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=PLzWGOASvSx6FIwIC2X1nObr1KcMCBBlqY

内容についての注意点

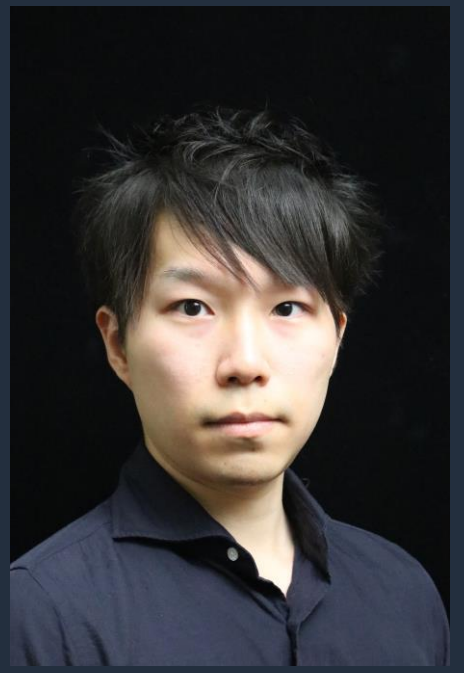
- 本資料では 2023 年 6 月時点のサービス内容および価格についてご説明しています。最新の情報はAWS公式ウェブサイト(https://aws.amazon.com/)にてご確認ください
- 資料作成には十分注意しておりますが、資料内の価格とAWS公式ウェブサイト記載の価格に相違があった場合、AWS公式ウェブサイトの価格を優先とさせていただきます
- 価格は税抜表記となっています。日本居住者のお客様には別途消費税をご請求させていただきます

自己紹介

名前：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

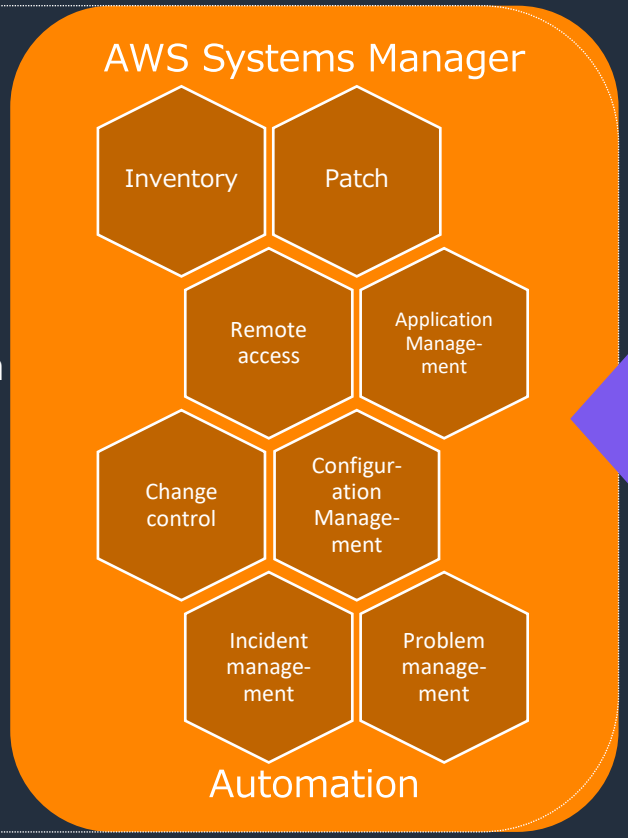
ハイブリッドクラウド環境のための安全なエンドツーエンドの管理ソリューション

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

Cloud On-premises Edge

(*) AWS Systems Manager = SSM と略します。

AWS Systems Manager の機能

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

Quick Setup

AWS Systems Manager の機能

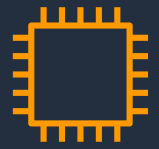
運用管理	アプリケーション管理	変更管理	ノード管理
Explorer	Application Manager	Change Manager	Fleet Manager
OpsCenter	AppConfig	Automation	Session Manager
Incident Manager	Parameter Store	Maintenance Windows	Inventory
		Change Calendar	Run Command
			Patch Manager
			Distributor
			State Manager

Quick Setup

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？



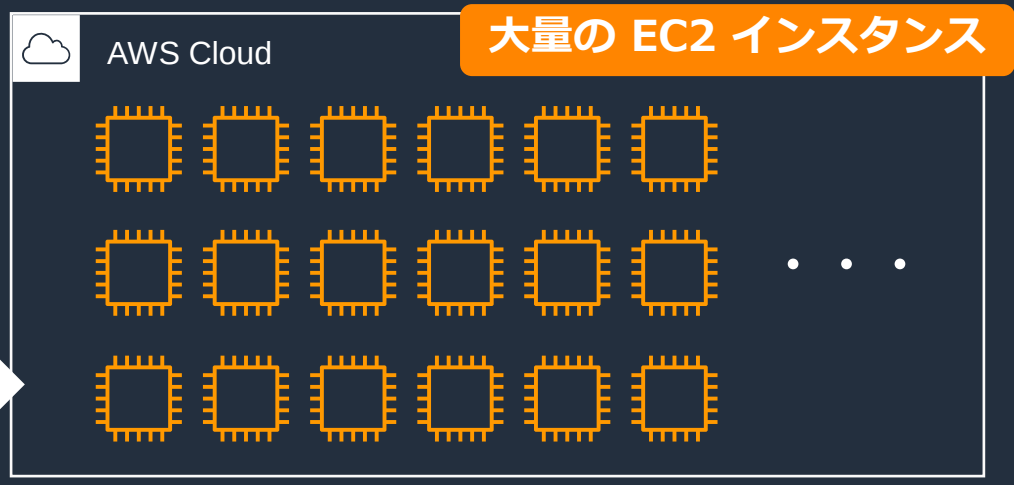
- **OS 情報**
- **ソフトウェア情報**
- **ファイル情報**
- **ネットワーク構成情報 etc**

インベントリデータ管理の例

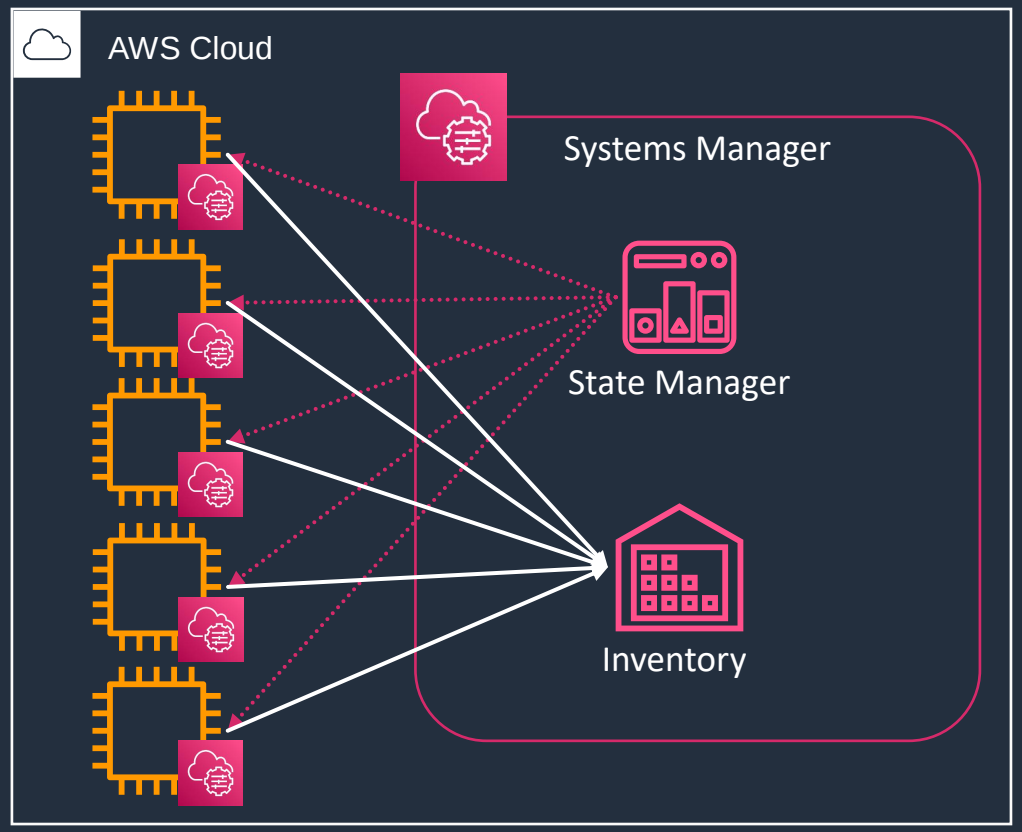
- Excel で手動管理している
- 管理表の更新漏れで実機と差異が発生
- 正しい情報確認のためにサーバー1台ずつ接続して確認しないといけない

○○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…



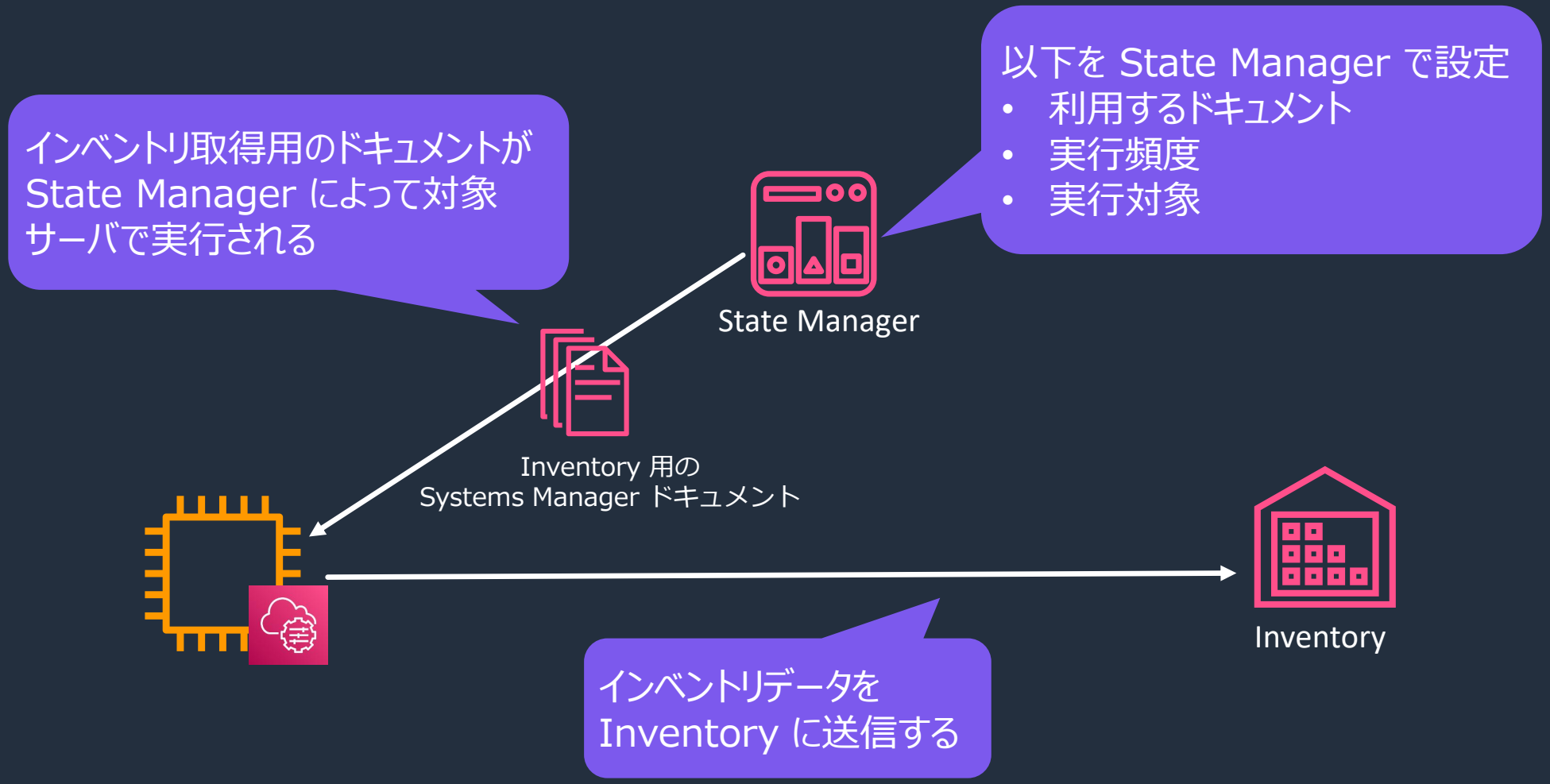
Systems Manager Inventory とは



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"
        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}`) + `"¥},`
```

rpm –qa コマンド

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

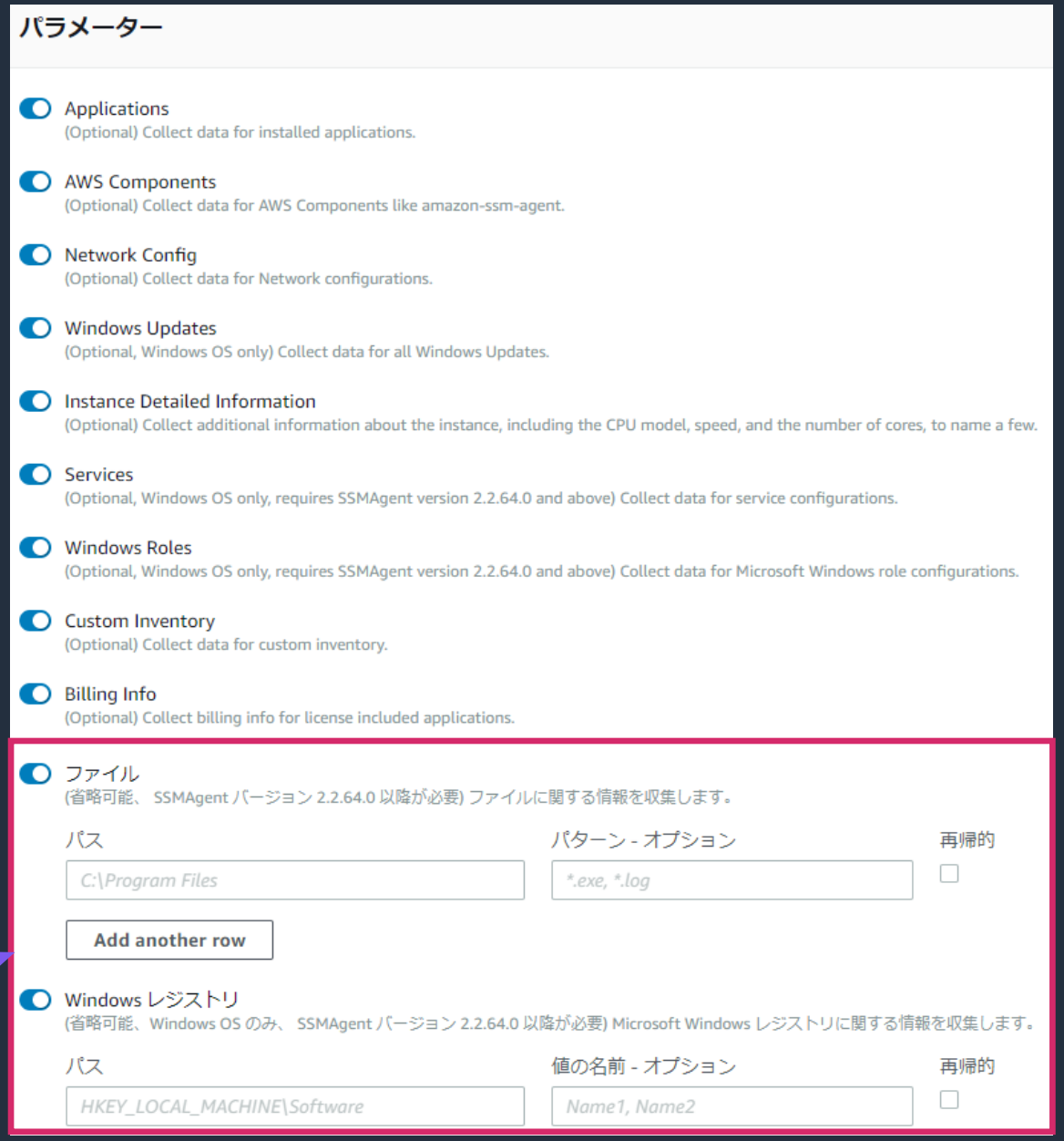
インベントリデータ収集対象のサーバーをマネージドノードにする必要があります。
詳細は、AWS Black Belt Online Seminar の「AWS Systems Manager Overview」をご覧ください

Inventory のセットアップ

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

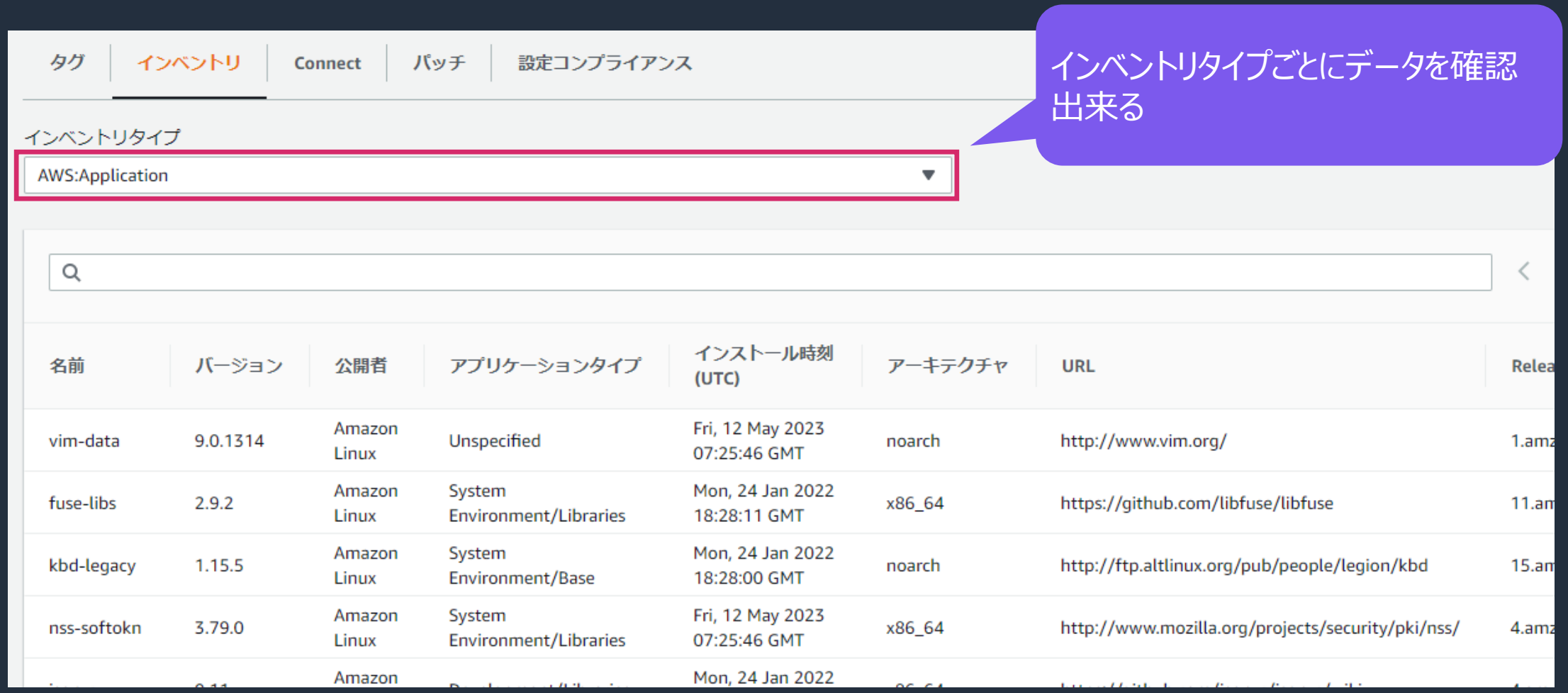
最短30分の設定が可能

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

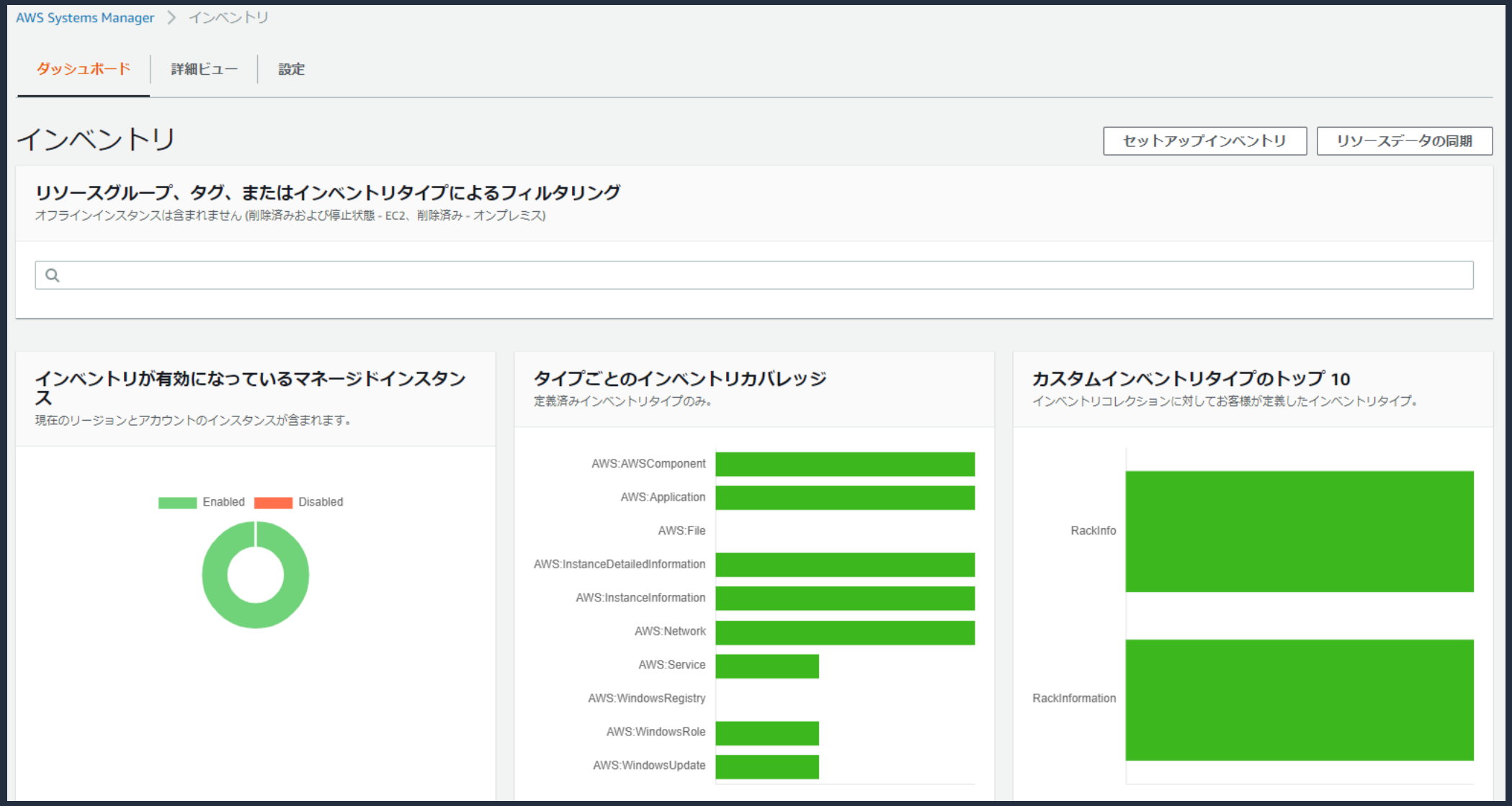


Fleet Manager からインベトリデータを確認可能

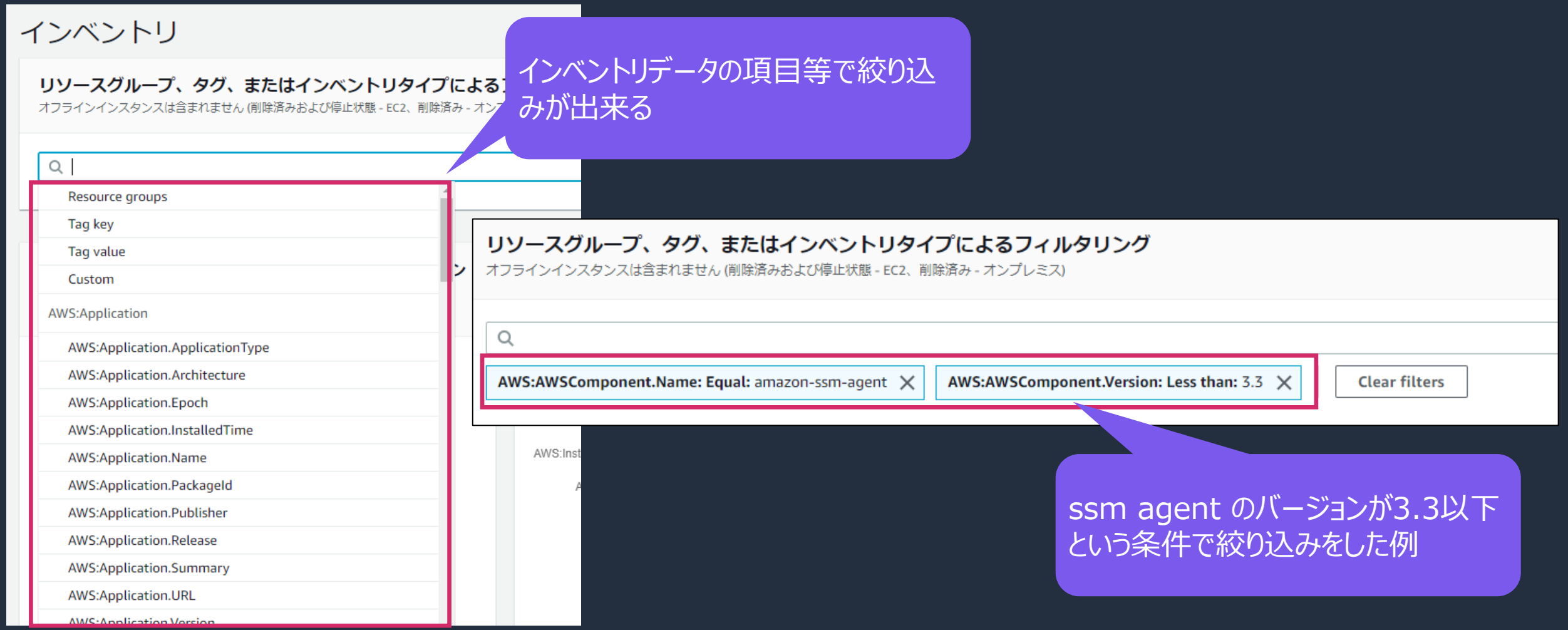
ノードの詳細ページに遷移し、インベントリタブを開く



ダッシュボード



インベントリデータのフィルタリング



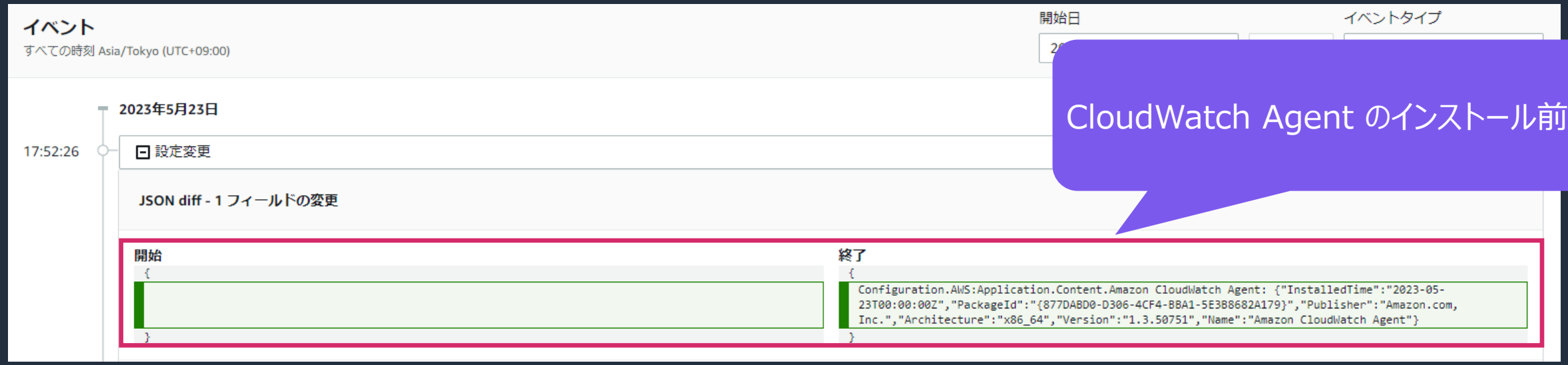
インベントリデータの項目等で絞り込みが出来る

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

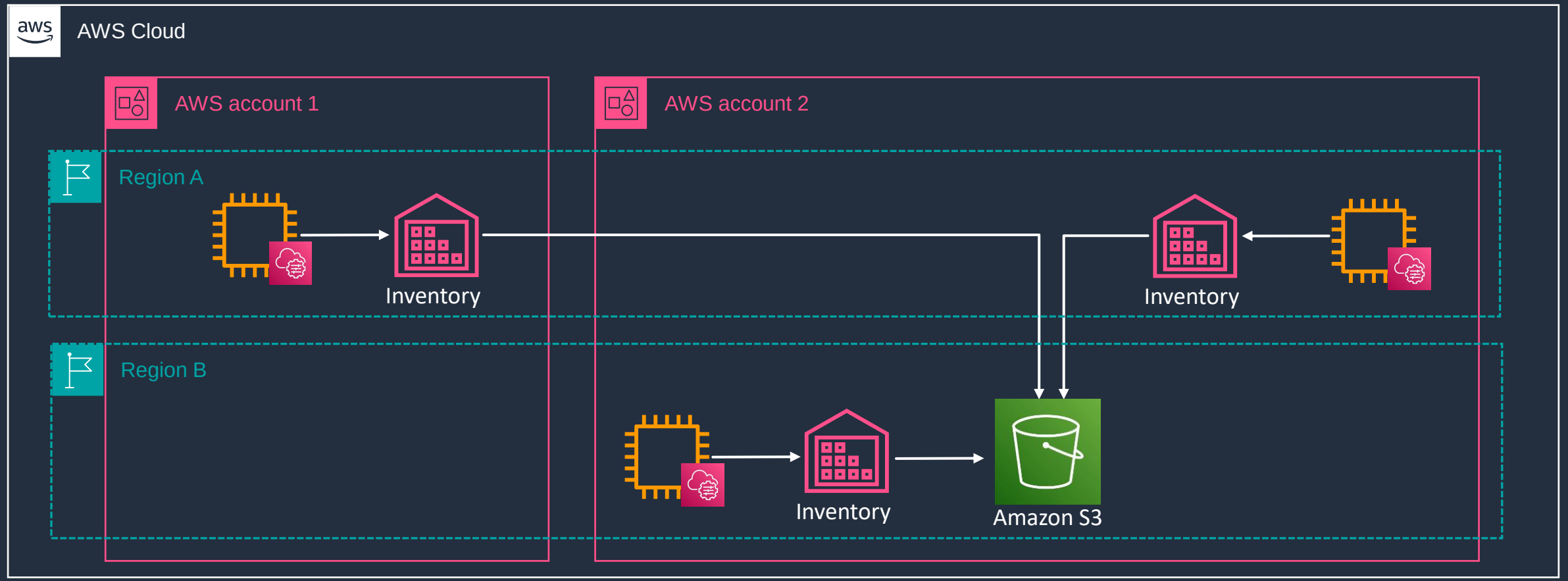
リソースタイプ	詳細
SSM:ManagedInstanceInventory	マネージドノードのインベントリデータ
SSM:PatchCompliance	Systems Manager Patch Managerでのパッチ適用状況
SSM:AssociationCompliance	Systems Manager State Manager の assciations(関連付け)の適用状況
SSM:FileData	サーバー内のファイル（Inventory でインベントリタイプ「AWS：File」を収集している場合 ）



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

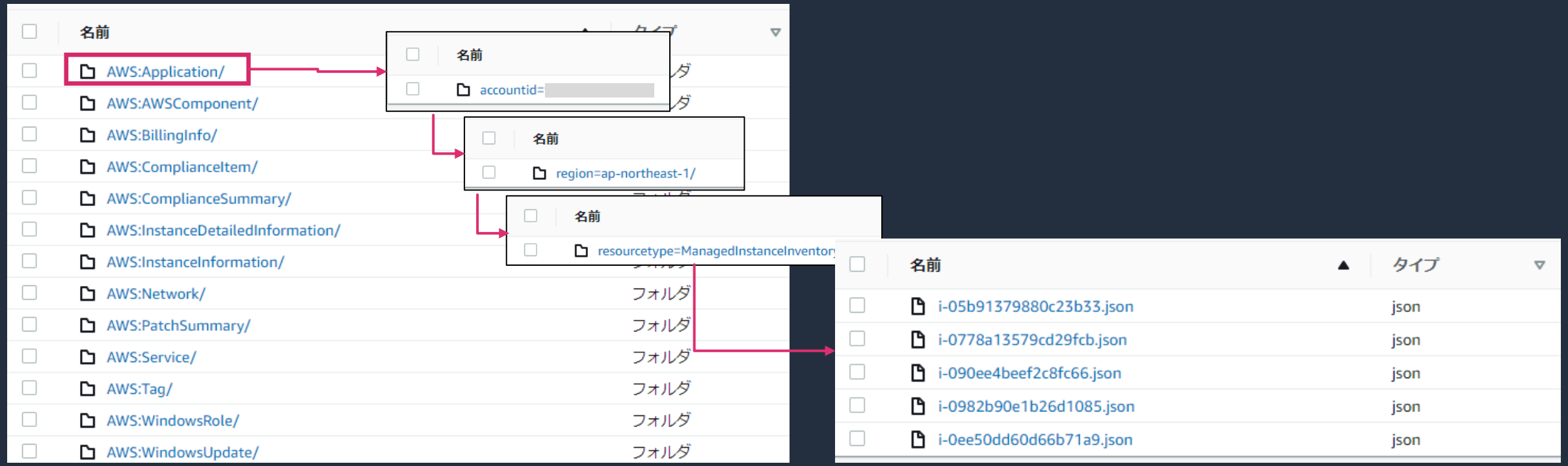
リソースデータ同期を使用して、リージョンおよび AWS アカウントを横断ですべてのマネージドノードから収集されたインベントリデータを、1 つの Amazon S3 バケットに送信できます。



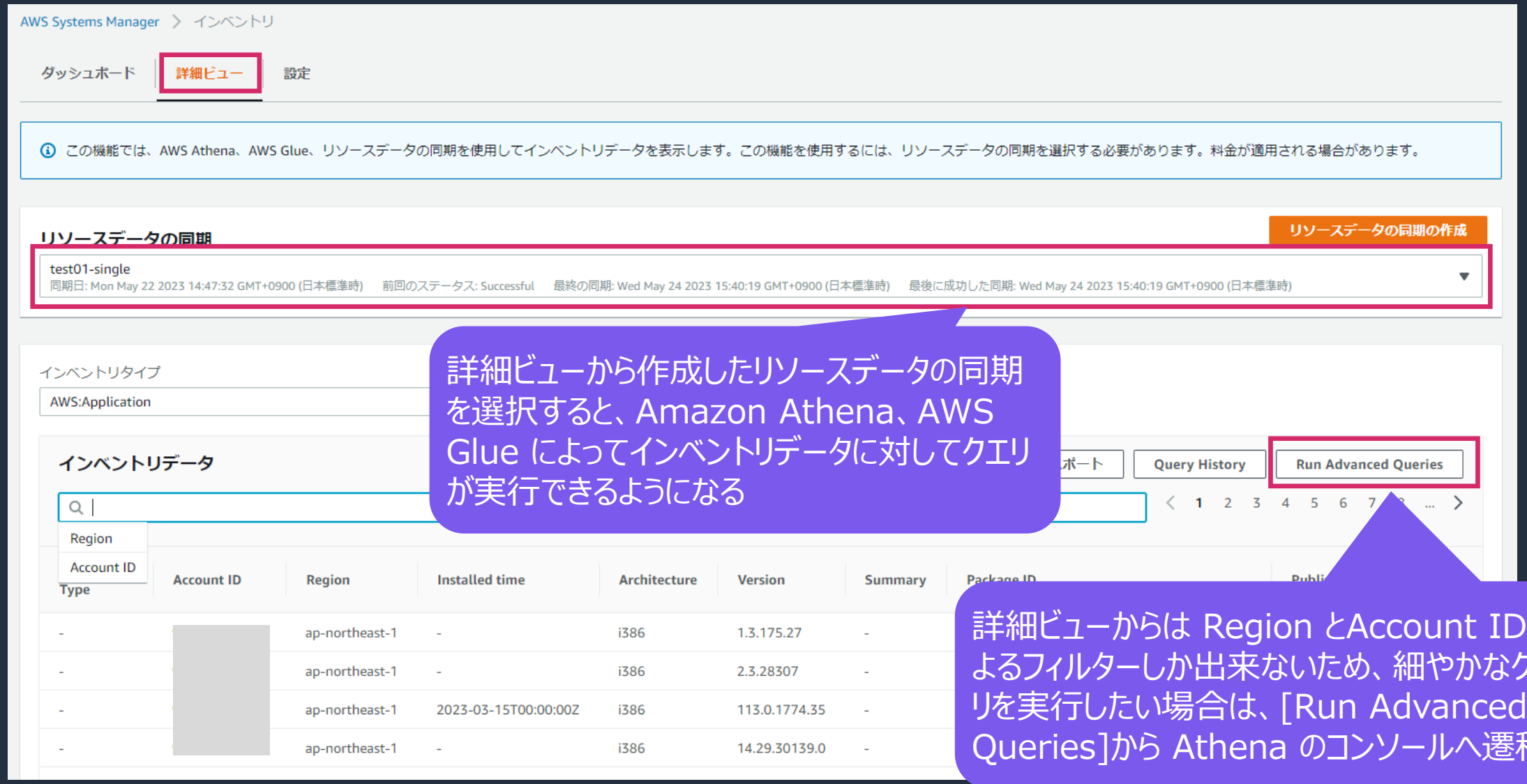
リソースデータの同期 2/3

同期タイミング
新しいイン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



Inventory 応用編

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/*node-id*/inventory/custom
macOS	/opt/aws/ssm/data/*node-id*/inventory/custom
Windows	%SystemDrive%¥ProgramData¥Amazon¥SSM¥InstanceData¥*node-id*¥inventory¥custom

JSON ファイルの例

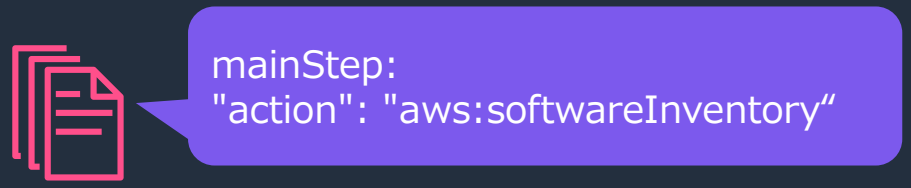
```
{
   "SchemaVersion": "1.0",
   "TypeName": "Custom:RackInformation",
   "Content": {
      "Location": "US-EAST-02.CMH.RACK1",
      "InstalledTime": "2016-01-01T01:01:01Z",
      "vendor": "DELL",
      "Zone" : "BJS12",
      "TimeZone": "UTC-8"
    }
}
```

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)



カスタムインベントリ用ドキュメント

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

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

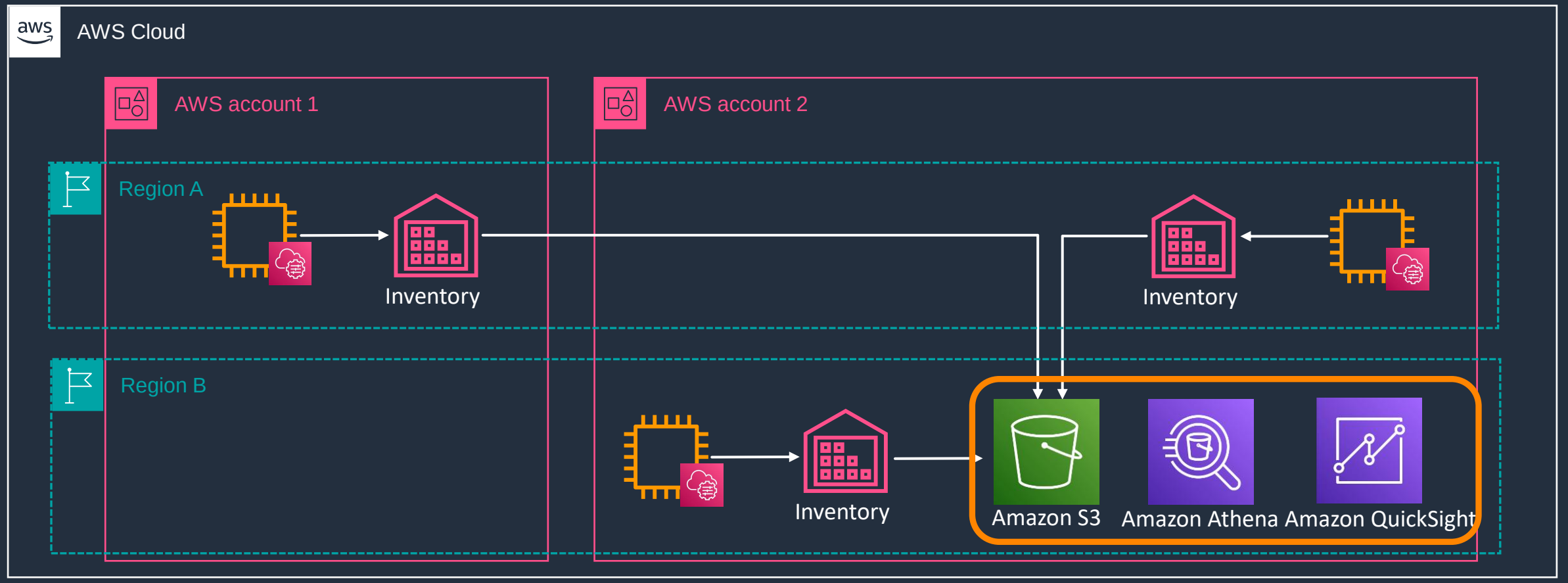
リソースデータの同期を作成する API で DestinationDataSharingType=Organization を指定して各リージョン、アカウントで実行

- 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

※Quick Setup ホスト管理
https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/quick-setup-host-management.html

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!