



AWS Systems Manager

Inventory 編

AWS Black Belt Online Seminar

上野 涼平

Solutions Architect
2023/06

AWS Black Belt Online Seminarとは

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

内容についての注意点

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

所属：ソリューションアーキテクト

経歴：AWS ユーザーの立場で、オンプレミスからの移行、AWS 環境の運用改善



好きなAWSサービス：AWS Systems Manager



本セミナーの対象者

- AWS の運用を担当されている方
- これから AWS の運用を担当予定の方

本セミナーの目的

- AWS Systems Manager Inventory 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 の全体像
→ [AWS Systems Manager Overview](#) を参照ください
- AWS Systems Manager Inventory 以外の機能の詳細
→ 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. AWS Systems Manager の概要
2. Systems Manager Inventory とは
3. Inventory 応用編
4. まとめ

AWS Systems 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



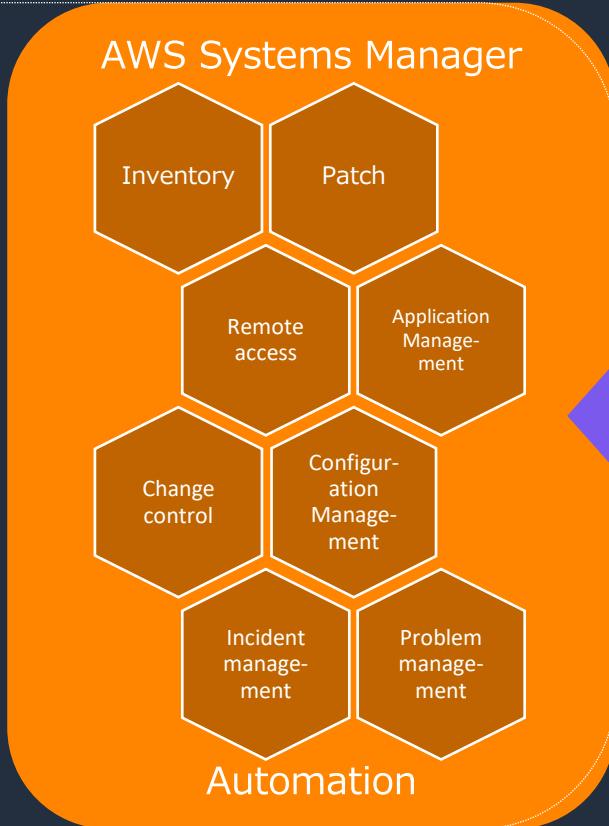
AWS CloudTrail

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

(*) AWS Systems Manager = SSM と略します。

AWS Systems Manager の機能

運用管理

-  Explorer
-  OpsCenter
-  Incident Manager

アプリケーション管理

-  Application Manager
-  AppConfig
-  Parameter Store

変更管理

-  Change Manager
-  Automation
-  Maintenance Windows
-  Change Calendar

ノード管理

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

Quick Setup

AWS Systems Manager の機能

運用管理

-  Explorer
-  OpsCenter
-  Incident Manager

アプリケーション管理

-  Application Manager
-  AppConfig
-  Parameter Store

変更管理

-  Change Manager
-  Automation
-  Maintenance Windows
-  Change Calendar

ノード管理

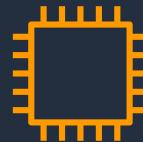
-  Fleet Manager
-  Session Manager
-  Inventory
-  Run Command
-  Patch Manager
-  Distributor
-  State Manager

Quick Setup

Systems Manager Inventory とは

インベントリデータ管理における従来の課題

インベントリデータとは？



- OS 情報
- ソフトウェア情報
- ファイル情報
- ネットワーク構成情報 etc

○○の脆弱性が
見つかったから
該当するサーバーの
調査よろしく！



管理表の最終更新が
2年前になっている…
直接確認しないと…

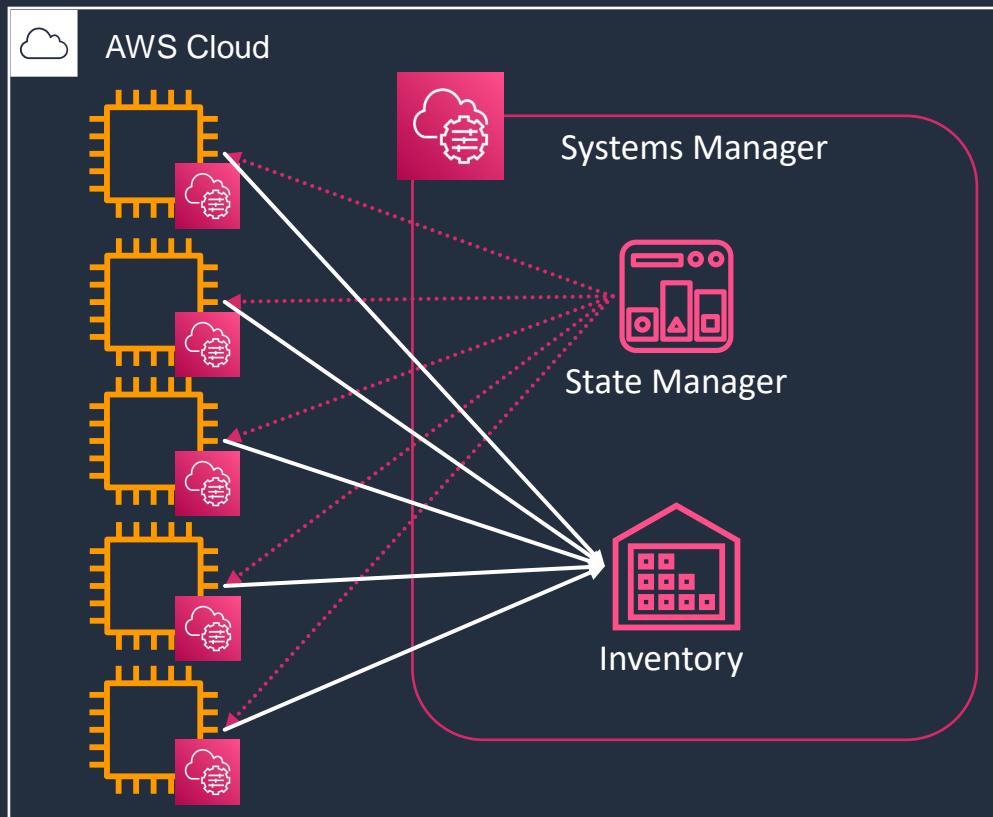


インベントリデータ管理の例

- Excel で手動管理している
- 管理表の更新漏れで実機と差異が発生
- 正しい情報確認のためにサーバー1台ずつ接続して確認しないといけない



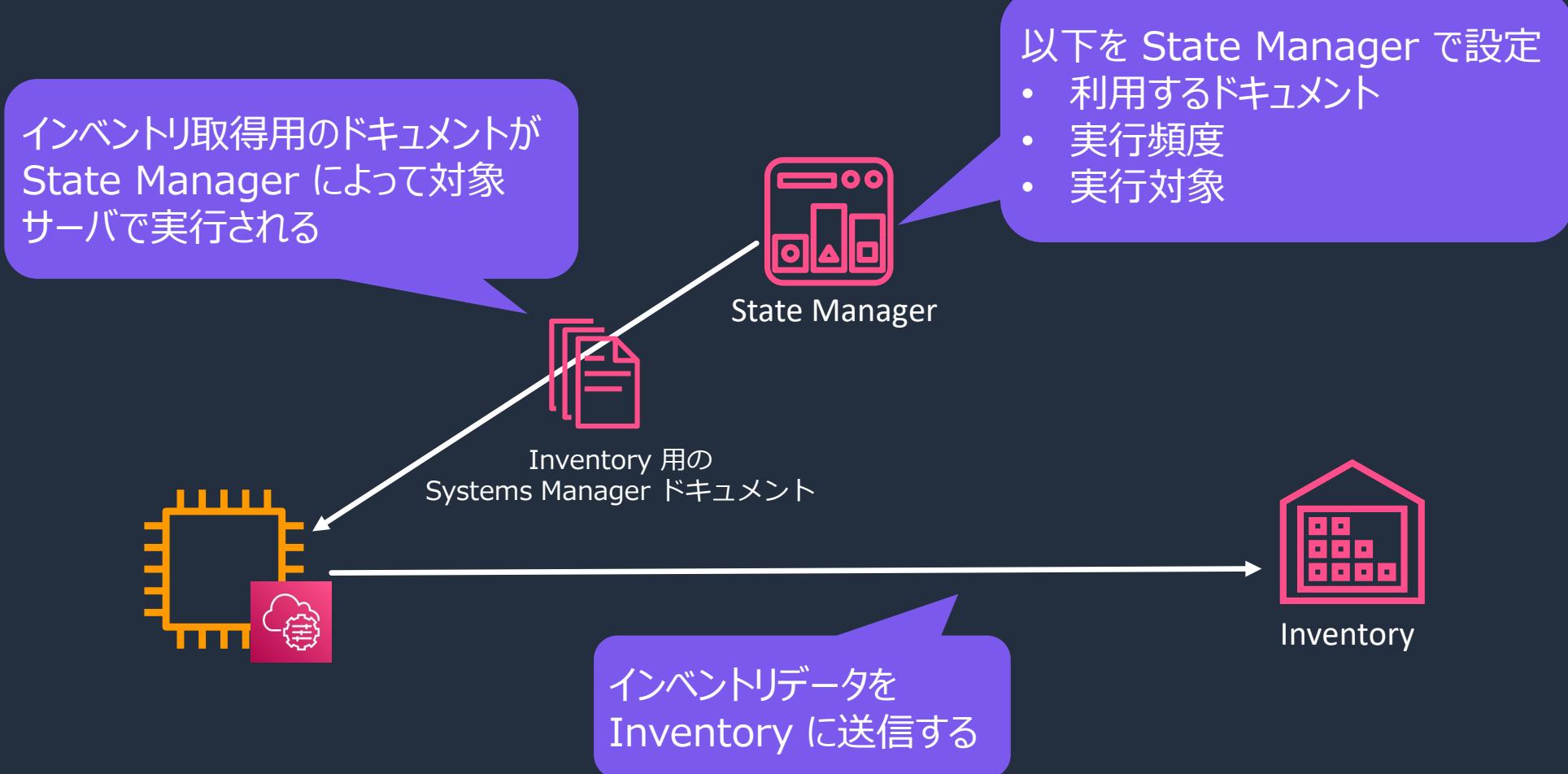
Systems Manager Inventory とは



インベントリデータの収集、一元的な管理が可能

- 最短 30分ごとにサーバーのインベントリデータを定期的に収集し、最新の状態を保つ
- Fleet Manager からマネージドノードごとにインベントリデータを確認可能
- ダッシュボードから特定のバージョン・ソフトウェア名などの条件もとにフィルタリングが可能
- State Manager の associations (関連付け)の設定により、インベントリデータの収集が行われる
- データは30日間保持。30日以上保存する必要がある場合、後述するリソースデータの同期を利用
- Inventory 利用に料金はかかりません

Inventory と State Manager



Inventory で収集出来るデータ

インベントリタイプ	詳細
アプリケーション	アプリケーション名、発行元、バージョンなど
AWS コンポーネント	EC2 ドライバ、エージェント、バージョンなど
ファイル	名前、サイズ、バージョン、インストール日、変更および最新アクセス時間など
ネットワーク構成情報	IP アドレス、MAC アドレス、DNS、ゲートウェイ、サブネットマスクなど
Windows Update	Windows Updateに関する情報 (Hotfix ID、インストール者、インストール日など)
インスタンスの詳細	OS名、OSバージョン、最終起動、DNS、ドメイン、ワークグループ、OS アーキテクチャなど
サービス	名前、表示名、ステータス、依存サービス、サービスのタイプ、起動タイプなど
タグ	インスタンスに割り当てられているタグ
Windows レジストリ	レジストリキーのパス、値の名前、値タイプおよび値
Windows ロール	名前、表示名、パス、機能タイプ、インストール日など
カスタムインベントリ	カスタムに割り当てられるメタデータ。例えばオンプレミスの各インスタンスのラック位置など

<https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-inventory.html>



補足：Inventory で取得されるアプリケーション情報

- インベントリタイプ：アプリケーションでは、OS 系パッケージを取得します。
- そのため、npm、pip、Composer などの各言語系のパッケージは取得対象外となっております。

Linux 系の例

```
// rpm commands related constants
  rpmCmd          = "rpm"
  rpmCmdArgToGetAllApplications = "-qa"    ➔ rpm -qa コマンド
  rpmQueryFormat      = "--queryformat"
  rpmQueryFormatArgs   = `¥{"Name":`` + mark(`%{NAME}`) + `","Publisher":`` + mark(`%{VENDOR}`) + `","Version":`` +
    mark(`%{VERSION}`) + `","Release":`` + mark(`%{RELEASE}`) + `","Epoch":`` + mark(`%{EPOCH}`) + `",
    "InstalledTime":`` + mark(`%{INSTALLTIME}`) + `","ApplicationType":`` + mark(`%{GROUP}`) + `",
    "Architecture":`` + mark(`%{ARCH}`) + `","Url":`` + mark(`%{URL}`) + `",
    "Summary":`` + mark(`%{Summary}`) + `","PackageId":`` + mark(`%{SourceRPM}`) + `"}},`
```

詳細は ssm-agent のソースコードをご確認ください

<https://github.com/aws/amazon-ssm-agent/tree/b292a1dae6be49964e1f10836bfe8eed766f6b44/agent/plugins/inventory/gatherers/application>

Inventory を利用する前に

インベントリデータ収集対象のサーバーをマネージドノードにする必要があります。

詳細は、AWS Black Belt Online Seminar の「[AWS Systems Manager Overview](#)」をご覧ください



AWS Systems Manager Overview

AWS Black Belt Online Seminar

石橋 香代子

Senior Solutions Architect
2023/02

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

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... 実行状況	ノード名	プラット... Linux	オペレーティ... Amazon Linux AMI	ソースタイプ	ソースアーチ... EC2 インスタンス
i-04970a7f373ac650b	実行中	LaunchedBy5...	Linux	Amazon Linux AMI	EC2 インスタンス	-
mi-0623bfef040aa8...	-	On-prem-Linux	Linux	Amazon Linux	AWS::SSM::Manage...	-
i-016d04a4ae09531af	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
含まれる。



Inventory のセットアップ

ターゲット

ターゲットの選択

- このアカウントのすべてのマネージドインスタンスの選択
- タグの指定
- インスタンスの手動選択

すべてのマネージドインスタンスを指定することが可能

スケジュール
(SSMAgent バージョン 2.0.790.0 以降が必要です)

インベントリデータの収集毎 分 ▾

最短30分の設定が可能

ファイルと Windows レジストリの情報を収集したい場合はパス指定で設定が必要

パラメーター

- Applications
(Optional) Collect data for installed applications.
- AWS Components
(Optional) Collect data for AWS Components like amazon-ssm-agent.
- Network Config
(Optional) Collect data for Network configurations.
- Windows Updates
(Optional, Windows OS only) Collect data for all Windows Updates.
- Instance Detailed Information
(Optional) Collect additional information about the instance, including the CPU model, speed, and the number of cores, to name a few.
- Services
(Optional, Windows OS only, requires SSMAgent version 2.2.64.0 and above) Collect data for service configurations.
- Windows Roles
(Optional, Windows OS only, requires SSMAgent version 2.2.64.0 and above) Collect data for Microsoft Windows role configurations.
- Custom Inventory
(Optional) Collect data for custom inventory.
- Billing Info
(Optional) Collect billing info for license included applications.
- ファイル
(省略可能、 SSMAgent バージョン 2.2.64.0 以降が必要) ファイルに関する情報を収集します。

パス	<input type="text" value="C:\Program Files"/>	パターン - オプション	<input type="text" value=".exe, *.log"/>	再帰的
<input type="button" value="Add another row"/>				
- Windows レジストリ
(省略可能、 Windows OSのみ、 SSMAgent バージョン 2.2.64.0 以降が必要) Microsoft Windows レジストリに関する情報を収集します。

パス	<input type="text" value="HKEY_LOCAL_MACHINE\Software"/>	値の名前 - オプション	<input type="text" value="Name1, Name2"/>	再帰的
----	--	--------------	---	-----



Fleet Manager からインベントリデータを確認可能

ノードの詳細ページに遷移し、インベントリタブを開く

The screenshot shows the AWS Fleet Manager interface with the 'Events' tab selected. A dropdown menu is open under the 'Event Type' heading, showing 'AWS:Application' as the current selection. A purple callout bubble points to this dropdown with the text 'インベントリタイプごとにデータを確認出来る' (You can check data by event type). Below the dropdown is a search bar and a table listing various software packages with columns for Name, Version, Publisher, Application Type, Install Time, Architecture, URL, and Release Date.

名前	バージョン	公開者	アプリケーションタイプ	インストール時刻 (UTC)	アーキテクチャ	URL	Release
vim-data	9.0.1314	Amazon Linux	Unspecified	Fri, 12 May 2023 07:25:46 GMT	noarch	http://www.vim.org/	1.amz
fuse-libs	2.9.2	Amazon Linux	System Environment/Libraries	Mon, 24 Jan 2022 18:28:11 GMT	x86_64	https://github.com/libfuse/libfuse	11.am
kbd-legacy	1.15.5	Amazon Linux	System Environment/Base	Mon, 24 Jan 2022 18:28:00 GMT	noarch	http://ftp.altlinux.org/pub/people/legion/kbd	15.am
nss-softokn	3.79.0	Amazon Linux	System Environment/Libraries	Fri, 12 May 2023 07:25:46 GMT	x86_64	http://www.mozilla.org/projects/security/pki/nss/	4.amz
...	0.11	Amazon	System Environment/Base	Mon, 24 Jan 2022	...	http://www.mozilla.org/projects/security/pki/nss/	...

ダッシュボード

AWS Systems Manager > インベントリ

ダッシュボード | 詳細ビュー | 設定

インベントリ

リソースグループ、タグ、またはインベントリタイプによるフィルタリング
オフラインインスタンスは含まれません (削除済みおよび停止状態 - EC2、削除済み - オンプレミス)

検索:

インベントリが有効になっているマネージドインスタンス

現在のリージョンとアカウントのインスタンスが含まれます。

Enabled Disabled



タイプごとのインベントリカバレッジ

定義済みインベントリタイプのみ。

インベントリタイプ	カバレッジ
AWS:AWSComponent	100%
AWS:Application	100%
AWS:File	100%
AWS:InstanceDetailedInformation	100%
AWS:InstanceInformation	100%
AWS:Network	100%
AWS:Service	100%
AWS:WindowsRegistry	100%
AWS:WindowsRole	100%
AWS:WindowsUpdate	100%

カスタムインベントリタイプのトップ 10

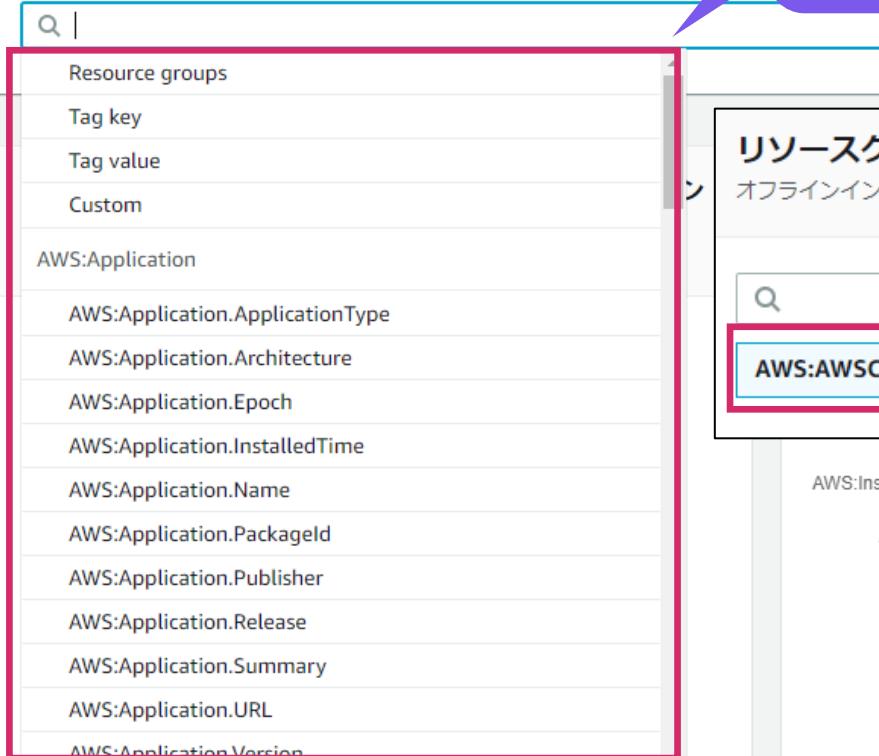
インベントリコレクションに対してお客様が定義したインベントリタイプ。

インベントリタイプ	カバレッジ
RackInfo	100%
RackInformation	100%

インベントリデータのフィルタリング

インベントリ

リソースグループ、タグ、またはインベントリタイプによる
オフラインインスタンスは含まれません (削除済みおよび停止状態 - EC2、削除済み - オンプレミス)



インベントリデータの項目等で絞り込みが出来る

リソースグループ、タグ、またはインベントリタイプによるフィルタリング
オフラインインスタンスは含まれません (削除済みおよび停止状態 - EC2、削除済み - オンプレミス)



AWS:AWSComponent.Name: Equal: amazon-ssm-agent X

AWS:AWSComponent.Version: Less than: 3.3 X

Clear filters

ssm agent のバージョンが3.3以下
という条件で絞り込みをした例

インベントリ履歴と変更の追跡

AWS Config を使用することで、インベントリの変更履歴を確認することができます

リソースタイプ	詳細
SSM:ManagedInstanceInventory	マネージドノードのインベントリデータ
SSM:PatchCompliance	Systems Manager Patch Managerでのパッチ適用状況
SSM:AssociationCompliance	Systems Manager State Manager の associations(関連付け)の適用状況
SSM:FileData	サーバー内のファイル (Inventory でインベントリタイプ「AWS : File」を収集している場合)

イベント

すべての時刻 Asia/Tokyo (UTC+09:00)

2023年5月23日

17:52:26 設定変更

JSON diff - 1 フィールドの変更

開始

```
{}
```

終了

```
{
  Configuration.AWS:Application.Content.Amazon CloudWatch Agent: {"InstalledTime": "2023-05-23T00:00:00Z", "PackageId": "(877DABD0-D306-4CF4-BBA1-5E3B8682A179)", "Publisher": "Amazon.com, Inc.", "Architecture": "x86_64", "Version": "1.3.50751", "Name": "Amazon CloudWatch Agent"}
}
```

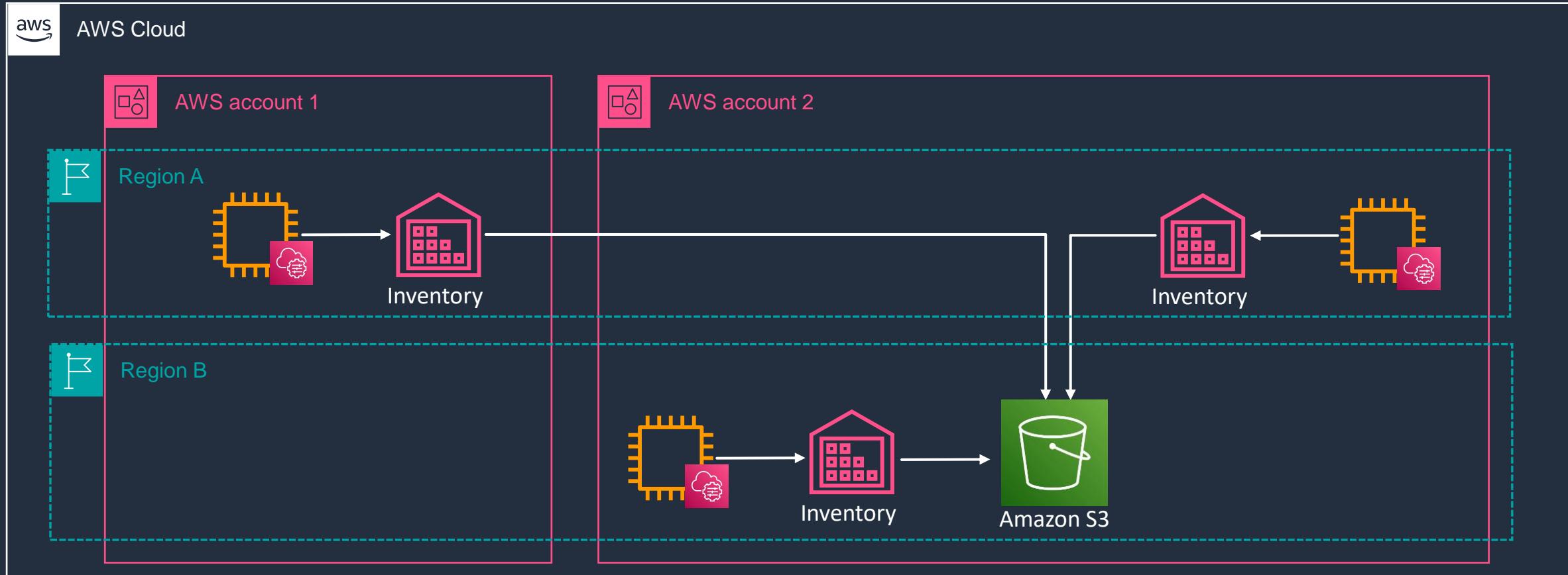
CloudWatch Agent のインストール前後

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



リソースデータの同期 1/3

リソースデータ同期を使用して、リージョンおよび AWS アカウントを横断ですべてのマネージドノードから収集されたインベントリデータを、1 つの Amazon S3 バケットに送信できます。

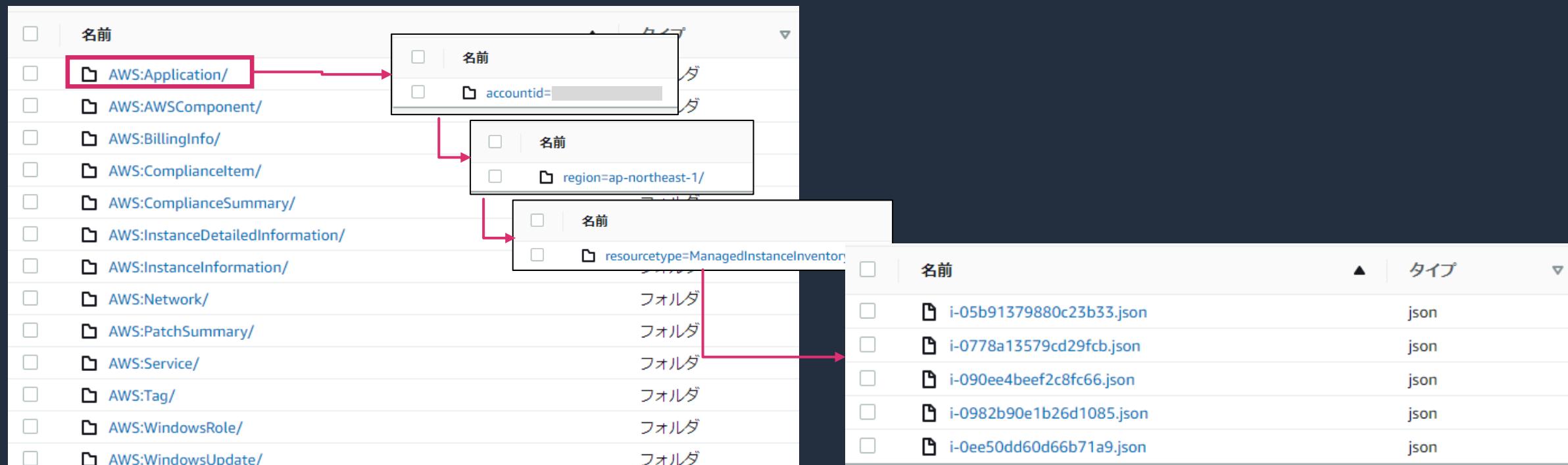


リソースデータの同期 2/3

同期タイミング

新しいイベントリデータが収集されると、Systems Manager は Amazon S3 バケットのデータを自動的に更新します。

リソースデータの同期によってS3に保存されたデータ



リソースデータの同期 3/3

AWS Systems Manager > インベントリ

ダッシュボード 詳細ビュー 設定

この機能では、AWS Athena、AWS Glue、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表示します。この機能を使用するには、リソースデータの同期を選択する必要があります。料金が適用される場合があります。

リソースデータの同期 リソースデータの同期の作成

test01-single
同期日: Mon May 22 2023 14:47:32 GMT+0900 (日本標準時) 前回のステータス: Successful 最終の同期: Wed May 24 2023 15:40:19 GMT+0900 (日本標準時) 最後に成功した同期: Wed May 24 2023 15:40:19 GMT+0900 (日本標準時)

インベントリタイプ AWS:Application

インベントリデータ

詳細ビューから作成したリソースデータの同期を選択すると、Amazon Athena、AWS Glue によってインベントリデータに対してクエリが実行できるようになる

Region	Account ID	Region	Installed time	Architecture	Version	Summary	Package ID
-		ap-northeast-1	-	i386	1.3.175.27	-	
-		ap-northeast-1	-	i386	2.3.28307	-	
-		ap-northeast-1	2023-03-15T00:00:00Z	i386	113.0.1774.35	-	
-		ap-northeast-1	-	i386	14.29.30139.0	-	

ポート Query History Run Advanced Queries

詳細ビューからは Region と Account ID によるフィルターしか出来ないため、細やかなクエリを実行したい場合は、[Run Advanced Queries]から Athena のコンソールへ遷移

Inventory 應用編

カスタムインベントリ

- ・ カスタムインベントリを作成することで、任意の固定値やコマンド実行で得られる結果などノードに必要なあらゆるメタデータを割り当てることが可能
- ・ API 実行（ PutInventory API ）または、 JSON ファイルを所定のパス配下に配置
- ・ API 実行では実行時にカスタムインベントリデータが割り当てられる。 JSON ファイル配置の場合、 State Manager の associations (関連付け) の設定に基づき JSON ファイル記載の内容が収集される

OS	JSON ファイル配置パス
Linux	/var/lib/amazon/ssm/ <i>node-id</i> /inventory/custom
macOS	/opt/aws/ssm/data/ <i>node-id</i> /inventory/custom
Windows	%SystemDrive%¥ProgramData¥Amazon¥SSM¥InstanceId ¥ <i>node-id</i> ¥inventory¥custom

JSON ファイルの例

```
{  
  "SchemaVersion": "1.0",  
  "TypeName": "Custom:RackInformation",  
  "Content": {  
    "Location": "US-EAST-02.CMH.RACK1",  
    "InstalledTime": "2016-01-01T01:01:01Z",  
    "vendor": "DELL",  
    "Zone" : "BJS12",  
    "TimeZone": "UTC-8"  
  }  
}
```

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/sysman-inventory-custom.html



動的なカスタムインベントリの設定

- JSON ファイルに定義した固定値ではなく、都度コマンド実行した動的な結果をカスタムインベントリデータとして収集することも可能
- Inventory はインベントリデータの収集アクションを定義した Systems Manager のドキュメントを State Manager が実行する仕組みになっている
- デフォルトで利用される”ドキュメント”の処理に、必要な情報を取得するコマンド実行およびその結果を JSON ファイルに上書きするステップを追加し、カスタムしたドキュメントを State Manager から実行することで実現可能

AWS-GatherSoftwareInventory
ドキュメント(デフォルト利用)



```
mainStep:  
"action": "aws:softwareInventory"
```



カスタムインベントリ用ドキュメント



```
mainStep:  
"action": "runPowerShellScript"  
"inputs": {  
  コマンド実行&JSONファイル上書き  
}  
"action": "aws:softwareInventory"
```

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

<https://aws.amazon.com/jp/blogs/news/use-aws-systems-manager-custom-inventory-to-locate-log4j-files-on-managed-nodes/>



マルチリージョン、マルチアカウント設定

マルチリージョン、マルチアカウントで横断的にインベントリデータの収集、可視化を行うには各リージョン・アカウントで**インベントリデータ収集の設定**および**リソースデータの同期設定**を実施する必要があります。

インベントリデータ収集の設定

AWS Systems Manager Quick Setup の Host Management を利用する

- Organizations の管理アカウントから実施
- 組織全体、OU 単位でインベントリデータ収集の設定を反映可能
- Inventory の画面から設定する場合と比較して、取得できるインベントリタイプに差異がある※
- カスタムインベントリ等でカスタマイズしたドキュメントを使う場合は、Quick Setup は利用できません

※Quick Setup ホスト管理

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/quick-setup-host-management.html



リソースデータの同期設定

マネージメントコンソールまたは API でリソースデータの同期を各リージョン、アカウントで作成

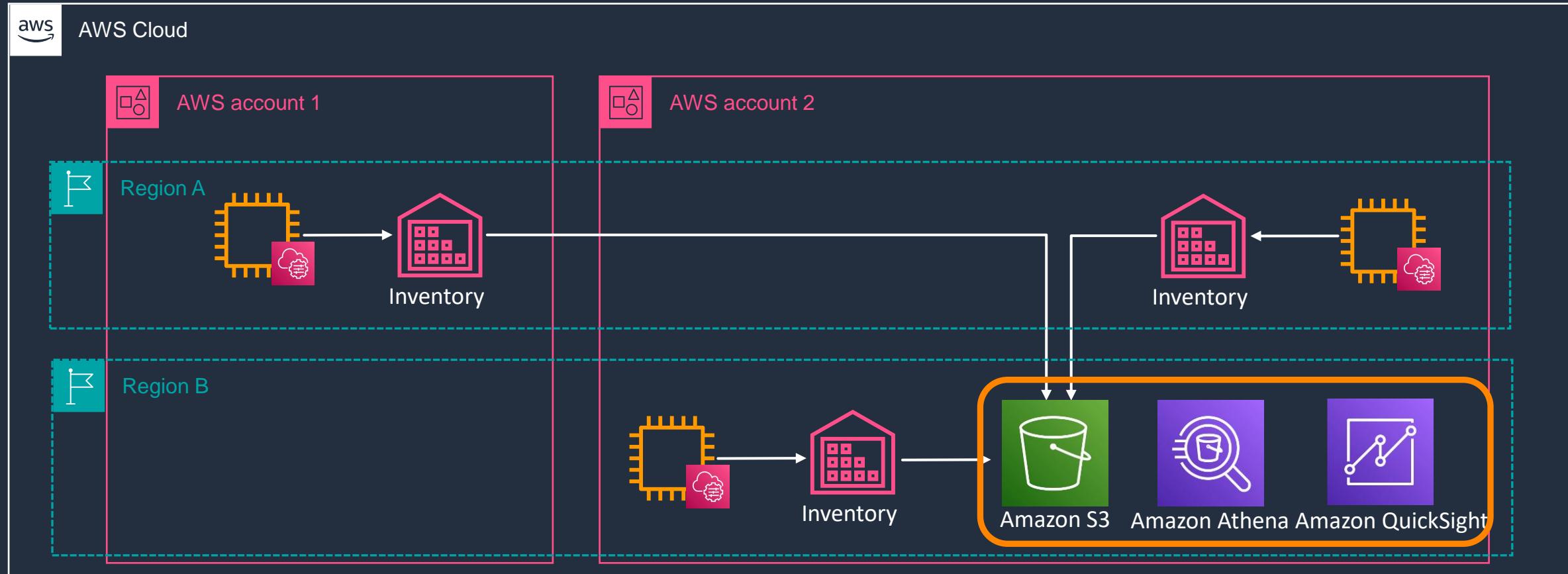
- データを集約する S3 のバケットポリシーにアカウントごとに許可設定を入れる必要あり

リソースデータの同期を作成する API で DestinationDataSharingType=Organization を指定して各リージョン、アカウントで実行

- データを集約する S3 のバケットポリシーには、組織 ID のみを指定

Amazon QuickSight による可視化

リソースデータの同期を設定することでデータが S3 に集約および Amazon Athena のテーブル作成まで行われるため、QuickSight による可視化がすぐに設定可能



Systems Manager & QuickSight ハンズオン

<https://catalog.us-east-1.prod.workshops.aws/workshops/b97f7cb6-0ec4-41c7-97ea-c4156f4f1e0d/ja-JP>

まとめ



まとめ

- Inventory を利用することで、インベントリデータの収集、一元的な管理が可能
 - サーバーに1台ずつ接続して構成情報を確認する運用から解放
- インベントリデータの検索やフィルタリングも可能
 - ダッシュボードの利用またはリソースデータの同期で出力されたデータを Athena や QuickSight で分析も可能
- マルチリージョン、マルチアカウントでインベントリデータの収集が可能

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!