aws

ユーザーガイド

Amazon Inspector Classic

Version Latest

Amazon Inspector Classic: ユーザーガイド

Table of Contents

..... ix
Amazon Inspector Classic とは 1
Amazon Inspector Classic のメリット 2
Amazon Inspector Classic の特徴 2
Amazon Inspector Classic へのアクセス 3
用語と概念 4
サービス制限 5
料金 7
ネットワーク到達可能性ルールパッケージの料金 7
ホスト評価ルールパッケージの料金 8
サポートされているオペレーティングシステムとリージョン 9
Amazon Inspector Classic エージェントでサポートされている Linux ベースのオペレーティングシステム 9
Amazon Inspector Classic エージェントでサポートされている Windows ベースのオペレーティングシステム 10
サポートしている AWS リージョン 10
Amazon Inspector Classic のサポート終了 12
ステップ 1: (オプション) 評価レポートと結果をエクスポートする 13
ステップ 2: Amazon Inspector Classic でスケジュールされた評価の実行をすべて削除する 14
ステップ 3: 新しい Amazon Inspector を有効にする 14
開始方法 15
にサインアップする AWS アカウント 15
ワンクリックでのセットアップ 15
詳細設定 16
チュートリアル 19
Amazon Inspector Classic チュートリアル - Red Hat Enterprise Linux 19
ステップ 1: Amazon Inspector Classic で使用する Amazon EC2 インスタンスをセットアップする 20
ステップ 2: Amazon EC2 インスタンスを変更する 20
ステップ 3: 評価ターゲットを作成して EC2 インスタンスにエージェントをインストールする 20
ステップ 4: 評価テンプレートを作成および実行する 22
ステップ 5: 結果を見つけて分析する 22
ステップ 6: 推奨される修正手順を評価ターゲットに適用する 24

Amazon Inspector Classic チュートリアル - Ubuntu Server 24
ステップ 1: Amazon Inspector Classic で使用する Amazon EC2 インスタンスをセットアップする 25
ステップ 2: 評価ターゲットを作成して EC2 インスタンスにエージェントをインストールする 25
ステップ 3: 評価テンプレートを作成および実行する 26
ステップ 4: 生成された結果を見つけて分析する 27
ステップ 5: 推奨される修正手順を評価ターゲットに適用する 28
セキュリティ 29
データ保護 30
保管中の暗号化 31
転送中の暗号化 31
Identity and Access Management 32
オーディエンス 32
アイデンティティを使用した認証 33
ポリシーを使用したアクセスの管理 34
Amazon Inspector Classic と IAM の連携 36
例 2: Amazon Inspector の検出結果に対する describe および list オペレーションのみの実行をユーザーに許可する 39
ポリシーリソース 40
ポリシー条件キー 40
ACL 41
ABAC 41
一時的な認証情報 42
プリンシパルアクセス権限 42
サービスロール 42
サービスリンクロール 42
アイデンティティベースのポリシーの例 43
サービスにリンクされたロールの使用 46
トラブルシューティング 49
ログ記録とモニタリング 51
インシデントへの対応 51
コンプライアンス検証 52
耐障害性 52
インフラストラクチャセキュリティ 53
設定と脆弱性の分析 54

セキュリティのベストプラクティス 54
Amazon Inspector Classic エージェント 55
Amazon Inspector Classic エージェントの権限 56
ネットワークと Amazon Inspector Classic エージェントのセキュリティ 56
Amazon Inspector Classic エージェントの更新 57
テレメトリデータのライフサイクル 57
Amazon Inspector Classic から AWS アカウントへのアクセスコントロール 58
Amazon Inspector Classic エージェントの制限 58
Amazon Inspector Classic エージェントのインストール 58
Systems Manager Run Command を使用して複数の EC2 インスタンスにエージェントをインストールする 59
Linux ベースの EC2 インスタンスにエージェントをインストールします。 60
Windows ベースの EC2 インスタンスにエージェントをインストールするには 62
Linux ベースのオペレーティングシステムでの Amazon Inspector Classic エージェントの操作 63
Amazon Inspector Classic エージェントの実行の確認 64
Amazon Inspector Classic エージェントの停止 64
Amazon Inspector Classic エージェントの起動 64
Amazon Inspector Classic エージェントの設定の変更 65
Amazon Inspector Classic エージェントのプロキシサポートの設定 65
Amazon Inspector Classic エージェントのアンインストール 67
Windows ベースのオペレーティングシステムでの Amazon Inspector Classic エージェントの操作 67
Amazon Inspector Classic エージェントの開始または停止、またはそのエージェントが実行中であることの確認 68
Amazon Inspector Classic エージェントの設定の変更 69
Amazon Inspector Classic エージェントのプロキシサポートの設定 69
Amazon Inspector Classic エージェントのアンインストール 70
(オプション) Linux ベースのオペレーティングシステムの Amazon Inspector Classic エージェントのインストールスクリプトの署名を確認します。 71
GPG ツールのインストール 72
パブリック キーの認証とインポート 72
パッケージの署名の確認 74
「オプショナル」 Windows ベースのオペレーティングシステムの Amazon Inspector Classic エージェントインストールスクリプトの署名を確認します。 76
Amazon Inspector Classic 評価ターゲット 78

リソースをタグ付けして評価ターゲットを作成する 78
Amazon Inspector Classic 評価ターゲットの制限 79
評価ターゲットを作成する 79
評価ターゲットを削除する 81
Amazon Inspector Classic ルールパッケージとルール 82
Amazon Inspector Classic のルールの重要度レベル 82
Amazon Inspector Classic のルールパッケージ 83
ネットワーク到達可能性 83
分析された設定 84
到達可能性ルート 85
結果のタイプ 85
共通脆弱性識別子 87
Center for Internet Security (CIS) ベンチマーク 89
Amazon Inspector Classic のセキュリティのベストプラクティス 92
SSH 経由の root ログインを無効化する 93
SSH バージョン 2 のみをサポート 93
SSH 経由のパスワード認証を無効化する 94
パスワードの有効期限を設定する 94
パスワードの最小文字数を設定する 95
パスワードの複雑さを設定する 96
ASLR の有効化 96
DEP の有効化 97
システムディレクトリに対するアクセス許可の設定 97
Amazon Inspector Classic の評価テンプレートと評価の実行 99
Amazon Inspector Classic 評価テンプレート 99
Amazon Inspector Classic 評価テンプレートの制限 100
評価テンプレートを作成する 100
評価テンプレートを削除する 102
評価の実行 103
評価の実行を削除する 103
Amazon Inspector Classic 評価実行の制限 104
Lambda 関数を使用した評価の自動実行のセットアップ 104
Amazon Inspector Classic 通知用の SNS トピックの設定 106
Amazon Inspector Classic 結果 109
結果を使用する 109
評価レポート 112

Amazon Inspector Classic の除外 114
除外タイプ 114
除外のプレビュー 127
評価後の除外の確認 128
サポートされているオペレーティングシステムの Amazon Inspector Classic ルールパッケージ .. 129
を使用した Amazon Inspector Classic API コールのログ記録 AWS CloudTrail 137
CloudTrail での Amazon Inspector Classic 情報 137
Amazon Inspector Classic ログファイルエントリの理解 138
Amazon CloudWatch を使用した Amazon Inspector Classic のモニタリング 141
Amazon Inspector Classic の CloudWatch メトリクス 141
を使用した Amazon Inspector Classic の設定 AWS CloudFormation 143
Security Hub CSPM の統合 144
Amazon Inspector が Security Hub CSPM に結果を送信する方法 144
Amazon Inspector が送信する検出結果のタイプ 145
検出結果が送信されるまでのレイテンシー 145
Security Hub CSPM が使用できない場合の再試行 145
Security Hub CSPM の既存の検出結果を更新する 145
Amazon Inspector からの典型的な検出結果 146
統合の有効化と構成 148
検出結果の送信を停止する方法 148
Amazon Inspector Classic ARN 149
Amazon Inspector Classic リソースの ARN 149
ルールパッケージの Amazon Inspector Classic ARN 150
米国東部 (オハイオ) 151
米国東部 (バージニア北部) 151
米国西部 (北カリフォルニア) 152
米国西部 (オレゴン) 153
アジアパシフィック (ムンバイ) 154
アジアパシフィック (ソウル) 154
アジアパシフィック (シドニー) 155
アジアパシフィック (東京) 156
欧州 (フランクフルト) 156
欧州 (アイルランド) 157
欧州 (ロンドン) 158
欧州 (ストックホルム) 159
AWS GovCloud (米国東部) 159

AWS GovCloud (米国西部) 160
ドキュメント履歴 161
AWS 用語集 168

サポート終了通知: 2026 年 5 月 20 日、 AWS は Amazon Inspector Classic のサポートを終了します。2026 年 5 月 20 日以降、Amazon Inspector Classic コンソールまたは Amazon Inspector Classic リソースにアクセスできなくなります。Amazon Inspector Classic は、過去 6 か月間に評価を完了していない新しいアカウントやアカウントで利用できなくなりました。他のすべてのアカウントでは、アクセスは 2026 年 5 月 20 日まで有効です。その後、Amazon Inspector Classic コンソールまたは Amazon Inspector Classic リソースにアクセスできなくなります。詳細については、Amazon Inspector Classic のサポート終了」を参照してください。

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。

Amazon Inspector Classic とは

> **Note**
>
> Amazon Inspector Classic の完全に再設計されたバージョンである新しい Amazon Inspector が、 AWS リージョンで使用可能になりました。新しい Amazon Inspector では、EC2 インスタンスに加えて Amazon Elastic Container Registry (Amazon ECR) に存在するコンテナイメージのサポートが追加され、カバレッジが拡張されました。新しい Amazon Inspector は AWS Organizations、 との統合、一般的な脆弱性と露出 (CVEs) に基づく継続的なソフトウェアの脆弱性とネットワーク到達可能性スキャンを通じて、マルチアカウントサポートを提供します。これらの機能と改善された機能をぜひ使用し、大幅に強化されたセキュリティ価値の利点を享受されることをお勧めします。新しい Amazon Inspector の機能と料金については、「Amazon Inspector」を参照してください。新しい Amazon Inspector に移行する方法については、「Amazon Inspector Classic のサポート終了」を参照してください。

Amazon Inspector Classic は、Amazon EC2 インスタンスのネットワークアクセシビリティとそれらのインスタンスで実行されるアプリケーションのセキュリティ状態をテストします。Amazon Inspector Classic は、アプリケーションを評価し、漏洩、脆弱性、ベストプラクティスからの逸脱がないか確認できます。評価を実行した後、Amazon Inspector Classic は、重要度のレベルごとに編成されたセキュリティ結果の詳細なリストを作成します。

Amazon Inspector Classic を使用すると、開発とデプロイのパイプラインや静的生産システムの全体的なセキュリティ脆弱性評価を自動化できます。これにより、セキュリティテストを開発および IT オペレーションの通常の一部にすることができます。

Amazon Inspector Classic には、評価対象の EC2 インスタンスのオペレーティングシステムにオプションでインストールできる、エージェントと呼ばれる定義済みソフトウェアがあります。エージェントは、EC2 インスタンスの動作 (ネットワーク、ファイルシステム、プロセスアクティビティなど) をモニタリングします。また、さまざまな動作と設定データを収集します (テレメトリ)。

> **Important**
>
> AWS は、提供された推奨事項に従うことで、潜在的なセキュリティ上の問題がすべて解決されることを保証するものではありません。Amazon Inspector Classic によって生成された検出結果は、各評価テンプレートに含まれるルールパッケージの選択、システム内の非AWS コンポーネントの存在、およびその他の要因によって異なります。お客様は、 AWS サービ

スで実行されるアプリケーション、プロセス、ツールのセキュリティに責任を負います。詳細については、セキュリティのAWS 責任分担モデルを参照してください。

> **Note**
>
> AWS は、 AWS クラウドで提供されるサービスを実行するグローバルインフラストラクチャを保護する責任があります。このインフラストラクチャは、 AWS サービスを実行するハードウェア、ソフトウェア、ネットワーク、および施設で構成されます。 は、さまざまなコンピュータセキュリティ標準および規制への準拠を検証したサードパーティーの監査者からのいくつかのレポート AWS を提供します。詳細については、「AWS クラウドのコンプライアンス」を参照してください。

Amazon Inspector Classic の用語については、「Amazon Inspector Classic の用語と概念」を参照してください。

Amazon Inspector Classic のメリット

Amazon Inspector Classic の主なメリットは以下のとおりです。

- 自動セキュリティチェックを通常のデプロイおよび本番プロセスに統合する – フォレンジック、トラブルシューティング、またはアクティブな監査の目的で、 AWS リソースのセキュリティを評価します。開発プロセス中に評価を実行するか、安定した本番環境で実行してください。
- アプリケーションのセキュリティ問題を発見 – アプリケーションのセキュリティ評価を自動化し、脆弱性を予防的に特定します。これにより、新しいアプリケーションの開発と反復実行を迅速に行い、ベストプラクティスやポリシーへのコンプライアンス状況を評価できます。
- AWS リソースをより深く理解する – Amazon Inspector Classic が生成する検出結果を確認して、AWS リソースのアクティビティと設定データに関する情報を入手します。

Amazon Inspector Classic の特徴

Amazon Inspector Classic の主な特徴は以下のとおりです。

- 設定スキャンおよびアクティビティモニタリングエンジン – Amazon Inspector Classic は、システムとリソースの設定を分析するエージェントを提供します。また、アクティビティをモニタリングして、評価ターゲットの状態、動作、および依存コンポーネントを判断します。このテレメトリの

組み合わせにより、ターゲットとその潜在的なセキュリティまたはコンプライアンスの問題の全体像が得られます。

- 組み込みコンテンツライブラリ – Amazon Inspector Classic には、ルールやレポートの組み込みライブラリがあります。これらには、ベストプラクティス、一般的なコンプライアンス基準や、脆弱性の点検が含まれます。この点検には、潜在的なセキュリティ上の問題を解決するための詳細な推奨ステップが含まれます。
- API を介した自動化 – Amazon Inspector Classic は API を介して完全に自動化できます。これにより、開発プロセスと設計プロセスにセキュリティ テストを組み込めるようになります。セキュリティ テストには、テスト結果の選択、実行、レポートが含まれます。

Amazon Inspector Classic へのアクセス

Amazon Inspector Classic サービスは、次のいずれかの方法で使用できます。

Amazon Inspector Classic コンソール

にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/inspector/ で Amazon Inspector Classic コンソールを開きます。

コンソールは、Amazon Inspector Classic サービスにアクセスして使用するためのブラウザベースのインターフェイスです。

AWS SDKs

AWS には、さまざまなプログラミング言語とプラットフォーム用のライブラリとサンプルコードで構成されるソフトウェア開発キット (SDKsが用意されています。これらには Java、Python、Ruby、.NET、iOS、Android など が含まれます。SDK は、Amazon Inspector Classic サービスへのプログラムによるアクセスを作成する際に役立ちます。 AWS SDKs「Amazon Web Services のツール」を参照してください。

Amazon Inspector Classic HTTPS API

Amazon Inspector Classic および に AWS プログラムでアクセスするには、Amazon Inspector Classic HTTPS API を使用します。これにより、HTTPS リクエストを サービスに直接発行できます。詳細については、「Amazon Inspector Classic API リファレンス」を参照してください。

AWS コマンドラインツール

AWS コマンドラインツールを使用して、システムのコマンドラインでコマンドを実行し、Amazon Inspector Classic タスクを実行できます。コマンドラインツールは、 AWS タス

クを実行するスクリプトを構築する場合にも役立ちます。詳細については、Amazon Inspector Classic AWS コマンドラインインターフェイス」を参照してください。

Amazon Inspector Classic の用語と概念

Amazon Inspector Classic の使用を開始するにあたり、その主要な概念を確認しておくとメリットがあります。

Amazon Inspector Classic エージェント

評価ターゲットに含まれている EC2 インスタンスにインストールできるソフトウェアエージェント。エージェントは、さまざまな設定データを収集します (テレメトリ)。詳細については、「Amazon Inspector Classic エージェント」を参照してください。

評価の実行

指定したルール パッケージで評価ターゲットの設定を分析し、潜在的なセキュリティ上の問題を発見するプロセスです。評価の実行中、Amazon Inspector は指定されたターゲット内のリソースからの設定データ (テレメトリ) をモニタリング、収集、分析します。次に、Amazon Inspector はデータを分析し、評価の実行中に使用される評価テンプレートで指定された一連のセキュリティルールパッケージと比較します。評価の実行が完了すると、結果 (様々な重大度の潜在的なセキュリティ上の問題) のリストが作成されます。詳細については、「Amazon Inspector Classic の評価テンプレートと評価の実行」を参照してください。

評価ターゲット

Amazon Inspector Classic のコンテキストでは、単位として連動してビジネス目標の達成を支援する AWS リソースの集合体です。Amazon Inspector Classic では、評価ターゲットを構成するリソースのセキュリティ状態が評価されます。

> **Important**
>
> 現時点では、Amazon Inspector Classic 評価ターゲットは EC2 インスタンスのみを含むことができます。詳細については、「Amazon Inspector Classic サービスの制限」を参照してください。

Amazon Inspector Classic 評価ターゲットを作成するには、まず EC2 インスタンスに選択したキーと値のペアをタグ付けする必要があります。次に、共通のキーまたは共通の値を持つこれら

のタグ付き EC2 インスタンスのビューを作成できます。詳細については、「Amazon Inspector Classic 評価ターゲット」を参照してください。

評価テンプレート

評価の実行中に使用される設定です。テンプレートは以下が含まれます:

- 評価ターゲットの評価に Amazon Inspector Classic が使用するルールパッケージ
- 評価の実行状態と結果に関する通知を Amazon Inspector Classic が送信する Amazon SNS トピック。
- 評価実行によって生成された結果に割り当てることができるタグ (キーと値のペア)。
- 評価の実行の時間

結果

指定されたターゲットの評価の実行中に Amazon Inspector Classic が発見する潜在的なセキュリティ問題。結果は Amazon Inspector Classic コンソールに表示されるか、API を介して取得されます。それらにはセキュリティ問題の詳細な説明と推奨される修正措置が含まれています。詳細については、「Amazon Inspector Classic 結果」を参照してください。

ルール

Amazon Inspector Classic のコンテキストで、評価の実行中に実行されるセキュリティチェックです。ルールが潜在的なセキュリティ上の問題を検出すると、Amazon Inspector Classic はその問題を説明する結果を生成します。

ルール パッケージ

Amazon Inspector Classic のコンテキストでは、ルールの集合体です。ルール パッケージは、セキュリティ上の目標に対応します。Amazon Inspector Classic の評価テンプレートを作成する際に適切なルールパッケージを選択することで、セキュリティ上の目標を指定できます。詳細については、「Amazon Inspector Classic ルールパッケージとルール」を参照してください。

テレメトリ

EC2 インスタンスのインストール済みパッケージ情報とソフトウェア設定。Amazon Inspector Classic は、評価の実行中にデータを収集します。

Amazon Inspector Classic サービスの制限

次の表に、AWS アカウントの Amazon Inspector Classic の制限を示します。

> **Important**
>
> 現時点では、評価ターゲットは EC2 インスタンスのみを含むことができます。

各リージョンの AWS アカウントごとの Amazon Inspector Classic の制限は以下のとおりです。

リソース	デフォルトの制限	コメント
評価を実行中のインスタンス	500	リージョンごとのアカウントごとに実行中のすべての評価に含めることができる EC2 インスタンスの最大数。
評価の実行	50000	リージョンごとに作成できる、評価の実行の最大数。評価の実行は、使用される評価ターゲットに EC2 インスタンスの重複が含まれない限り、同時進行させることができます。
評価テンプレート	500	リージョンごと、アカウントごとに任意の時点で保持できる評価テンプレートの最大数。
評価ターゲット	50	リージョンごと、アカウントごとに任意の時点で保持できる評価ターゲットの最大数。

特に明記されていない限り、これらの制限は AWS サポート センターに連絡してリクエストすることによって増やすことができます。

Amazon Inspector Classic の料金

Amazon Inspector Classic の料金は、各評価に含まれる EC2 インスタンスの数とそれらの評価で使用されるルールパッケージに基づいています。

ネットワーク到達可能性ルールパッケージの料金

ネットワーク到達可能性ルールパッケージを使用した Amazon Inspector Classic 評価は、1 か月あたりの評価 (インスタンス評価) ごとにインスタンス単位の料金が設定されます。例えば、1 つのインスタンスに対して 1 つの評価を実行すると、1 つのインスタンス評価になります。10 のインスタンスに対して 1 つの評価を実行すると、10 インスタンス評価になります。料金は、インスタンス評価あたり月額 0.15 USD から始まり、ボリュームディスカウントでインスタンス評価あたり月額 0.04 USD まで安くなります。

無料トライアルの詳細情報

Amazon Inspector Classic を使用する最初の 90 日間	インスタンス評価あたりの料金
First 250 instance-assessments	$0.00

料金詳細

特定の月	インスタンス評価あたりの料金
First 250 instance-assessments	$0.15
Next 750 instance-assessments	$0.13
Next 4,000 instance-assessments	$0.10
Next 45,000 instance-assessments	$0.07
All other instance-assessments	$0.04

ホスト評価ルールパッケージの料金

一般的脆弱性およびエクスポージャー (CVE)、インターネットセキュリティセンター (CIS) ベンチマーク、セキュリティのベストプラクティス、および評価に含まれるランタイム動作分析の任意の組み合わせについて

Amazon Inspector Classic のホスト評価ルールパッケージは、評価するアプリケーションを実行する Amazon EC2 インスタンスにデプロイされたエージェントを使用します。ホストルールパッケージを使用したアセスメントの価格は、1エージェント1アセスメント (エージェント-アセスメント) あたり月額です。例えば、1 エージェントに対して 1 評価を実行すると、1 エージェント評価になります。10 エージェントに対して 1 評価を実行すると、10 エージェント評価になります。料金は、エージェント評価あたり月額 0.30 USD から始まり、ボリュームディスカウントでエージェント評価あたり月額 0.05 USD まで安くなります。

無料トライアルの詳細情報

Amazon Inspector Classic を使用する最初の 90 日間	エージェント評価あたりの料金
First 250 agent-assessments	$0.00

料金詳細

特定の月	エージェント評価あたりの料金
First 250 agent-assessments	$0.30
Next 750 agent-assessments	$0.25
Next 4,000 agent-assessments	$0.15
Next 45,000 agent-assessments	$0.10
All other agent-assessments	$0.05

Amazon Inspector Classic でサポートされているオペレーティングシステムとリージョン

この章では、Amazon Inspector Classic がサポートするオペレーティングシステムと AWS リージョンについての情報を提供します。

> **Important**
>
> 現時点では、Amazon Inspector Classic 評価ターゲットは EC2 インスタンスのみを含むことができます。オペレーティングシステムに関係なく、任意の EC2 インスタンスで Network Reachability ルールパッケージを使用してエージェントレス評価を実行できます。

サポートされているオペレーティングシステム全体で利用可能な Amazon Inspector Classic ルールパッケージについては、「サポートされているオペレーティングシステムの Amazon Inspector Classic ルールパッケージ」を参照してください。

トピック

- Amazon Inspector Classic エージェントでサポートされている Linux ベースのオペレーティングシステム
- Amazon Inspector Classic エージェントでサポートされている Windows ベースのオペレーティングシステム
- サポートしている AWS リージョン

Amazon Inspector Classic エージェントでサポートされている Linux ベースのオペレーティングシステム

Amazon Inspector Classic エージェントは 64 ビット x86 および Arm EC2 インスタンスで使用できます。エージェントは、次の Linux ベースのオペレーティングシステムと互換性があります。

- 64 ビット x86 インスタンス
  - Amazon Linux 2
  - Amazon Linux
    (2018.03、2017.09、2017.03、2016.09、2016.03、2015.09、2015.03、2014.09、2014.03、2013.09、
  - Ubuntu (20.04 LTS, 18.04 LTS, 16.04 LTS, 14.04 LTS)

- Debian (10.x, 9.0 - 9.5, 8.0 - 8.7)
- Red Hat Enterprise Linux (8.x、7.2、6.2 - 6.9)
- CentOS (7.2 - 7.x, 6.2 - 6.9)

- Arm インスタンス
  - Amazon Linux 2
  - Red Hat Enterprise Linux (7.6 - 7.x)
  - Ubuntu (18.04 LTS, 16.04 LTS)

Amazon Inspector Classic エージェントでサポートされている Windows ベースのオペレーティングシステム

Amazon Inspector Classic エージェントは、64 ビットバージョンの次の Windows ベースのオペレーティングシステムを実行する EC2 インスタンスでのみ使用できます。

- Windows Server 2019 ベース
- Windows Server 2016 ベース
- Windows Server 2012 R2
- Windows Server 2012
- Windows サーバー 2008 R2

サポートしている AWS リージョン

Amazon Inspector Classic は次の AWS リージョンでサポートされています。

- 米国東部 (オハイオ) us-east-2
- 米国東部 (バージニア北部) us-east-1
- 米国西部 (北カリフォルニア) us-west-1
- 米国西部 (オレゴン) us-west-2
- アジアパシフィック (ムンバイ) ap-south-1
- アジアパシフィック (ソウル) ap-northeast-2
- アジアパシフィック (シドニー) ap-southeast-2
- アジアパシフィック (東京) ap-northeast-1

- 欧州 (フランクフルト) eu-central-1
- ヨーロッパ (アイルランド) eu-west-1
- 欧州 (ロンドン) eu-west-2
- 欧州 (ストックホルム) (eu-north-1)
- AWS GovCloud (米国東部) gov-us-east-1
- AWS GovCloud (米国西部) gov-us-west-1

> **Note**
>
> Network Reachability ルールパッケージは、 AWS GovCloud (米国) リージョンでは使用できません。

Amazon Inspector Classic のサポート終了

慎重に検討した結果、2026 年 5 月 20 日をもって Amazon Inspector Classic のサポートを終了することにしました。Amazon Inspector Classic は、2025 年 5 月 20 日以降、新規顧客を受け入れなくなります。2025 年 5 月 20 日より前にサービスにサインアップしたアカウントを持つ既存のお客様は、引き続き Amazon Inspector Classic の機能を使用できます。2026 年 5 月 20 日以降、Amazon Inspector Classic を使用することはできません。

新しい Amazon Inspector が、 AWS リージョンでグローバルに利用可能になりました。既存の Amazon Inspector の完全に再設計されたバージョンである新しい Amazon Inspector (Amazon Inspector Classic) が使用可能になりました。次の機能は、Amazon Inspector の主要な機能強化です。

- 規模に合わせて構築 – 新しい Amazon Inspector は、スケールと動的なクラウド環境向けに構築されています。があるスキャンできるインスタンスまたはイメージの数に制限はありませんアカウントで。
- コンテナイメージのサポート – 新しい Amazon Inspector は、Amazon Elastic Container Registry (Amazon ECR) に存在するコンテナイメージも、ソフトウェアの脆弱性をスキャンします。
- マルチアカウント管理のサポート— 新しい Amazon Inspector は Organizations と統合されています。これにより、Amazon Inspector の管理者アカウントを組織から委任できます。委任された管理者アカウントは、すべての結果を統合し、すべてのメンバーアカウントを設定できる一元化されたアカウントです。
- AWS Systems Manager エージェント (SSM エージェント) を使用 – 新しい Amazon Inspector を使用すると、すべての EC2 インスタンスにスタンドアロンの Amazon Inspector エージェントをインストールして維持する必要がなくなります。新しい Amazon Inspector は、広くデプロイされている SSM Agent を活用します。
- 自動で継続的なスキャン – Amazon Inspector Classic では、評価ターゲットと評価テンプレートを手動で設定し、評価の頻度を設定できます。ただし、Amazon Inspector の新しいバージョンでは、新しく起動されたすべての EC2 インスタンスと Amazon ECR にプッシュされた適格なコンテナイメージが自動的に検出され、ソフトウェアの脆弱性と予期しないネットワークエクスポージャーがないかすぐにスキャンされます。リソースは、起動する新しい EC2 インスタンス、Amazon ECR にプッシュされるコンテナイメージ、EC2 インスタンスへの新しいパッケージのインストール、パッチのインストール、リソースに影響を与える新しい一般的な脆弱性およびエクスポージャー (CVE) の公開など、いくつかのトリガーに基づいて自動的に再スキャンされます。

- Amazon Inspector リスクスコア – 新しい Amazon Inspector は、結果の優先順位付けに役立つ Amazon Inspector リスクスコアを計算します。リスクスコアは、最新の CVE 情報と、ネットワークのアクセシビリティやエクスプロイトビリティ情報などの時間的および環境的要因を関連付けることによって計算されます。
- その他の統合 — すべての検出結果は、新しく設計された Amazon Inspector コンソールに集約され、 AWS Security Hub CSPM と Amazon EventBridge にプッシュされ、チケット発行などのワークフローを自動化します。コンテナイメージ関連の結果も Amazon ECR にプッシュされます。

新しい Amazon Inspector のすべての機能と料金については、「Amazon Inspector ユーザーガイド」を参照してください。

Amazon Inspector Classic をしばらくサポートし続け、お客様は新しい Amazon Inspector と Amazon Inspector Classic の両方を同じアカウントで使用できますが、新しい Amazon Inspector に移行することを強くお勧めします。以下のセクションでは、Amazon Inspector Classic から新しい Amazon Inspector に移行する手順について説明します。

トピック

- ステップ 1: (オプション) 評価レポートと結果をエクスポートする
- ステップ 2: Amazon Inspector Classic でスケジュールされた評価の実行をすべて削除する
- ステップ 3: 新しい Amazon Inspector を有効にする

ステップ 1: (オプション) 評価レポートと結果をエクスポートする

Amazon Inspector Classic で評価レポートと結果を保存するには、評価レポートを生成します。

評価レポートを生成するには

1. [Assessment runs (評価の実行)] ページで、レポートを生成する評価実行を見つけます。そのステータスが、[Analysis complete (分析完了)] であることを確認してください。
2. この評価の実行の [Reports (レポート)] 列で、レポートのアイコンを選択します。

> **Important**
>
> レポートアイコンは、2017 年 4 月 25 日以降に実行された、または実行される予定の評価実行に対してのみ [Reports (レポート)] 列に表示されます。このとき Amazon Inspector Classic の評価レポートが利用可能になります。

3. [Assessment report (評価レポート)] ダイアログボックスで、表示するレポートの種類 (結果レポートまたはフルレポート) とレポート形式 (HTML または PDF) を選択します。次に、[Generate report (レポートの生成)] を選択します。

ステップ 2: Amazon Inspector Classic でスケジュールされた評価の実行をすべて削除する

Amazon Inspector Classic を無効にするには、すべてのアクティブな AWS リージョンでアカウントのすべての評価テンプレートを削除します。評価テンプレートを削除すると、予定されている将来の評価の実行がすべて停止します。

評価テンプレートを削除するには

- [Assessment Templates (評価テンプレート)] ページで、削除するテンプレートを選択し、[Delete (削除)] を選択します。確認を求めるメッセージが表示されたら、実行コマンドYes実行コマンド を選択します。

> **Important**
>
> 評価テンプレートを削除すると、すべての評価の実行、結果、このテンプレートに関連付けられたバージョンのレポートも削除されます。

ステップ 3: 新しい Amazon Inspector を有効にする

AWS マネジメントコンソール または新しい Amazon Inspector APIs を使用して、新しい Amazon Inspector を有効にできます。新しい Amazon Inspector の使用開始にあたっては、Amazon Inspector ユーザーガイドの「Getting Started (使用開始)」を参照してください。

Amazon Inspector Classic の開始方法

このチュートリアルでは、Amazon Inspector Classic を設定し、最初の評価を作成して実行する方法を示します。

にサインアップする AWS アカウント

の使用を開始するには AWS、 が必要です AWS アカウント。の作成の詳細については AWS アカウント、 AWS アカウント管理 リファレンスガイドの「 の開始方法 AWS アカウント」を参照してください。

ワンクリックでのセットアップ

次の手順では、現在の および で使用可能なすべての Amazon Elastic Compute Cloud (Amazon EC2) インスタンスで、構築済みのテンプレートと事前定義されたスケジューリングパラメータ (1 週間に 1 回または 1 AWS アカウント 回のみ) を使用して自動評価を作成して実行する方法を示します AWS リージョン。

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/inspector/ で Amazon Inspector Classic コンソールを開きます。
2. ようこそ ページで、実行する評価のタイプを選択します。ネットワーク評価は、 AWS 環境のネットワーク設定の脆弱性を分析し、Amazon Inspector Classic エージェントは必要ありません。ホスト評価 は、ホスト上のソフトウェアと EC2 インスタンスの設定の脆弱性を分析します。EC2 インスタンスにエージェントをインストールする必要があります。

   毎週実行推奨または 1 回実行 を選択します。選択するとすぐに、サービスは自動的に評価を作成します。具体的には、サービスは次の処理を行います。

   a. サービスにリンクされたロールを作成します。

   > **Note**
   >
   > 評価ターゲットで指定されている EC2 インスタンスを識別するには、Amazon Inspector Classic が EC2 インスタンスとタグを列挙する必要があります。Amazon Inspector Classic は、サービスにリンクされたロール `AWSServiceRoleForAmazonInspector`を使用して、 AWS アカウント のこれら

のリソースに対するアクセス権限を取得します。サービスにリンクされたロールの詳細については、「Amazon Inspector Classic でのサービスにリンクされたロールの使用」および「サービスにリンクされたロールの使用」を参照してください。

b. 必要に応じて、 は、 AWS アカウント および リージョンで使用可能なすべての EC2 インスタンスに Amazon Inspector Classic エージェントをインストールします。

> **Note**
>
> このサービスは、 AWS Systems Manager Run Command を許可する EC2 インスタンスにのみ Amazon Inspector Classic エージェントをインストールします。このオプションを使用するには、現在の AWS アカウント と のすべての EC2 インスタンスに AWS リージョン SSM エージェントがインストールされており、Run Command を許可する IAM ロールがあることを確認します。詳細については、「Systems Manager Run Command を使用して複数の EC2 インスタンスにエージェントをインストールする」を参照してください。

c. 評価ターゲット にこれらのインスタンスを追加します。

d. ルールテンプレートの標準化されたセットを含む評価テンプレートにそのターゲットを含めます。

e. 毎週実行推奨または 毎日1回実行 を選択したかどうかに応じて、毎週または 1 回だけ評価を実行します。

3. 確認 ダイアログボックスで OK を選択します。Amazon Inspector Classic は自動的に評価を実行します。

詳細設定

次の手順では、特定の Amazon EC2 インスタンス、ルールパッケージ、およびスケジューリングパラメータを選択し、評価ターゲットとテンプレートに含める方法を示します。

1. ようこそ ページで、拡張設定 を選択します。
2. 評価ターゲットの定義 ページで、評価ターゲットの名前を入力します。
3. すべてのインスタンスでは、チェックボックスをオンにしたまま、 AWS アカウント および リージョンのすべての EC2 インスタンスを評価ターゲットに含めることができます。どの EC2 インスタンスを含めるかを選択する場合は、すべてのインスタンス チェックボックスをオンにし、ターゲット EC2 インスタンスに関連付けられたキーおよび値タグを入力します。EC2 イン

スタンスへのタグ付けの詳細については、「Amazon EC2 リソースにタグを付ける」を参照してください。

4. エージェントのインストール では、インスタンスによって システムマネージャ 実行コマンド が許可されている場合、デフォルトでチェックボックスを選択したままにすることができます。このサービスは、 が許可する評価ターゲット内のすべての EC2 インスタンスに Amazon Inspector Classic エージェントをインストールします AWS Systems Manager。このオプションを使用するには、現在の AWS アカウント と のすべての EC2 インスタンスに SSM エージェントがインストールされ AWS リージョン ており、Run Command を許可する IAM ロールがあることを確認します。詳細については、「Systems Manager Run Command を使用して複数の EC2 インスタンスにエージェントをインストールする」を参照してください。エージェントを手動でインストールする場合は、「Amazon Inspector エージェントをインストールする」を参照してください。
5. 次へ をクリックします。
6. 評価テンプレートの定義 ページで、評価テンプレートの名前を入力します。
7. ルール・パッケージ では、評価テンプレートに含めるルールパッケージを選択します。ルールパッケージの詳細については、「Amazon Inspector ルール・パッケージとルール」を参照してください。
8. 期間 で、評価の実行の時間を選択します。
9. 「オプション」評価スケジュール では、定期的な評価実行のスケジュールを設定できます。
10. 次へ をクリックします。
11. レビューページで、評価ターゲットとテンプレートの選択内容を確認します。設定に問題がなければ、作成 を選択します。評価テンプレートの評価スケジュールを設定すると、作成作成を選択した後で評価が自動的に実行されます。

> **Note**
>
> 評価ターゲットで指定されている EC2 インスタンスを識別するには、Amazon Inspector Classic が EC2 インスタンスとタグを列挙する必要があります。Amazon Inspector Classic は、 というサービスにリンクされたロール AWS アカウント を通じて、 内のこれらのリソースにアクセスします`AWSServiceRoleForAmazonInspector`。Amazon Inspector Classicのサービスにリンクされたロールの詳細については、「Amazon Inspector Classic でのサービスにリンクされたロールの使用」を参照してください。サービスリンクロールの詳細については、AWS Identity and Access Management ユーザーガイドの「サービスにリンクされたロールの使用」を参照してください。

12. 評価スケジュールを設定していない場合は、コンソールから評価テンプレートに移動し、実行を選択します。
13. 評価実行の進捗状況を追跡するには、コンソールのナビゲーションペインで、評価実行 を選択し、結果 を選択します。調査結果についての詳細は、「Amazon Inspector Classic 結果」を参照してください。

Amazon Inspector Classic のチュートリアル

次のチュートリアルでは、Red Hat Enterprise Linux および Ubuntu オペレーティングシステムで Amazon Inspector Classic 評価を実行する方法を示します。

チュートリアル

- チュートリアル: Red Hat Enterprise Linux での Amazon Inspector Classic の使用
- チュートリアル: Ubuntu Server での Amazon Inspector Classic の使用

Amazon Inspector Classic チュートリアル - Red Hat Enterprise Linux

このチュートリアルの指示を実行する前に、Amazon Inspector Classic の用語と概念 に習熟しておくことをお勧めします。

このチュートリアルは、Amazon Inspector Classic を使用して、Red Hat Enterprise Linux 7.5 オペレーティングシステムを実行する EC2 インスタンスの動作を分析する方法を示します。Amazon Inspector Classic ワークフローをナビゲートする方法について、ステップバイステップで説明しています。このワークフローには、Amazon EC2 インスタンスの準備、評価テンプレートの実行、評価の結果で生成された推奨されるセキュリティ修正の実行が含まれます。初心者ユーザーであり、ワンクリックで Amazon Inspector Classic 評価を設定して実行したい場合は、「Creating a Basic Assessment」を参照してください。

トピック

- ステップ 1: Amazon Inspector Classic で使用する Amazon EC2 インスタンスをセットアップする
- ステップ 2: Amazon EC2 インスタンスを変更する
- ステップ 3: 評価ターゲットを作成して EC2 インスタンスにエージェントをインストールする
- ステップ 4: 評価テンプレートを作成および実行する
- ステップ 5: 結果を見つけて分析する
- ステップ 6: 推奨される修正手順を評価ターゲットに適用する

ステップ 1: Amazon Inspector Classic で使用する Amazon EC2 インスタンスをセットアップする

このチュートリアルでは、Red Hat Enterprise Linux 7.5 を実行する EC2 インスタンスを 1 つ作成し、名前 キーと **InspectorEC2InstanceLinux** の値を使用してタグ付けします。

> **Note**
>
> EC2 インスタンスのタグ付けの詳細については、「リソースとタグ」を参照してください。

ステップ 2: Amazon EC2 インスタンスを変更する

このチュートリアルでは、ターゲット EC2 インスタンスを変更し、潜在的な安全上の問題 CVE-2018-1111 に曝露します。詳細については、https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1111 および「共通脆弱性識別子」を参照してください。

インスタンス **InspectorEC2InstanceLinux** に接続し、次のコマンドを実行します。

```
sudo yum install dhclient-12:4.2.5-68.el7
```

EC2 インスタンスに接続する方法については、Amazon EC2 ユーザーガイド の「インスタンスへの接続」を参照してください。

ステップ 3: 評価ターゲットを作成して EC2 インスタンスにエージェントをインストールする

Amazon Inspector Classic は、評価ターゲットを使用して、評価する AWS リソースを指定します。

評価ターゲットを作成して EC2 インスタンスにエージェントをインストールするには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/inspector/ で Amazon Inspector Classic コンソールを開きます。
2. ナビゲーションペインで、評価ターゲット、作成 の順に選択します。

   以下の操作を実行します。

   a. 名前 に、評価ターゲットの名前を入力します。

      このチュートリアルでは、**MyTargetLinux** と入力します。

b. タグの使用 については、キー フィールドと 値 フィールドに値を入力して、この評価ターゲットに含める EC2 インスタンスを選択します。

このチュートリアルでは、キー フィールドに**Name** と 値 フィールドに **InspectorEC2InstanceLinux** を入力して、前のステップで作成した EC2 インスタンスを選択します。

AWS アカウントとリージョンのすべての EC2 インスタンスを評価対象に含めるには、すべてのインスタンス チェックボックスを選択します。

c. 保存を選択します。

d. ターゲット EC2 インスタンスに Amazon Inspector Classic エージェントをインストールします。評価対象に含まれるすべての EC2 インスタンスにエージェントをインストールするには、Install Agents (エージェントのインストール) チェックボックスを選択します。

> **Note**
>
> また、AWS Systems Manager Run Command を使用して Amazon Inspector Classic エージェントをインストールすることもできます。評価ターゲットのすべてのインスタンスにエージェントをインストールする場合は、その評価ターゲットの作成に使用したのと同じタグを指定できます。または、手動で EC2 インスタンスに Amazon Inspector Classic エージェントをインストールすることもできます。詳細については、「Amazon Inspector Classic エージェントのインストール」を参照してください。

e. 保存を選択します。

> **Note**
>
> この時点で、Amazon Inspector Classic は、`AWSServiceRoleForAmazonInspector` というサービスにリンクされたロールを作成します。ロールは Amazon Inspector Classic にリソースへの必要なアクセスを許可します。詳細については、「Amazon Inspector Classic のサービスリンクロールの作成」を参照してください。

ステップ 4: 評価テンプレートを作成および実行する

テンプレートを作成して実行するには

1. ナビゲーションペインの Assessment templates (評価テンプレート) を選択し、Create (作成) を選択します。
2. Name に、評価テンプレートの名前を入力します。このチュートリアルでは、**MyFirstTemplateLinux** と入力します。
3. Target name (ターゲット名) で、「**MyTargetLinux**」で作成した評価ターゲットを選択します。
4. Rules packages では、この評価テンプレートで使用するルールパッケージを選択します。

   このチュートリアルでは、Common Vulnerabilities and Exposures-1.1 を選択します。
5. Duration では、評価テンプレートの時間を指定します。

   このチュートリアルでは、15 minutes を選択します。
6. Create and run を選択します。

ステップ 5: 結果を見つけて分析する

評価の実行が完了すると、評価ターゲット内で Amazon Inspector Classic が発見した一連の結果または潜在的なセキュリティ上の問題が生成されます。この結果を確認し、推奨される手順に従って潜在的なセキュリティ上の問題を解決することができます。

このチュートリアルでは、前述のステップを完了すると、評価の実行によって一般的な脆弱性 CVE-2018-1111 に対する結果が生成されます。

結果を見つけて分析する

1. ナビゲーションペインで、Assessment runs (評価の実行) を選択します。MyFirstTemplateLinux という評価テンプレートの実行状況が Collecting data (データの収集) に設定されていることを確認します。これは、評価の実行が現在進行中で、選択されたルールパッケージに従ってターゲットのテレメトリーデータが収集および分析されていることを示します。
2. 評価の実行が進行中の間は、評価の実行で生成された結果を表示することはできません。ここでは、指定時間全体で評価の実行を完了させます。このチュートリアルでは、数分後に実行を停止できます。

MyFirstTemplateLinux のステータスが最初は Stopping で、数分後には Analyzing になり、最後に Analysis complete になります。このステータスの変化を表示するには、Refresh アイコンを選択します。

3. ナビゲーションペインで 結果 を選択します。

重要度が High (高) の新しい結果として Instance InspectorEC2InstanceLinux is vulnerable to CVE-2018-1111 (インスタンス InspectorEC2InstanceLinux は CVE-2018-1111 に対して脆弱です) が表示されます。

> **Note**
>
> 新しい結果が表示されない場合は、Refresh アイコンを選択します。

ビューを展開してこの結果の詳細を表示するには、結果の左にある矢印を選択します。結果の詳細には次の情報が含まれます。

- 結果の ARN
- この結果を生成した評価の実行の名前
- この結果を生成した評価ターゲットの名前
- この結果を生成した評価テンプレートの名前
- 評価の実行の開始時間
- 評価の実行の終了時間
- 評価の実行のステータス
- この結果をトリガーしたルールを含むルール パッケージの名前
- Amazon Inspector Classic エージェント ID
- 結果の名前
- 結果の重要度
- 結果の説明
- 結果で説明されている潜在的なセキュリティ上の問題を解決するために推奨される修正ステップ

ステップ 6: 推奨される修正手順を評価ターゲットに適用する

このチュートリアルでは、評価ターゲットを変更し、潜在的な安全上の問題 CVE-2018-1111 に曝露します。この手順では、この問題を解決するために推奨される修正手順を適用します。

修正手順を評価ターゲットに適用する

1. 前のセクションで作成したインスタンスの **InspectorEC2InstanceLinux** を接続し、次のコマンドを実行します。

   ```
   sudo yum update dhclient-12:4.2.5-68.el7
   ```

2. Assessment templates ページで、MyFirstTemplateLinux を選択した後、Run を選択し、このテンプレートを使用する新しい評価の実行を開始します。
3. ステップ 5: 結果を見つけて分析する のステップを実行し、MyFirstTemplateLinux テンプレートを使用したそれ以降の実行の結果を表示します。

   セキュリティの問題 CVE-2018-1111 は解決されたため、結果は表示されません。

Amazon Inspector Classic チュートリアル - Ubuntu Server

このチュートリアルの指示を実行する前に、Amazon Inspector Classic の用語と概念 に習熟しておくことをお勧めします。

このチュートリアルでは、Amazon Inspector Classic を使用して、Ubuntu Server 16.04 LTS オペレーティングシステムを実行する EC2 インスタンスの動作を分析する方法について説明します。Amazon Inspector Classic ワークフローをナビゲートする方法について、ステップバイステップで説明しています。

初心者ユーザーであり、ワンクリックで Amazon Inspector Classic 評価を設定して実行したい場合は、「Creating a Basic Assessment」を参照してください。

トピック

- ステップ 1: Amazon Inspector Classic で使用する Amazon EC2 インスタンスをセットアップする
- ステップ 2: 評価ターゲットを作成して EC2 インスタンスにエージェントをインストールする
- ステップ 3: 評価テンプレートを作成および実行する
- ステップ 4: 生成された結果を見つけて分析する
- ステップ 5: 推奨される修正手順を評価ターゲットに適用する

ステップ 1: Amazon Inspector Classic で使用する Amazon EC2 インスタンスをセットアップする

EC2 インスタンスをセットアップするには

- このチュートリアルでは、Ubuntu Server 16.04 LTS を実行する EC2 インスタンスを 1 つ作成し、[Name] キーと [**InspectorEC2InstanceUbuntu**] の値を使用してタグ付けします。

> **Note**
>
> EC2 インスタンスのタグ付けの詳細については、「リソースとタグ」を参照してください。

ステップ 2: 評価ターゲットを作成して EC2 インスタンスにエージェントをインストールする

Amazon Inspector Classic は、評価ターゲットを使用して、評価する AWS リソースを指定します。

評価ターゲットを作成して EC2 インスタンスにエージェントをインストールするには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/inspector/ で Amazon Inspector Classic コンソールを開きます。
2. ナビゲーションペインで、評価ターゲット、作成 の順に選択します。
3. 名前 に、評価ターゲットの名前を入力します。

   このチュートリアルでは、**MyTargetUbuntu** を入力します。
4. [Use Tags] では、[Key] フィールドと [Value] フィールドに値を入力して、この評価ターゲットに含める EC2 インスタンスを選択します。

   このチュートリアルでは、[Key] フィールドに **Name** と [Value] フィールドに **InspectorEC2InstanceUbuntu** を入力して、前のステップで作成した EC2 インスタンスを選択します。

   AWS アカウントとリージョンのすべての EC2 インスタンスを評価対象に含めるには、[すべてのインスタンス] ボックスを選択します。

5. ターゲット EC2 インスタンスに Amazon Inspector Classic エージェントをインストールします。評価対象に含まれるすべての EC2 インスタンスにエージェントをインストールするには、[Install Agents (エージェントのインストール)] ボックスを選択します。

   > **Note**
   >
   > また、Systems Manager Run Command を使用して Amazon Inspector エージェントをインストールすることもできます。評価ターゲットのすべてのインスタンスにエージェントをインストールする場合は、その評価ターゲットの作成に使用したのと同じタグを指定できます。または、手動で EC2 インスタンスに Amazon Inspector エージェントをインストールすることもできます。詳細については、「Amazon Inspector Classic エージェントのインストール」を参照してください。

6. [保存] を選択します。

> **Note**
>
> この時点で、Amazon Inspector Classic からリソースにアクセスできるように、サービスにリンクされたロール `AWSServiceRoleForAmazonInspector` が作成されます。詳細については、「Amazon Inspector Classic のサービスリンクロールの作成」を参照してください。

ステップ 3: 評価テンプレートを作成および実行する

テンプレートを作成して実行するには

1. [Advanced setup (高度なセットアップ)] を使用している場合は、[Define an assessment template (評価テンプレートの定義)] ページに移動します。[Assessment Templates (評価テンプレート)] ページに移動し、[Create (作成)] を選択します。
2. Name に、評価テンプレートの名前を入力します。このチュートリアルでは、**`MyFirstTemplateUbuntu`** と入力します。
3. Target name (ターゲット名) で、「**`MyTargetUbuntu`**」で作成した評価ターゲットを選択します。
4. [Rules packages (ルールパッケージ)] でドロップダウンメニューを使用し、この評価テンプレートで使用するルールパッケージを選択します。

このチュートリアルでは、Common Vulnerabilities and Exposures-1.1 を選択します。

5. Duration では、評価テンプレートの時間を指定します。

   このチュートリアルでは、[15 minutes (15 分)] を選択します。

6. [高度な設定] を使用している場合は、[次へ] を選択します。次の [Review] ページで、[Create Role] を選択します。それ以外の場合は、[Create and run (作成および実行)] を選択します。

ステップ 4: 生成された結果を見つけて分析する

評価の実行が完了すると、評価ターゲット内で Amazon Inspector Classic が発見した一連の結果または潜在的なセキュリティ上の問題が生成されます。この結果を確認し、推奨される手順に従って潜在的なセキュリティ上の問題を解決することができます。

1. [Assessment Runs (評価の実行)] ページに移動します。前述のステップで作成した [MyFirstTemplateUbuntu] という評価テンプレートの実行のステータスが [Collecting data (データを収集中)] になっていることを確認します。これは、評価の実行が現在進行中で、選択されたルールパッケージに従ってターゲットのテレメトリーデータが収集および分析されていることを示します。
2. 評価の実行が進行中の間は、評価の実行で生成された結果を表示することはできません。ここでは、指定時間全体で評価の実行を完了させます。

   [MyFirstTemplateUbuntu] のステータスが最初は [Stopping (停止中)] で、数分後には [Analyzing (分析中)] になり、最後に [Analysis complete (分析完了)] になります。このステータスの変化を表示するには、Refresh アイコンを選択します。

3. [Findings (結果)] ページに移動します。

   ビューを展開してこの結果の詳細を表示するには、結果の左にある矢印を選択します。結果の詳細には次の情報が含まれます。

   - 結果の ARN
   - この結果を生成した評価の実行の名前
   - この結果を生成した評価ターゲットの名前
   - この結果を生成した評価テンプレートの名前
   - 評価の実行の開始時間
   - 評価の実行の終了時間

- 評価の実行のステータス
- この結果をトリガーしたルールを含むルールパッケージの名前
- Amazon Inspector Classic エージェント ID
- 結果の名前
- 結果の重要度
- 結果の説明
- 結果で説明されている潜在的なセキュリティ上の問題を解決するために推奨される修正ステップ

ステップ 5: 推奨される修正手順を評価ターゲットに適用する

この手順では、更新を適用して、検出された問題を修正します。

1. インスタンス **InspectorEC2InstanceUbuntu** へ接続し、パッケージの更新を実行します。
2. [Assessment Templates (評価テンプレート)] ページで、[MyFirstTemplateUbuntu] を選択した後、[Run (実行)] を選択し、このテンプレートを使用する新しい評価の実行を開始します。
3. ステップ 4: 生成された結果を見つけて分析する のステップを実行し、[MyFirstTemplateUbuntu] テンプレートを使用したそれ以降の実行の結果を表示します。

   パッケージの更新によって、テンプレートの最初の実行の結果が解決されているはずです。

Amazon Inspector Classic のセキュリティ

でのクラウドセキュリティが最優先事項 AWS です。お客様は AWS 、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャからメリットを得られます。

セキュリティは、 AWS とお客様の間の責任共有です。責任共有モデルではこれをクラウドのセキュリティおよびクラウド内のセキュリティと説明しています。

- クラウドのセキュリティ – AWS クラウドで AWS サービスを実行するインフラストラクチャを保護する AWS 責任があります。 AWS また、 では、安全に使用できるサービスも提供しています。サードパーティーの監査者は、AWS コンプライアンスプログラムコンプライアンスプログラムの一環として、当社のセキュリティの有効性を定期的にテストおよび検証。Amazon Inspector Classic に適用するコンプライアンスプログラムの詳細については、コンプライアンスプログラムの範囲内となる AWS のサービスを参照してください。
- クラウド内のセキュリティ – お客様の責任は、使用する AWS サービスによって決まります。また、ユーザーは、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

このドキュメントは、Amazon Inspector Classic の使用時に責任共有モデルがどのように適用されるかを理解するのに役立ちます。以下のトピックでは、セキュリティおよびコンプライアンス上の目的を達成するように Amazon Inspector Classic を設定する方法について説明します。また、Amazon Inspector Classic リソースのモニタリングや保護に役立つ他の AWS のサービスの使用方法についても説明します。

トピック

- Amazon Inspector Classic におけるデータ保護
- Amazon Inspector ClassicのアイデンティティとAccess Management
- Amazon Inspector Classic でのログ記録とモニタリング
- Amazon Inspector Classic でのインシデントへの対応
- Amazon Inspector Classic のコンプライアンス検証
- Amazon Inspector Classic の耐障害性
- Amazon Inspector Classic のインフラストラクチャのセキュリティ
- Amazon Inspector Classic での設定と脆弱性の分析

- Amazon Inspector Classic のセキュリティベストプラクティス

Amazon Inspector Classic におけるデータ保護

責任 AWS 共有モデル、Amazon Inspector Classic でのデータ保護に適用されます。このモデルで説明されているように、 AWS はすべての を実行するグローバルインフラストラクチャを保護する責任があります AWS クラウド。ユーザーは、このインフラストラクチャでホストされるコンテンツに対する管理を維持する責任があります。また、使用する「 AWS のサービス 」のセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、「Data Privacy FAQChina」を参照してください。 欧州におけるデータ保護に関する情報については、General Data Protection Regulation (GDPR) Center を参照してください。

データ保護の目的で、認証情報を保護し AWS アカウント 、 AWS IAM アイデンティティセンターまたは AWS Identity and Access Management (IAM) を使用して個々のユーザーを設定することをお勧めします。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 は必須ですが、TLS 1.3 を推奨します。
- で API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。CloudTrail 証跡を使用して AWS アクティビティをキャプチャする方法については、「 AWS CloudTrail ユーザーガイド」のCloudTrail 証跡の使用」を参照してください。
- AWS 暗号化ソリューションと、その中のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- Amazon Macie などの高度な管理されたセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API AWS を介して にアクセスするときに FIPS 140-3 検証済み暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-3」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報を、タグ、または [名前] フィールドなどの自由形式のテキストフィールドに含めないことを強くお勧めします。これは、コンソール、API、または SDK を使用して Amazon Inspector Classic AWS CLIまたは他の AWS のサービス を使用する場合も同様です。 AWS SDKs タグ、または名前に使用される自由記述のテキストフィールドに入力し

たデータは、請求または診断ログに使用される場合があります。外部サーバーに URL を提供する場合、そのサーバーへのリクエストを検証できるように、認証情報を URL に含めないことを強くお勧めします。

トピック

- 保管中のデータの暗号化
- 転送中のデータの暗号化

保管中のデータの暗号化

評価を実行中に Amazon Inspector Classic エージェントによって生成されるテレメトリデータは JSON ファイルにフォーマットされています。これらのファイルは、TLS 経由でnear-real-time Amazon Inspector Classic に配信され、per-assessment-runエフェメラル AWS KMS派生キーで暗号化されます。

ファイルは、Amazon Inspector Classic 専用の S3 バケットに安全に保存されます。Amazon Inspector Classic のルールエンジンは、次のことを行います。

- S3 バケット内の暗号化されたテレメトリデータにアクセスします。
- メモリ内でそのデータを復号します。
- 設定された評価ルールに対してデータを処理し、結果を生成します。

転送中のデータの暗号化

マネージドサービスである Amazon Inspector Classic は、 AWS グローバルネットワークセキュリティで保護されています。 AWS セキュリティサービスと がインフラストラクチャ AWS を保護する方法については、AWS 「 クラウドセキュリティ」を参照してください。インフラストラクチャセキュリティのベストプラクティスを使用して環境を AWS 設計するには、「Security Pillar AWS Well-Architected Framework」の「Infrastructure Protection」を参照してください。

AWS 公開された API コールを使用して、ネットワーク経由で Amazon Inspector Classic にアクセスします。クライアントは次をサポートする必要があります。

- Transport Layer Security (TLS)。TLS 1.2 が必須で、TLS 1.3 をお勧めします。
- DHE (楕円ディフィー・ヘルマン鍵共有) や ECDHE (楕円曲線ディフィー・ヘルマン鍵共有) などの完全前方秘匿性 (PFS) による暗号スイート。これらのモードは Java 7 以降など、ほとんどの最新システムでサポートされています。

Amazon Inspector ClassicのアイデンティティとAccess Management

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS のサービス するのに役立つ です。IAM 管理者は、誰を認証 (サインイン) し、誰に Amazon Inspector リソースの使用を承認 (許可を付与) するかを制御します。IAM は、追加料金なしで使用できる AWS のサービス です。

トピック

- オーディエンス
- アイデンティティを使用した認証
- ポリシーを使用したアクセスの管理
- Amazon Inspector Classic と IAM の連携
- 例 2: Amazon Inspector の検出結果に対する describe および list オペレーションのみの実行をユーザーに許可する
- Amazon Inspector のポリシーリソース
- Amazon Inspector のポリシー条件キー
- Amazon Inspector の ACL
- Amazon Inspector と ABAC
- Amazon Inspector での一時的な認証情報の使用
- Amazon Inspector のクロスサービスプリンシパル許可
- Amazon Inspector のサービスロール
- Amazon Inspector でのサービスにリンクされたロール
- Amazon Inspector Classic のアイデンティティベースのポリシーの例
- Amazon Inspector Classic でのサービスにリンクされたロールの使用
- Amazon Inspector Classic アイデンティティとアクセスのトラブルシューティング

オーディエンス

AWS Identity and Access Management (IAM) の使用方法は、ロールによって異なります。

- サービスユーザー - 機能にアクセスできない場合は、管理者にアクセス許可をリクエストします (「Amazon Inspector Classic アイデンティティとアクセスのトラブルシューティング」を参照)。
- サービス管理者 - ユーザーアクセスを決定し、アクセス許可リクエストを送信します (「Amazon Inspector Classic と IAM の連携」を参照)
- IAM 管理者 - アクセスを管理するためのポリシーを作成します (「Amazon Inspector Classic のアイデンティティベースのポリシーの例」を参照)

アイデンティティを使用した認証

認証とは、ID 認証情報 AWS を使用して にサインインする方法です。、IAM ユーザー AWS アカウントのルートユーザー、または IAM ロールを引き受けることで認証される必要があります。

(AWS IAM アイデンティティセンター IAM Identity Center)、シングルサインオン認証、Google/Facebook 認証情報などの ID ソースからの認証情報を使用して、フェデレーティッド ID としてサインインできます。サインインの詳細については、「AWS サインイン ユーザーガイド」の「AWS アカウントにサインインする方法」を参照してください。

プログラムによるアクセスの場合、 は SDK と CLI AWS を提供してリクエストを暗号化して署名します。詳細については、「IAM ユーザーガイド」の「API リクエストに対するAWS 署名バージョン 4」を参照してください。

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、まず、すべての AWS のサービス および リソースへの完全なアクセス権を持つ AWS アカウント root ユーザーと呼ばれる 1 つのサインイン ID から始めます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザー認証情報を必要とするタスクについては、「IAM ユーザーガイド」の「ルートユーザー認証情報が必要なタスク」を参照してください。

フェデレーテッドアイデンティティ

ベストプラクティスとして、人間のユーザーが一時的な認証情報 AWS のサービス を使用して にアクセスするには、ID プロバイダーとのフェデレーションを使用する必要があります。

フェデレーティッド ID は、エンタープライズディレクトリ、ウェブ ID プロバイダー、または ID ソースの認証情報 AWS のサービス を使用して Directory Service にアクセスするユーザーです。フェデレーテッドアイデンティティは、一時的な認証情報を提供するロールを引き受けます。

アクセスを一元管理する場合は、 AWS IAM アイデンティティセンターをお勧めします。詳細については、「AWS IAM アイデンティティセンター ユーザーガイド」の「IAM アイデンティティセンターとは」を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、特定の個人やアプリケーションに対する特定のアクセス許可を持つアイデンティティです。長期認証情報を持つ IAM ユーザーの代わりに一時的な認証情報を使用することをお勧めします。詳細については、IAM ユーザーガイドの「ID プロバイダーとのフェデレーションを使用して にアクセスする必要がある AWS」を参照してください。

IAM グループは、IAM ユーザーの集合を指定し、大量のユーザーに対するアクセス許可の管理を容易にします。詳細については、「IAM ユーザーガイド」の「IAM ユーザーに関するユースケース」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可を持つアイデンティであり、一時的な認証情報を提供します。ユーザーから IAM ロール (コンソール) に切り替えるか、 または API オペレーションを呼び出すことで、ロールを引き受けることができます。 AWS CLI AWS 詳細については、「IAM ユーザーガイド」の「ロールを引き受けるための各種方法」を参照してください。

IAM ロールは、フェデレーションユーザーアクセス、一時的な IAM ユーザーのアクセス許可、クロスアカウントアクセス、クロスサービスアクセス、および Amazon EC2 で実行するアプリケーションに役立ちます。詳細については、IAM ユーザーガイド の IAM でのクロスアカウントリソースアクセス を参照してください。

ポリシーを使用したアクセスの管理

でアクセスを制御する AWS には、ポリシーを作成し、ID AWS またはリソースにアタッチします。ポリシーは、アイデンティティまたはリソースに関連付けられたときにアクセス許可を定義します。は、プリンシパルがリクエストを行うときにこれらのポリシー AWS を評価します。ほとんどのポリシーは JSON ドキュメント AWS として に保存されます。JSON ポリシードキュメントの詳細については、「IAM ユーザーガイド」の「JSON ポリシー概要」を参照してください。

管理者は、ポリシーを使用して、どのプリンシパルがどのリソースに対して、どのような条件でアクションを実行できるかを定義することで、誰が何にアクセスできるかを指定します。

デフォルトでは、ユーザーやロールにアクセス許可はありません。IAM 管理者は IAM ポリシーを作成してロールに追加し、このロールをユーザーが引き受けられるようにします。IAM ポリシーは、オペレーションの実行方法を問わず、アクセス許可を定義します。

アイデンティティベースのポリシー

アイデンティティベースのポリシーは、アイデンティティ (ユーザー、グループ、またはロール) にアタッチできる JSON アクセス許可ポリシードキュメントです。これらのポリシーは、アイデンティティがどのリソースに対してどのような条件下でどのようなアクションを実行できるかを制御します。アイデンティティベースポリシーの作成方法については、IAM ユーザーガイド の カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する を参照してください。

アイデンティティベースのポリシーは、インラインポリシー (単一の ID に直接埋め込む) または管理ポリシー (複数の ID にアタッチされたスタンドアロンポリシー) にすることができます。管理ポリシーとインラインポリシーのいずれかを選択する方法については、「IAM ユーザーガイド」の「管理ポリシーとインラインポリシーのいずれかを選択する」を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。例としては、IAM ロール信頼ポリシーや Amazon S3 バケットポリシーなどがあります。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシーでは、IAM の AWS マネージドポリシーを使用できません。

その他のポリシータイプ

AWS は、より一般的なポリシータイプによって付与されるアクセス許可の最大数を設定できる追加のポリシータイプをサポートしています。

- アクセス許可の境界 – アイデンティティベースのポリシーで IAM エンティティに付与することのできるアクセス許可の数の上限を設定します。詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可境界」を参照してください。
- サービスコントロールポリシー (SCP) - AWS Organizations内の組織または組織単位の最大のアクセス許可を指定します。詳細については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシー」を参照してください。

- リソースコントロールポリシー (RCP) – は、アカウント内のリソースで利用できる最大数のアクセス許可を定義します。詳細については、「AWS Organizations ユーザーガイド」の「リソースコントロールポリシー (RCP)」を参照してください。
- セッションポリシー – ロールまたはフェデレーションユーザーの一時セッションを作成する際にパラメータとして渡される高度なポリシーです。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成されるアクセス許可を理解するのがさらに難しくなります。が複数のポリシータイプが関与する場合にリクエストを許可するかどうか AWS を決定する方法については、「IAM ユーザーガイド」の「ポリシー評価ロジック」を参照してください。

Amazon Inspector Classic と IAM の連携

IAM を使用して Amazon Inspector へのアクセスを管理する前に、Amazon Inspectorで使用できる IAM 機能について理解しておく必要があります。

Amazon Inspector Classic で使用できる IAM の機能

IAM 機能	Amazon Inspector のサポート
アイデンティティベースのポリシー	あり
リソースベースのポリシー	なし
ポリシーアクション	あり
ポリシーリソース	はい
ポリシー条件キー (サービス固有)	はい
ACL	なし
ABAC (ポリシー内のタグ)	部分的
一時認証情報	あり

IAM 機能	Amazon Inspector のサポート
プリンシパルアクセス権限	あり
サービスロール	いいえ
サービスリンクロール	はい

Amazon Inspector およびその他の AWS のサービスがほとんどの IAM 機能と連携する方法の概要については、IAM ユーザーガイドのAWS 「IAM と連携する のサービス」を参照してください。

Amazon Inspector アイデンティティベースのポリシー

アイデンティティベースのポリシーのサポート: あり

アイデンティティベースポリシーは、IAM ユーザー、ユーザーグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」を参照してください。

IAM アイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、およびアクションを許可または拒否する条件を指定できます。JSON ポリシーで使用できるすべての要素について学ぶには、「IAM ユーザーガイド」の「IAM JSON ポリシーの要素のリファレンス」を参照してください。

Amazon Inspector アイデンティティベースのポリシーの例

Amazon Inspector アイデンティティベースのポリシーの例は、「Amazon Inspector Classic のアイデンティティベースのポリシーの例」でご確認ください。

Amazon Inspector内のリソースベースのポリシー

リソースベースのポリシーのサポート: なし

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシー や Amazon S3 バケットポリシー があげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスをコントロールできます。ポリシーがアタッチされているリ

ソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーで、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

クロスアカウントアクセスを有効にするには、全体のアカウント、または別のアカウントの IAM エンティティを、リソースベースのポリシーのプリンシパルとして指定します。詳細については、IAM ユーザーガイドのIAM でのクロスアカウントリソースアクセスを参照してください。

Amazon Inspector のポリシーアクション

ポリシーアクションのサポート: あり

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

JSON ポリシーの `Action` 要素にはポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。このアクションは関連付けられたオペレーションを実行するためのアクセス許可を付与するポリシーで使用されます。

Amazon Inspector アクションのリストを確認するには、「サービス認可リファレンス」のAmazon Inspector Classic で定義されるアクション」を参照してください。

Amazon Inspector のポリシーアクションは、アクションの前にプレフィックスを使用します。

```
inspector
```

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。

```
"Action": [
      "inspector:action1",
      "inspector:action2"
         ]
```

以下のアクセス許可ポリシーは、`Describe` および `List` で始まるすべての オペレーションを実行するためのユーザーアクセス許可を付与します。これらのオペレーションは、評価ターゲットや検出結果など、Amazon Inspector リソースに関する情報を表示します。`Resource` 要素内のワイルド

カード文字 (*) は、アカウントによって所有されるすべての Amazon Inspector リソースに対してそれらのオペレーションが許可されることを示します。

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action": [
            "inspector:Describe*",
            "inspector:List*"
            ],
         "Resource":"*"
      }
   ]
}
```

例 2: Amazon Inspector の検出結果に対する describe および list オペレーションのみの実行をユーザーに許可する

以下のアクセス許可ポリシーは、`ListFindings` および `DescribeFindings` オペレーションのみを実行するためのユーザーアクセス許可を付与します。これらのオペレーションは Amazon Inspector の検出結果に関する情報を表示します。`Resource` 要素内のワイルドカード文字 (*) は、アカウントによって所有されるすべての Amazon Inspector リソースに対してそれらのオペレーションが許可されることを示します。

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action": [
                  "inspector:DescribeFindings",
                  "inspector:ListFindings"
         ],
```

```
            "Resource":"*"
        }
    ]
}
```

Amazon Inspector アイデンティティベースのポリシーの例は、「Amazon Inspector Classic のアイデンティティベースのポリシーの例」でご確認ください。

Amazon Inspector のポリシーリソース

ポリシーリソースのサポート: あり

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

`Resource` JSON ポリシー要素はアクションが適用されるオブジェクトを指定します。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。リソースレベルのアクセス許可をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

```
"Resource": "*"
```

Amazon Inspectorリソースのタイプとその ARN のリストを確認するには、「サービス認可リファレンス」の「Amazon Inspector Classicで定義されるリソース」を参照してください。どのアクションで各リソースの ARN を指定できるかについては、「Amazon Inspector Classic で定義されるアクション」を参照してください。

Amazon Inspector アイデンティティベースのポリシーの例は、「Amazon Inspector Classic のアイデンティティベースのポリシーの例」でご確認ください。

Amazon Inspector のポリシー条件キー

サービス固有のポリシー条件キーのサポート: あり

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

Condition 要素は、定義された基準に基づいてステートメントが実行される時期を指定します。イコールや未満などの条件演算子を使用して条件式を作成して、ポリシーの条件とリクエスト内の値を一致させることができます。すべての AWS グローバル条件キーを確認するには、IAM ユーザーガイドのAWS 「グローバル条件コンテキストキー」を参照してください。

Amazon Inspector 条件キーのリストを確認するには、「サービス認可リファレンス」のAmazon Inspector Classic の条件キー」を参照してください。どのアクションやリソースで条件キーを使用できるかについては、「Amazon Inspectorで定義されるアクション」を参照してください。

Amazon Inspector アイデンティティベースのポリシーの例は、「Amazon Inspector Classic のアイデンティティベースのポリシーの例」でご確認ください。

Amazon Inspector の ACL

ACL のサポート: なし

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするためのアクセス許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Amazon Inspector と ABAC

ABAC (ポリシー内のタグ) のサポート: 一部

属性ベースのアクセスコントロール (ABAC) は、タグと呼ばれる属性に基づいてアクセス許可を定義する認可戦略です。IAM エンティティと AWS リソースにタグをアタッチし、プリンシパルのタグがリソースのタグと一致するときにオペレーションを許可するように ABAC ポリシーを設計できます。

タグに基づいてアクセスを管理するには、aws:ResourceTag/*key-name*、aws:RequestTag/*key-name*、または aws:TagKeys の条件キーを使用して、ポリシーの条件要素でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値はありです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。

ABAC の詳細については、「IAM ユーザーガイド」の「ABAC 認可でアクセス許可を定義する」を参照してください。ABAC をセットアップする手順を説明するチュートリアルについては、「IAM

ユーザーガイド」の「属性ベースのアクセスコントロール (ABAC) を使用する」を参照してください。

Amazon Inspector での一時的な認証情報の使用

一時的な認証情報のサポート: あり

一時的な認証情報は、 AWS リソースへの短期的なアクセスを提供し、フェデレーションまたはスイッチロールの使用時に自動的に作成されます。長期的なアクセスキーを使用する代わりに、一時的な認証情報を動的に生成 AWS することをお勧めします。詳細については、「IAM ユーザーガイド」の「IAM の一時的な認証情報」および「AWS のサービス と IAM との連携」を参照してください。

Amazon Inspector のクロスサービスプリンシパル許可

転送アクセスセッション (FAS) のサポート: あり

転送アクセスセッション (FAS) は、 を呼び出すプリンシパルのアクセス許可と AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストをリクエストする を使用します。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

Amazon Inspector のサービスロール

サービスロールのサポート: なし

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、IAM ユーザーガイドの AWS のサービスに許可を委任するロールを作成するを参照してください。

> **Warning**
>
> サービスロールの許可を変更すると、Amazon Inspectorの機能が破損する可能性があります。Amazon Inspector が指示する場合以外は、サービスロールを編集しないでください。

Amazon Inspector でのサービスにリンクされたロール

サービスリンクロールのサポート: あり

サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスリンクロールのアクセス許可を表示できますが、編集することはできません。

Amazon Inspector サービスにリンクされたロールの作成または管理の詳細については、「Amazon Inspector Classic でのサービスにリンクされたロールの使用」を参照してください。

Amazon Inspector Classic のアイデンティティベースのポリシーの例

デフォルトでは、ユーザーおよびロールにはAmazon Inspectorリソースを作成または変更する許可はありません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。

これらのサンプルの JSON ポリシードキュメントを使用して IAM アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「IAM ポリシーを作成する (コンソール)」を参照してください。

各リソースタイプの ARN の形式など、Amazon Inspector で定義されるアクションとリソースタイプの詳細については、「サービス認可リファレンス」のAmazon Inspector Classic のアクション、リソース、および条件キー」を参照してください。 ARNs

トピック

- ポリシーに関するベストプラクティス
- Amazon Inspector コンソールの使用
- 自分の権限の表示をユーザーに許可する
- Amazon Inspectorの検出結果に対する、説明とリスト操作のみの実行をユーザーに許可します。

ポリシーに関するベストプラクティス

ID ベースのポリシーは、ユーザーのアカウント内で誰かが Amazon Inspectorリソースを作成、アクセス、または削除できるどうかを決定します。これらのアクションでは、 AWS アカウントに費用が発生する場合があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行 – ユーザーとワークロードにアクセス許可の付与を開始するには、多くの一般的なユースケースにアクセス許可を付与するAWS 管理

ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義することで、アクセス許可をさらに減らすことをお勧めします。詳細については、IAM ユーザーガイド の AWS マネージドポリシー または ジョブ機能のAWS マネージドポリシー を参照してください。

- 最小特権を適用する – IAM ポリシーでアクセス許可を設定する場合は、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、IAM ユーザーガイド の IAM でのポリシーとアクセス許可 を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。たとえば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。条件を使用して、サービスアクションが などの特定の を通じて使用されている場合に AWS のサービス、サービスアクションへのアクセスを許可することもできます CloudFormation。詳細については、IAM ユーザーガイド の IAM JSON ポリシー要素:条件 を参照してください。
- IAM アクセスアナライザー を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM アクセスアナライザー は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、IAM ユーザーガイド の IAM Access Analyzer でポリシーを検証する を参照してください。
- 多要素認証 (MFA) を要求する – で IAM ユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、MFA をオンにしてセキュリティを強化します。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、IAM ユーザーガイド の MFA を使用した安全な API アクセス を参照してください。

IAM でのベストプラクティスの詳細については、IAM ユーザーガイド の IAM でのセキュリティのベストプラクティス を参照してください。

Amazon Inspector コンソールの使用

Amazon Inspector Classic コンソールにアクセスするには、許可の最小限のセットが必要です。アクセス許可により、 AWS アカウントの Amazon Inspector リソースの詳細をリストおよび表示できます。最小限必要な許可よりも制限が厳しいアイデンティティベースのポリシーを作成すると、そのポリシーを持つエンティティ (ユーザーまたはロール) に対してコンソールが意図したとおりに機能しません。

AWS CLI または AWS API のみを呼び出すユーザーには、最小限のコンソールアクセス許可を付与する必要はありません。代わりに、実行しようとしている API オペレーションに一致するアクションのみへのアクセスが許可されます。

ユーザーとロールが引き続き Amazon Inspector コンソールを使用できるようにするには、エンティティに Amazon Inspector *ConsoleAccess*または *ReadOnly* AWS 管理ポリシーもアタッチします。詳細については、「IAM ユーザーガイド」の「ユーザーへのアクセス許可の追加」を参照してください。

自分の権限の表示をユーザーに許可する

この例では、ユーザーアイデンティティにアタッチされたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーの作成方法を示します。このポリシーには、コンソールで、または AWS CLI または AWS API を使用してプログラムでこのアクションを実行するアクセス許可が含まれています。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
```

```
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Amazon Inspectorの検出結果に対する、説明とリスト操作のみの実行をユーザーに許可します。

以下のアクセス許可ポリシーは、ListFindings および DescribeFindings オペレーションのみを実行するためのユーザーアクセス許可を付与します。これらのオペレーションは Amazon Inspector の検出結果に関する情報を表示します。Resource 要素内のワイルドカード文字 (*) は、アカウントによって所有されるすべての Amazon Inspector リソースに対してそれらのオペレーションが許可されることを示します。

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action": [
                  "inspector:DescribeFindings",
                  "inspector:ListFindings"
         ],
         "Resource":"*"
      }
   ]
}
```

Amazon Inspector Classic でのサービスにリンクされたロールの使用

Amazon Inspector Classic は AWS Identity and Access Management (IAM) サービスにリンクされたロールを使用します。サービスリンクロールは、Amazon Inspector Classic に直接リンクされた特殊

なタイプの IAM ロールです。サービスリンクロールは Amazon Inspector Classic によって事前に定義されており、サービスがユーザーに代わって その他の AWS のサービス を呼び出すために必要なすべての許可が含まれています。

必要な許可を手動で追加する必要がないため、サービスリンクロールは Amazon Inspector Classic のセットアップを容易にします。サービスリンクロールの許可は Amazon Inspector Classic が定義し、別段の定義がない限り、Amazon Inspector Classic のみがそのロールを引き受けることができます。定義されるアクセス許可には、信頼ポリシーと許可ポリシーが含まれており、その許可ポリシーを他の IAM エンティティにアタッチすることはできません。

サービスリンクロールを削除するには、まずその関連リソースを削除します。これにより、リソースへの意図しないアクセスによる許可の削除が防止され、 Amazon Inspector Classic リソースは保護されます。

サービスにリンクされたロールをサポートする他のサービスの詳細については、AWS「IAM と連携するサービス」を参照し、「サービスにリンクされたロール」列で「はい」を持つサービスを探します。サービスにリンクされたロールに関するドキュメントをサービスで表示するには、はい リンクを選択します。

Amazon Inspector Classic のサービスにリンクされたロールの許可

Amazon Inspector Classic は、AWSServiceRoleForAmazonInspector – ServiceLinkedRoleDescription という名前のサービスリンクロールを使用します。

AWSServiceRoleForAmazonInspector サービスにリンクされたロールは、以下のサービスを信頼してロールを引き受けます。

- `inspector.amazonaws.com`

AmazonInspectorServiceRolePolicy という名前のロールのアクセス許可ポリシーは、指定したリソースに対して以下のアクションを実行することを Amazon Inspector に許可します。

- アクション: `iam:CreateServiceLinkedRole`。対象リソース: `arn:aws:iam::*:role/aws-service-role/inspector.amazonaws.com/AWSServiceRoleForAmazonInspector`

サービスにリンクされたロールの作成、編集、削除を IAM エンティティ (IAM ユーザー、グループ、ロールなど) に許可するには、許可を設定する必要があります。詳細についてはIAM ユーザーガイドの「サービスにリンクされた役割のアクセス許可」を参照してください。

Amazon Inspector Classic のサービスリンクロールの作成

サービスリンクロールを手動で作成する必要はありません。 AWS マネジメントコンソール、、AWS CLIまたは AWS API で CompleteThisCreateActionInThisServiceと、Amazon Inspector Classic がサービスにリンクされたロールを作成します。

Amazon Inspector Classic のサービスリンクロールの編集

Amazon Inspector は、AWSServiceRoleForAmazonInspector サービスリンクロールの編集を許可しません。サービスリンクロールの作成後は、さまざまなエンティティがロールを参照する可能性があるため、ロール名を変更することはできません。ただし、IAM を使用してロールの説明を編集することはできます。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの編集」を参照してください。

Amazon Inspector Classic のサービスリンクロールの削除

サービスリンクロールを必要とする機能やサービスが不要になった場合は、ロールを削除することをお勧めします。そうすることで、使用していないエンティティがアクティブにモニタリングされたり、メンテナンスされたりすることがなくなります。ただし、手動で削除する前に、サービスリンクロールのリソースをクリーンアップする必要があります。

> **Note**
>
> リソースを削除しようとしているときに Amazon Inspector Classic サービスがロールを使用している場合は、削除が失敗する可能性があります。失敗した場合は数分待ってから操作を再試行してください。

`AWSServiceRoleForAmazonInspector` で使用されている Amazon Inspector Classic リソースを削除するには

- Amazon Inspector Classic を実行しているすべての AWS アカウント で、 AWS リージョン この評価ターゲットを削除します。詳細については、「Amazon Inspector Classic 評価ターゲット」を参照してください。

サービスリンクロールを IAM で手動削除するには

IAM コンソール、 AWS CLI、または AWS API を使用して、AWSServiceRoleForAmazonInspector サービスにリンクされたロールを削除します。詳細については、「IAM ユーザーガイド」の「サービスにリンクされたロールの削除」を参照してください。

Amazon Inspector Classicのサービスにリンクされたロールをサポートするリージョン

Amazon Inspector は、サービスが利用可能なすべてのリージョンでサービスにリンクされたロールの使用をサポートします。詳細については、「AWS リージョンとエンドポイント」を参照してください。

Amazon Inspector Classic アイデンティティとアクセスのトラブルシューティング

以下の情報を使用して、Amazon Inspector と IAM の使用時に発生する可能性がある一般的な問題の診断と修正に役立てます。

トピック

- Amazon Inspector でアクションを実行する認可がない
- iam:PassRole を実行する権限がありません
- 自分の 以外のユーザーに Amazon Inspector リソース AWS アカウント へのアクセスを許可したい

Amazon Inspector でアクションを実行する認可がない

あるアクションを実行するアクセス許可がないというエラーが表示された場合、そのアクションを実行できるようにポリシーを更新する必要があります。

次のエラー例は、mateojackson IAM ユーザーがコンソールを使用して、ある *my-example-widget* リソースに関する詳細情報を表示しようとしたことを想定して、その際に必要な inspector:*GetWidget* アクセス許可を持っていない場合に発生するものです。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 inspector:GetWidget on resource: my-example-widget
```

この場合、inspector:*GetWidget* アクションを使用して *my-example-widget* リソースへのアクセスを許可するように、mateojackson ユーザーのポリシーを更新する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン認証情報を提供した担当者が管理者です。

iam:PassRole を実行する権限がありません

`iam:PassRole` アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新して Amazon Inspector にロールを渡せるようにする必要があります。

一部の AWS のサービス では、新しいサービスロールまたはサービスにリンクされたロールを作成する代わりに、そのサービスに既存のロールを渡すことができます。そのためには、サービスにロールを渡すアクセス許可が必要です。

以下のエラーの例は、`marymajor` という名前の IAM ユーザーがコンソールを使用して Amazon Inspector でアクションを実行しようする場合に発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与されたアクセス許可が必要です。Mary には、ロールをサービスに渡すアクセス許可がありません。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

この場合、Mary のポリシーを更新してメアリーに `iam:PassRole` アクションの実行を許可する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン資格情報を提供した担当者が管理者です。

自分の 以外のユーザーに Amazon Inspector リソース AWS アカウント へのアクセスを許可したい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセスコントロールリスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください:

- Amazon Inspector がこれらの機能をサポートしているかどうかを確認するには、「Amazon Inspector Classic と IAM の連携」を参照してください。
- 所有 AWS アカウント している のリソースへのアクセスを提供する方法については、IAM ユーザーガイドの「所有 AWS アカウント している別の の IAM ユーザーへのアクセスを提供する」を参照してください。

- リソースへのアクセスをサードパーティーに提供する方法については AWS アカウント、IAM ユーザーガイドの「サードパーティー AWS アカウント が所有する へのアクセスを提供する」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、IAM ユーザーガイド の 外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可 を参照してください。
- クロスアカウントアクセスにおけるロールとリソースベースのポリシーの使用方法の違いについては、IAM ユーザーガイド の IAM でのクロスアカウントのリソースへのアクセス を参照してください。

Amazon Inspector Classic でのログ記録とモニタリング

Amazon Inspector Classic は AWS CloudTrail、Amazon Inspector Classic のユーザー、ロール、または のサービスによって実行されたアクションを記録する AWS サービスである と統合されています。CloudTrail は、Amazon Inspector Classic コンソールからの呼び出しと Amazon Inspector Classic API オペレーションへのコード呼び出しを含む、Amazon Inspector Classic の API コールをイベントとしてキャプチャします。

Amazon Inspector Classic で CloudTrail ロギングを使用する方法については、「を使用した Amazon Inspector Classic API コールのログ記録 AWS CloudTrail」を参照してください。

Amazon CloudWatch を使用して Amazon Inspector Classic をモニタリングすることで、raw データを収集し、リアルタイムに近い読み取り可能なメトリクスに加工することができます。デフォルトでは、Amazon Inspector Classic は 5 分ごとにメトリクスデータを CloudWatch に送信します。

CloudWatch を Amazon Inspector Classic で使用する方法については、「Amazon CloudWatch を使用した Amazon Inspector Classic のモニタリング」を参照してください。

Amazon Inspector Classic でのインシデントへの対応

Amazon Inspector Classic のインシデント対応は AWS 責任です。 AWS には、インシデント対応を管理する正式な文書化されたポリシーとプログラムがあります。

AWS 広範な影響を与える運用上の問題は、AWS Service Health Dashboard に投稿されます。

運用上の問題も、 AWS Health Dashboardを介して個々のアカウントに投稿されます。の使用方法については Health Dashboard、AWS Health 「 ユーザーガイド」を参照してください。

Amazon Inspector Classic のコンプライアンス検証

サードパーティーの監査者は、複数のコンプライアンスプログラムの一環として Amazon Inspector Classic のセキュリティと AWS コンプライアンスを評価します。これらのプログラムには、SOC、PCI、FedRAMP、HIPAA などがあります。

特定のコンプライアンスプログラムの対象となる AWS サービスのリストについては、「コンプライアンスプログラムによる AWS 対象範囲内のサービスコンプライアンス」を参照してください。一般的な情報については、AWS 「 Compliance ProgramsAssurance」を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、Downloading Reports in AWS および を参照してください。

Amazon Inspector Classic を使用する際のお客様のコンプライアンス責任は、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。 は、コンプライアンスに役立つ以下のリソース AWS を提供します。

- 「セキュリティ & コンプライアンスクイックリファレンスガイド」 – これらのデプロイガイドには、アーキテクチャ上の考慮事項の説明と、 AWSでセキュリティとコンプライアンスに重点を置いたベースライン環境をデプロイするための手順が記載されています。
- アマゾン ウェブ サービスでの HIPAA セキュリティとコンプライアンスのアーキテクチャ – このホワイトペーパーでは、企業が AWS を使用して HIPAA 準拠のアプリケーションを作成する方法について説明します。
- AWS コンプライアンスリソース – このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- 「 デベロッパーガイド」の「ルールによるリソースの評価」 – この AWS Config サービスは、リソース設定が内部プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。 AWS Config
- AWS Security Hub CSPM – この AWS サービスは、 内のセキュリティ状態を包括的に把握 AWS し、セキュリティ業界標準とベストプラクティスへの準拠を確認するのに役立ちます。

Amazon Inspector Classic の耐障害性

AWS グローバルインフラストラクチャは、 AWS リージョンとアベイラビリティーゾーンを中心に構築されています。 AWS リージョンは、低レイテンシー、高スループット、高度に冗長なネットワークで接続された、物理的に分離された複数のアベイラビリティーゾーンを提供します。アベイラ

ビリティーゾーンでは、ゾーン間で中断することなく自動的にフェールオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性、フォールトトレランス、および拡張性が優れています。

AWS リージョンとアベイラビリティーゾーンの詳細については、AWS 「 グローバルインフラストラクチャ」を参照してください。

Amazon Inspector Classic は可用性が高く、複数のアベイラビリティーゾーンにまたがるコンピューティングリソースを使用してクエリを実行します。特定のアベイラビリティーゾーンに到達できない場合、クエリは自動的に適切にルーティングされます。

Amazon Inspector Classic は、その基盤となるデータストアとして Amazon S3 を使用しているため、データの可用性と耐久性が向上します。Amazon S3 は重要なデータを保存するための耐久性に優れたインフラストラクチャを提供します。オブジェクトの 99.999999999% の耐久性を持つよう設計されています。データは複数の施設間で冗長化され、各施設で複数のデバイスに保存されます。

Amazon Inspector Classic のインフラストラクチャのセキュリティ

マネージドサービスである Amazon Inspector Classic は、 AWS グローバルネットワークセキュリティで保護されています。 AWS セキュリティサービスと がインフラストラクチャ AWS を保護する方法については、AWS 「 クラウドセキュリティ」を参照してください。インフラストラクチャセキュリティのベストプラクティスを使用して環境を AWS 設計するには、「Security Pillar AWS Well-Architected Framework」の「Infrastructure Protection」を参照してください。

AWS 公開された API コールを使用して、ネットワーク経由で Amazon Inspector Classic にアクセスします。クライアントは次をサポートする必要があります。

- Transport Layer Security (TLS)。TLS 1.2 が必須で、TLS 1.3 をお勧めします。
- DHE (楕円ディフィー・ヘルマン鍵共有) や ECDHE (楕円曲線ディフィー・ヘルマン鍵共有) などの完全前方秘匿性 (PFS) による暗号スイート。これらのモードは Java 7 以降など、ほとんどの最新システムでサポートされています。

Amazon Inspector Classic ネットワークおよびエージェントのセキュリティの詳細については「the section called “ネットワークと Amazon Inspector Classic エージェントのセキュリティ”」 を参照してください。

Amazon Inspector Classic での設定と脆弱性の分析

Amazon Inspector Classic には、評価対象の EC2 インスタンスのオペレーティングシステムにオプションでインストールできる、エージェントと呼ばれる定義済みソフトウェアがあります。エージェントは、テレメトリと呼ばれるさまざまな設定データを収集します。Amazon Inspector Classic エージェントの詳細については、「Amazon Inspector Classic エージェント」を参照してください。

Amazon Inspector Classic のセキュリティベストプラクティス

Amazon Inspector Classic には、独自のセキュリティポリシーを策定および実装する際に考慮すべきさまざまなセキュリティ機能が用意されています。これらのベストプラクティスは一般的なガイドラインであり、完全なセキュリティソリューションを提供するものではありません。これらのベストプラクティスはお客様の環境に適切ではないか、十分ではない場合があるため、これらは指示ではなく、有用な考慮事項と見なしてください。

Amazon Inspector Classic のセキュリティのベストプラクティスのリストについては、「the section called “Amazon Inspector Classic のセキュリティのベストプラクティス”」を参照してください。

Amazon Inspector Classic エージェント

Amazon Inspector Classic エージェントは、Amazon EC2 インスタンスのインストール済みパッケージ情報とソフトウェア設定を収集するエンティティです。すべてのケースで必要というわけではありませんが、セキュリティを完全に評価するためには、ターゲットの Amazon EC2 インスタンスに Amazon Inspector Classic エージェントをインストールする必要があります。

エージェントのインストール、アンインストール、再インストール、インストールされたエージェントが実行されているかどうかを確認する方法、エージェントのプロキシサポートの設定方法の詳細については、「Linux ベースのオペレーティングシステムでの Amazon Inspector Classic エージェントの操作」および「Windows ベースのオペレーティングシステムでの Amazon Inspector Classic エージェントの操作」を参照してください。

> **Note**
>
> Amazon Inspector エージェントは、ネットワーク到達可能性ルールパッケージを実行する必要はありません。

> **Important**
>
> Amazon Inspector Classic エージェントは、正常に機能するために Amazon EC2 インスタンスメタデータに依存します。インスタンスメタデータにアクセスするために、Instance Metadata Service のバージョン 1 または 2 (IMDSv1 または IMDSv2) を使用します。EC2 インスタンスメタデータおよびアクセス方法の詳細については、「インスタンスメタデータとユーザーデータ」を参照してください。

トピック

- Amazon Inspector Classic エージェントの権限
- ネットワークと Amazon Inspector Classic エージェントのセキュリティ
- Amazon Inspector Classic エージェントの更新
- テレメトリデータのライフサイクル
- Amazon Inspector Classic から AWS アカウントへのアクセスコントロール
- Amazon Inspector Classic エージェントの制限

- Amazon Inspector Classic エージェントのインストール
- Linux ベースのオペレーティングシステムでの Amazon Inspector Classic エージェントの操作
- Windows ベースのオペレーティングシステムでの Amazon Inspector Classic エージェントの操作
- (オプション) Linux ベースのオペレーティングシステムの Amazon Inspector Classic エージェントのインストールスクリプトの署名を確認します。
- 「オプショナル」 Windows ベースのオペレーティングシステムの Amazon Inspector Classic エージェントインストールスクリプトの署名を確認します。

Amazon Inspector Classic エージェントの権限

Amazon Inspector Classic エージェントをインストールするには、管理者権限または root 権限が必要です。サポートされている Linux ベースのオペレーティングシステムでは、エージェントは root アクセスで実行されるユーザーモード実行可能ファイルで構成されます。サポートされている Windows ベースのオペレーティングシステムでは、エージェントはアップデータサービスとエージェントサービスで構成され、それぞれ `LocalSystem` の特権を持つユーザーモードで実行されます。

ネットワークと Amazon Inspector Classic エージェントのセキュリティ

Amazon Inspector Classic エージェントは、Amazon Inspector Classic サービスとのすべての通信を開始します。つまりエージェントには、テレメトリデータをエンドポイントに送信できるように、パブリックの のエンドポイントへのアウトバウンドネットワークパスが必要です。たとえば、エージェントが `arsenal.<region>.amazonaws.com` に接続するか、エンドポイントが の `s3.dualstack.<region>.amazonaws.com` Amazon S3 バケットである場合です。を Amazon Inspector Classic を実行している実際の AWS リージョン`<region>`に置き換えてください。詳細については、「AWS IP アドレスの範囲」を参照してください。さらに、エージェントからのすべての接続はアウトバウンドで確立されるため、セキュリティグループでポートを開き、Amazon Inspector Classic からエージェントへのインバウンド通信を許可する必要はありません。

エージェントは、TLS で保護されたチャネルを介して Amazon Inspector Classic と定期的に通信します。このチャネルは、EC2 インスタンスのロールに関連付けられた AWS ID、またはロールが割り当てられていない場合はインスタンスのメタデータドキュメントを使用して認証されます。認証されると、エージェントはサービスにハートビートメッセージを送信し、レスポンスとしてサービスから手順を受信します。評価がスケジュールされている場合、エージェントはその評価の手順を受信し

ます。これらの手順は構造化された JSON ファイルであり、エージェントで事前設定された特定のセンサーを有効または無効にするようにエージェントに指示します。それぞれの手順のアクションはエージェント内で事前に定義されています。任意の手順を実行することはできません。

評価中に、エージェントはシステムからテレメトリデータを収集し、TLS 保護チャネル経由で Amazon Inspector Classic に送り返します。エージェントは、データの収集元のシステムに変更を行いません。データを収集したら、エージェントはテレメトリデータを処理のために Amazon Inspector Classic に送信します。エージェントには、生成するテレメトリデータ以外には、評価するシステムまたは評価ターゲットに関するその他のデータを収集または送信する機能はありません。現在、エージェントでテレメトリデータを傍受して検査するために公開されているメソッドはありません。

Amazon Inspector Classic エージェントの更新

Amazon Inspector Classic エージェントの更新が利用可能になると、Amazon S3 から自動的にダウンロードされ、適用されます。これにより、必要な依存関係も更新されます。自動更新機能により、EC2 インスタンスにインストールしたエージェントのバージョニングを追跡して手動で維持する必要がなくなります。すべての更新は、該当するセキュリティ基準に準拠するため、監査された Amazon 変更管理プロセスに従っています。

さらにエージェントのセキュリティを確保するため、エージェントと自動更新リリースサイト (S3) 間のすべての通信は TLS 接続で実行され、サーバーが認証されます。自動更新プロセスに関連するすべてのバイナリはデジタル署名され、署名はインストール前にアップデータによって確認されます。自動更新プロセスは、評価以外の期間中にのみ実行されます。何らかのエラーが検出された場合、更新プロセスは更新をロールバックして再試行することができます。最後に、エージェント更新プロセスは、エージェント機能のみをアップグレードするのに役立ちます。アップデートワークフローの一部として、特定の情報がエージェントから Amazon Inspector Classic に送信されることはありません。更新プロセスの一部として通信される唯一の情報は基本的なインストールの成功/失敗のテレメトリであり、該当する場合は更新失敗の診断情報が含まれます。

テレメトリデータのライフサイクル

評価を実行中に Amazon Inspector Classic エージェントによって生成されるテレメトリデータは JSON ファイルにフォーマットされています。ファイルは TLS を介してほぼリアルタイムで Amazon Inspector Classic に配信され、そこで評価実行ごとにエフェメラル KMS 派生キーで暗号化されます。ファイルは、 Amazon Inspector Classic 専用の Amazon S3 バケットに安全に保存されます。Amazon Inspector Classic のルールエンジンは S3 バケットの暗号化テレメトリデータにアクセ

スし、これをメモリに復号します。設定された評価ルールに対してデータを処理し、結果を生成します。S3 に保存されているテレメトリデータは、サポートリクエストによる支援を可能にするためにのみ保持されます。これを他の目的のために Amazon が使用または集計することはありません。30 日後、テレメトリデータは Amazon Inspector Classic データの標準 S3 バケットライフサイクルポリシーに従って完全に削除されます。現在、Amazon Inspector Classic は収集したテレメトリに対して API または S3 バケットアクセスメカニズムを提供していません。

Amazon Inspector Classic から AWS アカウントへのアクセスコントロール

セキュリティサービスとして、Amazon Inspector Classic は、タグをクエリして評価する EC2 インスタンスを見つける必要がある場合にのみ、 AWS アカウントとリソースにアクセスします。これは、Amazon Inspector Classic サービスの初期セットアップ中に作成されたロールにより、標準 IAM アクセスを使って行われます。評価の間、環境とのすべての通信は、EC2 インスタンスにローカルでインストールされた Amazon Inspector Classic エージェントによって開始されます。評価ターゲット、評価テンプレート、サービスによって生成される結果など、ユーザーが作成する Amazon Inspector Classic サービスオブジェクトは、Amazon Inspector Classic によって管理され、Amazon Inspector Classic のみにアクセス可能なデータベースに保存されます。

Amazon Inspector Classic エージェントの制限

Amazon Inspector Classic エージェントの制限については「Amazon Inspector Classic サービスの制限」を参照してください。

Amazon Inspector Classic エージェントのインストール

Amazon Inspector Classic エージェントは、複数のインスタンス (Linux ベースおよび Windows ベースのインスタンスを含む) で Systems Manager Run Command を使用してインストールすることができます。または、それぞれの EC2 インスタンスにサインインしてエージェントを個別にインストールすることもできます。この章では、両方の方法について説明します。

別のオプションとして、コンソールの 評価ターゲットを定義 ページで インストール エージェント チェックボックスを選択して、評価ターゲットに含まれるすべての Amazon EC2 インスタンスにエージェントをすぐにインストールできます。

トピック

- Systems Manager Run Command を使用して複数の EC2 インスタンスにエージェントをインストールする
- Linux ベースの EC2 インスタンスにエージェントをインストールします。
- Windows ベースの EC2 インスタンスにエージェントをインストールするには

> **Note**
>
> この章の手順は、Amazon Inspector Classic でサポートされているすべての AWS リージョンに適用されます。

Systems Manager Run Command を使用して複数の EC2 インスタンスにエージェントをインストールする

また、Systems Manager Run Command を使用して EC2 インスタンスに Amazon Inspector Classic エージェントをインストールすることもできます。これにより、エージェントを複数のインスタンス (Linuxベースのインスタンスと Windowsベースのインスタンスの両方を同じコマンドで実行できる。) にリモートでインストールできます。

> **Important**
>
> Systems Manager Run Command を使用したエージェントのインストールは、現在 Debian オペレーティングシステムではサポートされていません。

> **Important**
>
> このオプションを使用するには、EC2 インスタンスに SSM エージェント がインストールされていて、Run Command を許可する IAM ロールがあることを確認します。SSM エージェント は、デフォルトでは、Amazon EC2 Windows インスタンスおよび Amazon Linux インスタンスにインストールされます。Amazon EC2 Systems Manager では、コマンドを処理する EC2 インスタンスの IAM ロールと、それとは別にコマンドを実行するユーザーのロールが必要です。詳細については、「SSM エージェントのインストールと設定」と「SSMのセキュリティロールの設定」を参照してください。

また、Systems Manager Run Command を使用して複数の EC2 インスタンスに エージェントをインストールするには

1. https://console.aws.amazon.com/systems-manager/ で AWS Systems Manager コンソールを開きます。
2. Node Tools のナビゲーションペインで、Run Command を選択します。
3. コマンドを実行を選択します。
4. コマンドのドキュメントで、Amazon が所有する AmazonInspector-ManageAWSエージェント という名前のドキュメントを選択します。このドキュメントには、EC2 インスタンスに Amazon Inspector Classic エージェントをインストールするスクリプトが含まれています。
5. ターゲット については、さまざまな方法を使用して EC2 インスタンスを選択できます。評価ターゲットのすべてのインスタンスにエージェントをインストールする場合は、その評価ターゲットの作成に使用したタグを指定できます。
6. 「コンソールからコマンドを実行する」の手順を使用して、利用可能なその他のオプションで選択し、実行 を選択します。

> **Note**
>
> 評価ターゲットを作成するときに、複数の EC2 インスタンス (Linux ベースと Windows ベースの両方) にエージェントをインストールすることもできます。または、既存のターゲットに対して 実行コマンドを実行してエージェントをインストール ボタンを使用することもできます。詳細については、評価ターゲットを作成するを参照してください。

Linux ベースの EC2 インスタンスにエージェントをインストールします。

以下の手順を実行して、Linux ベースの EC2 インスタンスに Amazon Inspector Classic エージェントをインストールします。

Linux ベースの EC2 インスタンスに エージェントをインストールするには

1. Amazon Inspector Classic エージェントをインストールする Linux ベースのオペレーティングシステムを実行している EC2 インスタンスにサインインします。

> **Note**
>
> Amazon Inspector Classic がサポートしているオペレーティングシステムの詳細については、Amazon Inspector Classic でサポートされているオペレーティングシステムとリージョンを参照してください。

2. 次のいずれかのコマンドを実行してエージェントのインストールスクリプトをダウンロードします。

   - wget https://inspector-agent.amazonaws.com/linux/latest/install
   - curl -O https://inspector-agent.amazonaws.com/linux/latest/install

3. (オプション) エージェントのインストールスクリプトに改変や破損がないことを確認します。詳細については、(オプション) Linux ベースのオペレーティングシステムの Amazon Inspector Classic エージェントのインストールスクリプトの署名を確認します。を参照してください。

4. エージェントをインストールするには、sudo bash install を実行します。

> **Note**
>
> SELinux 環境にエージェントをインストールする場合、Amazon Inspector Classic が制限されていないデーモンとして検出されることがあります。これを回避するには、エージェントプロセスのドメインをデフォルトの `initrc_t` から `bin_t` に変更します。SELinux のエージェントをインストールする前に、次のコマンドを実行して、Amazon Inspector Classic 実行スクリプトに `bin_t` コンテキストを割り当てます。
>
> ```
> sudo semanage fcontext -a -t bin_t /etc/rc\.d/init\.d/awsagent
> sudo semanage fcontext -a -t bin_t /etc/init\.d/awsagent
> ```

> **Note**
>
> エージェントの更新が利用可能になると、Amazon S3 から自動的にダウンロードされ、適用されます。詳細については、Amazon Inspector Classic エージェントの更新を参照してください。
>
> この自動更新プロセスをスキップする場合は、エージェントをインストールするときに、次のコマンドを実行します。
>
> ```
> sudo bash install -u false
> ```

> **Note**
>
> (オプション) エージェントのインストールスクリプトを削除するには、rm install を実行します。

5. エージェントが正常にインストールされて適切に機能するために必要な次のファイルがインストールされていることを確認します。

   - `libcurl4` (Ubuntu 18.04 にエージェントをインストールするために必要)
   - `libcurl3`
   - `libgcc1`
   - `libc6`
   - `libstdc++6`
   - `libssl1.0.1`
   - `libssl1.0.2` (Debian 9 にエージェントをインストールするために必要)
   - `libssl1.1` (Ubuntu 20.04 LTS にエージェントをインストールするために必要)
   - `libpcap0.8`

Windows ベースの EC2 インスタンスにエージェントをインストールするには

以下の手順を実行して、Windows ベースの EC2 インスタンスに Amazon Inspector Classic エージェントをインストールします。

Windows ベースの EC2 インスタンスに エージェントをインストールするには

1. エージェントをインストールする Windows ベースのオペレーティングシステムを実行している EC2 インスタンスにサインインします。

> **Note**
>
> Amazon Inspector Classic がサポートしているオペレーティングシステムの詳細については、Amazon Inspector Classic でサポートされているオペレーティングシステムとリージョンを参照してください。

2. 次の .exe ファイルをダウンロードします:

   ```
   https://inspector-agent.amazonaws.com/windows/installer/latest/
   AWSAgentInstall.exe
   ```

3. (管理者権限で) コマンドプロンプトウィンドウを開き、ダウンロードした `AWSAgentInstall.exe` を保存した場所に移動し、.exe file を実行してエージェントをインストールします。

> **Note**
>
> エージェントの更新が利用可能になると、Amazon S3 から自動的にダウンロードされ、適用されます。詳細については、Amazon Inspector Classic エージェントの更新を参照してください。
> この自動更新プロセスをスキップする場合は、エージェントをインストールするときに、次のコマンドを実行します。
> AWSAgentInstall.exe AUTOUPDATE=No

Linux ベースのオペレーティングシステムでの Amazon Inspector Classic エージェントの操作

Amazon Inspector Classic エージェントの動作をインストール、削除、確認および変更できます。Linux ベースのオペレーティングシステムを実行している Amazon EC2 インスタンスにサインインし、次のいずれかの手順を実行します。Amazon Inspector Classic でサポートされるオペレーティングシステムの詳細については、「Amazon Inspector Classic でサポートされているオペレーティングシステムとリージョン」を参照してください。

> **Important**
>
> Amazon Inspector Classic エージェントは、正常に機能するために Amazon EC2 インスタンスメタデータに依存します。インスタンスメタデータにアクセスするために、Instance Metadata Service のバージョン 1 または 2 (IMDSv1 または IMDSv2) を使用します。EC2 インスタンスメタデータおよびアクセス方法の詳細については、「インスタンスメタデータとユーザーデータ」を参照してください。

> **Note**
>
> このセクションのコマンドは、Amazon Inspector Classic でサポートされているすべての AWS リージョンで機能します。

トピック

- Amazon Inspector Classic エージェントの実行の確認
- Amazon Inspector Classic エージェントの停止
- Amazon Inspector Classic エージェントの起動
- Amazon Inspector Classic エージェントの設定の変更
- Amazon Inspector Classic エージェントのプロキシサポートの設定
- Amazon Inspector Classic エージェントのアンインストール

Amazon Inspector Classic エージェントの実行の確認

- エージェントがインストールされていて稼働していることを確認するには、EC2 インスタンスにサインインし、次のコマンドを実行します。

  ```
  sudo /opt/aws/awsagent/bin/awsagent status
  ```

  このコマンドは、現在実行しているエージェントのステータスやエージェントに接続できないことを示すエラーを返します。

Amazon Inspector Classic エージェントの停止

- エージェントを停止するには、次のコマンドを実行します。

  ```
  sudo /etc/init.d/awsagent stop
  ```

Amazon Inspector Classic エージェントの起動

- エージェントを開始するには、次のコマンドを実行します。

  ```
  sudo /etc/init.d/awsagent start
  ```

Amazon Inspector Classic エージェントの設定の変更

Amazon Inspector Classic エージェントが EC2 インスタンスにインストールされて実行されると、agent.cfg ファイルの設定を変更し、エージェントの動作を変更できるようになります。Linux ベースのオペレーティングシステムでは、agent.cfg ファイルは /opt/aws/awsagent/etc ディレクトリにあります。agent.cfg ファイルを変更して保存した後は、変更を有効にするためにエージェントを停止してから再開する必要があります。

> **Important**
>
> agent.cfg ファイルを変更する際は、必ず AWS Support のガイドを受けることをお勧めします。

Amazon Inspector Classic エージェントのプロキシサポートの設定

Linux ベースのオペレーティングシステムでエージェントのプロキシのサポートを得るには、固有の環境変数を使ってエージェント固有の設定ファイルを使用します。詳細については、https://wiki.archlinux.org/index.php/proxy_settings を参照してください。

以下の手順の 1 つを実行します。

プロキシサーバーを使用する EC2 インスタンスにエージェントをインストールするには

1. /etc/init.d/ ディレクトリに awsagent.env という名前のファイルを作成して保存します。
2. 次の環境変数を次の形式で含むように awsagent.env を編集します。

   - export https_proxy=hostname:port
   - export http_proxy=hostname:port
   - export no_proxy=169.254.169.254

> **Note**
>
> 前述のサンプルの値を、有効なホスト名とポート番号の組み合わせのみに置き換えます。インスタンスのメタデータ エンドポイント (169.254.169.254) の IP アドレスを no_proxy 変数に指定する必要があります。

3. Linux ベースの EC2 インスタンスにエージェントをインストールします。 手順のステップを完了して、Amazon Inspector Classic エージェントをインストールします。

エージェントを実行しながら、EC2 インスタンス上でプロキシサポートを設定するには

1. プロキシサポートを設定するには、EC2 インスタンスで実行しているエージェントが 1.0.800.1 以降である必要があります。エージェントの自動更新を有効にしている場合は、Amazon Inspector Classic エージェントの実行の確認の手順を使って、エージェントのバージョンが 1.0.800.1 以降であることを確認します。エージェントの自動更新を有効にしていない場合は、Linux ベースの EC2 インスタンスにエージェントをインストールします。 手順に従って、この EC2 インスタンスにエージェントを再度インストールする必要があります。
2. `/etc/init.d/` ディレクトリに `awsagent.env` という名前のファイルを作成して保存します。
3. 次の環境変数を次の形式で含むように `awsagent.env` を編集します。

   - `export https_proxy=hostname:port`
   - `export http_proxy=hostname:port`
   - `export no_proxy=169.254.169.254`

   > **Note**
   >
   > 前述のサンプルの値を、有効なホスト名とポート番号の組み合わせのみに置き換えます。インスタンスのメタデータ エンドポイント (169.254.169.254) の IP アドレスを `no_proxy` 変数に指定する必要があります。

4. 次のコマンドを使用してエージェントを停止し、それからエージェントを再起動します。

   ```
   sudo /etc/init.d/awsagent restart
   ```

   プロキシ設定は、エージェントと自動更新プロセスの両方で使用されます。

Amazon Inspector Classic エージェントのアンインストール

エージェントをアンインストールするには

1. エージェントをアンインストールする Linux ベースのオペレーティングシステムを実行している EC2 インスタンスにサインインします。

   > **Note**
   >
   > Amazon Inspector Classic でサポートされるオペレーティングシステムの詳細については、「Amazon Inspector Classic でサポートされているオペレーティングシステムとリージョン」を参照してください。

2. エージェントをアンインストールするには、次のコマンドの 1 つを使用します。

   - Amazon Linux、CentOS、および Red Hat では、次のコマンドを実行します。

     ```
     sudo yum remove 'AwsAgent*'
     ```

   - Ubuntu サーバーでは、以下のコマンドを実行します。

     ```
     sudo apt-get purge 'awsagent*'
     ```

Windows ベースのオペレーティングシステムでの Amazon Inspector Classic エージェントの操作

Amazon Inspector Classic エージェントの動作を開始、停止、および変更します。Windows ベースのオペレーティングシステムを実行している EC2 インスタンスにサインインし、この章の次のいずれかの手順を実行します。Amazon Inspector Classic でサポートされるオペレーティングシステムの詳細については、「Amazon Inspector Classic でサポートされているオペレーティングシステムとリージョン」を参照してください。

> **Important**
>
> Amazon Inspector Classic エージェントは、正常に機能するために Amazon EC2 インスタンスメタデータに依存します。インスタンスメタデータにアクセスするために、Instance Metadata Service のバージョン 1 または 2 (IMDSv1 または IMDSv2) を使用します。EC2 イ

ンスタンスメタデータおよびアクセス方法の詳細については、「インスタンスメタデータとユーザーデータ」を参照してください。

> **Note**
>
> この章のコマンドは、Amazon Inspector Classic でサポートされているすべての AWS リージョンで機能します。

トピック

- Amazon Inspector Classic エージェントの開始または停止、またはそのエージェントが実行中であることの確認
- Amazon Inspector Classic エージェントの設定の変更
- Amazon Inspector Classic エージェントのプロキシサポートの設定
- Amazon Inspector Classic エージェントのアンインストール

Amazon Inspector Classic エージェントの開始または停止、またはそのエージェントが実行中であることの確認

エージェントを開始、停止または確認するには

1. EC2 インスタンスで、[開始]、[実行] を選択し、「**services.msc**」と入力します。
2. エージェントが正常に実行されている場合、2 つのサービスがリストされ、Servicesウィンドウでそのステータスが Started または Running に設定されます。AWS エージェントサービスおよび AWS エージェントアップデーターサービス。
3. エージェントを開始するには、[AWS Agent Service] を右クリックし、[開始] を選択します。サービスが正常に開始されると、その状態は [開始] または [実行中] に更新されます。
4. エージェントを停止するには、[AWS Agent Service] を右クリックし、[停止] を選択します。サービスを正常に停止すると、その状態がクリアされます (空白として表示されます)。[AWS Agent Updater Service] を停止することはお勧めしません。停止すると、エージェントのそれ以降の機能強化や修正のインストールがすべて無効になります。
5. エージェントがインストールされていて稼働していることを確認するには、EC2 インスタンスにサインインし、管理者許可を使用してコマンドプロンプトを開きます。 `C:\Program Files\Amazon Web Services\AWS Agent` に移動して、以下のコマンドを実行します。

AWSAgentStatus.exe

このコマンドは、現在稼働しているエージェントのステータスやエージェントに接続できないことを示すエラーを返します。

Amazon Inspector Classic エージェントの設定の変更

Amazon Inspector Classic エージェントが EC2 インスタンスにインストールされて実行されると、agent.cfg ファイルの設定を変更し、エージェントの動作を変更できるようになります。Windows ベースのオペレーティングシステムでは、このファイルは C:\ProgramData\Amazon Web Services\AWS Agent ディレクトリにあります。agent.cfg ファイルを変更して保存した後は、変更を有効にするためにエージェントを停止してから再開する必要があります。

> **Important**
>
> agent.cfg ファイルを変更する際は、必ず AWS Support のガイドを受けることをお勧めします。

Amazon Inspector Classic エージェントのプロキシサポートの設定

Windows ベースのオペレーティングシステムでエージェントのプロキシサポートを取得するには、WinHTTP プロキシを 使用します。netsh ユーティリティを使用して WinHTTP プロキシを設定するには、Netsh Commands for Windows Hypertext Transfer Protocol (WINHTTP) を参照してください。

> **Important**
>
> Windows ベースのインスタンスでは HTTPS プロキシのみがサポートされています。

以下の手順の 1 つを実行します。

プロキシサーバーを使用する EC2 インスタンスにエージェントをインストールするには

1. 次の .exe ファイルをダウンロードします: https://d1wk0tztpsntt1.cloudfront.net/windows/installer/latest/AWSAgentInstall.exe

2. (管理アクセス許可を使用して) コマンドプロンプトウィンドウまたは PowerShell ウィンドウを開きます。AWSAgentInstall.exe を保存した場所に移動し、以下のいずれかのコマンドを実行します。

   ```
   .\AWSAgentInstall.exe /install USEPROXY=1
   ```

エージェントを実行しながら、EC2 インスタンス上でプロキシサポートを設定するには

1. プロキシサポートを設定するには、EC2 インスタンスで実行している Amazon Inspector Classic エージェントのバージョンが 1.0.0.59 以降である必要があります。エージェントの自動更新を有効にしている場合は、「Amazon Inspector Classic エージェントの開始または停止、またはそのエージェントが実行中であることの確認」の手順を使って、エージェントのバージョンが 1.0.0.59 以降であることを確認します。エージェントの自動更新プロセスを有効にしていない場合は、Windows ベースの EC2 インスタンスにエージェントをインストールするには 手順に従って、この EC2 インスタンスにエージェントを再度インストールする必要があります。
2. レジストリエディタを開きます (regedit.exe)。
3. 次のレジストリキーに移動します: "HKEY_LOCAL_MACHINE/SOFTWARE/Amazon Web Services/AWS Agent Updater"。
4. このレジストリキーの中で、レジストリの "UseProxy" と呼ばれる DWORD(32bit) 値を作成します。
5. 値をダブルクリックして、値を 1 に設定します。
6. 「**services.msc**」と入力して、Services ウィンドウで [AWS Agent Service] と [AWS Agent Updater Service] を見つけて各プロセスを再起動します。両方のプロセスが正常に再起動されたら、AWSAgentStatus.exe ファイルを実行します (「Amazon Inspector Classic エージェントの開始または停止、またはそのエージェントが実行中であることの確認」のステップ 5 を参照してください)。エージェントのステータスを表示して、設定されたプロキシを使用していることを確認します。

Amazon Inspector Classic エージェントのアンインストール

エージェントをアンインストールするには

1. Amazon Inspector Classic エージェントをアンインストールする Windows ベースのオペレーティングシステムを実行している EC2 インスタンスにサインインします。

> **Note**
>
> Amazon Inspector Classic でサポートされるオペレーティングシステムの詳細については、「Amazon Inspector Classic でサポートされているオペレーティングシステムとリージョン」を参照してください。

2. EC2 インスタンスで、[コントロールパネル]、[プログラムの追加と削除] に移動します。
3. インストールされたプログラムのリストで、[AWS Agent] を選択し、[Uninstall] を選択します。

(オプション) Linux ベースのオペレーティングシステムの Amazon Inspector Classic エージェントのインストールスクリプトの署名を確認します。

このトピックでは、Linux ベースのオペレーティングシステム用の Amazon Inspector Classic エージェントのインストールスクリプトの有効性を検証するための、推奨されるプロセスについて説明します。

インターネットからアプリケーションをダウンロードする場合は、常にソフトウェア発行元のアイデンティティを認証し、アプリケーションの発行後に改ざん、あるいは破損がないか確認することをお勧めします。これにより、ウイルスやマルウェアに感染したバージョンのアプリケーションをインストールせずに済みます。

このトピックのステップを実行した後に Amazon Inspector Classic エージェントのソフトウェアが変更または破損していることが判明した場合は、インストールファイルを実行しないでください。この場合は、AWS Support までお問い合わせください。

Linux ベースのオペレーティングシステム用の Amazon Inspector Classic エージェントファイルは、安全なデジタル署名のためのプリティグッドプライバシー (OpenPGP) 標準のオープンソース実装である GnuPG を使用して署名されています。GnuPG (GPG とも呼ばれます) は、デジタル署名による認証と整合性チェックを提供します。Amazon EC2 は、ダウンロードした Amazon EC2 CLI ツールの検証に使用できるパブリックキーと署名を公開します。PGP と GnuPG (GPG) の詳細については、http://www.gnupg.org を参照してください。

まず、ソフトウェア発行元との信頼を確立します。ソフトウェア発行元のパブリックキーをダウンロードし、キー所有者が一致していることを確認してから、キーリングに追加します。キーリングと

は、既知のパブリックキーの集合です。真正性が確立されたパブリック キーは、アプリケーションの署名を確認するために使用できます。

トピック

- GPG ツールのインストール
- パブリック キーの認証とインポート
- パッケージの署名の確認

GPG ツールのインストール

お使いのオペレーティングシステムが Linux または Unix の場合、GPG ツールが既にインストールされている場合があります。システムにツールがインストール済みかどうかをテストするには、コマンドラインプロンプトで gpg を入力します。GPG ツールがインストールされている場合、GPG のコマンドプロンプトが表示されます。GPG ツールがインストールされていない場合、コマンドが見つからないというエラーが表示されます。GnuPG パッケージはリポジトリからインストールできます。

Debian ベースの Linux に GPG ツールをインストールするには

- ターミナルから、次のコマンド apt-get install gnupg を実行します。

Red Hat ベースの Linux に GPG ツールをインストールするには

- ターミナルから、次のコマンド yum install gnupg を実行します。

パブリック キーの認証とインポート

プロセスの次のステップでは、Amazon Inspector Classic パブリックキーを認証し、信用されたキーとして GPG キーリングへ追加します。

Amazon Inspector Classic パブリックキーを認証してインポートするには

1. 次のいずれかを実行してパブリック GPG ビルドキーのコピーを取得します。
   - https://d1wk0tztpsntt1.cloudfront.net/linux/latest/inspector.gpg からダウンロードします。
   - 次のテキストからキーをコピーし、[inspector.gpg] という名前のファイルに貼り付けます。必ず次のすべてが含まれるようにしてください。

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2.0.18 (GNU/Linux)

mQINBFYDlfEBEADFpfNt/mdCtsmfDoga+PfHY9bdXAD68yhp2m9NyH3BOzle/MXI
8siNfoRgzDwuWnIaezHwwLWkDw2paRxp1NMQ9qRe8Phq0ewheLrQu95dwDgMcw90
gf9m1iKVHjdVQ9qNHlB2OFknPDxMDRHcrmlJYDKYCX3+MODEHnlK25tIH2KWezXP
FPSU+TkwjLRzSMYH1L8IwjFUIIi78jQS9a31R/cOl4zuC5fOVghYlSomLI8irfoD
JSa3csVRujSmOAf9o3beiMR/kNDMpgDOxgiQTu/Kh39cl6o8AKe+QKK48kqO7hra
h1dpzLbfeZEVU6dWMZtlUksG/zKxuzD6d8vXYH7Z+x09POPFALQCQQMC3WisIKgj
zJEFhXMCCQ3NLC3CeyMq3vP7MbVRBYE7t3d2uDREkZBgIf+mbUYfYPhrzy0qT9Tr
PgwcnUvDZuazxuuPzucZGOJ5kbptat3DcUpstjdkMGAId3JawBbps77qRZdA+swr
o9o3jbowgmf0y5ZS6KwvZnC6XyTAkXy2io7mSrAIRECrANrzYzfp5v7uD7w8Dk0X
1OrfOm1VufMzAyTu0YQGBWaQKzSB8tCkvFw54PrRuUTcV826XU7SIJNzmNQo58uL
bKyLVBSCVabfs0lkECIesq8PT9xMYfQJ421uATHyYUnFTU2TYrCQEab7oQARAQAB
tCdBbWF6b24gSW5zcGVjdG9yIDxpbnNwZWN0b3JAYW1hem9uLmNvbT6JAjgEEwEC
ACIFAlYDlfECGwMGCwkIBwMCBhUIAgkKCwQWAgMBAh4BAheAAAoJECR0CWBYNgQY
8yUP/2GpIl40f3mKBUiSTe0XQLvwiBCHmY+V9fOuKqDTinxssjEMCnz0vsKeCZF/
L35pwNa/oW0OJa8D7sCkKG+8LuyMpcPDyqptLrYPprUWtz2+qLCHgpWsrku7ateF
x4hWS0jUVeHPaBzI9V1NTHsCx9+nbpWQ5Fk+7VJI8hbMDY7NQx6fcse8WTlP/0r/
HIkKzzqQQaaOf5t9zc5DKwi+dFmJbRUyaq22xs8C81UODjHunhjHdZ21cnsgk91S
fviuaum9aR4/uVIYOTVWnjC5J3+VlczyUt5FaYrrQ5ov0dM+biTUXwve3X8Q85Nu
DPnO/+zxb7Jz3QCHXnuTbxZTjvvl60Oi8//uRTnPXjz4wZLwQfibgHmk1++hzND7
wOYA02Js6v5FZQlLQAod7q2wuA1pq4MroLXzziDfy/9ea8B+tzyxlmNVRpVZY4Ll
DOHyqGQhpkyV3drjjNZlEofwbfu7m6ODwsgMl5ynzhKklJzwPJFfB3mMc7qLi+qX
MJtEX8KJ/iVUQStHHAG7daL1bxpWSI3BRuaHsWbBGQ/mcHBgUUOQJyEp5LAdg9Fs
VP55gWtF7pIqifiqlcfgG0Ov+A3NmVbmiGKSZvfrc5KsF/k43rCGqDx1RV6gZvyI
LfO9+3sEIlNrsMib0KRLDeBt3EuDsaBZgOkqjDhgJUesqiCy
=iEhB
-----END PGP PUBLIC KEY BLOCK-----
```

2. inspector.gpg を保存したディレクトリのコマンドプロンプトで、次のコマンドを使用して Amazon Inspector Classic パブリックキーをキーリングにインポートします。

```
gpg --import inspector.gpg
```

コマンドで次のような結果が返されます。

```
gpg: key 58360418: public key "Amazon Inspector <inspector@amazon.com>" imported
                   gpg: Total number processed: 1
                   gpg:               imported: 1  (RSA: 1)
```

次のステップで必要になるため、キーの値を書きとめておきます。前述の例では、キーの値は 58360418 です。

3. 次のコマンドを使用してフィンガープリントを確認し、キー値を前述の手順の値と置き換えます。

```
gpg --fingerprint key-value
```

このコマンドで次のような結果が返されます。

```
pub   4096R/58360418 2015-09-24
                Key fingerprint = DDA0 D4C5 10AE 3C20 6F46  6DC0 2474 0960 5836
 0418
                uid                  Amazon Inspector <inspector@amazon.com>
```

さらに、前述の例のように、フィンガープリント文字列は「DDA0 D4C5 10AE 3C20 6F46 6DC0 2474 0960 5836 0418」になります。返されたキー フィンガープリントをこのページで公開されているものと比較します。これらは一致するはずです。一致しない場合は、Amazon Inspector Classic エージェントインストールスクリプトをインストールせず、AWS Support までお問い合わせください。

パッケージの署名の確認

GPG ツールをインストールした後、Amazon Inspector Classic パブリックキーを認証してインポートし、そのパブリック キーが信頼済みであることを確認すると、インストールスクリプトの署名を確認できるようになります。

インストールスクリプトの署名を確認するには

1. コマンド プロンプトで次のコマンドを実行し、インストール スクリプトの署名ファイルをダウンロードします。

```
curl -O https://inspector-agent.amazonaws.com/linux/latest/install.sig
```

2. `install.sig` と Amazon Inspector Classic インストールファイルを保存したディレクトリのコマンドプロンプトで次のコマンドを実行し、署名を確認します。ファイルが2つとも存在している必要があります。

```
gpg --verify ./install.sig
```

出力は次のようになります。

```
gpg: Signature made Thu 24 Sep 2015 03:19:09 PM UTC using RSA key ID 58360418
gpg: Good signature from "Amazon Inspector <inspector@amazon.com>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: DDA0 D4C5 10AE 3C20 6F46  6DC0 2474 0960 5836 0418
```

出力に「`Good signature from "Amazon Inspector <inspector@amazon.com>"`」という句が含まれる場合は、署名が正常に確認されており、Amazon Inspector Classic インストールスクリプトを実行できることを意味しています。

出力結果に「`BAD signature`」という句が含まれる場合、手順が正しいことをもう一度確認してください。この応答が続く場合は、以前にダウンロードしたインストールファイルを実行しないで、AWS Support にお問い合わせください。

以下は、表示される可能性のある警告の詳細です。

- 警告: このキーは、信用された署名で認定されていません! 署名が所有者に属していることが確認できません。これは、Amazon Inspector Classic の認証済みパブリックキーを所有していると考えるユーザーの個人レベルの信頼を参照します。本来は、ユーザーが AWS オフィスを訪問してキーを受け取ることが理想的です。しかし、キーは多くの場合 ウェブ サイトからダウンロードされます。この場合、ウェブサイトは AWS ウェブサイトです。
- gpg: 最終的に信用されたキーが見つかりません。これは、特定のキーがユーザー (またはユーザーが信頼する他のユーザー) によって「最終的に信用された」キーでないことを意味します。

詳細については、「http://www.gnupg.org」を参照してください。

「オプショナル」 Windows ベースのオペレーティングシステムの Amazon Inspector Classic エージェントインストールスクリプトの署名を確認します。

このトピックでは、Windows ベースのオペレーティングシステム用の Amazon Inspector Classic エージェントのインストールスクリプトの有効性を検証するための、推奨されるプロセスについて説明します。

インターネットからアプリケーションをダウンロードする場合は、常にソフトウェア発行元のアイデンティティを認証し、アプリケーションの発行後に改ざん、あるいは破損がないか確認することをお勧めします。これにより、ウイルスやマルウェアに感染したバージョンのアプリケーションをインストールせずに済みます。

このトピックのステップを実行した後に Amazon Inspector Classic エージェントのソフトウェアが変更または破損していることが判明した場合は、インストールファイルを実行しないでください。この場合は、AWS サポート までお問い合わせください。

Windows ベースのオペレーティングシステム用のダウンロードされたエージェントのインストールスクリプトの有効性を検証するには、Amazon Services LLC の署名者証明書のサムプリントが次の値と等しいことを確認してください。

E8 83 C5 3A F7 8C BA 7C F5 A2 47 E9 B8 86 FC E9 68 EE 0B 36

この値を検証するには、以下の手順を実行します。

1. ダウンロードした `AWSAgentInstall.exe` を右クリックして、プロパティウィンドウを開きます。
2. デジタル署名タブを選択します。
3. [署名リスト] で [Amazon Web Services] を選択し、[詳細] を選択します。
4. すでに選択していない場合は 一般タブにアクセスし、証明書の表示 を選びます。
5. 詳細 タブを選択し、まだの場合は すべてを表示 のドロップダウンリストで選択します。
6. 拇印 フィールドが表示されるまでスクロールして、拇印 を選択します。下のウィンドウにサムプリントの値全体が表示されます。

   - 下のウィンドウのサムプリントの値が次の値と等しい場合、

     E8 83 C5 3A F7 8C BA 7C F5 A2 47 E9 B8 86 FC E9 68 EE 0B 36

ダウンロードされたエージェントのインストールスクリプトは正規のものであり、安全にインストールすることができます。

- 下部の詳細ウィンドウのサムプリントの値が上記の値と等しくない場合には、AWSAgentInstall.exe を実行しないでください。

Amazon Inspector Classic 評価ターゲット

Amazon Inspector Classic を使用して、 AWS 評価ターゲット (AWS リソースのコレクション) で対処すべき潜在的なセキュリティ上の問題があるかどうかを評価できます。

> **Important**
>
> 現在、評価ターゲットは、サポートされているオペレーティングシステムで実行される EC2 インスタンスのみを含めることができます。サポートされているオペレーティングシステムとサポートされている AWS リージョンについては、「the section called “サポートされているオペレーティングシステムとリージョン”」を参照してください。

> **Note**
>
> EC2 インスタンスの起動の詳細については、「Amazon Elastic Compute Cloud のドキュメント」を参照してください。

トピック

- リソースをタグ付けして評価ターゲットを作成する
- Amazon Inspector Classic 評価ターゲットの制限
- 評価ターゲットを作成する
- 評価ターゲットを削除する

リソースをタグ付けして評価ターゲットを作成する

Amazon Inspector Classic の評価ターゲットを作成して評価するには、最初にターゲットに含める EC2 インスタンスのタグ付けを行います。タグは、インスタンスやその他の AWS リソースを識別して整理するためのメタデータとして機能する単語またはフレーズです。Amazon Inspector Classic は作成されたタグを使用し、ターゲットに属するインスタンスを識別します。

すべての AWS タグは、選択したキーと値のペアで構成されます。たとえば、キーの名前で 実行コマンドName実行コマンド、値で 実行コマンドMyFirstInstance実行コマンド を選択します。インスタンスをタグ付けした後は、Amazon Inspector Classic コンソールを使用して評価ターゲットにイン

スタンスを追加します。インスタンスが 1 つ以上のタグのキー/値のペアに一致する必要はありません。

EC2 インスタンスにタグを付けて評価ターゲットを構築する場合、独自のカスタムタグキーを作成するか、同じ AWS アカウントの他のユーザーによって作成されたタグキーを使用できます。 AWS が自動的に作成するタグキーを使用することもできます。たとえば、 は起動する EC2 インスタンスの名前タグキー AWS を自動的に作成します。

作成したタグは、EC2 インスタンスに追加できます。また、これらのタグは、それぞれの EC2 インスタンスのコンソールページで一度に 1 つずつ追加、変更、削除することができます。タグエディターを使用すると、一度に複数の EC2 インスタンスにタグを追加することもできます。

詳細については、「タグ エディター」を参照してください。EC2 インスタンスのタグ付けの詳細については、「 リソースとタグ」を参照してください。

Amazon Inspector Classic 評価ターゲットの制限

AWS アカウントごとに最大 50 の評価ターゲットを作成できます。詳細については、「Amazon Inspector Classic サービスの制限」を参照してください。

評価ターゲットを作成する

Amazon Inspector Classic コンソールを使用して評価ターゲットを作成できます。

評価ターゲットを作成するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/inspector/ で Amazon Inspector Classic コンソールを開きます。
2. ナビゲーションペインで、評価ターゲット、作成 の順に選択します。
3. 実行コマンドName (名前)実行コマンド に、評価ターゲットの名前を入力します。
4. 次のいずれかを行います。

   - この評価ターゲットにこの AWS アカウントとリージョンのすべての EC2 インスタンスを含めるには、すべてのインスタンスチェックボックスをオンにします。

> **Note**
>
> このオプションを使用する場合、評価の実行に含めることができるエージェントの最大数の制限が適用されます。詳細については、「Amazon Inspector Classic サービスの制限」を参照してください。

- この評価ターゲットに含める EC2 インスタンスを選択するには、実行コマンドUse Tags (使用するタグ)実行コマンド で、タグキー名とキーと値のペアを入力します。

5. (省略可能) ターゲットの作成中に、実行コマンドInstall Agents (エージェントのインストール)実行コマンド チェックボックスを選択し、エージェントをこのターゲットのすべての EC2 インスタンスにインストールします。このオプションを使用するには、EC2 インスタンスに SSM Agent がインストールされ、実行コマンド を許可する IAM ロールがある必要があります。SSM Agent は、デフォルトでは、Amazon EC2 Windows インスタンスおよび Amazon Linux インスタンスにインストールされます。Amazon EC2 Systems Manager では、コマンドを処理する EC2 インスタンスの IAM ロールと、それとは別にコマンドを実行するユーザーのロールが必要です。詳細については、「SSM Agent のインストールと設定」と「Configuring Security Roles for System Manager」を参照してください。

> **Important**
>
> すでに EC2 インスタンスで実行されているエージェントがある場合、このオプションを使用すると、インスタンスで現在実行されているエージェントが最新のエージェントバージョンに置き換えられます。

> **Note**
>
> 既存の評価ターゲットの場合、実行コマンドボタンを選択してエージェントをインストール を選択すると、このターゲット内のすべてのEC2インスタンスにエージェントをインストールできる。

> **Note**
>
> また、Systems Manager 実行コマンド を使用して、エージェントを複数の EC2 インスタンスに (同じコマンドで Linux ベースおよび Windows ベースのインスタンスの両方に)

リモートでインストールすることもできます。詳細については、「Systems Manager Run コマンドを使用した複数の EC2 インスタンスへの Amazon Inspector エージェントのインストール」を参照してください。

6. 保存を選択します。

> **Note**
>
> 評価ターゲット ページの プレビューターゲットを実行コマンド ボタンを使用して、評価ターゲットに含まれるすべての EC2 インスタンスを確認できます。EC2 インスタンスごとに、ホスト名、インスタンス ID、IP アドレス、および該当する場合はエージェントのステータスを確認できます。エージェントのステータス実行コマンド には、次の値を指定できます。HEALTHY、UNHEALTHY、UNKNOWN Amazon Inspector Classic は、EC2 インスタンスで実行中のエージェントがあるかどうかを判断できない場合、UNKNOWN ステータスを表示します。

評価ターゲットを削除する

評価ターゲットを削除するには、次の手順を実行します。

評価ターゲットを削除するには

- 実行コマンド評価ターゲット実行コマンド ページで、削除するターゲットを選択し、実行コマンド削除実行コマンド を選択します。確認を求めるメッセージが表示されたら、実行コマンドYes実行コマンド を選択します。

> **Important**
>
> 評価ターゲットを削除すると、すべての評価テンプレート、評価の実行、結果、およびターゲットに関連付けられたバージョンのレポートも削除されます。

`DeleteAssessmentTarget` API を使用して評価ターゲットを削除することもできます。

Amazon Inspector Classic ルールパッケージとルール

Amazon Inspector Classic を使用して、評価ターゲット (AWS リソースの集合体) の潜在的なセキュリティ上の問題や脆弱性を評価できます。Amazon Inspector Classic は、評価ターゲットの動作とセキュリティ設定を選択したセキュリティルールパッケージと比較します。Amazon Inspector Classic のコンテキストでは、ルールは、評価の実行中に Amazon Inspector Classic が実行するセキュリティチェックを意味します。

Amazon Inspector Classic では、ルールはカテゴリー、重要度、または料金ごとに個別のルールパッケージにグループ化されます。これにより、実行する分析の種類を選択できます。例えば、Amazon Inspector Classic はアプリケーションの評価に使用できる多数のルールを提供します。しかし、特定の部分をターゲットにしてセキュリティの問題を個別に発見するために、使用可能なルールの小さなサブセットを設定することが必要な場合があります。大規模な IT 部門を抱える企業は、自社のアプリケーションがセキュリティ上の脅威にさらされているかどうかを判断したいと考えるかもしれません。他の人たちは重要度レベルが高の問題だけに集中したいと思うかもしれません。

- Amazon Inspector Classic のルールの重要度レベル
- Amazon Inspector Classic のルールパッケージ

Amazon Inspector Classic のルールの重要度レベル

それぞれの Amazon Inspector Classic ルールには重要度が割り当てられています。これにより、分析で特定のルールを優先する必要性がなくなります。また、ルールが潜在的問題をハイライトする場合の応答を決定できます。

[High]、[Medium]、および [Low] の各レベルはすべて、評価ターゲット内での情報の機密性、完全性、および可用性を侵害する可能性のあるセキュリティ上の問題を示しています。レベルは、問題が解決につながる可能性がどの程度あるか、問題を解決することがどれほど緊急であるかによって区別されます。

[Informational] レベルは、評価ターゲットのセキュリティ設定の詳細を簡単にハイライトします。

重要度に基づいて問題に推奨される応答方法は、以下のとおりです。

- 高 – 重要度の高い問題は非常に緊急です。Amazon Inspector Classic は、このセキュリティ上の問題を緊急事態として対応し、直ちに改善を実施することをお勧めします。
- ミディアム – 中程度の重要度の問題はやや緊急です。Amazon Inspector Classic は、次の可能な機会 (例えば、次のサービスの更新中) にこの問題を修正することをお勧めします。

- 低 – 重要度が低い問題はそれほど緊急ではありません。Amazon Inspector Classic は、将来のサービスの更新の一部として、この問題を修正することをお勧めします。
- 情報提供 – これらの問題は純粋に情報提供されています。ビジネスおよび組織の目標に基づいて、単にこの情報に留意するか、これを使用して評価ターゲットのセキュリティを改善することができます。

Amazon Inspector Classic のルールパッケージ

Amazon Inspector の評価では、以下のルールパッケージを任意に組み合わせて使用できます。

ネットワーク評価:

- ネットワーク到達可能性

ホスト評価:

- 共通脆弱性識別子
- Center for Internet Security (CIS) ベンチマーク
- Amazon Inspector Classic のセキュリティのベストプラクティス

ネットワーク到達可能性

ネットワーク到達可能性パッケージのルールは、ネットワーク設定を分析して EC2 インスタンスのセキュリティ上の脆弱性を見つけます。Amazon Inspector が生成した結果から、安全ではないアクセスの許可に関するガイダンスも得られます。

Network Reachability ルールパッケージは、 AWS Provable Security イニシアチブの最新テクノロジーを使用します。

これらのルールによって生成された結果は、ポートがインターネットからインターネットゲートウェイ (アプリケーション ロード バランサー または クラシックロードバランサー の背後のインスタンスを含む)、VPC ピアリング接続、または仮想ゲートウェイを介した VPN を通じて到達可能かどうかを示します。これらの結果では、管理が誤っているセキュリティグループ、ACL、IGW など、潜在的に悪意のあるアクセスを許可するネットワーク設定もハイライトされています。

これらのルールは、AWS ネットワークのモニタリングを自動化し、EC2 インスタンスへのネットワークアクセスが誤って設定されている可能性がある場所を特定するのに役立ちます。このパッケー

ジを評価の実行に含めることで、スキャナーをインストールしてパケットを送信しなくても、特に VPC ピアリング接続と VPN では、維持するのに複雑でコストがかかる、詳細なネットワークセキュリティチェックを実装できます。

> **Important**
>
> Amazon Inspector Classic エージェントは、このルールパッケージを使用して EC2 インスタンスを評価する必要はありません。ただし、インストールされているエージェントは、ポートで待機しているプロセスの存在に関する情報を提供できます。Amazon Inspector Classic でサポートされていないオペレーティングシステムにエージェントをインストールしないでください。サポートされていないオペレーティングシステムを実行するインスタンスにエージェントが存在する場合、ネットワーク到達可能性ルールパッケージはそのインスタンスでは機能しません。

詳細については、「サポートされているオペレーティングシステムの Amazon Inspector Classic ルールパッケージ」を参照してください。

分析された設定

ネットワーク到達可能性ルールは以下のエンティティの設定の脆弱性を分析します。

- Amazon EC2 インスタンス
- アプリケーション ロード バランサー
- Direct Connect
- 弾性ロードバランサ
- 弾性ネットワークインターフェース
- インターネットゲートウェイ (IGW)
- ネットワークアクセスコントロールリスト (ACL)
- ルートテーブル
- セキュリティグループ (SG)
- サブネット
- 仮想プライベートクラウド (VPC)
- 仮想プライベートゲートウェイ (VGW)
- VPC ピアリング接続

到達可能性ルート

ネットワーク到達可能性ルールは、次の到達可能性ルートを確認します。これは、VPC の外部からポートにアクセスできる方法に対応しています。

- **Internet** - インターネットゲートウェイ (アプリケーション ロード バランサー および クラシック ロードバランサー を含む)
- **PeeredVPC** - VPC ピアリング接続
- **VGW** - 仮想プライベートゲートウェイ

結果のタイプ

ネットワーク到達可能性ルールパッケージを含む評価では、各到達可能性ルートについて次のタイプの結果が返される可能性があります。

- RecognizedPort
- UnrecognizedPortWithListener
- NetworkExposure

RecognizedPort

一般的によく知られているサービスに使用されるポートは到達可能です。エージェントがターゲット EC2 インスタンスに存在する場合、生成された結果はポートにアクティブなリスニングプロセスがあるかどうかも示します。このタイプの結果には、よく知られているサービスのセキュリティへの影響に基づいて重大度が指定されます。

- **RecognizedPortWithListener** – 認識されたポートは、特定のネットワークコンポーネントを介してパブリックインターネットにより外部から到達可能であり、プロセスはそのポートでリッスンしています。
- **RecognizedPortNoListener** – ポートは、特定のネットワークコンポーネントを介してパブリックインターネットにより外部から到達可能であり、そのポートでリッスンしているプロセスはありません。
- **RecognizedPortNoAgent** – ポートは、特定のネットワークコンポーネントを介してパブリックインターネットにより外部から到達可能です。ターゲットインスタンスにエージェントをインストールしないと、ポートをリッスンしているプロセスが存在するかどうかを判断できません。

次のテーブルは、認識されているポートの一覧を示しています。

サービス	TCP ポート	UDP ポート
SMB	445	445
NetBIOS	137、139	137、138
LDAP	389	389
TLS 経由の LDAP	636	
グローバルカタログ LDAP	3268	
TLS経由のグローバルカタログLDAP	3269	
NFS	111、2049、4045、1110	111、2049、4045、1110
Kerberos	88、464、54 3、544、749、751	88、464、749、750、751、752
RPC	111、135、530	111、135、530
WINS	1512、42	1512、42
DHCP	67、68、546、547	67、68、546、547
Syslog	601	514
印刷サービス	515	
Telnet	23	23
FTP	21	21
SSH	22	22
RDP	3389	3389

サービス	TCP ポート	UDP ポート
MongoDB	27017、27018、27019、28017	
SQL Server	1433	1434
MySQL	3306	
PostgreSQL	5432	
Oracle	1521、1630	
Elasticsearch	9300、9200	
HTTP	80	80
HTTPS	443	443

`UnrecogizedPortWithListener`

前記のテーブルに記載されていないポートは到達可能で、アクティブなリスニングプロセスがあります。このタイプの結果はリスニングプロセスに関する情報を示すため、Amazon Inspector エージェントがターゲット EC2 インスタンスにインストールされている場合にのみ生成できます。このタイプの結果は 低)の重要度が与えられます。

`NetworkExposure`

このタイプの結果は、EC2 インスタンスで到達可能なポートに関する集計情報を示しています。EC2 インスタンスの 弾性ネットワークインターフェース とセキュリティグループの組み合わせごとに、到達可能な TCP および UDP ポート範囲のセットが示されます。このタイプの結果の重要度は、情報)です。

共通脆弱性識別子

このパッケージのルールは、評価ターゲット内の EC2 インスタンスが共通脆弱性識別子 (CVE) に曝露されているかどうかを確認するのに役立ちます。攻撃は、パッチが適用されていない脆弱性を利用し、サービスまたはデータの機密性、完全性、可用性を侵害します。CVE システムは、セキュリ

ティの脆弱性や曝露についての既知の情報を参照する方法を提供します。詳細については、「https://cve.mitre.org/」を参照してください。

Amazon Inspector Classic の評価によって生成された結果に特定の CVE が表示される場合は、https://cve.mitre.org/ で CVE の ID (例えば、**CVE-2009-0021**) を検索できます。検索結果には、該当する CVE に関する詳細情報 (重大度や緩和方法) が表示されます。

一般的な脆弱性とエクスプロイト (CVE) ルールパッケージについては、Amazon Inspector が提供されている CVSS ベーススコアリングと ALAS 重要度レベルをマッピングしています。

Amazon Inspector 重要度	CVSS ベーススコア	ALAS 重要度 (CVSS がスコアリングされていない場合)
High	>= 5	Critical or Important
Medium	< 5 and >= 2.1	Medium
Low	< 2.1 and >= 0.8	Low
Informational	< 0.8	N/A

このパッケージに含まれているルールは、次のリージョンリストで EC2 インスタンスが CVE に対して公開されているかどうか評価するのに役立ちます。

- 米国東部 (バージニア北部)
- 米国東部 (オハイオ)
- 米国西部 (北カリフォルニア)
- 米国西部 (オレゴン)
- 欧州 (アイルランド)
- 欧州 (フランクフルト)
- 欧州 (ロンドン)
- 欧州 (ストックホルム)
- アジアパシフィック (東京)
- アジアパシフィック (ソウル)
- アジアパシフィック (ムンバイ)
- アジアパシフィック (シドニー)

- AWS GovCloud 西部 (米国)
- AWS GovCloud 東部 (米国)

CVE ルールパッケージは定期的に更新されます。このリストには、このリストが取得されるときに同時に発生する評価の実行に含まれる CVE があります。

詳細については、「サポートされているオペレーティングシステムの Amazon Inspector Classic ルールパッケージ」を参照してください。

Center for Internet Security (CIS) ベンチマーク

CIS Security Benchmarks プログラムは、組織がセキュリティを評価および改善するのに役立つ、明確に定義された、バイアスのない、コンセンサスベースの業界のベストプラクティスを提供します。AWS は CIS Security Benchmarks メンバー企業です。Amazon Inspector Classic 認定のリストについては、「CIS ウェブサイトの Amazon Web Services のページ」を参照してください。

Amazon Inspector Classic は、現在以下の CIS 認定ルールパッケージを提供し、次のオペレーティングシステムに安全な設定を確立できるようにしています。

Amazon Linux

- CIS Benchmark for Amazon Linux 2 Benchmark v1.0.0 Level 1
- CIS Benchmark for Amazon Linux 2 Benchmark v1.0.0 Level 2
- CIS Benchmark for Amazon Linux Benchmark v2.1.0 Level 1
- CIS Benchmark for Amazon Linux Benchmark v2.1.0 Level 2
- CIS Benchmark for Amazon Linux 2014.09-2015.03 v1.1.0 Level 1

CentOS Linux

- CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 1 Server
- CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 2 Server
- CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 1 Workstation
- CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 2 Workstation
- CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2 Level 1 Server
- CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2 Level 2 Server
- CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2 Level 1 Workstation

- CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2 Level 2 Workstation

Red Hat Enterprise Linux

- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 1 Server
- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 2 Server
- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 1 Workstation
- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 2 Workstation
- CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2 Level 1 Server
- CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2 Level 2 Server
- CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2. Level 1 Workstation
- CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2 Level 2 Workstation

Ubuntu

- CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 1 Server
- CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 2 Server
- CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 1 Workstation
- CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 2 Workstation
- CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 1 Server
- CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 2 Server
- CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 1 Workstation

- CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 2 Workstation
- CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0 Level 1 Server
- CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0 Level 2 Server
- CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0 Level 1 Workstation
- CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0 Level 2 Workstation

Windows

- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Level 1 Member Server Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Level 2 Member Server Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Level 1 Domain Controller Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Level 2 Domain Controller Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows 2016 RTM (Release 1607), v1.1.0, Next Generation Windows Security Profile)
- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows 2012 R2, v2.2.0, Level 1 Domain Controller Profile)
- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows 2012 R2, v2.2.0, Level 2 Domain Controller Profile)
- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows 2012 R2, v2.2.0, Level 1 Member Server Profile)
- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows 2012 R2, v2.2.0, Level 2 Member Server Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows 2012 non-R2, v2.0.0, Level 1 Member Server Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows 2012 non-R2, v2.0.0, Level 2 Member Server Profile)

- Windows Server 2012 (CIS Benchmark for Microsoft Windows 2012 non-R2, v2.0.0, Level 1 Domain Controller Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows 2012 non-R2, v2.0.0, Level 2 Domain Controller Profile)
- Windows Server 2008 R2 (CIS Benchmark for Microsoft Windows 2008 R2, v3.0.0, Level 1 Domain Controller Profile)
- Windows Server 2008 R2 (CIS Benchmark for Microsoft Windows 2008 R2, v3.0.0, Level 1 Member Server Profile)

特定の CIS ベンチマークが、Amazon Inspector Classic の評価の実行で生成された結果に表示される場合は、https://benchmarks.cisecurity.org/ からベンチマークの詳細な PDF 形式の説明をダウンロードできます (無料の登録が必要)。このベンチマークドキュメントには、この CIS ベンチマークに関する詳細情報、重大度、および緩和方法が表示されます。

詳細については、「サポートされているオペレーティングシステムの Amazon Inspector Classic ルールパッケージ」を参照してください。

Amazon Inspector Classic のセキュリティのベストプラクティス

システムが安全に設定されているかどうかを判断するには、Amazon Inspector Classic ルールを使用してください。

> **Important**
>
> 現時点では、Linux ベースまたは Windows ベースのオペレーティングシステムを実行している EC2 インスタンスを評価ターゲットに含めることができます。
> このセクションで説明されているルールでは、評価の実行中に、Linux ベースのオペレーティングシステムを実行している EC2 インスタンスのみの結果が生成されます。このルールでは、Windows ベースのオペレーティングシステムを実行している EC2 インスタンスの結果は生成されません。
> 詳細については、「サポートされているオペレーティングシステムの Amazon Inspector Classic ルールパッケージ」を参照してください。

トピック

- SSH 経由の root ログインを無効化する

- SSH バージョン 2 のみをサポート
- SSH 経由のパスワード認証を無効化する
- パスワードの有効期限を設定する
- パスワードの最小文字数を設定する
- パスワードの複雑さを設定する
- ASLR の有効化
- DEP の有効化
- システムディレクトリに対するアクセス許可の設定

SSH 経由の root ログインを無効化する

このルールは、SSH デーモンが root としての EC2 インスタンスへのログインを許可するように設定されているかどうかを判断するのに役立ちます。

重要度

[Medium] (中)

結果

ユーザーが root 認証情報を使用して SSH 経由でログインすることを許可するように設定された評価ターゲットに EC2 インスタンスがあります。これにより、ブルートフォース攻撃が成功する確率が高まります。

解決策

SSH 経由の root アカウントのログインを禁止するように EC2 インスタンスを設定することをお勧めします。代わりに、非 root ユーザーとしてログインして sudo を使用し、必要に応じて権限を昇格させます。SSH の root アカウントログインを無効化するには、`PermitRootLogin` を `/etc/ssh/sshd_config` ファイルの no に設定し、次に `sshd` を再起動します。

SSH バージョン 2 のみをサポート

このルールは、EC2 インスタンスが SSH プロトコルバージョン 1 をサポートするように設定されているかどうかを判断するのに役立ちます。

重要度

[Medium] (中)

結果

評価ターゲットの EC2 インスタンスが、セキュリティを大幅に低下させる先天的な設計上の欠陥を持つ SSH-1 をサポートするように設定されています。

解決策

SSH-2 以降のみをサポートするように評価ターゲットの EC2 インスタンスを設定することをお勧めします。OpenSSH では、`Protocol 2` を `/etc/ssh/sshd_config` ファイルに設定することでこれを実現できます。詳細については、「`man sshd_config`」を参照してください。

SSH 経由のパスワード認証を無効化する

このルールは、EC2 インスタンスが SSH プロトコル経由のパスワード認証をサポートするように設定されているかどうかを判断するのに役立ちます。

重要度

[Medium] (中)

結果

評価ターゲットの EC2 インスタンスが、SSH 経由のパスワード認証をサポートするように設定されています。認証は、パスワードのブルートフォース攻撃重視で、キーに認証を決定した可能な限り無効必要があります。

解決策

EC2 インスタンスで SSH 経由のパスワード認証を無効化し、代わりにキーベース認証のサポートを有効にします。これにより、ブルートフォース攻撃の成功率が大幅に下がります。詳細については、https://aws.amazon.com/articles/1233/ を参照してください。パスワード認証がサポートされている場合、信頼済み IP アドレスへの SSH サーバーへのアクセスを制限することが重要です。

パスワードの有効期限を設定する

このルールは、EC2 インスタンスでパスワードの有効期限が設定されているかどうかを判断するのに役立ちます。

重要度

[Medium] (中)

結果

評価ターゲットの EC2 インスタンスで、パスワードの有効期限が設定されていません。

解決策

パスワードを使用する場合、評価ターゲットのすべての EC2 インスタンスでパスワードの有効期限を設定することをお勧めします。このためには、ユーザーはパスワードを定期的に変更する必要がありますが、パスワード予測攻撃が成功する確率が低下します。既存のユーザーでこの問題を解決するには、chage コマンドを使用します。以降のすべてのユーザーでパスワードの有効期限を設定するには、`/etc/login.defs` ファイルの `PASS_MAX_DAYS` フィールドを編集します。

パスワードの最小文字数を設定する

このルールは、EC2 インスタンスでパスワードの最小文字数が設定されているかどうかを判断するのに役立ちます。

重要度

[Medium] (中)

結果

評価ターゲットの EC2 インスタンスで、パスワードの最小文字数が設定されていません。

解決策

パスワードを使用する場合、評価ターゲットのすべての EC2 インスタンスでパスワードの最小文字数を設定することをお勧めします。パスワードの最小文字数を設定することで、パスワード予測攻撃が成功する確率が低下します。そのためには、`pwquality.conf` ファイルの以下のオプションを使用します: `minlen`。詳細については、https://linux.die.net/man/5/pwquality.conf を参照してください。

インスタンスで `pwquality.conf` が使用できない場合は、`pam_cracklib.so` モジュールを使用して、`minlen` オプションを設定します。詳細については、「`man pam_cracklib`」を参照してください。

`minlen` オプションを 14 以上に設定する必要があります。

パスワードの複雑さを設定する

このルールは、EC2 インスタンスでパスワードの複雑さメカニズムが設定されているかどうかを判断するのに役立ちます。

重要度

[Medium] (中)

結果

評価ターゲットの EC2 インスタンスで、パスワードの複雑さメカニズムまたは制限が設定されていません。これにより、ユーザーは簡単なパスワードを設定できるため、不正なユーザーがアクセスしたりアカウントを悪用したりする可能性が高まります。

解決策

パスワードを使用している場合は、評価ターゲットのすべての EC2 インスタンスでパスワードの複雑性のレベルを要求するように設定することをお勧めします。そのためには、pwquality.conf ファイルの以下のオプションを使用します: lcredit、ucredit、dcredit、および ocredit。詳細については、https://linux.die.net/man/5/pwquality.conf を参照してください。

pwquality.conf が使用できない場合は、pam_cracklib.so モジュールを使用して、lcredit、ucredit、dcredit、および ocredit オプションを設定します。詳細については、「man pam_cracklib」を参照してください。

以下に示すように、これらの各オプションの期待値は -1 以下です。

```
lcredit <= -1, ucredit <= -1, dcredit<= -1, ocredit <= -1
```

さらに、remember オプションを 12 以上に設定する必要があります。詳細については、「man pam_unix」を参照してください。

ASLR の有効化

このルールは、評価ターゲット内の EC2 インスタンスのオペレーティングシステムでアドレス空間配置のランダム化 (ASLR) が有効であるかどうかを判断するのに役立ちます。

重要度

[Medium] (中)

結果

評価ターゲット内の EC2 インスタンスで ASLR は有効になっていません。

解決策

評価ターゲットのセキュリティを向上させるため、echo 2 | sudo tee /proc/sys/kernel/randomize_va_space を実行してターゲット内のすべての EC2 インスタンスのオペレーティングシステムで ASLR を有効にすることをお勧めします。

DEP の有効化

このルールは、評価ターゲット内の EC2 インスタンスのオペレーティングシステムでデータ実行防止 (DEP) が有効であるかどうかを判断するのに役立ちます。

> **Note**
>
> このルールは、ARM プロセッサを備えた EC2 インスタンスではサポートされません。

重要度

[Medium] (中)

結果

評価ターゲット内の EC2 インスタンスで DEP は有効になっていません。

解決策

評価ターゲット内のすべての EC2 インスタンスのオペレーティングシステムで DEP を有効にすることをお勧めします。DEP を有効にすることで、バッファオーバーフロー技術を使用してセキュリティ侵害からインスタンスを保護できます。

システムディレクトリに対するアクセス許可の設定

このルールは、バイナリとシステム設定情報を含むシステムディレクトリに対する権限をチェックします。root ユーザー (root アカウントの認証情報を使用してログインしたユーザー) のみがこれらのディレクトリに対する書き込み権限を持っていることを確認します。

重要度

高い

結果

評価ターゲット内の EC2 インスタンスに、非 root ユーザーが書き込み可能なシステムディレクトリが含まれています。

解決策

評価ターゲットのセキュリティを向上させ、悪意のあるローカルユーザーによる特権エスカレーションを防ぐため、ターゲット内のすべての EC2 インスタンスのシステムディレクトリを root アカウントの認証情報を使用してログインするユーザー以外が書き込みできないように設定します。

Amazon Inspector Classic の評価テンプレートと評価の実行

Amazon Inspector Classic は、セキュリティルールを使用して AWS リソースを分析することで、潜在的なセキュリティ問題を発見するのに役立ちます。Amazon Inspector Classic は、リソースに関する行動データ (テレメトリ) をモニタリングおよび収集します。データには、安全なチャネルの使用、実行中のプロセス間のネットワークトラフィック、 AWS サービスとの通信の詳細に関する情報が含まれます。次に Amazon Inspector Classic は、データを分析し、セキュリティルールパッケージのセットと比較します。最後に Amazon Inspector Classic は、様々なレベルの重要度の潜在的なセキュリティ上の問題を特定する、結果のリストを作成します。

開始するには、評価ターゲット (Amazon Inspector Classic に分析させる AWS リソースのコレクション) を作成します。次に、評価テンプレート (評価を構成するために使用する設計図) を作成します。テンプレートを使用して、評価の実行、モニタリング、分析プロセスを開始し、結果のセットを作成します。

トピック

- Amazon Inspector Classic 評価テンプレート
- Amazon Inspector Classic 評価テンプレートの制限
- 評価テンプレートを作成する
- 評価テンプレートを削除する
- 評価の実行
- Amazon Inspector Classic 評価実行の制限
- Lambda 関数を使用した評価の自動実行のセットアップ
- Amazon Inspector Classic 通知用の SNS トピックの設定

Amazon Inspector Classic 評価テンプレート

評価テンプレートでは、次のものを含む評価の実行の設定を指定できます。

- 評価ターゲットの評価で Amazon Inspector Classic が使用するルールパッケージ
- 評価の実行時間 – 評価の実行時間は、3 分から 24 時間の範囲で設定できます。評価の実行期間を 1 時間に設定することをお勧めします。
- Amazon Inspector Classic が評価の実行状態と結果について通知を送信する Amazon SNS トピック

- この評価テンプレートを使用する評価の実行で生成された結果を割り当てることができる Amazon Inspector Classic 属性 (キーと値のペア)。

Amazon Inspector Classic が評価テンプレートを作成すると、他の AWS リソースと同様にタグ付けすることができます。詳細については、「タグ エディタ」を参照してください。評価テンプレートにタグ付けすることで、テンプレートを整理してセキュリティ戦略をより適切に管理することができます。例えば、Amazon Inspector Classic は評価ターゲットについて評価できる多数のルールを提供します。評価テンプレートに利用可能なルールのさまざまなサブセットを含めて、問題がありそうな特定の領域をターゲットにしたり、特定のセキュリティ問題を発見したりすることができます。評価テンプレートにタグ付けすれば、セキュリティ戦略とその目的に応じて、任意のタイミングで素早くテンプレートを発見して実行できます。

> **Important**
>
> 評価テンプレートを作成したら、それを変更することはできません。

Amazon Inspector Classic 評価テンプレートの制限

AWS アカウントごとに最大 500 の評価テンプレートを作成できます。

詳細については、「Amazon Inspector Classic サービスの制限」を参照してください。

評価テンプレートを作成する

評価ターゲットテンプレートを作成するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/inspector/ で Amazon Inspector Classic コンソールを開きます。
2. ナビゲーションペインの [Assessment templates (評価テンプレート)] を選択し、[Create (作成)] を選択します。
3. [Name (名前)] に、評価テンプレートの名前を入力します。
4. [Target name] では、分析する評価ターゲットを選択します。

> **Note**
>
> 評価テンプレートを作成すると、[Assessment Templates] ページの [Preview Target] ボタンを使用して、評価ターゲットに含まれているすべての EC2 インスタンスを確認することもできます。EC2 インスタンスごとに、ホスト名、インスタンス ID、IP アドレス、および該当する場合はエージェントのステータスを確認できます。エージェントのステータス実行コマンド には、次の値を指定できます。HEALTHY、UNHEALTHY、UNKNOWN Amazon Inspector Classic は、EC2 インスタンスで実行中のエージェントがあるかどうかを判断できない場合、UNKNOWN ステータスを表示します。
> また、[Assessment Templates] ページの [Preview Target] ボタンを使用して、以前作成したテンプレートに含まれている評価ターゲットを構成する EC2 インスタンスを表示することもできます。

5. [Rules packages] では、評価テンプレートに含む 1 つ以上のルールパッケージを選択します。
6. Duration では、評価テンプレートの時間を指定します。
7. (オプション) SNS トピックについては、Amazon Inspector Classic が評価の実行状態と結果について通知を送信する SNS トピックを指定します。Amazon Inspector Classic は、次のイベントに関する SNS 通知を送信できます。

   - 評価の実行が開始された
   - 評価の実行が終了した
   - 評価の実行のステータスが変更された
   - 結果が作成された

   SNS トピックの設定の詳細については、「Amazon Inspector Classic 通知用の SNS トピックの設定」を参照してください。
8. (オプション) [Tag (タグ)] で [Key (キー)] と [Value (値)] の値を入力します。評価テンプレートには複数のタグを追加できます。
9. (オプション) [Attributes added to findings] については、[Key] と [Value] の値を入力します。Amazon Inspector Classic は、評価テンプレートによって生成された、すべての結果に属性を適用します。評価テンプレートには複数の属性を追加できます。結果と結果のタグ付けの詳細については、「Amazon Inspector Classic 結果」を参照してください。

10. (オプション) このテンプレートを使用して評価の実行スケジュールをセットアップするには、[Set up recurring assessment runs once every <number_of_days>, starting now (定期的な評価の実行をセットアップする、<number_of_days> に 1 回、今すぐ開始)] チェックボックスにチェックを選択し、上下の矢印を使用して繰り返しパターン (日数) を指定します。

> **Note**
>
> このチェックボックスを使用すると、Amazon Inspector Classic によってセットアップされた評価実行スケジュール用の Amazon CloudWatch Events ルールが自動的に作成されます。その後、Amazon Inspector Classic は、`AWS_InspectorEvents_Invoke_Assessment_Template` という名前の IAM ロールも自動的に作成します。このロールを使用して、CloudWatch Events が Amazon Inspector Classic のリソースに対して API コールを行うことができます。詳細については、「Amazon CloudWatch Events とは」および「CloudWatch Events のリソースベースのポリシーを使用する」を参照してください。

> **Note**
>
> また、 AWS Lambda 関数を使用して評価の自動実行をセットアップすることもできます。詳細については、「Lambda 関数を使用した評価の自動実行のセットアップ」を参照してください。

11. [Create and run] または [Create] を選択します。

評価テンプレートを削除する

評価テンプレートを削除するには、次の手順を実行します。

評価テンプレートを削除するには

- [Assessment Templates (評価テンプレート)] ページで、削除するテンプレートを選択し、[Delete (削除)] を選択します。確認を求めるメッセージが表示されたら、実行コマンドYes実行コマンド を選択します。

> **Important**
>
> 評価テンプレートを削除すると、すべての評価の実行、結果、このテンプレートに関連付けられたバージョンのレポートも削除されます。

`DeleteAssessmentTemplate` API を使用して評価テンプレートを削除することもできます。

評価の実行

作成した評価テンプレートは、評価の実行を開始するのに使用できます。各 AWS アカウントの実行制限内であれば、同じテンプレートを使用して複数の実行を開始できます。詳細については、「Amazon Inspector Classic 評価実行の制限」を参照してください。

Amazon Inspector Classic コンソールを使用する場合は、[Assessment templates (評価テンプレート)] ページから、新しい評価テンプレートの最初の実行を開始する必要があります。実行を開始した後、[Assessment runs] ページを使用して実行の進行状況をモニタリングできます。[Run]、[Cancel]、および [Delete] ボタンを使用して、実行を開始、キャンセル、または削除します。実行の ARN、実行するために選択されたルールパッケージ、実行に適用したタグと属性などの実行の詳細を表示できます。

評価テンプレートのそれ以降の実行では、[Assessment templates] ページまたは [Assessment runs] ページで [Run]、[Cancel]、[Delete] ボタンを使用することができます。

評価の実行を削除する

評価の実行を削除するには、次の手順を実行します。

実行を削除するには

- [評価の実行] ページで、削除する実行を選択し、[削除] を選択します。確認を求めるメッセージが表示されたら、実行コマンドYes実行コマンド を選択します。

> **Important**
>
> 実行を削除すると、その実行のすべての結果とすべてのバージョンのレポートも削除されます。

以下の DeleteAssessmentRun API を使用してディストリビューションを削除することもできます。

Amazon Inspector Classic 評価実行の制限

AWS アカウントごとに最大 50,000 の評価実行を作成できます。

評価の実行は、使用されるターゲットに EC2 インスタンスの重複が含まれない限り、同時進行させることができます。

詳細については、「Amazon Inspector Classic サービスの制限」を参照してください。

Lambda 関数を使用した評価の自動実行のセットアップ

評価の定期的なスケジュールをセットアップする場合は、 AWS Lambda コンソールを使用して Lambda 関数を作成し、評価テンプレートを自動的に実行するように設定できます。詳細については、Lambda 関数を参照してください。

AWS Lambda コンソールを使用して自動評価実行を設定するには、次の手順を実行します。

Lambda 関数を使用した評価の自動実行をセットアップするには

1. にサインインし AWS マネジメントコンソール、 AWS Lambda コンソールを開きます。
2. ナビゲーションペインで [Dashboard (ダッシュボード)] または [Functions (関数)] を選択し、[Create a Lambda Function(Lambda 関数の作成)] を選びます。
3. [Create function (関数の作成)] ページで、[Browse serverless app repository (サーバーレスアプリリポジトリの参照)] を選択し、検索フィールドに「**inspector**」と入力します。
4. 設計図として inspector-scheduled-run を選択します。
5. [Review, configure, and deploy (確認、設定、デプロイ)] ページで、関数をトリガーする CloudWatch イベントを指定して、自動実行用の定期的なスケジュールをセットアップします。これを行うには、ルールの名前と説明を入力し、スケジュール式を選択します。スケジュール式は、実行の頻度を決定します。たとえば、15 分ごと、または 1 日 1 回などです。CloudWatch イベントと概念の詳細については、「Amazon CloudWatch Events とは」を参照してください。

   [Enable trigger (トリガーの有効化)] のチェックボックスをオンにした場合、実行は関数の作成が完了した直後に開始されます。それ以降の自動的な実行は [Schedule expression (スケジュール式)] で指定した定期的なパターンに従います。関数の作成時に [Enable trigger] のチェックボックスをオンにしない場合は、後で関数を編集して、このトリガーを有効にすることができます。

6. [Configure function] ページで、次の項目を指定します。

   - [名前] に、関数の名前を入力します。
   - (オプション) [Description (説明)] に、関数を識別するための説明を入力します。
   - ランタイムの場合、デフォルト値の のままにします**Node.js 8.10**。 は、**Node.js 8.10**ランタイムに対してのみ inspector-scheduled-run ブループリント AWS Lambda をサポートします。
   - この関数を使用して自動的に実行される評価テンプレート。それには [assessmentTemplateArn] と呼ばれる環境変数の値を指定します。
   - ハンドラはデフォルト値の「**index.handler**」に設定します。
   - [Role] フィールドを使用する関数の権限。詳細については、「AWS Lambda のアクセス許可モデル」を参照してください。

     この関数を実行するには、 が実行 AWS Lambda を開始し、エラーを含む実行に関するログメッセージを Amazon CloudWatch Logs に書き込むことを許可する IAM ロールが必要です。 は、定期的な自動実行ごとにこのロール AWS Lambda を引き受けます。たとえば、次のサンプルポリシーをこの IAM ロールにアタッチできます。

     JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "inspector:StartAssessmentRun",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": "*"
    }
  ]
}
```

7. 場所を確認して [Create function] を選択します。

Amazon Inspector Classic 通知用の SNS トピックの設定

Amazon Simple Notification Service(Amazon SNS) は、サブスクライブしているエンドポイントやクライアントへのメッセージを送信する、ウェブサービスです。Amazon SNS を使用して Amazon Inspector Classic の通知をセットアップできます。

通知用の SNS トピックを設定するには

1. SNS トピックを作成します。チュートリアル :Amazon SNS トピックを作成するを参照してください。トピックを作成したら、[Access policy - optional (アクセスポリシー - オプション)] セクションを展開します。次に、以下の操作を実行し、評価からトピックへのメッセージを送信を許可します。

   a. [Choose method (メソッドの選択)] で、[Basic] を選択します。

   b. トピックにメッセージを発行できるユーザーを定義する で、指定した AWS アカウントのみを選択し、トピックを作成するリージョンのアカウントの ARN を入力します。

      - US East (Ohio) - arn:aws:iam::646659390643:root
      - US East (N. Virginia) - arn:aws:iam::316112463485:root
      - US West (N. California) - arn:aws:iam::166987590008:root
      - US West (Oregon) - arn:aws:iam::758058086616:root
      - Asia Pacific (Mumbai) - arn:aws:iam::162588757376:root
      - Asia Pacific (Seoul) - arn:aws:iam::526946625049:root
      - Asia Pacific (Sydney) - arn:aws:iam::454640832652:root
      - Asia Pacific (Tokyo) - arn:aws:iam::406045910587:root
      - Europe (Frankfurt) - arn:aws:iam::537503971621:root
      - Europe (Ireland) - arn:aws:iam::357557129151:root
      - Europe (London) - arn:aws:iam::146838936955:root
      - Europe (Stockholm) - arn:aws:iam::453420244670:root
      - AWS GovCloud (US-East) - arn:aws-us-gov:iam::206278770380:root
      - AWS GovCloud (US-West) - arn:aws-us-gov:iam::850862329162:root

   c. このトピックをサブスクライブできるユーザーを定義する で、指定された AWS アカウントのみを選択し、トピックを作成するリージョンのアカウントの ARN を入力します。

d. 「IAM ユーザーガイド」の「Confused deputy problem (混乱した代理の問題)」で説明されているように、Inspector が混乱した代理として使われることを防ぐため、次の作業を行います。

i. [Advanced] (アドバンスト) を選択します。これにより JSON エディタに移動します。

ii. 次の条件を追加します。

```
"Condition": {
   "StringEquals": {
     "aws:SourceAccount": <your account Id here>,
     "aws:SourceArn": "arn:aws:inspector:*:*:*"
   }
 }
```

e. (オプション) aws:SourceAccount および aws:SourceArn の詳細については、IAM ユーザーガイドの「グローバル条件コンテキストキー」を参照してください。

f. 必要に応じてトピックの他の設定を更新し、[Create topic (トピックの作成)] を選択します。

2. (オプション) 暗号化された SNS トピックを作成するには、SNS デベロッパーガイドの「保管時の暗号化」を参照してください。

3. Inspector が KMS キーの混乱した代理として使用されるのを防ぐには、以下の追加手順に従います。

a. KMS コンソールで CMK に移動します。

b. [編集] を選択します。

c. 次の条件を追加します。

```
"Condition": {
   "StringEquals": {
     "aws:SourceAccount": <your account Id here>,
     "aws:SourceArn": "arn:aws:sns:*:*:*"
   }
 }
```

4. 作成したトピックへのサブスクリプションを作成します。詳細については、チュートリアル :Amazon SNS トピックにエンドポイントをサブスクライブするを参照してください。
5. サブスクリプションが正しく設定されていることを確認するには、そのトピックに対してメッセージを発行します。詳細については、チュートリアル: Amazon SNS トピックにメッセージを発行するを参照してください。

Amazon Inspector Classic 結果

結果は、評価ターゲットの評価中に Amazon Inspector Classic が発見する潜在的なセキュリティ上の問題です。結果は Amazon Inspector Classic コンソールに表示されるか、API を介して取得されます。結果には、セキュリティ問題の詳細な説明とそれらを解決するための推奨事項が含まれています。

Amazon Inspector が生成した結果は、Amazon Inspector Classic 属性を割り当てて追跡することができます。これらの属性はキー値のペアで構成されています。

属性による結果の追跡は、セキュリティ戦略のワークフローを迅速化するのに非常に便利です。たとえば、評価を作成して実行すると、セキュリティ上の目標やアプローチに基づいて重大度、緊急度、ユーザーの関心度が様々に異なる結果のリストが生成されます。その中で緊急度の高いセキュリティ上の問題をすぐに解決するために、1 つの結果で推奨される手順を実行することが必要な場合があります。または、次のサービス更新まで別の結果の解決を保留することが必要な場合もあります。たとえば、すぐに解決する必要がある結果を追跡するには、[**Status**]/[**Urgent**] のキーと値のペアで属性を作成して結果に割り当てます。属性を使用して潜在的なセキュリティ上の問題の解決のワークロードを分散することもできます。たとえば、チームのセキュリティエンジニアである Bob にタスクとして結果の解決を割り当てるには、[**Assigned Engineer**]/[**Bob**] のキーと値のペアで属性を割り当てます。

結果を使用する

生成された Amazon Inspector Classic 結果で、次の手順を実行します。

結果を見つけて分析し、属性を割り当てるには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/inspector/ で Amazon Inspector Classic コンソールを開きます。
2. 評価を実行したら、Amazon Inspector Classic コンソールの [結果] ページに移動して結果を表示します。

   結果は、Amazon Inspector Classic コンソールのダッシュボードページの [注目すべき結果] セクションでも確認できます。

> **Note**
>
> 評価の実行が進行中の間は、評価の実行で生成された結果を表示することはできません。ただし、最後まで完了する前に評価を停止した場合、発見のサブセットを表示できます。本稼働環境では、完全な結果を得るために、すべての評価の実行を最後まで完了することをお勧めします。

3. 特定の結果の詳細を表示するには、結果の横の [Expand] ウィジェットを選択します。結果の詳細には次の情報が含まれます。

   - 結果が登録された EC2 インスタンスを含む評価ターゲットの名前。
   - この結果を生成するために使用された評価テンプレートの名前。
   - 評価の実行の開始時間。
   - 評価の実行の終了時間。
   - 評価の実行のステータス。
   - この結果をトリガーしたルールを含むルール パッケージの名前。
   - 結果の名前。
   - 結果の重要度。
   - 共通脆弱性評価システム (CVSS) によるネイティブの深刻度の詳細。これには、通脆弱性識別子ルールパッケージのルールによってトリガーされる結果に対する CVSS ベクトルと CVSS スコアのスコアメトリクス (CVSS バージョン 2.0 および 3.0 を含む) が含まれます。CVSS の詳細については、「https://www.first.org/cvss/」を参照してください。
   - Center for Internet Security (CIS) のネイティブ重要度の詳細。これらは CIS ベンチマーク パッケージのルールによってトリガーされた結果のための CIS 重み付けメトリクスを含みます。CIS の重み付けメトリクスの詳細については、https://www.cisecurity.org/ を参照してください。
   - 結果の説明。
   - 結果で説明されている潜在的なセキュリティ上の問題を解決するために推奨されるステップ。

4. 結果に属性を割り当てるには、結果を選択して [Add/Edit Attributes] を選択します。

   評価テンプレートを作成するときに、結果に属性を割り当てることもできます。これを行うには、評価実行によって生成されたすべての検出結果に属性を自動的に割り当てるように新しいテンプレートを設定します。[この評価の結果のタグ] フィールドには、[キー] フィールドと [値]

フィールドを使用できます。詳細については、「Amazon Inspector Classic の評価テンプレートと評価の実行」を参照してください。

5. 結果をスプレッドシートにエクスポートするには、[結果] ページの右上端にある下向きの矢印ボタンを選択します。ダイアログボックスで、[Export all columns (すべての列のエクスポート)] または [Export visible columns (表示された列のエクスポート)] を選択します。

   エクスポートされたコンテンツでは、すべての日時値はエポックタイムスタンプです。

6. 現在の結果をフィルタリングするには、インスタンス ID や CVE 番号など、フィルターの対象となる 1 つの文字列を、結果テーブルの上にあるフィルターバーに入力します。[追加情報] 列を表示または非表示にするには、[結果] ページの右上隅にある設定アイコンをクリックします。

7. 結果を削除するには、[評価の実行] ページに移動し、削除する結果の実行を選択します。その後、[削除] をクリックします。確認を求めるメッセージが表示されたら、実行コマンドYes実行コマンド を選択します。

> **Important**
>
> Amazon Inspector Classic では、個別の結果を削除することはできません。評価の実行を削除すると、その実行のすべての結果とすべてのバージョンのレポートも削除されます。

DeleteAssessmentRun API を使用して評価の実行を削除することもできます。

評価レポート

Amazon Inspector Classic 評価レポートは評価の実行で行われたテストの詳細と、評価の結果を記述したドキュメントです。レポートを保存したり、チームと修正処理のために共有したり、コンプライアンス監査データを増強するために使用することができます。実行が正常に完了した後に、評価実行のレポートを生成できます。

> **Note**
>
> 2017 年 4 月 25 日以降、つまり Amazon Inspector Classic の評価レポートが利用可能になった後の評価実行に対してのみレポートを生成できます。

次のタイプの評価レポートを表示できます。

- 結果レポート - このレポートには次の情報が含まれます。
  - 評価のサマリー
  - 評価の実行中に検証された EC2 インスタンス
  - 評価の実行に含まれているルールパッケージ
  - 結果が出た EC2 インスタンスを含むすべての結果に関する詳細情報
- フルレポート – このレポートは結果レポートに含まれるすべての情報と、評価ターゲットのインスタンスに対してチェックされたルールのリストを提供します。

評価レポートを生成するには

1. [Assessment runs (評価の実行)] ページで、レポートを生成する評価実行を見つけます。そのステータスが、[Analysis complete (分析完了)] に設定されていることを確認してください。
2. この評価の実行の [Reports (レポート)] 列で、レポートのアイコンを選択します。

> **Important**
>
> 2025 年 3 月 24 日以降、評価レポートにはネットワーク到達可能性の検出結果の重要度情報が含まれなくなります。この情報は Amazon Inspector コンソールで入手できます。

3. [Assessment report (評価レポート)] ダイアログボックスで、表示するレポートの種類 (結果またはフルレポート) とレポート形式 (HTML または PDF) を選択します。次に、[Generate report (レポートの生成)] を選択します。

評価レポートは GetAssessmentReport API からでも生成できます。

監査レポートを削除するには、次の手順を実行します。

レポートを削除するには

- [評価の実行] ページで、削除するレポートの基になっている実行を選択してから、[削除] を選択します。確認を求めるメッセージが表示されたら、実行コマンドYes実行コマンド を選択します。

  > **Important**
  >
  > Amazon Inspector Classic では、個別の結果を削除することはできません。評価の実行を削除すると、その実行のすべてのバージョンのレポートとすべての結果も削除されます。

  DeleteAssessmentRun API を使用して評価の実行を削除することもできます。

Amazon Inspector Classic の除外

除外は Amazon Inspector Classic 評価の実行の出力です。除外により、完了できないセキュリティチェックと問題を解決する方法が示されます。例えば、指定されたターゲットの EC2 インスタンスにエージェントが存在しない、サポートされていないオペレーティングシステムが使用されている、または予期しないエラーが原因で問題が発生する可能性があります。

除外は、コンソールの [Assessment runs (評価の実行)] ページで確認できます。詳細については、「評価後の除外の確認」を参照してください。

不要な AWS 料金が発生しないように、Amazon Inspector Classic では、評価を実行する前に除外をプレビューできます。除外のプレビューは、コンソールの [Assessment templates (評価テンプレート)] ページで確認できます。詳細については、「除外のプレビュー」を参照してください。

> **Note**
>
> 2018 年 6 月 25 日以降に発生した実行に対してのみ、評価後の除外を生成できます。それが Amazon Inspector Classic の除外が利用可能になったときです。ただし、除外のプレビューは日付に関係なくすべての評価テンプレートで確認できます。

トピック

- 除外タイプ
- 除外のプレビュー
- 評価後の除外の確認

除外タイプ

Amazon Inspector Classic で生成できる除外タイプは以下のとおりです。

除外タイプ	説明	推奨事項
ターゲットにインスタンスがない	評価ターゲットで指定したタグを含む EC2 インスタンスがありません。	評価ターゲットのタグとターゲット EC2 インスタンスのタグが一致していることを確認します。
エージェントが既に実行されている	ターゲット EC2 インスタンスで評価の実行が既に進行中です。	ターゲット EC2 インスタンスで現在進行中の評価の実行が完了するまで待ちます。
エージェ	ターゲット EC2 イ	ターゲット EC2 イ

除外タイプ	説明	推奨事項
ントが見つからない	ンスタンスで Amazon Inspector Classic エージェントが見つかりませんでした。	ンスタンスに Amazon Inspector Classic エージェントをインストールするか再インストールします。詳細については、「Amazon Inspector Classic エージェントのインストール」を参照してください。

除外タイプ	説明	推奨事項
エージェントが異常	ターゲット EC2 インスタンスの Amazon Inspector Classic エージェントが異常な状態になっています。	このインスタンスの Amazon Inspector Classic エージェントの状況をチェックして、必要なアクションを実行してください。詳細については、「Inspector エージェント」を参照してください。

除外タイプ	説明	推奨事項
サポート対象外の OS バージョン	Amazon Inspector Classic 評価で、ターゲット EC2 インスタンスのオペレーティングシステムがサポートされていません。	評価ターゲットからターゲット EC2 インスタンスを削除するか、このインスタンスを含まないターゲットを作成します。サポート対象のオペレーティングシステムのリストについては、「Amazon Inspector Classic のサポート対象のオペレーティングシステムとリージョン」を参照してください。

除外タイプ	説明	推奨事項
廃止されたルールパッケージ	評価テンプレートに廃止されたルールパッケージが含まれています。	廃止されたルールパッケージを含まない評価テンプレートを作成し、今後評価を実行するときに使用します。

除外タイプ	説明	推奨事項
OS でルールパッケージがサポートされていない	評価テンプレートに含まれるルールパッケージでターゲット EC2 インスタンスのオペレーティングシステムがサポートされていません。	競合するルールパッケージを含まない評価テンプレートを作成するか、評価テンプレートからターゲット EC2 インスタンスを削除します。オペレーティングシステムでサポートされるルールパッケージのリストについては、「サポート対象のオペレーティングシステムで使用できるルールパッケージ」を

除外タイプ	説明	推奨事項
		参照してください。
単一のインスタンスのルール評価エラー	内部エラーが原因となり、このインスタンスのルール評価が失敗しました。	もう一度評価の実行を試みます。評価を再実行しても除外された場合は、サポートにお問い合わせください。
ルール評価エラー	内部エラーが原因となり、評価のルール評価が失敗しました。	もう一度評価の実行を試みます。評価を再実行しても除外された場合は、サポートにお問い合わせください。

除外タイプ	説明	推奨事項
ネットワーク到達可能性エラー – インターネット	内部エラーにより、ネットワーク到達可能性の評価で、インターネットから到達可能なポートのチェックに失敗しました。他のネットワーク到達可能性タイプについて結果が表示される場合があります。	もう一度評価の実行を試みます。評価を再実行しても除外された場合は、サポートにお問い合わせください。

除外タイプ	説明	推奨事項
ネットワーク到達可能性エラー – Application Load Balancer を介したインターネット	内部エラーにより、ネットワーク到達可能性の評価で、Application Load Balancer を介したインターネットから到達可能なポートのチェックに失敗しました。他のネットワーク到達可能性タイプについて結果が表示される場合があります。	もう一度評価の実行を試みます。評価を再実行しても除外された場合は、サポートにお問い合わせください。

除外タイプ	説明	推奨事項
ネットワーク到達可能性エラー - Elastic Load Balan ロードバランサーを介したインターネット	内部エラーにより、ネットワーク到達可能性の評価で、Elastic Load Balancing ロードバランサーを介したインターネットから到達可能なポートのチェックに失敗しました。他のネットワーク到達可能性タイプについて結果が表示される場合があります。	もう一度評価の実行を試みます。評価を再実行しても除外された場合は、サポートにお問い合わせください。

除外タイプ	説明	推奨事項
ネットワーク到達可能性エラー - VPN	内部エラーにより、ネットワーク到達可能性の評価で、VPN から到達可能なポートのチェックに失敗しました。他のネットワーク到達可能性タイプについて結果が表示される場合があります。	もう一度評価の実行を試みます。評価を再実行しても除外された場合は、サポートにお問い合わせください。

除外タイプ	説明	推奨事項
ネットワーク到達可能性エラー – AWS Direct Conne	内部エラーにより、ネットワーク到達可能性の評価が、到達可能なポートのチェックで失敗しました AWS Direct Connect。他のネットワーク到達可能性タイプについて結果が表示される場合があります。	もう一度評価の実行を試みます。評価を再実行しても除外された場合は、サポートにお問い合わせください。

除外タイプ	説明	推奨事項
ネットワーク到達可能性エラー - VPC ピアリング	内部エラーにより、ネットワーク到達可能性の評価で、ピア接続の VPC から到達可能なポートのチェックに失敗しました。他のネットワーク到達可能性タイプについて結果が表示される場合があります。	もう一度評価の実行を試みます。評価を再実行しても除外された場合は、サポートにお問い合わせください。

除外のプレビュー

Amazon Inspector Classic では、評価の実行前に潜在的な除外をプレビューできます。

評価の除外をプレビューするには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/inspector/ で Amazon Inspector Classic コンソールを開きます。
2. ナビゲーションペインで、[Assessment templates (評価テンプレート)] を選択します。

3. 評価テンプレートを展開し、[Assessment templates (評価テンプレート)] セクションで [Preview exclusions (除外のプレビュー)] を選択します。
4. 検出されたすべての除外の説明とそれらに対処するための推奨事項を確認します。

   また、それぞれ `ListExclusions` と `DescribeExclusions` のオペレーションを使用して除外するものをリストし、記述することもできます。

評価後の除外の確認

評価の実行後に、除外の詳細を確認できます。

除外の詳細情報を表示するには

1. にサインイン AWS マネジメントコンソール し、https://console.aws.amazon.com/inspector/ で Amazon Inspector Classic コンソールを開きます。
2. ナビゲーションペインで、Assessment runs (評価の実行) を選択します。
3. [Exclusions (除外)] 列で、評価の実行に関連付けられているアクティブなリンクを選択します。
4. 検出されたすべての除外の説明とそれらに対処するための推奨事項を確認します。

   また、それぞれ `ListExclusions` と `DescribeExclusions` のオペレーションを使用して除外するものをリストし、記述することもできます。

サポートされているオペレーティングシステムの Amazon Inspector Classic ルールパッケージ

評価対象に含まれている EC2 インスタンスに対して Amazon Inspector Classic ルールパッケージを実行できます。次のテーブルは、サポートされているオペレーティングシステムのルールパッケージの可用性を示しています。

Important

オペレーティングシステムに関係なく、任意の EC2 インスタンスで Network Reachability ルールパッケージを使用してエージェントレス評価を実行できます。

Note

サポートされるオペレーティングシステムの詳細については、「Amazon Inspector Classic でサポートされているオペレーティングシステムとリージョン」を参照してください。

サポートされるオペレーティングシステム	共通脆弱性識別子	CIS ベンチマーク	ネットワーク到達可能性	セキュリティのベストプラクティス	ランタイム動作分析
Amaz Linux 2	サポート対象	サポート対象	サポート対象	サポート	非推奨
Amaz Linux 2018.	サポート対象	サポート対象	サポート対象	サポート	非推奨
Amaz Linux 2017.	サポート対象	サポート対象	サポート対象	サポート	非推奨
Amaz Linux 2017.	サポート対象	サポート対象	サポート対象	サポート	非推奨
Amaz Linux 2016.	サポート対象	サポート対象	サポート対象	サポート	非推奨

サポートされるオペレーティングシステム	共通脆弱性識別子	CIS ベンチマーク	ネットワーク到達可能性	セキュリティのベストプラクティス	ランタイム動作分析
Amaz Linux 2016.	サポート対象	サポート対象	サポート対象	サポート	非推奨
Amaz Linux 2015.	サポート対象	サポート対象	サポート対象	サポート	非推奨
Amaz Linux 2015.	サポート対象	サポート対象	サポート対象	サポート	非推奨
Amaz Linux 2014.	サポート対象		サポート対象	サポート	
Amaz Linux 2014.	サポート対象		サポート対象	サポート	

サポートされるオペレーティングシステム	共通脆弱性識別子	CIS ベンチマーク	ネットワーク到達可能性	セキュリティのベストプラクティス	ランタイム動作分析
Amaz Linux 2013.	サポート対象		サポート対象	サポート	
Amaz Linux 2013.	サポート対象		サポート対象	サポート	
Amaz Linux 2012.	サポート対象		サポート対象	サポート	
Amaz Linux 2012.	サポート対象		サポート対象	サポート	
Ubun 20.04 LTS	サポート対象		サポート対象	サポート	

サポートされるオペレーティングシステム	共通脆弱性識別子	CIS ベンチマーク	ネットワーク到達可能性	セキュリティのベストプラクティス	ランタイム動作分析
Ubun 18.04 LTS	サポート対象	サポート対象	サポート対象	サポート	非推奨
Ubun 16.04 LTS	サポート対象	サポート対象	サポート対象	サポート	非推奨
Ubun 14.04 LTS	サポート対象	サポート対象	サポート対象	サポート	非推奨
Debia 10.x, 9.0 - 9.5, 8.0 - 8.7	サポート対象		サポート対象	サポート	

サポートされるオペレーティングシステム	共通脆弱性識別子	CIS ベンチマーク	ネットワーク到達可能性	セキュリティのベストプラクティス	ランタイム動作分析
RHEL 8.x	サポート対象		サポート対象	サポート	
RHEL 7.6 - 7.x	サポート対象	サポート対象	サポート対象	サポート	
RHEL 6.2 - 6.9、 - 7.5	サポート対象	サポート対象	サポート対象	サポート	非推奨
Cent(7.6 ~ 7.X	サポート対象	サポート対象	サポート対象	サポート	

サポートされるオペレーティングシステム	共通脆弱性識別子	CIS ベンチマーク	ネットワーク到達可能性	セキュリティのベストプラクティス	ランタイム動作分析
Cent(6.2 ~ 6.9、 ~ 7.5	サポート対象	サポート対象	サポート対象	サポート	非推奨
Wind(Serve 2019 ベース	サポート対象		サポート		
Wind(Serve 2016 ベース	サポート対象	サポート対象	サポート		非推奨

サポートされるオペレーティングシステム	共通脆弱性識別子	CIS ベンチマーク	ネットワーク到達可能性	セキュリティのベストプラクティス	ランタイム動作分析
Windo Serve 2012 R2	サポート対象	サポート対象	サポート		非推奨
Windo Serve 2012	サポート対象	サポート対象	サポート		非推奨
Windo サーバー 2008 R2	サポート対象	サポート対象	サポート		非推奨

を使用した Amazon Inspector Classic API コールのログ記録 AWS CloudTrail

Amazon Inspector Classic は AWS CloudTrail、Amazon Inspector Classic のユーザー、ロール、または のサービスによって実行されたアクションを記録する AWS サービスである と統合されています。CloudTrail は、Amazon Inspector Classic コンソールからの呼び出しと Amazon Inspector Classic API オペレーションへのコード呼び出しを含む、Amazon Inspector Classic の API コールをイベントとしてキャプチャします。追跡を作成する場合は、Amazon Inspector Classic のイベントなど、Amazon S3 バケットへの CloudTrail イベントの継続的な配信を有効にすることができます。追跡を設定しない場合でも、CloudTrail コンソールの [イベント履歴] で最新のイベントを確認できます。CloudTrail で収集された情報を使用して、Amazon Inspector Classic に対するリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

CloudTrail の詳細については、「AWS CloudTrail ユーザーガイド」を参照してください。Amazon Inspector Classic API オペレーションの完全なリストについては、Amazon Inspector Classic API リファレンスのアクションを参照してください。

CloudTrail での Amazon Inspector Classic 情報

CloudTrail は、 AWS アカウントの作成時にアカウントで有効になります。Amazon Inspector Classic でアクティビティが発生すると、そのアクティビティはイベント履歴の他の AWS サービスイベントとともに CloudTrail イベントに記録されます。最近のイベントは、 AWS アカウントで表示、検索、ダウンロードできます。詳細については、CloudTrail イベント履歴でのイベントの表示を参照してください。

Amazon Inspector Classic のイベントなど、 AWS アカウントのイベントの継続的な記録については、証跡を作成します。証跡により、CloudTrail はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで証跡を作成するときに、証跡がすべての AWS リージョンに適用されます。証跡は、 AWS パーティション内のすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、CloudTrail ログで収集されたイベントデータをさらに分析して処理するように他の AWS サービスを設定できます。詳細については、次を参照してください:

- 証跡の作成のための概要
- CloudTrail がサポートするサービスと統合
- CloudTrail 用 Amazon SNS 通知の構成

- 複数のリージョンから CloudTrail ログファイルを受け取るおよび複数のアカウントから CloudTrail ログファイルを受け取る

CloudTrailは、読み取り専用オペレーション (`ListAssessmentRuns` や `DescribeAssessmentTargets` など)、および管理オペレーション (`AddAttributesToFindings` や `CreateAssessmentTemplate` など) を含むすべてのAmazon Inspector Classic オペレーションを記録します。

> **Note**
>
> CloudTrail は Amazon Inspector Classic 読み取りオペレーションのリクエスト情報のみをログに記録します。リクエストと応答の両方の情報が、他のすべての Amazon Inspector Classic オペレーションについて記録されます。

各イベントまたはログエントリには、誰がリクエストを生成したかという情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます。

- リクエストがルートまたは AWS Identity and Access Management (IAM) ユーザー認証情報を使用して行われたかどうか
- リクエストの送信に使用された一時的なセキュリティ認証情報に、ロールとフェデレーテッドユーザーのどちらが使用されたか
- リクエストが別の AWS サービスによって行われたかどうか

詳細については、「CloudTrail userIdentity 要素」を参照してください。

Amazon Inspector Classic ログファイルエントリの理解

「トレイル」は、指定した Amazon S3 バケットにイベントをログファイルとして配信するように設定できます。CloudTrail のログファイルには、ログエントリが 1 つ以上あります。イベントは任意の出典からの 1 つのリクエストを表し、リクエストされたアクション、アクションの日時、その他のリクエストのパラメータなどに関する情報が含まれます。CloudTrail ログファイルは、パブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

Amazon Inspector Classic `CreateResourceGroup` オペレーションを示す CloudTrail ログエントリの例は、次のとおりです。

```
{
    "eventVersion": "1.03",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::444455556666:user/Alice",
        "accountId": "444455556666",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2016-04-14T17:05:54Z"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::444455556666:user/Alice",
                "accountId": "444455556666",
                "userName": "Alice"
            }
        }
    },
    "eventTime": "2016-04-14T17:12:34Z",
    "eventSource": "inspector.amazonaws.com",
    "eventName": "CreateResourceGroup",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.179",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "resourceGroupTags": [
            {
                "key": "Name",
                "value": "ExampleEC2Instance"
            }
        ]
    },
    "responseElements": {
        "resourceGroupArn": "arn:aws:inspector:us-west-2:444455556666:resourcegroup/0-
oclRMp8B"
    },
    "requestID": "148256d2-0264-11e6-a9b5-b98a7d3b840f",
    "eventID": "e5ea533e-eede-46cc-94f6-0d08e6306ff0",
    "eventType": "AwsApiCall",
```

```
    "apiVersion": "v20160216",
    "recipientAccountId": "444455556666"
}
```

Amazon CloudWatch を使用した Amazon Inspector Classic のモニタリング

Amazon CloudWatch を使用して Amazon Inspector Classic をモニタリングすることで、raw データを収集し、リアルタイムに近い読み取り可能なメトリクスに加工することができます。デフォルトでは、Amazon Inspector Classic は 5 分ごとにメトリクスデータを CloudWatch に送信します。AWS マネジメントコンソール、 AWS CLI、または API を使用して、Amazon Inspector Classic が CloudWatch に送信するメトリクスを表示できます。

Amazon CloudWatch の詳細については、Amazon CloudWatch ユーザーガイドを参照してください。

Amazon Inspector Classic の CloudWatch メトリクス

Amazon Inspector Classic の名前空間には、次のメトリクスが含まれます。

`AssessmentTargetARN` メトリクス

メトリクス	説明
`TotalMatchingAgents`	このターゲットに一致するエージェントの数
`TotalHealthyAgents`	このターゲットに一致するエージェントで、正常なものの数
`TotalAssessmentRuns`	このターゲットの評価の実行の数
`TotalAssessmentRun Findings`	このターゲットの結果の数

`AssessmentTemplateARN` メトリクス

メトリクス	説明
`TotalMatchingAgents`	このテンプレートに一致するエージェントの数
`TotalHealthyAgents`	このテンプレートに一致するエージェントで、正常なものの数

メトリクス	説明
TotalAssessmentRuns	このテンプレートの評価の実行の数
TotalAssessmentRun Findings	このテンプレートの結果の数

メトリクス集約

メトリクス	説明
TotalAssessmentRuns	この AWS アカウントで実行された評価の数

を使用した Amazon Inspector Classic の設定 AWS CloudFormation

でサポートされている Amazon Inspector Classic リソースのリファレンス情報については AWS CloudFormation、以下のトピックを参照してください。

- AWS::Inspector::AssessmentTarget
- AWS::Inspector::AssessmentTemplate
- AWS::Inspector::ResourceGroup

> **Important**
>
> サポートされている AWS リージョンの Amazon Inspector Classic ルールパッケージの ARNs「」を参照してくださいルールパッケージの Amazon Inspector Classic ARN。

との統合 AWS Security Hub CSPM

AWS Security Hub CSPM は、 のセキュリティ状態を包括的に把握 AWS し、セキュリティ業界標準とベストプラクティスに照らして環境をチェックするのに役立ちます。Security Hub CSPM は、複数の AWS アカウント、サービス、サポートされているサードパーティーパートナー製品からセキュリティデータを収集し、セキュリティの傾向を分析し、最も優先度の高いセキュリティ問題を特定するのに役立ちます。

Amazon Inspector と Security Hub CSPM の統合により、Amazon Inspector から Security Hub CSPM に検出結果を送信できます。Security Hub CSPM は、これらの検出結果をセキュリティ体制の分析に含めることができます。

目次

- Amazon Inspector が Security Hub CSPM に結果を送信する方法
  - Amazon Inspector が送信する検出結果のタイプ
  - 検出結果が送信されるまでのレイテンシー
  - Security Hub CSPM が使用できない場合の再試行
  - Security Hub CSPM の既存の検出結果を更新する
- Amazon Inspector からの典型的な検出結果
- 統合の有効化と構成
- 検出結果の送信を停止する方法

Amazon Inspector が Security Hub CSPM に結果を送信する方法

Security Hub CSPM では、セキュリティの問題が検出結果として追跡されます。一部の検出結果は、他の AWS サービスまたはサードパーティーパートナーによって検出された問題から発生します。Security Hub CSPM には、セキュリティの問題を検出し、検出結果を生成するために使用する一連のルールもあります。

Security Hub CSPM には、これらすべてのソースからの検出結果を管理するためのツールが用意されています。検出結果の一覧を表示およびフィルタリングして、検出結果の詳細を表示できます。「AWS Security Hub ユーザーガイド」の「検出結果の表示」を参照してください。検出結果の調査状況を追跡することもできます 「AWS Security Hub ユーザーガイド」の「Taking action on findings」(検出結果に対するアクションの実行) を参照してください。

Security Hub CSPM のすべての検出結果は、 AWS Security Finding Format (ASFF) と呼ばれる標準 JSON 形式を使用します。ASFF には、問題のソース、影響を受けるリソース、および検出結果の現在のステータスに関する詳細が含まれます。 AWS Security Hub ユーザーガイド の「AWS Security Finding Format (ASFF)」を参照してください。

Amazon Inspector は、Security Hub CSPM に結果を送信する AWS サービスの 1 つです。

Amazon Inspector が送信する検出結果のタイプ

Amazon Inspector は、生成したすべての検出結果を Security Hub CSPM に送信します。

Amazon Inspector は、Security AWS Finding 形式 (ASFF) を使用して検出結果を Security Hub CSPM に送信します。ASFF では、Types フィールドが検出結果タイプを提供します。Amazon Inspectorの検出結果には、Types に対する次の値を指定できます。

- ソフトウェアと設定のチェック/脆弱性/CVE
- ソフトウェアと設定のチェック/AWS セキュリティのベストプラクティス/ネットワーク到達可能性
- ソフトウェアと設定のチェック/業界および規制基準/CIS ホスト強化ベンチマーク

検出結果が送信されるまでのレイテンシー

Amazon Inspector が新しい検出結果を作成すると、通常は 5 分以内に Security Hub CSPM に送信されます。

Security Hub CSPM が使用できない場合の再試行

Security Hub CSPM が使用できない場合、Amazon Inspector は結果を受信するまで結果の送信を再試行します。

Security Hub CSPM の既存の検出結果を更新する

Security Hub CSPM に検出結果を送信すると、Amazon Inspector は検出結果を更新して、検出結果アクティビティの追加の観察結果を反映します。これにより、Security Hub CSPM の Amazon Inspector の検出結果は Amazon Inspector よりも少なくなります。

Amazon Inspector からの典型的な検出結果

Amazon Inspector は、Security AWS Finding 形式 (ASFF) を使用して Security Hub CSPM に結果を送信します。

以下に、 Amazon Inspectorからの典型的な検出結果の例を示します。


```
{
  "SchemaVersion": "2018-10-08",
  "Id": "inspector/us-east-1/111122223333/629ff13fbbb44c872f7bba3e7f79f60cb6d443d8",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/inspector",
  "GeneratorId": "arn:aws:inspector:us-east-1:316112463485:rulespackage/0-PmNV0Tcd",
  "AwsAccountId": "111122223333",
  "Types": [
    "Software and Configuration Checks/AWS Security Best Practices/Network Reachability
 - Recognized port reachable from internet"
  ],
  "CreatedAt": "2020-08-19T17:36:22.169Z",
  "UpdatedAt": "2020-11-04T16:36:06.064Z",
  "Severity": {
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "6.0"
  },
  "Confidence": 10,
  "Title": "On instance i-0c10c2c7863d1a356, TCP port 22 which is associated with 'SSH'
 is reachable from the internet",
  "Description": "On this instance, TCP port 22, which is associated with SSH, is
 reachable from the internet. You can install the Inspector agent on this instance
 and re-run the assessment to check for any process listening on this port. The
 instance i-0c10c2c7863d1a356 is located in VPC vpc-a0c2d7c7 and has an attached ENI
 eni-078eac9d6ad9b20d1 which uses network ACL acl-154b8273. The port is reachable from
 the internet through Security Group sg-0af64c8a5eb30ca75 and IGW igw-e209d785",
  "Remediation": {
    "Recommendation": {
      "Text": "You can edit the Security Group sg-0af64c8a5eb30ca75 to remove access
 from the internet on port 22"
    }
  },
  "ProductFields": {
    "attributes/VPC": "vpc-a0c2d7c7",
    "aws/inspector/id": "Recognized port reachable from internet",
```

```
    "serviceAttributes/schemaVersion": "1",
    "aws/inspector/arn": "arn:aws:inspector:us-east-1:111122223333:target/0-8zh1cWkg/
template/0-rqtRV0u0/run/0-Ck2F6tY9/finding/0-B458MQWe",
    "attributes/ACL": "acl-154b8273",
    "serviceAttributes/assessmentRunArn": "arn:aws:inspector:us-
east-1:111122223333:target/0-8zh1cWkg/template/0-rqtRV0u0/run/0-Ck2F6tY9",
    "attributes/PROTOCOL": "TCP",
    "attributes/RULE_TYPE": "RecognizedPortNoAgent",
    "aws/inspector/RulesPackageName": "Network Reachability",
    "attributes/INSTANCE_ID": "i-0c10c2c7863d1a356",
    "attributes/PORT_GROUP_NAME": "SSH",
    "attributes/IGW": "igw-e209d785",
    "serviceAttributes/rulesPackageArn": "arn:aws:inspector:us-
east-1:111122223333:rulespackage/0-PmNV0Tcd",
    "attributes/SECURITY_GROUP": "sg-0af64c8a5eb30ca75",
    "attributes/ENI": "eni-078eac9d6ad9b20d1",
    "attributes/REACHABILITY_TYPE": "Internet",
    "attributes/PORT": "22",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/inspector/
inspector/us-east-1/111122223333/629ff13fbbb44c872f7bba3e7f79f60cb6d443d8",
    "aws/securityhub/ProductName": "Inspector",
    "aws/securityhub/CompanyName": "Amazon"
  },
  "Resources": [
    {
      "Type": "AwsEc2Instance",
      "Id": "arn:aws:ec2:us-east-1:193043430472:instance/i-0c10c2c7863d1a356",
      "Partition": "aws",
      "Region": "us-east-1",
      "Tags": {
        "Name": "kubectl"
      },
      "Details": {
        "AwsEc2Instance": {
          "ImageId": "ami-02354e95b39ca8dec",
          "IpV4Addresses": [
            "172.31.43.6"
          ],
          "VpcId": "vpc-a0c2d7c7",
          "SubnetId": "subnet-4975b475"
        }
      }
    }
  ],
```

```
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE"
}
```

統合の有効化と構成

Security Hub CSPM と Patch Manager 統合を使用するには、Security Hub CSPM を有効にする必要があります。Security Hub CSPM を有効にする方法については、「AWS Security Hub ユーザーガイド」の「Setting up Security Hub」(Security Hub の設定) を参照してください。

Amazon Inspector と Security Hub CSPM の両方を有効にすると、統合は自動的に有効になります。Amazon Inspector が Security Hub CSPM への検出結果の送信を開始します。

検出結果の送信を停止する方法

Security Hub CSPM への結果の送信を停止するには、Security Hub CSPM コンソールまたは API を使用できます。

「統合からの結果のフローの無効化と有効化 (コンソール)」または AWS Security Hub ユーザーガイドの「統合からの結果のフローの無効化 (Security Hub API、AWS CLI)」を参照してください。

Amazon Inspector Classic ARN

Amazon Inspector Classic の各リソースタイプとルールパッケージには、一意の Amazon リソースネーム (ARN) が関連付けられています。

目次

- Amazon Inspector Classic リソースの ARN
- ルールパッケージの Amazon Inspector Classic ARN
  - 米国東部 (オハイオ)
  - 米国東部 (バージニア北部)
  - 米国西部 (北カリフォルニア)
  - 米国西部 (オレゴン)
  - アジアパシフィック (ムンバイ)
  - アジアパシフィック (ソウル)
  - アジアパシフィック (シドニー)
  - アジアパシフィック (東京)
  - 欧州 (フランクフルト)
  - 欧州 (アイルランド)
  - 欧州 (ロンドン)
  - 欧州 (ストックホルム)
  - AWS GovCloud (米国東部)
  - AWS GovCloud (米国西部)

Amazon Inspector Classic リソースの ARN

Amazon Inspector Classic で、プライマリリソースとは Resource Groups、評価ターゲット、評価テンプレート、評価の実行、および検索結果です。これらのリソースには、次の表に示すとおり、一意の Amazon リソースネーム (ARN) が関連付けられています。

リソースタイプ	ARN 形式
リソースグループ	arn:aws:inspector: *region*:*account-id* :resource group/ *ID*
評価ターゲット	arn:aws:inspector: *region*:*account-id* :target/*ID*
評価テンプレート	arn:aws:inspector: *region*:*account-id* :target/*ID*:template: *ID*
評価の実行	arn:aws:inspector: *region*:*account-id* :target/*ID*/template/ *ID*/run/*ID*
結果	arn:aws:inspector: *region*:*account-id* :target/*ID*/template/ *ID*/run/*ID*/finding/ *ID*

ルールパッケージの Amazon Inspector Classic ARN

サポートされているすべてのリージョンにおける Amazon Inspector Classic ルールパッケージの ARN の一覧を次のテーブルに示します。

トピック

- 米国東部 (オハイオ)
- 米国東部 (バージニア北部)
- 米国西部 (北カリフォルニア)
- 米国西部 (オレゴン)
- アジアパシフィック (ムンバイ)
- アジアパシフィック (ソウル)
- アジアパシフィック (シドニー)
- アジアパシフィック (東京)
- 欧州 (フランクフルト)
- 欧州 (アイルランド)
- 欧州 (ロンドン)
- 欧州 (ストックホルム)

- AWS GovCloud (米国東部)
- AWS GovCloud (米国西部)

米国東部 (オハイオ)

ルールパッケージ名	ARN
共通脆弱性識別子	arn:aws:inspector:us-east-2:646659390643:rulespackage/0-JnA8Zp85
CIS オペレーティングシステムのセキュリティ設定ベンチマーク	arn:aws:inspector:us-east-2:646659390643:rulespackage/0-m8r61nnh
ネットワーク到達可能性	arn:aws:inspector:us-east-2:646659390643:rulespackage/0-cE4kTR30
セキュリティのベストプラクティス	arn:aws:inspector:us-east-2:646659390643:rulespackage/0-AxKmMHPX

米国東部 (バージニア北部)

ルールパッケージ名	ARN
共通脆弱性識別子	arn:aws:inspector:us-east-1:316112463485:rulespackage/0-gEjTy7T7

ルールパッケージ名	ARN
CIS オペレーティングシステムのセキュリティ設定ベンチマーク	arn:aws:inspector:us-east-1:316112463485:rulespackage/0-rExsr2X8
ネットワーク到達可能性	arn:aws:inspector:us-east-1:316112463485:rulespackage/0-PmNV0Tcd
セキュリティのベストプラクティス	arn:aws:inspector:us-east-1:316112463485:rulespackage/0-R01qwB5Q

米国西部 (北カリフォルニア)

ルールパッケージ名	ARN
共通脆弱性識別子	arn:aws:inspector:us-west-1:166987590008:rulespackage/0-TKgzoVOa
CIS オペレーティングシステムのセキュリティ設定ベンチマーク	arn:aws:inspector:us-west-1:166987590008:rulespackage/0-xUY8iRqX
ネットワーク到達可能性	arn:aws:inspector:us-west-1:166987590008:rulespackage/0-TxmXimXF

ルールパッケージ名	ARN
セキュリティのベストプラクティス	arn:aws:inspector:us-west-1:166987590008:rulespackage/0-byoQRFYm

米国西部 (オレゴン)

ルールパッケージ名	ARN
共通脆弱性識別子	arn:aws:inspector:us-west-2:758058086616:rulespackage/0-9hgA516p
CIS オペレーティングシステムのセキュリティ設定ベンチマーク	arn:aws:inspector:us-west-2:758058086616:rulespackage/0-H5hpSawc
ネットワーク到達可能性	arn:aws:inspector:us-west-2:758058086616:rulespackage/0-rD1z6dpl
セキュリティのベストプラクティス	arn:aws:inspector:us-west-2:758058086616:rulespackage/0-JJOtZiqQ

アジアパシフィック (ムンバイ)

ルールパッケージ名	ARN
共通脆弱性識別子	arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-LqnJE9dO
CIS オペレーティングシステムのセキュリティ設定ベンチマーク	arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-PSUlX14m
ネットワーク到達可能性	arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-YxKfjFu1
セキュリティのベストプラクティス	arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-fs0IZZBj

アジアパシフィック (ソウル)

ルールパッケージ名	ARN
共通脆弱性識別子	arn:aws:inspector:ap-northeast-2:526946625049:rulespackage/0-PoGHMznc
CIS オペレーティングシステムのセキュリティ設定ベンチマーク	arn:aws:inspector:ap-northeast-2:526

ルールパッケージ名	ARN
	946625049:rulespac kage/0-T9srhg1z
ネットワーク到達可能性	arn:aws:inspector: ap-northeast-2:526 946625049:rulespac kage/0-s3OmLzhL
セキュリティのベストプラクティス	arn:aws:inspector: ap-northeast-2:526 946625049:rulespac kage/0-2WRpmi4n

アジアパシフィック (シドニー)

ルールパッケージ名	ARN
共通脆弱性識別子	arn:aws:inspector: ap-southeast-2:454 640832652:rulespac kage/0-D5TGAxiR
CIS オペレーティングシステムのセキュリティ設定ベンチマーク	arn:aws:inspector: ap-southeast-2:454 640832652:rulespac kage/0-Vkd2Vxjq
ネットワーク到達可能性	arn:aws:inspector: ap-southeast-2:454 640832652:rulespac kage/0-FLcuV4Gz
セキュリティのベストプラクティス	arn:aws:inspector: ap-southeast-2:454

ルールパッケージ名	ARN
	640832652:rulespac kage/0-asL6HRgN

アジアパシフィック (東京)

ルールパッケージ名	ARN
共通脆弱性識別子	arn:aws:inspector: ap-northeast-1:406 045910587:rulespac kage/0-gHP9oWNT
CIS オペレーティングシステムのセキュリティ設定ベンチマーク	arn:aws:inspector: ap-northeast-1:406 045910587:rulespac kage/0-7WNjqgGu
ネットワーク到達可能性	arn:aws:inspector: ap-northeast-1:406 045910587:rulespac kage/0-YI95DVd7
セキュリティのベストプラクティス	arn:aws:inspector: ap-northeast-1:406 045910587:rulespac kage/0-bBUQnxMq

欧州 (フランクフルト)

ルールパッケージ名	ARN
共通脆弱性識別子	arn:aws:inspector: eu-central-1:53750

ルールパッケージ名	ARN
	3971621:rulespackage/0-wNqHa8M9
CIS オペレーティングシステムのセキュリティ設定ベンチマーク	arn:aws:inspector:eu-central-1:537503971621:rulespackage/0-nZrAVuv8
ネットワーク到達可能性	arn:aws:inspector:eu-central-1:537503971621:rulespackage/0-6yunpJ91
セキュリティのベストプラクティス	arn:aws:inspector:eu-central-1:537503971621:rulespackage/0-ZujVHEPB

欧州 (アイルランド)

ルールパッケージ名	ARN
共通脆弱性識別子	arn:aws:inspector:eu-west-1:357557129151:rulespackage/0-ubA5XvBh
CIS オペレーティングシステムのセキュリティ設定ベンチマーク	arn:aws:inspector:eu-west-1:357557129151:rulespackage/0-sJBhCr0F
ネットワーク到達可能性	arn:aws:inspector:eu-west-1:35755712

ルールパッケージ名	ARN
	9151:rulespackage/0-SPzU33xe
セキュリティのベストプラクティス	arn:aws:inspector:eu-west-1:357557129151:rulespackage/0-SnojL3Z6

欧州 (ロンドン)

ルールパッケージ名	ARN
共通脆弱性識別子	arn:aws:inspector:eu-west-2:146838936955:rulespackage/0-kZGCqcE1
CIS オペレーティングシステムのセキュリティ設定ベンチマーク	arn:aws:inspector:eu-west-2:146838936955:rulespackage/0-IeCjwf1W
ネットワーク到達可能性	arn:aws:inspector:eu-west-2:146838936955:rulespackage/0-AizSYyNq
セキュリティのベストプラクティス	arn:aws:inspector:eu-west-2:146838936955:rulespackage/0-XApUiSaP

欧州 (ストックホルム)

ルールパッケージ名	ARN
共通脆弱性識別子	arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-IgdgIewd
CIS オペレーティングシステムのセキュリティ設定ベンチマーク	arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-Yn8jlX7f
ネットワーク到達可能性	arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-52Sn74uu
セキュリティのベストプラクティス	arn:aws:inspector:eu-north-1:453420244670:rulespackage/0-HfBQSbSf

AWS GovCloud (米国東部)

ルールパッケージ名	ARN
共通脆弱性識別子	arn:aws-us-gov:inspector:us-gov-east-1:206278770380:rulespackage/0-3IFKFuOb
CIS オペレーティングシステムのセキュリティ設定ベンチマーク	arn:aws-us-gov:inspector:us-gov-east

ルールパッケージ名	ARN
	-1:206278770380:rulespackage/0-pTLCdIww
セキュリティのベストプラクティス	arn:aws-us-gov:inspector:us-gov-east-1:206278770380:rulespackage/0-vlgEGcVD

AWS GovCloud (米国西部)

ルールパッケージ名	ARN
共通脆弱性識別子	arn:aws-us-gov:inspector:us-gov-west-1:850862329162:rulespackage/0-4oQgcI4G
CIS オペレーティングシステムのセキュリティ設定ベンチマーク	arn:aws-us-gov:inspector:us-gov-west-1:850862329162:rulespackage/0-Ac4CFOuc
セキュリティのベストプラクティス	arn:aws-us-gov:inspector:us-gov-west-1:850862329162:rulespackage/0-rOTGqe5G

ドキュメント履歴

次の表は、2018 年 5 月以降の Amazon Inspector Classic のドキュメントのリリース履歴をまとめたものです。

変更	説明	日付
サポート終了通知	サポート終了通知: 2026 年 5 月 20 日に、 AWS は Amazon Inspector Classic のサポートを終了します。2026 年 5 月 20 日以降、Amazon Inspector Classic コンソールまたは Amazon Inspector Classic リソースにアクセスできなくなります。詳細については、Amazon Inspector Classic のサポート終了」を参照してください。	2025 年 5 月 20 日
パスワードのセキュリティのベストプラクティスの更新	EC2 インスタンスのパスワードの長さとパスワードの複雑さに対する Amazon Inspector Classic セキュリティのベストプラクティス要件が更新されました。「パスワードの最小文字数を設定する」および「パスワードの複雑さを設定する」を参照してください。	2021 年 3 月 8 日
新しいオペレーティングシステムのバージョンに対するサポートを追加	Amazon Inspector Classic では、Ubuntu 20.4 LTS、Debian 10.x、RHEL 8.x、Windows Server 2019 Base のオペレーティングシステムバージョン	2020 年 10 月 15 日

	がサポートされるようになりました。	
新しいセキュリティ章に統合されたセキュリティ情報	Identity and Access Management の管理に関する情報を含む Amazon Inspector Classic のセキュリティ情報を、セキュリティに関する章に統合しました。Amazon Inspector Classic のセキュリティを参照してください。	2020 年 4 月 7 日
ランタイム動作分析ルールパッケージのサポートを削除するためにドキュメントを更新しました。	複数のトピックが更新され、サポートされなくなった実行時の動作の分析ルールパッケージに関する情報が削除されました。	2019年9月5日
OS サポートの追加	CentOS 7.6 に対する Amazon Inspector Classic のサポートが追加されました。詳細については、「Amazon Inspector Classic でサポートされているオペレーティングシステムとリージョン」と「サポートされているオペレーティングシステム全体でのルールパッケージの可用性」を参照してください。	2018 年 12 月 3 日

新しいコンテンツ	Amazon Inspector Classic ネットワーク到達可能性ルールパッケージが追加されました。これにより、ユーザーはセキュリティの脆弱性についてネットワーク設定を分析するエージェントレス評価を実行できます。詳細については、「ネットワーク到達可能性」を参照してください。	2018 年 11 月 9 日
OS サポートの追加	RHEL 7.6 に対する Amazon Inspector Classic のサポートが追加されました。詳細については、「Amazon Inspector Classic でサポートされているオペレーティングシステムとリージョン」と「サポートされているオペレーティングシステム全体でのルールパッケージの可用性」を参照してください。	2018 年 10 月 30 日
OS サポートの追加	さまざまなオペレーティングシステムのサポートを CIS ベンチマークルールパッケージに追加しました。詳細については、「Center for Internet Security (CIS) Benchmarks」および「Rules Packages Availability Across Supported Operating Systems」を参照してください。	2018 年 8 月 13 日
リージョンサポートが追加されました	AWS GovCloud (US) のリージョンサポートの追加	2018 年 13 月 6 日

次の表は、2018 年 6 月以前の Amazon Inspector Classic のドキュメントのリリース履歴をまとめたものです。

変更	説明	日付
新しいコンテンツ	アカウントのすべての Amazon EC2 インスタンスをターゲットにする機能が追加されました。詳細については、「Amazon Inspector Classic 評価ターゲット」を参照してください。	2018 年 5 月 24 日
OS サポートの追加	Amazon Linux 2018.03 と Ubuntu 18.04 に対する Amazon Inspector Classic のサポートが追加されました。	2018 年 5 月 15 日
新しいコンテンツ	反復的 Amazon Inspector Classic 評価をセットアップする機能が追加されました。	2018 年 30 月 4 日
新しいコンテンツ	Inspector のコンソールを通じて Amazon Inspector Classic エージェントをインストールする機能が追加されました。	2018 年 30 月 4 日
OS サポートの追加	Amazon Linux 2 に対する Amazon Inspector Classic のサポートが追加されました。	2018 年 3 月 13 日
OS サポートの追加	Windows Server 2016 Base に対する Amazon Inspector Classic 評価のサポートが追加されました。	2018 年 2 月 20 日
リージョンサポートが追加されました	US East (Ohio) リージョンに対する Amazon Inspector	2018 年 2 月 7 日

変更	説明	日付
	Classic のサポートが追加されました。	
新しいコンテンツ	カーネルモジュールが使用できないときに Amazon Inspector Classic 評価を実行できるようになりました。	2018 年 1 月 11 日
リージョンサポートが追加されました	EU (Frankfurt) リージョンに対する Amazon Inspector Classic のサポートが追加されました。	2017 年 12 月 19 日
新しいコンテンツ	Amazon Inspector Classic API とコンソールで Amazon Inspector Classic エージェントのヘルスチェックを行う機能が追加されました。	2017 年 15 月 12 日
新しいコンテンツ	次の機能が追加されました。 • サービスにリンクされたロールの使用 • AWS Marketplace で利用可能な Amazon Inspector Classic エージェント AMI • Amazon Inspector Classic CloudFormation テンプレート	2017 年 5 月 12 日
OS サポートの追加	CentOS 7.4 に対する Amazon Inspector Classic 評価のサポートが追加されました。	2017 年 11 月 9 日

変更	説明	日付
OS サポートの追加	Amazon Linux 2017.09 に対する Amazon Inspector Classic 評価のサポートが追加されました。	2017 年 10 月 11 日
OS サポートの追加	RHEL 7.4 に対する Amazon Inspector Classic 評価のサポートが追加されました。	2018 年 2 月 20 日
HIPAA への対応の追加	Amazon Inspector Classic が HIPAA に対応するようになりました。	2017 年 7 月 31 日
新しいコンテンツ	Amazon CloudWatch Events によって Amazon Inspector Classic のセキュリティ評価を自動的にトリガーする機能が追加されました。	2017 年 7 月 27 日
リージョンサポートが追加されました	`US West (N. California)` リージョンに対する Amazon Inspector Classic のサポートが追加されました。	2018 年 6 月 6 日
OS サポートの追加	RHEL 6.2-6.9、RHEL 7.2-7.3、CentOS 6.9、および CentOS 7.2-7.3 に対する Amazon Inspector Classic 評価のサポートが追加されました。	2017 年 5 月 23 日
OS サポートの追加	Amazon Linux 2017.03 に対する Amazon Inspector Classic 評価のサポートが追加されました。	2017 年 4 月 25 日

変更	説明	日付
新しいコンテンツと OS サポートの追加	追加: • Ubuntu 16.04 に対する Amazon Inspector Classic のサポートが追加されました。 • Amazon Inspector Classic オペレーションを自動化するための Lambda ブループリントの可用性	2017 年 1 月 5 日
新しい OS サポート	Microsoft Windows に対する Amazon Inspector Classic サポートが追加されました。	2016 年 8 月 26 日
リージョンサポートが追加されました	`Asia Pacific (Seoul)` リージョンに対する Amazon Inspector Classic のサポートが追加されました。	2016 年 8 月 26 日
リージョンサポートが追加されました	`Asia Pacific (Mumbai)` リージョンに対する Amazon Inspector Classic のサポートが追加されました。	2016 年 4 月 25 日
リージョンサポートが追加されました	`Asia Pacific (Sydney)` リージョンに対する Amazon Inspector Classic のサポートが追加されました。	2016 年 4 月 25 日
サービスの起動	Amazon Inspector Classic サービスが開始されました。	2015 年 10 月 7 日

AWS 用語集

最新の AWS 用語については、 AWS の用語集 リファレンスのAWS 用語集を参照してください。