



AWS Systems Manager

Hybrid Activations 編

AWS Black Belt Online Seminar

村田 京介

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=PLzWGOASvSx6FlwIC2X1nObr1KcMCBBlqY>

内容についての注意点

- ・ 本資料では 2023 年 5 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

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 Hybrid Activations の機能とユースケースをご理解いただく。

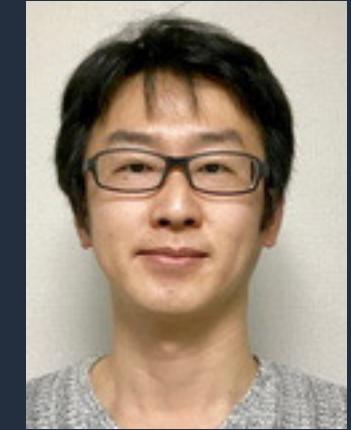
本日お話ししないこと

- AWS Systems Manager の全体的な説明
→ [AWS Systems Manager Overview](#) を参照ください
- AWS Systems Manager Hybrid Activations 以外の機能の詳細
→ [AWS サービス別資料](#)より各機能にフォーカスしたセッションをご参照ください。
検索結果に表示されない機能については今後公開予定です。

自己紹介

名前：村田 京介 (Kyosuke Murata)

所属：技術統括本部 エンタープライズ技術本部
サービスソリューション部



経歴：

ソフトウェアベンダーのコンサルタントを経て、
現在はソリューションアーキテクトとしてエンタープライズのお客様を担当

好きな AWS サービス： AWS Systems Manager



AWS Chatbot



アジェンダ

1. AWS Systems Manager (SSM) の概要
2. EC2 インスタンス以外を SSM で管理するには？
3. 具体的な構成手順とデモ
4. SSM Hybrid Activations の料金
5. まとめ

AWS Systems Manager (SSM) の概要



AWS Systems Manager (SSM)

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



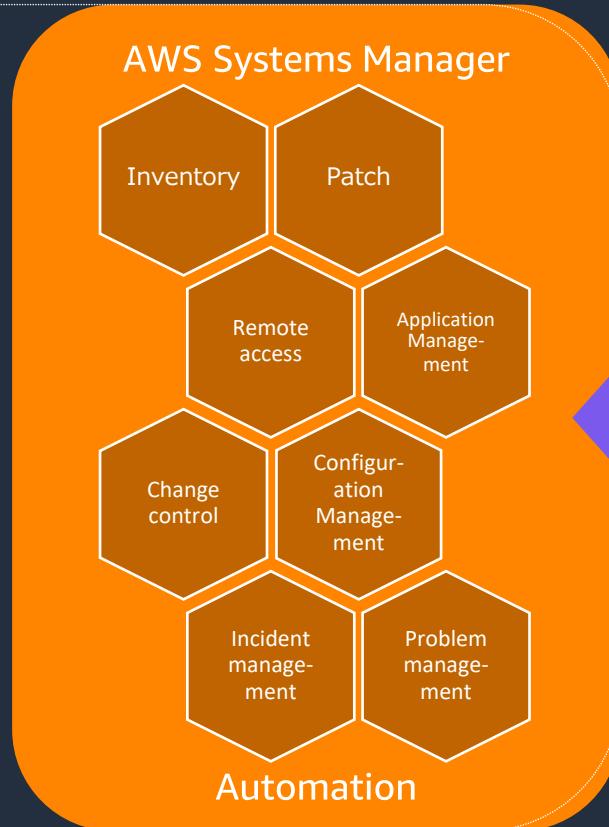
AWS CloudTrail

Audited actions



AWS Identity and Access Management (IAM)

Role-based access control



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

SSM の機能



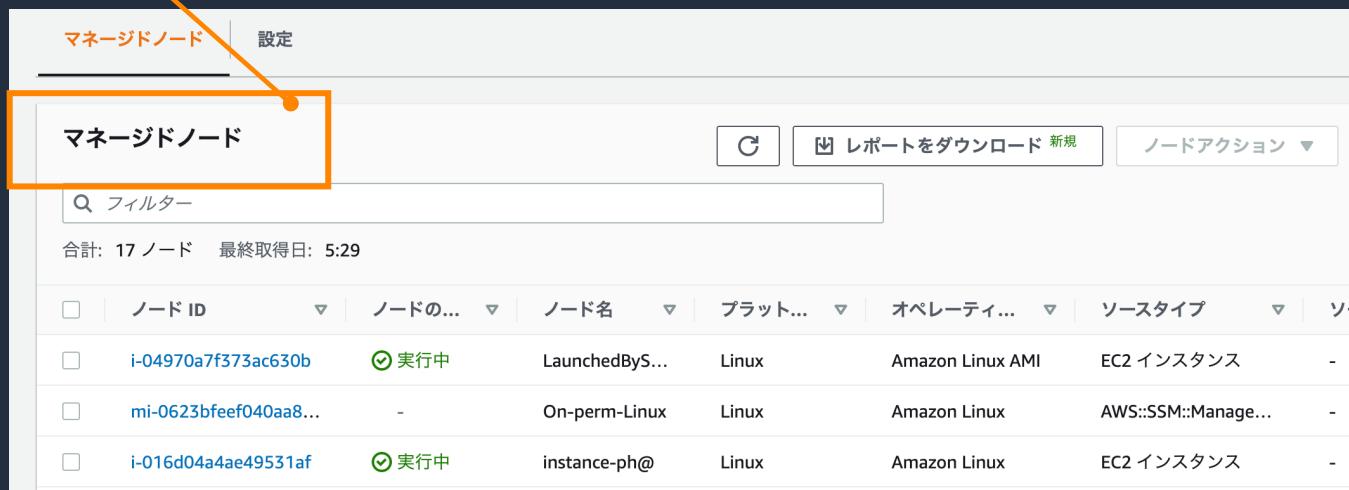
EC2 インスタンス以外を SSM で管理するには？



SSM を使って管理を行うためには

“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



The screenshot shows the AWS Systems Manager Managed Nodes console. At the top, there are two tabs: "マネージドノード" (selected) and "設定". Below the tabs is a search bar labeled "フィルター" and a status message "合計: 17 ノード 最終取得日: 5:29". To the right of the search bar are three buttons: "C" (refresh), "レポートをダウンロード" (download report), and "ノードアクション" (node actions). The main area is a table with columns: "ノード ID", "ノードの...", "ノード名", "プラット...", "オペレーター...", "ソースタイプ", and "ソースアーティ...", which is partially cut off. Three rows of data are visible:

ノード ID	ノードの...	ノード名	プラット...	オペレーター...	ソースタイプ	ソースアーティ...
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、
オンプレミスのサーバも
含まれられる。

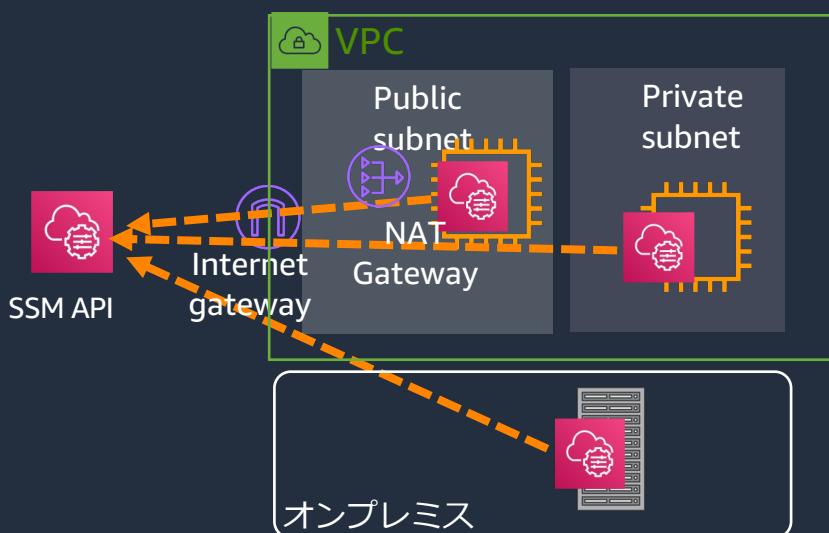
SSM でサポートされている EC2 以外のマシンタイプ

- オンプレミスサーバ
- 他のクラウド環境およびオンプレミスの仮想マシン
- エッジデバイス

① アウトバウンド経路の確保

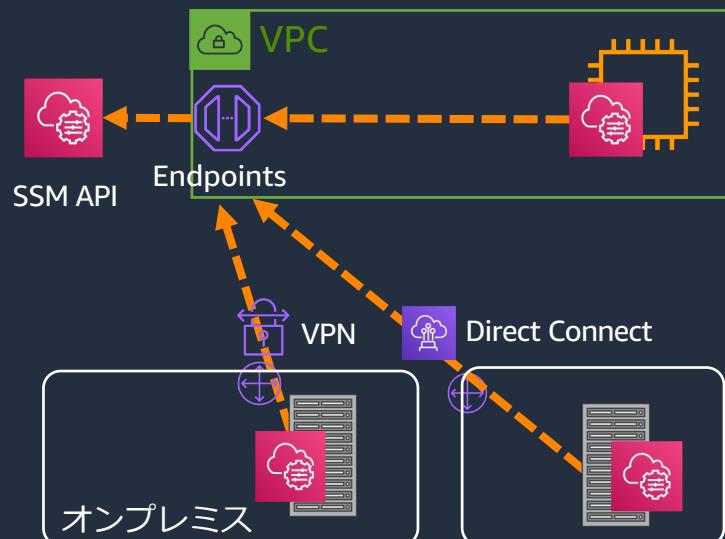
- 以下のいずれかのパターンで、SSM Agent からの HTTPS のアウトバウンド経路を確保
- インバウンドアクセスは不要

1. インターネット経由



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



② IAM サービスロールの作成

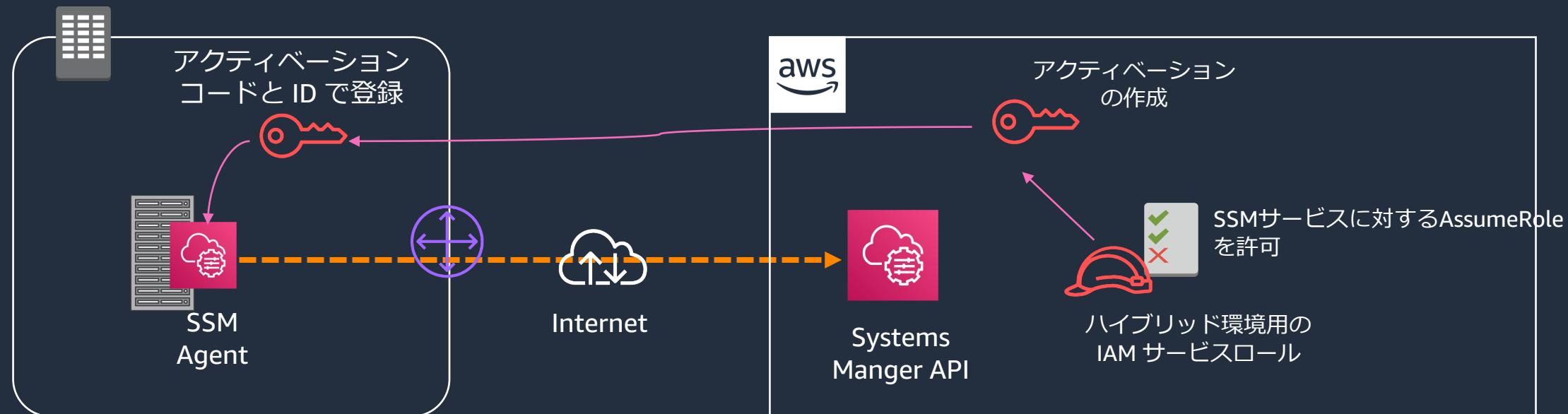
- マネージドノードが SSM と通信するために IAM サービスロールを作成
 1. 信頼できるエンティティに「Systems Manager」を選択 (必須)
 2. IAM ポリシーについては、まず「AmazonSSMManagedInstanceCore」でコア機能をアタッチ (必須)
 3. S3 などのポリシーをアタッチ (オプション)

IAM サービスロール作成の詳細は[こちら](#)

③ アクティベーション作成

1. アクティベーションコードとアクティベーション ID を生成
2. ハイブリッドノード(※)登録時に生成されたアクティベーションコードとアクティベーション ID を利用

※ ハイブリッドノードとは、オンプレミスサーバ、エッジデバイス、仮想マシンのことを指します。



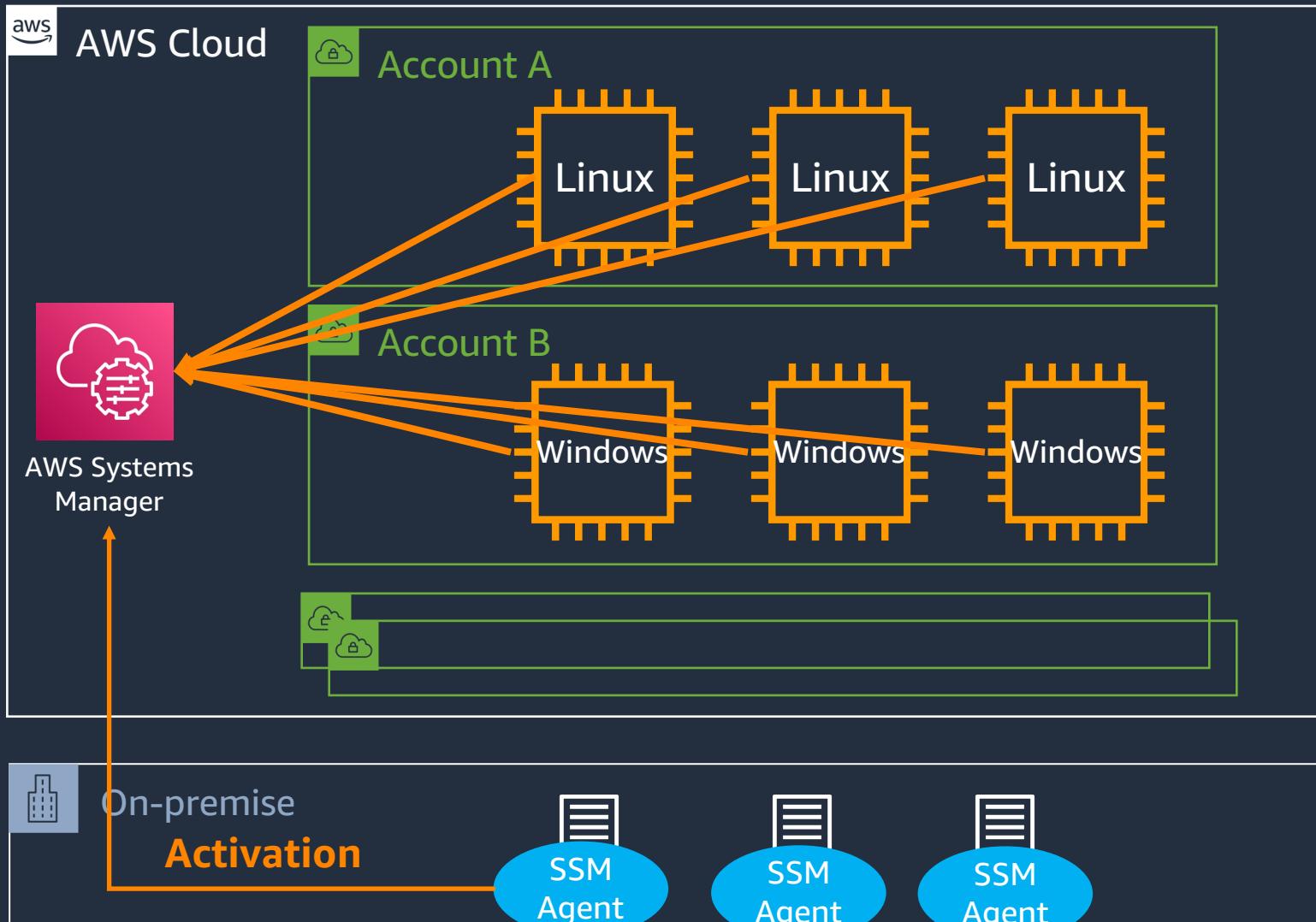
④ SSM Agent のインストールと登録

- ハイブリッドノードは、手動で SSM Agent をインストールし、マネージドノードとして SSM に登録する。

Linuxへのインストール手順は[こちら](#)、Windowsのインストール手順は[こちら](#)

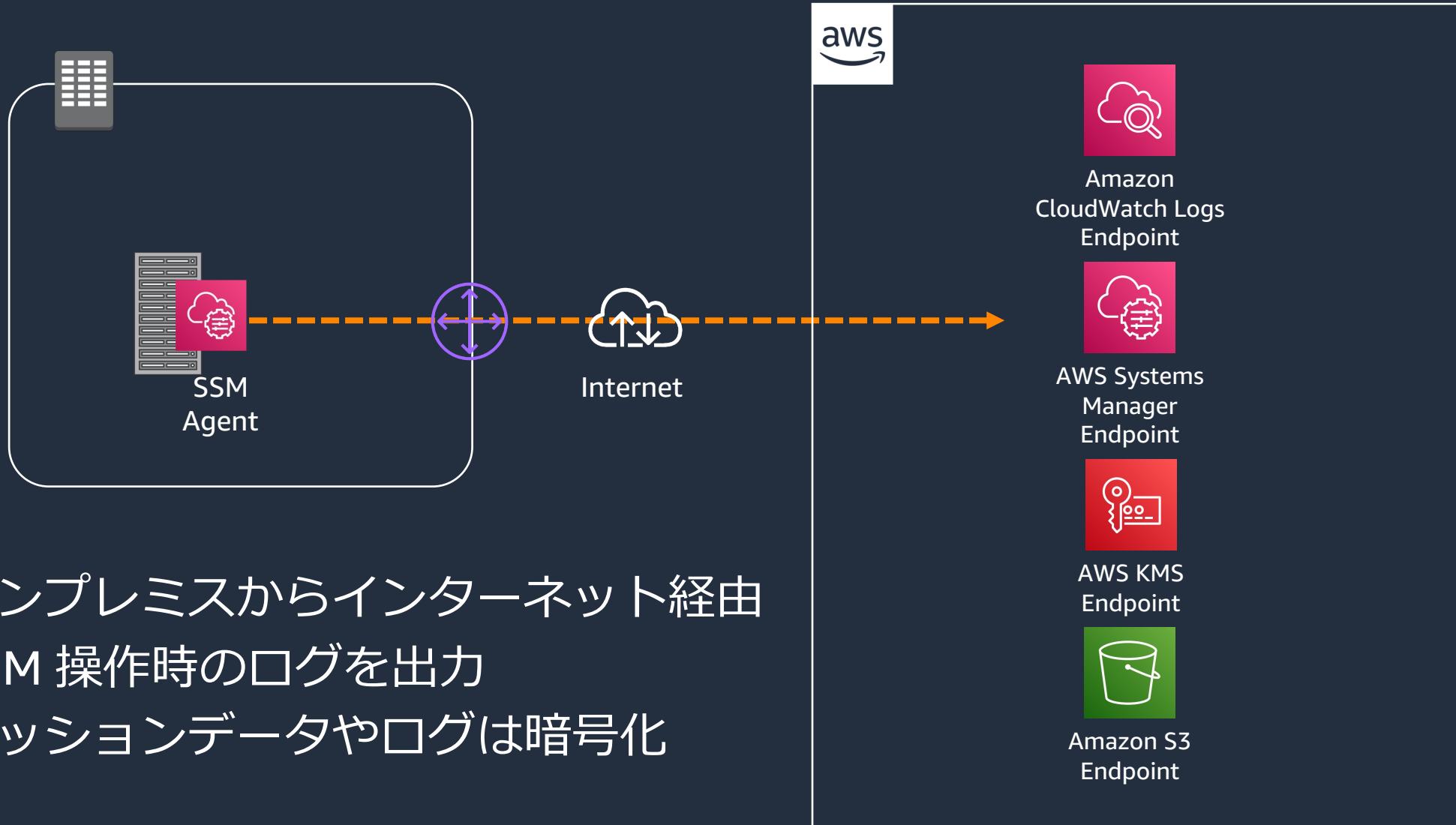


ここまでやれば、晴れてマネージドノードに！



具体的な構成手順とデモ

前提



- オンプレミスからインターネット経由
- SSM 操作時のログを出力
- セッションデータやログは暗号化

【ご参考】閉域網での構成例

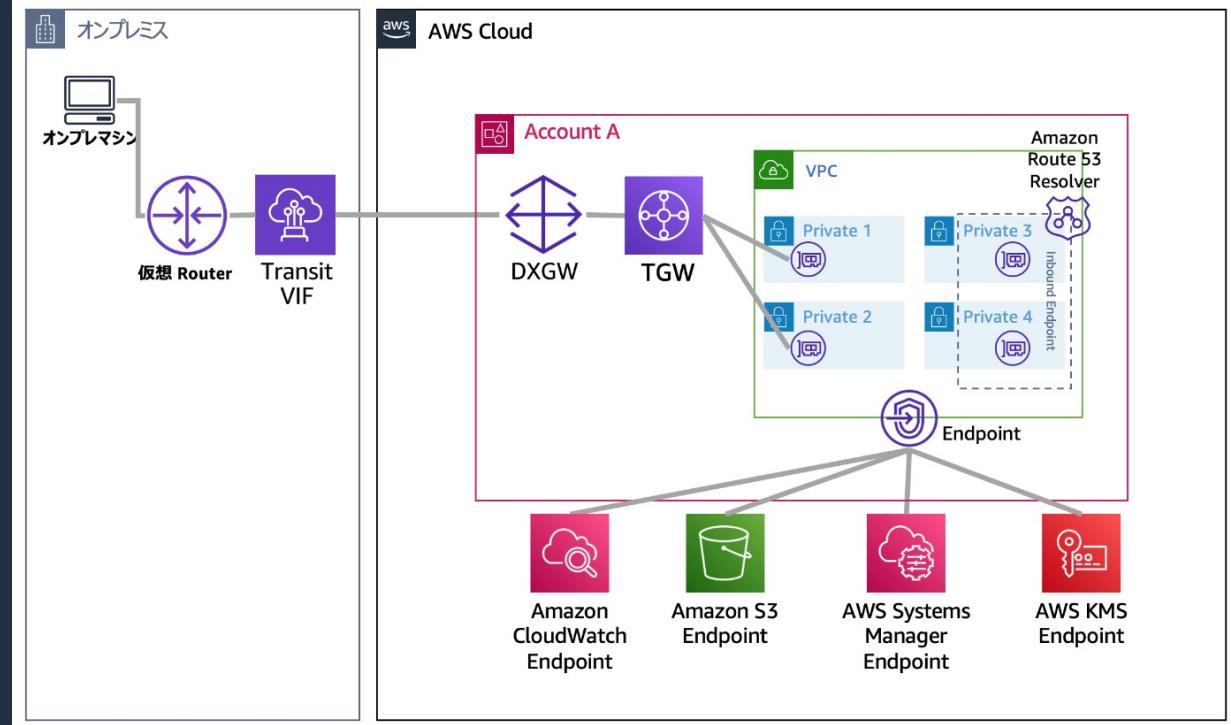
Amazon Web Services ブログ

ハイブリッド環境の運用・監視の実現 – 閉域網で AWS Systems Manager と Amazon CloudWatch を構成する

by Kyosuke Murata | on 26 7月 2022 | in [Amazon CloudWatch](#), [AWS Systems Manager](#), [Hybrid Cloud Management](#), [Management & Governance](#) | [Permalink](#) | [Share](#)

こんにちは。ソリューションアーキテクトの村田と申します。

昨今オンプレミスとクラウドを併用した環境が多く、運用・監視の仕組みを集約したいと考えたことはないでしょうか。私がソリューションアーキテクトとして仕事をさせて頂く中で、オンプレミスサーバを AWS の仕組みで運用・監視する場合の構成方法についてお客様からご相談頂くことがあります。オンプレミスと AWS は閉域網で接続したいというご要望を頂くことがあります。2022年7月時点できました情報が公開されていないため、このブログでは閉域接続のオンプレミスサーバを [AWS Systems Manager](#) と [Amazon CloudWatch](#) で運用・監視するための構成方法について詳しくご紹介します。



閉域網での構成例について記載したブログは[こちら](#)

手順 1. インターネットへの疎通確認

Ubuntu Server 20.04 LTS の場合

インターネット向けの HTTPS アクセスができることの確認

```
$ curl https://checkip.amazonaws.com/
```

SSM の各種エンドポイントと通信プロトコルについては[こちら](#)

手順 2-1. IAM サービスロールの作成

IAM > ロール > ロールを作成

ステップ 1
信頼されたエンティティを選択

ステップ 2
許可を追加

ステップ 3
名前、確認、および作成

信頼されたエンティティを選択 情報

信頼されたエンティティタイプ

- AWS のサービス
EC2、Lambda、その他の AWS サービスが、このアカウントでアクションを実行することを許可します。
- AWS アカウント
お客様またはサードパーティに属する他の AWS アカウントのエンティティが、このアカウントでアクションを実行することを許可します。
- ウェブアイデンティティ
指定された外部ウェブアイデンティティ プロバイダーによってフェデレーションされたユーザーが、このロールを引き受け、このアカウントでアクションを実行することを許可します。
- SAML 2.0 フェデレーション
会社のディレクトリから SAML 2.0 を使用してフェデレーションされたユーザーが、このアカウントでアクションを実行することを許可します。
- カスタム信頼ポリシー
カスタム信頼ポリシーを作成して、他のユーザーがこのアカウントでアクションを実行できるようにします。

ユースケース

EC2、Lambda、その他の AWS のサービスがこのアカウントでアクションを実行することを許可します。

一般的なユースケース

- EC2
Allows EC2 instances to call AWS services on your behalf.
- Lambda
Allows Lambda functions to call AWS services on your behalf.

他の AWS のサービスのユースケース:

- Systems Manager
- Systems Manager
Allows SSM to call AWS services on your behalf
- Systems Manager - Inventory and Maintenance Windows
Allow AWS Systems Manager to call AWS resources on your behalf.

キャンセル 次へ

手順 2-2. IAM サービスロールの作成

The screenshot shows the AWS IAM service role configuration page. At the top, it displays the ARN: arn:aws:iam::[REDACTED]:role/BB_Hybrid_Activation and the maximum session duration: 1 hour. Below this, there are tabs for Permissions, Trust Relationships, Tags, Access Advisor, and Session Token Refresh. The Permissions tab is selected, showing four attached policies: CloudWatchAgentServerPolicy, AmazonSSMManagedInstanceCore, bb_hybrid_activations_kms, and bb_hybrid_activations_s3_access. The last two policies are highlighted with an orange border.

Amazon CloudWatch Logs へのセッションデータのログ記録と暗号化については[こちら](#)

Amazon S3 へのセッションデータをログ記録と暗号化については[こちら](#)

Session Manager のセッションデータ暗号化については[こちら](#)

Session Manager、S3 や CloudWatch Logs の暗号化を利用する場合、適したポリシーを IAM サービスロールにアタッチする必要があります。

今回の構成では、セッションデータやログの暗号化を行っています。

手順 3-1. アクティベーションの作成

The screenshot shows the AWS Systems Manager console. On the left, there's a sidebar with navigation links for Change Management and Node Management, with 'Hybrid Applications' highlighted in orange. The main content area has a title 'AWS Systems Manager のアクティベーション ハイブリッド環境の一元管理' and a description about registering on-premises servers or devices. A prominent orange button labeled 'アクティベーションを作成する' is highlighted with a red border.

▼ 変更管理

Change Manager
オートメーション
Change Calendar
メンテナンスウィンドウ

▼ ノード管理

フリートマネージャー
コンプライアンス
インベントリ
ハイブリッドアクティベーション

マネジメント

AWS Systems Manager のアクティベーション ハイブリッド環境の一元管理

オンプレミスのサーバーまたはデバイスの登録

アクティベーションを作成する

手順 3-2. アクティベーションの作成

AWS Systems Manager > アクティベーション > アクティベーションの作成

アクティベーションの作成

アクティベーション設定
新しいアクティベーションを作成します。アクティベーションの完了後、アクティベーションコードと ID が送信されます。このコードと ID を使用して SSM エージェントをハイブリッドおよびオンプレミスのサーバー、または仮想マシンに登録してください。[詳細情報はこちらをご覧ください](#)

アクティベーションの説明- オプション
最大 256 文字です。

インスタンス制限
AWS に登録するサーバーと VM の合計数を指定します。
1

IAM ロール
マネージドインスタンス上の SSM エージェントと AWS の間での通信を有効にするには、IAM ロールを指定します
 システムによって作成されたデフォルトのロール (AmazonEC2RunCommandRoleForManagedInstances) を使用する
 必要な許可を持つ既存のカスタム IAM ロールを選択する

① このオプションを選択すると、AWS はユーザーが指定している既存のロールを使用します。ロールには必要な許可を持たせておく必要があります。許可がない場合、コマンドの実行に失敗します。[詳細情報はこちらをご覧ください](#)

BB_Hybrid_Activation

アクティベーションの有効期限
この日付はアクティベーションの有効期限が切れる日付を指定します。有効期限日後に追加のマネージドインスタンスを登録したい場合は、新しいアクティベーションを作成する必要があります。この有効期限日は、既に登録済みで実行中のインスタンスには影響しません。
2023-04-27T12:00+09:00

有効期限日は、今日から 30 日以内の日付に設定してください

デフォルトのインスタンス名- オプション
このマネージドインスタンスがコントロールされるとき、または List API を呼び出すときに、このマネージドインスタンスの特定に役立つ名前を指定します。
最大 256 文字です。

キャンセル アクティベーションの作成

設定項目	内容
アクティベーションの説明 (オプション)	このアクティベーションの説明を入力
インスタンス制限	このアクティベーションで登録するノードの合計数 ※ デフォルト値は 1 インスタンス
IAM ロール	事前に作成した IAM サービスロールを選択 ※ デフォルトはシステムによって作成されたデフォルトのロール
アクティベーション有効期限	アクティベーションが期限切れになる時間を指定 (例 : 2023-04-27T12:00+09:00) ※ 有効期限は将来の日付で 30 日以内で入力、デフォルト値は 24 時間
デフォルトのインスタンス名 (オプション)	このアクティベーションで関連付けられる全てのノードに表示する識別名 (ノード名に表示される。指定しないと “-” となる。)

② 新しいアクティベーションが正常に作成されました。アクティベーションコードを以下に記載します。このコードに再度アクセスすることはできないため、コードをコピーして安全な場所に保存してください。

Activation Code



Activation ID 255996e5-f42d-44c8-8fb8-eb17f76696bc

これで、amazon-ssm-agent をインストールして、Run Command でインスタンスを管理できるようになりました。 [詳細情報はこちらをご覧ください](#)

手順 4. SSM Agent インストール

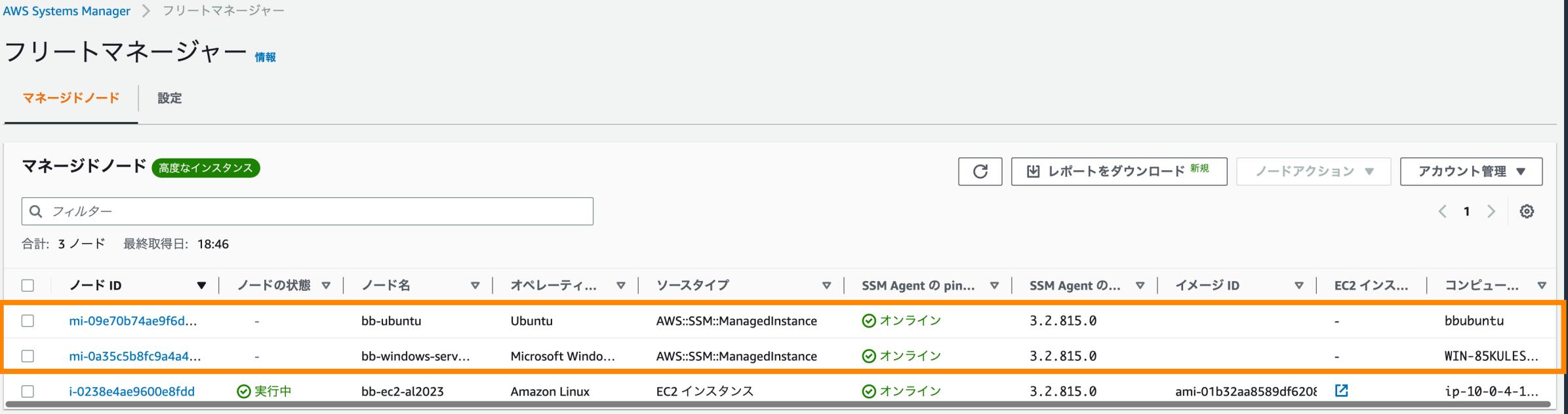
Ubuntu Server 20.04 LTS の場合 (.deb パッケージ使用)

```
$ mkdir /tmp/ssm  
  
$ curl https://s3.amazonaws.com/ec2-downloads-  
windows/SSMAgent/latest/debian_amd64/amazon-ssm-agent.deb -o /tmp/ssm/amazon-  
ssm-agent.deb  
  
$ sudo dpkg -i /tmp/ssm/amazon-ssm-agent.deb  
  
$ sudo service amazon-ssm-agent stop  
  
$ sudo -E amazon-ssm-agent -register -code "activation-code" -id "activation-id" -region  
"region"  
  
$ sudo service amazon-ssm-agent start
```

※ Linuxへのインストール手順は[こちら](#)、Windowsのインストール手順は[こちら](#)



晴れてマネージドノードに



The screenshot shows the AWS Systems Manager Fleet Manager interface. The top navigation bar includes 'AWS Systems Manager' and 'フリートマネージャー'. Below it, the title 'フリートマネージャー' has a '情報' link. The main section is titled 'マネージドノード' with a '高度なインスタンス' button. The table lists three nodes:

ノード ID	ノードの状態	ノード名	オペレーティ...	ソースタイプ	SSM Agent の pin...	SSM Agent の...	イメージ ID	EC2 インス...	コンピュー...
mi-09e70b74ae9f6d...	-	bb-ubuntu	Ubuntu	AWS::SSM::ManagedInstance	オンライン	3.2.815.0	-	-	bbubuntu
mi-0a35c5b8fc9a4a4...	-	bb-windows-serv...	Microsoft Windo...	AWS::SSM::ManagedInstance	オンライン	3.2.815.0	-	-	WIN-85KULES...
i-0238e4ae9600e8fdd	実行中	bb-ec2-al2023	Amazon Linux	EC2 インスタンス	オンライン	3.2.815.0	ami-01b32aa8589df620e	ip-10-0-4-1...	

- ハイブリッドノードの Fleet Manager への表示のされ方
 - ノード ID は “mi-” から始まる
 - ソースタイプは “AWS::SSM::ManagedInstance”
 - ノード名の列は “アクティベーション時の入力値” (ホスト名はコンピュータ名の列)

手順 5. インスタンス枠を変更（オプション）



- 以下のシナリオではアドバンスドティアのアクティブ化が必要（追加料金が発生）
 - アカウント毎にリージョンあたり 1,000 を越えるハイブリッドノード（オンプレミスサーバ、エッジデバイス、仮想マシン）を登録
 - ハイブリッドノードに接続するために Session Manager を使用
 - ハイブリッドノードで Microsoft がリリースしたアプリケーション（OS 以外）にパッチを適用

手順 5. インスタンス枠を変更（オプション）



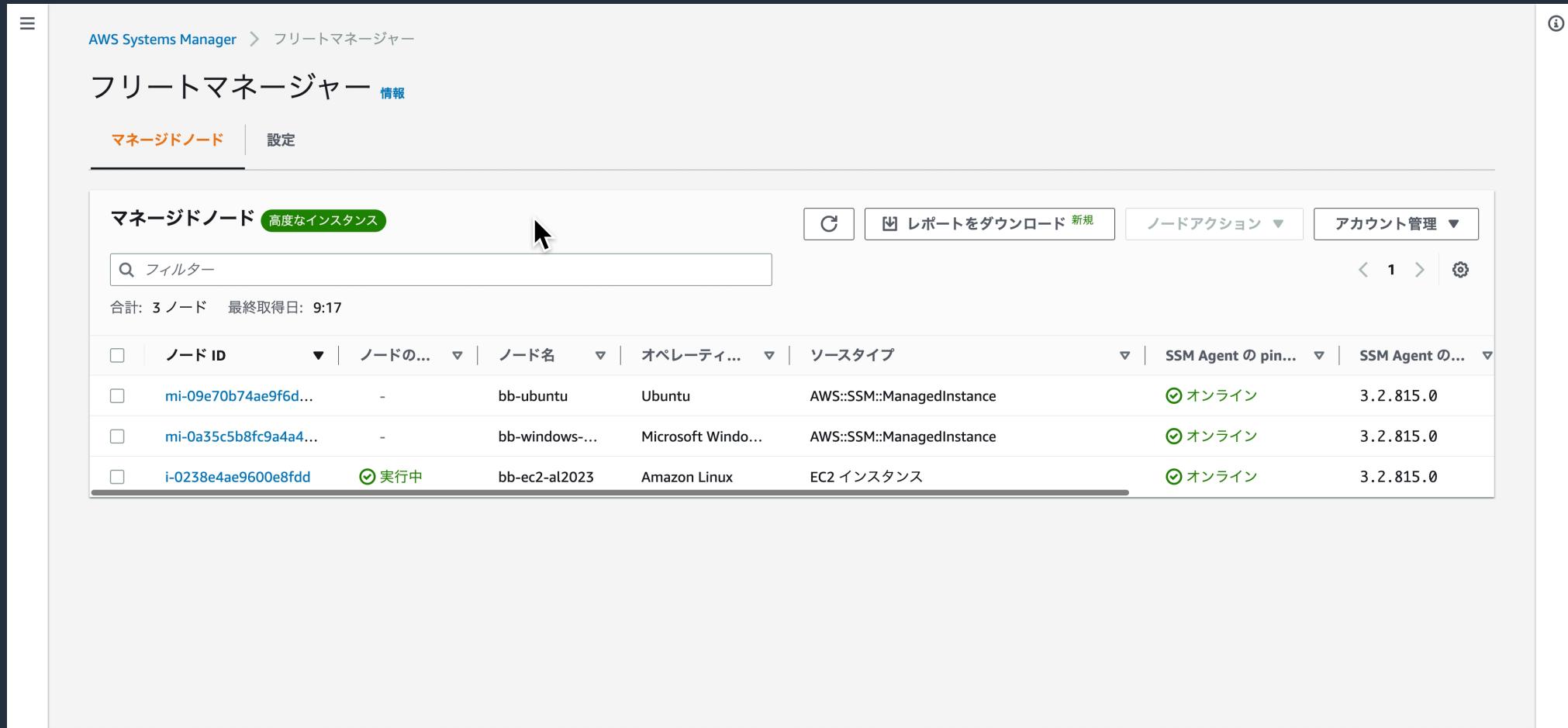
- 以下のシナリオではアドバンスドティアのアクティブ化が必要（追加料金が発生）
 - アカウント毎にリージョンあたり 1,000 を越えるハイブリッドノード（オンプレミスサーバ、エッジデバイス、仮想マシン）を登録
 - ハイブリッドノードに接続するために Session Manager を使用
 - ハイブリッドノードで Microsoft がリリースしたアプリケーション（OS 以外）にパッチを適用

手順 5. インスタンス枠を変更（オプション）

The screenshot shows the AWS Systems Manager Fleet Manager interface. On the left, there's a sidebar with 'AWS Systems Manager > フリートマネージャー' and tabs for 'マネージドノード' (selected) and '設定'. The main area has a title '標準層から高度な層への変更を確認' (Confirm migration from standard layer to advanced layer). It contains text about the action changing instance types to advanced ones, mentioning session manager and EC2 instances, and a note about regional limits. A checkbox is checked for 'アカウントとリージョン内のすべてのオンプレミスのインスタンス (または Systems Manager Session Manager を使用する Amazon EC2 インスタンス) を高度なインスタンスに変更する' (Change all on-premises instances (or Amazon EC2 instances using Systems Manager Session Manager) in the account and region to advanced instances). The '高度なインスタンス' button in the 'マネージドノード' tab is highlighted with an orange box.

- 以下のシナリオではアドバンスドティアのアクティブ化が必要（追加料金が発生）
 - アカウント毎にリージョンあたり 1,000 を越えるハイブリッドノード（オンプレミスサーバ、エッジデバイス、仮想マシン）を登録
 - ハイブリッドノードに接続するために Session Manager を使用
 - ハイブリッドノードで Microsoft がリリースしたアプリケーション（OS 以外）にパッチを適用

デモ 1



The screenshot shows the AWS Systems Manager Fleet Manager interface. The top navigation bar includes the AWS logo, account information, and a search bar. The main header reads "AWS Systems Manager > フリートマネージャー". Below it, the title "フリートマネージャー" has a "情報" link. The left sidebar has two tabs: "マネージドノード" (selected) and "設定". The main content area is titled "マネージドノード [高度なインスタンス]" and contains a table of managed nodes. The table columns are: ノード ID, ノードの状態, ノード名, オペレーティングシステム, ソースタイプ, SSM Agent の ping 状況, and SSM Agent のバージョン. There are 3 nodes listed:

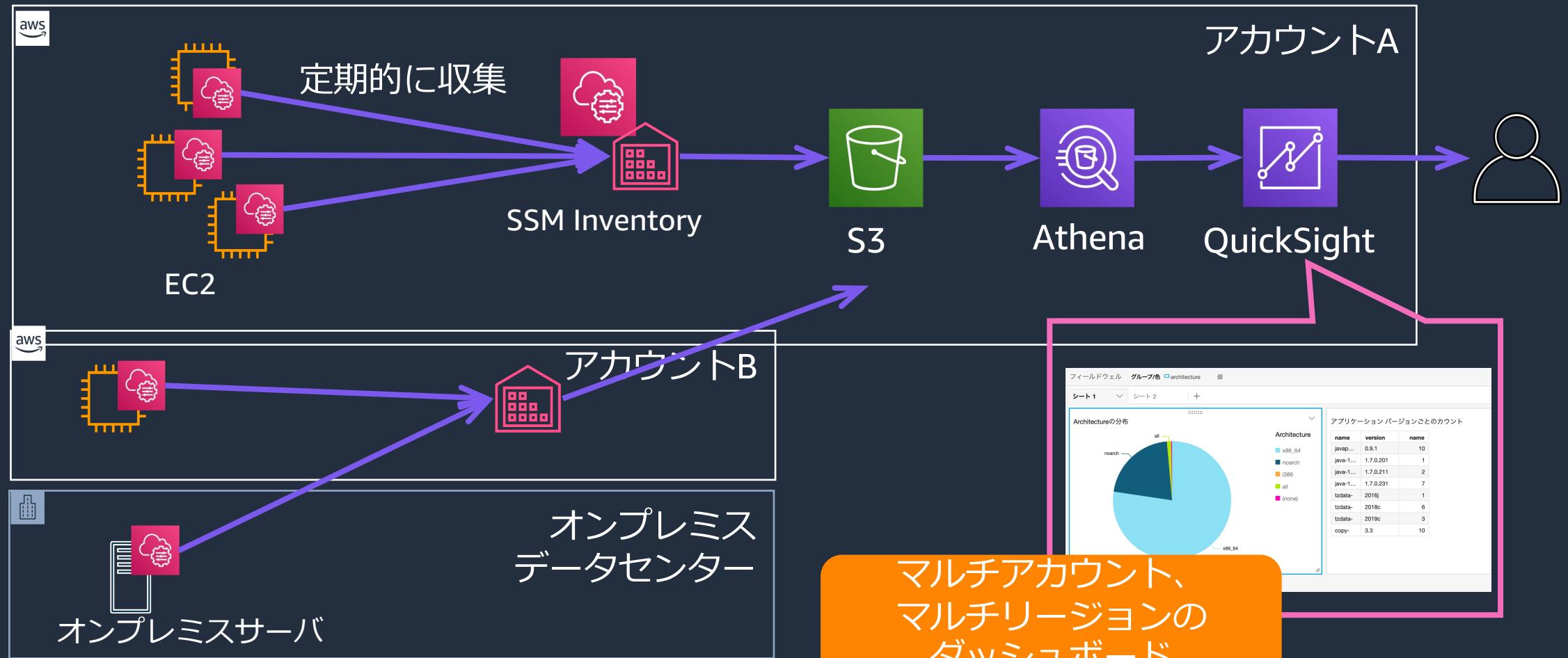
ノード ID	ノードの状態	ノード名	オペレーティングシステム	ソースタイプ	SSM Agent の ping 状況	SSM Agent のバージョン
mi-09e70b74ae9f6d...	-	bb-ubuntu	Ubuntu	AWS::SSM::ManagedInstance	オンライン	3.2.815.0
mi-0a35c5b8fc9a4a4...	-	bb-windows-...	Microsoft Windo...	AWS::SSM::ManagedInstance	オンライン	3.2.815.0
i-0238e4ae9600e8fdd	実行中	bb-ec2-al2023	Amazon Linux	EC2 インスタンス	オンライン	3.2.815.0

デモ 2

The screenshot shows the AWS Systems Manager Run Command page. At the top, there are tabs for 'コマンド' (Command) and 'コマンド履歴' (Command History), with 'コマンド' being the active tab. Below the tabs is a search bar and a row of buttons: 'C' (Cancel), '詳細の表示' (View details), 'コマンドのキャンセル' (Cancel command), 'コマンドの再実行' (Re-run command), 'Copy to new' (Copy to new), and 'Run command' (highlighted in orange). A navigation bar below the buttons shows the current page is '1' of 1.

コマンド ID	ステータス	リクエストされた日付	ドキュメント名	コメント	ターゲット数	エラー数
6a82c62a-e3ea-4a38-925a-71ef9518080b	① 進行中	Mon, 29 May 2023 12:17:44 GMT	AmazonInspector2-ConfigureInspectorSsmPlugin	a3b32cc3-88fe-4bcf-9c75-83f6d210cfe9:df87473b-b02a-4932-8623-53ecf03ad6d7	1	0
7df719b3-c952-4d1a-a5a8-758ed5b3c567	① 進行中	Mon, 29 May 2023 12:17:44 GMT	AmazonInspector2-InvokeInspectorSsmPlugin	b8ffce21-2d33-453d-8483-98f99b71555b:e63cee71-b924-451e-9aa8-574630bffda1	1	0

【ご参考】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

「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」

SSM Hybrid Activations の料金

Hybrid Activations の料金

- アカウント毎にリージョンあたり 1,000 のハイブリッドノード（オンプレミスサーバ、エッジデバイス、仮想マシン）を追加料金なしで登録可能
- 以下のシナリオではアドバンスドティアのアクティブ化が必要（追加料金が発生）
 - 1,000 を越えるハイブリッドノードを登録
 - ハイブリッドノードに接続するために Session Manager を使用
 - ハイブリッドノードで Microsoft がリリースしたアプリケーション（OS 以外）にパッチを適用

インスタンスティア	料金
スタンダード	追加料金無し アカウントごとにリージョンあたり最大 1,000 までの制限
アドバンスド	Systems Manager Hybrid Activations を使用して登録されたノードごとに時間あたり 0.00695 USD 無料利用枠なし

【参考】

インスタンス層の設定

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/systems-manager-managed-instances-tiers.html

AWS Systems Manager の料金

<https://aws.amazon.com/jp/systems-manager/pricing/>



計算例

アカウント A でインスタンスティアをスタンダードで 500 のオンプレミスサーバを登録、
アカウント B でインスタンスティアをアドバンスドで 1,500 のオンプレミスサーバを登録し、
10 日間経過しているとします。

アカウント	インスタンスティア	管理台数	料金
A	スタンダード	オンプレミス サーバ 500 台	請求無し
B	アドバンスド	オンプレミス サーバ 1,500 台	$1,500 \text{ (台)} * 0.00695 \text{ USD (/時間)} * 10 \text{ (日)} * 24 \text{ (時間)} = 2,502 \text{ USD}$

【参考】

AWS Systems Manager の料金

<https://aws.amazon.com/jp/systems-manager/pricing/>

まとめ



まとめ

- SSM は EC2 インスタンスはもちろん、ハイブリッドノード（AWS 以外の仮想マシン、オンプレミスサーバー、さらにはエッジデバイス）を管理可能
- アクティベーションは、ハイブリッドノードをマネージドノードとして登録する際に利用する機能

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!