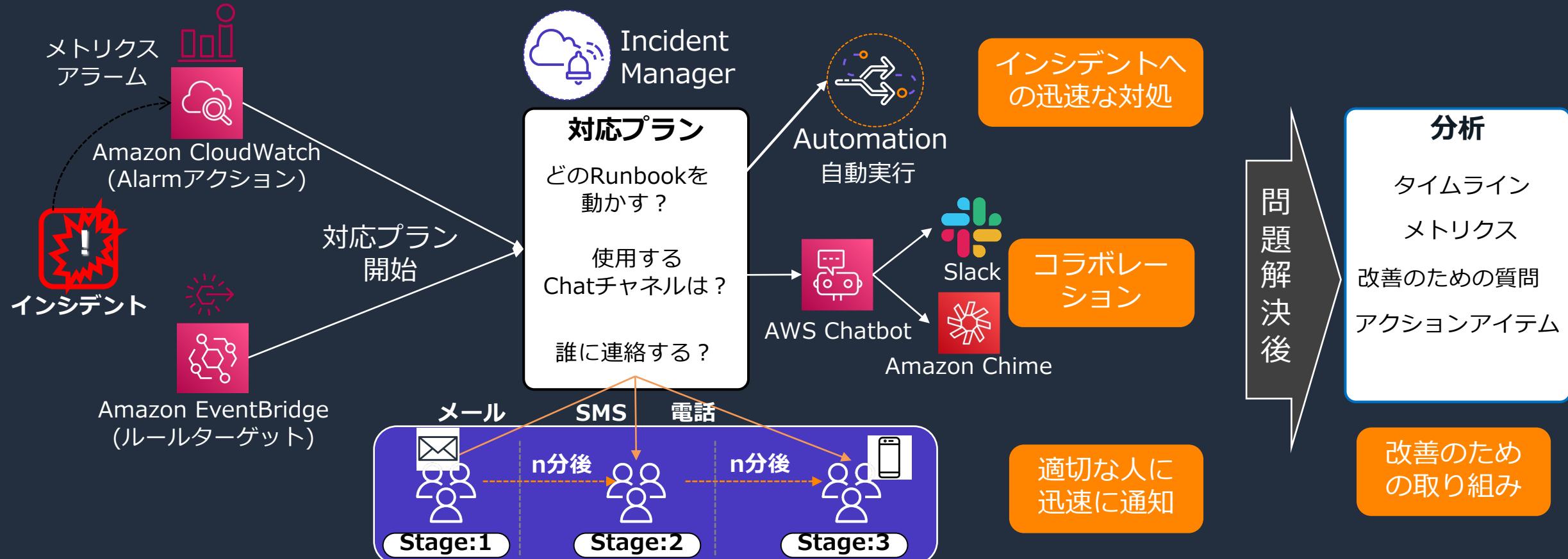
© 2023, Amazon Web Services, Inc. or its affiliates.



Remediate Issues

Incident Manager

事前に準備された対応計画、ランブック、分析による改善



aws Incident Managerについての詳細は[こちら](#)。

© 2023, Amazon Web Services, Inc. or its affiliates.

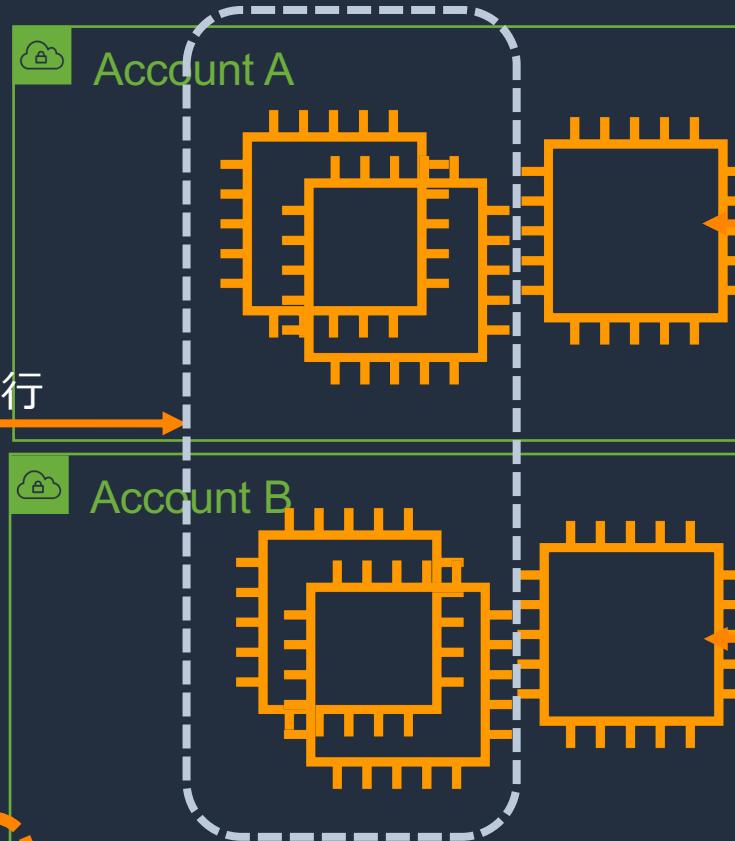
おさらい

対象サーバ群に
コマンド一括実行したいなら・・



Run Command

コマンド一括実行



個々のサーバに対して
インタラクティブにコマンド
操作したいなら・・



Session Manager

リモートデスクトップ接続



Fleet Manager

AWS Systems Manager の機能

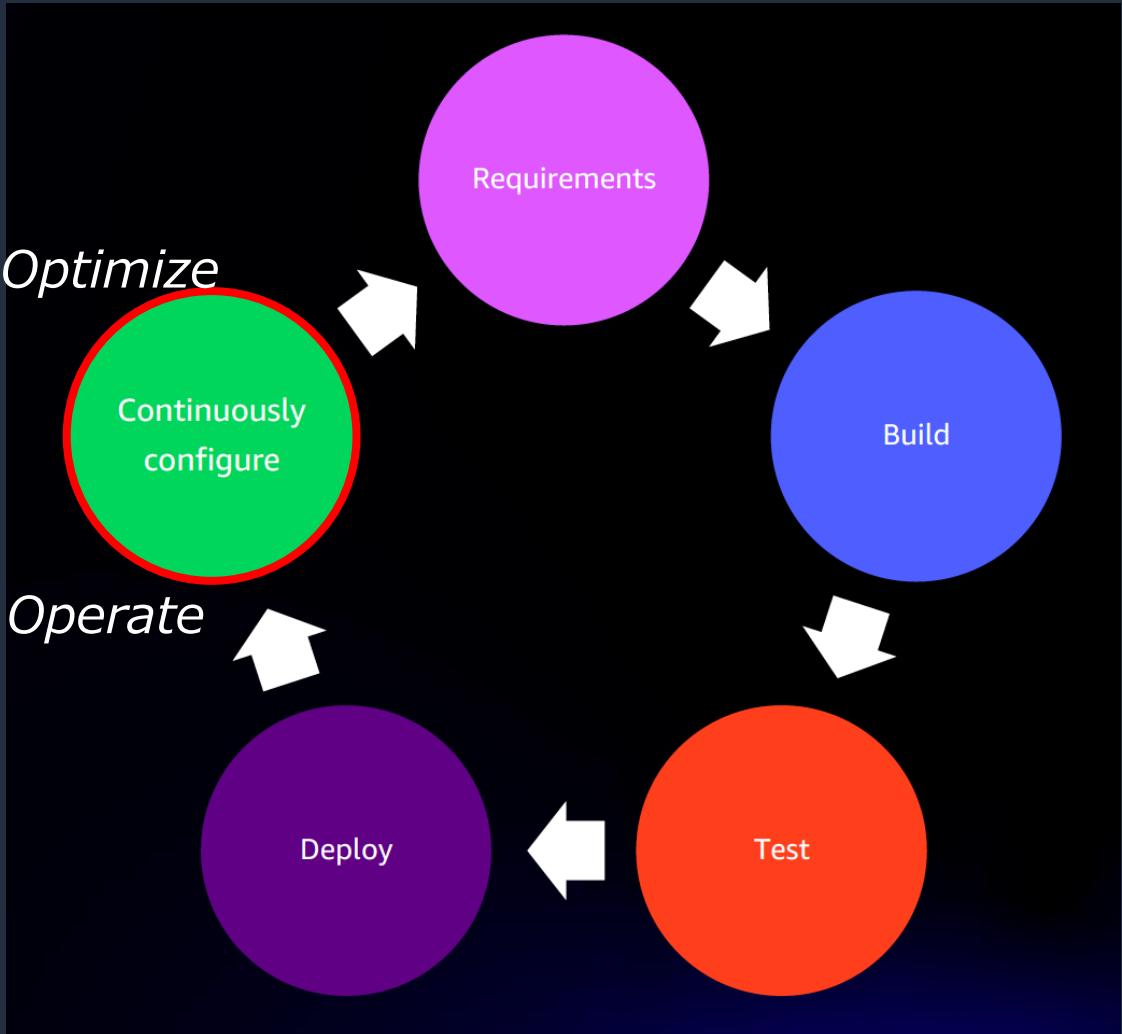


AWS Systems Manager の機能



Application Management

- アプリケーションはローンチして終わりではない。
- メンテナンスも含めて、ライフサイクルの管理が必要。
- 運用し、最適化していくための機能を用意。

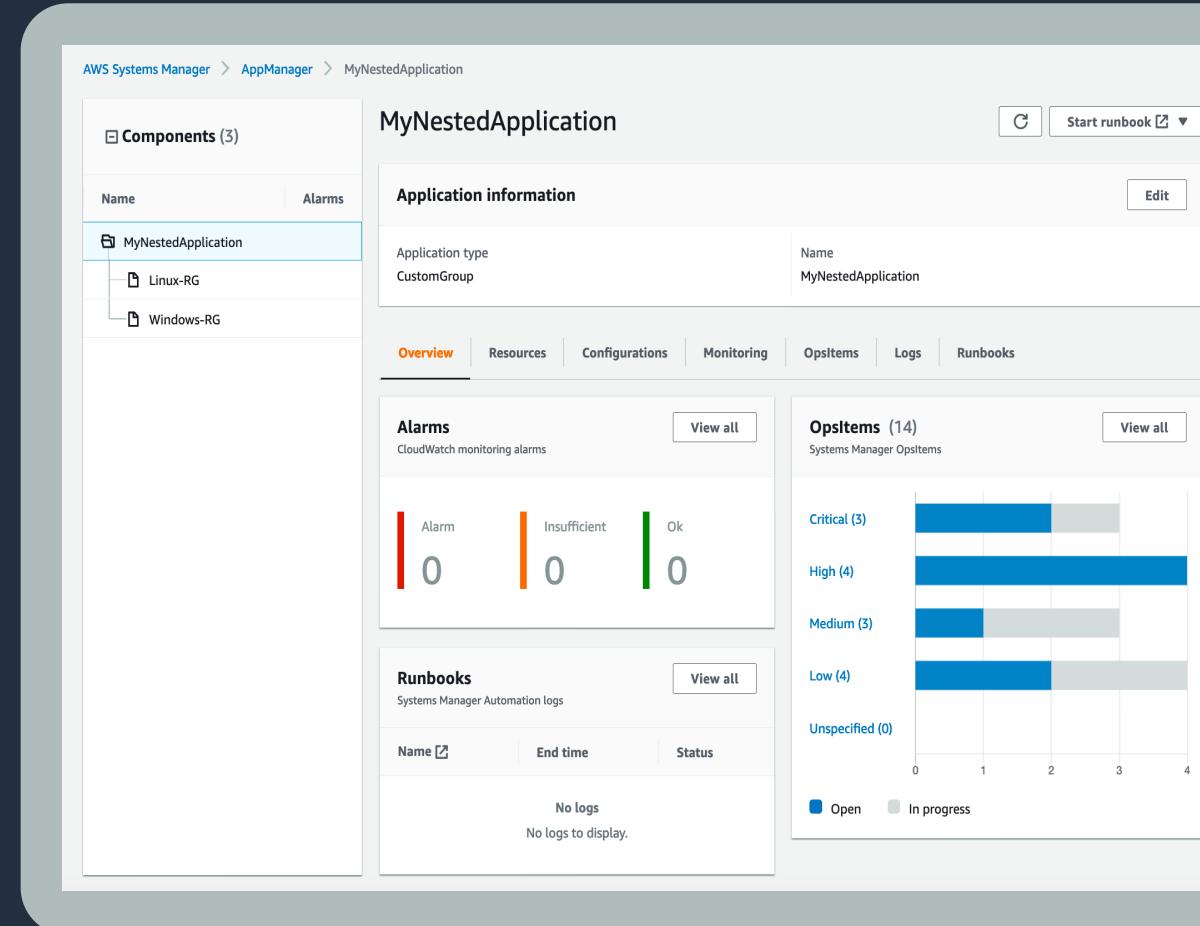


Application Manager

個々のリソースだけでなく、アプリケーションを管理する

- 一つのコンソールからアプリケーションを管理できる。
- アプリケーションのコンテキストで、CloudWatch アラームやコンプライアンスステータス、アプリケーションコストなどが確認できる。
- これらの AWS サービスをまだ有効にしている場合、Application Manager のコンソールから簡単に設定も可能

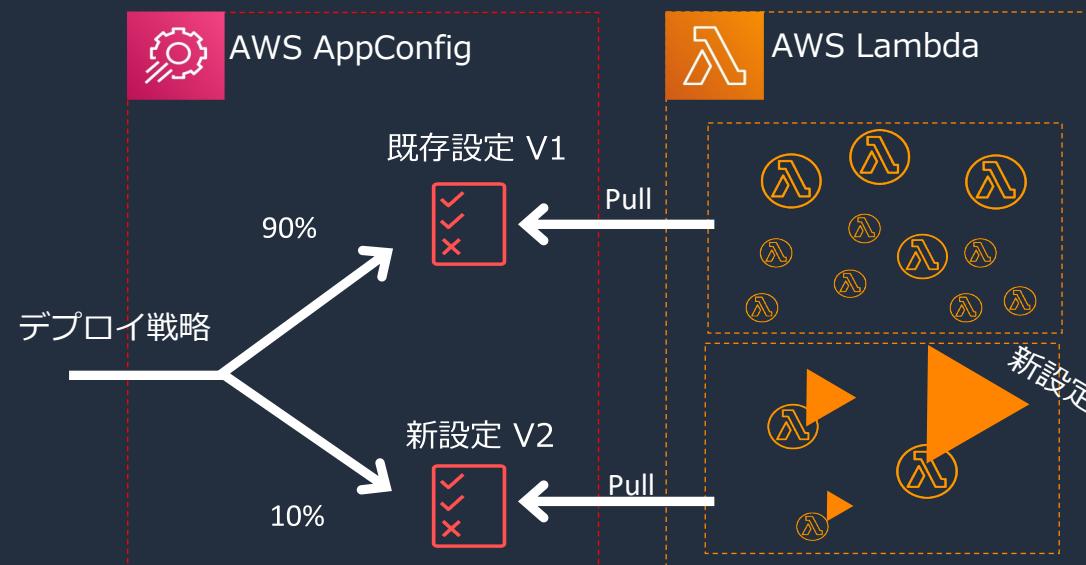
NEW
2022/07



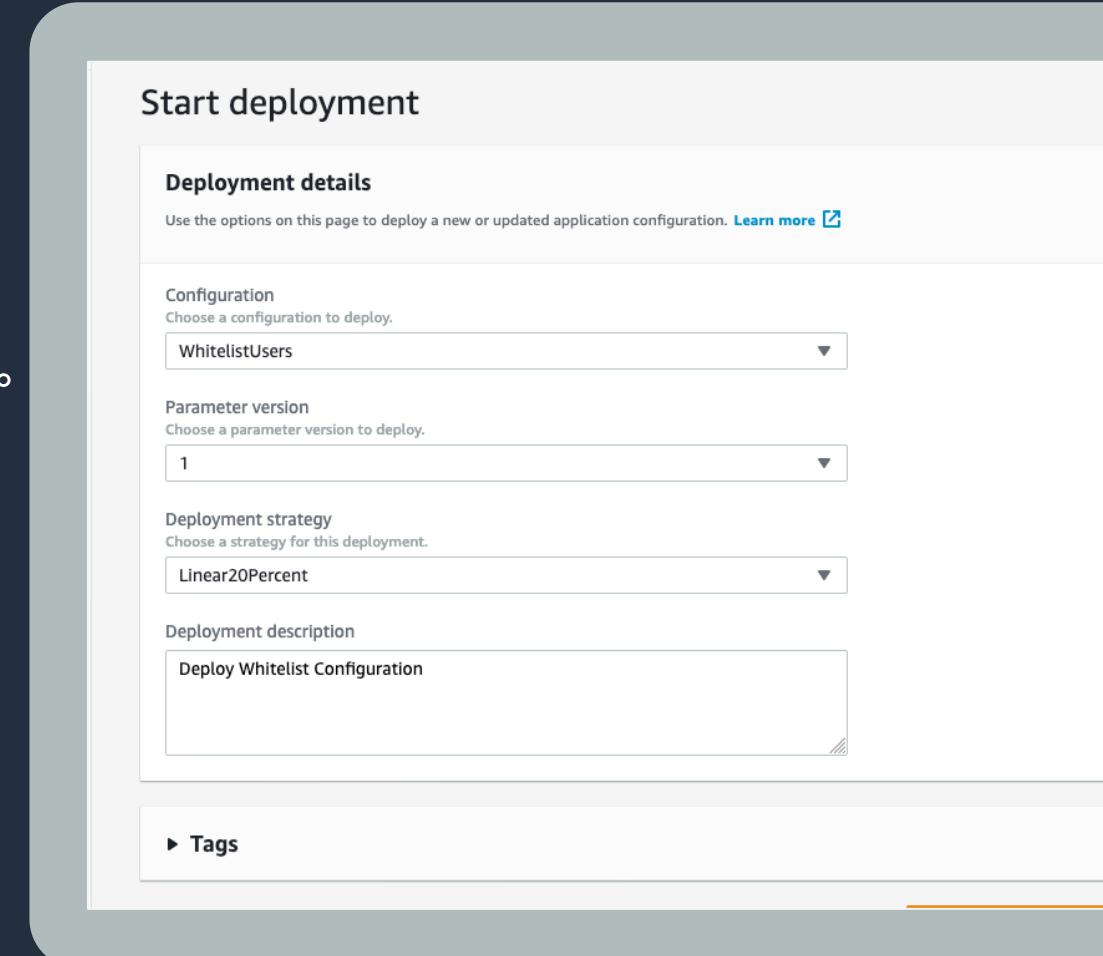
AppConfig

アプリケーション構成を作成、管理、デプロイ

- アプリケーションを実行したまま、
アプリケーション構成の変更をデプロイ。
- 製品の新発表など、タイムリーな展開が必要な
新機能の展開を、機能フラグで実現。
- デプロイ戦略を指定でき、少しずつデプロイが可能。



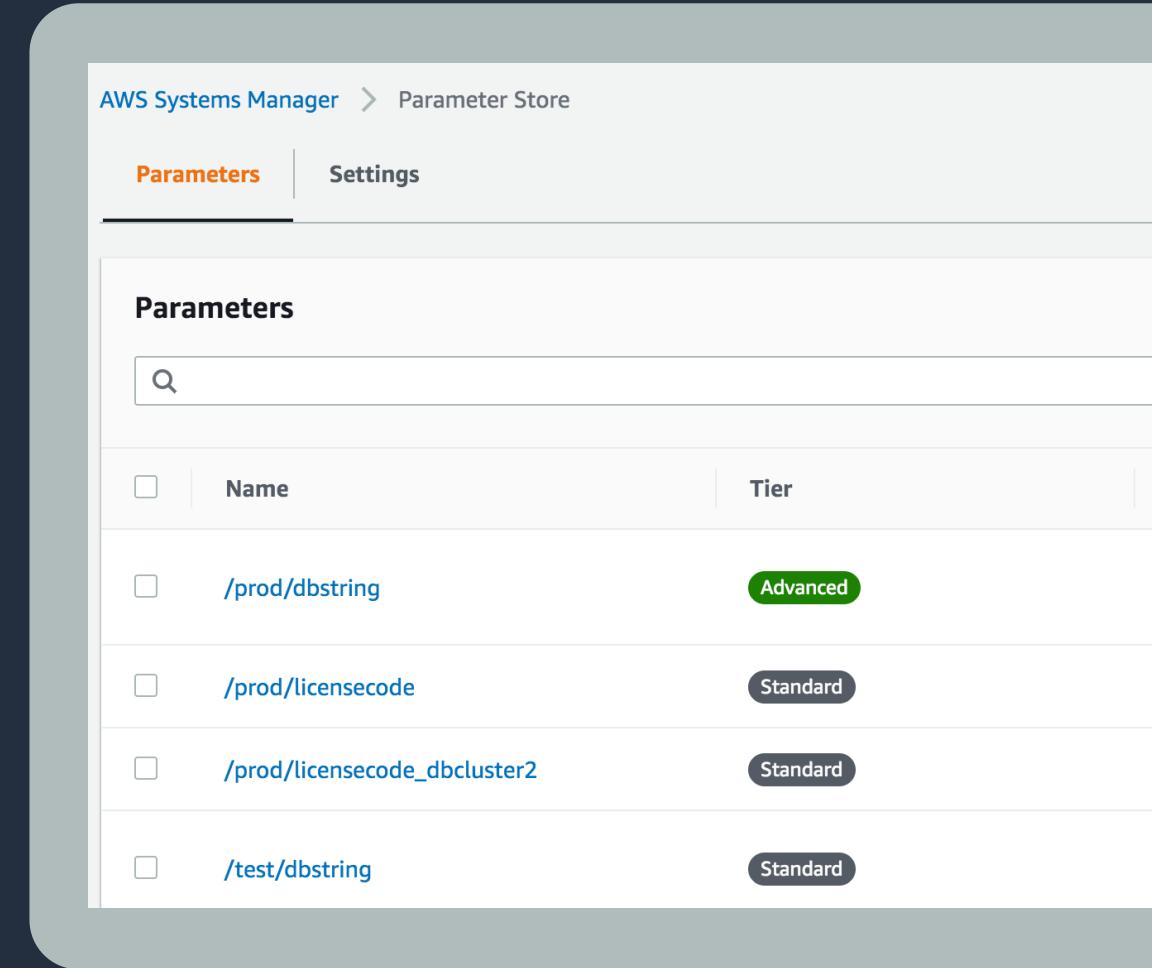
aws AppConfig についての詳細は[こちら](#)。



Parameter Store

アプリケーション構成値の一元的な格納

- ④ アプリケーションの設定値とシークレットを格納。
- ④ すべてのパラメーターを 1 か所で一元的に更新することで、コードのメンテナンスと自動化を簡素化。



 Parameter Store についての詳細は[こちら](#)。

AWS Systems Manager の機能

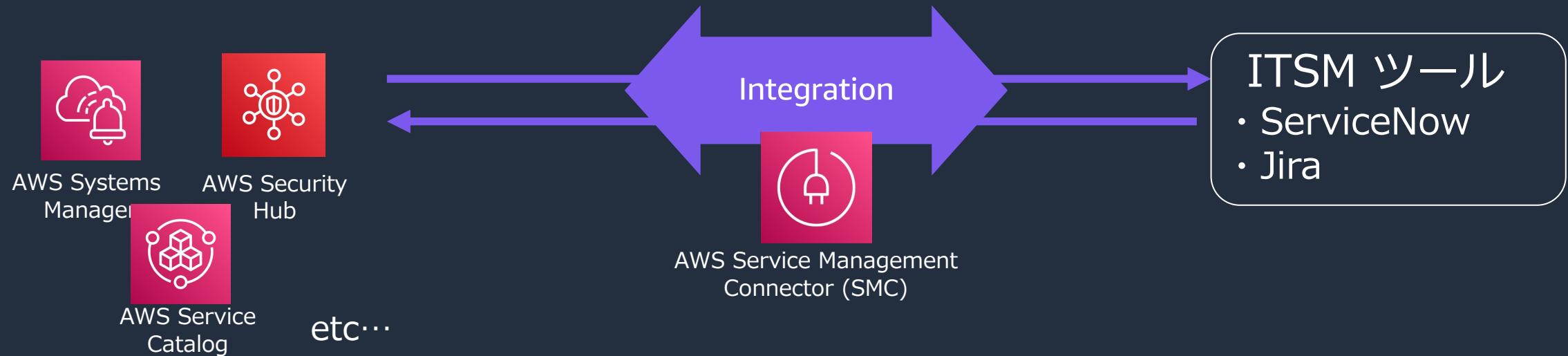
運用管理	アプリケーション管理	変更管理	ノード管理
 Explorer	 Application Manager	 Change Manager	 Fleet Manager
 OpsCenter	 AppConfig	 Automation	 Session Manager
 Incident Manager	 Parameter Store	 Maintenance Windows	 Inventory
		 Change Calendar	 Run Command
			 Patch Manager
			 Distributor
			 State Manager

Quick Setup

3rd Party の ITSM ツールとの連携

AWS Service Management Connector (SMC)

- ServiceNow や Jira などの使い慣れた ITSM ツールで AWS ネイティブのリソースと機能を管理、操作するためのコネクター
- 対象の ITSM ツール (2023/2現在)
 - ServiceNow
 - Atlassian Jira Service Management



aws SMCの詳細は[こちら](#)。

AWS Systems Manager にて連携できる機能

ITSM ツール	SSM Features	詳細
ServiceNow	OpsCenter	ServiceNow で OpsCenter 統合機能を有効にできる。ServiceNow で実行されたアクションを OpsCenter と同期、また、その逆の場合も同様に同期可能
	Incident Manager	Incident Manager でインシデント対応計画を自動化し、インシデントを ServiceNow に自動的に同期できる。インシデントの解決も可能。
	Automation	ServiceNow にて Runbook の実行・確認が可能。
	Change Manager	変更テンプレート、変更リクエストの確認、変更リクエストの実施、関連する CloudTrail イベントの確認が可能。 ※ 変更テンプレートがApprove済みなど前提あり。詳細は こちら
Jira Service Management	OpsCenter	Jira で OpsCenter 統合機能を有効にできる。ServiceNow で実行されたアクションを OpsCenter と同期、また、その逆の場合も同様に同期可能。
	Incident Manager	Incident Manager でインシデント対応計画を自動化し、インシデントを JSM に自動的に同期できる。インシデントの解決も可能。
	Automation	Jira にて Runbook の実行・確認が可能。

NEW
2022/6

NEW
2022/10

AWS Service Management Connector for ServiceNow の詳細は[こちら](#)

AWS Service Management Connector for Jira Service Management Data Center の詳細は[こちら](#)

AWS Service Management Connector for Jira Service Management Cloud の詳細は[こちら](#)



Systems Manager の セキュリティベストプラクティス



SSM を使用する上でのセキュリティーベストプラクティス

- ・ 「Systems Manager のセキュリティのベストプラクティス」をご参照ください
 - https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/security-best-practices.html

<一部を紹介>

- ・ 最小特権アクセスを実装する
 - ・ ユーザの IAM ポリシーは、該当リソース・特定アクションについてのみ有効に
 - ・ 例えば“ssm.StartSession”を Deny することで、セッションマネージャを使用しない設定が可能。
- ・ VPC エンドポイントを使用可能
- ・ 特別セキュアな処理が必要な場合は Session Manager に对话型コマンドのみを使用する
- ・ AWS および Systems Manager ツールを最新に保つ
- ・ CloudWatch / CloudTrail / AWS Config を使用

Systems Manager の料金

AWS Systems Manager の料金

- AWS Systems Manager の利用は**基本的に無料**
- 一部の機能は有料。詳細は[料金ページ](#)を参照してください。
 - OpsCenter (OpsItem の数とAPI コールの数に基づく課金)
 - IncidentManager (対応計画の数とSMS/音声メッセージの数に基づく課金)
 - AppConfig (APIコールの数とターゲットごとの構成更新の合計数に対して課金)
 - Parameter Store (アドバンスドパラメータ/スループットの上限を上げた場合課金)
 - Change Manager (変更リクエストの件数と API リクエスト数に基づく課金)
 - Automation (ステップカウント、ステップ実行時間、プレイブックに対して課金)
 - Distributor (独自パッケージのストレージ、APIコール、データ転送に基づく課金)
 - オンプレミス管理のアドバンストインスタンスティア (次ページ参照)
- その他関連サービスの使用量に応じた料金
 - Athena + QuickSight / Config / CloudWatch (カスタムメトリクス、Logs) / S3に格納したログデータ など

(参考) インスタンスティアの設定

- SSMでは、ハイブリッド環境のオンプレミスサーバ、エッジサービスおよび仮想マシン(VM)に、標準インスタンスティアとアドバンストインスタンスティアを提供。

	標準インスタンスティア (デフォルト)	アドバンストインスタンスティア
課金	無料	インスタンス実行時間に基づく 従量課金
登録できる サーバ数	リージョン/アカウントごとに 最大1000まで	リージョン/アカウントごとに 1000を超えるサーバを登録可能
その他	登録されているハイブリッドノードが 1,000 未満であっても、以下の場合はアドバンストインスタンスティアが必要 <ul style="list-style-type: none">EC2 以外のノードに接続するために Session Manager を使用したい。EC2 以外のノードで Microsoft がリリースしたアプリケーションにパッチを適用したい ※両者とも、EC2インスタンスでは無料で使用できます。	

まとめ



まとめ

- AWS Systems Manager は一つの統合された運用ソリューションとして進化しています。
- まずは SSM Agent を立ち上げてマネージドノードにするところから、ぜひ始めてみてください。
- AWS Systems Manager の活用により、みなさまの運用が、少しでも楽になりますように。

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!