Amazon Inspector

ユーザーガイド

Version Latest

Amazon Inspector: ユーザーガイド

Table of Contents

Amazon Inspector とは 1
Amazon Inspector の利点 1
Amazon Inspector の機能 1
Amazon Inspector 料金表 2
Amazon Inspector へのアクセス 2
Amazon Inspector の用語と概念 2
Amazon Inspector サービスの制限 4
Amazon Inspector 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 4
Amazon Inspector 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 5
Amazon Inspector 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 5
サポートされている AWS リージョン 6
ご利用開始にあたって 7
Amazon Inspector を使用するための前提条件 7
ワンクリックでのセットアップ 7
高度な設定 8
チュートリアル 10
Amazon Inspector チュートリアル - Red Hat Enterprise Linux 10
ステップ 1: Amazon EC2 で使用する Amazon Inspector インスタンスを設定する 10
ステップ 2: Amazon EC2 インスタンスを変更する 10
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 11
ステップ 4: 評価テンプレートの作成および実行 12
ステップ 5: 結果を見つけて分析する 12
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 13
Amazon Inspector チュートリアル - Ubuntu Server 13
ステップ 1: Amazon EC2 で使用する Amazon Inspector インスタンスを設定する 14
ステップ 2: Amazon EC2 インスタンスを変更する 14
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 14
ステップ 4: 評価テンプレートの作成および実行 15
ステップ 5: 生成された結果を見つけて分析する 15
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 16
サービスにリンクされたロールの使用 17
Amazon Inspector のサービスにリンクされたロールのアクセス許可 17
Amazon Inspector のサービスにリンクされたロールの作成 18
初めて Amazon Inspector を開始する場合 18
AWS アカウントで実行されている Amazon Inspector がすでにある場合 18
Amazon Inspector のサービスにリンクされたロールの編集 19
Amazon Inspector のサービスにリンクされたロールの削除 19
Amazon Inspector エージェント 20
Amazon Inspector エージェントのアクセス許可 20
ネットワークと Amazon Inspector エージェントセキュリティ 21
Amazon Inspector エージェントの更新 21
テレメトリデータのライフサイクル 22
Amazon Inspector から AWS アカウントへのアクセス制御 22
Amazon Inspector エージェントの制限 22
Amazon Inspector エージェントのパブリックライセンス 22
Amazon Inspector エージェントのインストール 22
Amazon Inspector エージェントを使用した Amazon Linux AMI 23
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 23
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 24
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 25
Linux ベースのオペレーティングシステムでの Amazon Inspector エージェントの操作 26

Amazon Inspector エージェントが実行されていることを確認する 26
Amazon Inspector エージェントを停止する 26
Amazon Inspector エージェントを開始する 26
Amazon Inspector エージェントの設定を変更する 27
Amazon Inspector エージェントのプロキシサポートを設定する 27
Amazon Inspector エージェントをアンインストールする 28
Windows ベースのオペレーティングシステムでの Amazon Inspector エージェントの操作 28
Amazon Inspector エージェントの開始中または停止中またはそのエージェントが実行中であることの確認 29
Amazon Inspector エージェントの設定を変更する 29
Amazon Inspector エージェントのプロキシサポートを設定する 29
Amazon Inspector エージェントをアンインストールする 30
(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 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。 30
GPG ツールのインストール 31
パブリック キーの認証とインポート 31
パッケージの署名の確認 33
(オプション) Windows ベースのオペレーティングシステムの Amazon Inspector 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。 34
Amazon Inspector の評価ターゲット 35
リソースをタグ付けして評価ターゲットを作成する 35
Amazon Inspector 評価ターゲットの制限 35
評価ターゲットを作成する 36
評価ターゲットを削除する 37
Amazon Inspector のルール パッケージとルール 38
Amazon Inspector でのルールの重大度 38
Amazon Inspector のルールパッケージ 38
ネットワーク到達可能性 39
分析された設定 39
到達可能性ルート 40
結果のタイプ 40
共通脆弱性識別子 42
Center for Internet Security (CIS) ベンチマーク 42
実行時の動作の分析 44
安全でないクライアントプロトコル (ログイン) 44
安全でないクライアントプロトコル (一般) 45
未使用のリッスンする TCP ポート 45
安全でないサーバープロトコル 46
データ実行防止機能を持たないソフトウェア (DEP) 46
安全でないアクセス権限を持つ Root プロセス 47
Amazon Inspector のセキュリティのベストプラクティス 47
SSH 経由の root ログインを無効化する 48
SSH バージョン 2 のみをサポート 48
SSH 経由のパスワード認証を無効化する 49
パスワードの有効期限を設定する 49
パスワードの最小文字数を設定する 49
パスワードの複雑さを設定する 50
ASLR の有効化 50
DEP の有効化 50
システムディレクトリに対するアクセス権限の設定 51
Amazon Inspector の評価テンプレートと評価の実行 52
Amazon Inspector の評価テンプレート 52
Amazon Inspector の評価テンプレートの制限 53
評価テンプレートを作成中 53
評価テンプレートを削除する 54
評価の実行 54
評価の実行を削除する 55

Amazon Inspectorの評価の実行の制限 55
Lambda 関数を使用した評価の自動実行をセットアップする 55
Amazon Inspector 通知用の SNS トピックを設定するには 56
Amazon Inspector の結果 58
結果を使用する 58
評価レポート 60
Amazon Inspector での除外 61
除外タイプ 61
除外のプレビュー 67
評価後の除外の確認 68
サポートされているオペレーティングシステムに関して、Amazon Inspector ルールパッケージ 69
AWS CloudTrail を使用した Amazon Inspector API 呼び出しのログ作成 72
CloudTrail 内の Amazon Inspector 情報 72
Amazon Inspector ログファイルエントリの概要 73
Amazon CloudWatch を使用した Amazon Inspector のモニタリング 75
Amazon Inspector CloudWatch のメトリクス 75
AWS CloudFormation の使用による Amazon Inspector の設定 77
Amazon Inspector に対する認証とアクセスコントロール 78
認証 78
アクセスコントロール 79
Amazon Inspector リソースに対するアクセス許可の管理の概要 79
Amazon Inspector リソースおよびオペレーション 80
リソース所有権について 80
リソースへのアクセスの管理 81
ポリシー要素の指定 : アクション、効果、リソース、プリンシパル 82
ポリシーでの条件の指定 82
Amazon Inspector でアイデンティティベースのポリシー (IAM ポリシー) を使用する 83
Amazon Inspector コンソールを使用するために必要なアクセス権限 83
Amazon Inspector での AWS 管理 (事前定義) ポリシー 84
お客様が管理するポリシーの例 84
Amazon Inspector API のアクセス権限: アクション、リソース、条件リファレンス 85
ルールパッケージの Amazon Inspector ARN 86
米国西部 (オレゴン) 86
米国東部 (バージニア北部) 87
米国東部 (オハイオ) 87
米国西部 (北カリフォルニア) 88
アジアパシフィック (ムンバイ) 88
アジアパシフィック (シドニー) 89
アジアパシフィック (ソウル) 89
アジアパシフィック (東京) 90
欧州 (アイルランド) 90
欧州 (フランクフルト) 91
AWS GovCloud (米国東部) 91
AWS GovCloud (米国西部) 92
ドキュメント履歴 93
AWS の用語集 97

Amazon Inspector とは

Amazon Inspector は、Amazon EC2 instances 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 は、露出、脆弱性、およびベストプラクティスからの逸脱についてアプリケーションを評価します。評価が実行された後、重大性の順に結果を表示した詳細なリストが Amazon Inspector によって作成されます。

Amazon Inspector を使用すると、開発とデプロイパイプライン全体や静的生産システムの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 には、評価対象の EC2 instances 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もあります。エージェントは、EC2 instances 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、次の推奨事項によってすべての潜在的なセキュリティ上の問題が解決することを保証しません。Amazon Inspector によって作成される結果は、評価テンプレートに含まれるルールパッケージの選択やシステム内の非 AWS コンポーネントの存在などの要因によって異なります。AWS サービスで起動するアプリケーション、プロセス、ツールのセキュリティについては、ユーザーに責任があります。セキュリティの詳細については、「AWS 責任共有モデル」を参照してください。
>
> **Note**
>
> AWS は、AWS クラウドで提供されるすべてのサービスを実行するグローバルインフラストラクチャの保護を担います。このインフラストラクチャは、AWS の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。AWS は、さまざまなコンピューターセキュリティ基準や規制への AWS の順守について検証した、第三者の監査人からのレポートを公開しています。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 の用語については、「Amazon Inspector の用語と概念 (p. 2)」を参照してください。

Amazon Inspector の利点

Amazon Inspector を使用する主要な利点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します – 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目的のために 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見つけます – 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 が生み出す調査結果を確認して、AWS リソースのアクティビティおよび設定データについて常に情報を入手してください。

Amazon Inspector の機能

以下は Amazon Inspector の主な特徴です。

- 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 はエンジン分析システムおよびリソース設定を提供します。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 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 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 料金表

Amazon Inspector の価格は、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。Amazon Inspector の料金体系の詳細については、「Amazon Inspector 料金表」を参照してください。

Amazon Inspector へのアクセス

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

Amazon Inspector コンソール

Sign in to the AWS マネジメントコンソール and open the Amazon Inspector console at https://console.aws.amazon.com/inspector/.

コンソールは、Amazon Inspector 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 SDK

AWS には、さまざまなプログラミング言語およびプラットフォームのライブラリとサンプルコードで構成されたソフトウェア開発キット (SDK) 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 サービスへのプログラムによるアクセス権限を作成する際に役立ちます。AWS SDK のダウンロードやインストールなどの詳細については、「アマゾン ウェブ サービスのツール」を参照してください。

Amazon Inspector HTTPS API

サービスに HTTPS リクエストを直接発行できる Amazon Inspector HTTPS API を使用して、プログラムにより Amazon Inspector と AWS にアクセスできます。詳細については、「Amazon Inspector 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使用することで、Amazon Inspector のタスクを実行できます。コマンドラインツールは、AWS のタスクを実行するスクリプトを作成する場合にも便利です。詳細については、「Amazon Inspector の 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 の用語と概念

Amazon Inspector の使用を開始するにあたり、その主要コンセプトを確認しておくとメリットがあります。

Amazon Inspector エージェント

評価ターゲットに含まれている Amazon EC2 instances 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、EC2 instances 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)。詳細については、「Amazon Inspector エージェント (p. 20)」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や動作を分析し、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行動データ (テレメトリ) をモニタリング、収集、および分析します。このデータには、AWS のサービスとの通信の詳細、安全な交信の使用、実行プロセスの詳細、実行プロセス間のネットワーク トラフィックなどが含まれます。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 の評価テンプレートと評価の実行 (p. 52)」を参照してください。

評価ターゲット

Amazon Inspector のコンテキストでは、評価ターゲットとは、単位として連動してビジネス目標の達成を支援する AWS リソースの集合体を意味します。Amazon Inspector 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を評価します。

> **Important**
>
> 現時点では、Amazon Inspector 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 サービスの制限 (p. 4)」を参照してください。

Amazon Inspector 評価ターゲットを作成するには、まず EC2 instances 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 instances のビューを作成できます。詳細については、「Amazon Inspector の評価ターゲット (p. 35)」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 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 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 が発見する潜在的なセキュリティ問題。結果は Amazon Inspector 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 の結果 (p. 58)」を参照してください。

ルール

Amazon Inspector 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 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 のコンテキストでは、ルールの集合体を意味します。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 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 のルール パッケージとルール (p. 38)」を参照してください。

テレメトリ

ネットワーク接続の記録やプロセス作成 Amazon Inspector サービスなどの EC2 インスタンスデータ (動作、設定など) は、評価の実行中にデータを収集します。

Amazon Inspector サービスの制限

次の表に、AWS アカウントの Amazon Inspector 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 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 instances 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 instances 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。
の評価テンプレート	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。
の評価ターゲット	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 Support Center に連絡することでリクエストによって増やすことができます。

Amazon Inspector 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 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 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、どの EC2 instances でもネットワーク到達可能性 (p. 39)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 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に関して、Amazon Inspector ルールパッケージ (p. 69)」を参照してください。

トピック

- Amazon Inspector 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 (p. 5)
- Amazon Inspector 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 (p. 5)
- サポートされている AWS リージョン (p. 6)

Amazon Inspector 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 エージェントは、64 ビット x86 バージョンと、次の Linux ベースのオペレーティングシステムの Arm バージョンを実行する EC2 インスタンスで使用できます。

- Amazon Linux 2 (LTS、2017.12)
- Amazon Linux (2018.03、2017.09、2017.03、2016.09、2016.03、2015.09、2015.03、2014.09、2014.03、2013.09、2013.03、201
- Ubuntu (18.04 LTS、16.04 LTS、14.04 LTS)
- Debian (9.0 ~ 9.5、8.0 ~ 8.7)
- Red Hat Enterprise Linux (7.2 ~ 7.6、6.2 ~ 6.9)
- CentOS (7.2 ~ 7.6、6.2 ~ 6.9)

Important

以下のリストには、Linux、Ubuntu、Red Hat Enterprise Linux、および CentOS 上で実行されている Amazon Inspector エージェントと互換性のあるすべてのカーネルバージョンが含まれています。https://s3.amazonaws.com/aws-agent.us-east-1/linux/support/supported_versions.json。CVE (p. 42)、CIS (p. 42)、またはセキュリティのベストプラクティス (p. 47)を使用して、Linux ベースの OS で EC2 インスタンスの評価を成功させることができます。このリストに含まれているカーネルバージョンがインスタンスにない場合でも、評価は成功します。Linux ベースの OS で 実行時の動作の分析 (p. 44) ルールパッケージを使用して、EC2 インスタンスの評価を適切に実行するには、インスタンスが、このリストに含まれているカーネルバージョンに該当する必要があります。インスタンスにエージェントと互換性のないカーネルバージョンがある場合、EC2 インスタンスを評価する実行時の動作の分析ルールパッケージは 1 つの検出結果のみをもたらします。この結果で、使用している EC2 インスタンスのカーネルバージョンがサポートされていないことがわかります。

Amazon Inspector 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 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 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016 Base

サポートされている AWS リージョン

Amazon Inspector は、以下の AWS リージョンでサポートされています。

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

> **Note**
>
> ネットワーク到達可能性 (p. 39)ルールパッケージは、AWS GovCloud (米国) リージョンでは利用できません。

Amazon Inspector の使用開始

このチュートリアルでは、Amazon Inspector 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。

Important

Amazon Inspector を使用するには、AWS アカウントが必要です。AWS にサインアップすると、アカウントは自動的に Amazon Inspector などの AWS のすべてのサービスにサインアップします。AWS アカウントをお持ちでない場合は、次に説明する手順にしたがってアカウントを作成してください。

AWS にサインアップするには

1. https://portal.aws.amazon.com/billing/signup を開きます。
2. オンラインの手順に従います。

   サインアップ手順の一環として、通話呼び出しを受け取り、電話のキーパッドを用いて確認コードを入力することが求められます。

トピック

- Amazon Inspector を使用するための前提条件 (p. 7)
- ワンクリックでのセットアップ (p. 7)
- 高度な設定 (p. 8)

Amazon Inspector を使用するための前提条件

最初に Amazon Inspector コンソールを起動した場合、[Get Started] を選択して次の前提条件タスクを実行します。Amazon Inspector の評価を実行するには、これらのタスクを完了する必要があります。

- Amazon Inspector の評価を実行するには、AWS 環境内で少なくとも 1 つの Amazon EC2 インスタンスを実行している必要があります。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。
- ほとんどの場合、Amazon Inspector エージェントは、評価ターゲットのそれぞれの EC2 instance で実行されている必要があります。エージェントをインストールする方法の詳細については、「Amazon Inspector エージェントのインストール (p. 22)」を参照してください。また、Systems Manager Run Command を使用して Amazon EC2 インスタンスにエージェントをインストールできます。Amazon Inspector エージェントの詳細については、「Amazon Inspector エージェント (p. 20)」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 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 インスタンスに対して、事前に作成された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 回のみ) を使用して自動評価を作成および実行する方法を示します。

1. Sign in to the AWS マネジメントコンソール and open the Amazon Inspector console at https://console.aws.amazon.com/inspector/.
2. [Welcome (ようこそ)] ページで、実行する評価のタイプを選択します。[Network Assessments (ネットワーク評価)] では、AWS 環境のネットワーク設定の脆弱性を分析します。Amazon Inspector エー

ジェントを必要としません。[Host Assessments (ホスト評価)] は、ホスト上のソフトウェアと EC2 instances の設定の脆弱性を分析します。EC2 instances 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 (p. 17)を作成します。

   Note

   評価ターゲットで指定された EC2 インスタンスを識別するために、Amazon Inspector は EC2 インスタンスとタグを列挙する必要があります。Amazon Inspector は、`AWSServiceRoleForAmazonInspector` と呼ばれるサービスに関連付けられたロールを通じて AWS アカウントのこれらのリソースにアクセスします。サービスにリンクされたロールの詳細については、「Amazon Inspector のサービスにリンクされたロールの使用 (p. 17)」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. 該当する場合は、AWS アカウントと AWS リージョンにある利用可能なすべての Amazon EC2 インスタンスに Amazon Inspector エージェント (p. 20)をインストールします。

   Note

   このサービスは、AWS Systems Manager の実行コマンドを許可する EC2 instances にのみ Amazon Inspector 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 AWS リージョンのすべての EC2 インスタンスに SSM エージェントがインストールされており、実行コマンドを許可する IAM ロールがあることを確認してください。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 (p. 23)」を参照してください。

c. [評価ターゲット (p. 35)] 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 (p. 52)にそのターゲットを含めます。

e. [Run weekly (推奨)] または [Run once] 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] をクリックします。Amazon Inspector は評価を自動的に実行します。

高度な設定

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. [Welcome] ページで、[Advanced setup] を選択します。
2. [Define an assessment target] 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選択したままにして、AWS アカウントのすべての EC2 instances リージョンを評価ターゲットに含めることができます。含める EC2 instances 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フにして、ターゲット EC2 instances に関連付けられた [Key (キー)] タグと [Value (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. [Install Agents] では、インスタンスによって [System Manager Run Command] 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、System Manager Run Command を許可する評価ターゲットのすべての EC2 instances 上にのみ Amazon Inspector 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 AWS リージョンのすべての EC2 インスタンスに SSM エージェントがインストール

されており、実行コマンドを許可する IAM ロールがあることを確認してください。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 (p. 23)」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 (p. 22)」を参照してください。

5. [Next] を選択します。
6. [Define an assessment template] ページで、評価テンプレートの名前を入力します。
7. [Rules packages] 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 Rules Packages and Rules (p. 38)」を参照してください。
8. [Duration] で、評価の実行の時間を選択します。
9. [Assessment Schedule] 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. [Next] を選択します。
11. [Review]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、[Create] 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、[Create (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た EC2 インスタンスを識別するために、Amazon Inspector は EC2 インスタンスとタグを列挙する必要があります。Amazon Inspector は、`AWSServiceRoleForAmazonInspector` と呼ばれるサービスに関連付けられたロールを通じて AWS アカウントのこれらのリソースにアクセスします。サービスにリンクされたロールの詳細については、「Amazon Inspector のサービスにリンクされたロールの使用 (p. 17)」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。
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、[Run (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、[Assessment runs] を選択し、[結果] を選択します。結果についての詳細は、「Amazon Inspector の結果 (p. 58)」を参照してください。

Amazon Inspector 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 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の使用 (p. 10)
- チュートリアル :Ubuntu Server での Amazon Inspector の使用 (p. 13)

Amazon Inspector 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 の用語と概念 (p. 2) 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に従って、Amazon Inspector 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 instance の動作を分析します。Amazon Inspector 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。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。初心者ユーザーの場合でワンクリックで Amazon Inspector 評価を設定して実行する場合は、「Creating a Basic Assessment (p. 7)」を参照してください。

トピック

- ステップ 1: Amazon EC2 で使用する Amazon Inspector インスタンスを設定する (p. 10)
- ステップ 2: Amazon EC2 インスタンスを変更する (p. 10)
- 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 (p. 11)
- ステップ 4: 評価テンプレートの作成および実行 (p. 12)
- ステップ 5: 結果を見つけて分析する (p. 12)
- 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 (p. 13)

ステップ 1: Amazon EC2 で使用する Amazon Inspector インスタンスを設定する

このチュートリアルでは、Red Hat Enterprise Linux 7.5 を実行する EC2 instance を 1 つ作成し、[Name] キーと **`InspectorEC2InstanceLinux`** の値を使用してタグ付けします。

> Note
>
> EC2 instances 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 instance 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 (p. 42)」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 instance に接続する方法の指示については、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 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. Sign in to the AWS マネジメントコンソール and open the Amazon Inspector console at https://console.aws.amazon.com/inspector/.
2. ナビゲーションペインで、[Assessment Targets (評価ターゲット)]、[Create (作成)] の順に選択します。

   次の作業を行います。

   a. [Name] 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** を入力します。

   b. [Use Tags (使用するタグ)] に、[キー] フィールドと [値] フィールドの値を入力して、この評価対象に含める EC2 instances を選択します。

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

      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. [Save] を選択します。

   d. タグ付けされた EC2 インスタンスに Amazon Inspector 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 (p. 23) 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 エージェントのインストール (p. 22)」を参照してください。

   e. [Save] を選択します。

   Note

   この時点で、Amazon Inspector 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 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 のサービスにリンクされたロールの作成 (p. 18)」を参照してください。

ステップ 4: 評価テンプレートの作成および実行

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`** を入力します。
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 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 [Findings] 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 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 (p. 12) 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 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 の用語と概念 (p. 2) 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 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 instance の動作を分析する方法について説明します。Amazon Inspector 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。これには、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。

初心者ユーザーの場合でワンクリックで Amazon Inspector 評価を設定して実行する場合は、「Creating a Basic Assessment (p. 7)」を参照してください。

トピック

- ステップ 1: Amazon EC2 で使用する Amazon Inspector インスタンスを設定する (p. 14)
- ステップ 2: Amazon EC2 インスタンスを変更する (p. 14)
- 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 (p. 14)

- ステップ 4: 評価テンプレートの作成および実行 (p. 15)
- ステップ 5: 生成された結果を見つけて分析する (p. 15)
- 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 (p. 16)

ステップ 1: Amazon EC2 で使用する Amazon Inspector インスタンスを設定する

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 instance 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 instances 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 instance を変更し、潜在的な安全上の問題 CVE-2017-6507 に曝露します。詳細については、https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6507 および「共通脆弱性識別子 (p. 42)」を参照してください。

EC2 インスタンスを変更するには

- 前のセクションで作成したインスタンスの **InspectorEC2InstanceUbuntu** を接続し、次のコマンドを実行します。

  ```
  sudo apt-get install apparmor=2.10.95-0ubuntu2.5
  ```

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 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 instance にエージェントをインストールするには

1. Sign in to the AWS マネジメントコンソール and open the Amazon Inspector console at https://console.aws.amazon.com/inspector/.
2. ナビゲーションペインで、[Assessment Targets (評価ターゲット)]、[Create (作成)] の順に選択します。
3. [Name] 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 (使用するタグ)] に、[キー] フィールドと [値] フィールドの値を入力して、この評価対象に含める EC2 instances を選択します。

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

   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. タグ付けされた EC2 インスタンスに Amazon Inspector 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 (p. 23) 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 エージェントのインストール (p. 22)」を参照してください。
6. [Save] を選択します。

   Note

   この時点で、Amazon Inspector 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 のサービスにリンクされたロールの作成 (p. 18)」を参照してください。

ステップ 4: 評価テンプレートの作成および実行

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`** を入力します。
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 5: 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 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、推奨されるステップ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-2017-6507] に対する結果が生成されます。

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。

   重要度が [High (高)] の新しい結果として [Instance InspectorEC2InstanceUbuntu is vulnerable to CVE-2017-6507 (インスタンス InspectorEC2InstanceUbuntu は CVE-2017-6507 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 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-2017-6507] 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。

1. インスタンス **`InspectorEC2InstanceUbuntu`** に接続し、次のコマンドを実行します。

   ```
   sudo apt-get install apparmor=2.10.95-0ubuntu2.6
   ```
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 5: 生成された結果を見つけて分析する (p. 15) 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。

   セキュリティの問題 [CVE-2017-6507] は解決されたため、結果は表示されません。

Amazon Inspector のサービスにリンクされたロールの使用

Amazon Inspector 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。サービスにリンクされたロールは、Amazon Inspector に直接リンクされた一意のタイプの IAM ロールです。サービスにリンクされたロールは、Amazon Inspector による事前定義済みのロールであり、ユーザーに代わってサービスから AWS の他のサービスを呼び出すために必要なすべてのアクセス権限を備えています。

サービスにリンクされたロールを使用すると、必要なアクセス許可を手動で追加する必要がなくなるため、Amazon Inspector の設定が簡単になります。Amazon Inspector はこのサービスにリンクされたロールのアクセス許可を定義し、特に定義されている場合を除き、Amazon Inspector のみがそのロールを引き受けます。定義されるアクセス権限には、信頼ポリシーやアクセス許可ポリシーなどがあり、そのアクセス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。

サービスにリンクされたロールを削除するには、まず、Amazon Inspector を実行しているすべてのリージョンの AWS アカウントの評価ターゲットを削除する必要があります。

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については、「IAM と連携する AWS サービス」を参照の上、サービスにリンクされたロール列が「Yes (あり)」になっているサービスを検索してください。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 のサービスにリンクされたロールのアクセス許可

Amazon Inspector では、サービスにリンクされたロールとして `AWSServiceRoleForAmazonInspector` を使用します。サービスにリンクされたロール `AWSServiceRoleForAmazonInspector` は、このロールを引き受けるために Amazon Inspector を信頼します。

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: `arn:aws:iam::*:role/aws-service-role/inspector.amazonaws.com/AWSServiceRoleForAmazonInspector` で `iam:CreateServiceLinkedRole`

`AWSServiceRoleForAmazonInspector` ロールを適切に作成するには、Amazon Inspector を使用する IAM アイデンティティ (ユーザー、ロール、またはグループ) に、必要なアクセス権限が付与されている必要があります。必要なアクセス許可を付与するには、`AmazonInspectorFullAccess` 管理ポリシーをこの IAM ユーザー、グループ、またはロールにアタッチします。管理ポリシーの詳細については、「Amazon Inspector での AWS 管理 (事前定義) ポリシー (p. 84)」を参照してください。

サービスにリンクされたロールの詳細については、『IAM ユーザーガイド』の「サービスにリンクされたロールのアクセス許可」を参照してください。

Amazon Inspector のサービスにリンクされたロールの作成

`AWSServiceRoleForAmazonInspector` サービスにリンクされたロールを手動で作成する必要はありません。

`AWSServiceRoleForAmazonInspector` サービスリンクロールは自動的に作成されますが、最初に最小限の設定を行う必要がある場合があります。以下のセクションでは、`AWSServiceRoleForAmazonInspector` サービスにリンクされたロールの設定と使用の詳細について説明します。

初めて Amazon Inspector を開始する場合

- `AWSServiceRoleForAmazonInspector` サービスにリンクされたロールは、コンソールの [Amazon Inspector の使用を開始する] ウィザードを使用した場合、または API の CreateAssessmentTarget オペレーション実行時に自動的に作成されます。
- `AWSServiceRoleForAmazonInspector` サービスにリンクされたロールが作成されるのは、現在サインイン中のリージョンの AWS アカウントに対してのみです。そのリージョン内でのみ、AWS アカウントのリソースへの Amazon Inspector サービスアクセスを許可します。同じ AWS アカウントで [Amazon Inspector の使用を開始する] コンソールウィザードを使用するか、他のリージョンで API の CreateAssessmentTarget オペレーションを実行する場合は、AWS アカウントにすでに作成されている、サービスにリンクされた同ロールがこのようなリージョンに適用されるため、このリージョンの AWS アカウントのリソースに対するアクセス権も Amazon Inspector に付与されます。

AWS アカウントで実行されている Amazon Inspector がすでにある場合

- AWS アカウントで実行されている Amazon Inspector がすでにある場合、リソースに対するアクセス権を Amazon Inspector に付与する IAM ロールは、すでに AWS アカウントに付与されています。この場合、新しい評価ターゲットまたは新しい評価テンプレートを作成すると (Amazon Inspector コンソールまたは API オペレーション)、`AWSServiceRoleForAmazonInspector` サービスにリンクされたロールが自動作成されます。以前作成し、現在までリソースに対するアクセス権を Amazon Inspector に付与していた IAM ロールは、新しく作成されたサービスにリンクされたロールに置き換わります。

  また、Amazon Inspector の [Dashboard (ダッシュボード)] ページの [Accounts Setting (アカウント設定)] セクションの [Manage Amazon Inspector service-linked role (Amazon Inspector のサービスにリンクされたロールの管理)] リンクを選択して、`AWSServiceRoleForAmazonInspector` サービスにリンクされたロールを手動で作成することもできます。以前作成し、現在までリソースに対するアクセス権を Amazon Inspector に付与していた IAM ロールは、新しく作成されたサービスにリンクされたロールに置き換わります。

  > **Note**
  >
  > 以前に作成したこの IAM ロールは削除されません。そのまま残りますが、リソースに対するアクセス権を Amazon Inspector に付与することを目的として使用されることはありません。この IAM ロールをさらに管理または削除するには IAM コンソールを使用します。

- `AWSServiceRoleForAmazonInspector` サービスにリンクされたロールが作成されるのは、現在サインイン中のリージョンの AWS アカウントに対してのみです。Amazon Inspector がこのロールを使用してアクセスできるのは、このリージョンの AWS アカウントに含まれるリソースのみです。同じ AWS アカウントを使用して、他のリージョンで実行されている Amazon Inspector の評価ターゲットまたは評価テンプレートを作成すると、AWS アカウントにすでに作成されているのと同じサービスにリンクさ

れたロールが適用されます。Amazon Inspector がこのロールを使用してアクセスできるのは、これらのリージョンの AWS アカウントに含まれるリソースです。

IAM コンソールを使用して、Inspector サービスにリンクされたロールを作成することもできます。IAM CLI または IAM API で、サービスにリンクされたロールをサービス名 (`Amazon Inspector`) で作成します。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を作成する」を参照してください。

このサービスにリンクされたロールを削除した後で再度作成する必要が生じた場合は、同じ方法でアカウントにロールを再作成できます。Get started with Amazon Inspector again を実行すると、サービスにリンクされたロールが自動的に再作成されます。

Amazon Inspector のサービスにリンクされたロールの編集

Amazon Inspector では、`AWSServiceRoleForAmazonInspector` サービスにリンクされたロールを編集することはできません。サービスにリンクされたロールを作成すると、多くのエンティティによってロールが参照され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 を使用したロールの説明の編集はできます。詳細については、IAM ユーザーガイド の「サービスにリンクされたロールの編集」を参照してください。

Amazon Inspector のサービスにリンクされたロールの削除

サービスにリンクされたロールが必要な機能またはサービスが不要になった場合には、その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、サービスにリンクされた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
>
> リソースを削除する際に、Amazon Inspector サービスでロールが使用されている場合、削除は失敗することがあります。失敗した場合は、数分待ってから再度オペレーションを実行してください。

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

- Amazon Inspector を実行しているすべてのリージョンにある、この AWS アカウントの評価ターゲットを削除します。詳細については、「Amazon Inspector の評価ターゲット (p. 35)」を参照してください。

IAM を使用して、サービスにリンクされたロールを手動で削除するには

IAM コンソール、IAM CLI、または IAM 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 エージェント

Amazon Inspector エージェントは、Amazon EC2 インスタンスの動作データ (ネットワーク設定、ファイルシステムのセキュリティ、プロセスアクティビティなど) を収集およびモニタリングするエンティティです。すべてのケースで必要ではありませんが、セキュリティを完全に評価するためには、ターゲットの各 Amazon 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 エージェントの操作 (p. 26)」および「Windows ベースのオペレーティングシステムでの Amazon Inspector エージェントの操作 (p. 28)」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 (p. 39)ルールパッケージを実行する必要はありません。

トピック

- Amazon Inspector エージェントのアクセス許可 (p. 20)
- ネットワークと Amazon Inspector エージェントセキュリティ (p. 21)
- Amazon Inspector エージェントの更新 (p. 21)
- テレメトリデータのライフサイクル (p. 22)
- Amazon Inspector から AWS アカウントへのアクセス制御 (p. 22)
- Amazon Inspector エージェントの制限 (p. 22)
- Amazon Inspector エージェントのパブリックライセンス (p. 22)
- Amazon Inspector エージェントのインストール (p. 22)
- Linux ベースのオペレーティングシステムでの Amazon Inspector エージェントの操作 (p. 26)
- Windows ベースのオペレーティングシステムでの Amazon Inspector エージェントの操作 (p. 28)
- (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 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。 (p. 30)
- (オプション) Windows ベースのオペレーティングシステムの Amazon Inspector 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。 (p. 34)

Amazon Inspector エージェントのアクセス許可

Amazon Inspector 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と、エージェントが機能するために必要なカーネルモジュールで構成されます。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。エージェントには、エージェントが機能するために必要なカーネルモードドライバーも含まれています。

> **Important**
>
> 以下のリストには、Linux、Ubuntu、Red Hat Enterprise Linux、および CentOS 上で実行されている Amazon Inspector エージェントと互換性のあるすべてのカーネルバージョンが含まれています。https://s3.amazonaws.com/aws-agent.us-east-1/linux/support/supported_versions.json
> CVE (p. 42)、CIS (p. 42)、またはセキュリティのベストプラクティス (p. 47)ルールパッケージを使用して、Linux ベースの OS で EC2 instance の Amazon Inspector 評価を実行できます。インスタンスにリストに含まれているカーネルバージョンがない場合でも、評価は成功します。

Linux ベースの OS での 実行時の動作の分析 (p. 44) ルールパッケージを使用して、EC2 instance の評価を正しく実行するには、お使いのインスタンスがこのリストに含まれているカーネルバージョンに該当していなければなりません。インスタンスにエージェントと互換性のないカーネルバージョンがある場合、EC2 instance を評価する実行時の動作の分析 (p. 44)ルールパッケージは 1 つの検出結果のみをもたらします。この結果で EC2 instance のカーネルバージョンがサポートされていないことがわかります。

ネットワークと Amazon Inspector エージェントセキュリティ

Amazon Inspector エージェントは、Amazon Inspector サービスとのほぼすべての通信を開始します。つまり、エージェント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、パブリックエンドポイントへのアウトバウンドネットワークパスを持っている必要があります。たとえば、エージェントは `arsenal.<region>.amazonaws.com` で、エンドポイントは `s3.dualstack.aws-region.amazonaws.com` の Amazon S3 バケットです。(`<region>` は、Amazon Inspector を実行している実際の AWS リージョン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 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、EC2 instance のロール、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に関連付けられた AWS ID を使用して認証される TLS 保護チャネル経由で Amazon Inspector と定期的に通信します。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 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 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 エージェントの更新

Amazon Inspector 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 instances 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 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 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 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 専用の Amazon S3 バケットに安全に保存されます。Amazon Inspector 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 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 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 から AWS アカウントへのアクセス制御

セキュリティサービスである Amazon Inspector は、評価する EC2 instances を見つけるために必要な場合のみ、タグのクエリを実行して AWS アカウントおよびリソースにアクセスします。これは、Amazon Inspector 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、標準の 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 instances にインストールされた Amazon Inspector 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オブジェクトは、Amazon Inspector によって管理され、Amazon Inspector 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 エージェントの制限

Amazon Inspector エージェントの制限数の詳細については「Amazon Inspector サービスの制限 (p. 4)」を参照してください。

Amazon Inspector エージェントのパブリックライセンス

Amazon Inspector エージェントは、エージェント全体のコンポーネントとしてカーネルモジュール (`amznmon64`) を使用します。このカーネルモジュールでは、一般的なパブリックライセンス (GPLv2) を使用します。モジュールのソースコードとライセンス情報は一般公開されており、以下でアクセスできます。

- ソースコード :https://s3.amazonaws.com/aws-agent.us-east-1/linux/support/AwsAgentKernelModule.tar.gz
- 署名ファイル :https://s3.amazonaws.com/aws-agent.us-east-1/linux/support/AwsAgentKernelModule.tar.gz.sig

Amazon Inspector エージェントのインストール

Systems Manager 実行コマンドを使用して、Amazon Inspector エージェントを複数のインスタンス (Linux ベースおよび Windows ベースの両方のインスタンス) にインストールできます。または、各 EC2

instance 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。または、エージェントを インストールしてサインインすることによって 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 [Define an Assessment target (評価ターゲットの定義)] ページで [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することで、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ばやくインストールできます。

トピック

- Amazon Inspector エージェントを使用した Amazon Linux AMI (p. 23)
- 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 (p. 23)
- 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 (p. 24)
- 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 (p. 25)

> Note
>
> この章の手順は、Amazon Inspector 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。

Amazon Inspector エージェントを使用した Amazon Linux AMI

評価ターゲットに含める Amazon Linux EC2 instances に手動で Amazon Inspector エージェントをインストールしない場合は、[Amazon Linux AMI with Amazon Inspector Agent] を使用します。この AMI には、エージェントがあらかじめインストールされているため、エージェントをインストールまたはセットアップするための追加のステップは不要です。このような EC2 instances で Amazon Inspector の使用を開始するには、必要な評価ターゲットを一致させるようにタグ付けします。[Amazon Linux AMI with Amazon Inspector Agent] を設定すると、2 つの主なセキュリティ目標 (アクセス制限、ソフトウェア脆弱性の軽減) に焦点を当てることでセキュリティが強化されます。

これは、あらかじめインストールされた Amazon Inspector エージェントで現在利用できる唯一の EC2 instance AMI です。Ubuntu サーバーまたは Windows サーバーを実行する EC2 instances の場合は、エージェントのインストールステップを手順で行う必要があります。

[Amazon Linux AMI with Amazon Inspector Agent (Amazon Inspector Agent エージェントを使用した Amazon Linux AMI)] は、EC2 コンソール、および AWS Marketplace で使用できます。

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

Systems Manager Run Command を使用して EC2 instances に Amazon Inspector エージェントをインストールできます。これにより、AWS エージェントを複数のインスタンス (Linux ベースおよび Windows ベースの両方) 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 instance に 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。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 instances 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「Configuring Security Roles for System Manager」を参照してください。

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

1. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
2. [Systems Manager Services] にあるナビゲーションペインで、[Run Command] を選択します。
3. [Run a command] を選択します。
4. [Command document (コマンドのドキュメント)] で、[Amazon] が所有する AmazonInspector-ManageAWSAgent 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 instances に Amazon Inspector 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. [Select targets by (ターゲットの選択)] で、[Specifying a Tag (タグの指定)] オプションを選択するか、[Manually Selecting Instances (インスタンスの手動選択)] を選択して EC2 instances を指定します。次に [Select instances (インスタンスの選択)] を選択します。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。
6. 「EC2 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を行い、[Run (実行)] を選択します。

Note

また、新しい評価ターゲットの作成中に、既存のターゲットの [Install Agents with Run Command (Run Command を使用したエージェントのインストール)] ボタンを使用して、エージェントを複数の EC2 instances (Linux ベースおよび Windows ベースの両方) に インストールできます。詳細については、「評価ターゲットを作成する (p. 36)」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する

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

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

1. Amazon Inspector 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 instance にサインインします。

   Note

   Amazon Inspector がサポートするオペレーティングシステムの詳細については、「Amazon Inspector 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 (p. 4)」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 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。 (p. 30)」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

   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 エージェントの更新 (p. 21)」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)
   - `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 instance に Amazon Inspector エージェントをインストールします。

Windows ベースの EC2 instance 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 instance にサインインします。

   Note

   Amazon Inspector がサポートするオペレーティングシステムの詳細については、「Amazon Inspector 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 (p. 4)」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 エージェントの更新 (p. 21)」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 エージェントの操作

Amazon Inspector エージェントの動作をインストール、削除、確認および変更します。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 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 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 (p. 4)」を参照してください。

> **Note**
>
> このセクションの次のコマンドは、Amazon Inspector 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 エージェントが実行されていることを確認する (p. 26)
- Amazon Inspector エージェントを停止する (p. 26)
- Amazon Inspector エージェントを開始する (p. 26)
- Amazon Inspector エージェントの設定を変更する (p. 27)
- Amazon Inspector エージェントのプロキシサポートを設定する (p. 27)
- Amazon Inspector エージェントをアンインストールする (p. 28)

Amazon Inspector エージェントが実行されていることを確認する

- 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 instance 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 エージェントを停止する

- 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 エージェントを開始する

- 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 エージェントの設定を変更する

Amazon Inspector エージェントが EC2 instance 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 サポートのガイドを受けることをお勧めします。

Amazon Inspector エージェントのプロキシサポートを設定する

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 instance 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する (p. 24) のステップを実行して、Amazon Inspector エージェントのインストールを完了します。

エージェントを実行しながら、EC2 instance 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 instance 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 エージェントが実行されていることを確認する (p. 26)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する (p. 24)の手順に従って、この EC2 instance 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 エージェントをアンインストールする

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 instance にサインインします。

   Note

   Amazon Inspector 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 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 (p. 4)」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 エージェントの操作

Amazon Inspector 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 instance 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 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 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 (p. 4)」を参照してください。

Note

この章の次のコマンドは、Amazon Inspector 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 エージェントの開始中または停止中またはそのエージェントが実行中であることの確認 (p. 29)
- Amazon Inspector エージェントの設定を変更する (p. 29)
- Amazon Inspector エージェントのプロキシサポートを設定する (p. 29)

- Amazon Inspector エージェントをアンインストールする (p. 30)

Amazon Inspector エージェントの開始中または停止中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 instance 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している場合、2 つのサービス ([AWS Agent Service] および [AWS Agent Updater Service]) が、状態が [開始] または [実行中] に設定されて [サービス] ウィンドウに表示されます。
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 instance にサインインし、管理者アクセス許可を使用して次の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 エージェントの設定を変更する

Amazon Inspector エージェントが EC2 instance 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 サポートのガイドを受けることをお勧めします。

Amazon Inspector エージェントのプロキシサポートを設定する

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` プロキシをセットアップするには、「https://technet.microsoft.com/en-us/library/cc731131%28v=ws.10%29.aspx」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 instance 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 instance 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 instance で実行している Amazon Inspector エージェントが 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 エージェントの開始中または停止中またはそのエージェントが実行中であることの確認 (p. 29)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 (p. 25)の手順に従って、この EC2 instance 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、[AWS Agent Service] を検索し、[サービス] ウィンドウで [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 エージェントの開始中または停止中またはそのエージェントが実行中であることの確認 (p. 29)」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 エージェントをアンインストールする

エージェントをアンインストールするには

1. Amazon Inspector 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 instance にサインインします。

   Note

   Amazon Inspector 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 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 (p. 4)」を参照してください。
2. EC2 instance 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 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 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 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。

Linux ベースのオペレーティングシステム用の Amazon Inspector 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 ツールを検証するために使用できるパブリックキーと署名を発行します。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 (p. 31)
- パブリック キーの認証とインポート (p. 31)
- パッケージの署名の確認 (p. 33)

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

次のステップでは、Amazon Inspector のパブリックキーを認証し、信頼されたキーとして GPG キーリングへ追加します。

Amazon Inspector のパブリック 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.key] 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.key 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 の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.key
```

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、キー値を前述のステップ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 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 サポート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後、Amazon Inspector 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://d1wk0tztpsntt1.cloudfront.net/linux/latest/install.sig
```

2. `install.sig` と Amazon Inspector 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 のインストール 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 サポート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、信頼済みの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 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: 最終的に信頼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「最終的に信頼された」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。

(オプション) Windows ベースのオペレーティングシステムの Amazon Inspector 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、Windows ベースのオペレーティングシステム用の Amazon Inspector 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 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。

5C 2C B5 5A 9A B9 B1 D6 3F F4 1B 0D A2 76 F2 A9 2B 09 A8 6A

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、[Properties (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. [Signature List] で [Amazon Services LLC] を選択し、[Details] をクリックします。
4. すでに選択していない場合は [General] タブにアクセスし、[View Certificate] を選びます。
5. [Details (詳細)] タブを選択し、まだの場合は [All (すべて)] を [Show (表示)] のドロップダウンリストで選択します。
6. [Thumbprint] フィールドが表示されるまでスクロールして、[Thumbprint] 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、

     5C 2C B5 5A 9A B9 B1 D6 3F F4 1B 0D A2 76 F2 A9 2B 09 A8 6A

     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 の評価ターゲット

Amazon Inspector を使用すると、AWS 評価ターゲット (AWS リソースの集合体) に対処が必要な潜在的なセキュリティ上の問題が存在す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、「Amazon Inspector サービスの制限 (p. 4)」を参照してください。

> Note
>
> EC2 instances 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 (p. 35)
- Amazon Inspector 評価ターゲットの制限 (p. 35)
- 評価ターゲットを作成する (p. 36)
- 評価ターゲットを削除する (p. 37)

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 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 instances 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 は、作成したタグを使用して、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、ユーザーが選択したキーと値のペアで構成されています。たとえば、キーの名前で [Name]、値で [MyFirstInstance] を選択します。インスタンスをタグ付けした後は、Amazon Inspector 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 instances をタグ付けし、評価ターゲットを作成している場合、固有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が作成したタグキーを使用することができます。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、AWS は起動した EC2 instances の [Name (名前)] タグキーを自動的に作成します。

作成した EC2 instances にはタグを追加できます。これらのタグは、各 EC2 instance のコンソールページで 1 度に 1 つずつ追加、変更、または削除できます。タグ エディターを使用すると、一度に複数の EC2 instances 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 instances 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 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 サービスの制限 (p. 4)」を参照してください。

評価ターゲットを作成する

Amazon Inspector 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. Sign in to the AWS マネジメントコンソール and open the Amazon Inspector console at https://console.aws.amazon.com/inspector/.
2. ナビゲーション ペインで、[Assessment Targets (評価ターゲット)]、[Create (作成)] の順に選択します。
3. [Name (名前)] に、評価ターゲットの名前を入力します。
4. 以下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 instances を含めるには、[All instances (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 サービスの制限 (p. 4)」を参照してください。
   - この評価ターゲットに含める EC2 instances を選択するには、[Use Tags (使用するタグ)] 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、[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てエージェントをこのターゲットのすべての EC2 instances 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 instances に 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 ロールがなければなりません。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 instances 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「Configuring Security Roles for System Manager」を参照してください。

   Important

   既に EC2 instance 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は、[Run Command でエージェントをインストール] ボタンを選択して、このターゲットのすべての EC2 instances にエージェントをインストールします。

   Note

   また、Systems Manager Run Command を使用して、エージェントを複数の EC2 instances 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 (p. 23)」を参照してください。
6. [保存] を選択します。

   Note

   [Assessment Targets (評価ターゲット)] ページの [Preview Target (ターゲットをプレビュー)] を使用して、評価ターゲットに含まれるすべての EC2 instances を確認できます。EC2 instance

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。エージェントステータスには、次の値があります。[HEALTHY (正常)]、[UNHEALTHY (異常)]、および [UNKNOWN (不明)]。[UNKNOWN (不明)] ステータスは EC2 instance で実行中のエージェントの有無を判断できない場合に Amazon Inspector に表示されます。

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

- [評価ターゲット] ページで、削除するターゲットを選択し、[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、[Yes] 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 のルール パッケージとルール

Amazon Inspector を使用し、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 は、評価ターゲットの動作とセキュリティ設定を、選択されたセキュリティルールパッケージと比較します。Amazon Inspector のコンテキストでは、ルールは、評価の実行中に Amazon Inspector が実行するセキュリティチェックを意味します。

Amazon Inspector 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。たとえば、Amazon Inspector 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 でのルールの重大度 (p. 38)
- Amazon Inspector のルールパッケージ (p. 38)

Amazon Inspector でのルールの重大度

Amazon Inspector の各ルールには重大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。[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。以下は、各レベルで推奨される応答方法です。

- [High] - 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。このセキュリティ上の問題は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。
- [Medium] - 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。次の可能な機会 (たとえば、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。
- [Low] - 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。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。
- [Informational] - 評価ターゲットの特定のセキュリティ設定の詳細を示しています。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 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 (p. 39)

ホスト評価:

- 共通脆弱性識別子 (p. 42)
- Center for Internet Security (CIS) ベンチマーク (p. 42)
- Amazon Inspector のセキュリティのベストプラクティス (p. 47)
- 実行時の動作の分析 (p. 44)

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 instances 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。

ネットワーク到達可能性ルールパッケージは、AWS の Provable Security イニシアチブの最新のテクノロジを使用しています。

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 (Application Load Balancers または Classic Load Balancer 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 instance 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 エージェントは、このルールパッケージを使用して EC2 instance 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。

> **Important**
>
> このルールパッケージは Amazon EC2 Classic ネットワークをサポートしません。

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に関して、Amazon Inspector ルールパッケージ (p. 69)」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
- Application Load Balancer
- Direct Connect
- Elastic Load Balancers
- Elastic Network Interface

- 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)
- Subnets
- Virtual Private Cloud (VPC)
- 仮想プライベートゲートウェイ (VGW)
- VPC ピアリング接続

Important

ネットワーク到達可能性ルールパッケージは、インバウンドアクセスを許可または制限する他の設定素を考慮していません。

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 (Application Load Balancer および Classic Load Balancer 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` (p. 40)
- `UnrecognizedPortWithListener` (p. 41)
- `NetworkExposure` (p. 42)

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 instance 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
LDAP over TLS	636	
グローバルカタログ LDAP	3268	
グローバルカタログ LDAP over TLS	3269	
NFS	111、2049、4045、1110	111、2049、4045、1110
Kerberos	88、464、543、544、749、750	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
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 instance 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 [Low (低)] の重要度が与えられます。

NetworkExposure

このタイプの結果は、EC2 instance 到達可能なポートに関する集計情報 を示しています。EC2 instance の Elastic Network Interface 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、[Informational (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 instances 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 の評価で作成された結果に特定の CVE が表示される場合は、CVE の ID (**CVE-2009-0021** など) を https://cve.mitre.org/ で検索できます。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。

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 instancesが CVE に対して公開されているかどうか評価するために役立ちます。

- 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)
- 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に関して、Amazon Inspector ルールパッケージ (p. 69)」を参照してください。

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

CIS セキュリティベンチマークプログラムは、組織がセキュリティを評価して強化できるよう明確に定義された、公平で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 セキュリティベンチマークのメンバー企業です。Amazon Inspector 認証のリストについては、「CIS ウェブサイトのアマゾンウェブサービス」を参照してください。

Amazon Inspector 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 7 Benchmark v2.0.2 Level 2 Server
- CIS Benchmark for CentOS Linux 7 Benchmark v2.0.2 Level 1 Workstation
- CIS Benchmark for CentOS Linux 7 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 7 Benchmark v2.0.2 Level 2 Server
- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.0.2. Level 1 Workstation
- CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.0.2 Level 2 Workstation

Ubuntu

- 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 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)
- 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 1 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 1 Domain Controller Profile)

特定の CIS ベンチマークが、Amazon Inspector 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に関して、Amazon Inspector ルールパッケージ (p. 69)」を参照してください。

実行時の動作の分析

ランタイム動作分析ルールパッケージのルールは、評価実行中のインスタンスの動作を分析します。また、EC2 instances をより安全にする方法についてのガイダンスも提供します。

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に関して、Amazon Inspector ルールパッケージ (p. 69)」を参照してください。

トピック

- 安全でないクライアントプロトコル (ログイン) (p. 44)
- 安全でないクライアントプロトコル (一般) (p. 45)
- 未使用のリッスンする TCP ポート (p. 45)
- 安全でないサーバープロトコル (p. 46)
- データ実行防止機能を持たないソフトウェア (DEP) (p. 46)
- 安全でないアクセス権限を持つ Root プロセス (p. 47)

安全でないクライアントプロトコル (ログイン)

このルールでは、リモートマシンにログインするためのクライアントによる安全でないプロトコルの使用を検出します。

> 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 instances を評価ターゲットに含めることができます。
> このルールは 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 instances の結果を生成します。

重大度: [Medium (p. 38)]

結果

評価ターゲットの EC2 instance は、安全でないプロトコルを使用してログインのためにリモートホストに接続しています。これらのプロトコルは認証情報を保護せずプレーンテキストで渡すため、証明書の盗難リスクが高まります。

解決方法

これらの安全でないプロトコルを、SSH などの安全なプロトコルと置き換えることをお勧めします。

安全でないクライアントプロトコル (一般)

このルールは、クライアントによる安全でないプロトコルの使用を検出します。

> **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 instances を評価ターゲットに含めることができます。
> このルールは 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 instances の結果を生成します。

重大度: [Low (p. 38)]

結果

評価ターゲットの EC2 instance は、安全でないプロトコルを使用してリモートホストに接続しています。これらのプロトコルはトラフィックを保護しないため、トラフィック傍受攻撃が成功するリスクが高まります。

解決方法

これらの安全でないプロトコルは、暗号化されたバージョンと置き換えることをお勧めします。

未使用のリッスンする TCP ポート

このルールは、評価ターゲットで必要ではない可能性のある、リッスンする TCP ポートを検出します。

> **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 instances を評価ターゲットに含めることができます。
> このルールは 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 instances の結果を生成します。

重大度: [Informational (p. 38)]

結果

評価ターゲットの EC2 instance は TCP ポートでリッスンしていますが、Amazon Inspector は、評価の実行中にこれらのポートへのトラフィックを発見しませんでした。

解決方法

デプロイの攻撃対象領域を減らすため、使用していないネットワークサービスは無効にすることをお勧めします。ネットワークサービスが必要な場合、VPC ACL、EC2 セキュリティグループ、ファイアウォールなどのネットワークコントロールメカニズムを採用して、そのサービスの公開を制限することをお勧めします。

安全でないサーバープロトコル

このルールは、EC2 instances が FTP、Telnet、HTTP、IMAP、POP バージョン 3、SMTP、SNMP バージョン 1 および 2、RSH、`rlogin` などの安全でないおよび暗号化されていないポート/サービスのサポートを許可しているかどうかを判断するのに役立ちます。

> **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 instances を評価ターゲットに含めることができます。
> このルールは 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 instances の結果を生成します。

重大度: [Informational (p. 38)]

結果

評価ターゲットの EC2 instance は、安全でないプロトコルをサポートするように設定されています。

解決方法

評価ターゲットの EC2 instance でサポートされている安全でないプロトコルを無効化し、以下に示す安全な代替プロトコルと置き換えることをお勧めします。

- Telnet、RSH、`rlogin` を無効にして SSH に置き換えます。これが不可能な場合、安全でないサービスが VPC ネットワーク ACL や EC2 セキュリティグループなどの適切なネットワーク アクセス コントロールで保護されていることを確認する必要があります。
- 可能な場合は FTP を SCP または SFTP と置き換えます。これが不可能な場合、FTP サーバーが VPC network ACL や EC2 セキュリティ グループなどの適切なネットワーク アクセス コントロールで保護されていることを確認する必要があります。
- 可能な場合は HTTP を HTTPS と置き換えます。問題のウェブサーバーに固有の詳細については、「`http://nginx.org/en/docs/http/configuring_https_servers.html`」および「`http://httpd.apache.org/docs/2.4/ssl/ssl_howto.html`」を参照してください。
- IMAP、POP3、SMTP の各サービスが必要ない場合はこれらを無効にします。必要な場合は、これらの E メール プロトコルを TLS などの暗号化プロトコルとともに使用することをお勧めします。
- SNMP サービスが必要ない場合はこれを無効にします。必要な場合は、SNMP v1 および v2 を、暗号化通信を使用するより安全な SNMP v3 と置き換えます。

データ実行防止機能を持たないソフトウェア (DEP)

このルールでは、データ実行防止 (DEP) のサポートなしでコンパイルされたサードパーティー製ソフトウェアの存在を検出します。DEP は、スタックベースのバッファオーバーフローやその他のメモリ破損攻撃を防御して、システムセキュリティを向上させます。

> **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 instances を評価ターゲットに含めることができます。

評価の実行中に、このルールは 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 instances の結果のみを生成します。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 instances の結果は生成されません。

重大度: [Medium (p. 38)]

結果

評価ターゲットの EC2 instance に、DEP をサポートしていない実行ファイルがあります。

解決方法

このソフトウェアを使用していない場合は、評価ターゲットからアンインストールします。または、DEP が有効な更新バージョンについてベンダーに問い合わせます。

安全でないアクセス権限を持つ Root プロセス

このルールは、不正ユーザーによる変更が可能なモジュールをロードする root プロセスを検出します。

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 instances を評価ターゲットに含めることができます。
評価の実行中に、このルールは 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 instances の結果のみを生成します。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 instances の結果は生成されません。

重大度: [High (p. 38)]

結果

評価ターゲットに、許可されていない変更が行われる危険がある共有オブジェクトを使用する、1 つ以上の root 所有プロセスを持つインスタンスがあります。これらの共有オブジェクトには不適切なアクセス権限/所有権があるため、改ざんの危険があります。

解決方法

評価ターゲットのセキュリティを向上させるため、関連モジュールの権限を修正して root ユーザー以外が書き込みできないようにすることをお勧めします。

Amazon Inspector 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 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 instances 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 instances 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 instances 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に関して、Amazon Inspector ルールパッケージ (p. 69)」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 (p. 48)
- SSH バージョン 2 のみをサポート (p. 48)
- SSH 経由のパスワード認証を無効化する (p. 49)
- パスワードの有効期限を設定する (p. 49)
- パスワードの最小文字数を設定する (p. 49)
- パスワードの複雑さを設定する (p. 50)
- ASLR の有効化 (p. 50)
- DEP の有効化 (p. 50)
- システムディレクトリに対するアクセス権限の設定 (p. 51)

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 instance への口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。

重大度: [Medium (p. 38)]

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の EC2 instance 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。

解決方法

SSH 経由の root アカウントを禁止するように EC2 instance 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 instances 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。

重大度: [Medium (p. 38)]

結果

評価ターゲットの EC2 instance 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。

解決方法

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 instances 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 instances 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。

重大度: [Medium (p. 38)]

結果

評価ターゲットの EC2 instance 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。

解決方法

EC2 instances 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することをお勧めします。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 instances 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。

重大度 - [Medium (p. 38)]

結果

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

解決方法

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 instances 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 instances 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。

重大度: [Medium (p. 38)]

結果

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

解決方法

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 instances 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。パスワード最小文字数を設定するには、PAM 設定で `pam_cracklib.so` の `minlen` パラメータを設定します。詳細については、「`man pam_cracklib`」を参照してください。

パスワードの複雑さを設定する

このルールは、EC2 instances でパスワードの複雑さ要件が設定されているかどうかを判断するのに役立ちます。

重大度: [Medium (p. 38)]

結果

評価ターゲットの EC2 instances で、パスワードの複雑さ要件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。

解決方法

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 instances 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。

ASLR の有効化

このルールは、評価ターゲット内の EC2 instances 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。

重大度: [Medium (p. 38)]

結果

評価ターゲット内の EC2 instance で ASLR は有効になっていません。

解決方法

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 を実行して評価ターゲット内のすべての EC2 instances 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 instances 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。

重大度: [Medium (p. 38)]

結果

評価ターゲット内の EC2 instance で DEP は有効になっていません。

解決方法

評価ターゲット内のすべての EC2 instances 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権限の設定

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。

重大度: [High (p. 38)]

結果

評価ターゲット内の EC2 instance 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。

解決方法

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 instances 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 の評価テンプレートと評価の実行

Amazon Inspector 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によって、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 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。このデータには、AWS サービスとの通信の詳細、安全な交信の使用、実行プロセスの詳細、実行プロセス間のネットワーク トラフィックなどが含まれます。次に Amazon Inspector 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 は、様々な重大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 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 の評価テンプレート (p. 52)
- Amazon Inspector の評価テンプレートの制限 (p. 53)
- 評価テンプレートを作成中 (p. 53)
- 評価テンプレートを削除する (p. 54)
- 評価の実行 (p. 54)
- Amazon Inspectorの評価の実行の制限 (p. 55)
- Lambda 関数を使用した評価の自動実行をセットアップする (p. 55)
- Amazon Inspector 通知用の SNS トピックを設定するには (p. 56)

Amazon Inspector の評価テンプレート

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に Amazon Inspector が使用するルールパッケージ
- 評価の実行の時間

  Note

  時間は次のいずれかの値に設定できます。
  - 15 分
  - 1 時間 (推奨)
  - 8 時間
  - 12 時間
  - 24 時間

  評価テンプレートの時間が長いほど、Amazon Inspector は、より詳細かつ包括的なテレメトリのセットを収集して分析します。つまり、分析時間が長くなることで、Amazon Inspector は評価ターゲットの動作を細部に渡って確認し、より詳細な結果を提示できるようになります。同様に、ターゲットに含まれる AWS リソースが評価の実行中により広く使用されているほど、Amazon Inspector はより詳細かつ包括的なテレメトリのセットを収集して分析します。
- Amazon Inspector 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
- Amazon Inspector の属性 (キーと値のペア): この評価テンプレートを使用する評価の実行で作成された結果を割り当てることができます。

Amazon Inspector が作成した評価テンプレートは、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 エディター」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。たとえば、Amazon Inspector には評価ターゲットを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 の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 サービスの制限 (p. 4)」を参照してください。

評価テンプレートを作成中

評価ターゲットテンプレートを作成するには

1. Sign in to the AWS マネジメントコンソール and open the Amazon Inspector console at https://console.aws.amazon.com/inspector/.
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

   [Assessment Templates (評価テンプレート)] ページの [Preview Target (ターゲットをプレビュー)] を使用して、評価ターゲットに含まれるすべての EC2 instances を確認できます。EC2 instance 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。エージェントステータスには、次の値があります。[HEALTHY (正常)]、[UNHEALTHY (異常)]、および [UNKNOWN (不明)]。[UNKNOWN (不明)] ステータスは EC2 instance で実行中のエージェントの有無を判断できない場合に Amazon Inspector に表示されます。
   また、[Assessment Templates (評価テンプレート)] ページの [Preview Target (プレビューターゲット)] 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 instances 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. [SNS トピック] では、Amazon Inspector で評価の実行の状態や結果についての通知の送信先となる SNS トピックを指定します。Amazon Inspector 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 通知用の SNS トピックを設定するには (p. 56)」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 (結果に追加された属性)] には、[Key (キー)] と [Value (値)] の値を入力します。Amazon Inspector は、評価テンプレートによって生成されたすべての検出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 の結果 (p. 58)」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 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 によって `AWS_InspectorEvents_Invoke_Assessment_Template` という IAM ロールも自動的に作成されます。このロールを使用して、CloudWatch イベント が Amazon Inspector のリソースに対して API コールを行うことができます。CloudWatch イベントと概念の詳細については、「Amazon CloudWatch Evente 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をセットアップする (p. 55)」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、[Yes] 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。AWS アカウントごとの評価の実行の制限を超えない限り、同じテンプレートを使用して複数の評価の実行を開始できます。詳細については、「Amazon Inspectorの評価の実行の制限 (p. 55)」を参照してください。

Amazon Inspector 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、[Run]、[Cancel]、[Delete] ボタンを [Assessment templates] ページまたは [Assessment runs] ページで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、[Yes] 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の評価の実行の制限

AWS アカウントごとに最大 50,000 の評価の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 instances 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 サービスの制限 (p. 4)」を参照してください。

Lambda 関数を使用した評価の自動実行をセットアップする

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 コンソールで Lambda 関数を作成して、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。

自動的な評価の実行をセットアップするには、AWS Lambda コンソールを使用して、以下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. AWS マネジメントコンソール にサインインして、AWS Lambda コンソールを開きます。
2. 左側の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、[Lambda 関数の作成] を選びます。
3. [Select blueprint] ページで [inspector-scheduled-run] 設計図を選択します。[フィルター] フィールドで「**`inspector`**」と入力して、この設計図を検索できます。
4. [Configure triggers (トリガーの設定)] ページで、関数をトリガーする CloudWatch イベントを指定して、自動的な評価の実行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 イベントおよび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。

5. [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。
   - [runtime (ランタイム)] は、デフォルト値のままにしておき、デフォルト値の **`Node.js 8.10`** をそのまま使用します。AWS Lambda は、**`Node.js 8.10`** ランタイムに対してのみ、[inspector-scheduled-run] 設計図をサポートします。
   - 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、AWS Lambda が実行を開始し、実行に関するログメッセージ (エラーを含む) を Amazon CloudWatch Logs に書き込むことを可能にする IAM ロールが必要です。AWS Lambda は、繰り返し実行される自動実行ごとにこのロールを引き受けます。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。

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

6. 場所を確認して [Create function] を選択します。

Amazon Inspector 通知用の SNS トピックを設定するには

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に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 の通知を設定できます。詳細については、「Amazon Simple Notification Service サービスとは?」を参照してください。

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。詳細については、「トピックの作成」を参照してください。

2. 作成した SNS トピックにサブスクライブします。詳細については、「トピックへのサブスクライブ」を参照してください。
3. SNS トピックに発行します。詳細については、「トピックへの発行」を参照してください。
4. Amazon Inspector にこのトピックへのメッセージの発行を許可:

   a. https://console.aws.amazon.com/sns/ で Amazon SNS コンソールを開きます。
   b. SNS トピックを選択し、[Actions (アクション)] の [Edit topic policy (トピックのポリシーの編集)] を選択します。
   c. [Allow these users to publish messages to this topic (次のユーザーにこのトピックへのメッセージの発行を許可)] で、[Only these AWS users (以下の AWS ユーザーのみ)] を選択します。リージョンに応じて、次の ARN のいずれかを入力します。

      - `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
      - `EU (Frankfurt)` - arn:aws:iam::537503971621:root
      - `EU (Ireland)` - arn:aws:iam::357557129151:root
      - `US East (Northern Virginia)` - arn:aws:iam::316112463485:root
      - `US East (Ohio)` - arn:aws:iam::646659390643:root
      - `US West (Northern California)` - arn:aws:iam::166987590008:root
      - `US West (Oregon)` - arn:aws:iam::758058086616:root
      - `AWS GovCloud (US-East)` - arn:aws-us-gov:iam::206278770380:root
      - `AWS GovCloud (US-West)` - arn:aws-us-gov:iam::850862329162:root

Amazon Inspector の結果

結果は、評価ターゲットの評価中に Amazon Inspector 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 コンソールに表示されるか、API を介して表示されます。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 の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 の結果で、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. Sign in to the AWS マネジメントコンソール and open the Amazon Inspector console at https://console.aws.amazon.com/inspector/.
2. 評価を実行したら、Amazon Inspector 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 コンソールの [Dashboard] ページの [Notable Findings] セクションにも表示されます。

   > **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 instance 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 of Internet Security (CIS) に基づくネイティブの重大度の詳細。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。[Tags for findings from this assessment (この評価から結果にタグ付する)] フィールドの [Key (キー)] フィールドと [Value (値)] フィールドを使用できます。詳細については、Amazon Inspector の評価テンプレートと評価の実行 (p. 52) 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。
6. 生成された結果の列を表示または非表示にするには、また生成された結果をフィルタリングするには、[結果] ページの右上隅にある設定の歯車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、[Delete] を選択します。確認を求めるメッセージが表示されたら、[Yes] を選択します。

   > **Important**
   >
   > Amazon Inspector 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 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 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 – このレポートには以下の情報が含まれています。
  - 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 – このレポートに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**
   >
   > 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。それが Amazon Inspector の評価レポートが利用可能になった時です。
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、[Yes] を選択します。

  > **Important**
  >
  > Amazon Inspector では、個別のレポート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 での除外

除外は Amazon Inspector の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。たとえば、指定されたターゲットの EC2 instance 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 (p. 68)」を参照してください。

不要な AWS の料金を支払わなくて済むよう、Amazon Inspector で評価の実行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 (p. 67)」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 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 (p. 61)
- 除外のプレビュー (p. 67)
- 評価後の除外の確認 (p. 68)

除外タイプ

Amazon Inspector で生成できる評価の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 instances 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 instance で評価の実行が既に進行中です。	ターゲット EC2 instance で現在進行中の評価の実行が完了するまで待ちます。								

除外タイプ	説明	推奨事項								
エージェントが見つからない	ターゲット EC2 instance で Amazon Inspector エージェントが見つかりませんでした。	ターゲット EC2 instance に Amazon Inspector 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 エージェントのインストール (p. 22)」を参照してください。								
エージェントが異常	ターゲット EC2 instance の Amazon Inspector 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 エージェントの状況を確認して、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								
カーネルモジュールを使用できない	ターゲット EC2 instance の Amazon Inspector エージェントでは、カーネルモジュールを使用できません。	サポート対象のカーネルバージョンのリストについては、「Amazon Inspector 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。								
サポート対象外の OS バージョン	Amazon Inspector の評価では、ターゲット EC2 instance 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 instance を削除するか、このインスタンスを含まない評価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 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。								
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 instance 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 instance 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。								

除外タイプ	説明	推奨事項								
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。								
Network 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。								
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 を介して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 Balancing 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て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。								
Network 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								
Network 到達可能性エラー – AWS Direct Connect	内部エラーにより、ネットワーク到達可能性の評価で、AWS Direct Connect を介した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。								
Network 到達可能性エラー – VPC ピア接続	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 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. Sign in to the AWS マネジメントコンソール and open the Amazon Inspector console at https://console.aws.amazon.com/inspector/.
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. Sign in to the AWS マネジメントコンソール and open the Amazon Inspector console at https://console.aws.amazon.com/inspector/.
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に関して、Amazon Inspector 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 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、どの EC2 instance でもネットワーク到達可能性 (p. 39)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 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 (p. 4)」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	実行時の動作の分析
Amazon Linux 2 LTS、2017.12	サポート対象		サポート対象	サポート対象	サポート対象
Amazon Linux 2018.03	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
Amazon Linux 2017.09	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
Amazon Linux 2017.03	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
Amazon Linux 2016.09	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
Amazon Linux 2016.03	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象

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	実行時の動作の分析
Amazon Linux 2015.09	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
Amazon Linux 2015.03	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
Amazon Linux 2014.09	サポート対象		サポート対象	サポート対象	
Amazon Linux 2014.03	サポート対象		サポート対象	サポート対象	
Amazon Linux 2013.09	サポート対象		サポート対象	サポート対象	
Amazon Linux 2013.03	サポート対象		サポート対象	サポート対象	
Amazon Linux 2012.09	サポート対象		サポート対象	サポート対象	
Amazon Linux 2012.03	サポート対象		サポート対象	サポート対象	
Ubuntu 18.04 LTS	サポート対象		サポート対象	サポート対象	サポート対象
Ubuntu 16.04 LTS	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
Ubuntu 14.04 LTS	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
Debian 9.0-9.5 8.0-8.7	サポート対象		サポート対象	サポート対象	

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	実行時の動作の分析
RHEL 7.6	サポート対象	サポート対象	サポート対象	サポート対象	
RHEL 6.2 - 6.9、7.2 - 7.5	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
CentOS 7.6	サポート対象	サポート対象	サポート対象	サポート対象	
CentOS 6.2 ~ 6.9、7.2 ~ 7.5	サポート対象	サポート対象	サポート対象	サポート対象	サポート対象
Windows Server 2012 R2	サポート対象	サポート対象	サポート対象		サポート対象
Windows Server 2012	サポート対象	サポート対象	サポート対象		サポート対象
Windows Server 2008 R2	サポート対象	サポート対象	サポート対象		サポート対象
Windows Server 2016 Base	サポート対象		サポート対象		サポート対象

AWS CloudTrail を使用した Amazon Inspector API 呼び出しの口グ作成

Amazon Inspector は AWS CloudTrail と統合されています。このサービスは、Amazon Inspector 内でユーザーやロール、または AWS のサービスによって実行されたアクションを記録するサービスです。CloudTrail は、Amazon Inspector コンソールからのコールや Amazon Inspector API オペレーションへのコードすべての呼び出しを含む、Amazon Inspector の API コールをイベントとしてキャプチャします。証跡を作成する場合は、Amazon Inspector 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。証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表示できます。CloudTrail によって収集された情報を使用して、リクエストの作成元の IP アドレス、リクエストの実行者、リクエストの実行日時などの詳細を調べて、Amazon Inspector に対してどのようなリクエストが行われたかを判断できます。

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

CloudTrail 内の Amazon Inspector 情報

CloudTrail は、アカウント作成時に AWS アカウントで有効になります。Amazon Inspector でアクティビティが発生すると、そのアクティビティは [Event history (イベント履歴)] の AWS の他のサービスのイベントとともに 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 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 は口グファイルを 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。証跡では、AWS パーティションのすべてのリージョンからのイベントが口グに記録され、指定した Amazon S3 バケットに口グファイルが配信されます。さらに、より詳細な分析と AWS 口グで収集されたデータに基づいた行動のためにその他の CloudTrail サービスを設定できます。詳細については、以下を参照してください。

- 証跡を作成するための概要
- CloudTrail でサポートされるサービスと統合
- CloudTrail の Amazon SNS 通知の設定
- 「複数のリージョンから CloudTrail 口グファイルを受け取る」と「複数のアカウントから CloudTrail 口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 オペレーションを記録します。

> Note
>
> CloudTrail は Amazon Inspector 読み取りオペレーションのリクエスト情報のみを口グに記録します。リクエストと応答の両方の情報が、他のすべての Amazon Inspector 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、リクエストの生成者に関する情報が含まれます。この ID 情報は以下のことを確認するのに役立ちます。

- リクエストが、ルートと AWS Identity and Access Management (IAM) ユーザー認証情報のどちらを使用して送信されたか
- リクエストが、ロールとフェデレーティッドユーザーのどちらの一時的なセキュリティ認証情報を使用して送信されたか
- リクエストが、別の AWS サービスによって送信されたかどうか

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

Amazon Inspector ログファイルエントリの概要

証跡は、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できる設定です。CloudTrail ログファイルには、1 つ以上のログエントリが含まれます。イベントは任意の送信元からの単一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、その他リクエストのパラメーター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。

以下の例は、Amazon Inspector `CreateResourceGroup` 操作を表す CloudTrail ログエントリを示しています。


```
{
    "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 のモニタリング

Amazon CloudWatch を使用して Amazon Inspector をモニタリングすることで、raw データを収集し、ほぼリアルタイムの読み取り可能なメトリクスに加工できます。デフォルトでは、Amazon Inspector 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 が CloudWatch に送信するメトリクスを一覧表示できます。

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 CloudWatch のメトリクス

Amazon Inspector 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			
`TotalAssessmentFindings`	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			
`TotalAssessmentRuns`	このテンプレートの評価の実行の数			
`TotalAssessmentFindings`	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			
TotalAssessmentRunsAWS	この AWS アカウントの評価の実行の数			

AWS CloudFormation の使用による Amazon Inspector の設定

AWS CloudFormation でサポートされている Amazon Inspector リソースに関するリファレンス情報については、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 ルールパッケージの ARN のリストについては、「ルールパッケージの Amazon Inspector ARN (p. 86)」を参照してください。

Amazon Inspector に対する認証とアクセスコントロール

Amazon Inspector へのアクセスには、リクエストを認証するために AWS によって使用される認証情報が必要です。これらの認証情報には、Amazon Inspector の評価ターゲット、評価テンプレート、結果などの AWS リソースにアクセスするためのアクセス許可が必要です。次のセクションでは、AWS Identity and Access Management (IAM) と Amazon Inspector を使用して、リソースにアクセスできるユーザーを制御することで、リソースをセキュリティで保護する方法について詳しく説明します。

- 認証 (p. 78)
- アクセスコントロール (p. 79)

認証

AWS には、次のタイプのアイデンティティでアクセスできます。

- AWS アカウントのルートユーザー – AWS アカウントを初めて作成する場合は、このアカウントのすべての AWS サービスとリソースに対して完全なアクセス権限を持つシングルサインインアイデンティティで始めます。このアイデンティティは AWS アカウント ルートユーザー と呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでのサインインによりアクセスします。強くお勧めしているのは、日常的なタスクには、それが管理者タスクであっても、ルートユーザーを使用しないことです。代わりに、最初の IAM ユーザーを作成するためだけに ルートユーザー を使用するというベストプラクティスに従います。その後、ルートユーザー認証情報を安全な場所に保管し、それらを使用して少数のアカウントおよびサービス管理タスクのみを実行します。
- IAM ユーザー – IAM ユーザーは、特定のカスタム権限 (たとえば、AWS Directory Service で a directory を作成するアクセス権限) を持つ AWS アカウント内のアイデンティティです。IAM のユーザー名とパスワードを使用して、AWS マネジメントコンソール、AWS ディスカッションフォーラム、AWS Support Center などのセキュリティ保護された AWS ウェブページにサインインできます。

  ユーザー名とパスワードに加えて、各ユーザーのアクセスキーを生成することもできます。いくつかの SDK の 1 つまたは AWS Command Line Interface (CLI) を使ってプログラムで AWS サービスにアクセスするときに、これらのキーを使用できます。SDK と CLI ツールでは、アクセスキーを使用してリクエストが暗号で署名されます。AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。AWS Directory Service supports では、署名バージョン 4 がサポートされています。これは、インバウンド API リクエストを認証するためのプロトコルです。リクエストの認証の詳細については、『AWS General Reference』の「署名バージョン 4 の署名プロセス」を参照してください。

- IAM ロール – IAM ロールは、特定のアクセス権限を持ち、アカウントで作成できる IAM アイデンティティです。IAM ロールは、AWS で許可/禁止する操作を決めるアクセス権限ポリシーが関連付けられている AWS アイデンティティであるという点で、IAM ユーザーと似ています。ただし、ユーザーは 1 人の特定の人に一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。また、ロールには標準の長期認証情報 (パスワードやアクセスキーなど) も関連付けられません。代わりに、ロールを引き受けると、ロールセッション用の一時的なセキュリティ認証情報が提供されます。 IAM ロールと一時的な認証情報は、次の状況で役立ちます。

- フェデレーティッドユーザーアクセス – IAM ユーザーを作成する代わりに、AWS Directory Service、エンタープライズユーザーディレクトリ、またはウェブ ID プロバイダーに既存のアイデンティティを使用できます。このようなユーザーはフェデレーティッドユーザーと呼ばれます。AWS では、ID プロバイダーを通じてアクセスがリクエストされたとき、フェデレーティッドユーザーにロールを割り当てます。フェデレーティッドユーザーの詳細については、IAM ユーザーガイドの「フェデレーティッドユーザーとロール」を参照してください。

- AWS のサービスのアクセス – サービスロールは、サービスがお客様に代わってお客様のアカウントでアクションを実行するために引き受ける IAM ロールです。一部の AWS のサービス環境を設定するときに、サービスが引き受けるロールを定義する必要があります。このサービスロールには、サービスが必要とする AWS のリソースにサービスがアクセスするために必要なすべてのアクセス権限を含める必要があります。サービスロールはサービスによって異なりますが、多くのサービスロールでは、そのサービスの文書化された要件を満たしている限り、アクセス権限を選択することができます。サービスロールは、お客様のアカウント内のみでアクセスを提供します。他のアカウントのサービスへのアクセス権を付与するためにサービスロールを使用することはできません。IAM 内部からロールを作成、修正、削除できます。たとえば、Amazon Redshift がお客様に代わって Amazon S3 バケットにアクセスし、バケットからデータを Amazon Redshift クラスターにロードすることを許可するロールを作成できます。詳細については、IAM ユーザーガイドのAWS サービスにアクセス権限を委任するロールの作成を参照してください。

- Amazon EC2 で実行中のアプリケーション – IAM ロールを使用して、EC2 インスタンスで実行され、AWS CLI または AWS API リクエストを作成しているアプリケーションの一時的な認証情報を管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。AWS ロールを EC2 インスタンスに割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時認証情報を取得することができます。詳細については、IAM ユーザーガイドの「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用してアクセス権限を付与する」を参照してください。

アクセスコントロール

有効な認証情報があればリクエストを認証できますが、アクセス許可を持っていないかぎり Amazon Inspector リソースの作成やアクセスはできません。たとえば、評価の実行を開始するには、Amazon Inspector の評価ターゲットおよび評価テンプレートを作成するアクセス許可が必要です。

以下のセクションでは、Amazon Inspector のアクセス許可を管理する方法について説明します。最初に概要のセクションを読むことをお勧めします。

- Amazon Inspector リソースに対するアクセス許可の管理の概要 (p. 79)
- Amazon Inspector でアイデンティティベースのポリシー (IAM ポリシー) を使用する (p. 83)
- Amazon Inspector API のアクセス権限: アクション、リソース、条件リファレンス (p. 85)

Amazon Inspector リソースに対するアクセス許可の管理の概要

すべての AWS リソースは AWS アカウントによって所有され、リソースの作成またはアクセスは、AWS Identity and Access Management (IAM) アクセス権限のポリシーによって管理されます。アカウント管理者は、IAM ID (ユーザー、グループ、ロール) にアクセス権限ポリシーをアタッチできます。一部のサービス (AWS Lambda など) は、アクセス許可ポリシーをリソースにアタッチすることができます。

Note

アカウント管理者 (または管理者ユーザー) は、管理者権限を持つ IAM ユーザーです。詳細については、『IAM ユーザーガイド』の「IAM のベストプラクティス」を参照してください。

アクセス権限を付与する場合、アクセス権限を取得するユーザー、取得するアクセス権限の対象となるリソース、およびそれらのリソースに対して許可される特定のアクションを決定します。

トピック

- Amazon Inspector リソースおよびオペレーション (p. 80)
- リソース所有権について (p. 80)
- リソースへのアクセスの管理 (p. 81)
- ポリシー要素の指定 : アクション、効果、リソース、プリンシパル (p. 82)
- ポリシーでの条件の指定 (p. 82)

Amazon Inspector リソースおよびオペレーション

Amazon Inspector では、プライマリリソースはリソースグループ、評価ターゲット、評価テンプレート、評価の実行、および結果です。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
Resource Group	`arn:aws:inspector:region:account-id:resourcegroup/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`

Amazon Inspector には、Amazon Inspector リソースを操作するための一連のオペレーションが用意されています。可能なオペレーションのリストについては、「アクション」を参照してください。

リソース所有権について

リソース所有者は、リソースを作成する AWS アカウントです。つまり、リソース所有者は、リソースの作成リクエストを認証するプリンシパルエンティティ (ルートアカウント、IAM ユーザー、または IAM ロール) の AWS アカウントです。以下の例では、このしくみを示しています。

- AWS アカウントの root アカウントの認証情報を使用して Amazon Inspector 評価ターゲットを作成する場合、AWS アカウントはこのリソースの所有者です。
- AWS アカウントに IAM ユーザーを作成し、そのユーザーに 評価ターゲットを作成するためのアクセス許可を付与する場合、そのユーザーはターゲットを作成できます。ただし、ユーザーが属する AWS アカウントは評価ターゲットリソースを所有しています。
- 評価ターゲットを作成するためのアクセス許可を持つ AWS アカウントに IAM ロールを作成する場合は、ロールを引き受けることのできるいずれのユーザーもターゲットを作成できます。ただし、ユーザーが属する AWS アカウントは Amazon Inspector 評価ターゲットリソースを所有しています。

リソースへのアクセスの管理

アクセスポリシーでは、誰が何にアクセスできるかを記述します。 以下のセクションで、アクセス許可のポリシーを作成するために使用可能なオプションについて説明します。

> Note
>
> このセクションでは、Amazon Inspector のコンテキストでの IAM の使用について説明します。これは、IAM サービスに関する詳細情報を取得できません。完全な IAM ドキュメントについては、IAM ユーザーガイドの「IAM とは?」を参照してください。IAM ポリシー構文の詳細および説明については、『IAM ユーザーガイド』の「AWS IAM ポリシーリファレンス」を参照してください。

IAM ID にアタッチされているポリシーは、アイデンティティベースのポリシー (IAM ポリシー) と呼ばれます。リソースにアタッチされたポリシーはリソースベースのポリシーと呼ばれます。Amazon Inspector では、アイデンティティベースのポリシーのみがサポートされています。

トピック

- アイデンティティベースのポリシー (IAM ポリシー) (p. 81)
- リソースベースのポリシー (p. 82)

アイデンティティベースのポリシー (IAM ポリシー)

ポリシーを IAM アイデンティティにアタッチできます。たとえば、次の操作を実行できます。

- アカウントのユーザーまたはグループにアクセス許可ポリシーをアタッチする – アカウント管理者は、特定のユーザーに関連付けられるアクセス許可ポリシーを使用して、そのユーザーに IAM 評価ターゲットの作成を許可するアクセス許可を付与することができます。
- アクセス権限ポリシーをロールにアタッチする (クロスアカウントのアクセス権限を付与する) – アイデンティティベースのアクセス権限ポリシーを IAM ロールにアタッチして、クロスアカウントのアクセス権限を付与することができます。たとえば、アカウント A の管理者は、次のように別の AWS アカウント (たとえば、アカウント B) または AWS サービスにクロスアカウントアクセス許可を付与するロールを作成できます。
  - アカウント A の管理者は、IAM ロールを作成して、アカウント A のリソースにアクセス許可を付与するロールに権限ポリシーをアタッチします。
  - アカウント A の管理者は、アカウント B をそのロールを引き受けるプリンシパルとして識別するロールに、信頼ポリシーをアタッチします。
  - アカウント B の管理者は、アカウント B の任意のユーザーにロールを引き受けるアクセス許可を委任できるようになります。これにより、アカウント B のユーザーにアカウント A のリソースの作成とアクセスが許可されます。AWS のサービスにロールを引き受けるアクセス許可を付与する場合は、信頼ポリシーのプリンシパルは AWS のサービスのプリンシパルともなることができます。

  IAM を使用したアクセス許可の委任の詳細については、『IAM ユーザーガイド』の「アクセス管理」を参照してください。

すべてのリソースの `inspector:ListFindings` オペレーションのアクセス許可を付与するポリシーの例を次に示します:

```
                {
"Version": "2012-10-17",
"Statement": [
    {
        "Effect": "Allow",
        "Action": [
```

```
                "inspector:ListFindings"
            ],
            "Resource": "*"
        }
    ]
}
```

Amazon Inspector でアイデンティティベースのポリシーを使用する方法の詳細については、「Amazon Inspector でアイデンティティベースのポリシー (IAM ポリシー) を使用する (p. 83)」を参照してください。ユーザー、グループ、ロール、アクセス権限の詳細については、IAM ユーザーガイド の「アイデンティティ (ユーザー、グループ、ロール)」を参照してください。

リソースベースのポリシー

Amazon S3 などの他のサービスでは、リソースベースのアクセス許可ポリシーもサポートされています。たとえば、ポリシーを S3 バケットにアタッチして、そのバケットに対するアクセス権限を管理できます。Amazon Inspector はリソースベースのポリシーをサポートしていません。

ポリシー要素の指定 : アクション、効果、リソース、プリンシパル

Amazon Inspector リソースごとに (「Amazon Inspector リソースおよびオペレーション (p. 80)」を参照) 、サービスは一連の API オペレーションを定義します (「アクション」を参照) 。これらの API オペレーションのアクセス権限を付与するために、Amazon Inspector は、ポリシー内に指定できる一連のアクションを定義します。1 つの API オペレーションの実行で、複数のアクションのアクセス権限が必要になる場合があります。特定のアクションのアクセス権限を付与した場合は、アクションを許可または拒否するリソースを識別します。

以下は、最も基本的なポリシーの要素です。

- リソース – ポリシーで Amazon Resource Name (ARN) を使用して、ポリシーを適用するリソースを識別します。詳細については、「Amazon Inspector リソースおよびオペレーション (p. 80)」を参照してください。
- アクション – アクションのキーワードを使用して、許可または拒否するリソースオペレーションを識別します。たとえば、`inspector:ListFindings` 権限は、Amazon Inspector `ListFindings` オペレーションの実行をユーザーに許可します。
- 効果 – ユーザーが特定のアクションをリクエストするときの効果を指定します。effect は、Allow または Deny にすることができます。リソースへのアクセスを明示的に許可していない場合、アクセスは暗黙的に拒否されます。リソースへのアクセスを明示的に拒否することもできます。これにより、別のポリシーでアクセスが許可されている場合でも、ユーザーがリソースにアクセスすることを禁止できます。
- プリンシパル – アイデンティティベースのポリシー (IAM ポリシー) で、ポリシーがアタッチされているユーザーが黙示的なプリンシパルとなります。

IAM ポリシーの構文と説明の詳細については、『IAM ユーザーガイド』の「AWS IAM ポリシーを参照」を参照してください。

すべての Amazon Inspector API アクションとそれらが適用されるリソースの表については、「Amazon Inspector API のアクセス権限: アクション、リソース、条件リファレンス (p. 85)」を参照してください。

ポリシーでの条件の指定

アクセス許可を付与するとき、IAM ポリシー言語を使用して、ポリシーを有効にするために満たす必要がある条件を指定できます。たとえば、特定の日付の後にのみ適用されるポリシーが必要になる場合があり

ます。ポリシー言語での条件の指定の詳細については、『IAM ユーザーガイド』の「条件」を参照してください。

条件を表すには、あらかじめ定義された条件キーを使用します。Amazon Inspector に固有の条件キーはありません。ただし、AWS の条件キーを必要に応じて使用できます。AWS 全体を対象とするすべてのキーのリストについては、『IAM ユーザーガイド』の「条件に利用可能なキー」を参照してください。

Amazon Inspector でアイデンティティベースのポリシー (IAM ポリシー) を使用する

この章では、ID ベースの アクセス許可ポリシー (IAM ポリシーとも呼ばれます) の例を示します。アカウント管理者は、IAM ID (ユーザー、グループ、ロール) にアクセス権限ポリシーをアタッチできます。

> Important
>
> 初めに、Amazon Inspector リソースへのアクセスを管理するための基本概念と使用可能なオプションについて説明する概要トピックをお読みになることをお勧めします。詳細については、「Amazon Inspector リソースに対するアクセス許可の管理の概要 (p. 79)」を参照してください。

この章のこのセクションでは、次のトピックを対象としています。

- Amazon Inspector コンソールを使用するために必要なアクセス権限 (p. 83)
- Amazon Inspector での AWS 管理 (事前定義) ポリシー (p. 84)
- お客様が管理するポリシーの例 (p. 84)

以下は、アクセス権限ポリシーの例です。

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

このサンプルポリシーには、Amazon Inspector の結果をリストするアクセス許可を付与するステートメントが含まれています。Amazon Inspector は、この特定のアクションに対するリソースレベルでのアクセス許可をサポートしていません。したがって、ポリシーでは `Resource` の値としてワイルドカード文字 (*) を指定します。

Amazon Inspector コンソールを使用するために必要なアクセス権限

Amazon Inspector コンソールを使用するには、ユーザーには「Amazon Inspector での AWS 管理 (事前定義) ポリシー (p. 84)」で説明されている `AmazonInspectorFullAccess` または

AmazonInspectorReadOnlyAccess ポリシーで付与されるアクセス許可が必要です。これらのいずれかのポリシーで示されている、最小限必要なアクセス許可よりも制限の高い IAM ポリシーを作成した場合 (前述の例のポリシー)、コンソールはそのポリシーを使用するユーザーに対して目的どおりに機能しません。

> Note
>
> 前述の例のポリシーがアタッチされた IAM ユーザーは、ListFindings API オペレーションまたは list-findings CLI コマンドを呼び出して、Amazon Inspector の結果を正しく一覧表示できます。

Amazon Inspector での AWS 管理 (事前定義) ポリシー

AWS は、AWS によって作成され管理されるスタンドアロンの IAM ポリシーが提供する多くの一般的ユースケースに対応します。これらの管理ポリシーは、一般的ユースケースに必要なアクセス権限を付与することで、どの権限が必要なのかをユーザーが調査する必要をなくすことができます。詳細については、『IAM ユーザーガイド』の「AWS 管理ポリシー」を参照してください。

アカウントの IAM ユーザーにアタッチ可能な以下の AWS 管理ポリシーは、Amazon Inspector に固有のものです。

- AmazonInspectorFullAccess – Amazon Inspector へのフルアクセスを提供します。
- AmazonInspectorReadOnlyAccess – Amazon Inspector への読み取り専用アクセスを許可します。

また、ユーザーが必要な API オペレーションおよびリソースにアクセスできるカスタム IAM ポリシーを作成できます。これらのカスタムポリシーは、それらのアクセス許可が必要な IAM ユーザーまたはグループにアタッチできます。

お客様が管理するポリシーの例

このセクションでは、さまざまな Amazon Inspector オペレーションのアクセス許可を付与するユーザーポリシー例を示しています。

> Note
>
> すべての例で、米国西部 (オレゴン) リージョン (us-west-2) を使用し、架空のアカウント ID を使用しています。

例

- 例 1: Amazon Inspector リソースに対する任意の Describe および List オペレーションの実行をユーザーに許可する (p. 84)
- 例 2: Amazon Inspector の結果に対する 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 (p. 85)

例 1: Amazon Inspector リソースに対する任意の Describe および List オペレーション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、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、割り当てのターゲットや結果など、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。

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

例 2: Amazon Inspector の結果に対する 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。

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

Amazon Inspector API のアクセス権限: アクション、リソース、条件リファレンス

以下のテーブルに、各 Amazon Inspector API オペレーションを示します。アクションを実行するためのアクセス許可を付与できる対応するアクション、およびアクセス許可を付与できる AWS リソースを示しています。アクセスコントロール (p. 79) をセットアップし、IAM アイデンティティ (アイデンティティベースのポリシー) にアタッチできるアクセス許可ポリシーを作成する際、次の表を参考にできます。ポリシーの `Action` フィールドでアクションを指定し、ポリシーの `Resource` フィールドでリソースの値を指定します。

Amazon Inspector ポリシーで AWS 条件キーを使用して、条件を表現することができます。AWS 全体を対象とするすべてのキーのリストについては、『IAM ユーザーガイド』の「条件に利用可能なキー」を参照してください。

> **Note**
>
> アクションを指定するには、`inspector:` プレフィックスに続けて API オペレーション名を使用します (例: `inspector:CreateResourceGroup`)。

ルールパッケージの Amazon Inspector 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 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

- 米国西部 (オレゴン) (p. 86)
- 米国東部 (バージニア北部) (p. 87)
- 米国東部 (オハイオ) (p. 87)
- 米国西部 (北カリフォルニア) (p. 88)
- アジアパシフィック (ムンバイ) (p. 88)
- アジアパシフィック (シドニー) (p. 89)
- アジアパシフィック (ソウル) (p. 89)
- アジアパシフィック (東京) (p. 90)
- 欧州 (アイルランド) (p. 90)
- 欧州 (フランクフルト) (p. 91)
- AWS GovCloud (米国東部) (p. 91)
- AWS GovCloud (米国西部) (p. 92)

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	
実行時の動作の分析	arn:aws:inspector:us-west-2:758058086616:rulespackage/0-vg5GGHSD	

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	
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	
実行時の動作の分析	arn:aws:inspector:us-east-1:316112463485:rulespackage/0-gBONHN9h	

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	
実行時の動作の分析	arn:aws:inspector:us-east-2:646659390643:rulespackage/0-UCYZFKPV	

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	
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	
実行時の動作の分析	arn:aws:inspector:us-west-1:166987590008:rulespackage/0-yeYxlt0x	

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	
実行時の動作の分析	arn:aws:inspector:ap-south-1:162588757376:rulespackage/0-EhMQZy6C	

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-2:454640832652:rulespackage/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-2:454640832652:rulespackage/0-Vkd2Vxjq	
ネットワーク到達可能性	arn:aws:inspector:ap-southeast-2:454640832652:rulespackage/0-FLcuV4Gz	
セキュリティのベストプラクティス	arn:aws:inspector:ap-southeast-2:454640832652:rulespackage/0-asL6HRgN	
実行時の動作の分析	arn:aws:inspector:ap-southeast-2:454640832652:rulespackage/0-P8Tel2Xj	

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-2:526946625049:rulespackage/0-T9srhg1z	
ネットワーク到達可能性	arn:aws:inspector:ap-northeast-2:526946625049:rulespackage/0-s3OmLzhL	
セキュリティのベストプラクティス	arn:aws:inspector:ap-northeast-2:526946625049:rulespackage/0-2WRpmi4n	
実行時の動作の分析	arn:aws:inspector:ap-northeast-2:526946625049:rulespackage/0-PoYq7lI7	

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-1:406045910587:rulespackage/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-1:406045910587:rulespackage/0-7WNjqgGu	
ネットワーク到達可能性	arn:aws:inspector:ap-northeast-1:406045910587:rulespackage/0-YI95DVd7	
セキュリティのベストプラクティス	arn:aws:inspector:ap-northeast-1:406045910587:rulespackage/0-bBUQnxMq	
実行時の動作の分析	arn:aws:inspector:ap-northeast-1:406045910587:rulespackage/0-knGBhqEu	

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-1:357557129151: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	
実行時の動作の分析	arn:aws:inspector:eu-west-1:357557129151:rulespackage/0-lLmwe1zd	

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-1:537503971621: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	
実行時の動作の分析	arn:aws:inspector:eu-central-1:537503971621:rulespackage/0-0GMUM6fg	

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-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	
実行時の動作の分析	arn:aws-us-gov:inspector:us-gov-east-1:206278770380:rulespackage/0-850TmCFX	

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	
実行時の動作の分析	arn:aws-us-gov:inspector:us-gov-west-1:850862329162:rulespackage/0-JMyjuzoW	

ドキュメント履歴

文書の最終更新: 2018 年 11 月 12 日

次の表は、2018 年 5 月以降の Amazon Inspector ドキュメントのリリース履歴をまとめたものです。

update-history-change	update-history-description	update-history-date
OS サポートの追加 (p. 93)	CentOS 7.6 の Amazon Inspector サポートを追加しました。詳細については、「Amazon Inspector 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に関して、提供されているルールパッケージ」を参照してください。	December 3, 2018
新しいコンテンツ (p. 93)	Amazon Inspector 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。	November 9, 2018
OS サポートの追加 (p. 93)	RHEL 7.6 の Amazon Inspector サポートが追加されました。詳細については、「Amazon Inspector 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に関して、提供されているルールパッケージ」を参照してください。	October 30, 2018
OS サポートの追加 (p. 93)	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。	August 13, 2018
リージョンサポートの追加 (p. 93)	`AWS GovCloud (US)` のリージョンサポートの追加	June 13, 2018

次の表は、2018 年 6 月以前の Amazon Inspector 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 の評価ターゲット (p. 35)」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 の Amazon Inspector 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	反復的な Amazon Inspector の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	コンソールを通じて Amazon Inspector 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 の Amazon Inspector サポートの追加	2018 年 3 月 13 日
OS サポートの追加	Windows Server 2016 Base の Amazon Inspector の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の追加	Amazon Inspector に、`US East (Ohio)` リージョンのサポートが追加されました。	2018 年 2 月 7 日
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 の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の追加	Amazon Inspector に、`EU (Frankfurt)` リージョン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 の API とコンソールで Amazon Inspector 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 で入手できる Amazon Inspector エージェントの AMI • Amazon Inspector AWS CloudFormation テンプレート	2017 年 5 月 12 日

変更	説明	日付
OS サポートの追加	CentOS 7.4 の Amazon Inspector の評価のサポートが追加されました。	2017 年 11 月 9 日
OS サポートの追加	Amazon Linux 2017.09 の Amazon Inspector の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 の Amazon Inspector の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 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 イベントによって Amazon Inspector 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 27 月 7 日
リージョンサポートの追加	Amazon Inspector に、`US West (N. California)` リージョン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 の Amazon Inspector の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 の Amazon Inspector の評価のサポートが追加されました。	2017 年 4 月 25 日
新しいコンテンツと OS サポートの追加	以下を追加。 • Ubuntu 16.04 の Amazon Inspector のサポート。 • Amazon Inspector のオペレーションを自動化するための Lambda 設計図の使用	2017 年 1 月 5 日
新しい OS サポート	Microsoft Windows の Amazon Inspector 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の追加	Amazon Inspector に、`Asia Pacific (Seoul)` リージョン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の追加	Amazon Inspector に、`Asia Pacific (Mumbai)` リージョンのサポートが追加されました。	2016 年 4 月 25 日

変更	説明	日付
リージョンサポートの追加	Amazon Inspector に、`Asia Pacific (Sydney)` リージョン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 のサービスの提供が開始されました。	2015 年 10 月 7 日

AWS の用語集

最新の AWS の用語については、『AWS General Reference』の「AWS の用語集」を参照してください。