AWS-20

# クラウドのシステム運用最前線！
# 上手く使いこなし運用を楽にしよう。

石橋 香代子
技術統括本部 シニアソリューションアーキテクト
アマゾン ウェブ サービス ジャパン合同会社

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# 自己紹介

## 石橋 香代子 (いしばし かよこ)

シニアソリューションアーキテクト

- 流通・小売業界のエンタープライズ企業をサポート
- 運用系サービス

好きなAWSのサービス： **AWS Systems Manager**
**Amazon CloudWatch**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# このセッションでお話しすること

- ✓ 話すこと：
  - AWS Systems Manager の全体像
  - AWS Systems Manager の全体像を把握する上で必要となる各機能のオーバービュー

- ✓ お願いしたい心構え：
  - AWS Systems Manager は多機能です。各機能のオーバービューだけでも、30分では情報量が多いです。
  - 本セッションでは一気にご紹介しますので、詳細は後ほど資料を振り返っていただければと思います。

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Agenda

1. **AWS Cloud Operations** の全体像
2. **AWS Systems Manager** で実現する一元化された運用管理
3. **AWS Systems Manager** で実現するアプリケーション管理
4. マルチアカウント・ハイブリッド環境での使用

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# AWS Cloud Operations の全体像

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# AWS Cloud Operations がもたらす効果

**Cost savings**

5 年間のコスト
オペレーションの
**51%** 低下

**Staff productivity**

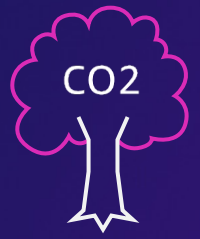
ITインフラストラクチャ
スタッフの効率が
**62%** 向上

**Operational resilience**

ダウンタイムが
**57%** 減少

**Business agility**

市場投入までの時間を
**37%** 短縮




**Carbon savings**

IT 運用の
二酸化炭素排出量を
**88%** 削減

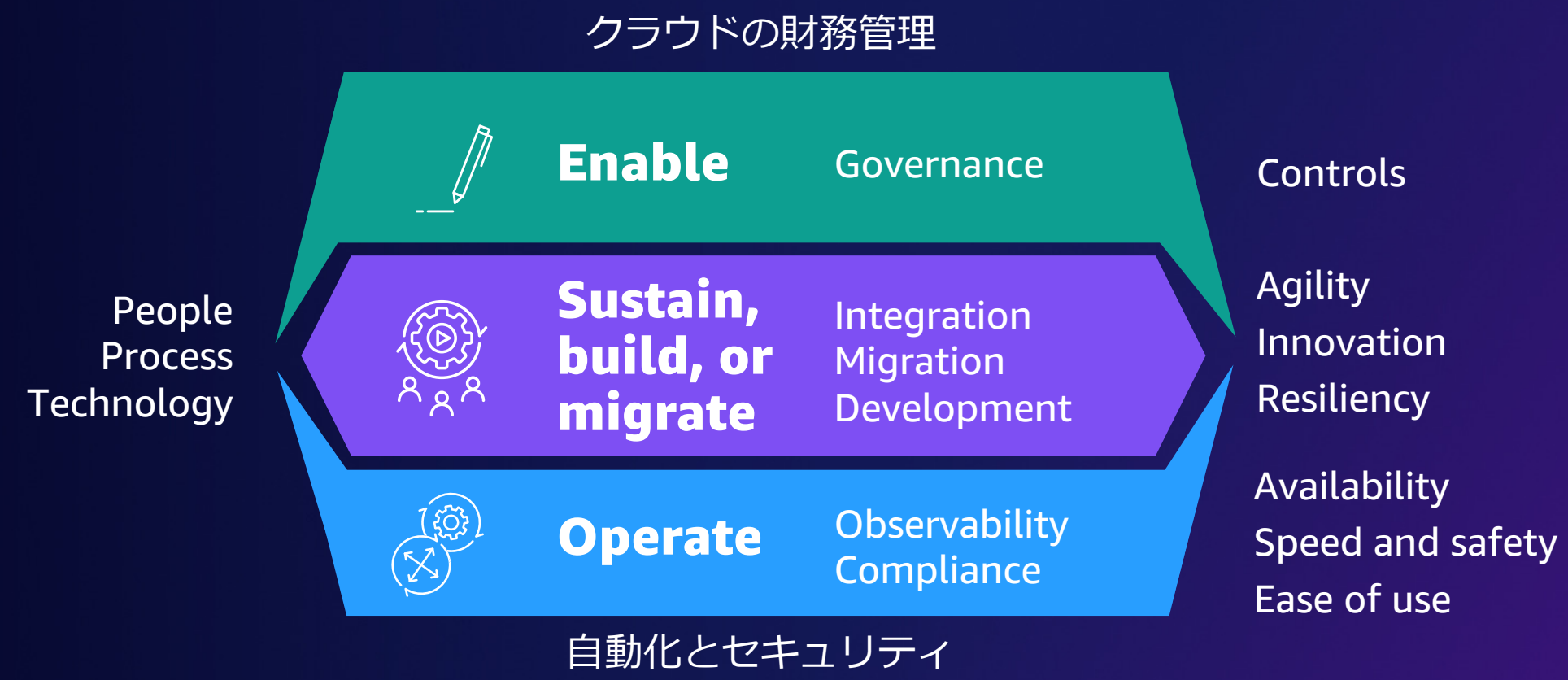
1,500 社の AWS エンタープライズ顧客を対象とした独立した調査に基づく

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# **AWS Cloud Operations** で
# ビジネスアジリティとガバナンスの両方を得る

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# AWS Cloud Operations の全体像



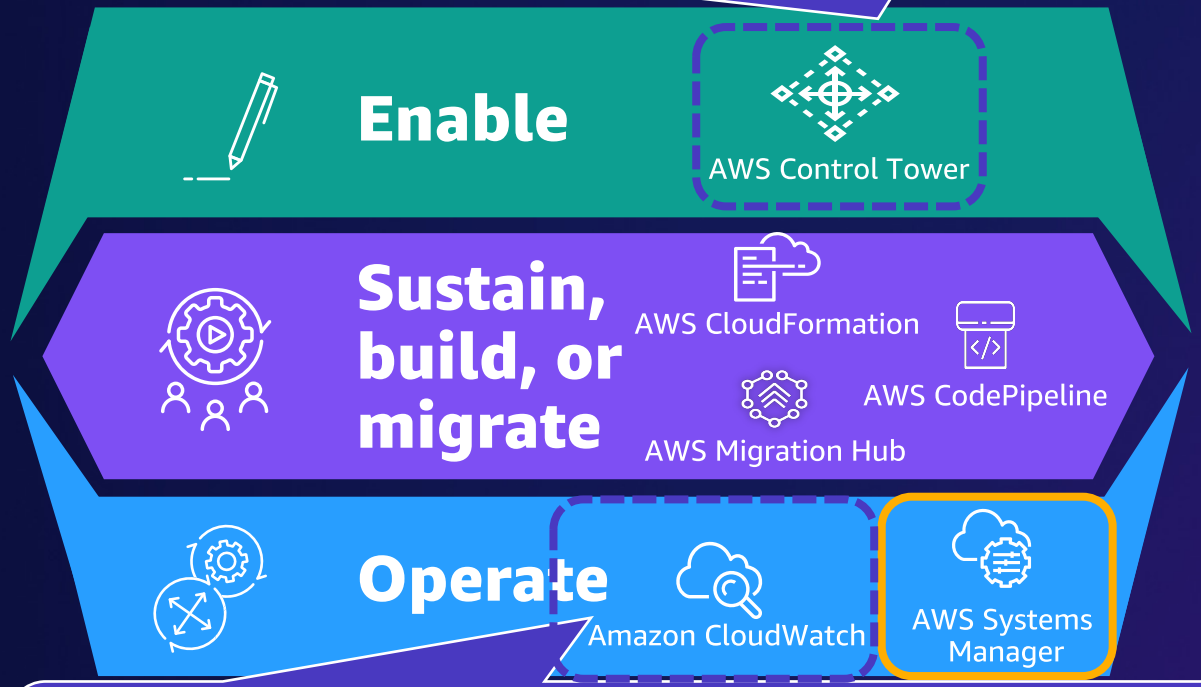

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# AWS Cloud Operations の全体像

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# AWS Cloud Operations の全体像

***AWS-19***
セキュアでスケーラブルなAWSアカウント統制プラクティス
最新動向




People
Process
Technology

Controls

Agility
Innovation
Resiliency

Availability
Speed and safety
Ease of use

***AWS-21***
AWSのObservability（可観測性）の全体像
～Amazon CloudWatchとオープンソースの活用～

© 2022, Amazon Web Services, Inc. or its affiliates

# **AWS Systems Manager** で実現する一元化された運用管理

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# AWS Systems Manager

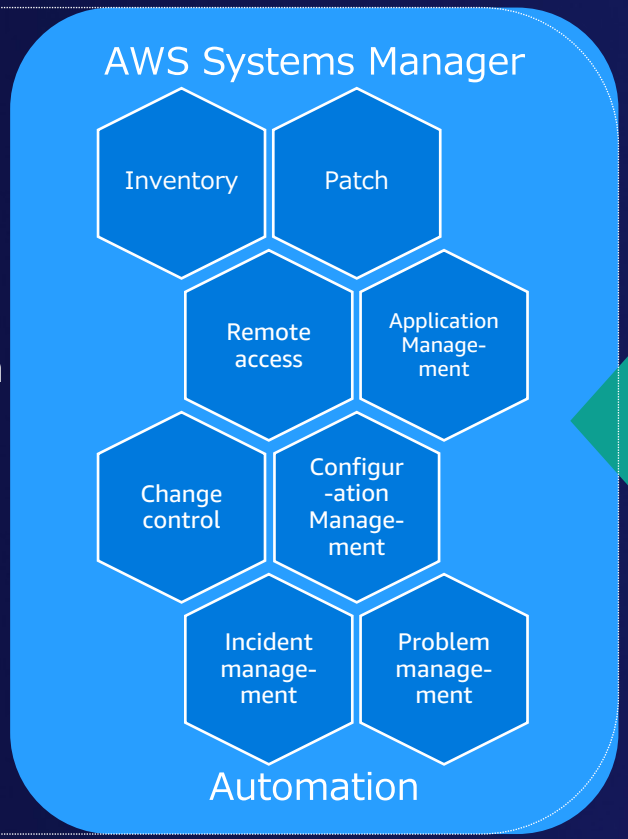
## ハイブリッドクラウド環境のための安全なエンドツーエンドの管理ソリューション

**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

Cloud On-premises Edge

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

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

(*) 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

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# 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

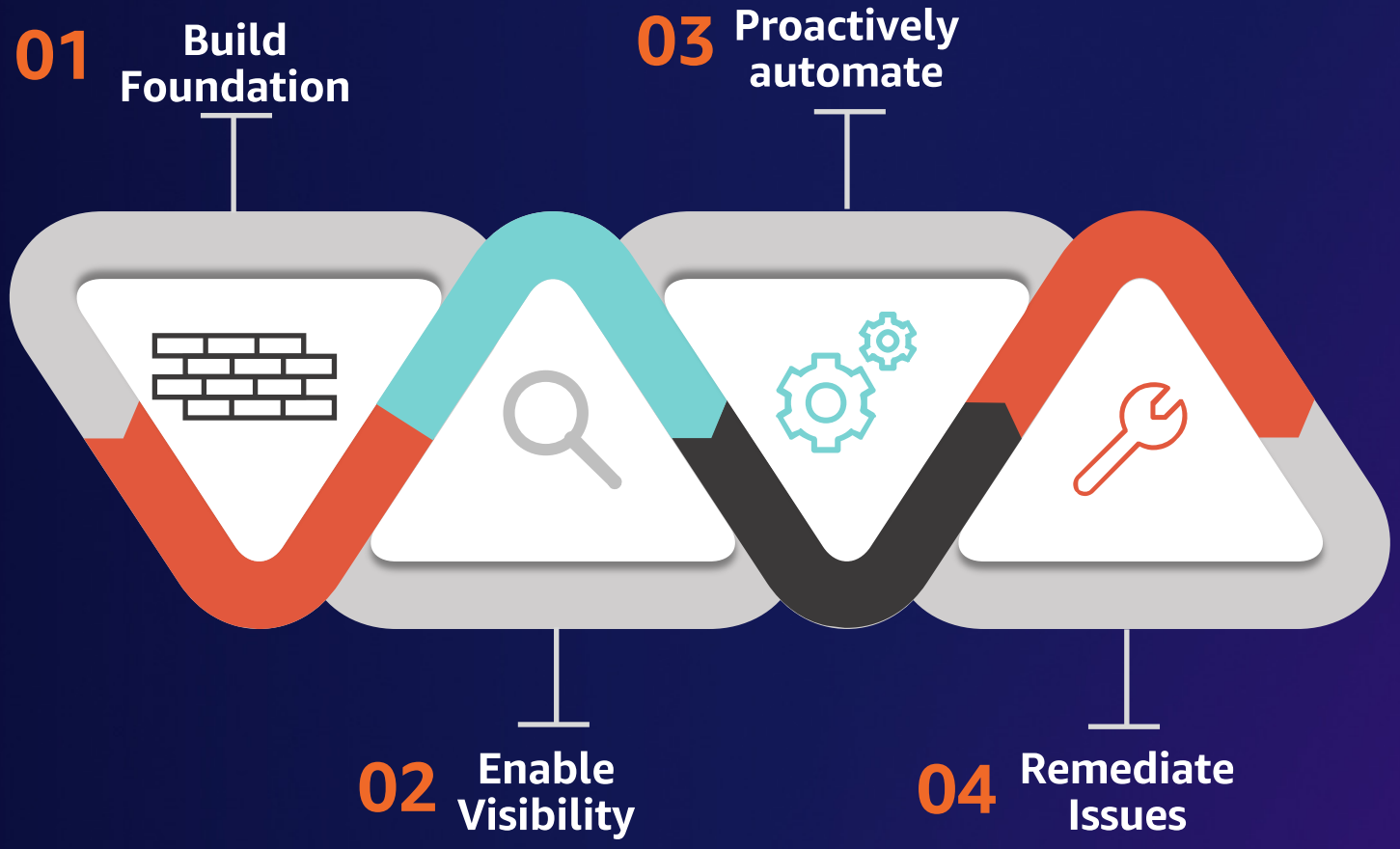
Distributor

State Manager

Quick Setup

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# コンプライアンスを実現するための 4 段階の実装

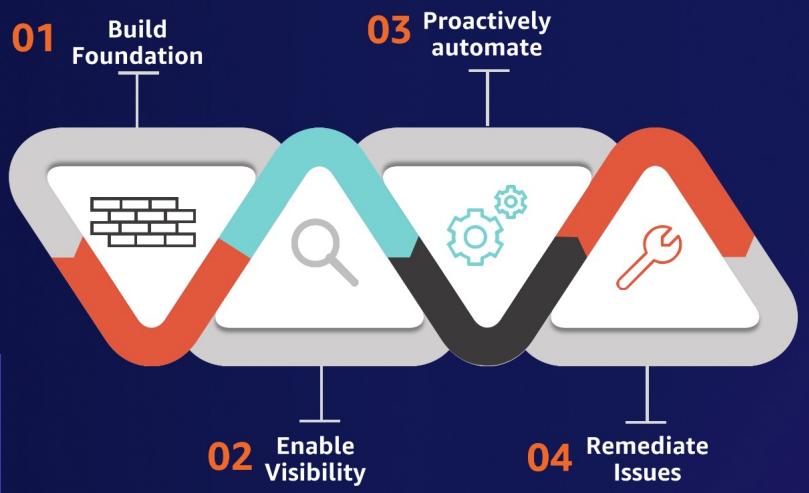



aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# 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




## 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

ハイレベルやノードレベルの
ダッシュボードと管理

## 02. Enable Visibility

ノードへの一括コマンド発行や、
安全な特権アクセス

## 04. Remediate Issues

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# 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

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

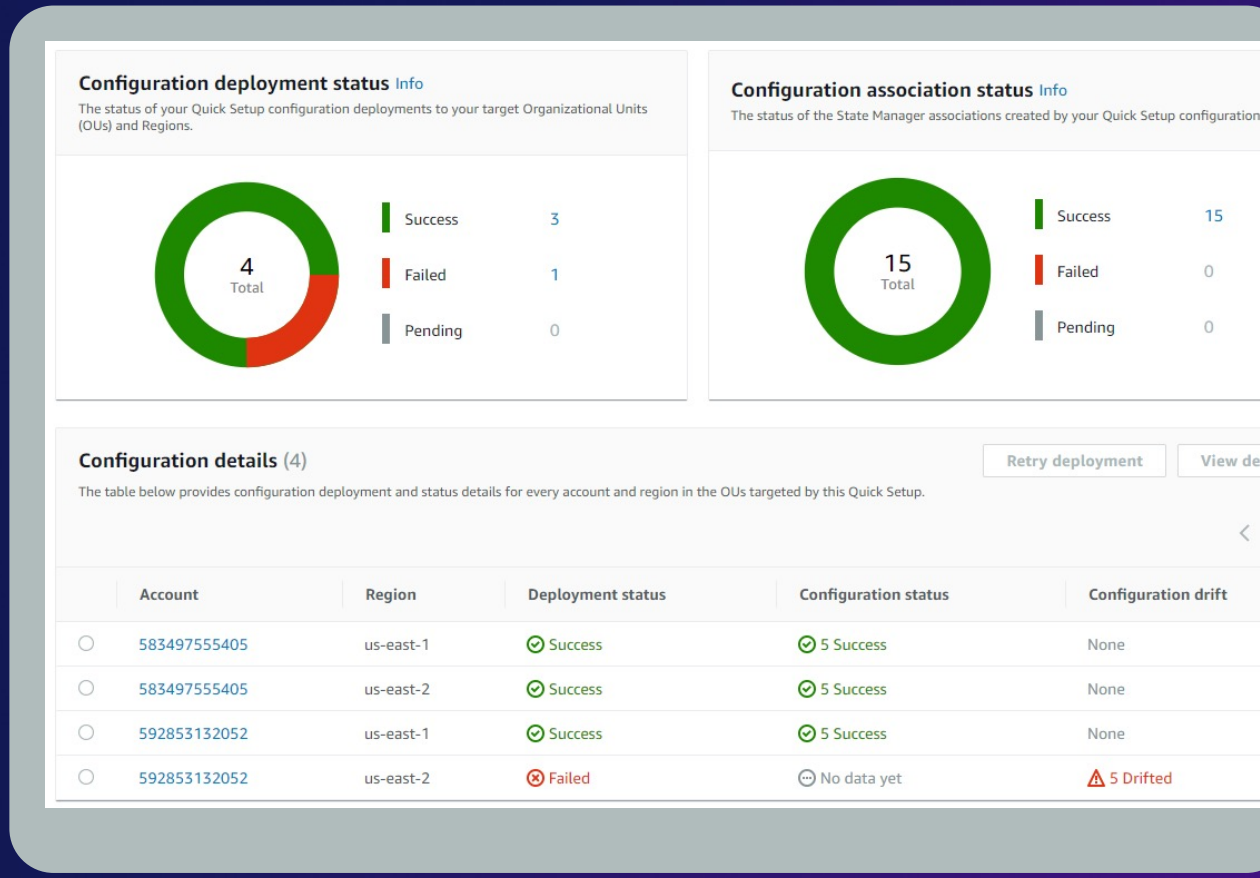
Build Foundation

# 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<br>AWS Systems Manager | Config Recording<br>AWS Config | Conformance pack<br>AWS Config |
| Change Manager<br>AWS Systems Manager | DevOps Guru<br>Amazon DevOps Guru | Distributor<br>AWS Systems Manager |




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Quick Setupの詳細はこちら。

# 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

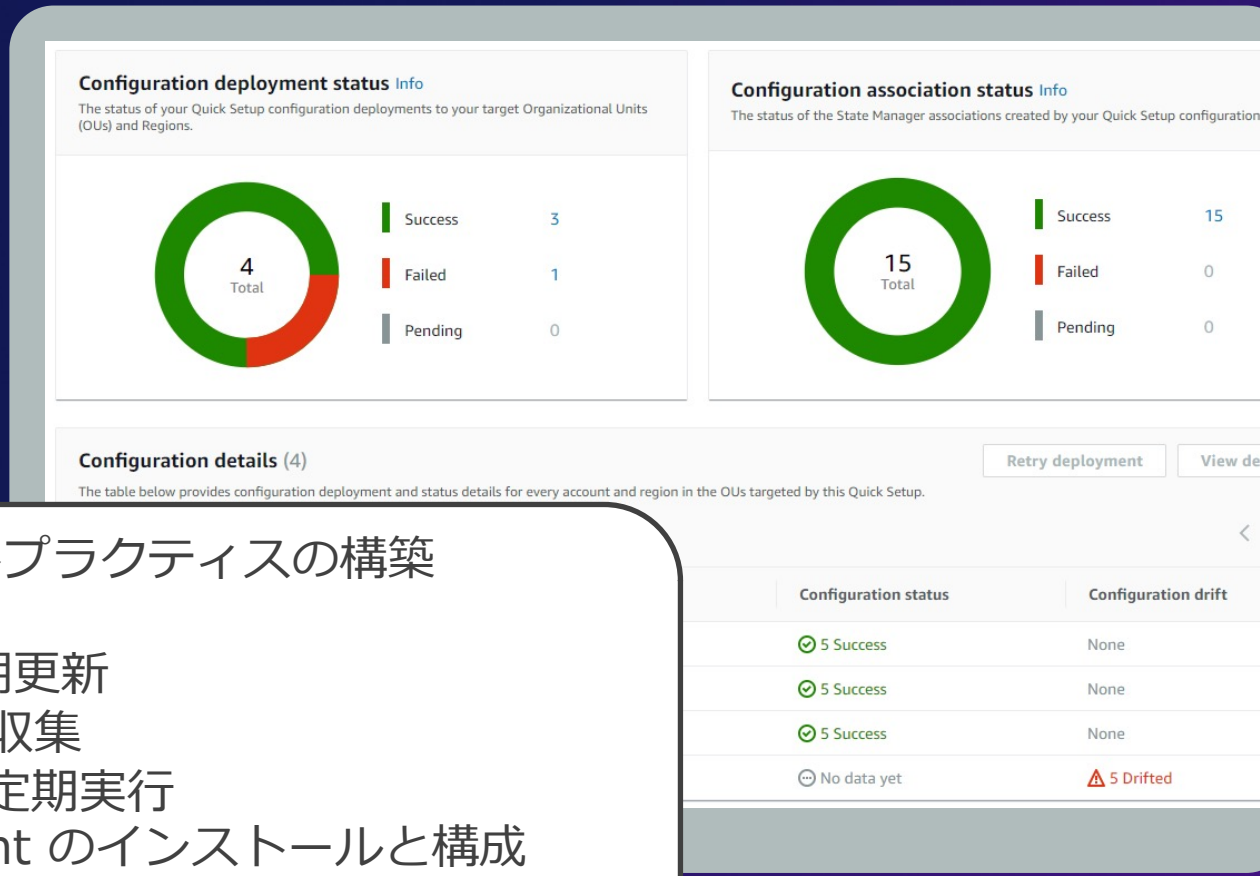
Conformance pack

Change Manager

AWS Systems Manager

DevOps

Amazon DevOps




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
- パッチスキャンの定期実行
- CloudWatch Agent のインストールと構成
- CloudWatch Agent の定期更新

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

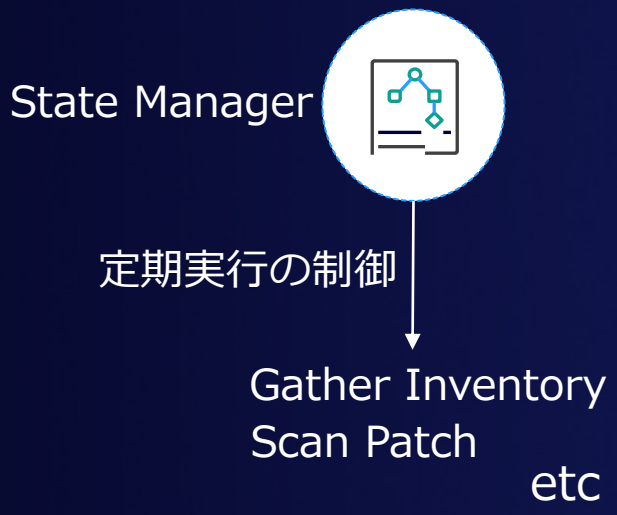
Quick Setup の Host Management についてはこちら。

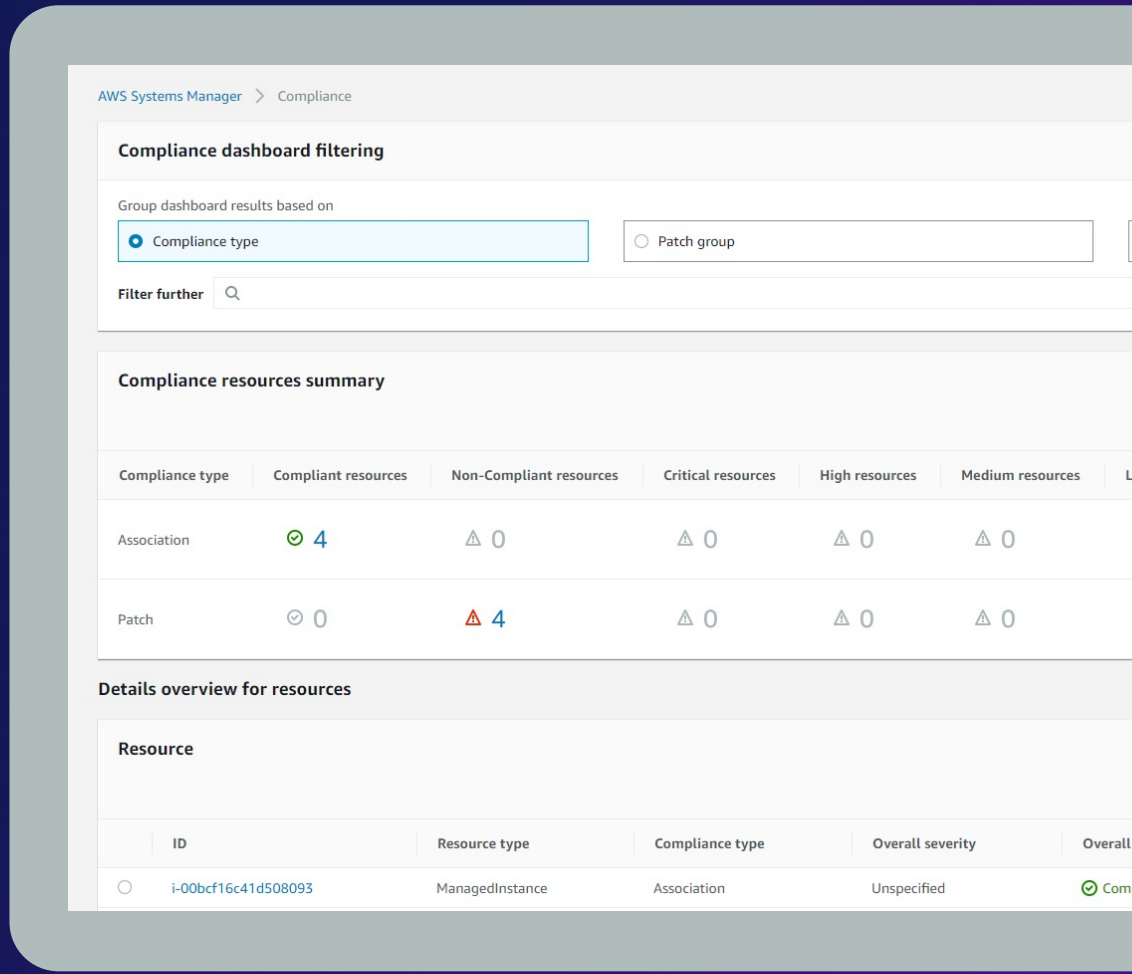
Build Foundation

# 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。



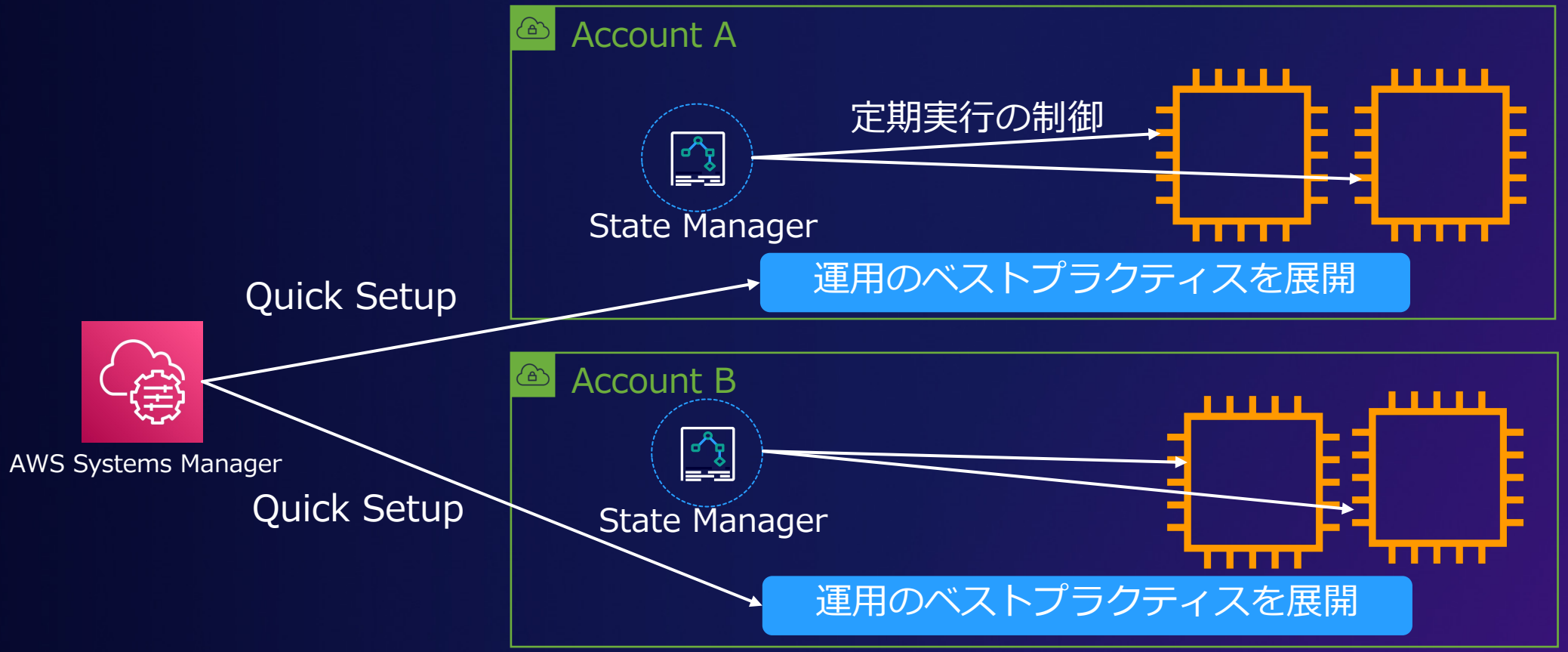




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

State Manager については、こちら。

# おさらい

ここまでで何ができたかというと・・・




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# 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

- Explorer
- OpsCenter

ノードの状態を俯瞰・確認する

- Fleet Manager
- Inventory

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Enable Visibility

# Explorer

## ハイレベルの運用ダッシュボード

- 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

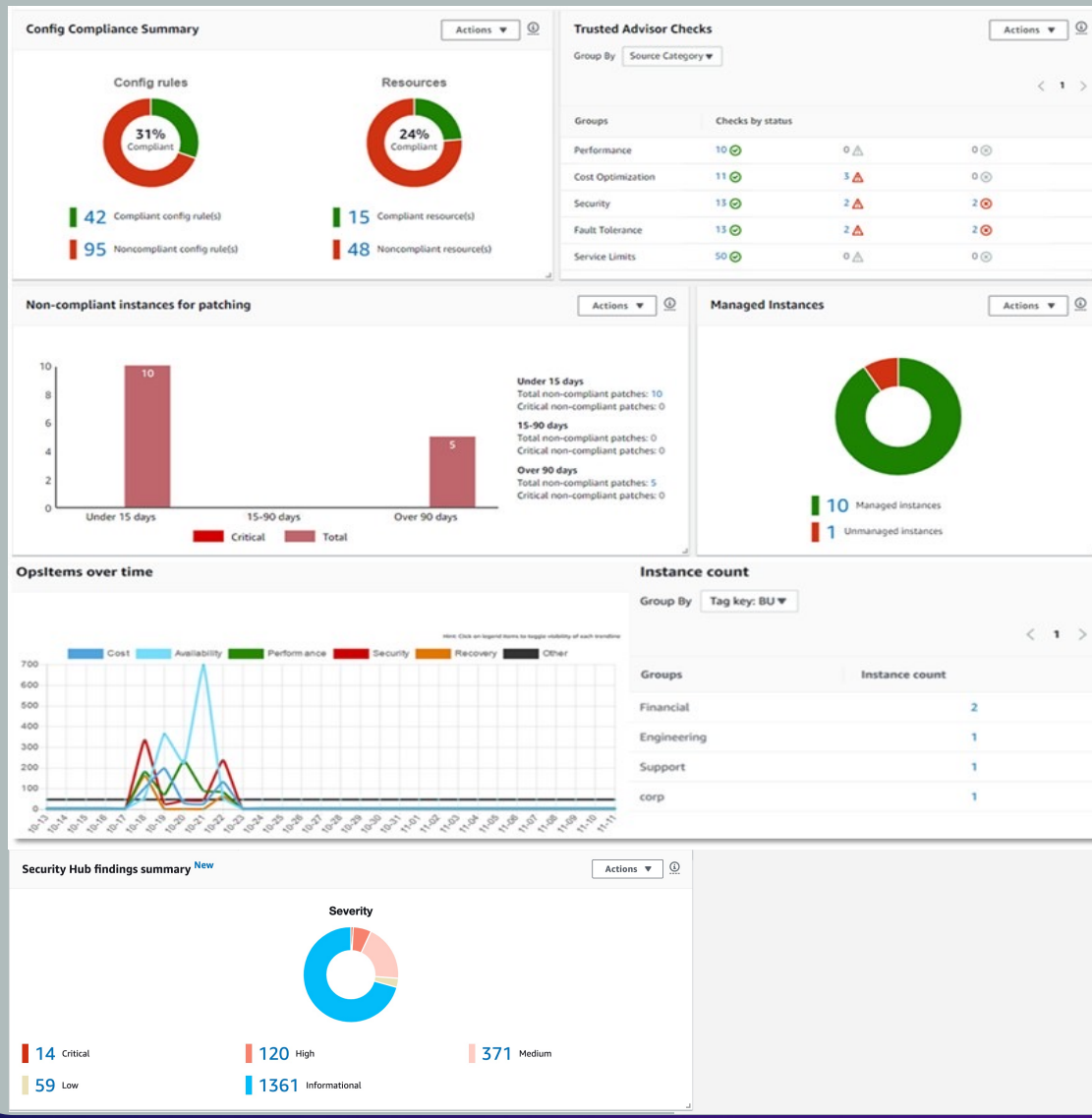
AWS Security Hub

AWS Systems Manager

Patch Compliance

OpsCenter OpsItems

Inventory




Explorerについての詳細はこちら。

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Explorer

Enable Visibility

## ハイレベルの運用ダッシュボード

- 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

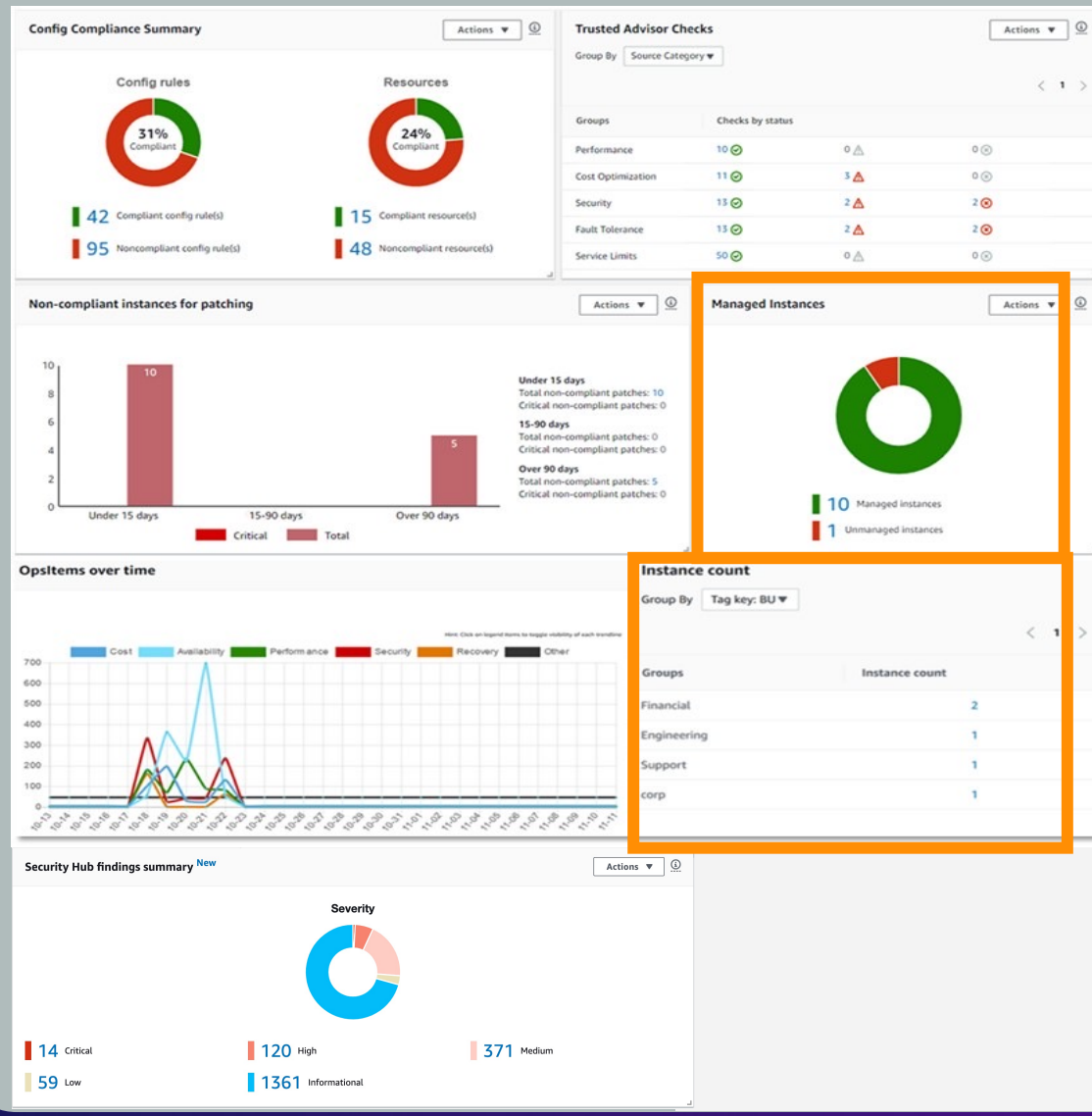
AWS Security Hub

AWS Systems Manager

Patch Compliance

OpsCenter OpsItems

Inventory




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Explorerについての詳細はこちら。

Enable Visibility

# Explorer

## ハイレベルの運用ダッシュボード

- 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

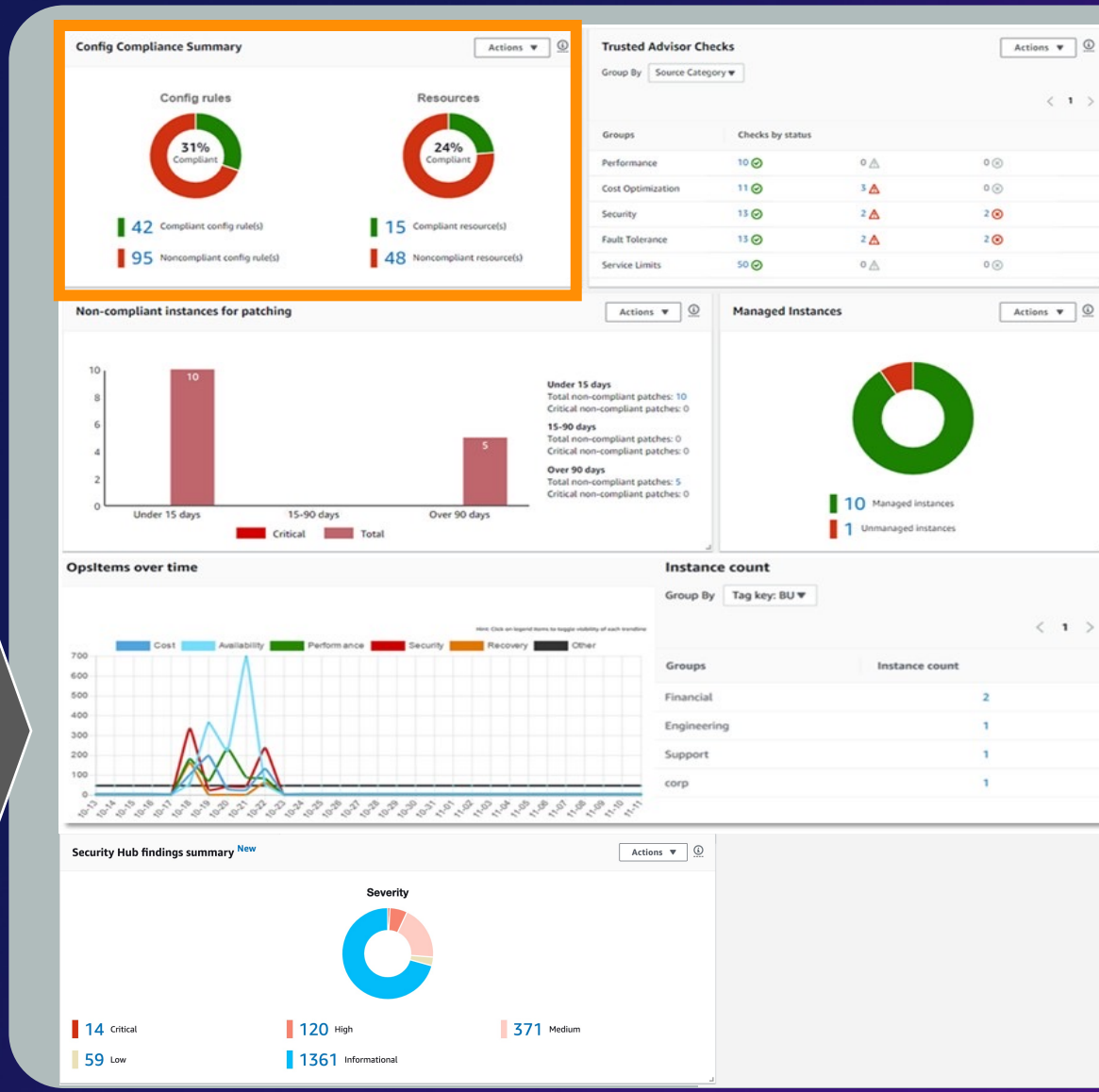
AWS Security Hub

AWS Systems Manager

Patch Compliance

OpsCenter OpsItems

Inventory




Explorerについての詳細はこちら。

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Enable Visibility

# Explorer

## ハイレベルの運用ダッシュボード

- 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

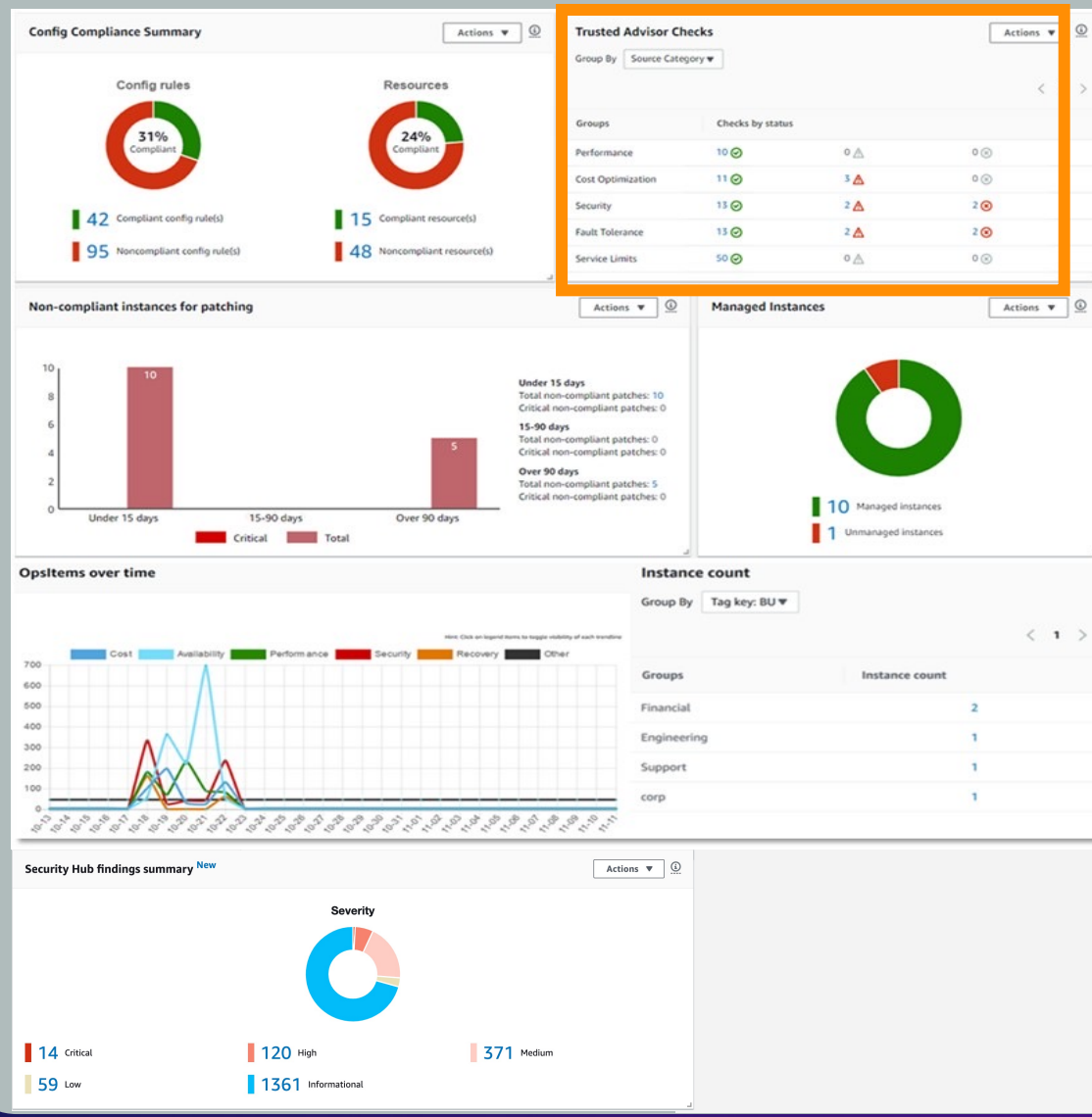
AWS Security Hub

AWS Systems Manager

Patch Compliance

OpsCenter OpsItems

Inventory




Explorerについての詳細はこちら。

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Explorer

Enable Visibility

## ハイレベルの運用ダッシュボード

- 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

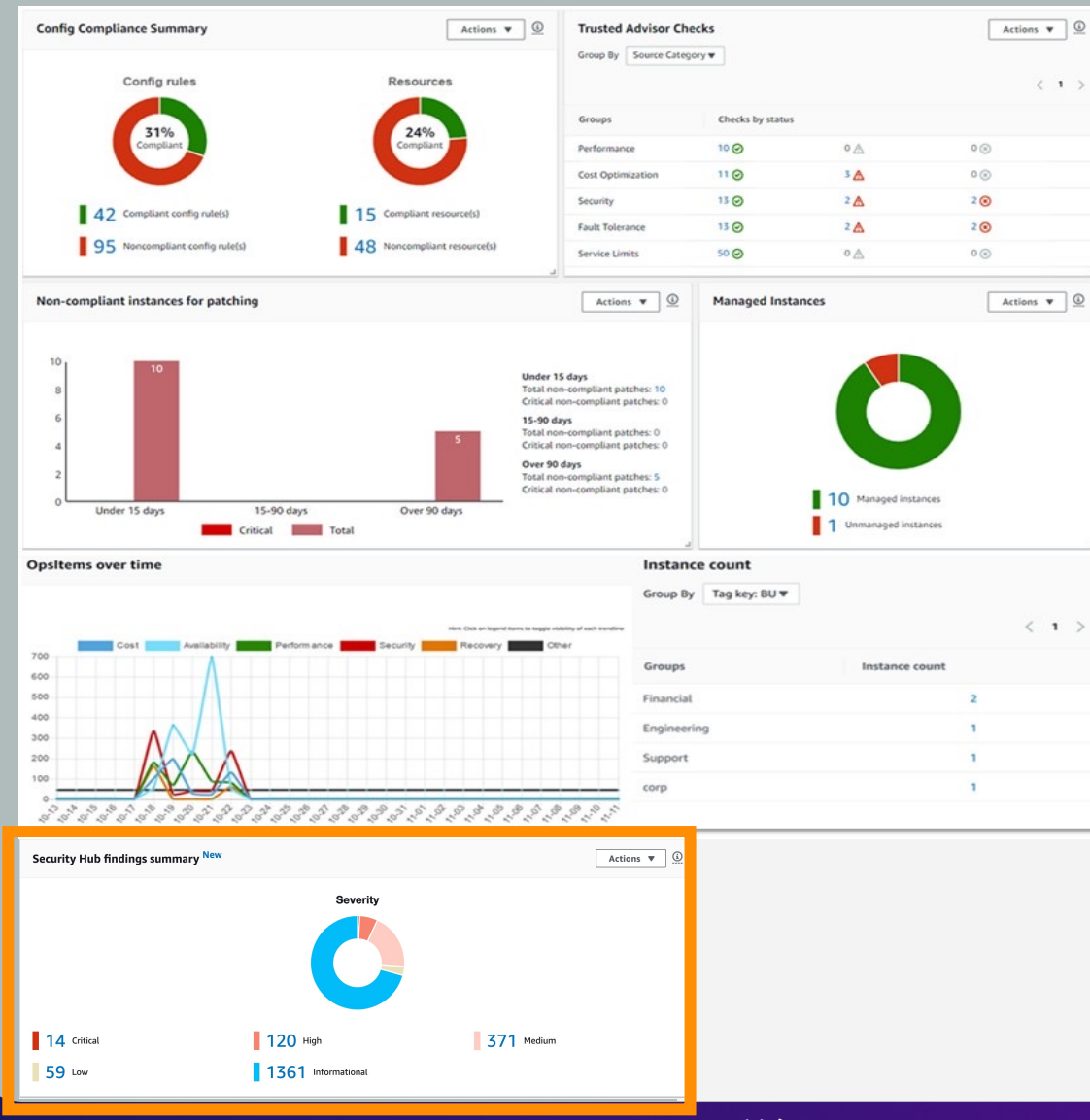
AWS Security Hub

AWS Systems Manager

Patch Compliance

OpsCenter OpsItems

Inventory




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Explorerについての詳細はこちら。

# Explorer

Enable Visibility

## ハイレベルの運用ダッシュボード

- 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

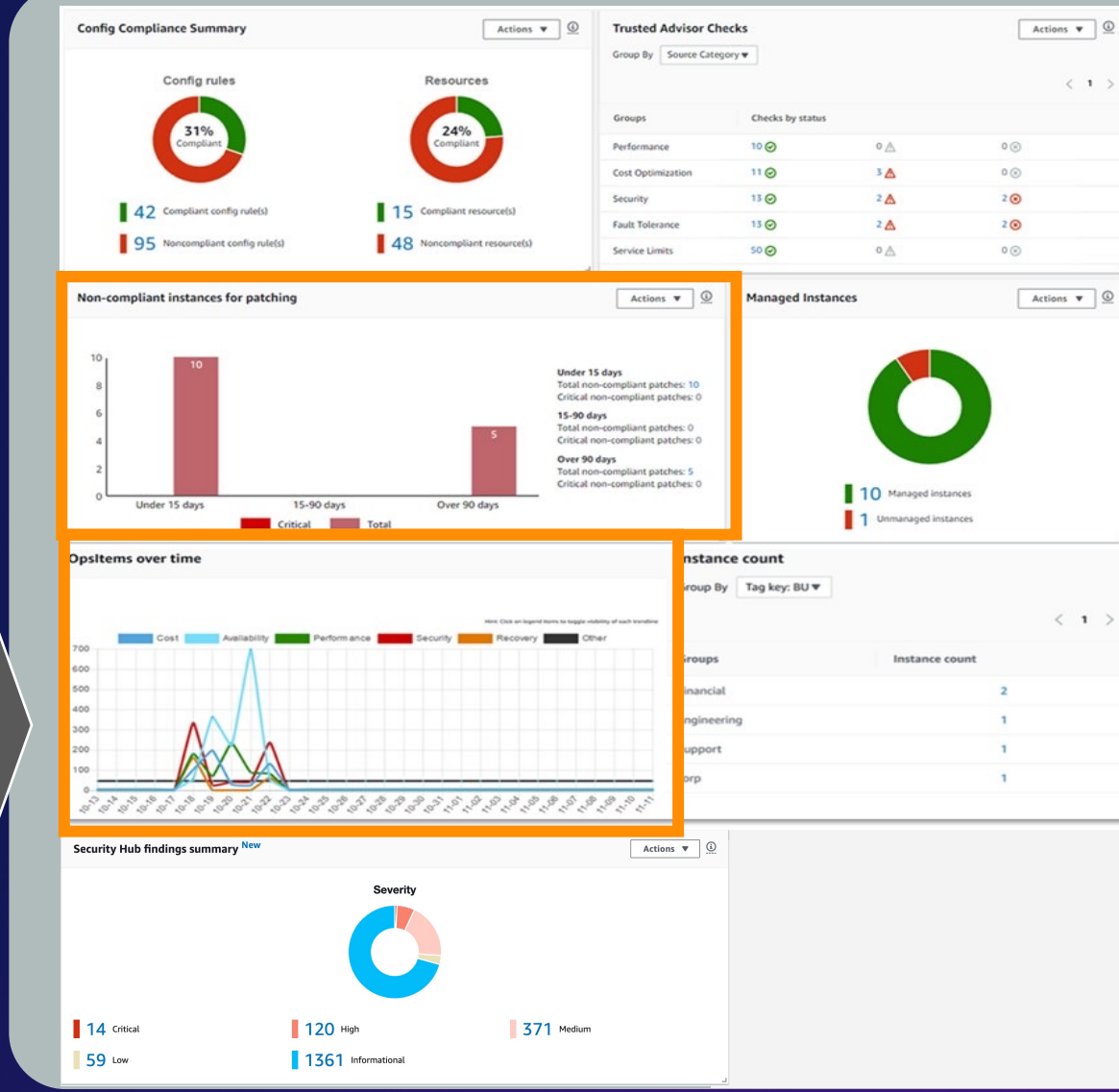
AWS Security Hub

AWS Systems Manager

Patch Compliance

OpsCenter OpsItems

Inventory




Explorerについての詳細はこちら。

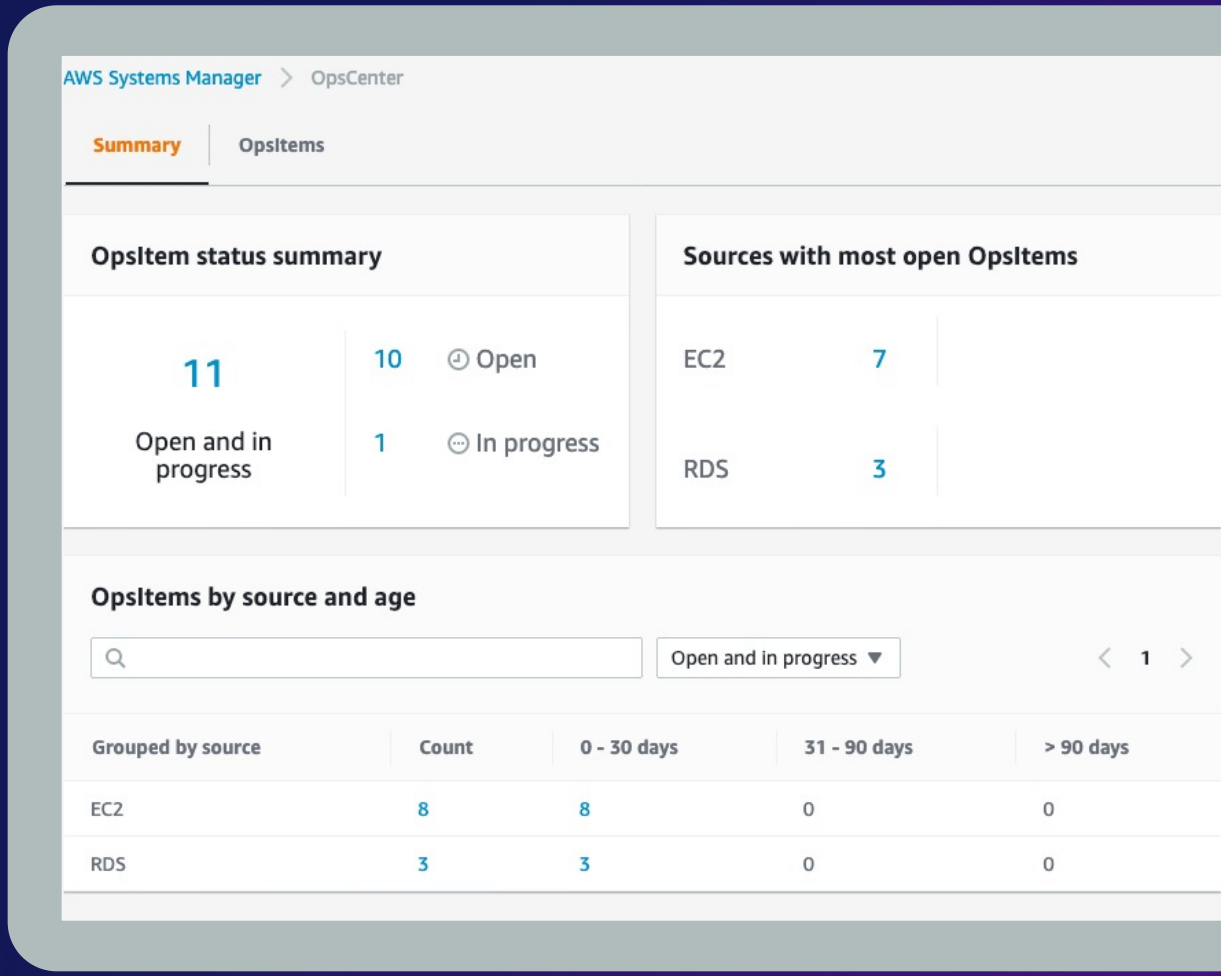
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Enable Visibility

# OpsCenter

## 対応すべき運用アイテムの可視化、問題解決の支援

- 運用上の問題 (OpsItem) の集約ビューを提供。
- OpsItem に関連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。




OpsCenterについての詳細はこちら。

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# OpsCenter

Enable Visibility

## 対応すべき運用アイテムの可視化、問題解決の支援

AWS Security Hub
セキュリティアラート

Amazon DynamoDB
スロットルイベント

Amazon EC2
AutoScale失敗

etc

Amazon DynamoDB
アクションの閾値

Amazon EC2
CPU使用率

Amazon Elastic Block Store (Amazon EBS)
ディスク使用率

etc

Amazon EventBridge

Amazon CloudWatch

Incident Manager

OpsItem

OpsItem

OpsItem

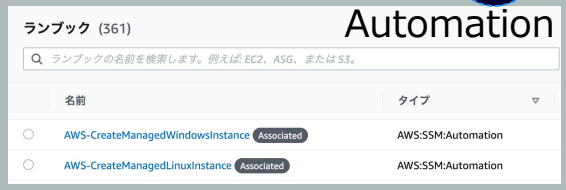
OpsCenter

統合

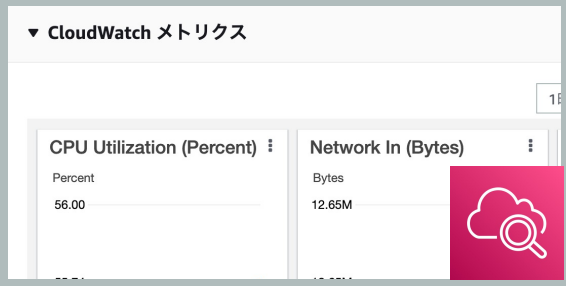
**ServiceNow**
**Jira Service Desk**

### Runbook の提供

Automation

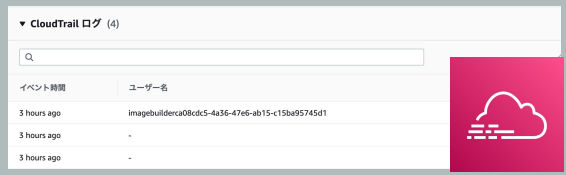



### 関連リソースの情報




Amazon CloudWatch

AWS Config




AWS CloudTrail

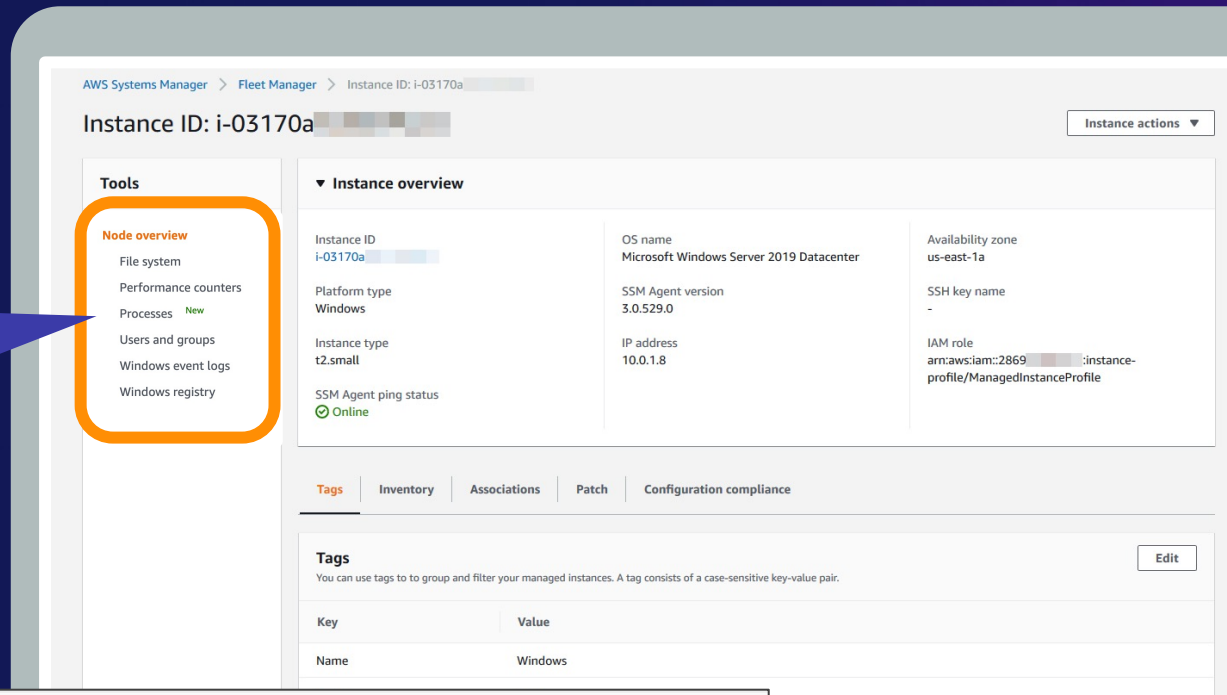
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Enable Visibility

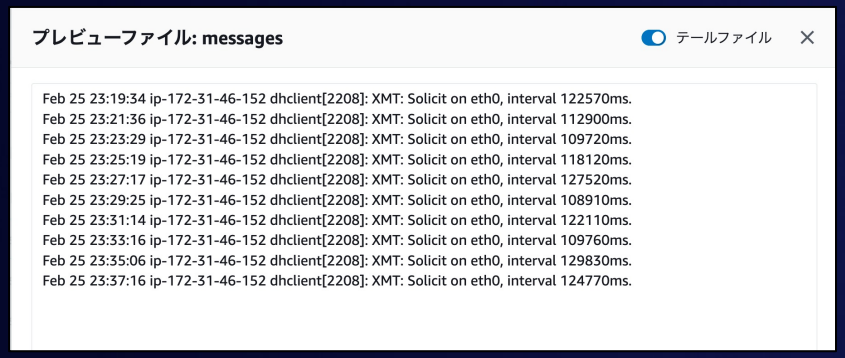
# Fleet Manager
## ノードフリートの管理

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

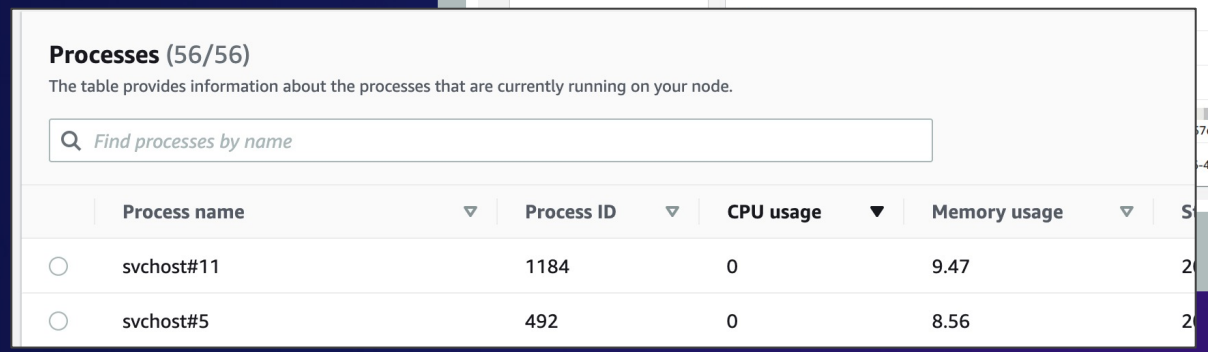
- ファイルシステム
- パフォーマンスカウンタ
- プロセス
- ユーザー・グループ
- Windows レジストリ (Windows のみ)
- Windows イベントログ (Windows のみ)




ログのTail




プロセス稼働状況




Fleet Manager についての詳細はこちら。

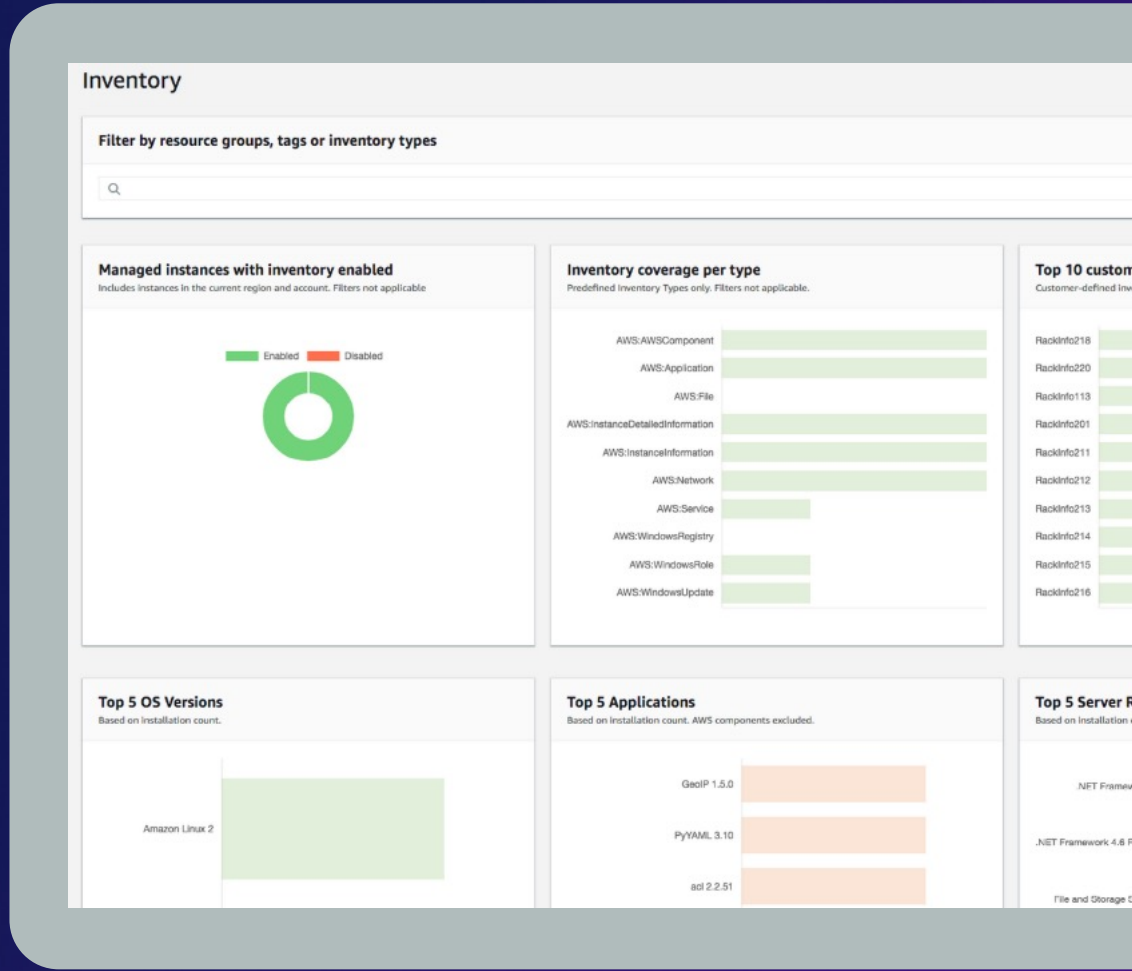
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Enable Visibility

# Inventory

## ノードのメタデータ可視化

- 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
- カスタムインベントリとして独自アイテムも
  収集可能。

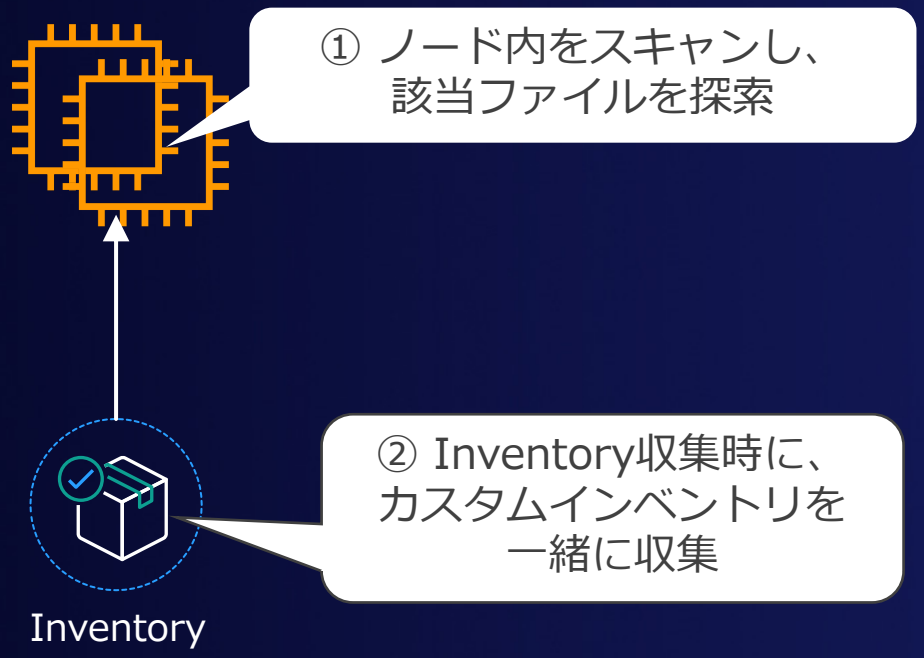



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

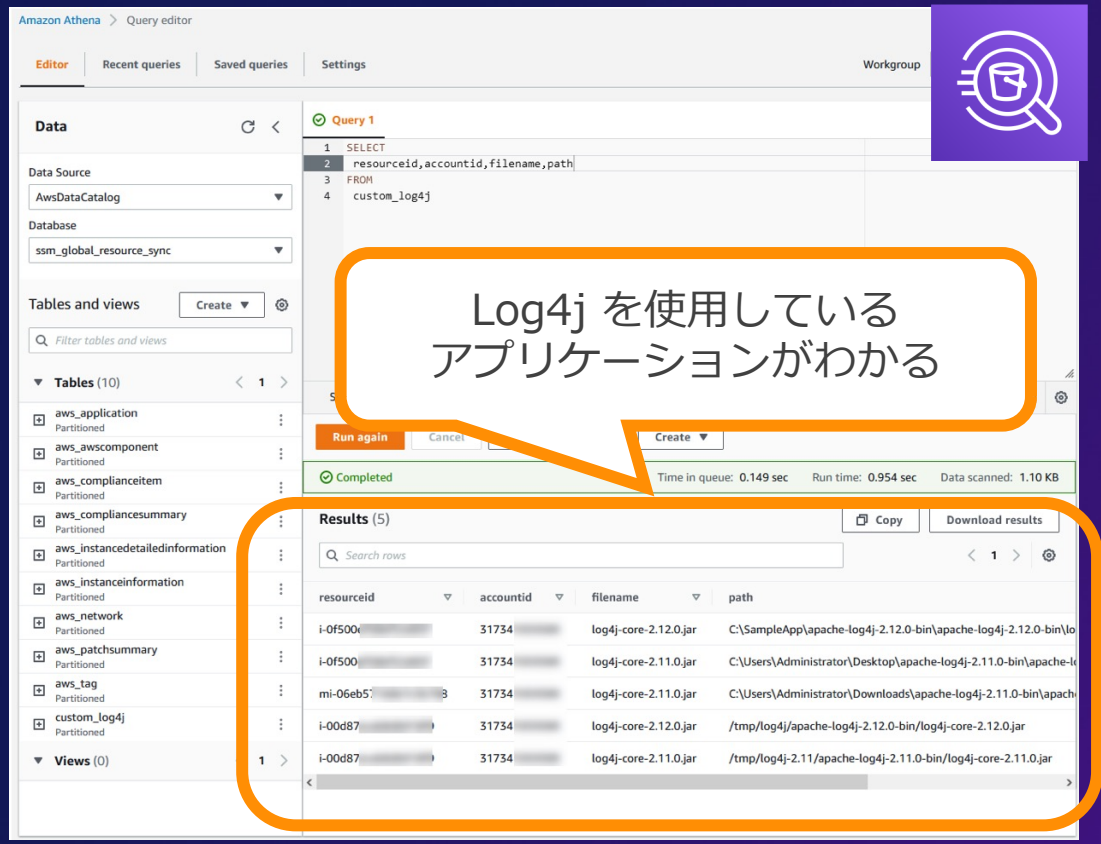
Inventory についての詳細はこちら。

# Inventory の活用：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。




Amazon Athena




詳細はこちらのブログを参照

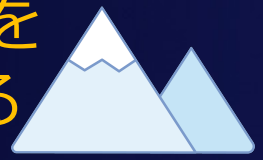
「AWS Systems Manager カスタムインベントリを使ったマネージドノード上の Log4j ファイル検索」

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

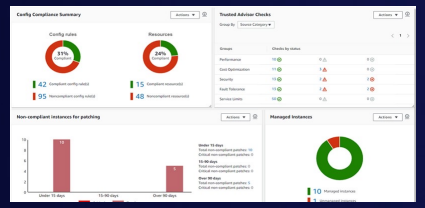
# おさらい

ここまでで何ができたかというと・・・

AWS環境全体を
俯瞰・確認する

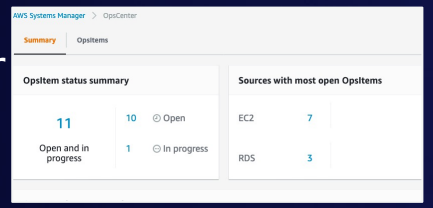


ハイレベルの運用ダッシュボード

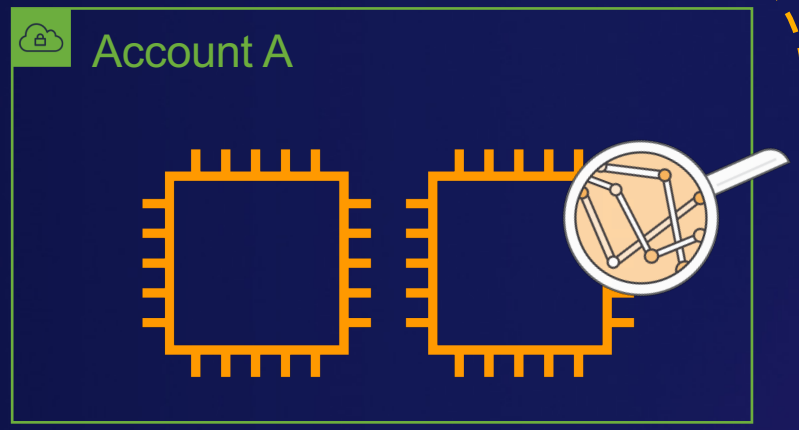


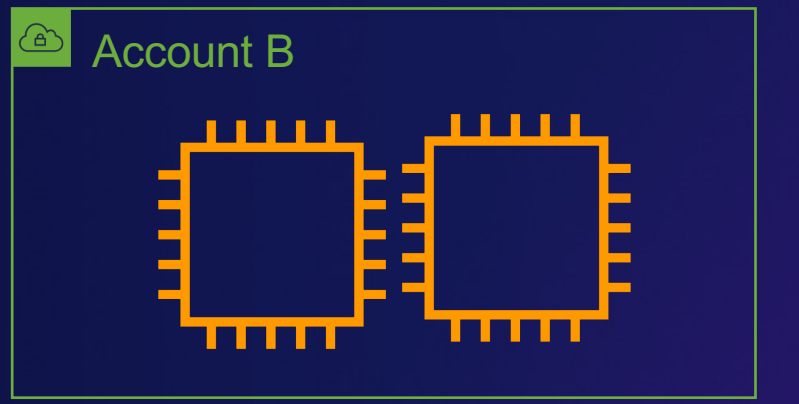
Explorer

運用アイテムの管理



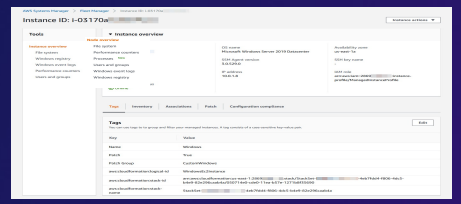

OpsCenter



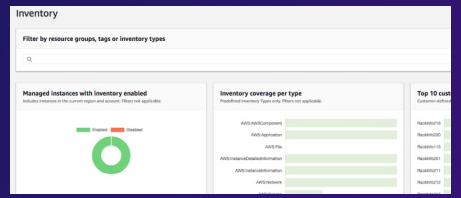

ノードの状態を
俯瞰・確認する

ノードフリート管理



Fleet Manager

ノードのメタデータ可視化




Inventory

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# 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

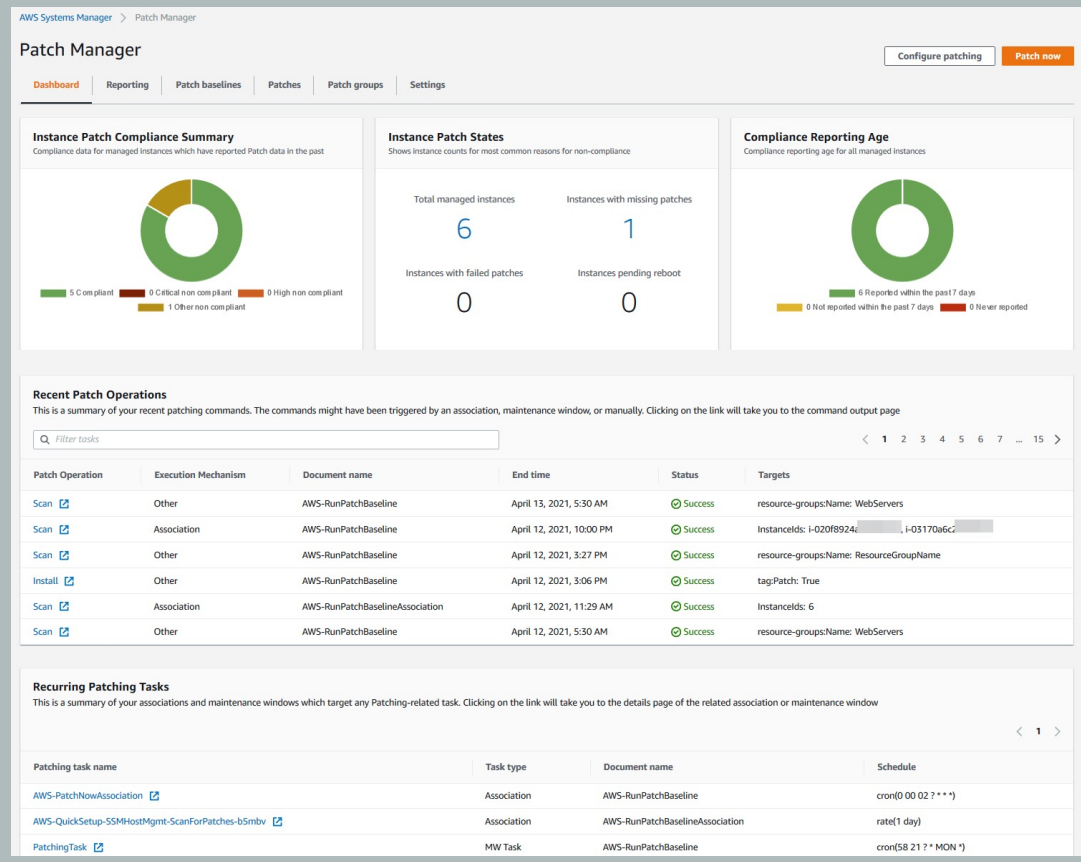
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Proactively Automate

# Patch Manager

## パッチ適用を自動化

- 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。
- パッチベースラインで適用ルールを定義できる。




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

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

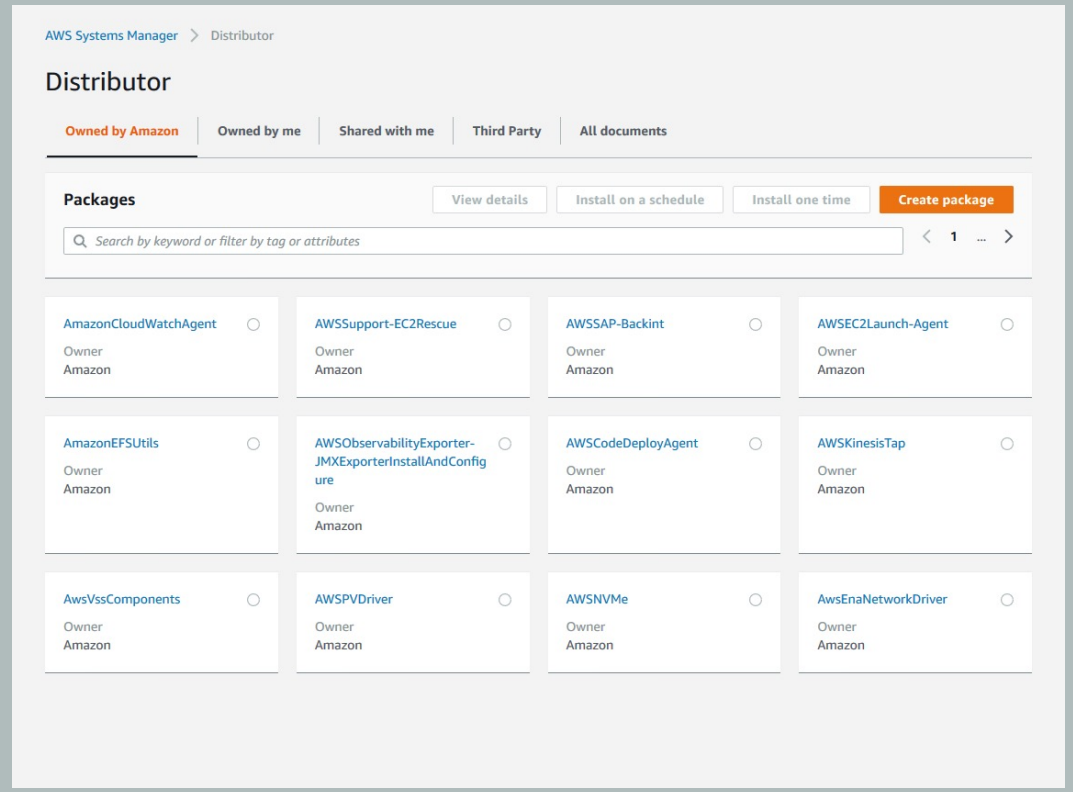
Patch Manager についての詳細はこちら。

Proactively Automate

# Distributor

## ソフトウェアのインストール・更新の自動化

- ソフトウェアパッケージのデプロイ自動化を実現。
- 一つのパッケージで Windows も Linux も。
- CloudWatch Agent などの多くの AWS が提供する Package も含まれており、それらの利用もおすすめ。




Distributor についての詳細はこちら。

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Proactively Automate

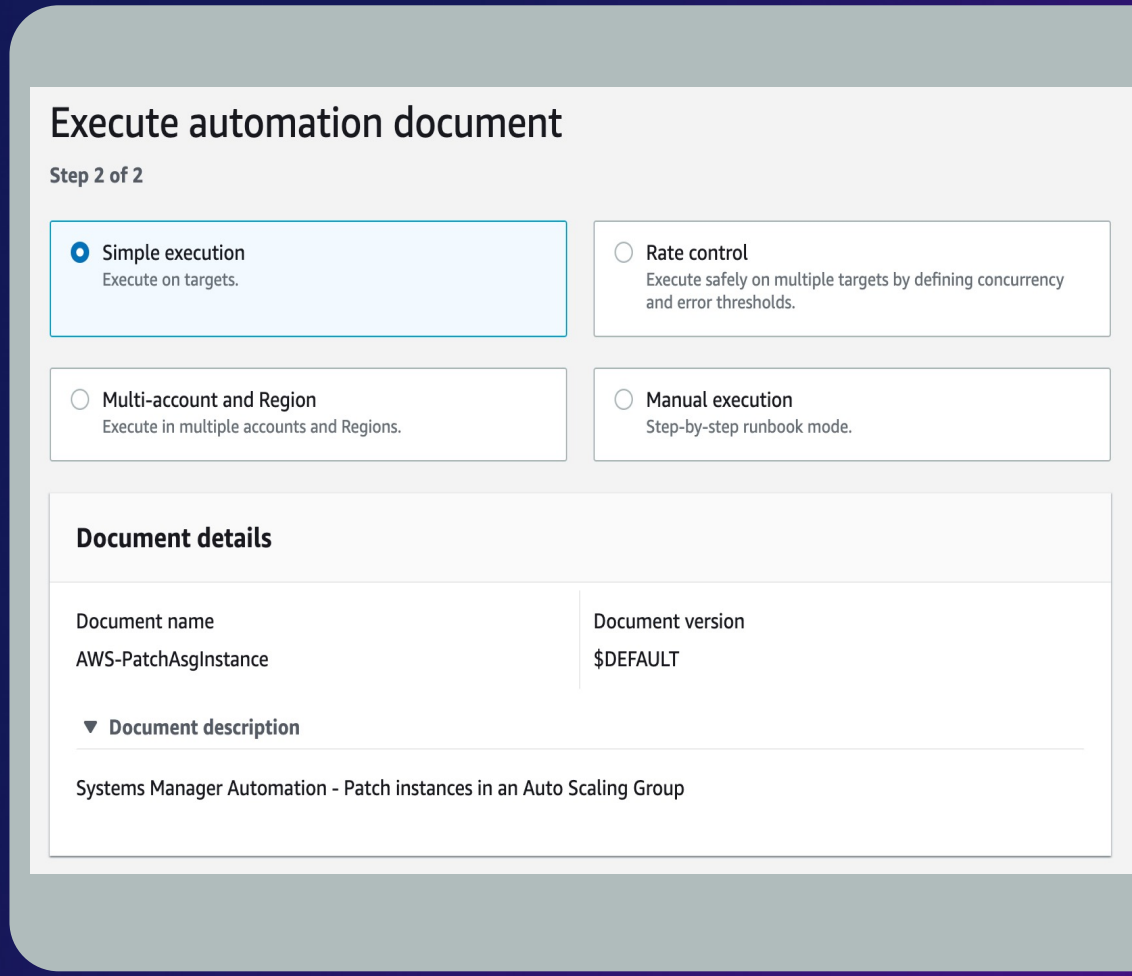
# Automation

## カスタム処理の自動化と修復アクション

自動化ワークフローである Runbook を実行できる。

- **タスクを安全に一括実行**
  組織の大規模なノードフリートに対し、
  レートコントロールしながら変更をロールアウト
- **複雑なタスクの簡素化:**
  ゴールデン AMI の作成など
- **ベストプラクティスの共有:**
  ベストプラクティスを組織の他のメンバーと共有

いろいろな
ユースケースに！




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Automation についての詳細はこちら。

Proactively Automate

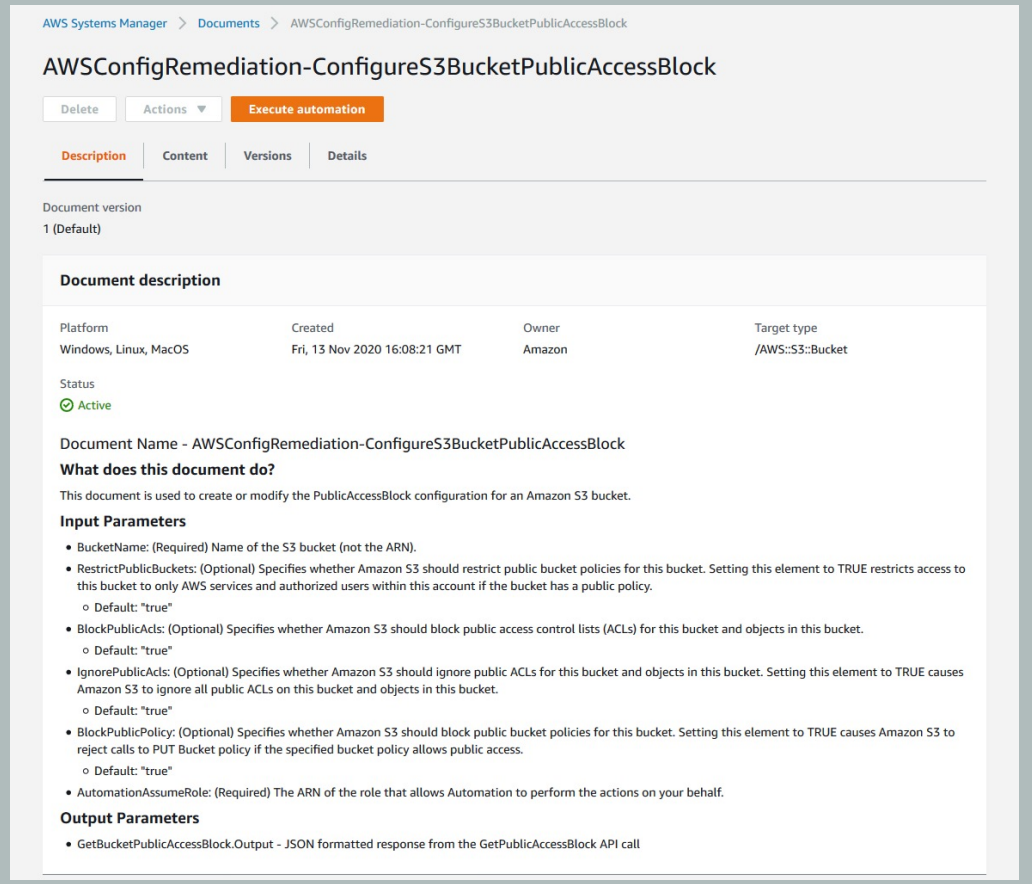
# Automation - Runbook

## カスタム処理の自動化と修復アクション

- Runbook は、Document Builder を使って自作できる。
- 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。

### 事前定義された Runbook のカテゴリ

| | | |
|---|---|---|
| Remediation | Instance Management | Self Service Support Workflows |
| Patching | Data Backup | Resource Management |
| Security | AMI Management | Cost Management |



AWS Systems Manager > Documents > AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock

AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock

Delete | Actions | Execute automation

Description | Content | Versions | Details

Document version
1 (Default)

**Document description**

| Platform | Created | Owner | Target type |
|---|---|---|---|
| Windows, Linux, MacOS | Fri, 13 Nov 2020 16:08:21 GMT | Amazon | /AWS::S3::Bucket |

Status
Active

Document Name - AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock

**What does this document do?**

This document is used to create or modify the PublicAccessBlock configuration for an Amazon S3 bucket.

**Input Parameters**

- BucketName: (Required) Name of the S3 bucket (not the ARN).
- RestrictPublicBuckets: (Optional) Specifies whether Amazon S3 should restrict public bucket policies for this bucket. Setting this element to TRUE restricts access to this bucket to only AWS services and authorized users within this account if the bucket has a public policy.
  - Default: "true"
- BlockPublicAcls: (Optional) Specifies whether Amazon S3 should block public access control lists (ACLs) for this bucket and objects in this bucket.
  - Default: "true"
- IgnorePublicAcls: (Optional) Specifies whether Amazon S3 should ignore public ACLs for this bucket and objects in this bucket. Setting this element to TRUE causes Amazon S3 to ignore all public ACLs on this bucket and objects in this bucket.
  - Default: "true"
- BlockPublicPolicy: (Optional) Specifies whether Amazon S3 should block public bucket policies for this bucket. Setting this element to TRUE causes Amazon S3 to reject calls to PUT Bucket policy if the specified bucket policy allows public access.
  - Default: "true"
- AutomationAssumeRole: (Required) The ARN of the role that allows Automation to perform the actions on your behalf.

**Output Parameters**

- GetBucketPublicAccessBlock.Output - JSON formatted response from the GetPublicAccessBlock API call

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

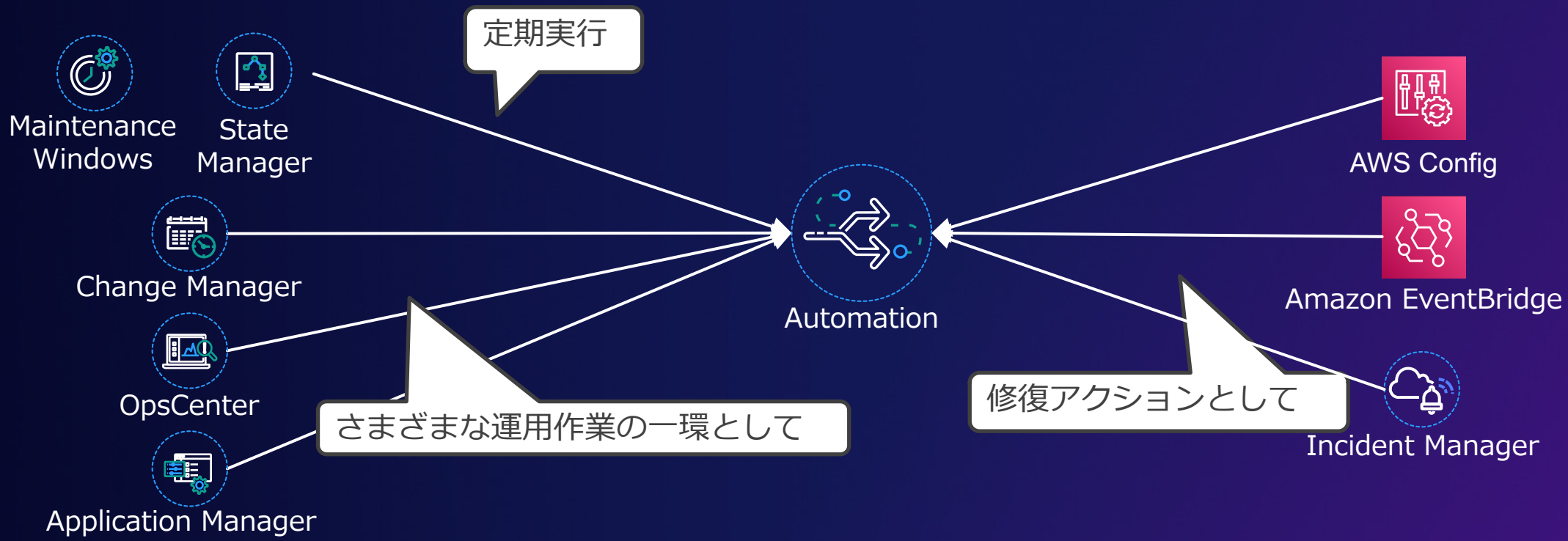
Runbook についての詳細はこちら。

Proactively Automate

# Automation – さまざまなトリガーで起動

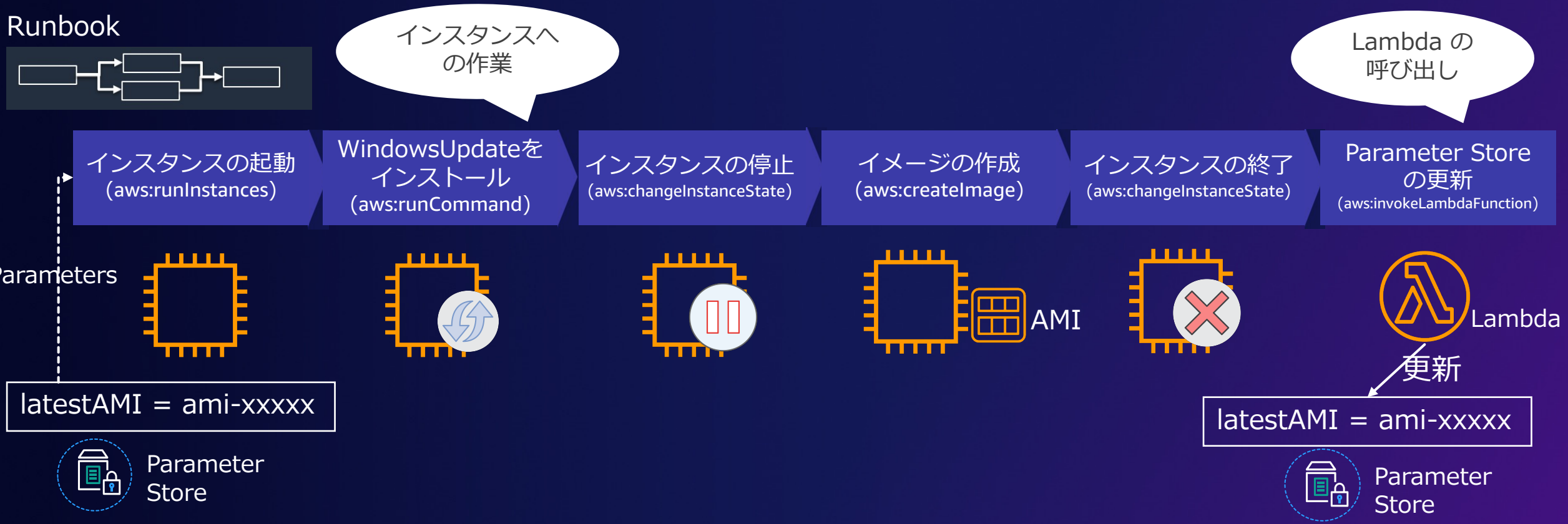
## カスタム処理の自動化と修復アクション

- 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。




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Runbook 例：カスタム AMI パッチ適用

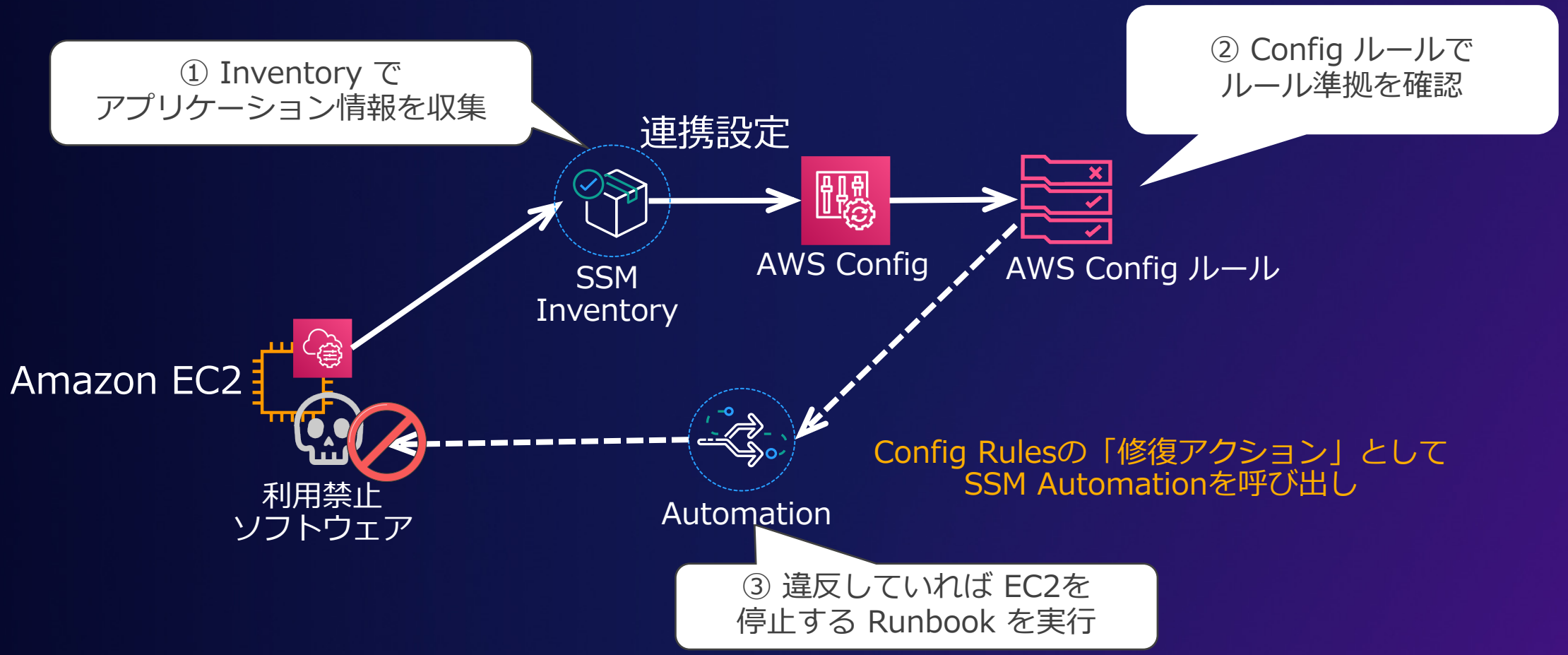



詳細はこちらのドキュメントを参照
「チュートリアル: オートメーション、AWS Lambda、Parameter Store を使用した AMI パッチ適用の簡素化」

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# 修復自動化例：不正 SW の検知・自動停止

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



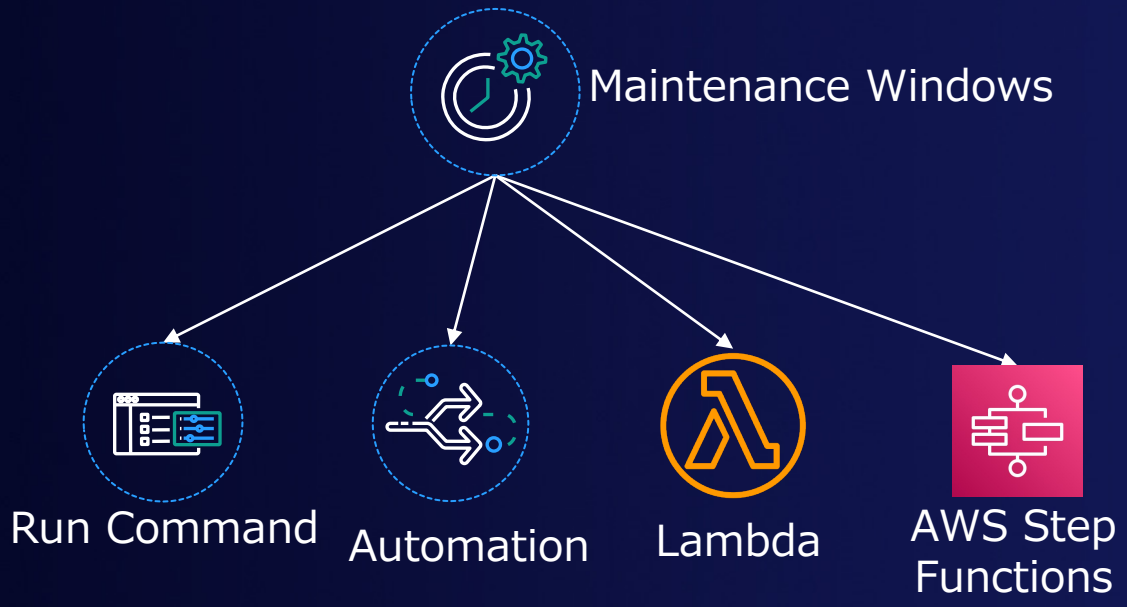

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

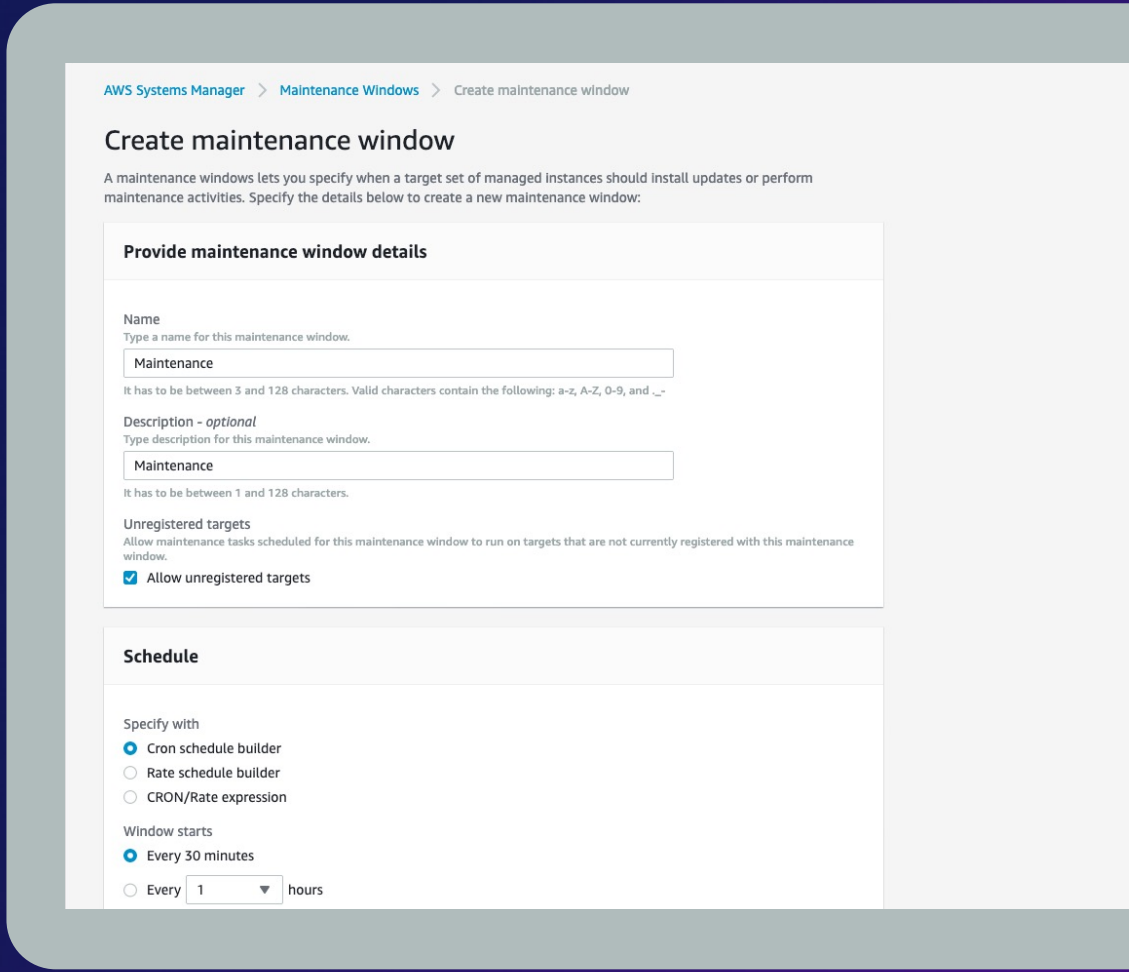
# Maintenance Windows

Proactively Automate

## 自動処理のタイミング制御

- 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。



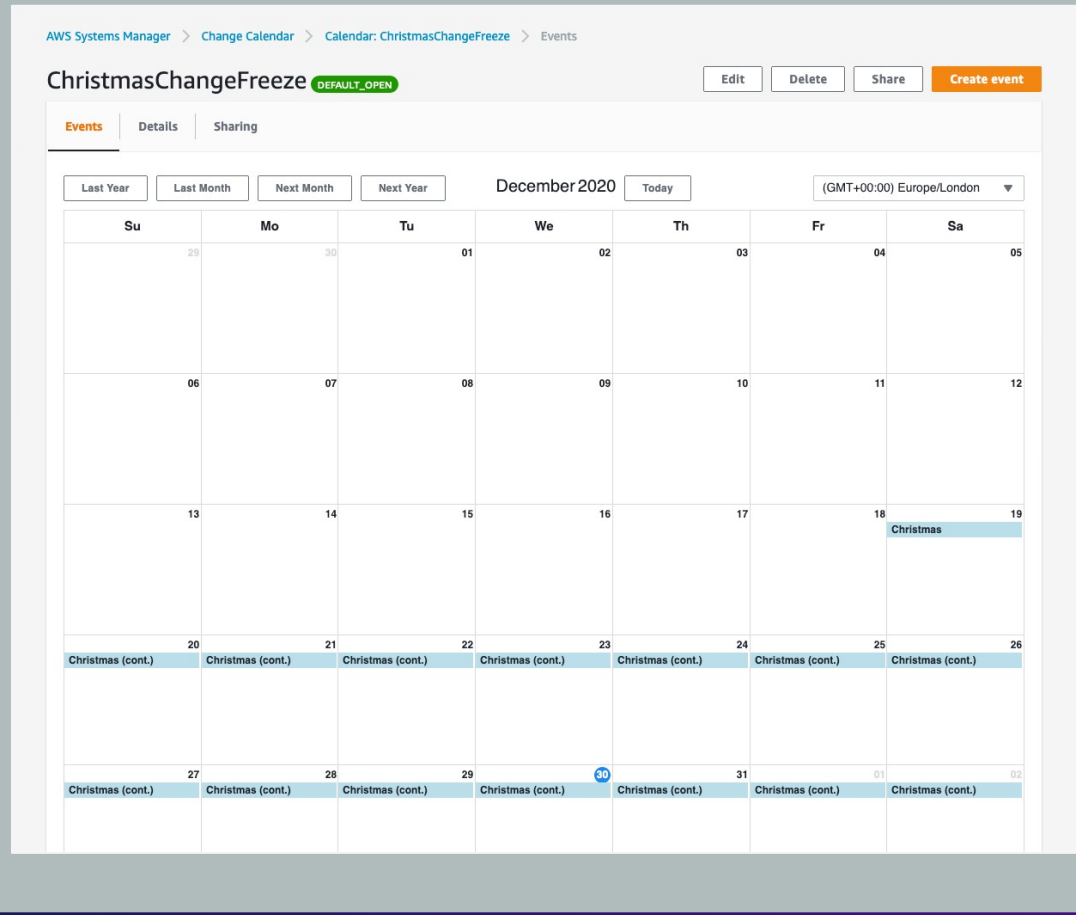

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Maintenance Windows についての詳細はこちら。

# Change Calendar

Proactively Automate 自動処理のタイミング制御

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。




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Change Calendar についての詳細はこちら。

# おさらい

## 汎用的な管理作業の自動化

- パッチ適用
- SWインストール、更新
- その他カスタム処理

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

Automation

## タイミング制御

- 定期実行
- カレンダーでの制御

Maintenance Windows

Change Calendar

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# おさらい

## 汎用的な管理作業の自動化

- パッチ適用
- SWインストール、更新
- その他カスタム処理

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

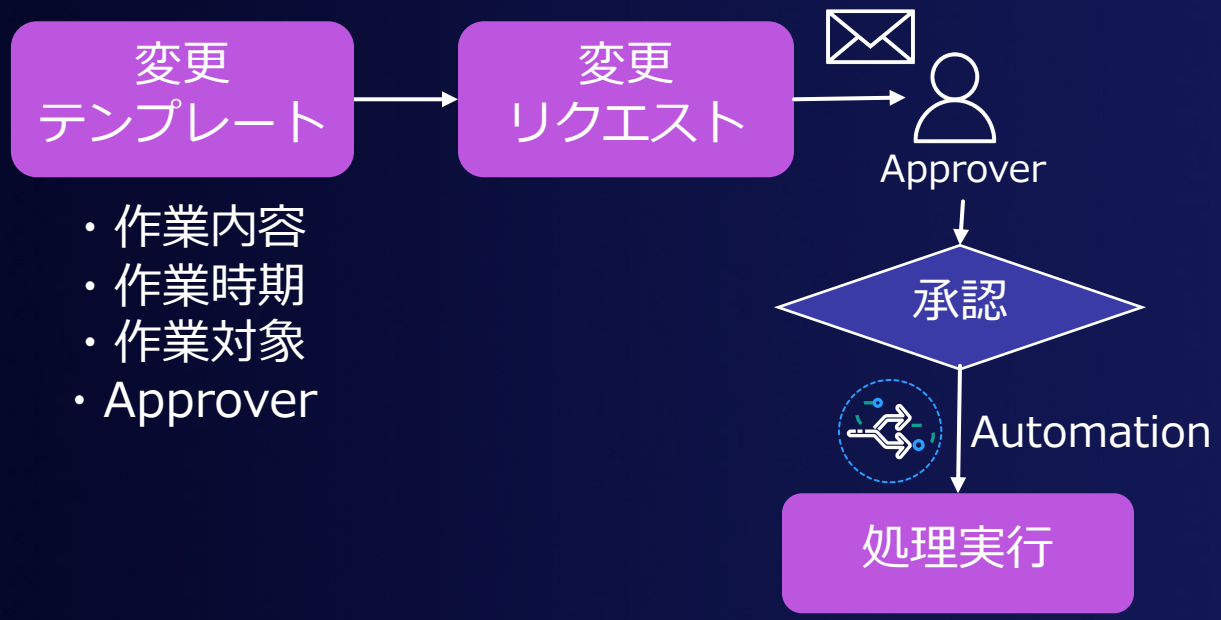
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Proactively Automate

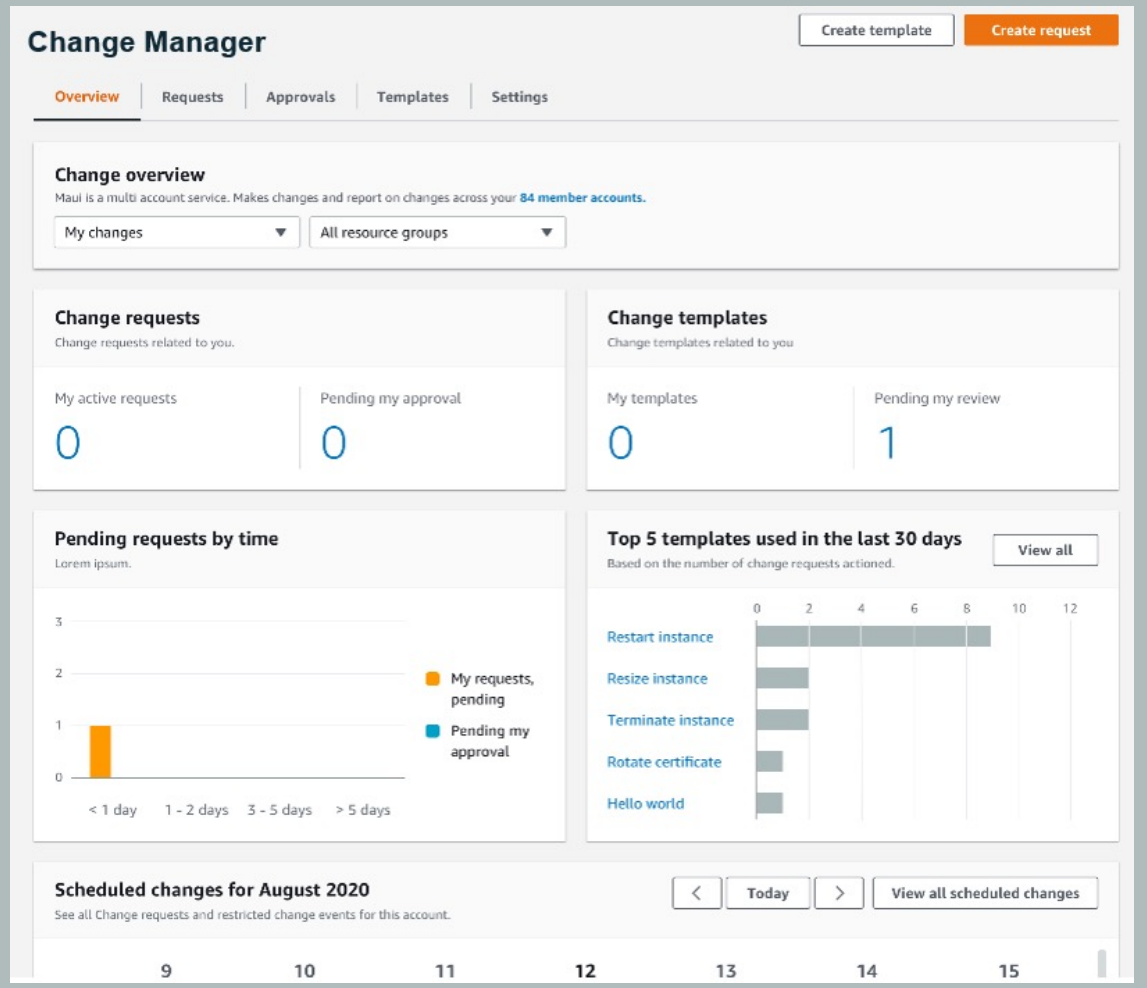
# Change Manager

## 変更を安全に行うための承認ワークフローの自動化

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。




- 作業内容
- 作業時期
- 作業対象
- Approver




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Change Manager についての詳細はこちら。

# おさらい

## 汎用的な管理作業の自動化

- パッチ適用
- SWインストール、更新
- その他カスタム処理

Patch Manager

Distributor

Automation

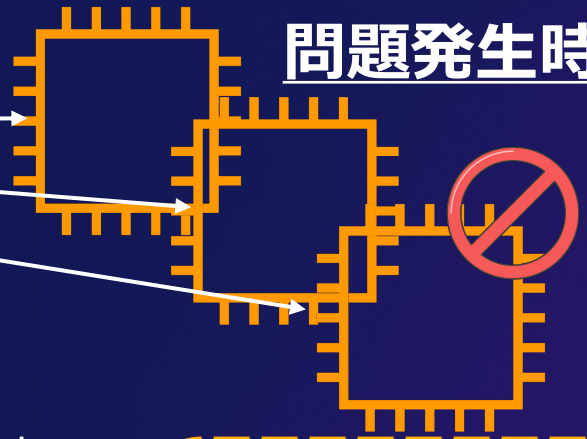
AWS Systems Manager

## タイミング制御

- 定期実行
- カレンダーでの制御

Maintenance Windows

Change Calendar



## 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

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# 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

Run Command

### ノードへのセキュアな特権アクセス

Session Manager

Fleet Manager

aws

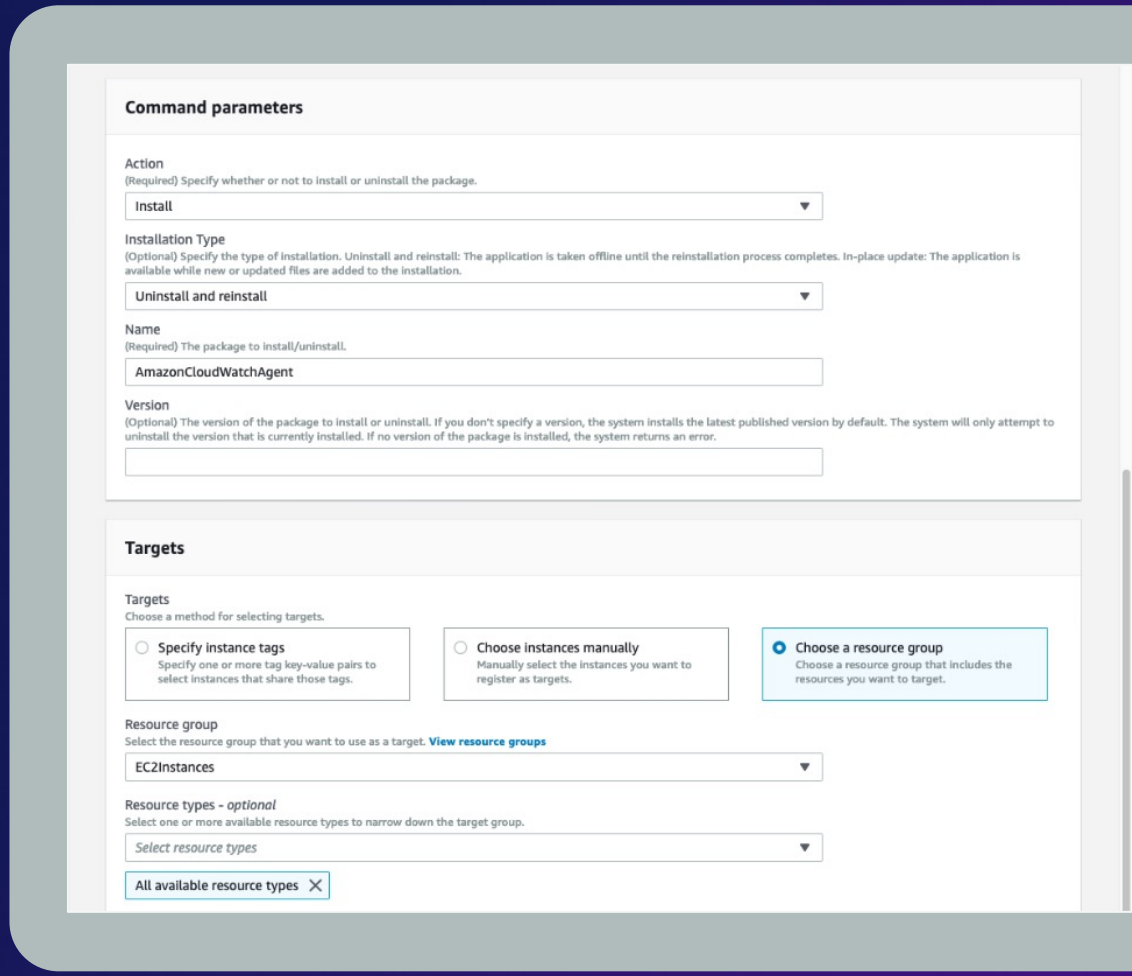
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Run Command

## ノードへの一括コマンド発行

- サーバー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。
- “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！



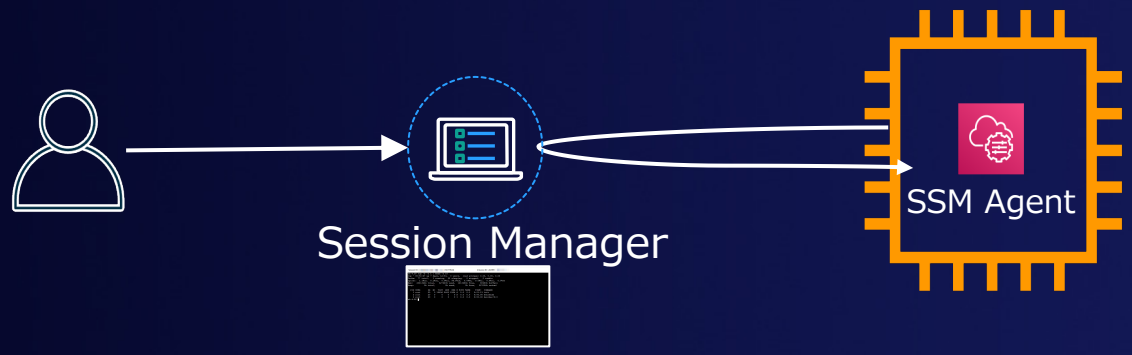

Run Command についての詳細はこちら。

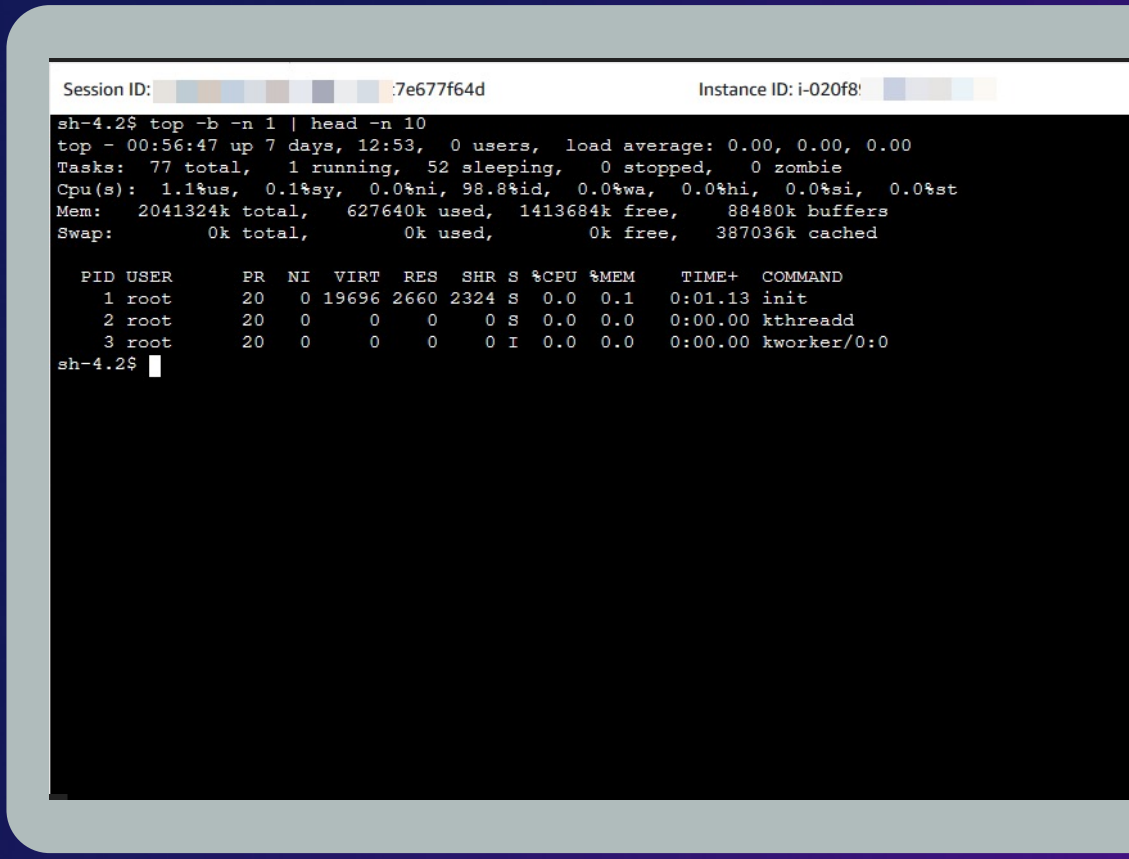
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# 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。




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Session Manager についての詳細はこちら。

# Session Manager でのアクセス統制例

## 接続履歴

AWS CloudTrail

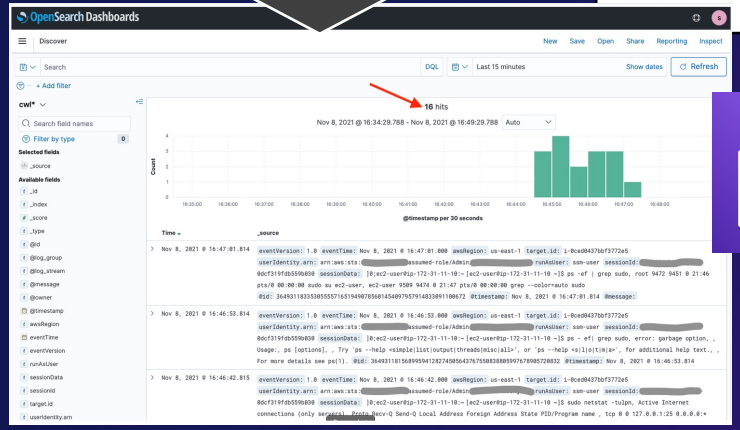

```
"eventTime": "2021-03-07T09:29:54Z",
"eventSource": "ssm.amazonaws.com",
"eventName": "StartSession",
"awsRegion": "ap-northeast-1",
```

誰かがサーバーにアクセスすると、
Slack に通知

## 操作履歴

S3 Bucket　CloudWatch Logs

```
Script started on Thu Mar 18 17:48:03 2021
/bin/bash
cd /usr
[?1034hsh-4.2$ /bin/bash
]0;@ip-172-31-46-152:/[?1034h[kayoko@ip-172-31-46-152 /]$ cd /usr
]0;@ip-172-31-46-152:/usr[kayoko@ip-172-31-46-152 usr]$
[K[kayoko@ip-172-31-46-152 usr]$ whoami
kayoko
]0;@ip-172-31-46-152:/usr[kayoko@ip-172-31-46-152 usr]$ exit
exit
sh-4.2$ exit
```




Amazon OpenSearch Service

「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」

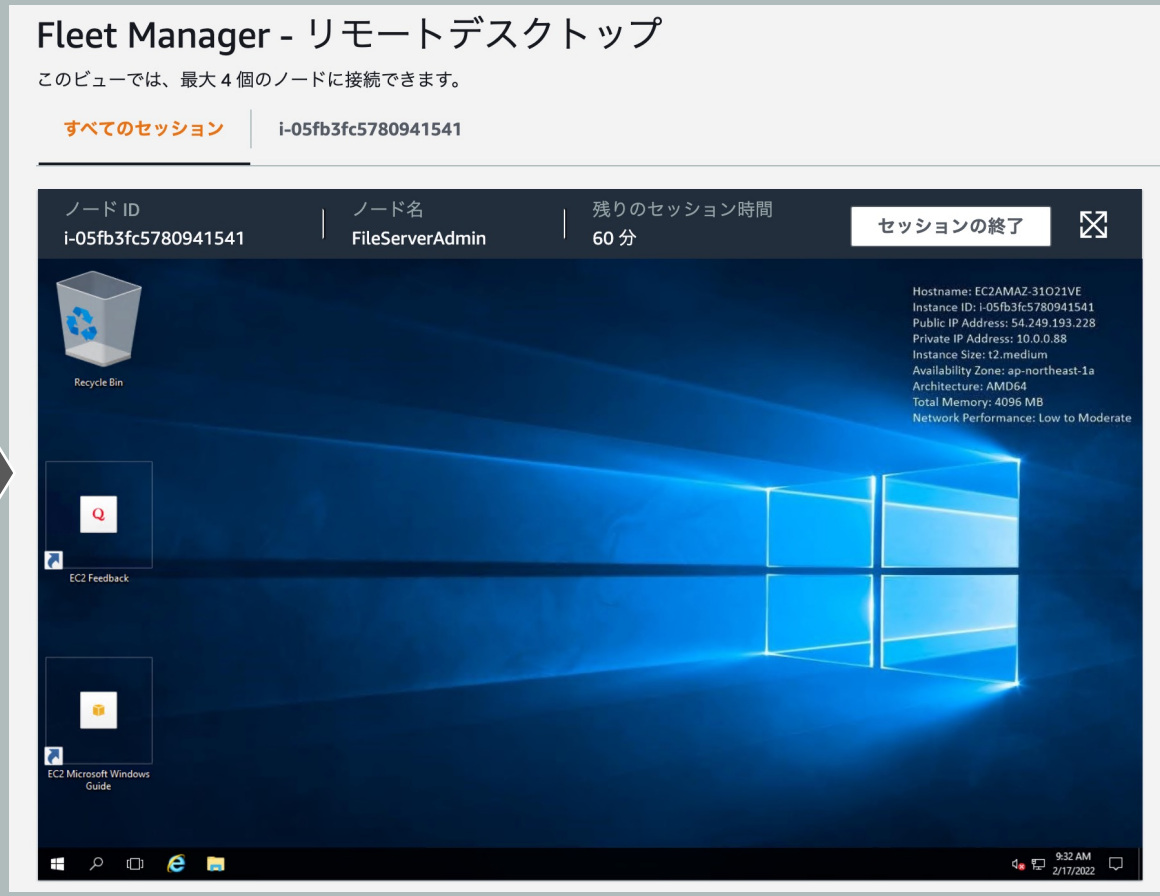
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Remediate Issues

# Fleet Manager

## Windows サーバー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。

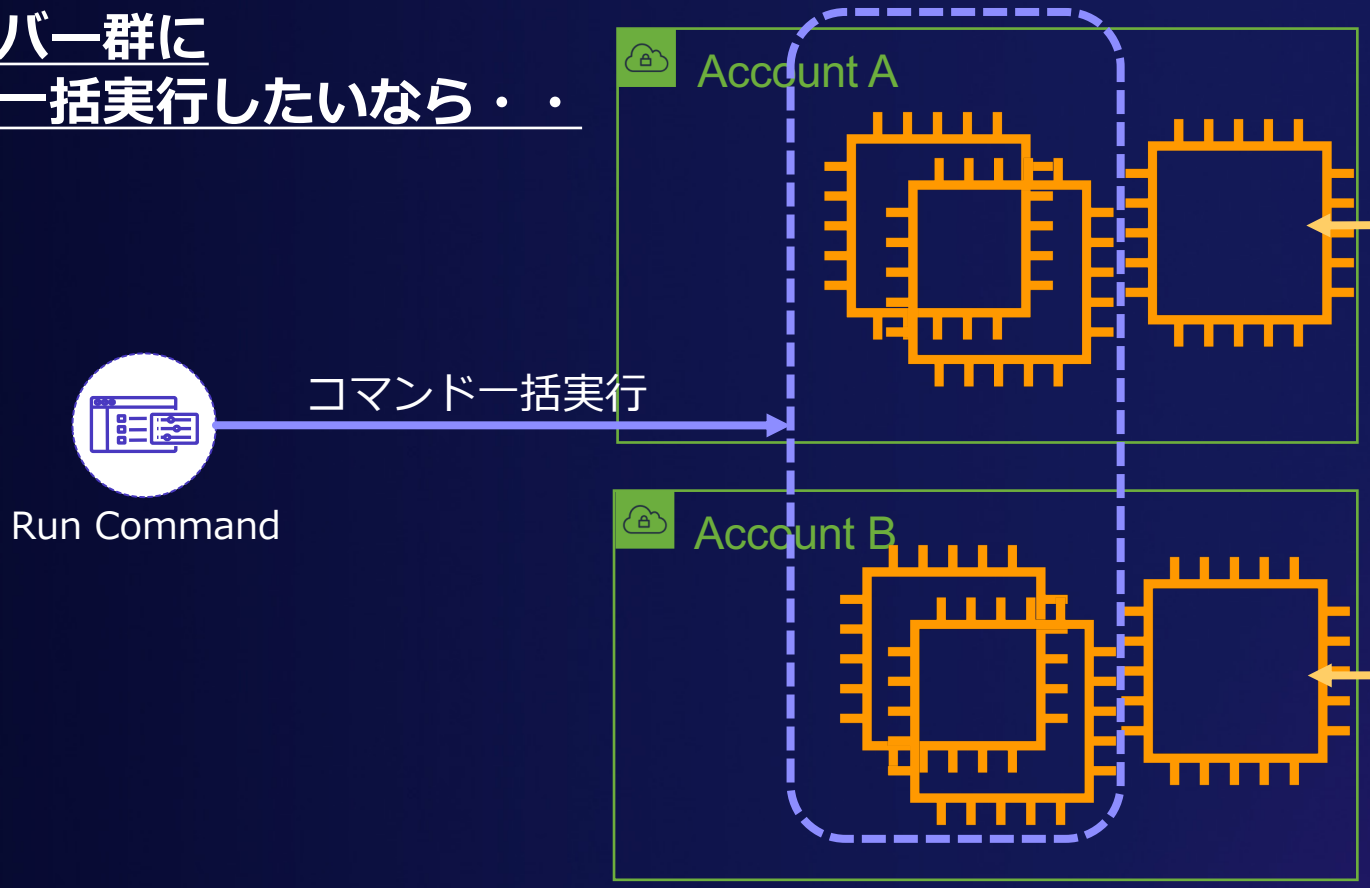



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Fleet Manager の RDP 接続機能についての詳細はこちら。

# おさらい

**対象サーバー群に**
**コマンド一括実行したいなら・・**

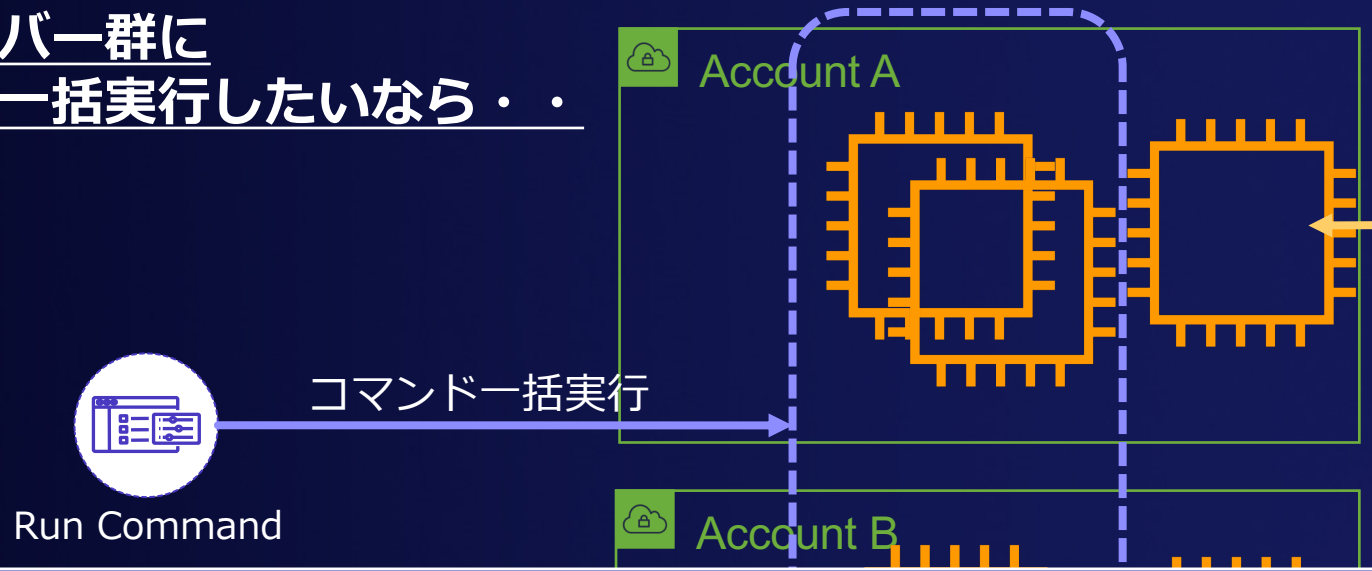



**個々のサーバーに対して**
**インタラクティブにコマンド**
**操作したいなら・・**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# おさらい

**対象サーバー群に**
**コマンド一括実行したいなら・・**




**個々のサーバーに対して**
**インタラクティブにコマンド**
**操作したいなら・・**

インシデント管理って
どうしたらいいの？

Incident Manager

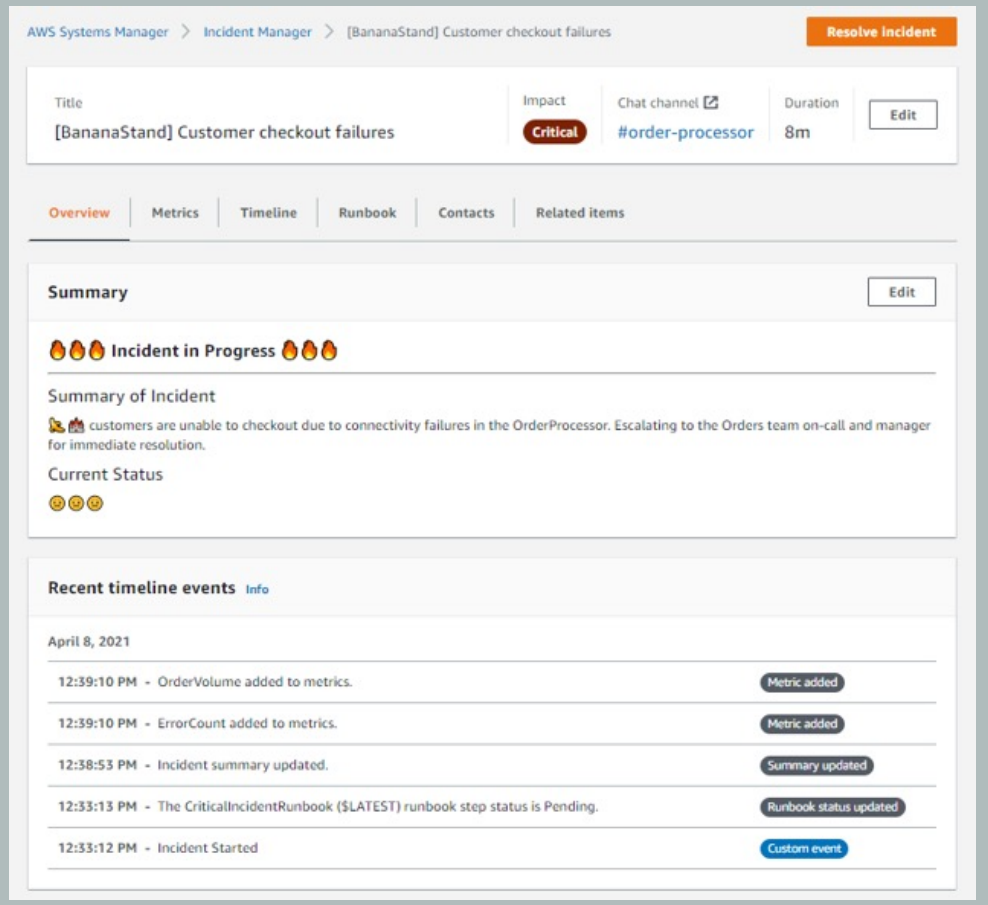
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Incident Manager

Remediate Issues

## 事前に準備された対応計画、ランブック、分析による改善

- 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。



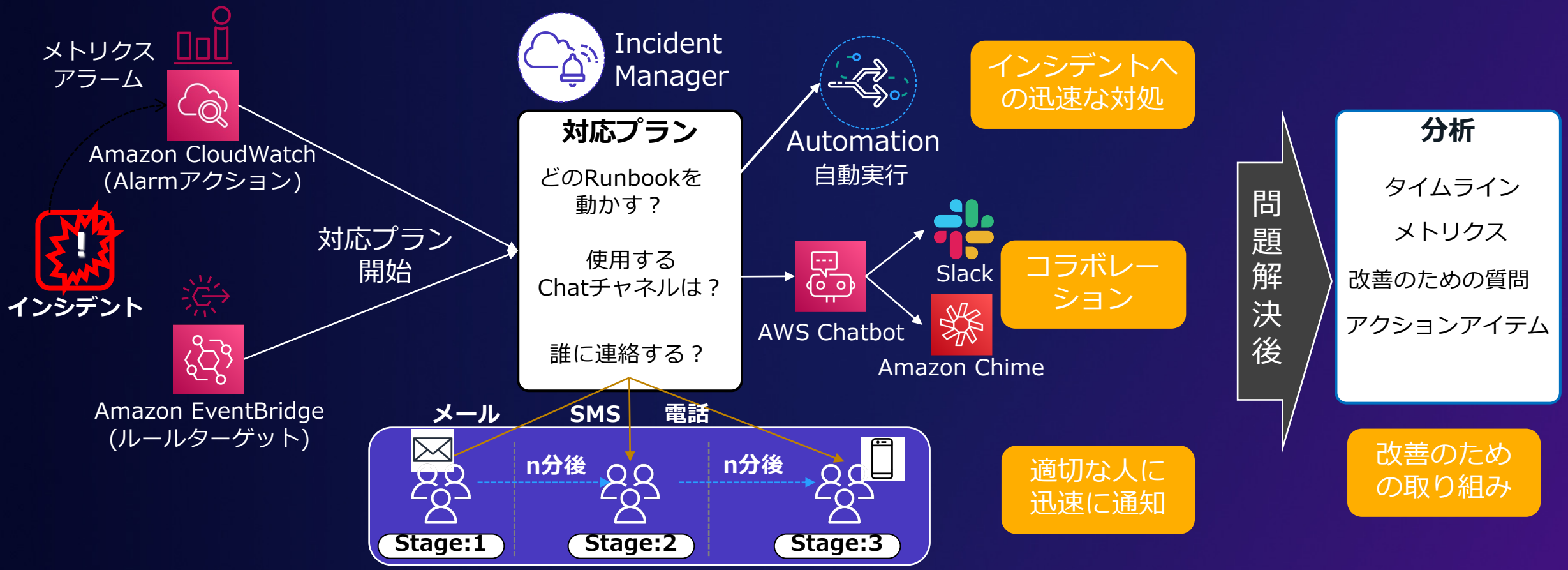

Incident Manager についての詳細はこちら。

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Incident Manager

Remediate Issues

## 事前に準備された対応計画、ランブック、分析による改善

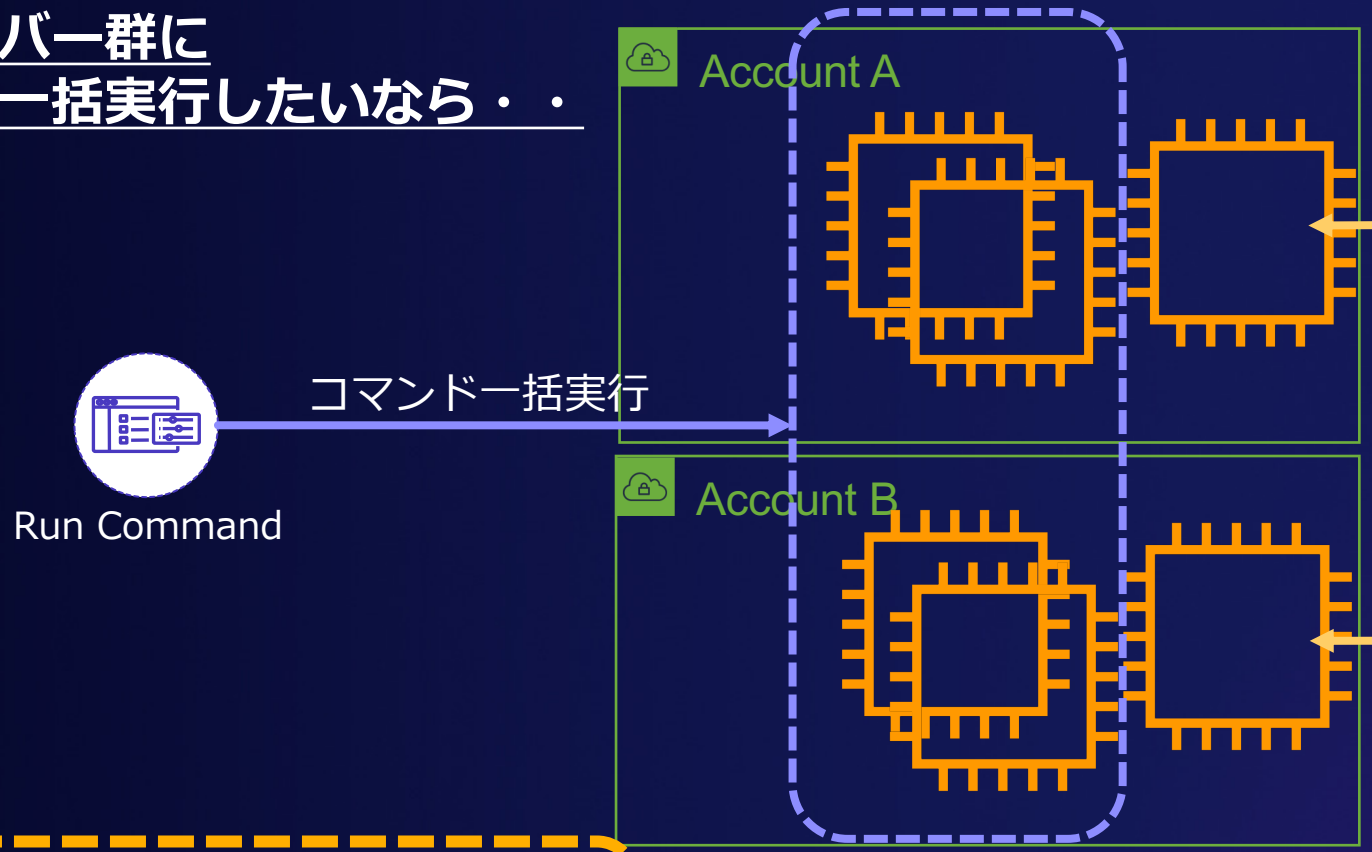



Incident Manager についての詳細はこちら。

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# おさらい

**対象サーバー群に**
**コマンド一括実行したいなら・・**




**個々のサーバーに対して**
**インタラクティブにコマンド**
**操作したいなら・・**

**インシデント管理**

Incident Manager

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# 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

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# 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

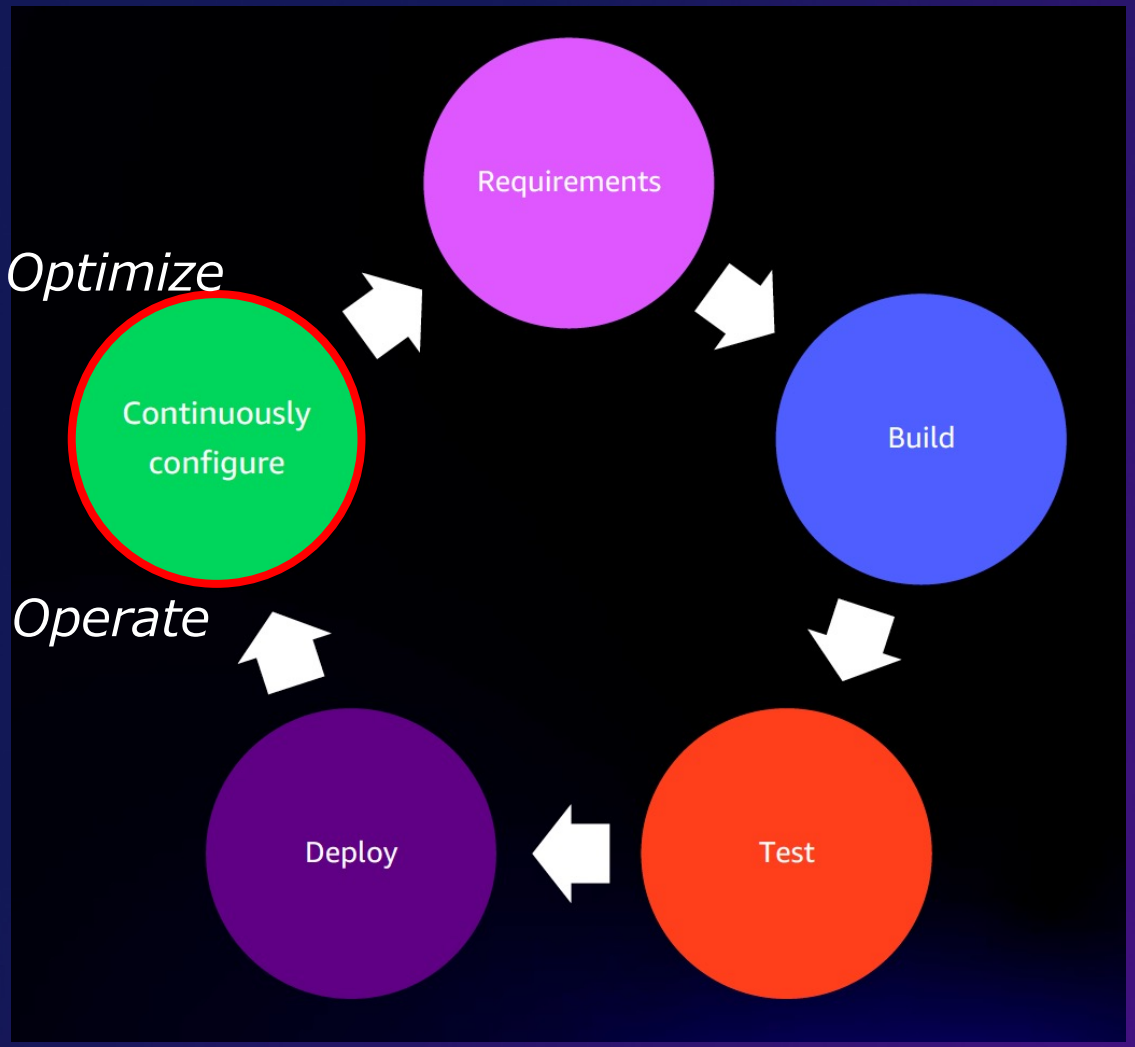
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# AWS Systems Manager で実現するアプリケーション管理

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# 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。

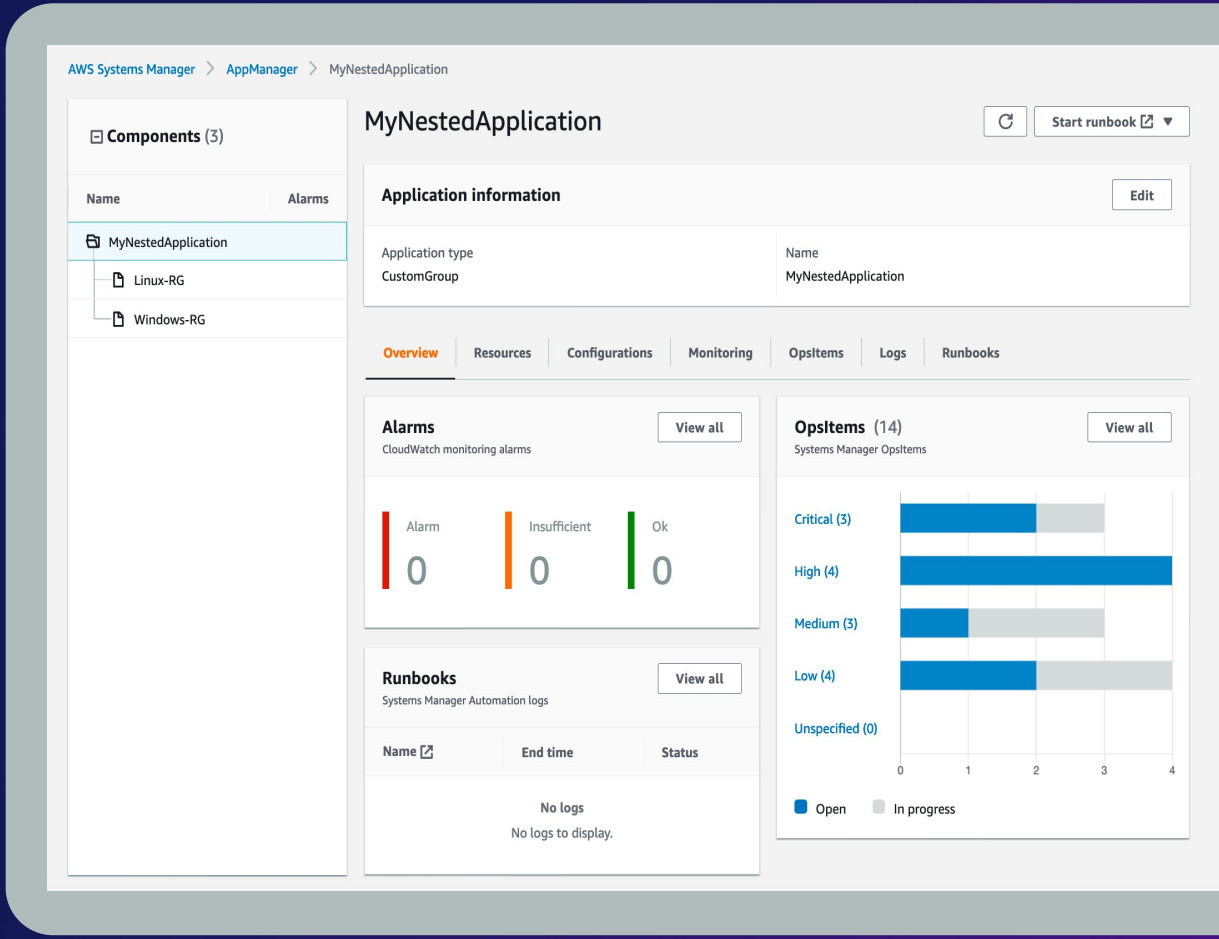



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# 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、デプロイステータスや CloudWatch アラーム、リソース設定や OpsItem などが確認できる。



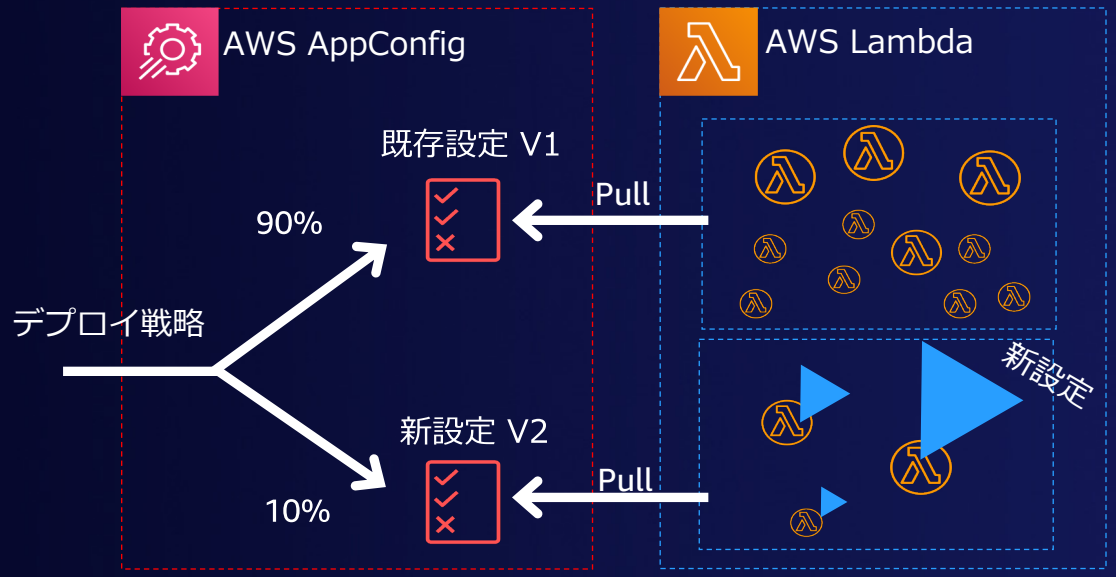

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

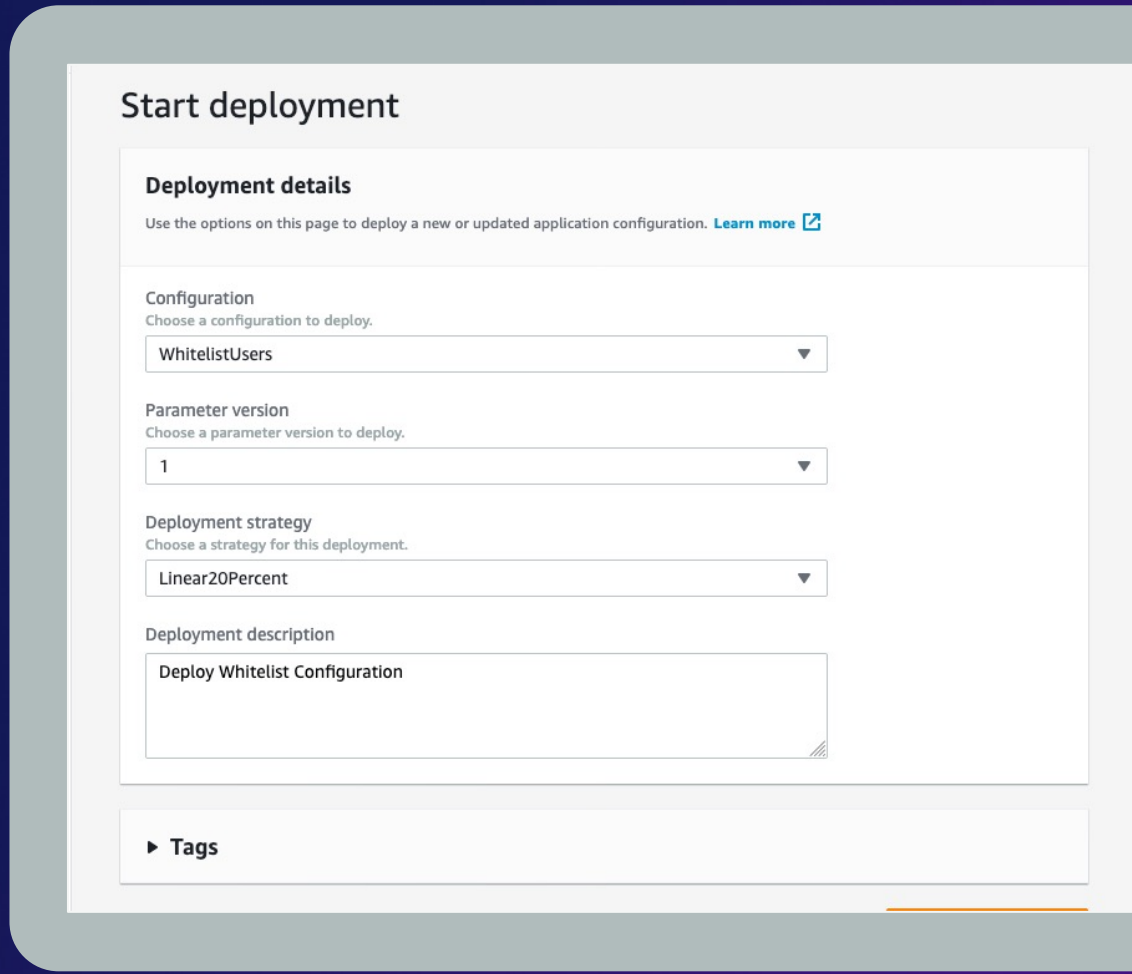
Application Manager についての詳細はこちら。

# 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。



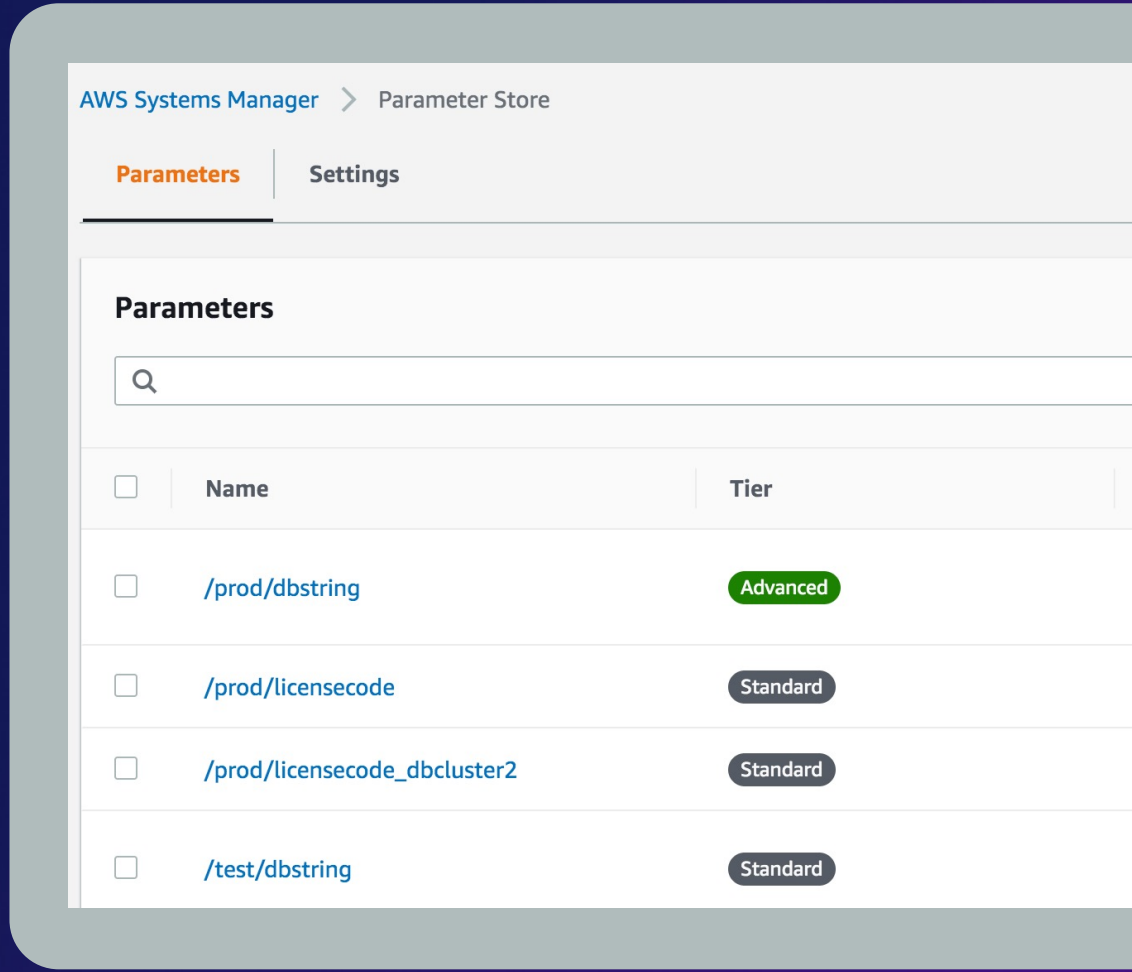

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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

- アプリケーションの設定値とシークレットを格納。
- 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。

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# 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

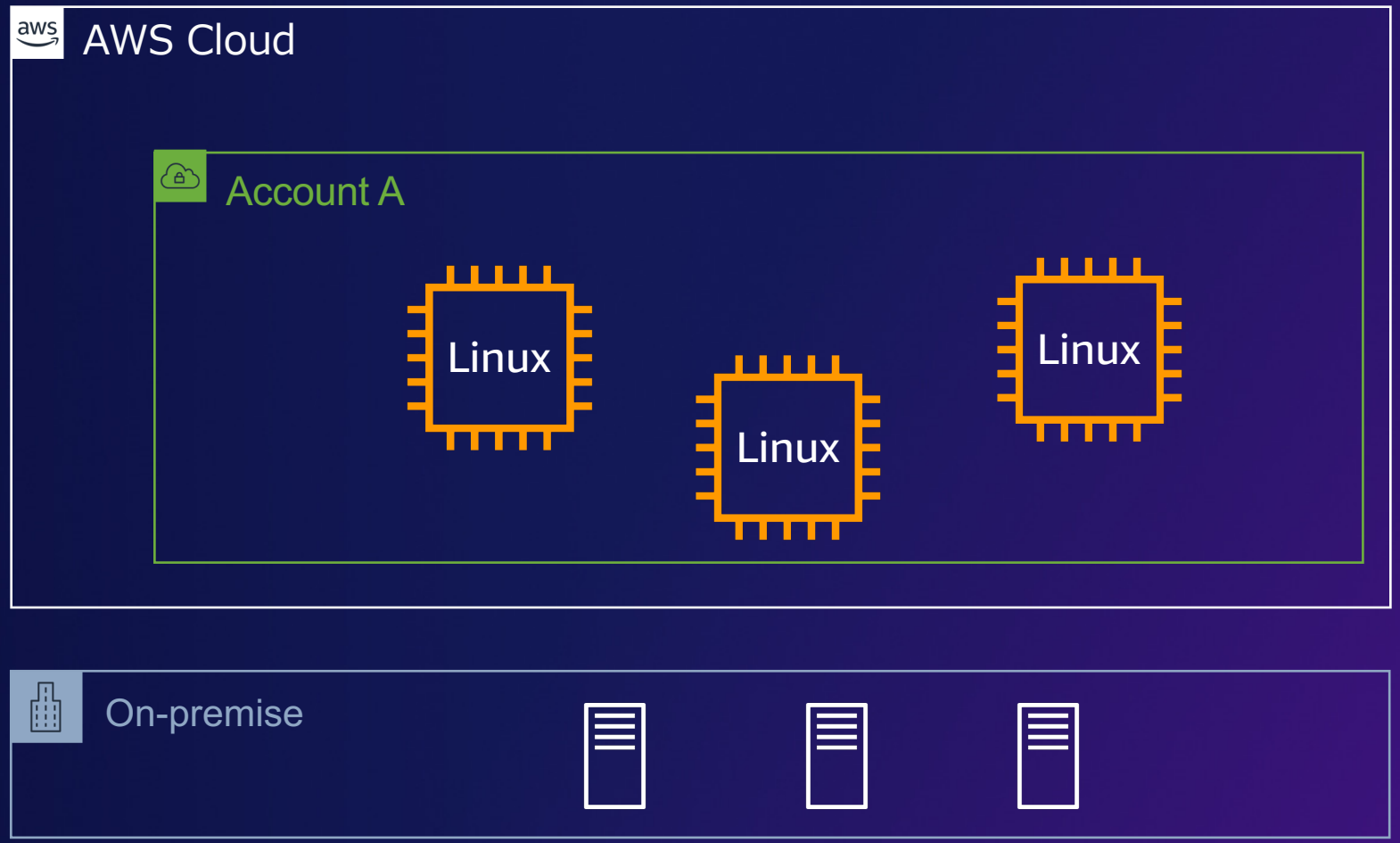
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# マルチアカウント・ハイブリッド環境での使用

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# AWS の使いはじめ

はじめは小規模から。
アカウントは一つだけ。



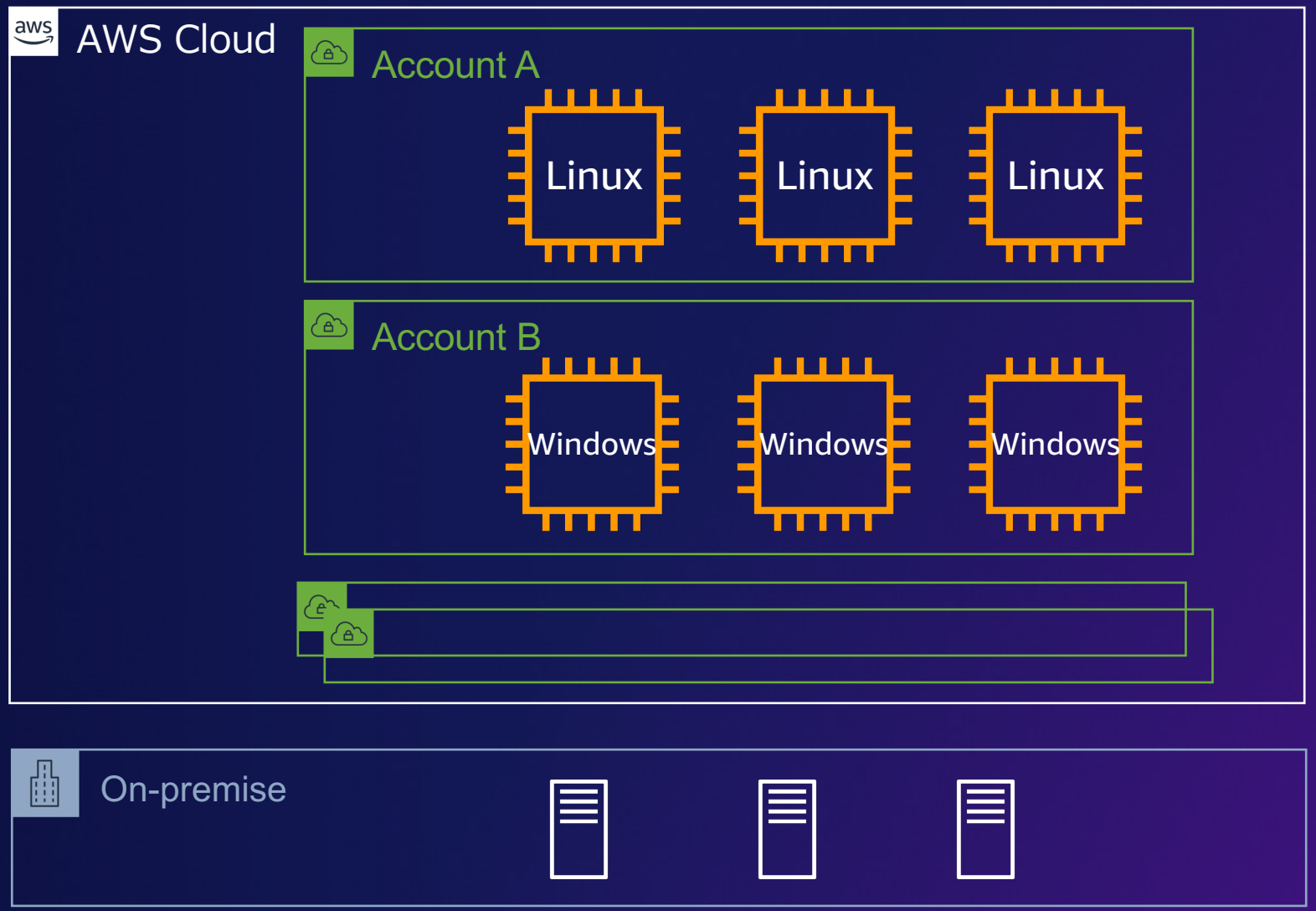

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# いつの間にやら、こんなことに

はじめは小規模から。
アカウントは一つだけ。

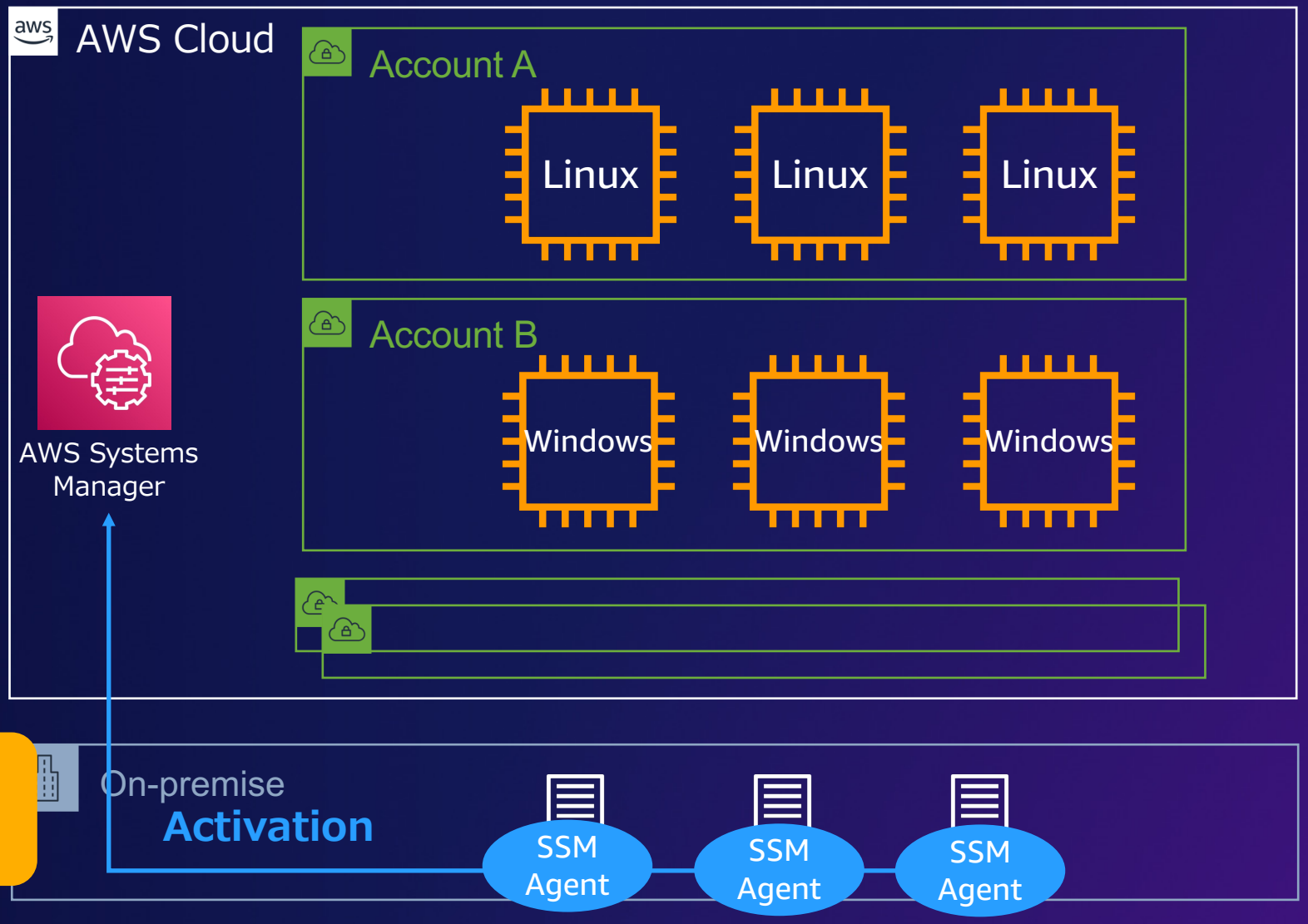
しかし、管理すべき
アカウントは増えていく。

オンプレミスとの
ハイブリッド運用も
負担になってきた。




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# まず、ハイブリッド運用

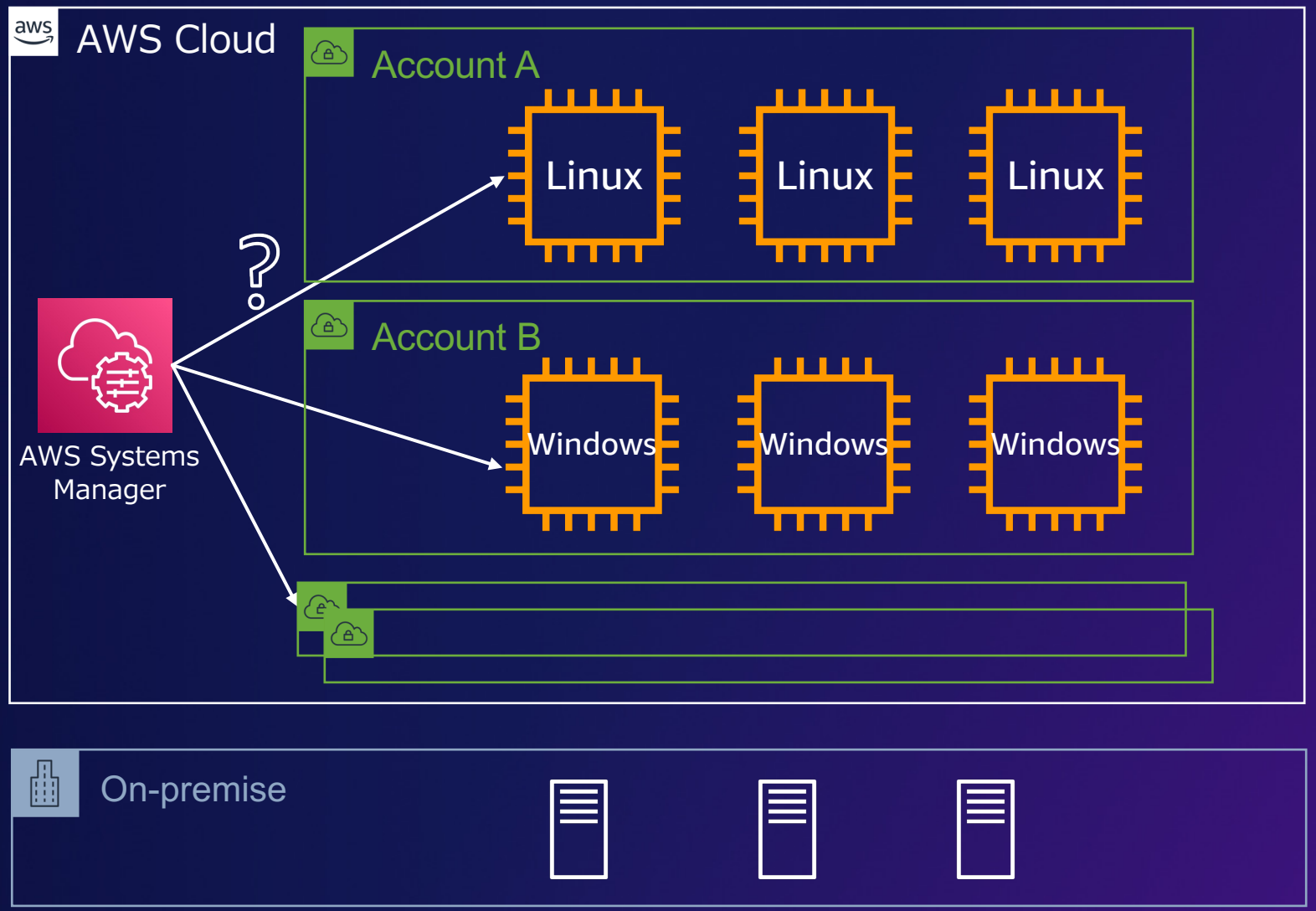



オンプレミスも AWS も同じ運用が実現できる！

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

ハイブリッド環境での使用については、こちら。

# では、マルチアカウント運用は？




© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# マルチアカウントにて使用できる機能群

| 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 ※4 |
| OpsCenter | AppConfig | Automation | Session Manager |
| Incident Manager ※1 | Parameter Store | Maintenance Windows | Inventory ※2 |
| | | Change Calendar ※1 | Run Command |
| | | | Patch Manager |
| | | | Distributor ※3 |
| | | | State Manager ※5 |

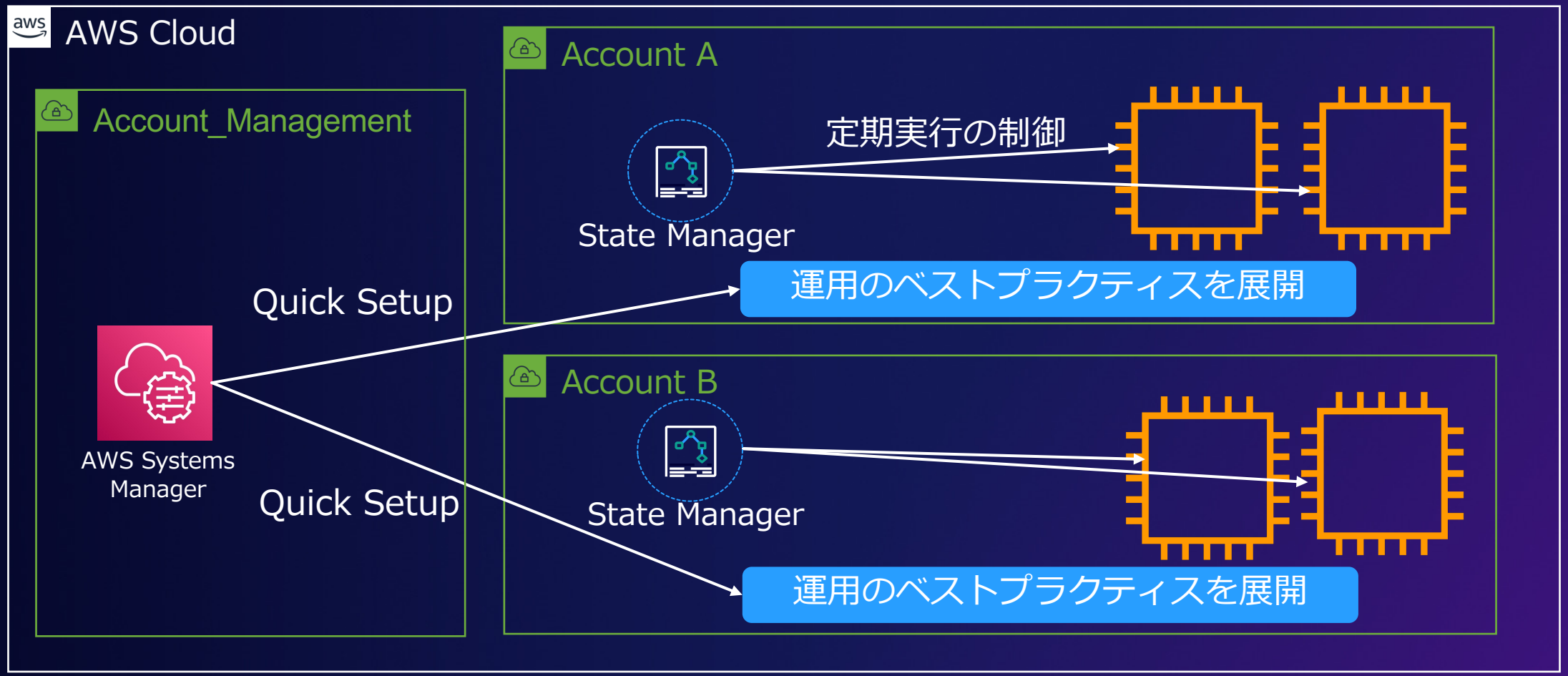
(※1) リソース共有が可能
(※2) S3に同期することでマルチアカウントのダッシュボードが作成可能
(※3) Runbook でラップすることで可能
(※4) Explorer側で集約が可能
(※5) Runbook の実行のみ。APIにて実施可能

Quick Setup

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Build Foundation

# マルチアカウントに運用のベストプラクティスを展開可能

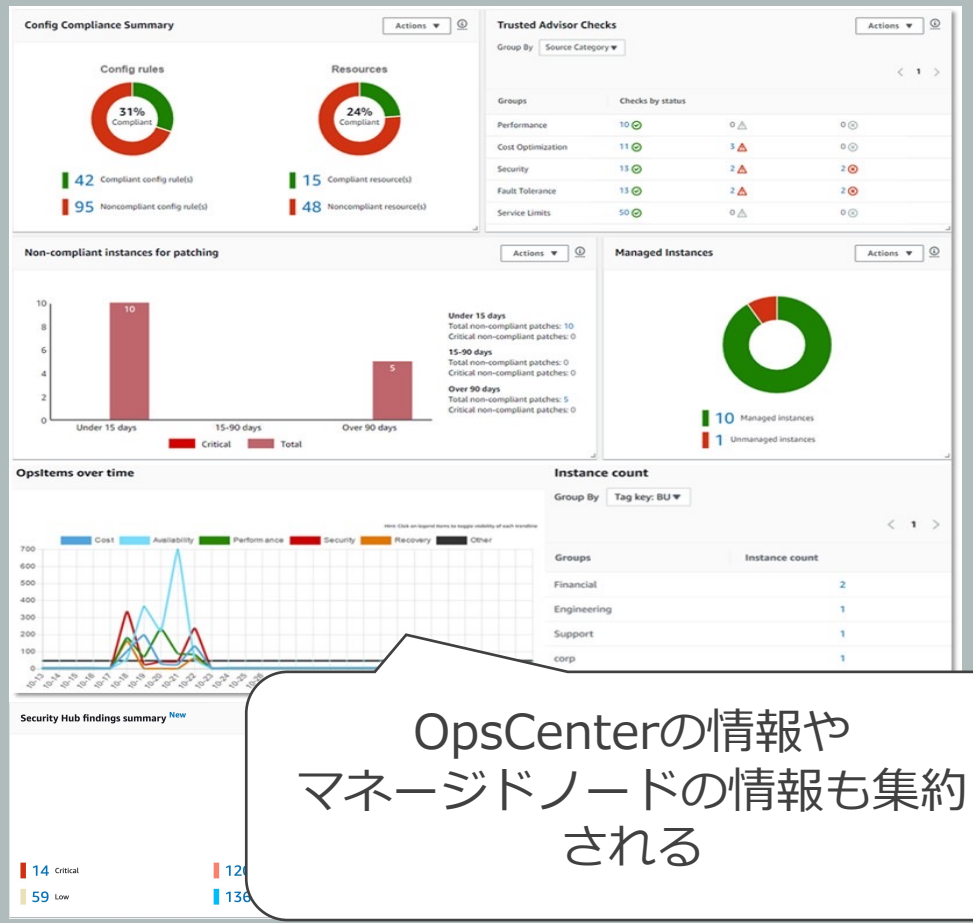



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# マルチアカウントでの可視化

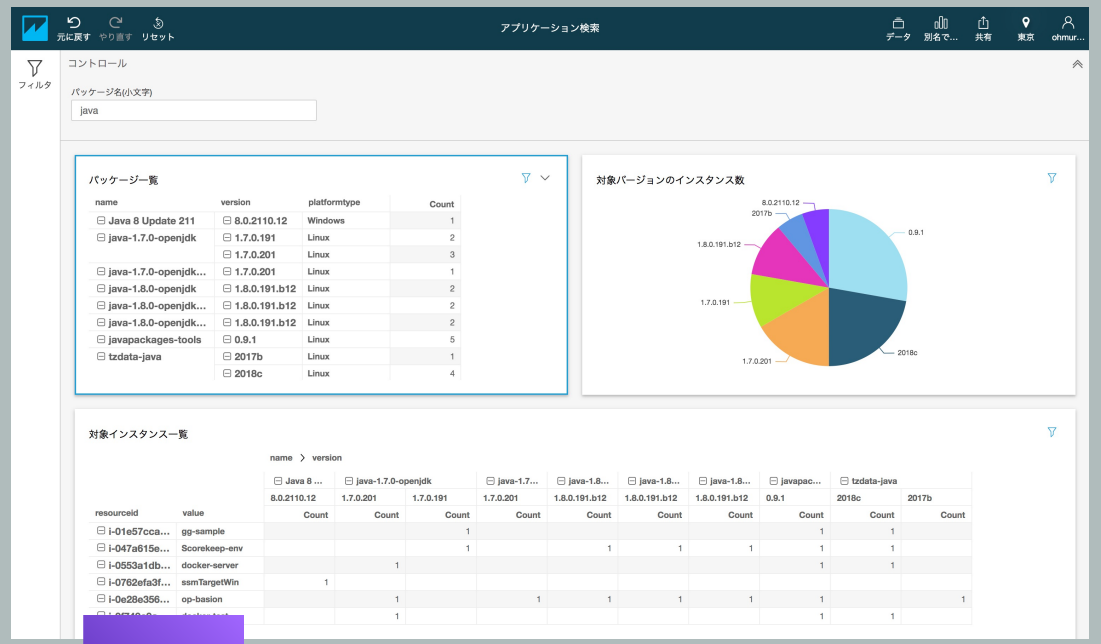
Enable Visibility

## Explorer ダッシュボード




OpsCenterの情報や
マネージドノードの情報も集約
される

## Inventory データの QuickSight ダッシュボード



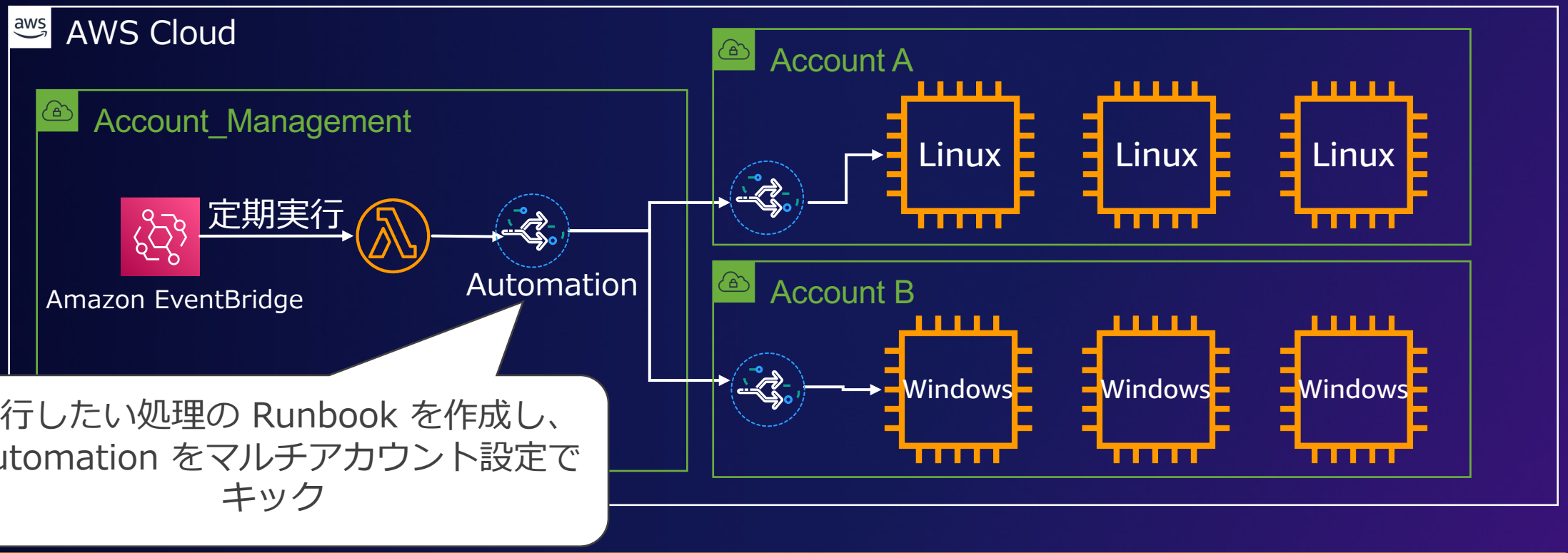

Amazon QuickSight

Inventory の QuickSight 連携はこちらを参照

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Proactively Automate

# マルチアカウントでの自動化処理



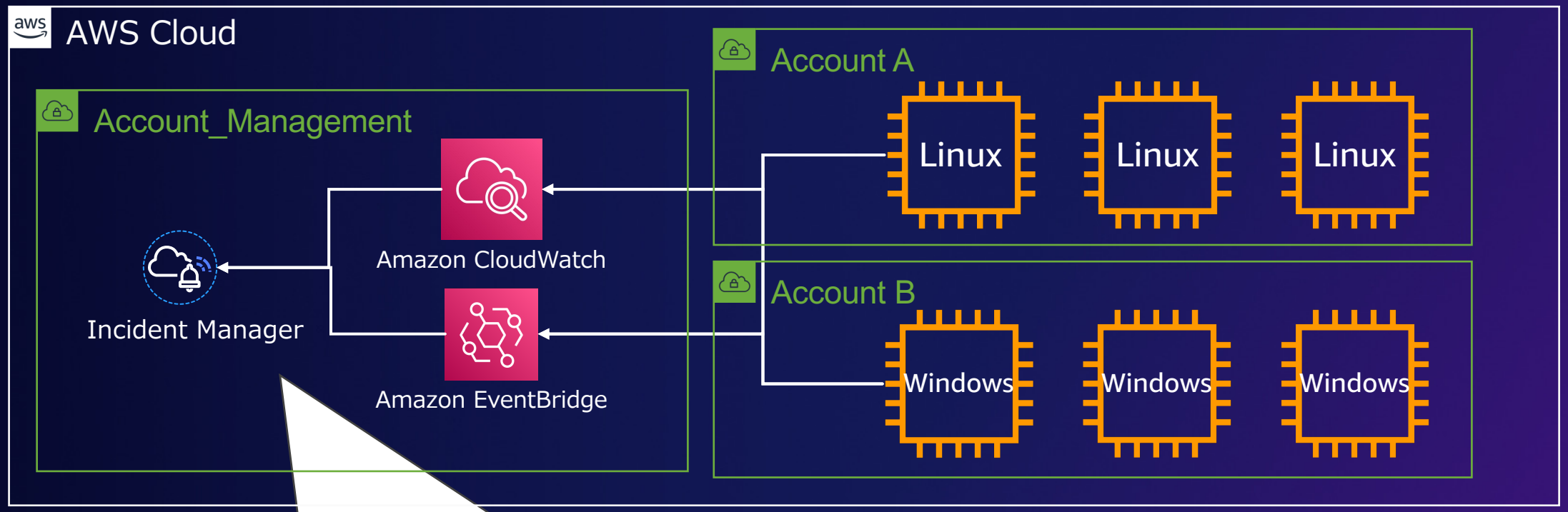

**Automationを使えば、組織内のアカウントに対し、一括でコマンド発行が可能**

パッチのマルチアカウントでの適用についてはこちらのブログ参照
「AWS Systems Manager Automation を使用したマルチアカウントおよびマルチリージョン環境のパッチ管理」
ソフトウェアパッケージのマルチアカウントへの配布についてはこちらのブログ参照
「AWS Systems Manager Distributor による AWS Organizations 管理下のアカウントへのソフトウェアパッケージ配布」

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# マルチアカウントでのインシデント管理

Remediate Issues




EventBridge やCloudWatch Alarm にて
アラートを集約。
Incident Manager の起動が可能

アラートを集約することで、組織内のインシデントの管理が可能に

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# まとめ

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# 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。

マルチアカウント環境でもお使いいただけるような機能群も用意されています。

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。

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Thank you!

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.